Created: 5 October 2011
Last Revised: 8 August 2012
Document Revision 1.5

Cherry Bomb:
System Requirements Specification Document
For Contract Year 2011-2012

For Cherry Blossom Version 5.0

(CDRL 10)
(U)

Prepared by:
XXXXX Y
XXXXX Y
XXXXX Y
XXXXX Y
XXXXX Y
XXXXX Y

Prepared for:
US Government

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

Document No. SLO-FF-2012-176
Copy No. 1 of 1

_

Version	Description of Document Version	Date Completed
1.0	Initial draft – created after numerous meetings and discussions with COTR, sponsor staff, operational personnel, and contractor personnel.	5 October 2011
1.1	Update based on internal review comments	10 October 2011
1.2	Update based on Sponsor review comments	14 Feb 2012
1.3	Added CB v5.0 info	6 March 2012
1.4	Minor grammatical error corrections	19 July 2012
1.5	Updated per reviewers comments	8 August 2012

1 (U) Introduction

(U) This document specifies the requirements for the Cherry Blossom (CBlossom) project of the Cherry Bomb (CBomb) program for the contract year 2011-2012.

(S) The focus of CBlossom is to develop implanted firmware for wireless networking devices, including wireless access points (APs) and routers. An implanted device can then be used to monitor the internet activity of and deliver software exploits to targets of interest. It should be noted, however, that the CBlossom architecture does not limit itself to wireless devices – in general, wired network devices could be implanted/compromised in the same fashion to achieve the same goals.

(U) This document is for CBlossom version 5.0. CBlossom version 5.0 will include new releases of the CBlossom Flytrap and Cherry Tree products, each being referred to as version 5.0. CBlossom version 5.0 will be derived from the last FAT tested versions of the CBlossom Flytrap and Cherry Tree products (see the *Cherry Bomb Configuration Management Plan [CDRL 2]* for detailed info on Cherry Bomb products and product versions).

(U) This document should be used in conjunction with *Cherry Blossom: Requirements Verification Traceability Matrix* [CDRL 11], which shall be updated to reflect the additional requirements described herein.

2 (U) Related Documents

(S) The following documents, of the exact issue shown, form a part of this specification to the extent specified herein. In the event of a conflict between the documents referenced herein and the contents of this specification, the contents of this specification will be considered a superseding requirement. The following documents may be found within S:\DO\IOC\EDG ALL\EDG ES\EDG_ES_Wireless and Geolocation Branch\03_Projects\Branch Teams\:

1. Cherry Blossom System Requirements Specification Document [CDRL 10]: "CherryBlossom_SystemSpecDoc_CDRL-10_SLO-FF-(most recent version).doc"
2. Cherry Blossom FAT Procedures [CDRL 14]: "CherryBlossom_FATProcedures_CDRL-14.doc" (most recent version)
3. Cherry Blossom User's Manual [CDRL 12]: "CherryBlossom_UsersManual_CDRL-12_SLO-FF-(most recent version).doc"
4. Cherry Bomb Configuration Management Plan [CDRL 2]: "CherryBomb_ConfigMgmtPlan_CDRL-2.doc" (most recent version)
5. Cherry Blossom User's Manual [CDRL 12]: "CherryBlossom_UsersManual_CDRL-12_SLO-FF-(most recent version).doc"
6. Cherry Blossom: Requirements Verification Traceability Matrix [CDRL 11]: "CherryBlossom_RVTMatrix_CDRL-11_SLO-FF-(most recent version).doc"
7. (S) Tradecraft Guidelines for ESD/WGB Implant and Exploit Developments (Rev 1.0 dated 25 November 2009)

3 (U) Architecture and Definitions

(U) This section discusses the architecture of the Cherry Blossom system, and defines a number of terms used throughout the document. For a more complete system description, see the Cherry Blossom User's Manual [CDRL 12]

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

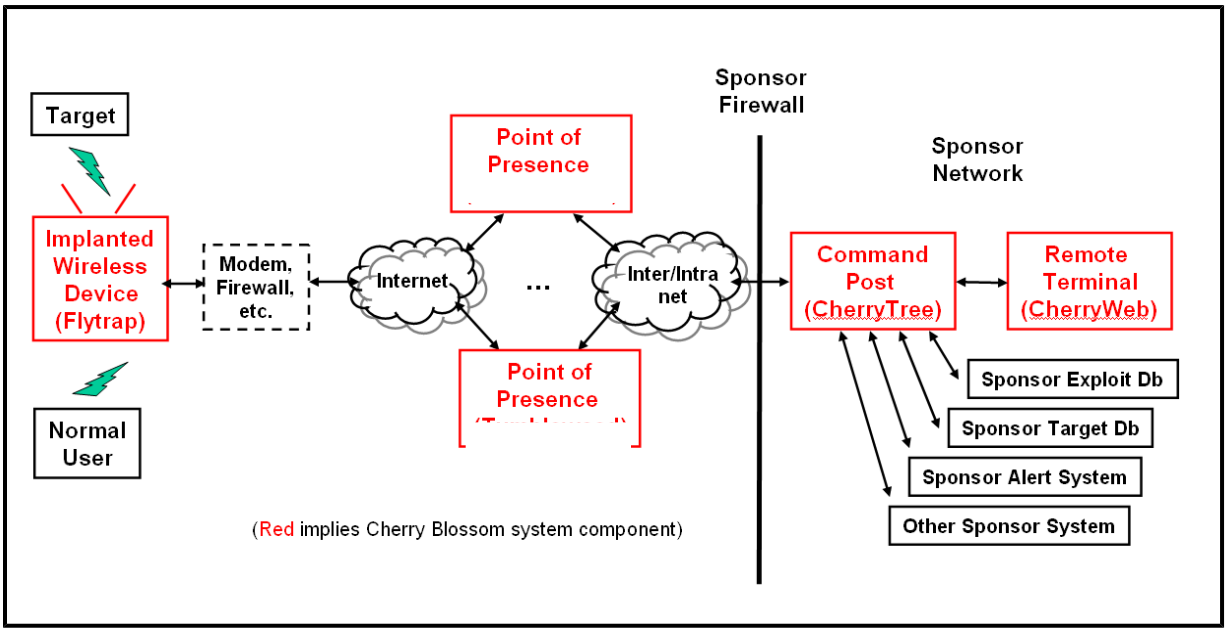

Figure 1: Cherry Blossom Architecture (U)

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

- **(S) Flytrap** – a wireless access point (AP), router, or other device that has been implanted with Cherry Blossom firmware. Flytraps execute Missions to detect and exploit Targets
- **(U) Command Post (Cherry Tree or CT)** – server/software that manages:
  - Handling and storage of Flytrap Missions
  - Handling and storage of Flytrap status
  - Handling, storage, and further distribution of Flytrap Alerts
- **(U) Remote Terminal (CherryWeb or CW)** – browser-based interface that allows Sponsor users to view system status, configure the system, view target activity, and plan/assign Missions
- **(U) Point of Presence (PoP) or Listening Post (LP)** – relay that forwards communication between a Flytrap and the Cherry Tree
- **(U) User** – a person with access to the Cherry Web Remote Terminal. Users, for example, can log into CW, plan and assign Missions, view system status, etc.

- **(S) Target** – a computer/person that should be monitored and at which exploits should be targeted. Flytraps use MAC address, email address, or chat username to detect/identify Targets
- **(U) Target Deck** – a grouping of related Targets
- **(U) Mission** – tasking and Target data given to a Flytrap in response to a Beacon
- **(U) Operation (formerly Customer)** – a CherryWeb-defined entity around which Cherry Blossom system data is organized and to which this data is reported. System data can be compartmentalized according to Operation via assigning permissions to a User on a per-Operation basis.
- **(U) Beacon** – 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 gives the Flytrap a Mission.
- **(U) Alert** – a communication sent from a Flytrap to the CT when the Flytrap has detected Target activity
- **(U) One-way Transfer** – a process of packaging and moving Cherry Blossom system data to a secure computer.
- **(U) Flash** – (noun) non-volatile RAM where the system image and persistent configuration data is typically stored on devices
- **(U) Flash/Reflash** – (verb) the process of upgrading a device with a new firmware image.

(S) The key element of the Cherry Blossom system is the Flytrap. In typical operation, a wireless device of interest is implanted with Cherry Blossom firmware, either using the Claymore tool or via a supply chain operation. After implanting has occurred, the wireless device is known as a Flytrap. The Flytrap will send a Beacon (according to parameters specified at Flytrap implant build time) to the CT to report status and retrieve a Mission. The CT logs all Beacon information (status info and security settings) from a Flytrap to a local database. Flytrap status, security info, etc. can be viewed using the web browser-based Remote Terminal (Cherry Web) user interface. All communications between a Flytrap and the CT are done through Sponsor-maintained PoP's.

(S) A Mission includes instructions on Targets to monitor, exploits to perform on a Target (e.g., copy traffic, proxy traffic, redirect browser), and instructions on when and how to send the next Beacon and retrieve the next Mission. Targets typically include email addresses, chat usernames, and MAC addresses (Roundhouse devices also support VoIP addresses). Missions are created using the web browser-based Remote Terminal (Cherry Web) user interface.

(S) Upon receipt of a Mission, a Flytrap will begin Mission execution, typically configuring the necessary software modules on the Flytrap, running the necessary applications, etc. This includes configuring the software to detect Target network activity and direct exploits at Targets. When the Flytrap detects a Target it performs any Mission-configured exploits against that Target and sends an Alert to the CT. The CT will log the Alert to a local database, and, potentially distribute Alert information to interested parties (via sending an email to Catapult). Detailed Alert information can be viewed with Cherry Web.

4 (U) Cherry Blossom General System Requirements

(U) This section enumerates the general requirements of the Cherry Blossom system for the contract year 2011-2012. These are broad requirements intended to give general guidance to system design and development.

4.1 (U) Cherry Tree Requirements

(U) Two major Cherry Tree enhancements shall be provided in this contract period: a new algorithm for selecting LPs, and the capability to edit active Flytrap missions. In addition, changes to the Windex connection logic and a mobile VPN server capability shall also be provided. Depending upon difficulties encountered, these enhancements shall be delivered in one release or spread across two releases.

4.1.1 (S) Algorithm for Selecting LPs

(S) Cherry Tree shall provide the capability to disable use of the default (firmware embedded) LP for a deployed Flytrap. This disable operation shall be in the form of an operator-configurable mission flag which specifies either to use or not to use the embedded beacon address. Cherry Web shall force a user to provide a PoP/LP in a mission if the default LP is to be disabled in the mission.

4.1.2 (S) Windex Connection

(S) The current Windex connection logic shall be removed from the Cherry Tree code. This change shall involve the removal of the “Administer->Windex” and the “Plan->Exploits->Windex” pages.

(S) Cherry Tree shall continue to show Windex information (redirect status, client IP, original Web page) received from Flytraps.

4.1.3 (U) Mobile VPN Server

(U) Cherry Tree shall provide a mobile VPN server capability using the Fedora Core 10 operating system.

(U) The current FAT VPN tests shall also be performed on the mobile VPN server.

(U) The proper internet setup (e.g. VPNC), installation, and auto start capability shall be tested on the mobile VPN server.

4.1.4 (U) Target Decks with Persistent Actions

(U) Cherry Tree shall improve the ability to persist Target Actions in Missions when an associated Target Deck is changed. If new Targets are added to a Target Deck via the

"Plan->Target Decks" link, the user will be prompted for the Actions to associate with each of those Targets. Cherry Tree will then automatically create a new Mission revision, incorporating the new Targets and Target Actions, and automatically assign this new Mission revision to any Flytraps currently executing the Mission.

4.1.5 (U) One-Way Transfer Reports

(U) Cherry Tree shall provide the capability to run the current one-way transfer scripts from Cherry Web, which shall cause the creation of a file containing the desired data as is the case when the scripts are run from the command line.

(U) It shall be possible to display the file name and status of one-way transfer data in the Cherry Web interface. This shall augment the existing capability to write one-way transfer data to a file.

4.1.6 (U) Sorting Flytraps Based on Recent Activity

(U) Cherry Tree shall provide a sortable "Last Beacon Date" column on the Overview, Flytraps, and 'Flytrap Deployments' pages which will allow the most recently active Flytraps to be displayed at the beginning of the list.

4.1.7 (U) Searching Targets

(U) Cherry Tree shall provide the capability to search Target Decks for a desired Target name on the current View -> Target Decks page.

(U) The Target search capability shall allow the use of asterisk (" * ") wildcard syntax.

4.2 (U) Flytrap Requirements

4.2.1 (S) PoP / LP Selection

(S) Flytraps shall read a flag in the mission (downloaded from Cherry Tree) which specifies either to use or not use the beacon addresses embedded in the Flytrap's firmware image. This flag shall persist across Flytrap power cycles. If this flag is set, the Flytrap shall not use the firmware embedded beacon address.

(S) If the firmware embedded beacon address is disabled or fails, the Flytrap shall cycle through the beacon addresses contained in the downloaded mission. The highest priority (first in the list) beacon address shall always be the first used, followed by subsequent addresses in the list in order until a successful beacon occurs. All Flytrap beacon attempts shall follow this protocol.

4.2.2 (U) New Device support

(U) Support shall be provided for up to three new Flytrap devices, depending on level of effort and subject to selection by the sponsor.

(S) A study shall be performed addressing the use of Wiviz technology in Cherry Blossom operations; specifically how undocumented ioctl calls could increase the number of packets that could be examined. The result of the study shall be a description of how Wiviz could be used and the level of effort required to incorporate Wiviz into Cherry Blossom.

4.2.3 (U) User Interface for Building Flytrap Firmware Images

(U) At the sponsor's option, the development of a user interface which provides access to the Flytrap image formation process shall be substituted for one new device support. The estimated labor for this task is estimated to be approximately equivalent to a single new device support; thus if the sponsor chooses this option, two new Flytrap devices shall be supported.

4.3 (U) Roundhouse (Sunflower) Requirements

4.3.1 (U) Deliver RH package with verified application execution support

(U) A verified RH SDK that includes official support for mission deliverable application execution shall be built, tested and delivered.

(U) Flytrap operations based the Roundhouse contractor's recommended volatile and persistent memory locations for application and file storage shall be verified and tested.

4.4 (U) Documentation

(U) This section describes the documentation that shall be provided to support changes and additions to Cherry Blossom for the contract year 2011-2012.

4.4.1 (U) User's Guide

(U) The Cherry Blossom User's Manual [CDRL 12] shall be updated to reflect the Cherry Blossom changes and additions as described in this document.

4.4.2 (U) Abbreviated "Quick Start" User's Guide

(U) An initial section shall be added to the Cherry Blossom User's Manual which shall contain the minimum information needed to operate Cherry Blossom core features. This section shall serve as a "Quick Start" manual, and shall have hyperlinks to more detailed information in the User's Manual proper.

5 (U) Cherry Blossom System Test Requirements

(S) All components of the Cherry Blossom system shall be tested before being deployed. This section enumerates system test requirements. *NOTE: system test procedures are documented in* Cherry Blossom System Test Plan [CDRL 13] *and* Cherry Blossom System Test Procedures [CDRL 14]; both shall be updated to reflect the new requirements contained in this document.

5.1 (U) System Testbed

(S) To support all of the necessary testing of the system, a testbed shall be created. The testbed shall include all of the necessary equipment to simulate all components of the system. The testbed shall include at least one of each supported Flytrap device, as well as device spares. The testbed shall be capable of simulating multiple users connected to a Flytrap.

5.2 (U) Automated Software Unit Testing

(U) All classes, libraries, functions, etc. of software developed for the Cherry Blossom system shall include a comprehensive unit test. A unit test framework shall be used (e.g., Junit for java software) to automate unit testing by incorporating it into the software build.

5.3 (U) Component Level Software Testing

(U) Each component of the system (Flytrap software modules, TW software, CT software, CT remote terminal, etc.) shall have a test plan that must be successfully completed before the software can be deployed. The component level testing shall be as automated as possible, although this will not be entirely possible as some components of the system involve user input (e.g., CT remote terminal).

5.4 (U) System Level Testing

(U) A test plan shall be developed for testing all functionality of the testbed Cherry Blossom system as a whole. Before upgrading the production (operational) system, the testbed system shall successfully complete the test plan. The testbed system test shall be as automated as possible, although this will not be entirely possible as some components of the system involve user input.

(U) Testing shall be performed through multiple PoPs/proxies.

5.5 (U) Production System Testing

(U) A test plan shall be developed for testing all functionality of the production (operational) Cherry Blossom system as a whole. After upgrading the production system, the system shall successfully complete the test plan.