

A satellite view of Earth is shown on the left side of the slide, featuring the Gulf of Mexico, the Atlantic Ocean, and parts of North and South America. A thick red horizontal band spans across the middle of the slide, containing the main title in white text.

Leaning Into Large Ground System Vulnerabilities with Machine Learning

Raytheon Intelligence, Information and Services

David A Wilson, Addy Moran, Joshua Welch

February 26, 2019

Current Situation

Modern ground systems have complex combinations of COTS/FOSS products

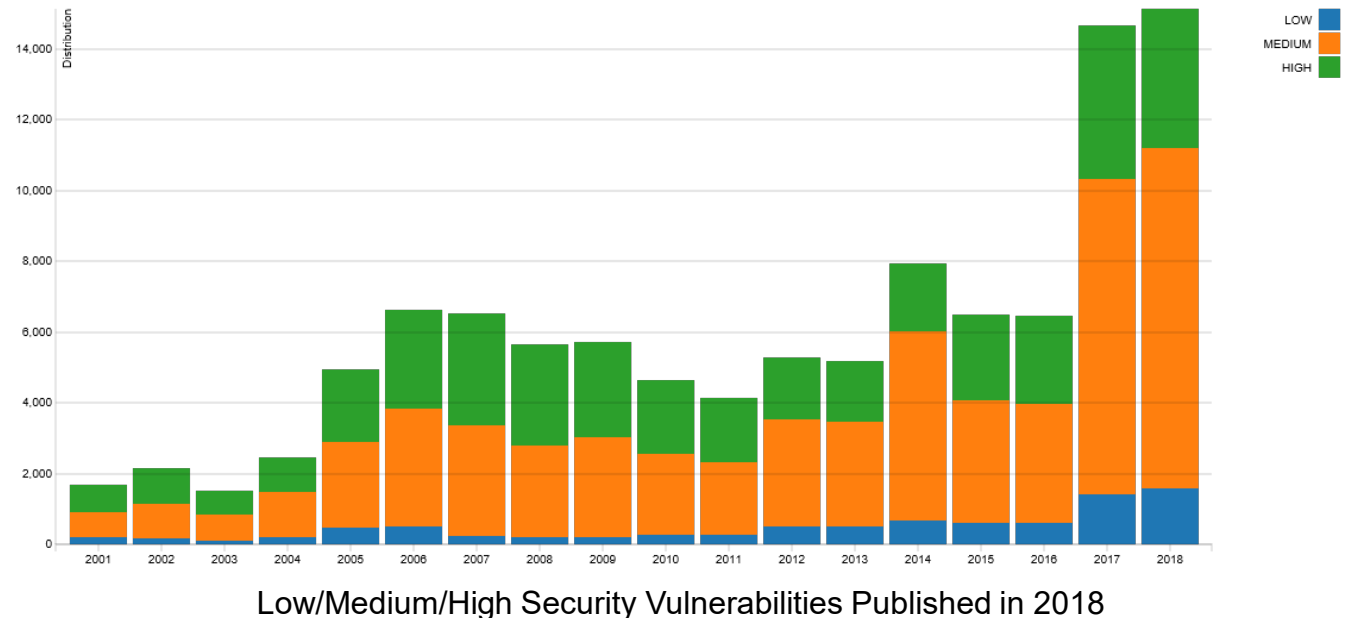
Vulnerability updates can become an unmanageable amount of work for system administrators.

Potential for:

- Alert fatigue
- Updates unsuccessfully processed

4,800+ open source vulnerabilities were reported in 2017¹

15,130 Security Vulnerabilities published in 2018
(**3,944** High Priority)²



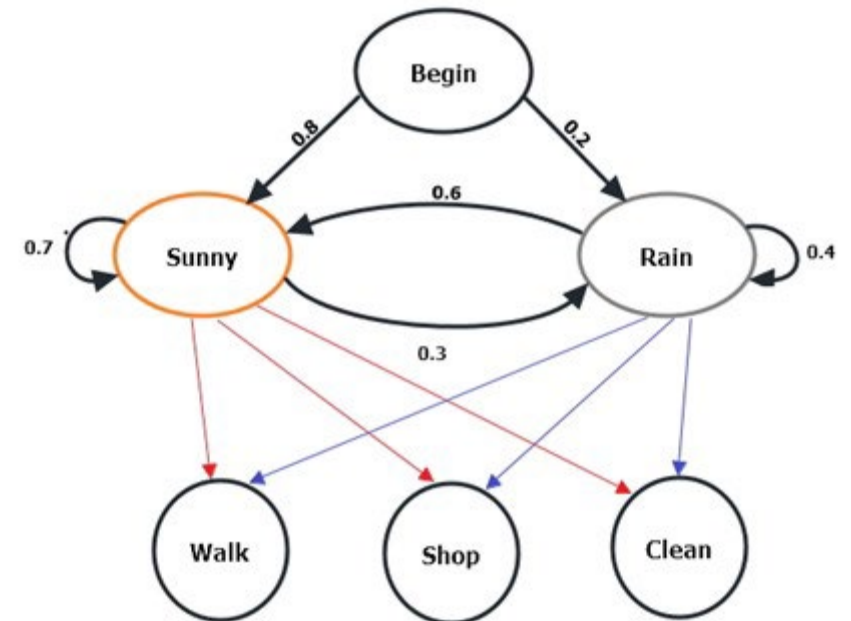
(1) 2018 Open Source Security and Risk Analysis, Synopsys Center for Open Source Research & Innovation
(2) As of 12/31/2018, <https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time>

Approach

Create a risk model that provides risk posture of sum of COTS/FOSS vulnerabilities and provide suggested patches to improve risk

Use Markov chains, Human-Interactive Machine learning, and data-mining to prioritize system patches

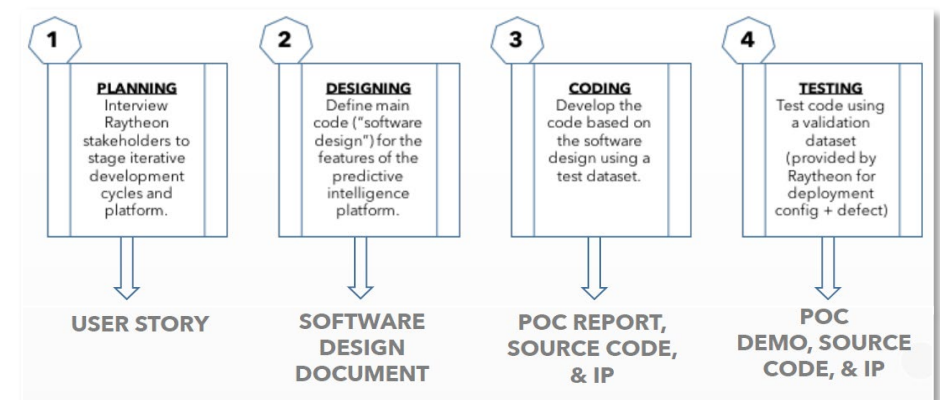
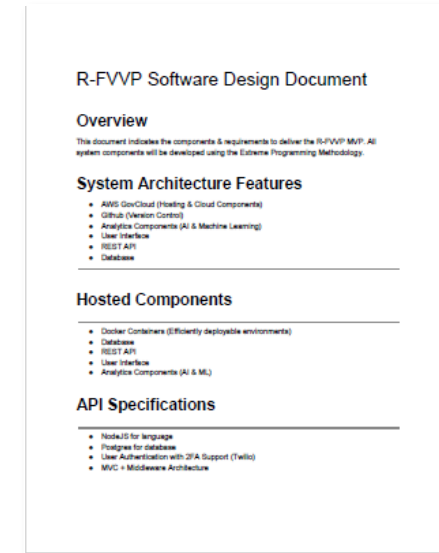
Administrator can easily improve overall system risk posture by applying suggested prioritized patches



Example Markov Chain Model

Approach

- Use a Markov chain model to simulate the movements of a hacker inside a system.
- Quantitative security data such as Operating System (OS) scans, network scans, and network topologies to classify the severity of each vulnerability.
- Takes into account the number of connections per each component and classifies a weight per vulnerability, and uses this to rank patches.
- This vulnerability rank is used as a prioritization scheme.
- The algorithm uses vulnerability data and integrates the data into the network topology and builds an absorbing Markov model to predict which systems an attacker is most likely to attack (and therefore patching priorities).



Vulnerability Data

- The Common Vulnerability Scoring System 3.0 (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
- CVSS 3.0 metrics for risk assessment



Exploitability Metrics: Reflect the characteristics of the thing that is vulnerable. It has Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR) and User Interaction (UI).

Scope (S): Scope refers to the collection of privileges defined by a computing authority when granting access to computing resources. When the vulnerability of a software component governed by one authorization scope is able to affect resources governed by another authorization scope, a Scope change has occurred.

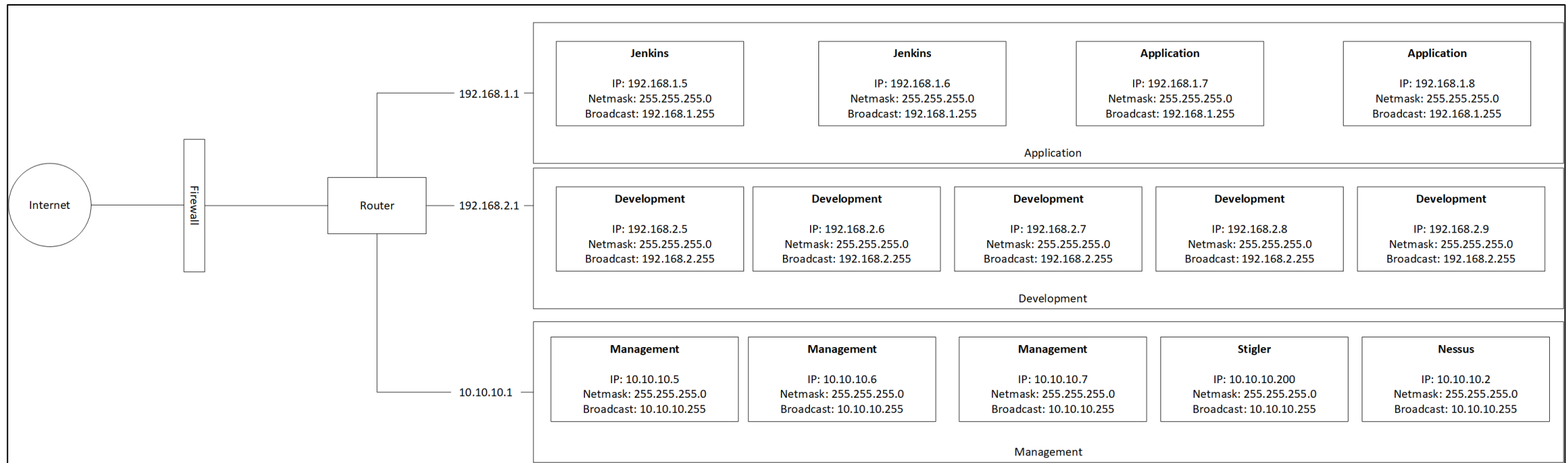
Impact Metrics: Refer to the properties of the impacted component. It has Confidentiality Impact (C), Integrity Impact (I) and Availability Impact (A).

Temporal Metrics: Measure the current state of exploit techniques or code availability, the existence of any patches or workarounds, or the confidence that one has in the description of a vulnerability: Exploit Code Maturity (E), Remediation level (RL), Report Confidence (RC).

Environmental Metrics: Enable the analyst to customize the CVSS score depending on the importance of the affected IT asset to a user's organization, measured in terms of complementary/alternative security controls in place, Confidentiality, Integrity, and Availability.

Representative System

- Secure DevOps Environment instantiated on Raytheon's internal Cyber Range
- ~50 FOSS Products
- VMWare, STIG Hardened RHEL 7.5, Containers, etc.



Decision Support Process

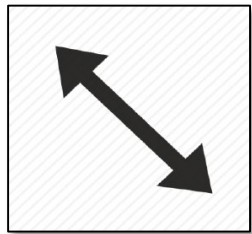
Assess System Risk

Baseline System Patches

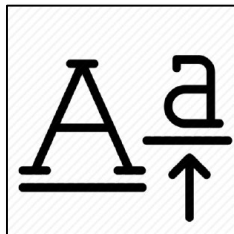
Rank Vulnerabilities / Patches

Provide Decision Logic for Validation

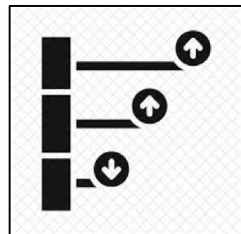
Provide Upgrade Path



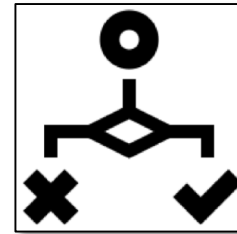
Using known vulnerabilities (e.g. NVD), display a risk assessment of a subject FOSS stack and network topology “system”.



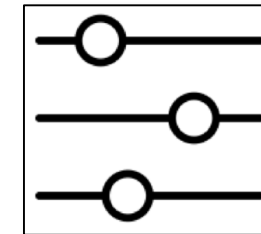
Utilizing the subject system, create a baseline of the patches required for a fully qualified (patched) system.



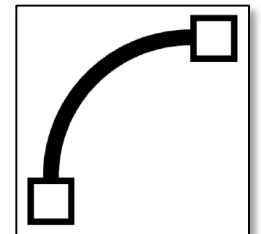
Using a graphing or data visualization interface, rank the most critical patches to the least critical.



Provide decision logic for the ranking utilizing text and visual components.



Create decision logic parameters to display tangible evidence that supports the ranking (severity, exploitability, etc.).



Provide the most optimal upgrade path (prescriptive) for the patch.

Decision Support System

- Provides a comprehensive, prioritized list of patches
- Patches are organized in the order that is suggested the patch administrator apply them
- Can be deployed in AWS or as a containerized service

The screenshots illustrate the FVWP (Firmware Vulnerability Workbench) interface, which provides a comprehensive view of system vulnerabilities and patches. The interface is organized into several key sections:

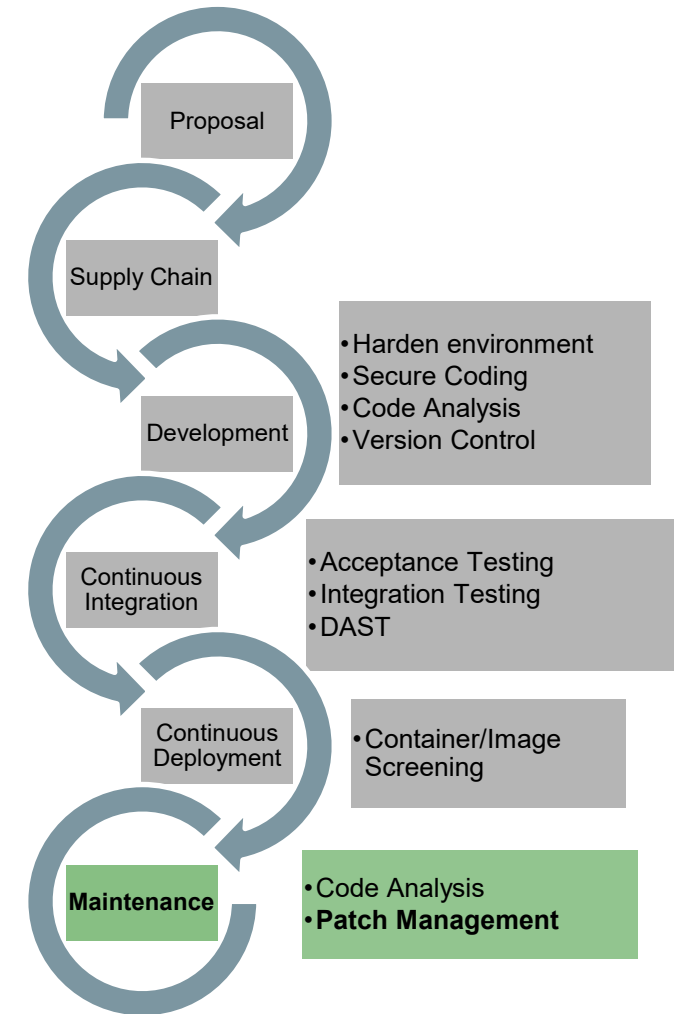
- Network Host List:** A table showing IP addresses and the number of FOSS updates for each host.

IP	FOSS Updates
10.10.10.6	5
192.168.1.6	5
192.168.2.6	32
192.168.1.5	33
- Vulnerability Details:** A detailed view of a specific vulnerability, such as RHEL 7 : dhcp (RHSA-2018:1453). It includes:
 - Plugin Info:** ID (109839), NASL Family (Red Hat Local Security Checks), Type (local), Protocol (tcp), Service Name (unspecified), Port (0), Publish Date (2018/05/16), and Updated Date (2018/09/07).
 - Vulnerability Info:** ID (redhat-RHSA-2018-1453.nasl), IAVA (2018-A-0162), Risk Factor (High), Severity (5), Exploit available (true), Exploit Ease (Exploits are available), and Metasploit (DHCP Client Command Injection (DynoRoot)).
 - Patch Info:** FNAME (redhat-RHSA-2018-1453.nasl), Publication Date (2018/05/15), and References (https://access.redhat.com/security/vulnerabilities/3442151, http://rhn.redhat.com/errata/RHSA-2018-1453.html, https://www.redhat.com/security/data/cve/CVE-2018-1111.html).
 - Description:** An update for dhcp is now available for Red Hat Enterprise Linux 7. This update is rated as having a security impact. (CVSS base score, which gives a detailed the CVE link(s) in the References section. This protocol that allows individual devices on a network, including an IP address, a sub package provides a relay agent and ISC DHCP server. Security Fix(es) : * A command integration script included in the DHCP client packages provide a relay agent and ISC DHCP server, or an attacker on the local network.
- System Patch Summary:** A dashboard showing the overall system status, including 24 patches, 2:35 time needed, and a risk summary with 4 High, 5 Medium, and 12 Low priority items.
- FOSS Patch List:** A table listing patches for various FOSS (Free and Open Source Software) components, including their CVSS Base Score, Impact, Exploitability, and Vulnerability Risk.

Name	CVSS3 Base Score	Impact	Exploitability	Vulnerability Risk
RHEL 7 : dhcp (RHSA-2018-1453)	7.5	5.87	1.62	0.014
RHEL 7 : gnupg2 (RHSA-2018-2181)	7.5	3.60	3.89	0.014
RHEL 7 : Red Hat Ceph Storage 1.3.3 (RHSA-2016-1972)	7.5	3.60	3.89	0.014
RHEL 7 : ceph (RHSA-2016-1384)	6.5	3.60	2.84	0.012
RHEL 7 : samba (RHSA-2018-2613)	3.1	1.41	1.62	0.006

Future Work

- Algorithm Improvements: integrate additional vulnerability data sources
- UI/UX Optimization: Develop system status visualization
- Develop “patching pipeline” for use in Secure DevOps by automating:
 - the gathering of information
 - the screening process
 - patch testing and deployment



Example of a Secure DevOps Pipeline