PSCR 2021

THE DIGITAL EXPERIENCE

#PSCR2021 • PSCR.GOV

NIST

PSCR

Riding the Tide of an IoT Tsunami

Gema Howell

Kevin Brady

Donald Harriss

NIST

#PSCR2021

PSCR

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately.

Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

*** Please note, unless mentioned in reference to a NIST Publication, all information and data presented is preliminary/in-progress and subject to change**

INTRODUCTION

WHO AM I?

- Gema Howell - 1 of 3 Speakers
- Background:
  - Project Lead & Computer Scientist
  - 7 years working with PSCR
  - Focus on mobile device and Internet of Things (IoT) security for first responders
  - Other work:
    - Enterprise mobile security management
    - Election security

THE IOT TSUNAMI

IOT DEVICES ARE THE NEW WAVE

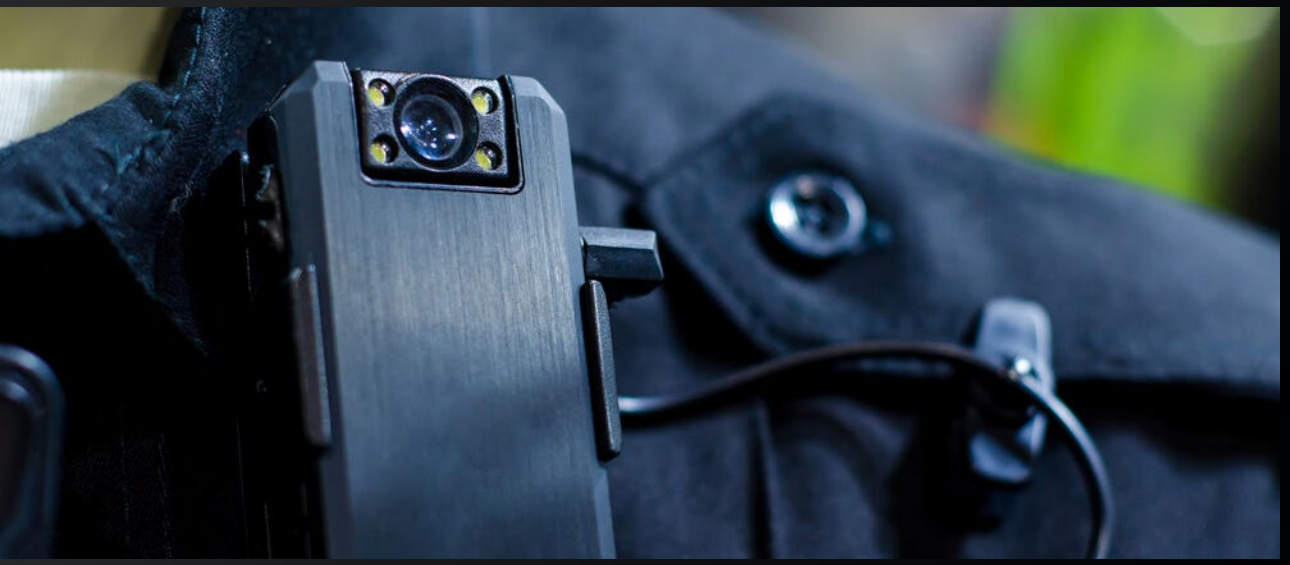
IoT devices are everywhere: in our homes, on our body, and connecting our cities

POTENTIAL BENEFITS OF IOT

- Convenience
- Efficiency
- Automation
- Wellness


An Estimated
25
Billion
IoT Connected Devices
by the Year
2030

PUBLIC SAFETY IOT DEVICES



IOT FOR FIRST RESPONDERS

First Responders can leverage IoT devices to help perform their daily life-saving activities

EXAMPLES OF PUBLIC SAFETY IOT

- Police body cameras
- Emergency Medical Services (EMS) vital sign monitors
- Situational awareness drones
- Traffic light sensors

CHALLENGES
(Not an Exhaustive List)

How can first responders take advantage of the technology benefits and ensure minimal impact on their daily duties?

INTEROPERABILITY

Finding solutions that integrate with current systems

CONFIGURATION OPTIONS

The lack of configurations options for low power IoT devices

UPDATE & PATCH MANAGEMENT

Managing a healthy ecosystem to ensure devices are not vulnerable to attack

DOCUMENTATION

The lack of informative documentation to assist with implementing a secure deployment of devices

KNOWN IOT DEVICE THREATS

ars TECHNICA

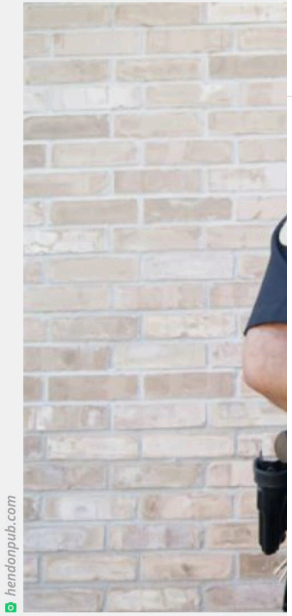
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

BIZ & IT —

Police body cams found pre-installed with notorious Conficker worm

One of the world's most prolific pieces of malware is found in cams from Martel.

DAN GOODIN - 11/16/2015, 1:19 PM



CSO UNITED STATES INSIDER

PRIVACY AND SECURITY FANATIC

By Ms. Smith, CSO | AUG 14, 2018 9:08 AM PDT

About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

NEWS

Security flaws in police body cameras open the devices to attack

A researcher presenting at Def Con 26 said security flaws in police body cameras could enable hackers to edit and delete footage and weaponize the devices with malware.

WHITE PAPERS

Akamai Executive Summary: 2020 Gartner Magic Quadrant for Web...

Getting Started with SASE On-demand Webinar: A Conversation About SAS...

Connect your business with Spectrum Enterprise Unified Communications

INSIDER

Log in Subscribe

HOME > MILITARY & DEFENSE

A map of fitness-tracker data may have compromised top-secret US military bases around the world

Alex Lockie Jan 29, 2018, 5:23 AM

A map of activity in Djibouti that has drawn comment from security analysts. Strava

- **An interactive heat map from the fitness-tracking app Strava appears to have exposed sensitive sites.**

PRESENTATION OVERVIEW

IOT SECURITY FOUNDATION – KEVIN BRADY

Provide background information about NIST's IoT security work and share some of our recent documents focused on securing devices for first responders

THE FUTURE OF IOT MANAGEMENT – DON HARRISS

Describe our current project and how it can address managing cybersecurity threats to IoT devices used by Public Safety

IOT SECURITY FOUNDATION

WHO AM I?

KEVIN BRADY JR

Computer Scientist – Applied Cybersecurity Division (ACD)

BACKGROUND:

- Automated testing methods
- IoT system design
- Precision timing in IoT
- PSCR – IoT Management Solutions
- NIST Cybersecurity for IoT Program

NIST CYBERSECURITY FOR IOT PUBLICATIONS

NISTIR 8228

- **Considerations for Managing IoT Cybersecurity and Privacy Risks**

NISTIR 8259 SERIES

- NISTIR 8259 - Foundational Cybersecurity Activities for IoT Device Manufacturers
- NISTIR 8259A - IoT Device Cybersecurity Capability Core Baseline
- NISTIR 8259B - IoT Non-Technical Supporting Capability Core Baseline (DRAFT)

NIST IOT CYBERSECURITY CONCEPTS

MANUFACTURERS' ROLE IN DEVICE SECURABILITY

IoT devices as components of larger systems

FOUNDATIONAL CONCEPTS TO CREATING PROFILES

Device Centricity

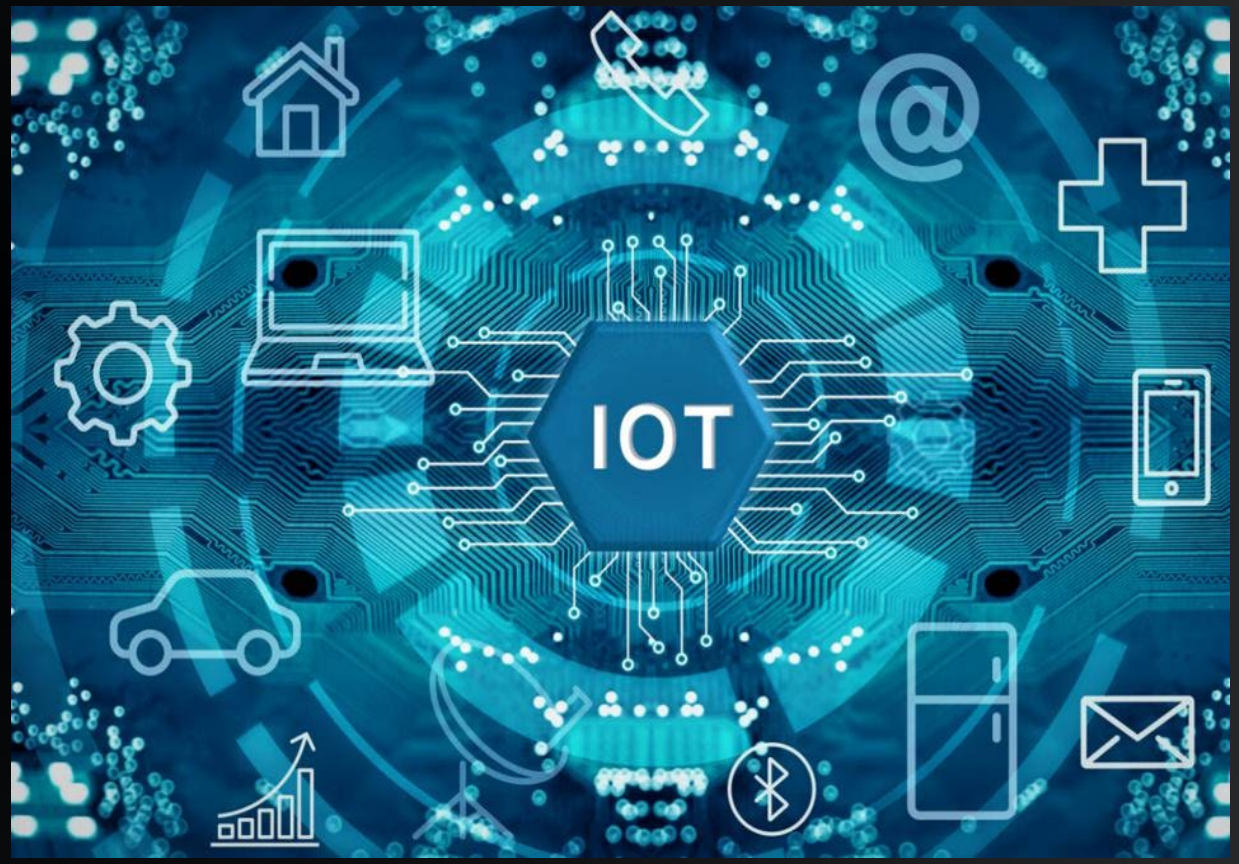
Cybersecurity Focus

Minimal Securability

MANUFACTURERS AND CUSTOMERS NEED TO WORK TOGETHER TO ACCOMPLISH CYBERSECURITY GOALS

WHAT CAPABILITIES DO PUBLIC SAFETY DEVICES NEED?

- How can we determine what capabilities need to be included in IoT devices for public safety to make them securable?
- How do IoT device management solutions manage devices?
- How do approaches for managing IoT devices affect what device capabilities may be necessary?



NISTIR 8196: SECURITY ANALYSIS OF FIRST RESPONDER MOBILE AND WEARABLE DEVICES

- Identify threats to public safety devices to be able to categorize them based on severity and likelihood
- Identify security objectives for public safety devices to be able to mitigate these threats
- Identify device capabilities that are necessary to satisfy security objectives based on:
  - First Responder Use Cases
  - Threat Analysis of Use Cases
  - Interviews with public safety professionals

Security Objectives for Public Safety

- ***Availability***
- ***Ease of Management***
- ***Interoperability***
- ***Isolation***
- ***Confidentiality***
- ***Authentication***
- ***Integrity***
- ***Healthy Ecosystem***

NISTIR 8235: SECURITY GUIDANCE FOR FIRST RESPONDER MOBILE AND WEARABLE DEVICES

- Mobile devices have the capabilities to meet security objectives due to their size, storage capabilities, and operating systems.
- Wearable devices are often constrained and built to accomplish a specific use.
- The limitations of constrained (i.e., wearable and IoT) devices lead to technical gaps where security objectives cannot be met from the device itself.

HOW DO IOT MANAGEMENT SOLUTIONS ADDRESS THESE ISSUES?

- How do IoT Management Solutions on the market today handle the limitations of IoT and wearable devices?
- What system architectures and strategies are being used to help to compensate for the limitations of IoT devices?
- Examining management solutions provides insight into what will be required from devices.

THE FUTURE OF IOT MANAGEMENT

WHO AM I?

Don Harriss

IT Security Specialist – NIST/PSCR

Background:
Network Architecture and Administration
IoT Data Structures, Security and Implementation
UAS and Satcom Network Systems Integration

IOT SECURITY MANAGEMENT OVERVIEW

TESTING AND INTEGRATION

Develop test environments at NIST labs for testing public safety IoT devices

OBSERVE CAPABILITIES

Understand functionality and effectiveness of management solutions

DEFINE TECHNOLOGY GAPS

Determine gaps and deficiencies for managing public safety IoT devices, networks and systems

PROVIDE GUIDANCE

Share current management capabilities and identify areas for improvement/innovation to help public safety manage IoT devices

KNOW WHAT YOU ARE PROTECTING

INVENTORY TRACKING

- Numerous IoT devices utilized by public safety require automated solutions
- Manual audits of IoT devices is not feasible or practical
- IoT devices need to be available and ready for field deployment

DEVICE LOCATION

- Geotracking, Global Positioning System (GPS), cellular triangulation
- Ownership and responsible personnel
- Profile by device function, data usage, metadata

BENEFITS TO PUBLIC SAFETY

DEVICE READINESS

- IoT device access to public safety networks
  - Authentication of allowed devices to allow or disallow devices onto public safety networks
  - Authorization of IoT devices to network servers, resources and individuals
  - Device accountability for tracking device behavior and activity on the network
- Operational Functionality
  - Device and associated data is mission ready
  - Secure and cleared of malicious malware, viruses or code
  - Device is up-to-date with latest patches, firmware, software
  - Device can securely transmit and/or store data

SOLUTION CONSIDERATIONS

NETWORK BASED

- Traditional network gateways, firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS)
- Intelligence based (AI) network monitoring solutions
- Overlay and isolated networks or Virtual Private Networking (VPN) solutions
- Software defined networks with threat analysis orchestration and control
- Cloud-based solutions or Security As A Service

HOST BASED

- Antivirus, anti-malware
- Host based IDS, IDP
- Hardware embedded solutions, e.g., Federal Information Processing Standards (FIPS) encryption module

SOLUTION CONSIDERATIONS

HYBRID

- Security Information and Event Management (SIEM)
- Network media layer encryption such as MACSec
- End-to-end encryption or host-to-host, host-to-server encryption
- Single vendor, vetted device solutions or turn-key multi-vendor solutions

TECHNOLOGY CONSIDERATIONS

PHYSICAL SECURITY

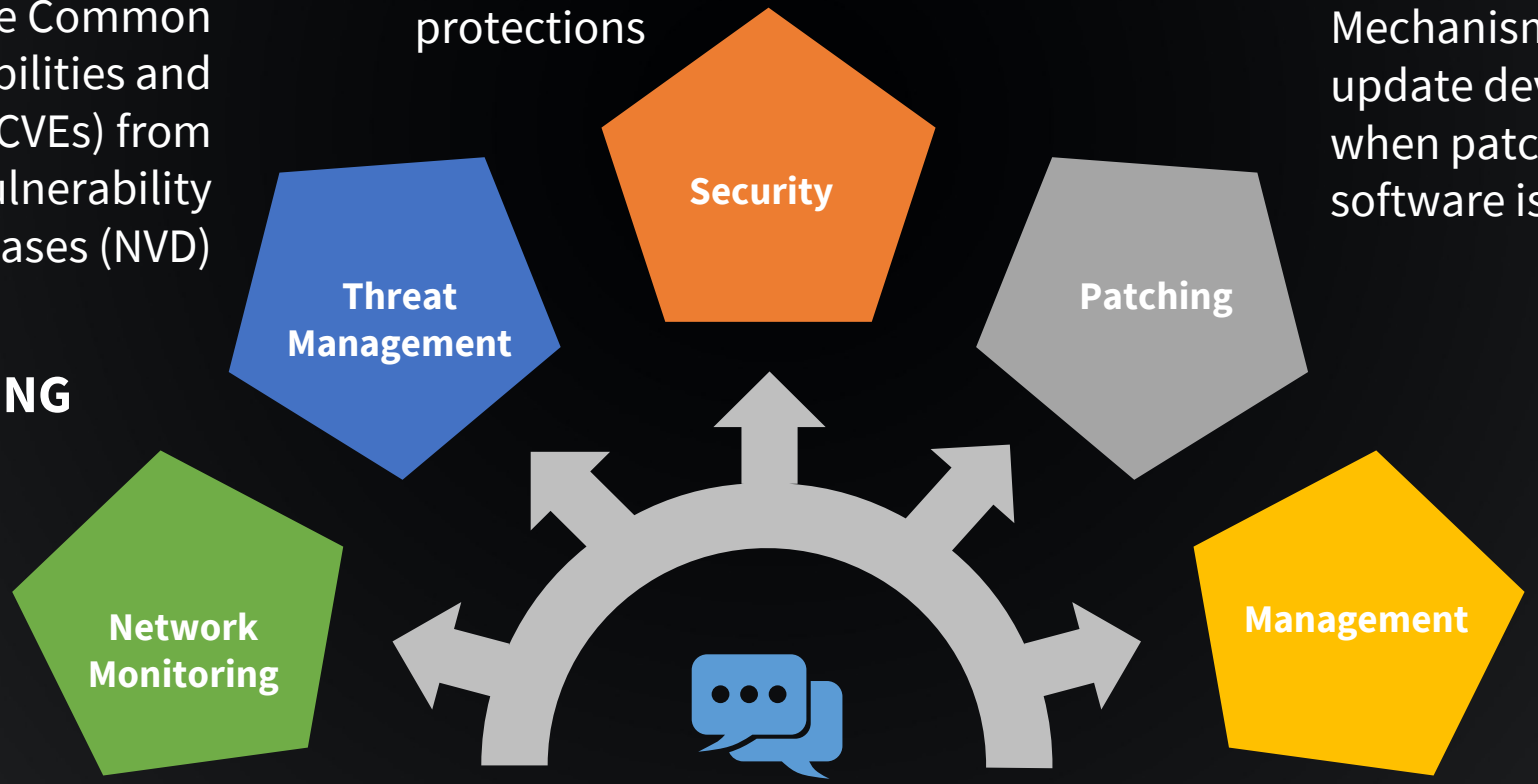
Covers a multitude of concerns, from physical security of the devices, device ownership, security of personally identifiable information (PII), and network protections

THREAT MANAGEMENT

Mitigate Common Vulnerabilities and Exposures (CVEs) from National Vulnerability Databases (NVD)

PATCHING

Mechanisms to update devices when patches or software is available



NETWORK MONITORING

"Bumps in the wire," middleware or gateways that protects devices that are unable to update or lack network protection

MANAGEMENT

Centralized system or "pane of glass" that monitors, tracks, updates and assigns IoT devices

CONCLUSION

- Address and identify the challenges of IoT Security
- Build upon IoT Security Fundamentals, NIST Publications and use lessons learned to address the unique requirements of public safety
- Identify the devices that are lacking security solutions
- Determine solutions that meet the needs of public safety
- Consider multiple solution potentials and identify technology gaps, if any exist

THANK YOU

#PSCR2021 • PSCR.GOV

GET CONNECTED

Kevin Brady
kevin.g.brady@nist.gov

Don Harriss
donald.harriss@nist.gov

Gema Howell
gema.howell@nist.gov