System Requirements Specification

for

Aircraft Domain Security Enhancement

Version 1.04 approved

Prepared by Group 6

Embry-Riddle Aeronautical University

September 28, 2021

Table of Contents

Revision History

Name	Date	Reason For Changes	Version
Max Wilson	9/17/21	Document Initiation/Set-up	1
Anthony Johnson	9/17/21	Purpose & Product Scope	1.01
Max Wilson	9/26/21	Addition of more details to product description	1.02
Anthony Johnson, Max Wilson, & Maxwell Gorley	9/27/21	Completion of SRS rough draft for sprint 1	1.03
Max Wilson	9/28/21	Final overview and completion of SRS draft 1	1.04

1. Introduction

1.1 Purpose

This document specifies the requirements for an aircraft domain emulation and testing environment called the Aircraft Domain Security Enhancement version 1.0. This involves the development and configuration of an Aircraft Information Services Domain (AISD) emulation, and a compatible penetration testing kit.

1.2 Document Conventions

Not applicable for current documentation.

1.3 Intended Audience and Reading Suggestions

This document is intended for cybersecurity experts, researchers, and users who interact with aircraft networks every day. It is recommended to begin with product scope, to get a vision of this project. For all readers, it is best to review the external interface requirement sections here, to get a better understanding of how the project was implemented and tested.

1.4 Product Scope

The aircraft domain security enhancement is intended to provide a testing ground for aircraft networks before they are implemented with real hardware. There are two stages of development for this project. First, the AISD will be emulated allowing for remote testing and configuration. The emulated network will encompass several mediums to low priority components to the network. Second, a penetration testing kit will be developed to test the security of the overall domain. The aircraft domain is a complex system containing many communicating critical and non-critical components. Testing these systems becomes increasingly difficult as more components are added which further leads to the importance of a flexible emulated environment. The completion of this project will provide a virtual environment capable of testing the security of the aviation domain being evaluated.

1.5 References

At this time there are no applicable references.

2. Overall Description

2.1 Product Perspective

This product is an emulation of current aircraft network nodes, such as the aircraft printer, control console, and entertainment network. Below is a breakdown of each network "node" and how it interacts with each system to create a fully interactive aircraft network. It has the ability to be expanded upon and is isolated. This allows users to be able to test malicious cyberattacks against the machine and learn how to improve the security of the network over time.

2.2 Product Functions

Below is a breakdown of both hardware and software capabilities for the product:

- AISD network
- Printer network
- Pentesting (Kali Linux) malware virtual box
- TFTP server network
- Gate-access point
- Web/Log server
- Software-firewalls
- SSH capabilities
- Expansion of software virtualization over multiple systems
- Secure access to all hardware and software

2.3 User Classes and Characteristics

Not applicable for current systems.

2.4 Operating Environment

The software used for the aircraft network system is Linux-based with QEMU as the virtualization software. Multiple versions of Ubuntu OS were used to set up each node and physical host machines. The hardware being used is multiple laptops with eight to sixteen gigabytes of RAM, and up to one terabyte hard drive.

2.5 Design and Implementation Constraints

Due to the scale of the project, as well as the timeframe, there are several constraints of the system. The first is hardware limitations due to shipping times, funding, and integration with the QEMU virtualization software. Another main limitation is the security considerations. Although the main part of the project is to design and harden an aircraft network system, there are always "zero-day" flaws that are unknown.

2.6 User Documentation

Not applicable to current systems.

2.7 Assumptions and Dependencies

It is assumed that a high-speed broadband internet connection will be available so that all virtual machines can be managed. An additional assumption is that an SSH client will be installed on all computers trying to connect to the virtual machine network. The virtual machines depend on a sufficiently powerful Linux-based host with at least 16 gigabytes of RAM to run them.

3. External Interface Requirements

3.1 User Interfaces

The users will interact with the system via a command-line interface (CLI) in order to perform maintenance tasks and manage the system via SSH.

3.2 Hardware Interfaces

The hardware encompasses a Linux operating system (OS) on a Laptop that has 16 GB of RAM and a 500 GB hard drive. This hardware hosts the software which runs QEMU (see below for details regarding software). Future iterations of the hardware will include servos to mimic wings, a joystick for flight control, along with additional interface instruments to give the feel of an actual aircraft and its network. Through these interfaces, users can run physical pen testing attacks against the machine instead of only virtual ones.

3.3 Software Interfaces

Due to issues trying to integrate Windows OS with QEMU, the OS was changed over to a Debian/Ubuntu-based system. Linux has more built-in functionality that allows ease of access for the user when working with the QEMU emulator. The emulator hosts the entirety of the aircraft network system consisting of multiple "nodes" or aircraft components.

3.4 Communications Interfaces

The main communication interface of the project is the TFTP (Trivial File Transfer Protocol) server. The TFTP server acts as a bridge between the ADIS and other nodes of the aircraft network system. The server is hosted by a QEMU emulator that has a built-in TFTP network that can be incorporated with the rest of the systems for this project. The TFTP has built-in encryption and is interacted with via an SSH (Secure Shell) server.

The SSH server is the main hub of the aircraft network emulator. It allows the user remote access via logging in through a terminal or command prompt. The SSH server is encrypted and only available to users who have been cleared to access it. The server is on a Linux-based computer that hosts all of the QEMU network interfaces. By doing this, multiple people have access to the server at one time to simulate cyber-attacks, harden security, or do maintenance on the network.

4. System Features

4.1 SSH Server

4.1.1 Description and Priority

The SSH server provides a way for authorized users to remotely manage machines on the aircraft domain network.

4.1.2 Stimulus/Response Sequences

1. The client will initiate a connection to the SSH server.
2. The SSH server will respond with a login prompt.
3. The username of the desired user will be entered.
4. The user is prompted to enter a passphrase for the private key.
5. Once the private key is unlocked, the public key for that user is calculated from the private key and sent to the server for verification.

6. If the keys match, the user will be prompted to enter a six-digit code presented by a Google Authenticator-compliant app or security key.
7. If the code is entered correctly, the user will be presented with a Bourne-Again Shell (Bash) prompt where commands may be entered.
8. If any of the above steps fail, the user will be disconnected from the SSH server.

4.1.3 Functional Requirements

REQ-1: TBD
REQ-2: TBD

4.2 System Feature 2 (and so on)

5. Other Nonfunctional Requirements

5.1 Performance Requirements

Not applicable to the current system.

5.2 Safety Requirements

SAF-1: The aircraft domain network system shall be backed up in case of hardware or software failure.
SAF-2: The flight crew shall have the option to override any and all automated systems at all times.
SAF-3: The pitch and roll of the aircraft shall not exceed thirty degrees unless the flight crew chooses to override this limit.

5.3 Security Requirements

SEC-1: The SSH server shall use public-key authentication.
SEC-2: The SSH server shall not use password authentication.
SEC-3: The SSH server shall only be accessible by those authorized to use it.
SEC-4: A firewall shall be installed on the virtual machine network.
SEC-5: All ports other than the ones needed for the AISD network shall be closed on the firewall.
SEC-6: Only team members, professors, and Boeing shall have access to the aircraft domain network system.

5.4 Software Quality Attributes

The software used for the project is adaptable, portable, and readily available. The virtual network can be expanded upon at any point to include more aircraft network systems. The network is also available via SSH for ease of access across users.

5.5 Business Rules

Only authorized users will be permitted to access network resources.

6. Other Requirements

Appendix A: Glossary

Term	**Definition**
RAM	Random Access Memory
OS	Operating System
TFTP	Trivial File Transfer Protocol
AISD	Aircraft Information Services Domain
SSH	Secure Shell
CLI	Command-line interface
VM	Virtual machine
Bash	Bourne-Again Shell, the default Linux command shell
Zero-day	A type of cyberattack that uses a previously unknown vulnerability of a system, to carry out malicious activity.

Appendix B: Analysis Models

Not applicable at this time.

Appendix C: To Be Determined List

Not applicable at this time.