AGENDA

• Cybersecurity Test Facility (CyTF) - Description & FAA Mission
• Planning a Cybersecurity Test Facility
  • System Engineering (CONOPS, Requirements, Functional Analysis)
  • Design
  • Connections
  • Operations: processes (CM, Procedures, other SOPs)
• Activities – Cybersecurity Testing, Evaluation & Related (evolution)
  • Security tool evaluation/comparison
  • Cybersecurity exercises/training
  • Penetration testing
  • Requirements Development
  • Operations – ISCM, Security Assessment/Risk Mitigation
• Lessons Learned & Current Challenges
Cybersecurity in the Aviation Ecosystem

**Aircraft**
- Flight Deck Avionics
- Airline Information Systems
- Passenger Devices

**Airsports**
- Internet / Wi-Fi
- Power & A/C
- Ground & Air Support

**Airlines**
- Flight Planning
- Operation Centers
- Web-sites

**Aviation Operators**
- FAA networks (NAS, MSN, R&D)
- Surveillance Sensors
- Decision Support

**Challenges**
- Increasing attack surface due to increasing interconnectivity
- Responsibility for securing this infrastructure is widely distributed
FAA NextGen
(Next Generation Air Transportation System)
FAA Cybersecurity Test Facility Development

1. Plan
   - Research
   - System Engineering
   - Design

2. Stand Up
   - Location
   - Connections

3. Operate
   - Procedures
   - Tools

FAA William J. Hughes Technical Center
Key Characteristics

- **Isolated** from the FAA operational environment
- **High-fidelity replication** of FAA Air Transportation System services & systems
- **Extensible**, to allow growth
- **Adaptable**, but with a number of stable baseline environments
- **Support collaboration** with industry, academia, and government
- **Evaluate security controls** in the FAA Air Transportation System enterprise & systems

System Engineering

- Concept of Operations
- Functional Architecture
- Requirements
FAA Cybersecurity Test Facility

Opened January 2016

Mission: Provide cybersecurity evaluation and research services to strengthen FAA information security in a Research and Development (R&D) environment.

CyTF Capabilities

- Product Evaluations
- Security Capability Prototyping
- Enterprise Security Support
- Cyber Incident Training
- Vulnerability Assessments
- Penetration Testing
FAA Cybersecurity Test Facility
Locating & Connecting

Test Objectives:
• Detailed,
• Repeatable,
• Adaptable

Cybersecurity Test Facility (CyTF)
Reconfigurable VM Environment; Scalable, repeatable, adaptable

FAA William J. Hughes Technical Center
Example CyTF Support Tools

**Detection**
- ArcSight
- Blue Coat
- CheckPoint
- FireEye
- IronPort
- McAfee ePO
- Nessus
- NetWitness
- QRadar
- SourceFire
- Splunk
- WatchTower

**Offensive**
- Cobalt Strike
- Core Impact
- Kali Linux
- Looking Glass
- Metasploit
- Nessus
- NMAP
- Simulation Deck

**GOTS/FOSS Visualization & Analysis**
- ALIVE
- CCER
- Dagger
- Galaxy
- GHidra
- K0ALA
- LARIAT
- MATT
- Network Miner
- Python-evtx
- SILK
- Wireshark
Cyber Testing, Evaluation & Related (Evolution)

1. Security Tool Evaluations
2. Cybersecurity Exercises/Training
3. Cybersecurity Situational Awareness
4. Requirements Development
5. Vulnerability/Penetration Testing
6. Security Assessment/Risk Mitigation
CyTF is a safe environment to evaluate cybersecurity tools

- Example 1: CyTF evaluated 2 functionally similar Information Security tools comparing:
  
  1. **Functionality**
     against Continuous Monitoring functionality requirements, and
  
  2. **Performance in NAS**
     against NAS performance specifications, after integrating each tool individually with FAA’s EnRoute Automation System
Example 2: CyTF supported FAA Cyber Investigations staff to analyze effects on workstations with clients for a prospective security tool

1. CyTF created FAA Win07 VM images and installed clients for security tool under test,
2. The VMs went through test cases based on Continuous Monitoring requirements,
3. VM images were sent out to FAA Cyber Investigations Team for forensic analysis
4. Investigations Team compared before & after file hashes and found no changes.
<table>
<thead>
<tr>
<th>Exercises</th>
<th>Sponsor</th>
<th>Description</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal “Whole of Nation” Exercise</td>
<td>USCYBERCOM</td>
<td>Tactical exercise focused on “whole of nation” solutions to protect from cyber-attacks against U.S. critical infrastructure</td>
<td>Exercise coordination, communications &amp; information sharing of U.S. agencies (DoD, DHS, DOT, States) and with coordinating entities (A-ISAC)</td>
</tr>
<tr>
<td>FAA Incident Response Process Exercise</td>
<td>FAA</td>
<td>FAA functional (virtual machine) exercise hosted by CyTF with participation of FAA security ops specialists.</td>
<td>Examine decisions, coordination &amp; communications during a cyber event; validate the NAS Cyber Incident Response Team (NCIRT) process</td>
</tr>
<tr>
<td>FAA Tabletops (TTXs)</td>
<td>FAA</td>
<td>Examine incident response processes using use cases for Malware Analysis, Suspicious User Activity, VPN Monitoring, etc.</td>
<td>Produce an After Action Report detailing the tools used for each Use Case and gaps noted between the playbook Use Cases and incident tracking workflow</td>
</tr>
<tr>
<td>Caribbean Initiative Tabletop (TTX)</td>
<td>ICAO</td>
<td>Develop and promote common understanding of cyber threats, vulnerabilities, and resultant risk across the Aviation Ecosystem.</td>
<td>Identify gaps in state policies &amp; operations and Identify and promote regional partnerships &amp; mechanisms for sharing information on threats &amp; incident response</td>
</tr>
<tr>
<td>International Tabletop (TTX)</td>
<td>ICAO</td>
<td>Provide a common understanding of cyber threats, vulnerabilities, and the potential risks to the Aviation Ecosystem.</td>
<td>Identify gaps in international policy, standards, and processes &amp; Identify partnerships and mechanisms for sharing info on threats, vulnerabilities, and response.</td>
</tr>
</tbody>
</table>
Simulated FAA Exercise Network

Air Route Traffic Control Centers
William G. Hughes Technical Center
FAA Administrative Offices

Towers and Terminals

OPERATIONAL NETWORK
ATC Cybersecurity Operations

RESEARCH & DEVELOPMENT NETWORK
Security Operations Center

ADMINISTRATIVE NETWORK

VIRTUAL FAA DOMAIN

INTERNET
Internet Access Point
Hackers

4,000 simulated websites
Find gap between current monitoring capability & monitoring with data flow added

- Introduced COTS data flow monitoring products into FAA R&D network labs
- Developed initial set of data flow monitoring requirements
  - Generated 150 requirements that cover data modeling, security, GUI, ....
  - Coordinated requirements with stakeholders (NAS Cyber Ops, FAA Security Ops, FAA Telecomm Infrastructure, etc)
- Developed test and evaluation scenarios to support requirements validation
- Validated data flow requirements utilizing COTS products
- Provided the ability for stakeholders to test and evaluate products utilizing CyTF services.
Phase 1 | Pre-Assessment Planning
Collaborate with the sponsoring organization to establish the test plan, schedule and Rules of Engagement, and to identify the resources required to perform the depth of testing desired.

Phase 2 | Vulnerability Assessment Planning
Conduct the information discovery and gather scoping information to develop test cases; identify the appropriate tools and resources to perform the vulnerability assessment.

Phase 3 | Vulnerability Assessment Execution
Execute the test cases and look for additional vulnerabilities that may become apparent during the course of the active assessment.

Phase 4 | Penetration Test Planning
Use the results of the vulnerability assessment, observations and impressions to develop additional test cases and formulate a plan of attack to perform the Penetration test.

Phase 5 | Penetration Test Execution
Execute the test cases and look for additional vulnerabilities including chaining and cross-domain exploitation (use an exploit on one domain to gain a foothold in another).

Phase 6 | Post-Assessment Activities
Analyze results of the assessment and prepare the test report. Brief results, findings and recommendations. Assist system owner with cleanup activities.
Information Security Continuous Monitoring (ISCM)

- Mandated by OMB M-14-03 (*Enhancing the Security of Federal Information & Systems*)
- CyTF conducted proof-of-concept & deployed Phase 1 Continuous Diagnostic & Mitigation (CDM) tools for ISCM in the R&D Domain
  - CyTF worked with Tech Center laboratory management to implement an ISCM policy.
- Starting planning CDM Phase 2
  - CyTF staff also deployed an Incident Detection System (IDS) infrastructure
Lessons Learned & Current Challenges

General

• A lab specialized for cybersecurity is becoming an enterprise need
• Standup Rule: building & outfitting costs frequently exceed estimates by ~30%
• Hiring and retaining cyber security professionals can be problematic and is dependent on location
• Cyber lab systems cannot be subject to all the security controls that the organization requires for its other machines; e.g.; CM-7 Least Functionality
Lessons Learned Collaboration

- Collaboration between agencies, the private sector and academia is vital to:
  - Facilitate the interchange of current and emerging cyber technology and ideas,
  - Maintain cyber expertise,
  - Leverage cyber resources for cybersecurity training to practice response processes.

- The need for classified testing & training is growing; secure labs are needed
  - Supports full collaboration with DoD/DHS/FFRDC/State Cyber Ranges
Lessons Learned

Functional Exercises

• Include the Range Support Team in each phase of the event process – start with the planning phase
• Start the security approval process for distributed range exercises early - minimizes risk to the event schedule
• Establish a living cyber exercise plan - organizations can leverage it to shape & ensure the security of their environment/mission space
Contact Us

Enterprise Safety and Information Security Division Manager

John Chung
Office: 609-485-7896
Email: john.chung@faa.gov

Information Security Branch Manager

Ruben Bigio
Office: 609-485-6721
Email: ruben.bigio@faa.gov

CyTF POC

Dominic Timoteo
Office: 609-485-4055
Email: dominic.timoteo@faa.gov