CS 490: Engineering Notebook
Anthony Johnson

Notes:

Aerospace Aircraft Domain Security Enhancement

Icao standards

Aircraft domain:

ACD – Aircraft Control Domain (high trust)

- Complete avionics, controls, and automation
- Afdx & arinc 429

AISD – Airline Information Services Domain (moderate trust)

- Facilitate info for pilot and crew
- Ipv4 ethernet and some aviation to acd

PIESD – passenger information and entertainment services domain (low trust)

Arinc standards

Arinc 429, A664p7 (afdx)

Linux box for network management

Design network topology for access point

Web server to access applications in node 2

QEMU

The group has come out of the first stages of the project and will begin towards development soon. An issue is that it is hard to get people to work on deadlines or together in any sense. I will issue a new work paradigm in the end of sprint 1 to be started with sprint 2.

Step 1: Finish Demo

Step 2: Decouple people from tasks

For a minimum viable product (first demo), I think it would make sense to have AISD machines on one network, and the Gate access machine works on the AISD network, and bridges to the host machines network to enable a 802.1x connection.

The 802.1x connection is not yet determined but we can use an ssh server on the GAP. Client computers will then use that connection to send files through.

Approaching the end of the first semester. We have effectively accomplished the first iteration of this project with a watered down emulated AISD network as well as an initial pentest to evaluate the security at a basic level. For the next semester, the development will focus on refining the work we have contributed through two ways:

1: Revising the emulated AISD network to pass first order security tests

2: Seeking out more threats the exploit

Some sub tasks include:

Investigating NIST standards to add more rigor to testing documents.

Using funding to order hardware for final tests.

First sprint of 2nd semester.

Boeing notes:

> Work on fully portable product to pass to next team. Prescott should be able to easily initialize network for pentesting CTF

Collaboration with Prescott highly emphasized. CTF will be conducted on virtualized interface through ssh. Interface for pentester will be Ubuntu machine with all tools on the desktop ready to use. Readme will be provided with CTF requirements.

Most of sprint has been planning and working around bottlenecks that include:

1: Waiting for funding

2: Hardware limitations (RAM)

Next sprint:

1: Focus on securing platform for CTF (cloud)

2: Run test CTF in virtualbox

Third sprint: put both of these components together using qemu and cloudserver.

2nd Sprint of Second Semester

This sprint has been focused heavily on the design of the CTF and Setting up cloud server

After meeting with prescott, the understanding of our demo is a proof of concept for the application of emulating an aircraft network. This CTF will mostly be used for educational experience so the exploits needed to finish it are first order security threats.

Cloud service decided: Linode high ram server

Sprint 2 demo goals:

- Walk through Confidentiality Keyhunt (MITM)
- Walk through Log server Keyhunt (DDOS)
- Walk through Setting up cloud server

Connection test with prescott will be done april week of the 11th

Fill CTF will be conducted April week of he 18th

Failed to set up cloud due to lack of funding. Funding must be requested from department

---