NASA's IV&V Program
Safety and Mission Assurance (SMA) Office
Information Assurance/Cybersecurity Support

Addressing SW Security

11/30/15

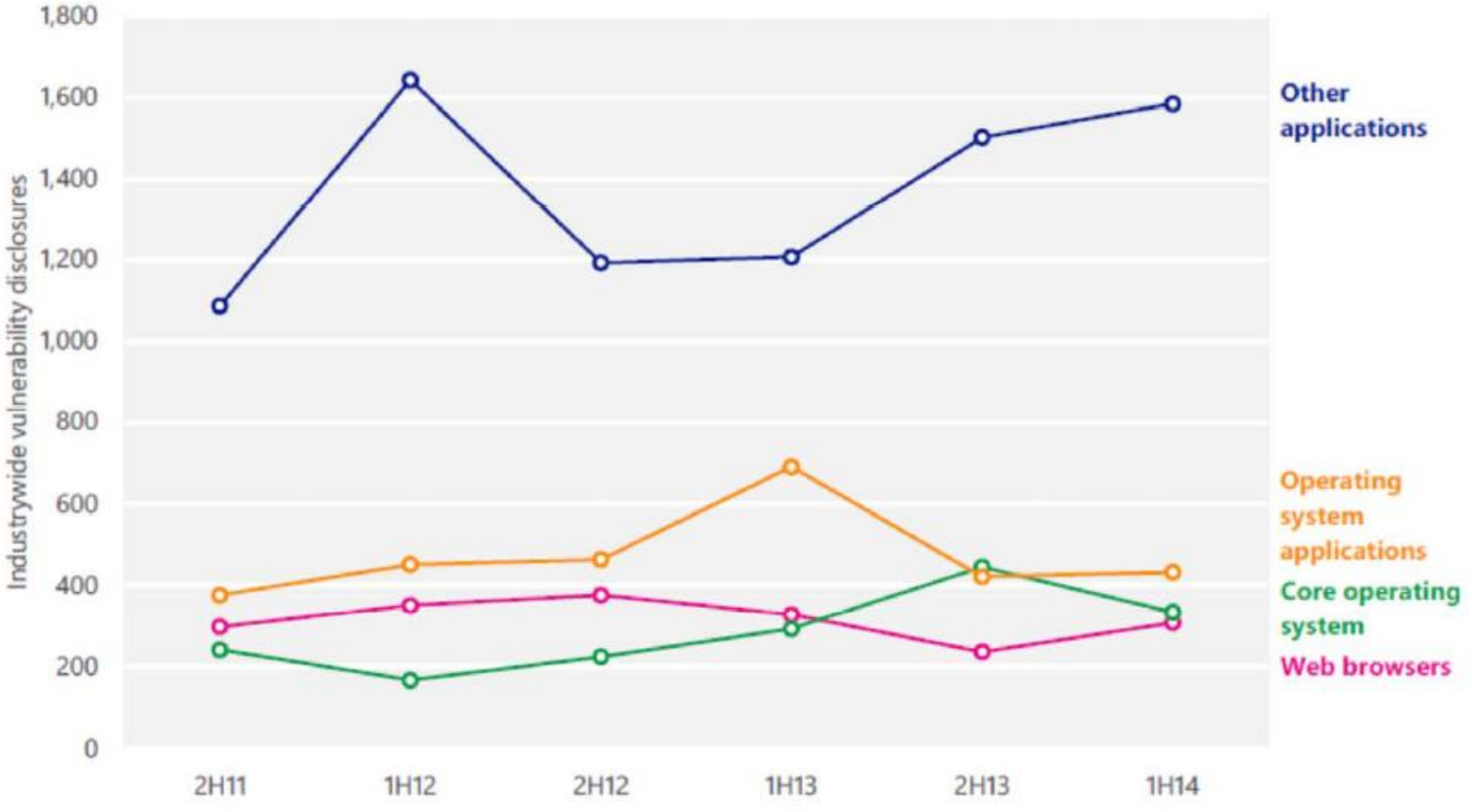
Brandon Bailey
brandon.t.bailey@nasa.gov
304-629-8992

http://www.nasa.gov/centers/ivv

Introduction

- Historically security within organizations was thought of as an IT function (web sites/servers, email, workstation patching, etc.)
- Threat landscape has evolved (Script Kiddies, Hackers, Advanced Persistent Threat (APT), Nation States, etc.)
- Attack surface has expanded – Networks interconnected!!
- Some security posture factors
  - Network Layer (Routers, Firewalls, etc.)
  - Computer Network Defense (IPS/IDS, Sensors, Continuous Monitoring, etc.)
  - Industrial Control Systems (ICS)
  - Software Security (COTS, FOSS, Custom, etc.)

Custom SW – Gets Exploited!



Key: 2H11 = 2nd half 2011; 1H14 = 1st half of 2014

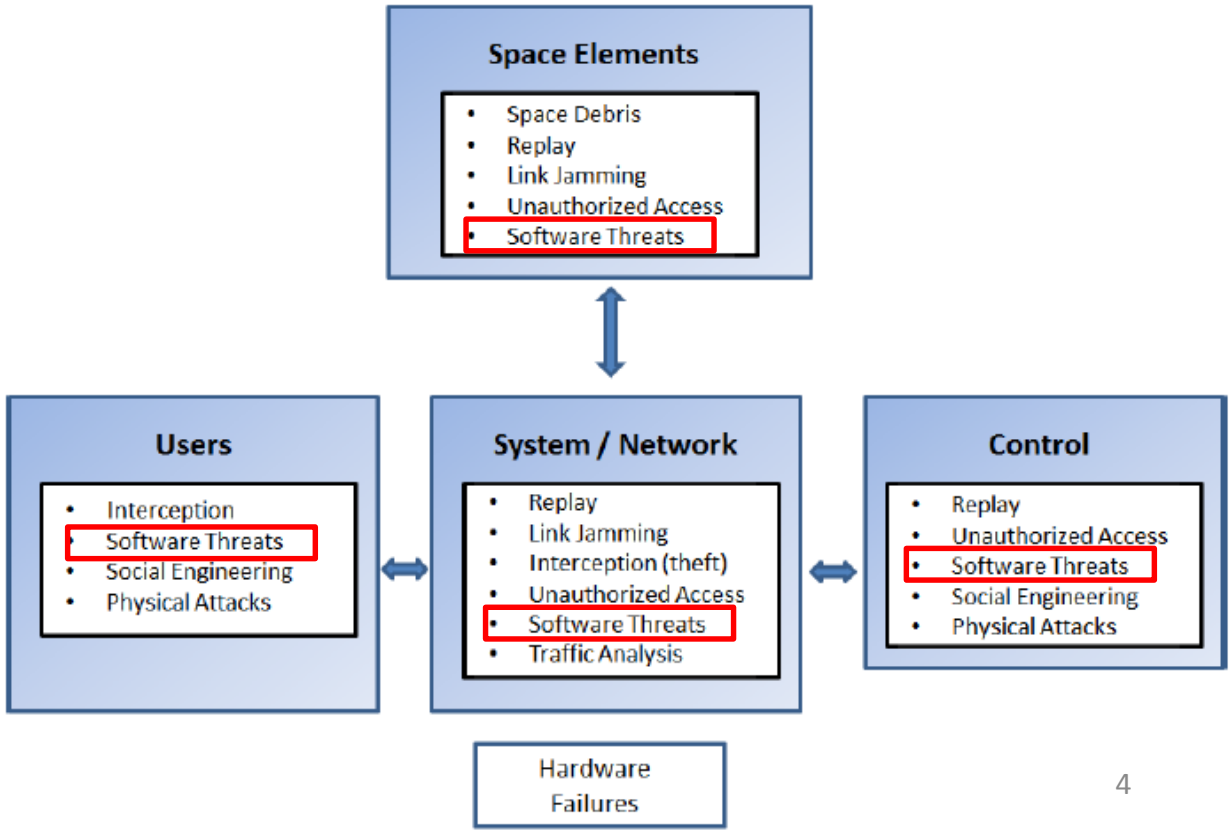
Source: Microsoft Security Intelligence Report, Vol. 17, June 2014

Threats in Space

SECURITY THREATS AGAINST SPACE MISSIONS
CCSDS 350.1-G-1
March 2015

CCSDS was founded in 1982 by the major space agencies of the world, the CCSDS is a multi-national forum for the development of communications and data systems standards for spaceflight.

Security Threats Against Space Missions was developed to provide mission planners with an overview on threat assessment as well as the common threats and threat sources that exist for various categories of civilian space missions.

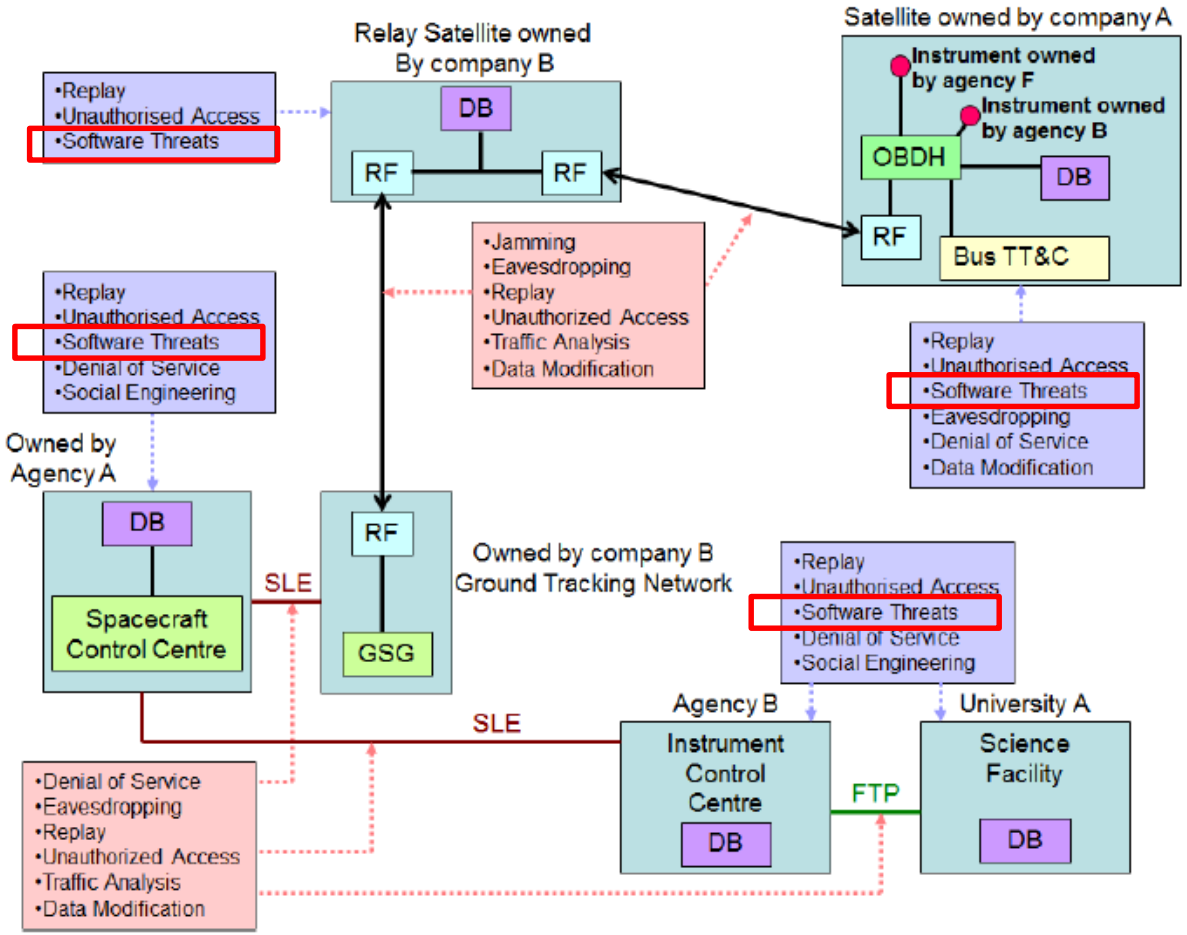


Threats in Space

SECURITY THREATS AGAINST SPACE MISSIONS
CCSDS 350.1-G-1
March 2015

Security Threats Against Space Missions was developed to provide mission planners with an overview on threat assessment as well as the common threats and threat sources that exist for various categories of civilian space missions.

CCSDS was founded in 1982 by the major space agencies of the world, the CCSDS is a multi-national forum for the development of communications and data systems standards for spaceflight.



Threats in Space

Applicable Threats to Space Missions	Impacts	Could Software Be Involved?
Data Corruption	• Modification of information • System damage	Yes; SW attacks could result in data corruption
Ground Facility Physical Attack	Loss of command, control and data	No
Interception	Loss of sensitive data	No
Jamming	• Loss of Command telemetry link • Loss of access to resources	No
Denial-of-Service	Loss of access to resources	Yes; SW DoS attacks are common and can affect both ground, flight and web applications
Masquerade	• Potential to disrupt operations (uplink) • Potential to receive false information (downlink)	Yes; SW protections can be placed to prevent
Replay	System damage (possible safety of life issues)	Yes; SW protections can be placed to prevent
Software threats	• Undesirable events • System damage • Enable other threats	Yes
Unauthorized Access	• Disruption of operations • System damage (possible safety of life issues)	Yes; SW protections can be placed to prevent or SW can be used to gain unauthorized access
Tainted Hardware Components	• Hidden, Malicious capabilities • System instability • System damage • Undesirable System effects	No

Reducing the SW Risk

- NASA knows that software is one of many vulnerabilities that could adversely impact Mission Ops
- Levying requirements from the top (NPRs 2810 , 7150.2B, 7120.5E, and the SW Assurance Standard/Handbook)
- Software security “defects” are arguably preventable in most cases
  - During custom code development
    - Awareness, Training, Tooling (i.e. **SCP**)
    - **Secure Development**
    - Rigorous SwA (**Project** and **IV&V**)
  - Software supply chain
    - COTS and Open Source (i.e. **Origin Analysis**)

Secure Coding Portal (SCP) Background

- Recognizing the need to counteract the threat of exploitation of custom developed software
- A single touch point for NASA developers was established to learn how to develop code securely
- Utilizes existing NASA Engineering Network (NEN) infrastructure
  - Initial deployment is behind NASA firewall
- Partnerships established with experts
  - CMU-SEI
  - Robert Seacord (Author of CERT C Std.)
  - Safari Books Online (custom secure coding tutorial)
- Launched July 20, 2015
  - Two Newsletters Distributed (can be shared)
  - Custom Secure Coding Tutorial Deployed
  - Contact securecodingportal@lists.nasa.gov for additional information

Secure Coding Portal Content

- **Secure Coding Discussion Forum** – providing a friendly environment to discuss all aspects of Secure Coding with fellow engineers and experts
- **Vulnerability Updates** – containing information about the latest software vulnerabilities and any insight into what systems, or types of systems, could be affected along with how to detect and mitigate these vulnerabilities
  - Vulnerability Newsletter will also be distributed directly to stakeholders
- **Tools** – containing information about tools utilized by NASA for security analysis of software, including references, available training, and any relative insight/lessons learned from NASA practitioners
- **Links** – containing references to security standards, documentation, and information
- **Top 25 CWEs** – using CWSS to classify Top 25 CWEs for ground and flight
- **Tutorial** – custom made tutorial by secure coding experts
- **Ask an Expert** – providing the ability for any community member to request assistance from field experts

Secure Development

- Utilize Best Practices from Secure Coding Portal
  - Coding Standards (Ex. CERT C, C++ or JAVA Stds)
  - Integrate tools into development environment
    - Code Analyzers (i.e. Klockwork, Fortify, Flexelint, CodeSonar, Sonatype, BlackDuck, etc.)
    - Great resource for identifying tools (Report | Spreadsheet)
  - Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE), and Common Attack Pattern Enumeration and Classification (CAPEC) information
  - Defense in Depth
  - …
- Training
  - Secure Coding Tutorial
  - Defensive Programming (available online in SATERN)
  - Codiscope

"Herding the Cats"

Services sponsored by Department of Homeland Security and managed by Mitre

CWE:

- Serves as a common language for describing software security weaknesses in architecture, design, or code
- Provides a:
  - Standard measuring stick for software security tools targeting these weaknesses
  - Common baseline standard for weakness identification, mitigation, and prevention efforts
- Utilize CWE to better understand, identify, fix, and prevent weaknesses and vulnerabilities

CVE:

- Identifies publicly known information security vulnerabilities and assign them a CVE_ID.
- Scored 1 to 10 on CVSS scale

CAPEC:

- Community-developed list of common attack patterns
- Comprehensive schema and classification taxonomy
- International in scope

Taking into account attack pattern and any other factors to generate list of CWEs that are critical. Tools report findings in CVEs (known) and CWEs (potential) -> Identify then Fix!

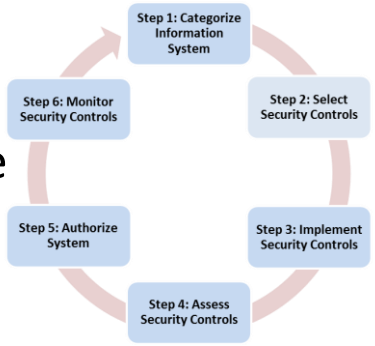
Project SwA – Assuring Security

- Currently updating SwA Standard and SwA Handbook
- Educating SwA personnel
  - Educate on importance of SW security
  - SwA personnel can leverage the same training as developers (i.e. SCP)
    - In order to "assure" it, you must understand it!
- Not a clipboard exercise – SwA needs to use tools or ensure tools are being used to ensure SW is secure
  - Tools have latest security signatures and integrate industry's best practices
  - Dynamic & static code analysis as well as binary analysis (i.e. identifying CWEs/CVEs)
- Verify and validate project is accounting for security during requirements, testing, etc.
  - Ex: Security Requirement Traceability Matrix (SRTM), Whitebox/Blackbox Testing, Negative Testing, PenTesting, etc.

IV&V's Mission

Ensuring Mission and Safety Critical Software and Systems Operate Reliably, Safely, and Securely

- Perform the ***"information system and security control assessment and monitoring"*** techniques that NIST attributes to the IV&V assessor role in its Risk Management Framework for the design, development, implementation, operation, maintenance, and disposition of federal information systems.



- Perform **Security Analyses** throughout the development life-cycle per IEEE-1012 Standard for System and Software V&V

- Counteract the threat landscape throughout the system life-cycle
  - Ground, Satellite, and Command & Control systems

- IA Techniques deployed throughout project life-cycle phases

Origin Analysis

- From Institute for Defense Analyses (IDA) SOAR Report – *"Origin analyzers are tools that analyze source code, bytecode, or binary code to determine their origins (e.g., pedigree and version)."*
- NASA IV&V is beginning to invest in Origin Analysis to reduce the software supply chain risk
  - Identifies CVEs that may be present in re-used open source libraries/code
  - Providing scanning as a service as a part of the Secure Coding Portal – performed by SCP team
- Tools being used
  - Sonatype (auditor version)
  - Black Duck HUB
  - OWASP Dependency Check
  - Work being performed to automate and consolidate report creation from all three tools

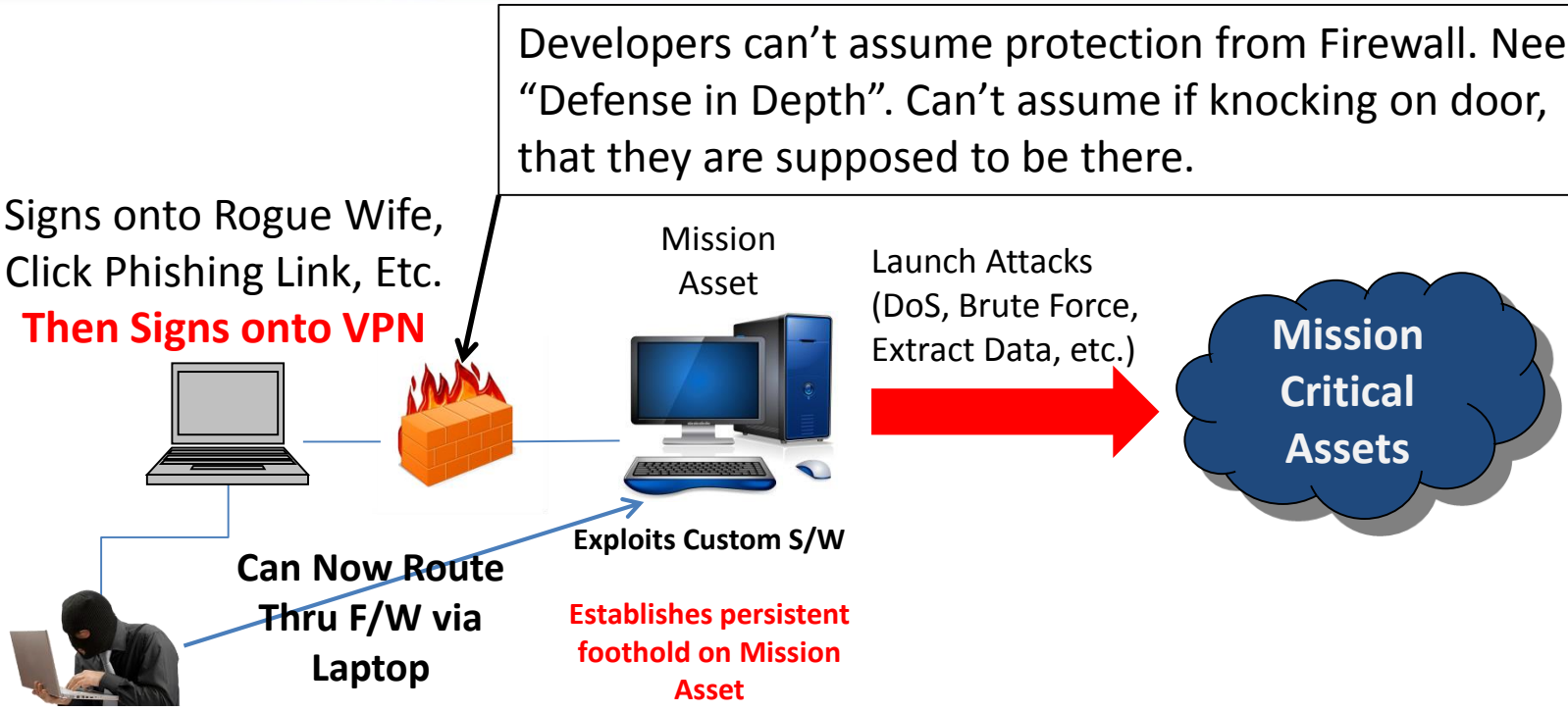
Developers should be using tools BUT IV&V / SwA could also use tools!!

Summary

- NASA starting to make conscious effort to reduce the number of vulnerabilities in their missions
  - IV&V is now looking at security as a part of mission assurance approach
  - NASA Procedural Requirements (NPRs) now have “security” requirements
  - SwA assurance standard security updates are being worked
  - OCIO Provided Security Training (i.e. Codiscope)
  - Secure Coding Portal
  - Blue Team Vulnerability Assessment Program (BT-VAP) assesses mission survivability to cyber attack
    - Custom SW assessments are integral part of approach but is accompanied by network exposure (i.e. Threat Pairing)

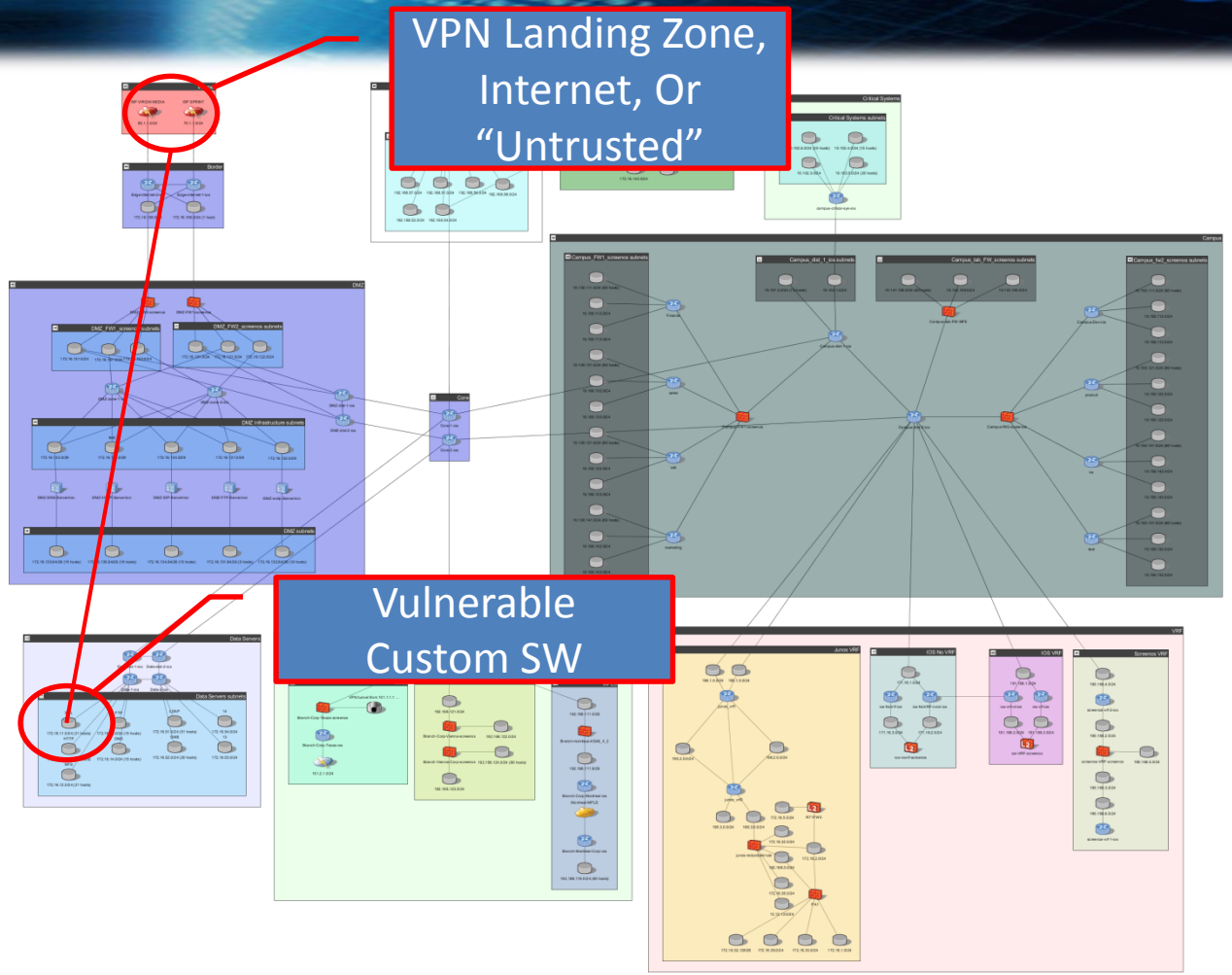
BACKUP SLIDES

Example SW Impacting Mission



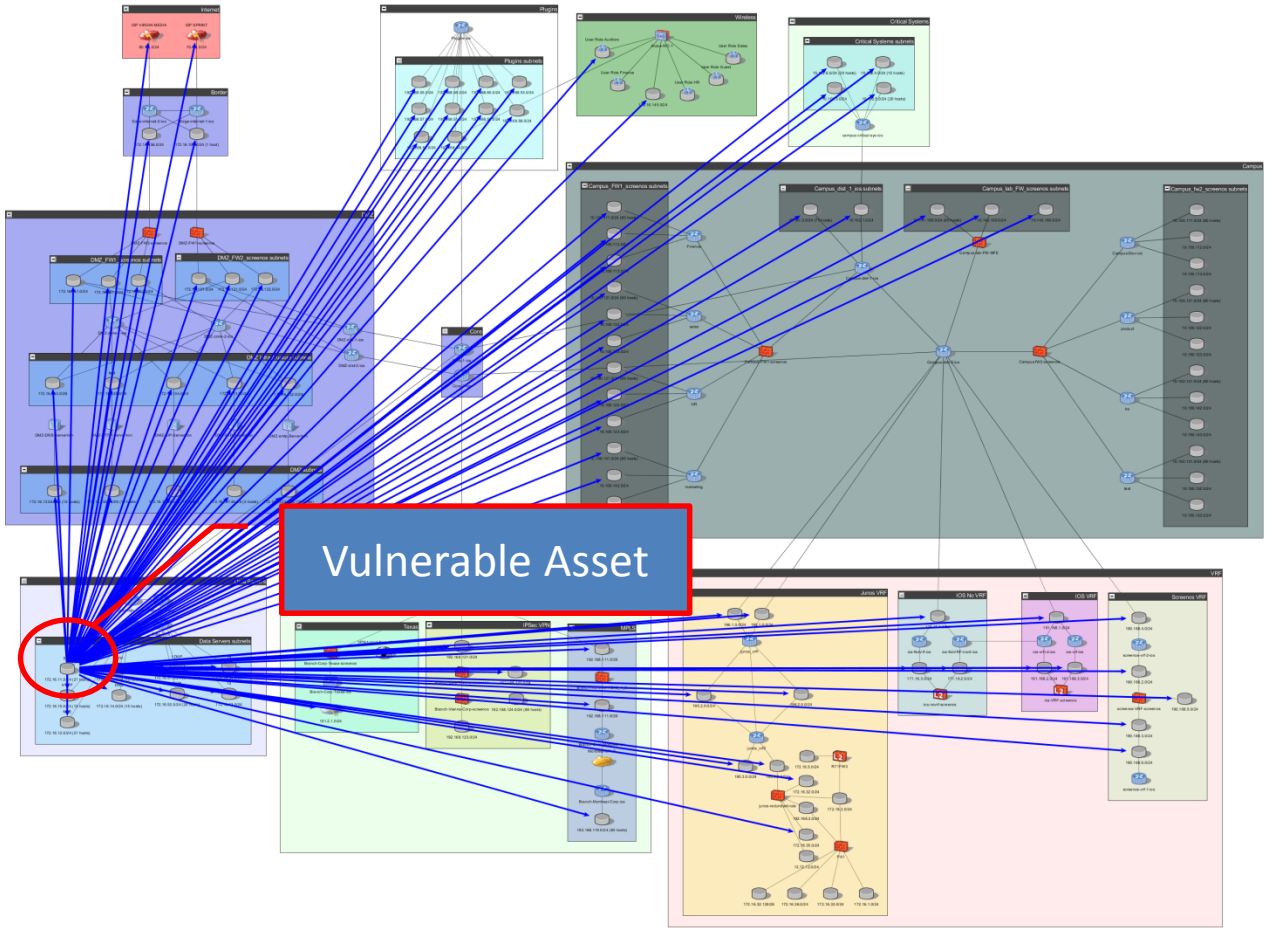
This example will depict how unsecure software within a network can potentially impact critical mission assets

Sample Exposure



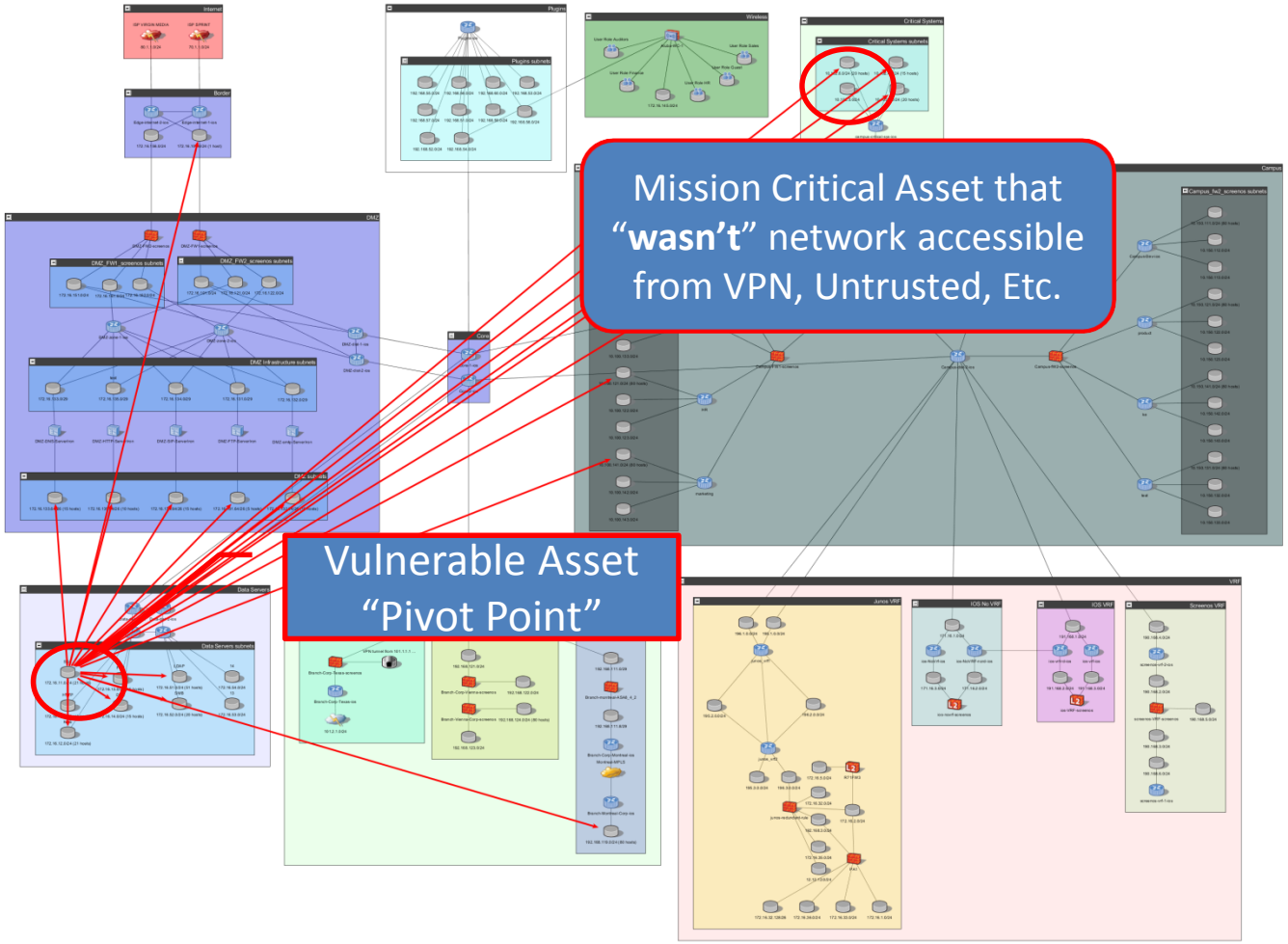
Demonstrates that a pathway exists from the VPN Landing Zone, Internet, Or Untrusted. Has network access to a vulnerability that was identified by software analysis (binary and source).

Sample Exposure



Demonstrates all outbound access paths (**Pivoting**) from the vulnerable asset

Sample Exposure



Demonstrates potential vulnerabilities that could be exploited from this server

BT-VAP Overview

- Blue Team Vulnerability Assessment Program (BT-VAP) Defined:

  An evaluation to ascertain the operational security posture of an agency's critical mission systems/networks; focusing on the IT assets & supporting infrastructures that enable the mission to operate

- Blue Team refers to the tactics and techniques employed: a blue team is done in full coordination with the mission elements being assessed in a transparent manner with no impact to mission ops

- As BT-VAP evaluates missions "end-to-end"; it is often perceived (incorrectly) as duplicative of other assessment type activities:

Blue Team VAP Evaluation Focus	Focus of Other Assessment Type Activities
Determine Operational Security Risk Posture	FISMA: State of Regulatory Compliance (per NIST 800-53)
Assist Mission Elements to understand/mitigate Security Risks	Audits: Detecting fraud or error/ evaluate adequacy of controls
Comprehensively Assess all factors (backups, infrastructure etc)	Pen Test: Simulate attack on asset(s) to discover vulnerabilities
Fully evaluate without disrupting mission operations	IG: Examine actions of a government agency; focus on misuse

BT-VAP Team

- Need for a Blue Team to comprehensively evaluate CS-IA factors in a methodical manner results in needing Subject Matter Expertise across multiple areas to focus on this specific evaluation
- Use of a "risk jury" with SMEs from multiple disciplines with varying perspectives to provide a comprehensive "360°" assessment view

Five Key Role Specialists on this BT-VAP Risk Jury:

Security Analyst/ Threat Protection	***Network Security/ Information Assurance***	***ICS/SCADA /Computer Network Defense***	***Space Systems/ Program Protection***	***Software Security/ Cybersecurity Operations***

We evaluate an organization "top to bottom" (from policy/plans to operational posture) to examine IF and HOW they address CS-IA risk factors to determine what their operational security posture is compared to other similar environments

CS-IA = Cybersecurity - Information Assurance

BT-VAP Testing Capabilities

- **<u>Cybersecurity Evaluation:</u>** determine critical assets, model the "mission thread" that these critical assets use to enable the mission – then do a selective "deep dive" on potential points of vulnerability based on a test plan & approved rules of engagement to cover:
  - Space/Mission Systems (ground)
  - Industrial Control Systems/SCADA
  - Supporting Infrastructure: (Layer-2/Layer-3 Network Devices, Controlled Interfaces/Firewalls, Cybersecurity Defense (CND) mechanisms, etc)
- **<u>Software Security Evaluation:</u>** analyze the software code base which supports critical assets and mission threads
  - Source Code Analysis
  - Binary/Compiled Code Analysis (S/W Origin Analysis)
- BT-VAP Testing Techniques involve a combination of three principal methods:
  - Analytic/Tabletop Analysis
  - In the Lab Testing (modeling-simulation environment)
  - On-Site with a "flyaway" team with mobile assets

We evaluate an organization to examine IF and HOW they address CS-IA risk factors to determine what your operational security posture is compared to other similar environments

Back

CS-IA = Cybersecurity - Information Assurance