WELCOME TO THE  SEPT. 14, 2022
ISOAG MEETING
<table>
<thead>
<tr>
<th>AGENDA</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>Ed Miller / VITA</td>
</tr>
<tr>
<td>The Data-first Approach; Managing the Tension Between Security and Productivity</td>
<td>Brian Vecci &amp; Brandon Lapetina/Varonis</td>
</tr>
<tr>
<td>Activities at the Virginia Smart Community Testbed</td>
<td>David Ihrie/CIT</td>
</tr>
<tr>
<td>A Dynamic Process for Minimizing the Likelihood and Impact of Cyber Attacks</td>
<td>Chris Jensen/Tenable</td>
</tr>
<tr>
<td>Upcoming Events</td>
<td>Ed Miller/VITA</td>
</tr>
<tr>
<td>Adjourn</td>
<td></td>
</tr>
</tbody>
</table>
There are no slides available for Varonis Presentation
IoT and Related Challenges For Cybersecurity

ISOAG Meeting
September 14, 2022

Funding for many of the technologies incorporated into the Virginia Smart Community Testbed has been provided by the U.S. Department of Homeland Security, Science & Technology Directorate, under contract number 70RSAT19CB000025

David Ihrie, CTO/CIO
David.Ihrie@VirginiaIPC.Org

UNCLASSIFIED
Topics

- VIPC?
- So what have you been up to lately?
- Cybersecurity Implications
- Facing the Challenges
Virginia Innovation Partnership Authority

Mission
Support and connection for entrepreneurial ecosystems and stakeholders around Virginia, including startup incubators and accelerators

Commercialization Division
Mission
Grant funding in support of tech-based research, development and commercialization to drive economic growth in Virginia

Investment Division
Mission
Seed and early-stage funding for Virginia-based companies with high potential for rapid growth and significant economic returns

Strategic Initiatives
Mission
Leadership for strategic initiatives that explore and shape programs designed to attract and grow innovation and new industries

Strategic Initiatives Current Portfolio

[Images of SCITI Labs, VIPC Smart, Virginia Smart Community Tested Stafford, Va., VIPC Public Safety Innovation Center, Virginia Unmanned Systems Center]
Topics

- VIPC?
- So what have you been up to lately?
- Cybersecurity Implications
- Facing the Challenges
WHAT IS THE TESTBED?

The Commonwealth’s home for developing Smart Technology

Mission: Serves as Virginia’s “living laboratory” to test new smart technology and be a “model smart community” by communities across the nation

Vision: Lead the county and Commonwealth in Smart Community implementation and serves to accelerate technology solutions for the Commonwealth

Purpose: Foster growth through public-private partnerships, sponsors, investors, entrepreneurs, and pilot projects opportunities

From Innovation to Impact Under One Virtual Roof
A GROWING SUCCESS STORY

Recently recognized as a 'Smart 50 Awards' recipient: this award presented by Smart Cities Connect recognizes global smart city projects, honoring the most innovative and influential work.

Attracting global businesses:
"One of the efforts we highlighted at INTERSCHUTZ was the Virginia Smart Community Testbed (VA Testbed), a dynamic lab showcasing innovations developed to provide new solutions for homeland security and dual-use technologies— one of S&T’s most successful public-private partnerships to date. The idea for the VA Testbed was born more than three years ago, as S&T came together with the Virginia Innovation Partnership Corporation (VIPC), the Commonwealth of Virginia, and Stafford, Virginia, to convert a former convenience store into a cutting-edge testbed for technologies that can be applied to real-world uses benefiting the public."

Dan Cotter
A Network of Living Laboratories
Many made possible by DHS Support

Winchester, Virginia
Municipal Drone Ops

Roanoke, Virginia
Integrated Water Management

Town of Cary, North Carolina
Civic Infrastructure

WASHINGTON DC
In-Building Sensors

Stafford, Virginia
Smart Communities
Secure IoT
Public Safety

RVA
Airspace Awareness

Port Security
Advanced Air Mobility

Smart Bases
Workforce Development
AR/VR/Immersive Tech

A Network of Living Laboratories
Public-Private Partnership Deploys Flood Sensors

Commonwealth Investment

VA-FIX Supports Airspace Coordination For Drone Operators

Commonwealth Data Trust

Legacy IFLOWS Network Informs NWS Flood Alerts

Stafford County Using Data for Emergency Management of Flooding

Virginia Department of Emergency Management

Homeland Security

Science and Technology

VIPC

VIRGINIA INNOVATION PARTNERSHIP CORPORATION

Public-Private Partnership Deploys Flood Sensors

Commonwealth Investment

VA-FIX Supports Airspace Coordination For Drone Operators

Commonwealth Data Trust

Legacy IFLOWS Network Informs NWS Flood Alerts

Stafford County Using Data for Emergency Management of Flooding

Virginia Department of Emergency Management

Homeland Security

Science and Technology

VIPC

VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Flood Sensors in Operation

Flood map for Harrel Road

Flood chart for Brooke Road

Harrel Road Sensor Activated

Email Alert Notification

400 Nationwide

100 in Virginia

14 in Stafford County
SMART LIGHTING

- First deployment of its kind in North America
- Reduced energy and increase cost savings
- Provides a wireless mesh broadband network
- 90% faster implementation of gigabit networks
Digital Transformation of Infrastructure

- Air Quality/Wildfire
- Weather Stations
- Smart Lighting/WiFi
- Drone Video/Data
- Information Kiosks
- Robotic Devices
- Flood
AAM/Airspace Awareness
Smart Facilities for Building Management and Public Safety
Topics

- VIPC?
- So what have you been up to lately?
- Cybersecurity Implications
- Facing the Challenges
IoT / ICS Security at the Edge Challenge – Fit For Purpose Security

IoT Device Categories

1. Informational
   - Air Quality
   - Animal Tracking
   - Cost: $10

2. Operational
   - Flood
   - Cost: $100

3. Protected
   - School Bus Cameras
   - Cost: $1,000

4. Critical
   - Grid Protection Sensors
   - Energy, Internet, Banking
   - Cost: $10,000

5. National Security
   - National Security Infrastructure or DoD/DHS Operational Usage
   - Cost: $100,000

Data Sensitivity

- Data provided, no direct action
- Data provided, automated action may result
- Protected data (HIPAA, FERPA)
- Critical Infrastructure/Security Applications
- National Security Infrastructure or DoD/DHS Operational Usage

Cost Per Device
Functional Block Diagram

IoT Block Diagram and Threats
(Not all elements present in all systems)

<table>
<thead>
<tr>
<th>Point of Attack</th>
<th>Threat</th>
<th>Potential Solution</th>
<th>Applicable Device Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Data Skimming (Theft)</td>
<td>Device Storage Encrypted</td>
<td>3+</td>
</tr>
<tr>
<td></td>
<td>Repurposed Infrastructure</td>
<td>Behavioral Controls on Data Flow</td>
<td>1+</td>
</tr>
<tr>
<td></td>
<td>Bogus Commands</td>
<td>Data Diode</td>
<td>2+</td>
</tr>
<tr>
<td></td>
<td>Corrupted Data</td>
<td>Operational Checks</td>
<td>1+</td>
</tr>
<tr>
<td>In Transit</td>
<td>Device Spoofing</td>
<td>Device Validation</td>
<td>2+</td>
</tr>
<tr>
<td></td>
<td>Data Skimming (Theft)</td>
<td>End-to-End Encryption</td>
<td>2+</td>
</tr>
<tr>
<td>System</td>
<td>Physical Access</td>
<td>Zero Trust</td>
<td>2+</td>
</tr>
<tr>
<td></td>
<td>Data Leakage (Inappropriate Sharing)</td>
<td>Event-driven sharing</td>
<td>2+</td>
</tr>
</tbody>
</table>

Demarc Point – IoT Security Ends Here, Other Security Measures Beyond This Point

- Assumes other security procedural controls in place (e.g., personnel controls, training, response plans)
- Categories per prior diagram of data sensitivity
IoT/IIoT/ICS Security is *Different*

(-) Large numbers of devices
(-) Limited/no physical security
(-) Increasingly driving critical operations
(-) Public comms networks for data

(+/-) Autonomous operation
(+/-) Quantum computing

(+) Limited range of acceptable behaviors (for now)
(+) Network effect for self-healing
(+) Power at the edge
(+) No humans in the loop

Secure the Data
Topics

➢ VIPC?

➢ So what have you been up to lately?

➢ Cybersecurity Implications

➢ Facing the Challenges
# Landscape Assessment Report

## Table of Contents

- **Acknowledgement**
- **Executive Summary**
- **Background**
- **Objectives**
- **Overview of IoT Solutions and Technologies**
- **Transformational Effort on Society**
- **IoT Reference Architecture**
- **IoT Cybersecurity Challenges**
- **Generic Cybersecurity Threats**
- **Common Attack Vectors**
- **Cybersecurity Threats Specific to IoT**
- **Magnification of Attack Surfaces and Security Vulnerabilities**
- **No Active Security Monitoring and Autonomous Operations**
- **No Physical Security Guarantees**
- **Cost-Effectiveness Constraints**
- **Long Service Life Without Support/patching**
- **Low Adoption of Standard Protocols**
- **IoT Protocol Rood Attacks**
- **Unintentional Radio Frequency Threats**
- **Intentional Radio Frequency Attacks**
- **IoT Privacy, Regulatory, and Legal Challenges**
- **Reviewing IoT Design Considerations**
- **Guiding Standards and Frameworks for Analyzing IoT Cybersecurity Needs**
- **IoT Device Cybersecurity Guidance for Federal Government**
- **IoT Approach and Main Concepts**
- **Impact/Relevance to IoT Cybersecurity Standards**
- **Industrial Control Systems Security**
- **IoT Approach and Main Concepts**
- **Impact/Relevance to IoT Cybersecurity Standards**
- **Protecting Information and System Integrity in ICS Environments**
- **IoT Approach and Main Concepts**
- **Impact/Relevance to IoT Cybersecurity Standards**
- **Zero Trust Architecture**
- **IoT Approach and Main Concepts**
- **Impact/Relevance to IoT Cybersecurity Standards**
- **Framework for Improving Critical Infrastructure Cybersecurity**
- **IoT Approach and Main Concepts**
- **Impact/Relevance to IoT Cybersecurity Standards**
- **Security and Privacy Controls**
- **IoT Approach and Main Concepts**

## IoT Cybersecurity

### Landscape and Standards Assessment

**Table of Figures**

- Figure 1 - IoT Security Types (Source: IoT Security and Automation: Infographic, www.postscript.com)
- Figure 2 - Example of Homogeneity within IoT Networks (Source: www.crispideasystems.com)
- Figure 3 - Various Types of Radio Frequency Antennas

---

**IoT Cybersecurity**

Page iii
Landscape Assessment Report

17 Cybersecurity
Landscape and Standards Assessment
March 31, 2022

- Poor antenna design, implementation, and/or placement of transmitters and receivers
- Intentional Radio Frequency Attacks
  - Intentional interference or jamming is performed by an entity with a deliberate intent to disrupt, disconnect, or degrade communications. Malicious jamming and nuisance jammers are two types of intentional interference. Individuals with malicious and criminal intent conduct malicious jamming, and such nefarious intent may be to prevent friendly organizations or systems from operating as required, conceal an ongoing criminal activity, or as other possible motivations.
  - There are generally two types of intentional radio frequency attacks: transmission spoofing, where malicious nodes masquerade as authentic transmitters via high power RF transmissions that overpower legitimate transmitters and node cloning, where malicious nodes masquerade as authentic network members using cloned manipulated channels.

Figure 3 - Various Types of Radio Frequency Jamming

Bad actors target Wi-Fi networks using usually by directly affecting 802.11n and 802.11ac devices (2.4GHz - 5GHz) to increase aggregate bit error rate or overpower individual device's ability to transmit or receive. Common Wi-Fi attacks include:
- De-authentication DDoS attacks: Force Wi-Fi clients to disconnect from an authorized access point and attempt to reestablish the connection handshake, so an adversary can collect the retransmission information or credential exchange.
- Rogue access points: Wireless access points that broadcast at a much higher decibel level, effectively overpowering and making invisible authorized access points and forcing Wi-Fi clients to connect to the rogue access point.
- Access point impersonation: Wireless access points that masquerade as authorized or otherwise innocuous access points to entice users to connect, so credentials or other protected information can be stolen, or services hijacked.
- MAC spoofing: Impersonating a valid hardware identifier to gain access to a secure network that uses a whitelist filter to only allow authorized clients to connect.
- WEP/WPA-PSK cracking: Collecting enough information over time to reconstruct network passwords.

Protecting Information and System Integrity in Industrial Control System Environments - NIST SP 1800-10

Intent/Approach and Main Concepts

The goal of this NIST Cybersecurity Practice Guide is to help organizations protect the integrity of systems and information by securing historical system data, preventing execution or installation of unauthorized programs, detecting anomalous behavior on the network.

This publication is broken into three sections:
- 1800-10A Executive Summary: Senior information technology (IT) executive, including chief information security and technology officers, will be interested in the Executive Summary, which describes the following topics: challenges that enterprises face in ICS environments in the manufacturing sector, example solution built at the National Cybersecurity Center of Excellence (NCCoE), benefits of adopting the example solution.
- Technology or security program managers might share the Executive Summary, NIST SP 1800-10A, with your leadership to help them understand the importance of adopting a standards-based solution. Doing so can strengthen their information and system integrity practices by leveraging capabilities that may already exist within their operating environment or by implementing new capabilities.
- 1800-10B Approach: Architecture, and Security Characteristics: Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this document, which describes what we did and why. The following
Controlled Data Sharing and Governance

- Real-time IoT Data streams shared via Data Trust permissions and governance
- VA-FIX now registered user, VIPC as Data Trust Member can upload streams or provide metadata for access
Zero Trust concepts include:

- least privilege
- identity verification
- role-based authorization
- software attestation
- policy-based data protection

Zero Trust Will Yield Zero Results Without A Risk Analysis

Over the past four years there has been an avalanche of new Zero Trust products. However during the same period there has been no measurable reduction in cyber breaches. To the contrary, ransomware, data exfiltration and lateral moving malware attacks seem to be increasing. If the emergence of Zero Trust was supposed to make us safer, it hasn’t happened yet.
IoT Critical Infrastructure Security

- “Zero Trust Security”
- Makes groups of IoT devices invisible to hackers
- Widespread adoption growing across many applications
- Critical infrastructure demo at Ft. Belvoir for power infrastructure
Device Life Cycle Management

Provisioning the Network, Automatically

- Automated creation of strong machine identities at IoT scale, managed throughout the device life cycle

- Automated device provisioning, authentication, credential management, policy-based end-to-end data security, secure updated, anomalous behavior detection, automated de-provisioning/re-provisioning
Quantum Computing

*Threat and Opportunity*

- May solve currently intractable computing problems

- Biggest advantage over traditional computing in “high-dimensionality” problems...those with lots of variables that need to be optimized at once, or...

- Public Key Encryption, making many current security architectures obsolete

- NIST has published approved list of 8....oops, 7.... Quantum-resistant encryption algorithms, such as AES 256

- We are working to validate key algorithms on intermediate computing platforms such as photonics as true quantum platforms evolve
IoT and Related Challenges For Cybersecurity

Questions?

Funding for many of the technologies incorporated into the Virginia Smart Community Testbed has been provided by the U.S. Department of Homeland Security, Science & Technology Directorate, under contract number 70RSAT19CB000025

David Ihrie, CTO/CIO
David.Ihrie@VirginiaIPC.Org
A Dynamic Process for Minimizing the Likelihood and Impact of Cyber Attacks

Chris Jensen
Public Sector Business Development
Agenda

Who is Tenable?
Start with Visibility
Risk-Based Vulnerability Management
Web Application Scanning
Securing Identity Systems
Steps to Reduce Cyber Risk
Who is Tenable?

Creator of the Nessus vulnerability scanner, Tenable is the first and only provider of Cyber Exposure solutions. We work with more than 40,000 organizations around the world to help them manage and measure cybersecurity risk in the digital era. We are building on our deep technology expertise as a pioneer in the vulnerability assessment and management market, providing broad visibility across the modern attack surface and deep insights to help security teams, as well as business and government executives, prioritize and measure Cyber Exposure.
Why Tenable?

TRUSTED BY OVER 40,000 ORGANIZATIONS WORLDWIDE

SEE EVERYTHING

PREDICT WHAT MATTERS

ACT TO REDUCE RISK

VISIBILITY INTO YOUR ENTIRE ATTACK SURFACE

#1 in coverage, accuracy and zero day research

On-prem & cloud solutions

#1 in VM Market Share*

100+ Integrations with leading industry partners
Start with Visibility

“You can’t protect what you can’t see”
THE MODERN ATTACK SURFACE

Adaptive approaches to assess assets across the modern attack surface
What is Risk-Based Vulnerability Management?

Attackers don’t choose from hundreds of thousands of vulnerabilities they could leverage, they choose a few they know will always work. These flaws are known and generally a fix is available but the sheer number of issues discovered and the complex environments operations teams are tasked with remediating means that it could take weeks or months to fix what matters most.
CVSS is designed to identify the technical severity of a vulnerability. What people seem to want to know, instead, is the risk a vulnerability or flaw poses to them, or how quickly they should respond to a vulnerability.”
Risk-Based Vulnerability Management

A process that employs machine learning analytics to automatically correlate:

- Assessments of traditional and modern assets across the entire attack surface
- Vulnerability severity
- Threat and exploit intelligence
- Asset criticality

... to identify which vulnerabilities pose the greatest risk.
YOU’VE GOT 99 FLAWS BUT ALL THEY NEED IS ONE
18k vulnerabilities disclosed in 2020 nearly 3x more than 2016

57% of all vulnerabilities have a CVSS base score of 7 or above

CVSS 7+

- Wastes 76% of the security teams time
- Leaves 44% of risky vulnerabilities in your environment

20% vulnerabilities have an exploit available
Conti Ransomware as a Service - Vulnerabilities Utilized

- 6 out of 7 - VPR ‘Critical’
- 1 - CVSS Critical

<table>
<thead>
<tr>
<th>CVSSv3 Score</th>
<th>VPR Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>9.8</td>
</tr>
<tr>
<td>8.3</td>
<td>9.8</td>
</tr>
<tr>
<td>8.1</td>
<td>9.2</td>
</tr>
<tr>
<td>8.1</td>
<td>9.2</td>
</tr>
<tr>
<td>5.9</td>
<td>7.4</td>
</tr>
</tbody>
</table>

| CVE-2021-34527 | 8.8 | 10.0 |

| CVE-2020-1472 | 10.0 | 10.0 |

CISA Advisory - Conti Ransomware, Sept 22, 2021
Elevation of privilege vulnerability in Windows
Used in 2019 ransomware attacks
What A Modern VM Program Looks Like

Lower Effort, Higher ROI
More efficient use of security resources
Increased ROI and cost control by discovering common issues in minutes

Unified Visibility
A holistic view of your attack surface - including IT and cloud assets with web app components
Prioritize remediation for critical assets

Comprehensive Coverage
Detect both known and unknown vulnerabilities
Identify the greatest number of vulnerabilities with fewer false positives
Reactive
Proactive
Web Application Scanning

**Dynamic Application Security Testing (DAST):** A DAST crawls a running web application through the front end to create a site map with all of the pages, links and forms for testing. Once the DAST creates a site map, it interrogates the site through the front end to identify any vulnerabilities in the application custom code or known vulnerabilities in the third-party components that comprise the bulk of the application. **Only a DAST tool can identify runtime flaws, which are not apparent in a static environment.**

**Static Application Security Testing (SAST):** A SAST analyzes static environments, i.e., meaning the source code of an application. Used for periodic assessment, It looks at the application and searches for vulnerabilities in the code.
DAST vs. SAST – Use the Right Tool for the Job
SECURE THE IDENTITY SYSTEMS THEMSELVES

“...Directory Services is the underlying infrastructure that supports authentication and authorization. Its compromise would de facto render any zero trust implementation ineffective.”

- NSTAC Report to the President on Communications Resiliency, 2022
But can you trust your identity system?

Trust is a tricky thing.
Secure the Trust Provider

Active Directory holds the keys to everything

- Governs authentication, holds all passwords
- Manages access rights to every vital asset
- Ensures the user is known and managed at all times

“...trusted identity management solutions are unquestionably foundational, as zero trust is based on a continuous cycle of credentialing, verifying, and authorizing identity for person and non-person entities.”

-NSTAC Report to the President on Communications Resiliency, 2022
Recent Department of Commerce IG Report
Recommendations to NOAA included:

1. Establish processes and procedures to *periodically review* all active directory accounts to ensure consistent adherence to the principle of least privilege per Department policy.

2. Determine the feasibility of requiring all NOAA line offices to use specialized active directory security tool(s) to conduct *periodic reviews*.

3. Establish procedures to *periodically review* active directories and ensure compliance with account management requirements as stated in the Department’s policy and following industry best practices.
Understanding Common Attack Paths

**Initial Foothold**

- **Explore**: Understand the target environment - RECON
- **Elevate**: Elevate Access - PASSWORD SPRAY
- **Evade**: Pivot to evade detection - DCSYNC
- **Establish**: Establish backdoor access & wait… - AdminSDHolder

**Phase 1**: Phish / CVE Exploit

**Phase 2**: AD Attack – Elevate / Persist

**Phase 3**: Extract / Encrypt

- **Exfil**: Extract sensitive data
- **Encrypt**: Data encryption and ransom
Identity Access Management

Indicators of Exposure

1) FIND AND FIX EXISTING WEAKNESSES
   - Immediately discover, map, and score existing weaknesses
   - Follow step-by-step remediation tactics and prevent attacks

2) MAINTAIN HARDENED SECURITY SETTINGS
   - Instantly detect new weaknesses and misconfigurations
   - Break attack pathways and keep your threat exposure in check

Indicators of Attack

3) DETECT ATTACKS IN REAL-TIME
   - Get real-time alerts and actionable remediation plans on AD attacks
   - Visualize notifications and trigger responses in your SIEM / SOAR / SOC

4) ENHANCE INCIDENT RESPONSE & THREAT INVESTIGATIONS
   - Trigger response playbooks in your SOAR
   - Search and correlate AD changes at object and attribute levels

5) Disrupt Attack Pathways

No Agents
No Elevated Privils
AD Native
Near Real Time
Steps to Reduce Cyber Risk

1. Start with visibility
2. Take a risk-based approach
3. Use a dynamic tool for a dynamic environment
4. Continuously monitor
Thank You!
UPCOMING EVENTS
IS ORIENTATION

IS Orientation

Remote - WebEx

Sept. 29, 2022

Start time: 1:00 p.m.

End time: 3:00 p.m.

Instructor: Marlon Cole

https://covaconf.webex.com/covaconf/onstage/g.php?MTID=ecbe083f9321db08a0c81eca667f50575
The next scheduled meeting for the IS Council:

Sept. 21, 2022

Noon – 1p.m. (virtual)

If you would like an invite to the meeting contact:

tina.gaines@vita.virginia.gov
The next scheduled meeting for the ISOAG is:

Oct. 5, 2022

This is the annual mandatory meeting. All primary agency ISOs should attend. If you can’t attend yourself, please be sure to delegate attendance to someone else in your agency. Please let us know if you can’t attend and who will attend in your place.
Sept. 26th will start the statewide phishing campaign for the third quarter.

Please contact commonwealthsecurity@vita.Virginia.gov for more information.
Everyone needs to take steps to retain your ISO Certification for CY 2022. Please contact Tina Gaines (tina.gaines@vita.Virginia.gov) to see what requirements you need to complete your certification.

Also, please complete your Security Awareness Training Solution Form by 9/30/2022. You may complete the form in Archer or by completing the form and emailing it Commonwealthiseguridad@vita.Virginia.gov
OCTOBER IS CYBERSECURITY AWARENESS MONTH