Cyber Risk Scoring and Mitigation (CRISM)
Customer Need - Life in the Security Operation Center

- Intrusion Detection System alerts
- Network configuration
- Security Risk Assessment
- Vulnerability reports
- Prioritized Mitigation Plan
- Users and data assets
- Apache HTTP Server 2.4 vulnerabilities
- Security advisories
Market Needs

- Security metrics will play a key role in supporting risk management and mitigation decisions for critical infrastructure.

- Availability of quantitative insights ensure operational resilience and assist in development of cost-effective mitigation plan.

- IT and OT organizations need tools to aid in continuous assessment of their cyber resilience capabilities.
Approach

• Quantitatively analyze *cyber risk* of company’s hardware and software systems

• Provide *security scores* provided at several levels of granularity

• Provide prioritized *mitigation* plan to reduce cyber risk and improve cyber resilience

• Adapt to *diverse* network configurations and dynamically scaling cloud environments
Enumerating Vulnerabilities Misses the Big Picture!
Requirements

• Lateral propagation analysis
  • Analysis provides information on stepping-stones, pivot points, attack paths, vulnerable nodes that provides insights into adversarial strategies

• Security metrics
  • Quantification of attack surfaces based on exploitability and impact analysis

• Prioritized mitigation plan
  • Ordered list of vulnerabilities to patch or apply security controls to achieve a desired security score.

• Compliance with NIST cyber security framework
## Potential Solutions

<table>
<thead>
<tr>
<th></th>
<th>Cyber Risk analysis based on lateral propagation analysis</th>
<th>Scoring based on vulnerability graphs</th>
<th>Prioritize mitigation plan</th>
<th>Identify most vulnerable paths and nodes</th>
<th>Impact analysis based on asset importance</th>
<th>Quantify and visualize risk scores at several levels of granularities</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRISM</td>
<td>✓ ✓ ✓</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓</td>
<td>✓ ✓ ✓</td>
<td>✓ ✓ ✓</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>Quadmetrics</td>
<td>✓ ✓</td>
<td>✓ ✓</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>Bitsight</td>
<td>✓ ✓</td>
<td>✓ ✓</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>SecurityScorecard</td>
<td>✓ ✓</td>
<td>✓ ✓</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>Efortresses</td>
<td>✓ ✓</td>
<td>✓ ✓</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>Beyond Security</td>
<td>✓ ✓</td>
<td>✓ ✓</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>Nexpose</td>
<td>✓ ✓</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓</td>
<td>❌</td>
<td>❌</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>Core Security</td>
<td>✓ ✓</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓</td>
<td>❌</td>
<td>❌</td>
<td>✓ ✓ ✓</td>
</tr>
</tbody>
</table>
Cyber Risk Scoring and Mitigation (CRISM©)

- Provides cyber security scores and prioritized mitigation plan
- Works with diverse software, networking and cloud environment.
- Provides quantitative risk assessment and categorizes attack paths based on the impact of vulnerabilities
Measure Cyber Risk - Attack Graphs

- Adversaries penetrate network through a **chain of exploits**
  - Each exploit lays foundation for subsequent exploits
- Chain is called an **attack path**
- All possible attack paths form an **attack graph**
- Generate attack graphs to mission critical resources
- Report only those **vulnerabilities** associated with the **attack graphs**
Multi-step Attacks

Internet

Demilitarized zone (DMZ)

Web Server

Firewall 1

Buffer Overflow

Shared Executable

NFS shell

Firewall 2

Trojan horse

Organization

WebPages

File Server

workStation
Bayesian Attack Graph

A 192.168.51.59 Web Server

B 192.168.51.60 Database Server

C 192.168.51.61 Proxy Server

D Remote Attacker

Probability of successful exploit:
- A to B: 0.65
- A to C: 1.00

Pr(A)=0.61 Unconditional Probability

<table>
<thead>
<tr>
<th></th>
<th>Pr(B)</th>
<th>Pr(¬B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.85</td>
<td>0.15</td>
</tr>
<tr>
<td>0</td>
<td>0.00</td>
<td>1.00</td>
</tr>
</tbody>
</table>

Pr(B)=0.60

<table>
<thead>
<tr>
<th></th>
<th>Pr(C)</th>
<th>Pr(¬C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.70</td>
<td>0.30</td>
</tr>
<tr>
<td>0</td>
<td>0.00</td>
<td>1.00</td>
</tr>
</tbody>
</table>

Pr(C)=0.49

<table>
<thead>
<tr>
<th></th>
<th>Pr(D)</th>
<th>Pr(¬D)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.70</td>
<td>0.30</td>
<td></td>
</tr>
</tbody>
</table>

Pr(D)=0.70

<table>
<thead>
<tr>
<th></th>
<th>Pr(A)</th>
<th>Pr(¬A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.00</td>
<td>0.00</td>
</tr>
<tr>
<td>1</td>
<td>0.65</td>
<td>0.35</td>
</tr>
<tr>
<td>0</td>
<td>1.00</td>
<td>0.00</td>
</tr>
<tr>
<td>0</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

Pr(A)=0.61 Unconditional Probability

D 192.168.51.61.60 Database Server

C 192.168.51.61 Proxy Server

D Remote Attacker
Criticality Analysis

- Network Scanning
- Network Logs
- Graph Generation
- Attack Graph
- Minimized Network Risk in Optimized Resource Allocation
- Critical Path Analysis
- Resource Allocation
- Critical Paths
- Criticality Calculation
- Node Ranking
- Host Scanning
- Host Logs
- Wireshark TCP/DNP3 dump

Instruments:
- Network Scanner (Nessus)
- Host Scanner (Qualys)
- EDS Network

Tools:
- CRISM

Technologies:
- Nessus
- Qualys
- Wireshark

Methods:
- Graph Generation
- Criticality Calculation
- Node Ranking

Resources:
- Critical Path Analysis
- Optimized Resource Allocation
Cyber Risk Scoring and Mitigation (CRISM©)

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Identification of Attack Surfaces</td>
<td>Acquisition of vulnerability scores from live threat intelligence feeds and vulnerability databases</td>
</tr>
<tr>
<td>Lateral Propagation Analysis</td>
<td>Network Vulnerability Tests and attack graph generation</td>
</tr>
<tr>
<td>Security Metrics and Prioritized Mitigation Plan</td>
<td>Bayesian attack graph modeling techniques to categorize attack paths by impact, cost and degree of difficulty</td>
</tr>
<tr>
<td>Compliance</td>
<td>NIST Cybersecurity Framework</td>
</tr>
<tr>
<td>On demand and real-time access to quantifiable cyber risks</td>
<td>Cloud based risk assessment tool</td>
</tr>
</tbody>
</table>
CRISM Benefits

• Distills *complex threat analysis* processes into numerical risk score.
• Provides a detailed, *prioritized mitigation plan*.
• Employs *visualization* techniques to ensure information synthesis.
• Provides *insights* into risk posed by external vs. *insider* adversaries
• Adaptable in diverse network configuration, *low overhead* and scalable
Transition Activities

• CRISM© is property of ODU
• Software License available from www.crism.org
• Patent Pending
• Working with CIRI on commercialization plan
Transition Activities

• **FBI (Norfolk Cyber Crime Unit)**- Scalable testing of CRISM© on a network with 100 nodes

• **Sentara Health** – Evaluation of CRISM© in production environment

• **Naval Surface Warfare Center Crane** – CRISM© demonstration at Glendora Lake Test Facility

• **Accenture** – Evaluation of CRISM© for OT customers
Evaluation of CRISM at Sentara Healthcare

• Sentara Healthcare serves over 2 million residents in 100 sites in Virginia and North Carolina

• Interested in complementary suite of tools that provide security risk assessment and prioritized mitigation plan

• Evaluation on Sentara Healthcare’s cyber infrastructure
  • Production IT systems at Norfolk site running diverse Windows and Linux distributions
  • Complement to Nessus
## Evaluation of CRISM at Sentara Healthcare

<table>
<thead>
<tr>
<th>Test Cases</th>
<th>Date</th>
<th>Duration</th>
<th>Objective</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test 1</td>
<td>Jun 15, 2018</td>
<td>3:30 – 5:45</td>
<td>Test effectiveness of CRISM in Sentara’s IT cyber infrastructure</td>
<td>37 nodes, 65 vulnerabilities</td>
</tr>
<tr>
<td>Test 2</td>
<td>Jun 21, 2018</td>
<td>11:07 – 13:38</td>
<td>Estimate the total time for assessing target machines with mix of different OS (Windows &amp; Linux)</td>
<td>Scanning time – approximately 2 hours and 30 minutes</td>
</tr>
<tr>
<td>Test 3</td>
<td>June 22, 2018</td>
<td>11:33 – 13:50</td>
<td>Develop test scenarios with varied combinations of mission specific IT configurations</td>
<td>Two groups of OS i.e. Windows and Linux. There are 6 nodes in each group. Windows group took less time than Linux group.</td>
</tr>
<tr>
<td>Test 4</td>
<td>July 27, 2018</td>
<td>14:36 – 15:17</td>
<td>Develop test scenarios with varied combinations of mission specific IT configurations</td>
<td>Two groups of OS i.e. Windows and Linux. There are 6 nodes in each group. Windows group took less time than Linux group.</td>
</tr>
<tr>
<td>Test 5</td>
<td>Dec 12, 2018</td>
<td>10:37 – 18:17</td>
<td>Conduct live testing on operational environments, Conduct maximum capacity testing with varying application traffic speeds and incoming connections</td>
<td>167 nodes, 111 vulnerabilities, scanning time – approx. 9.5 hours.</td>
</tr>
</tbody>
</table>
Summary

• Deployment of CRISM in additional Sentara Healthcare sites in Virginia

• Aiding Sentara sites without a full fledged security team with easy to digest analytics that provide increased visibility into risk and strength of existing defenses

• Exploring with Accenture on deployment of the tool in the power utility sector.