

TEST PLAN 2070 TRAFFIC CONTROL UNIT VOLPE CYBER LAB

Document Change History

Version Number	Date	Contributor	Description
V1.0			What changes (additions and deletions) were made for this version?
V2.0	9/15/2011	Brendan	Test Plan, Test Log, Test Results

Table of Contents

1	INTRODUCTION.....	2
1.1	SCOPE	2
1.1.1	<i>In Scope</i>	2
1.1.2	<i>Out of Scope</i>	2
1.2	OBJECTIVE	2
1.2.1	<i>Primary Objective</i>	2
1.2.2	<i>Secondary Objective</i>	2
1.3	ROLES AND RESPONSIBILITIES	3
1.3.1	<i>Test Engineers</i>	3
1.3.2	<i>Testing Process Management Team</i>	3
1.4	ASSUMPTIONS FOR TEST EXECUTION.....	3
1.5	CONSTRAINTS FOR TEST EXECUTION	3
1.6	DEFINITIONS.....	4
2	TEST METHODOLOGY.....	4
2.1	PURPOSE	4
2.1.1	<i>Overview</i>	4
2.1.2	<i>Normalcy Testing</i>	4
2.1.3	<i>Attack Testing (Multiple)</i>	4
2.1.4	<i>Testing completeness Criteria</i>	4
3	TEST DELIVERABLES.....	5
3.1	DELIVERABLES MATRIX.....	5
3.2	DOCUMENTS	5
3.2.1	<i>Test Scenarios</i>	5
3.2.2	<i>Test Logs</i>	5
3.2.3	<i>Test Results</i>	5
3.2.4	<i>Test Results Final Report</i>	5
4	RESOURCE & ENVIRONMENT NEEDS.....	6
4.1	TESTING TOOLS.....	6
4.1.1	<i>Attack Tools</i>	6
4.1.1.1	<i>Hardware Management</i>	6
4.2	TEST ENVIRONMENT	6
4.2.1	<i>Hardware</i>	6
4.2.2	<i>Software</i>	6

1 Introduction

This test approach document describes the appropriate strategies, processes, and methodologies used to plan, organize, execute and manage testing of the 2070 Traffic Control unit.

1.1 Scope

The Volpe Cyber laboratory (VCL) has been asked to examine the 2070 traffic control unit to determine if the unit is vulnerable to cyber based attacks.

1.1.1 In Scope

The Volpe Cyber Lab 2070 *Test Plan* defines the unit, system, and testing approach. The test scope includes the following:

- Testing the 2070's response to various cyber attacks
- Repeatability of successful attacks
- Testing to see if the 2070 can be used to harbor a virus or other malicious code that could be transferred to authorized computers that connect to the 2070.

1.1.2 Out of Scope

The following are considered out of scope for Volpe Cyber Lab 2070 system Test Plan and testing scope:

- Testing for system vulnerabilities outside the 2070 traffic controller
- Testing of every possible attack vector that can occur

1.2 Objective

1.2.1 Primary Objective

A primary objective of testing the 2070 traffic controller is to: Ascertain whether or not the 2070 traffic controller is susceptible and or venerable to cyber attacks in which normal operations of the 2070 is disrupted either by the attacker taking over functional control of the 2070 or causing the 2070 to cease operations.

1.2.2 Secondary Objective

The secondary objective of testing the 2070 traffic controller is to: Ascertain whether or not the 2070 traffic controller can be used to store a virus or malicious code that could infect authorized devices connected to the 2070.

1.3 Roles and Responsibilities

1.3.1 Test Engineers

VCL designated test engineers will be responsible for:

- Creating simulated environment for 2070
- Developing cyber attack scenarios
- Running cyber attack scenarios
- Recording results
- Validating results
- Reporting results

1.3.2 Testing Process Management Team

Manages the entire testing process, workflow and quality and responsibilities to include:

- (a) Monitor and manage testing integrity and Support testing activities
- (b) Coordinate testing activities

1.4 Assumptions for Test Execution

- Test results will be reported. Not every attack will result in successful penetration of the 2070 unit. Failed attacks will be included in test reports.
- Not every conceivable type of cyber attack will be attempted.
- The testing will only reflect vulnerabilities of the 2070 unit itself, supporting hardware and systems will not be tested at this time.

1.5 Constraints for Test Execution

- Test engineers should clearly understand the procedures for each test.
- Any test that could possibly result in the “bricking” of the 2070 unit shall only be conducted after receiving permission from the equipment’s owner.
- All results will be recorded in the test log
- All test scripts will be written in a step wise manner to ensure repeatability

Sensitive But Unclassified

1.6 Definitions

Attack: Any form of electronic communication with the 2070 who's intent is to disrupt, control, or destroy the 2070's functionality.

2 Test Methodology

2.1 Purpose

2.1.1 Overview

The purpose of the 2070 Test Plan is to achieve the following:

- Define testing strategies
- Identify testing risks.
- Identify required resources and related information.
- Provide testing Schedule.

2.1.2 Normalcy Testing

The purpose of normalcy testing is to ensure that the 2070 traffic controller is functioning in the simulated environment in the same manner as it functions day to day.

The simulated environment will employ the minimum of functionality of the 2070 unit to achieve the test plan goals. A McCain C11S Tester will be used to simulate traffic lights and inputs.

2.1.3 Attack Testing (Multiple)

The VCL will attempt to alter the operation of the ATC by either causing a complete shutdown or alteration of normal operations such as light cycles. The attacks can occur either by an autonomous payload or by opening up the device to remote control, also the ability to "store" a virus onboard the ATC and having that virus transferred to another device will be investigated. Standard attacks methods such as injection; man in the middle etc. will be used. All successful attack scenarios will be repeated in order to verify the test plan steps and results.

2.1.4 Testing completeness Criteria

After all attack scenarios have been run against the 2070 and all results verified by repeat testing. The testing cycle for the 2070 unit will be complete.

3 Test Deliverables

Testing will provide specific deliverables during the project. These deliverables fall into three basic categories: Test scenarios, Test logs, Test results, and final reports.

There is a progression from one deliverable to the next. Each deliverable has its own dependencies, without which it is not possible to fully complete the final test report deliverable.

The following page contains a matrix depicting all of the deliverables that Testing will use.

3.1 Deliverables Matrix

Deliverable
Documents
Test Scenarios
Test logs
Test results
Reports
Test results Final report

3.2 Documents

3.2.1 Test Scenarios

The test scenarios document will include the step by step approach for each attack on the 2070 unit, along with the hardware and software used in each attack.

3.2.2 Test Logs

The test log documents will contain the observations obtained while running the test scenarios. Separate entries for each time a scenario is run will be made.

3.2.3 Test Results

The test results document will contain the results of each attack scenario in a matrix format giving the nature, name and result of the attack.

3.2.4 Test Results Final Report

The final report document will contain data from the test scenario, test log, and test results reports. The final report document will also contain any recommendations or mitigations based on the vulnerabilities discovered during the testing phase.

4 Resource & Environment Needs

4.1 Testing Tools

4.1.1 Attack Tools

Various known cyber attack tools will be employed in this test. In addition any known vulnerabilities of the 2070 unit will be tested for verification. The VCL workstation used to launch the attacks will consist of a typical high-end desktop PC loaded with BackTrack 5 Linux.

4.1.1.1 Hardware Management

The 2070 units received for testing will be managed using the VCL's inventory management system.

4.2 Test Environment

4.2.1 Hardware

The main hardware components required for the 2070 test are:

- 2070 Unit
- Workstation
- McCain C11S Tester
- Standard network switch to communicate with the 2070 Units

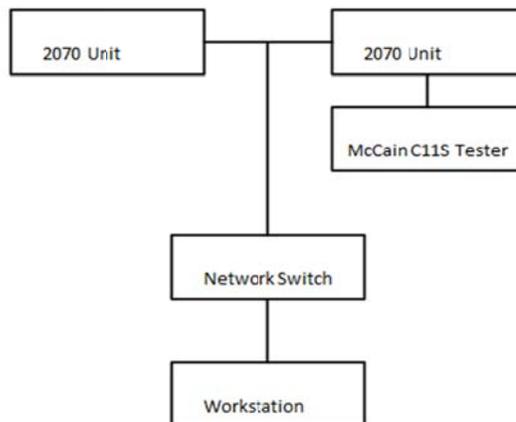


Figure 1 Test Environment Diagram

4.2.2 Software

- BackTrack 5 Linux
- zeNmap Portscanning tool

- Hydra Password Cracking Tool

5 Test Scenarios

The following test scenarios will be investigated by Volpe Cyber Lab Engineers. All findings will be recorded in the test log. Successful attacks will be repeated on the second traffic controller to confirm the repeatability of the attack.

5.1 Network Attacks

The Volpe Cyber Lab technicians will investigate the vulnerability of the box's network interface in 3 ways. The first step will be a scan of the available ports and services running on the box. The next step will be to investigate the available ports and attempt to gain access to the box. The final stage will be attempting to add, remove and modify files on box and to execute remote commands.

5.1.1 Port Scanning

Port scanning is the first step in target identification. By finding the available ports, the ATC can be jeopardized by a number of automatic tools. The Volpe Cyber Lab will utilize the zeNmap software on BackTrack 5 Linux in order to investigate open ports on the system. Ports which are open will be recorded in the Test Log.

5.1.2 Gaining Access

The Volpe Cyber Lab will attempt to gain access to the box through publicly available information and through attacks on available ports by using the Hydra password cracking tool on Backtrack 5. After gaining access, lab personnel will attempt to communicate with other network devices using the 2070 as a pivot.

5.1.3 Modifying Data & Executing Commands

After gaining access to the 2070 ATC the Volpe Cyber Lab will attempt to run remote commands through TELNET. Lab personnel will also attempt to download the system configuration through FTP, and attempt to upload, create, and delete files. Additionally the file system will be investigated and we will attempt to modify existing processes on the box.

5.2 Physical Attacks

Physical Security is another vital aspect of the 2070 controller. We have deduced that the 2070 can be programmed through the use of a data key, a proprietary device used to download and upload system configurations. The Volpe Cyber Lab believes that the Data Key could be used to upload a malicious configuration to the traffic controller and will investigate manipulating the system configuration through datakeys.

6 Test Log

The Purpose of this document is to log the attacks performed and to prove the repeatability of what was found.

6.1 Network Attacks

6.1.1 Port Scanning

The first part of the VCL's testing was to gather as much information as possible before executing an attack. This was done through the use of the use of the ZeNmap tool, which scans for available IP addresses and open ports on the network. Technicians ran the tool successfully against both of the 2070 units in the lab. They were able to recover the IP Addresses of each, and found that ports 21 and 23 were open. Ports 21 and 23 are the standard ports for the FTP and TELNET protocols, respectively.

Device Investigated	Tool Used	Ports Scanned	Open Ports & Protocols
10.160.209.23	ZeNmap	1-65535	21 – FTP; 23 - TELNET
10.160.209.24	ZeNmap	1-65535	21 – FTP; 23 - TELNET

The lab engineers then attempted to connect to the boxes through Telnet and FTP and were able to gather some interesting information. The engineers found that when the box was contacted through the TELNET protocol the box responded by telling the user that it was a TEES compliant Advanced Traffic Controller. The box also asked for a user name and password and would allow up to 3 attempts before closing the TELNET connection. FTP Yielded less information and was utilized more after a user name and password could be recovered.

The information gleaned from TELNET led to some astonishing discoveries. One of the items of interest was finding the TEES specifications, which the ATC boxes followed, publicly online. These specifications detailed not only the hardware specifications of the traffic control boxes, but also contained information on the default software settings, including a root password.

6.1.2 Gaining Access

After the VCL engineers performed the necessary reconnaissance it was time to try to gain access to the box through the information they had gathered and through the use of common hacking tools available on BackTrack 5. The first thing that the engineers tried was to use the default user name and password, found in the TEES specifications. The combination worked on both of the machines and confirmed that at least some of the boxes operating in the field might be using this combination as well.

The VCL engineers also ran a simulated brute force attack using the common password cracking tool Hydra. The attack utilized a dictionary of random words in

addition to the known combination. The attack was successfully executed on the FTP port of both machines and returned the correct username and password. The attack was unsuccessful on the TELNET port, although the same username and password combination worked for both protocols.

Device Investigated	Tool Used	Number of UN/Pass Combinations	Protocols	Successful?
10.160.209.23	Hydra	2500	FTP	Yes
10.160.209.24	Hydra	2500	FTP	Yes
10.160.209.23	Hydra	2500	TELNET	No
10.160.209.24	Hydra	2500	TELNET	No

After successfully recovering the passwords to the machines the VCL Engineers wanted to see if it was possible to connect remotely from one machine to other machines on the same network. In order to do this the engineers logged in to one of the boxes and attempted to connect to the other box via both TELNET and FTP.

Host Device	Destination Device	Protocol	Successful?
10.160.209.23	10.160.209.24	FTP	Yes
10.160.209.24	10.160.209.23	FTP	Yes
10.160.209.23	10.160.209.24	TELNET	Yes
10.160.209.24	10.160.209.23	TELNET	Yes

The VCL staff was able to successfully connect from one ATC to another using the recovered login information.

6.1.3 Modifying Data & Executing commands

After gaining access to the traffic controller, technicians wanted to evaluate the possible actions which a malicious user would take. The first goal of the VCL staff was to gain as much information on the file structure as possible through the use of the FTP protocol.

Device Investigated	Protocol Used	Goal	Successful?
10.160.209.23	FTP	Download File	Yes
10.160.209.24	FTP	Download File	Yes
10.160.209.23	FTP	Upload File	Yes
10.160.209.24	FTP	Upload File	Yes
10.160.209.23	FTP	Create File	Yes
10.160.209.24	FTP	Create File	Yes
10.160.209.23	FTP	Remove File	Yes
10.160.209.24	FTP	Remove File	Yes

The technicians were able to perform a number of the desired actions on both of the boxes. The first step was to create a copy of all of the files in the existing file structure, in order to examine the way which the files interacted. There were a number of files which were immediately interesting. The startup file, which controls what the box

does when it is first turns on, was an immediate target. The technicians found that the file was a simple script which could be edited using a text editor.

After attempting to copy the files, technicians decided to remove files. While they did not remove any critical files, we hypothesize that any file could be removed. In addition to being able to copy and delete files, VCL engineers were also able to place their own files on the box, even files which were already on the ATC, overwriting the intended purpose with their own. By examining the file structure of the box, the VCL staff also found a wealth of additional commands which could be run in a TELNET session.

Another goal of the VCL staff was to issue remote commands to the boxes, and to attempt to change the way which they operated. The Volpe staff was successful in issuing remote commands, although none of them allow direct control of the traffic management system. However, they have discovered one command of interest. The command completely halts the box, it no longer responded to any TELNET or FTP commands and even stopped controlling the lights. The only way for the box to recover was through a complete restart of the system. Another interesting command allowed the user to alter the IP address of the box from within the TELNET interface, which could be used to cut off communication to the box from its usual network. The engineers also found a way to end the TELNET service running on the box, preventing anybody from entering the box until it is restarted.

6.2 Physical Attacks

As of this version no physical attacks have been discovered.

7 Test Results

The Purpose of this document is to report the results of our findings.

7.1 Network Attacks

The Volpe Cyber Lab has determined that the 2070 Advanced Traffic Controller is susceptible to a number of basic network intrusion techniques, and the potential impact is severe.

7.1.1 Port Scanning

The technicians identified two open ports, 21 and 23, which are commonly used for TELNET and FTP respectively. These protocols are what enable damage to be done because their intended purpose is to enable file transfer and remote command execution.

7.1.2 Gaining Access

While the technicians were able to simulate a successful brute force password attack on the FTP protocol, the real issue with these systems is publically available standardized configurations. The ATC will notify the user what TEES specification it is using, and within the TEES Specification the default user name/password pair can be found. If it fell into the wrong hands the TEES specifications would enable anybody to access these devices.

In addition to finding the User/Password pairs we able to pivot from one box to another on the network. This means that a malicious user could hop from one 2070 box to another, or depending on the network configuration, from a 2070 box to other networked devices such as traffic control center computers.

7.1.3 Modifying Data & Executing Commands

The Volpe Cyber Lab was able to perform a number of commands on the box. The lab's first idea was to get a copy of all of the software running on the system. After VCL Engineers obtained the configuration, they examined the startup files and were able to understand the syntax of the box and where it stores its commands and configurations. A malicious user would be able to modify the startup file to run whatever commands he wished. Additionally a malicious user is able to remove files from the system as well, and could use this ability to corrupt the box in order to take it offline.

In addition to modifying files technicians were also able to issue remote commands. While most of the commands executed were common UNIX commands, they discovered one flaw which crashed the box completely, due to an internal configuration issue. Another command of interest enables a user to alter the IP configuration of the box making it possible to disrupt its ability to communicate with other machines it is networked with. The technicians were also able to kill the TELNET service running on the box, which would remain off until the box was restarted manually.