NIST Mobile Device Security Resources

Gema Howell
Computer Scientist, Applied Cybersecurity Division
November 2022

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

About Me

Gema Howell

- **8 years** at National Institute of Standards & Technology (NIST) as a computer scientist
- **Mobile device security project lead** at the National Cybersecurity Center of Excellence (NCCoE)
- Focus on enterprise mobile security management
- Federal Mobility Group Co-Chair
- Other work:
    - mobile device and IoT security for first responders (fire, ems, and law enforcement)
    - Election security

What are Mobile Devices?

Key Takeaways

- Have a general **understanding of NIST and the NCCoE**
- **Share NIST Resources** for Mobile Device Security
- **Highlight relevant cybersecurity considerations** for NMFTA

NIST AT A GLANCE

3,400+
FEDERAL EMPLOYEES

5
NOBEL PRIZES

2 CAMPUSES
GAITHERSBURG, MD [HQ]
BOULDER, CO

3,500+
ASSOCIATES

10
COLLABORATIVE INSTITUTES

400+
BUSINESSES USING NIST FACILITIES

ManufacturingUSA®
NATIONAL OFFICE COORDINATING 16 MANUFACTURING INSTITUTES

51
MANUFACTURING EXTENSION PARTNERSHIP CENTERS

U.S. BALDRIGE PERFORMANCE EXCELLENCE PROGRAM

NIST vs. Other Agencies

- Large campus of mostly scientists
- Research facility
- Non-regulatory agency
- Our work is commonly publicly available

What We're Known For…

NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations

800-53 Controls

Security and Privacy Controls used to protect the system and organization commensurate with risk.

Cryptographic Standards and Guidelines

Open and transparent process that enlists the worldwide cryptography community to help us develop and vet algorithms included in our cryptographic guidance.

Risk Management Framework Cybersecurity Framework

Frameworks designed to help organizations plan and prioritize their resources to address their cybersecurity needs.

National Cybersecurity Center of Excellence (NCCoE)

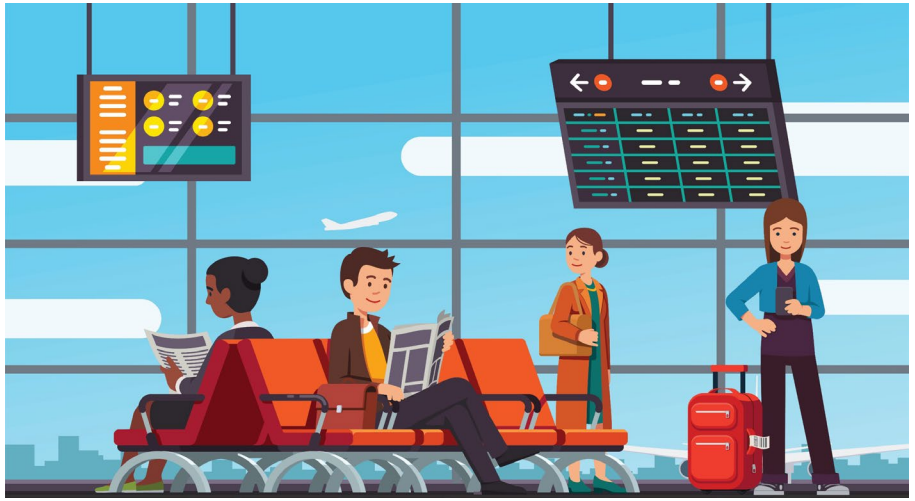
A **solution-driven**, **collaborative** hub addressing complex cybersecurity problems

The NCCoE is where we bring standards to life!

Let’s Talk About Mobile Device Security

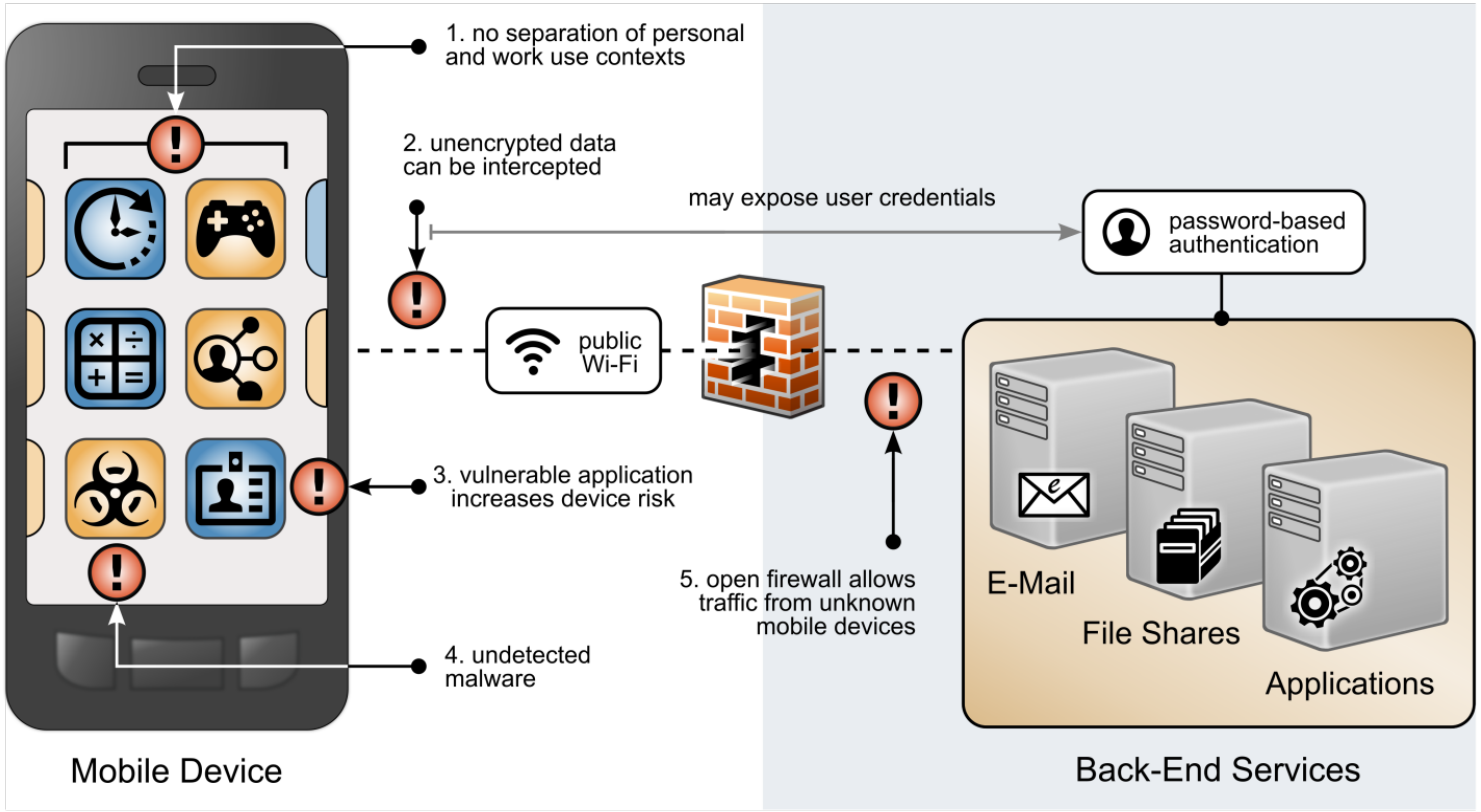
Mobile Museum

Enterprise Mobility



Mobile Device Security for the Enterprise

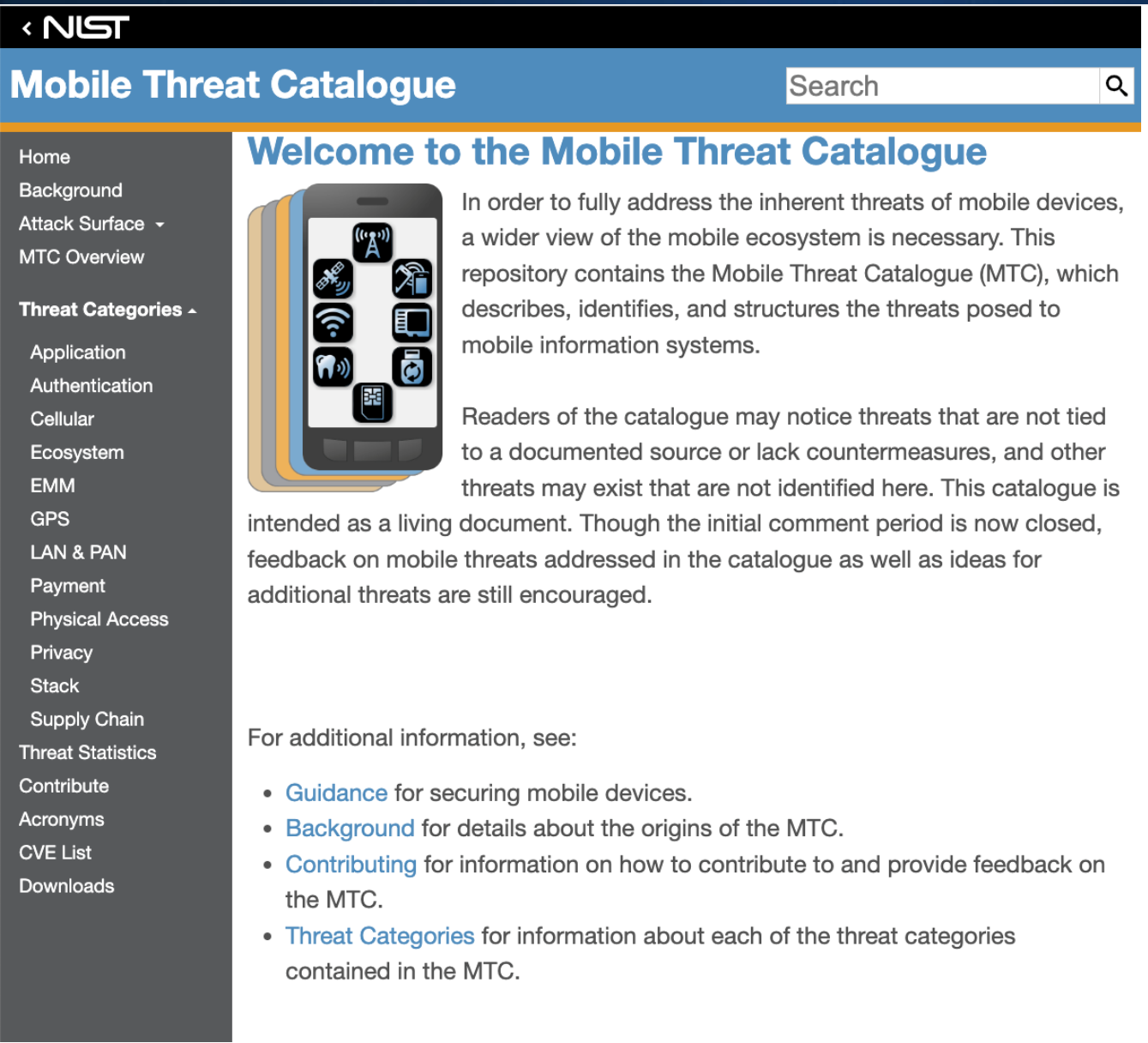
- Identify threats to mobile devices and mobile environment
- Research mobile device security tools available to address threats
- Provide guidance to help secure mobile devices used to achieve organization's mission



12

NIST Resource: Mobile Threat Catalogue

Mobile Threat Catalogue



- **Inform risk assessments**
- **Build threat models**
- **Enumerate attack surface for enterprise mobile systems**
- **Identify threats to devices, applications, networks, & infrastructure**
- **Collect countermeasures that IT security engineers can deploy to mitigate threats**

https://pages.nist.gov/mobile-threat-catalogue/

Example Mobile Threats

Mobile Threat Catalogue

Search

Home
Background
Attack Surface
MTC Overview

Threat Categories
Threat Statistics
Contribute
Acronyms
CVE List
Downloads

Unauthorized Information Disclosure via Lockscreen

Contribute

Threat Category: Authentication: User to Device

ID: AUT-1

Threat Description: When notification features are enabled for a device and mobile app, any sensitive information contained in a notification may be displayed on screen, even when the device is locked. An attacker with proximity to a locked device may gain unauthorized access to that information. Additional device features, such as voice-operated assistants (e.g., Siri, Cortana) may also allow an attacker with physical or voice access to a locked device to access sensitive information, such as contacts or reminders.

Threat Origin

About the security content of iOS 10.3 [Apple-1]

Exploit Examples

How hackers can access iPhone contacts and photos without a password [1]

CVE Examples

CVE-2017-2397 CVE-2017-2399 CVE-2017-2452

Possible Countermeasures

Mobile Device User
To limit opportunity for lockscreen bypass attacks, strongly secure mobile devices when not directly attended.

To reduce the success of lockscreen bypass exploits, ensure mobile OS security updates are installed in a timely manner

To reduce the potential that sensitive information is displayed on the lock screen, use mobile OS settings to disable access to notification features for apps that may receive sensitive content, or configure such notifications to only display when the device is unlocked.

Use mobile OS settings or deploy MDM solutions that can effectively enforce policies to limit the data or services available while the device screen is locked (e.g., notifications, voice-operated assistants, camera)

Enterprise
To reduce the success of lockscreen bypass exploits, ensure mobile OS security updates are installed in a timely manner

Use mobile OS settings or deploy MDM solutions that can effectively enforce policies to limit the data or services available while the device screen is locked (e.g., notifications, voice-operated assistants, camera)

References

1. D. Goodin, "How hackers can access iPhone contacts and photos without a password", Ars Technica, 25 Sept. 2015;

NIST National Institute of Standards and Technology U.S. Department of Commerce
NCCoE National Cybersecurity Center of Excellence
NIST Website | About NIST | usnistgov on GitHub

Mobile Threat Catalogue

Search

Home
Background
Attack Surface
MTC Overview

Threat Categories
Threat Statistics
Contribute
Acronyms
CVE List
Downloads

Pre-Installed Apps Invading Privacy

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-36

Threat Description: Mobile devices with cellular capability must generally be registered with a cellular carrier, and many devices are sold pre-configured to operate with a given carrier so users can have a fully functional device by the end of the initial purchase and activation at a retailer. As part of the configuration, the device may come with carrier-specific apps pre-installed, which may not be removable by the user. Because these apps come pre-installed, they may also may be granted implicit permission to access device resources without explicit knowledge or consent of the device owner. Privacy violations by such pre-installed apps may be more difficult to mitigate than by user-installed apps, which can be uninstalled at any time.

Threat Origin

Not Applicable, See Exploit or CVE Examples

Exploit Examples

Device Squad: The story behind the FTC's first case against a mobile device maker [1]

Certifi-gate: Hundreds of Millions of Android Devices Could Be Pwned [2]

Samsung Keyboard Security Risk Disclosed [3]

CVE Examples

CVE-2015-4640 CVE-2015-4641

Possible Countermeasures

Mobile Device User
To mitigate the potential for abuse or exploits by pre-installed apps, ensure that devices have the latest security updates installed.

Uninstall pre-installed apps that are not in use.

For pre-installed apps that cannot be uninstalled, revoke access to device sensors and OS-provided services.

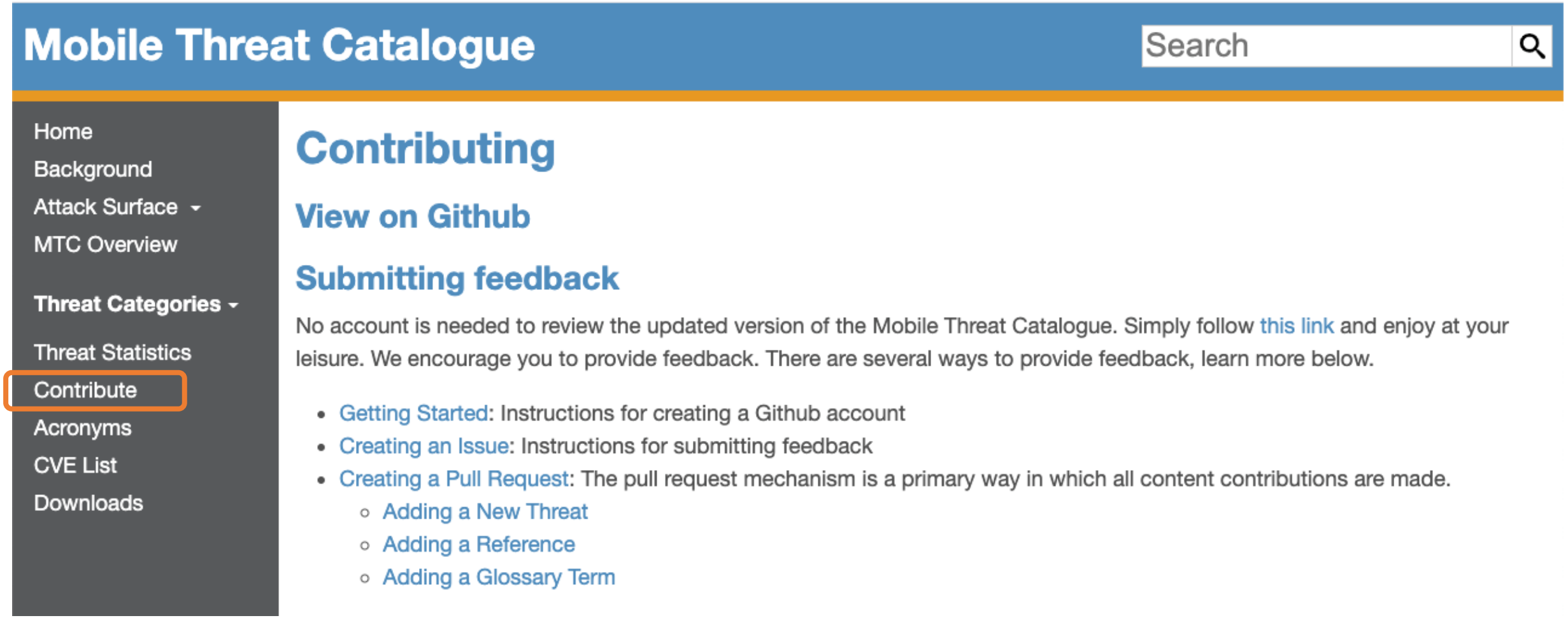
For pre-installed apps that cannot be uninstalled, disable the app so that it cannot be launched.

Enterprise
To mitigate the potential for abuse or exploits by pre-installed apps, ensure that devices have the latest security updates installed.

Deploy MAM solutions to identify and block access to devices running high-risk pre-installed apps.

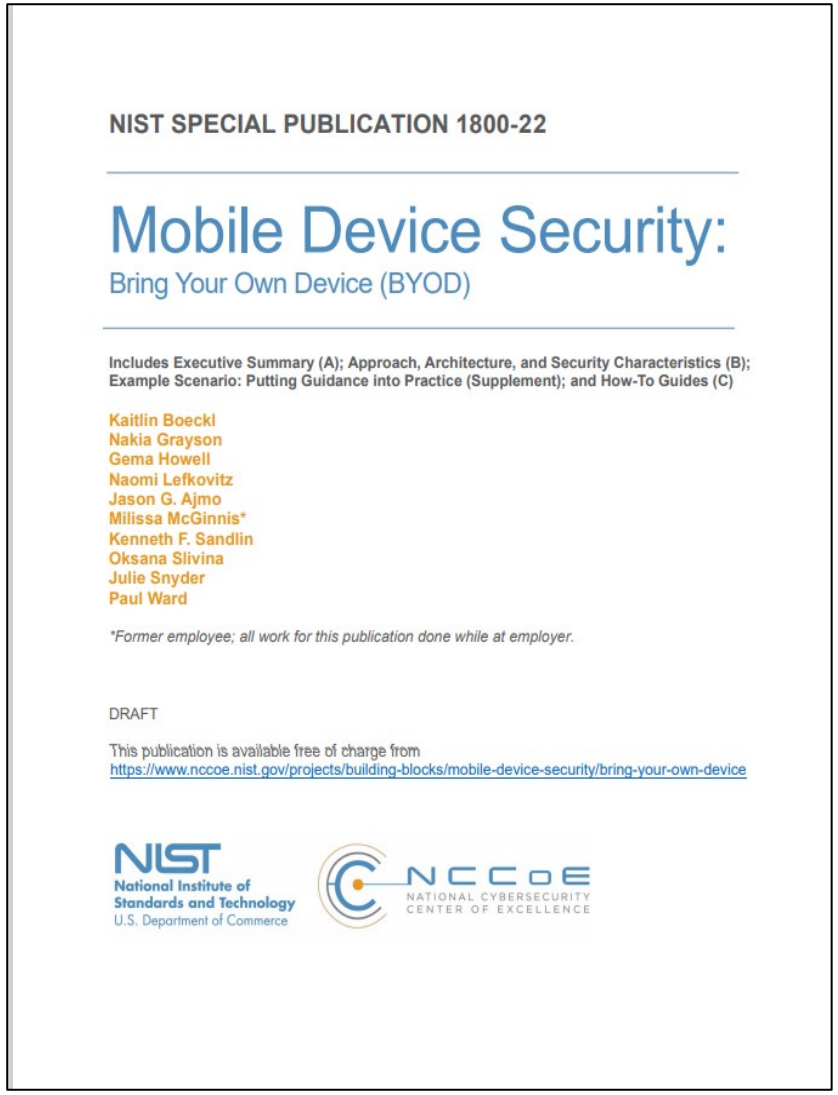
NIST National Institute of Standards and Technology U.S. Department of Commerce
NCCoE National Cybersecurity Center of Excellence
NIST Website | About NIST | usnistgov on GitHub

How to Contribute to the Catalogue



NIST Resource(s): Mobile Device Security Practice Guides

Mobile Device Security Guides



NIST SPECIAL PUBLICATION 1800-22

Mobile Device Security:

Bring Your Own Device (BYOD)

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); Example Scenario: Putting Guidance into Practice (Supplement); and How-To Guides (C)

Kaitlin Boeckl
Nakia Grayson
Gema Howell
Naomi Lefkovitz
Jason G. Ajmo
Milissa McGinnis*
Kenneth F. Sandlin
Oksana Slivina
Julie Snyder
Paul Ward

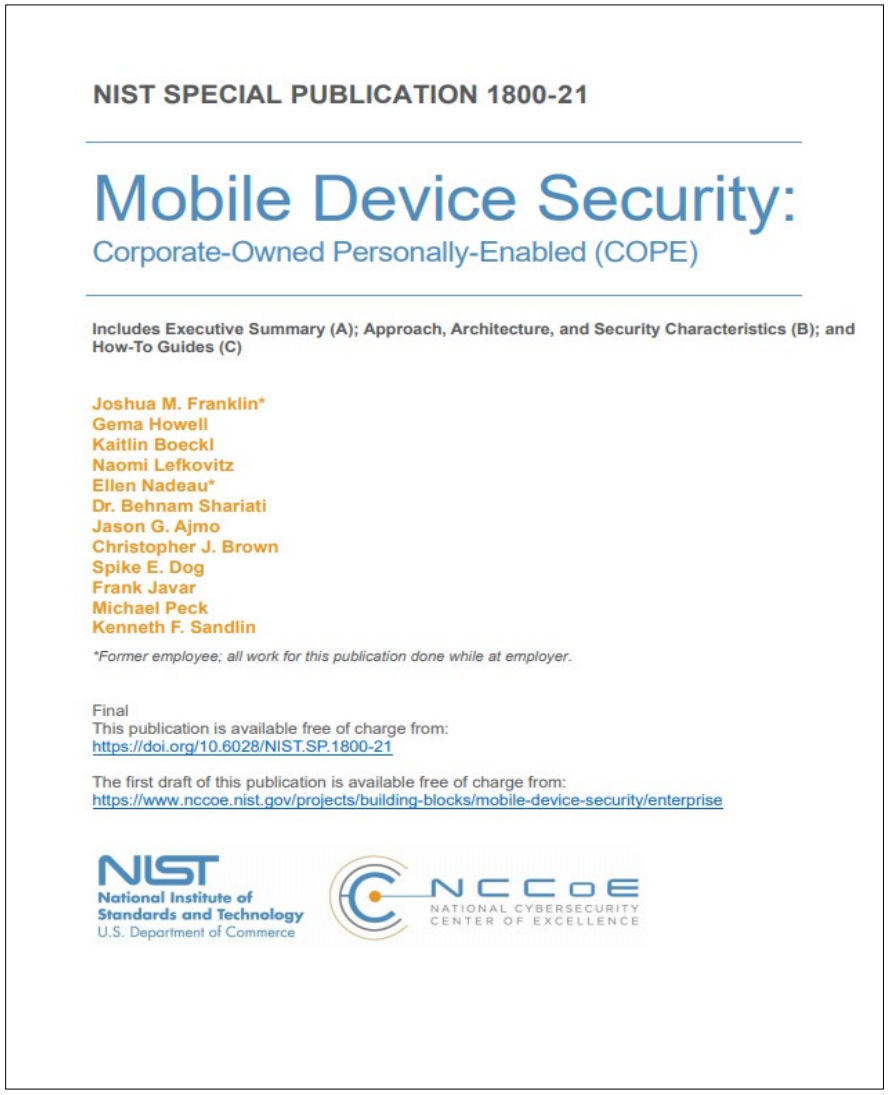
*Former employee; all work for this publication done while at employer.

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



NIST SPECIAL PUBLICATION 1800-21

Mobile Device Security:

Corporate-Owned Personally-Enabled (COPE)

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Joshua M. Franklin*
Gema Howell
Kaitlin Boeckl
Naomi Lefkovitz
Ellen Nadeau*
Dr. Behnam Shariati
Jason G. Ajmo
Christopher J. Brown
Spike E. Dog
Frank Javar
Michael Peck
Kenneth F. Sandlin

*Former employee; all work for this publication done while at employer.

Final
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-21

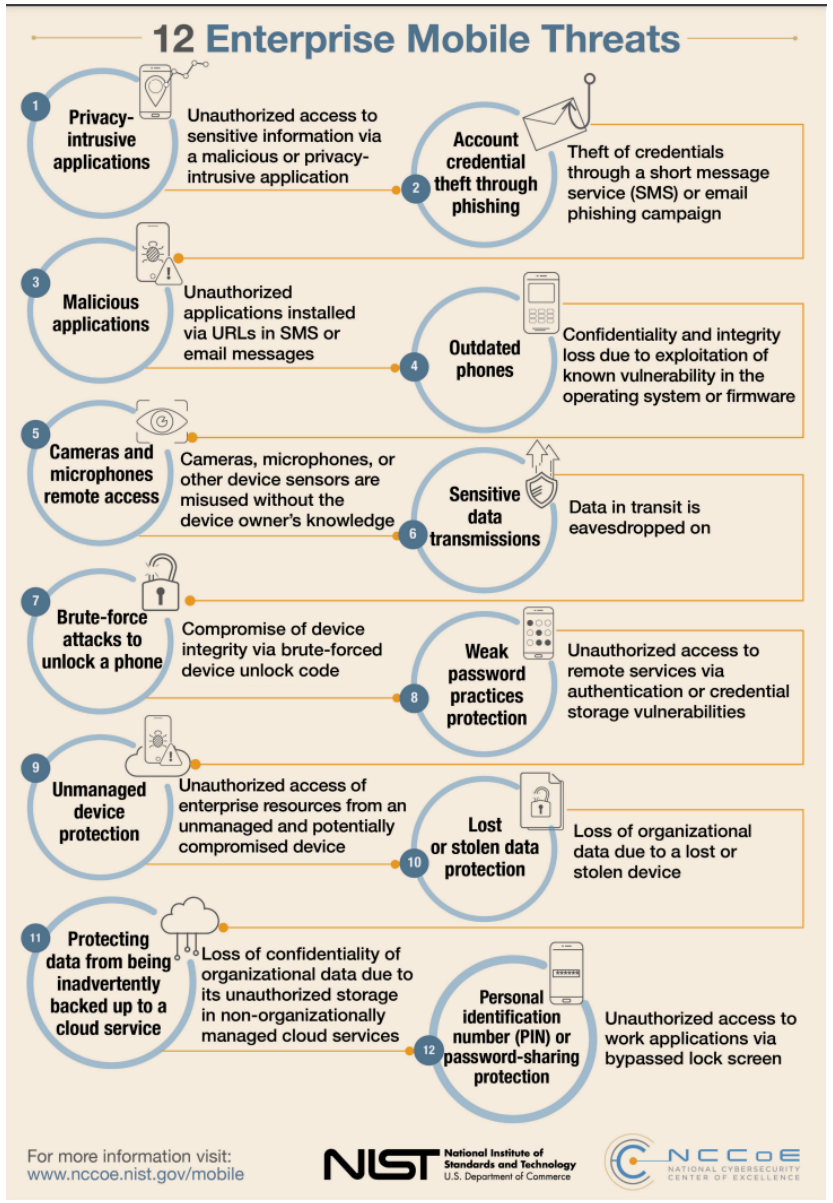
The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/enterprise

National Institute of Standards and Technology
U.S. Department of Commerce

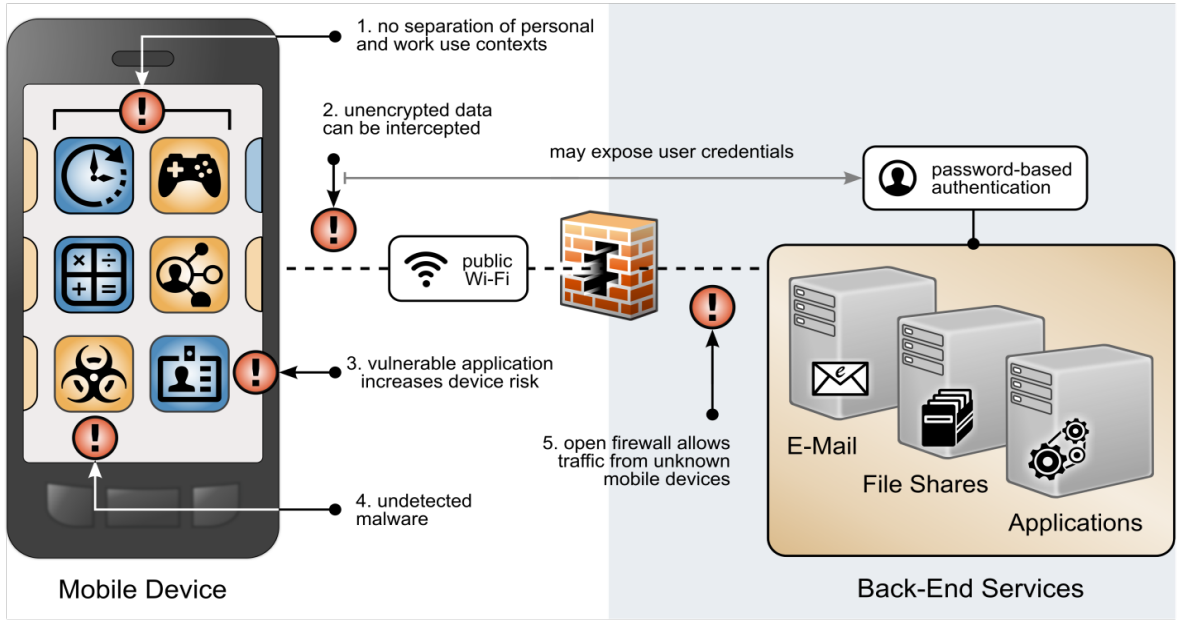
NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

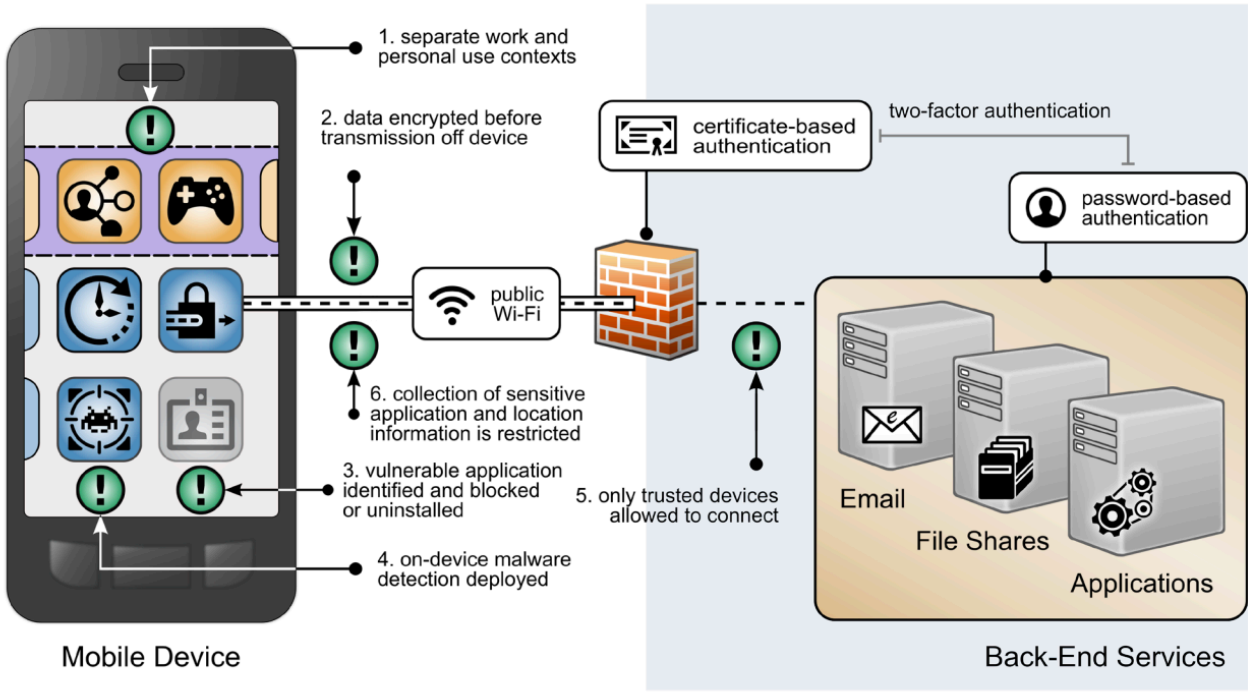
18

Enterprise Mobile Security and Privacy Risks

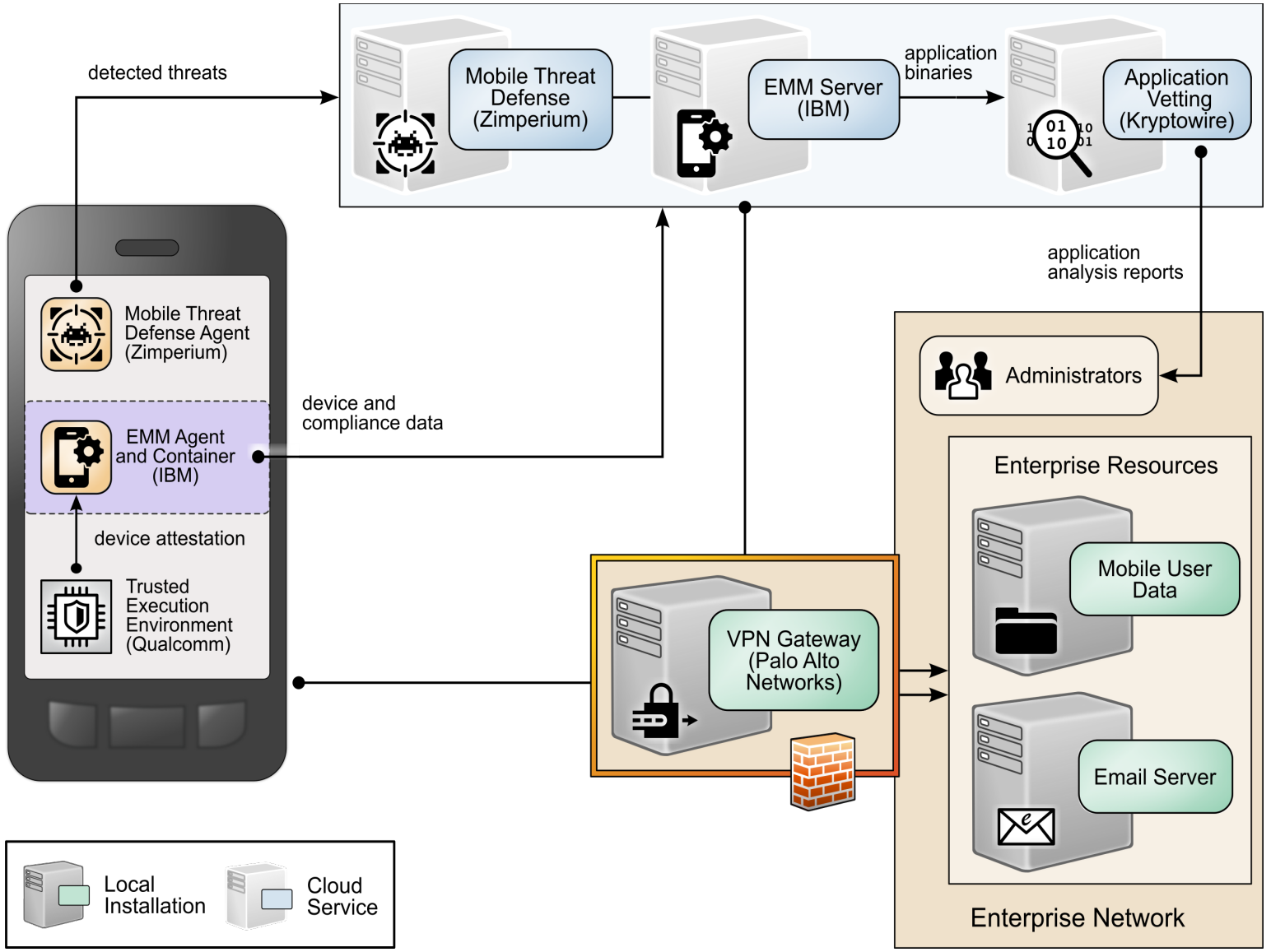


Use Risk Analysis to Develop a Plan





Example Architecture Diagram



Mitigations

Table 5-1 Threat Events and Findings Summary

Threat Event	How the Example Solution Architecture Helped Mitigate the Threat Event	The Technology Function that Helps Mitigate the Threat Event
Threat Event 1: unauthorized access to sensitive information via a malicious or privacy-intrusive application	Provides administrators with insight into what corporate data that applications can access.	MTD EMM
Threat Event 2: theft of credentials through a short message service (SMS) or email phishing campaign	Utilized PAN-DB and URL filtering to block known malicious websites.	Firewall
Threat Event 3: unauthorized applications installed via URLs in SMS or email messages	Alerted the user and administrators to the presence of a sideloaded application.	EMM MTD
Threat Event 4: confidentiality and integrity loss due to exploitation of known vulnerability in the OS or firmware	Alerted the user that their OS is noncompliant.	EMM MTD
Threat Event 5: violation of privacy via misuse of device sensors	Application vetting reports indicated the sensors to which an application requested access.	Application vetting

E.4 Threat Event 4

Summary: Confidentiality and integrity loss due to exploitation of known vulnerability in the operating system or firmware.

Test Activity: Attempt to access enterprise resources from a mobile device with known vulnerabilities (e.g., running an older, unpatched version of iOS or Android).

Desired Outcome: The enterprise's security architecture should identify the presence of devices that are running an outdated version of iOS or Android susceptible to known vulnerabilities. It should be possible, when warranted by the risks, to block devices from accessing enterprise resources until system updates are installed.

Observed Outcome: Zimperium was able to identify devices that were running an outdated version of iOS or Android, and it informed MaaS360 when a device was out of compliance.

NIST Resource:
Zero Trust Architecture
Practice Guide

Zero Trust Architecture Guide

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

IMPLEMENTING A ZERO TRUST ARCHITECTURE

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of implementing a zero trust architecture (ZTA) through collaborative efforts with industry and the information technology (IT) community, including cybersecurity solutions providers. This fact sheet provides an overview of the Implementing a Zero Trust Architecture project, including background, goal, potential benefits, and project collaborators.

BACKGROUND

The conventional security approach has focused on perimeter defenses. Once inside the network perimeter, users are "trusted" and often given broad access to many corporate resources. But malicious actors can come from inside or outside the perimeter, and several high-profile cyberattacks in recent years have undermined the case for the perimeter-based model. Moreover, the perimeter is becoming less relevant due to several factors, including the growth of cloud computing and mobility, and changes in the modern workforce.

Zero trust is a cybersecurity strategy that focuses on moving perimeter-based defenses from wide, static perimeters to narrow dynamic and risk-based access control for enterprise resources regardless of where they are located. Zero trust access control is based on a number of attributes such as identity and endpoint health.

CHALLENGES

The challenges to implementing a ZTA include:

- Leveraging existing investments and balancing priorities while making progress toward a ZTA
- ZTA Deployment requiring leveraging integration of many deployed existing technologies of varying maturities and identifying technology gaps to build a complete ZTA
- Concern that ZTA might negatively impact the operation of the environment or end-user experience
- Lack of common understanding of ZTA across the organization, gauging the organization's ZTA maturity, determining which ZTA approach is most suitable for the business, and developing an implementation plan

GOAL

The goal of this NCCoE project is to demonstrate several example ZTA solutions—applied to a conventional, general-purpose enterprise IT infrastructure—that are designed and deployed according to the concepts and tenets documented in NIST Special Publication (SP) 800-207, Zero Trust Architecture.

BENEFITS

The potential business benefits of the example solutions include:

- Support teleworkers with access to resources regardless of user location
- Protect resources regardless of their location (on-premises or in the cloud)
- Limit the insider threat (insiders are not automatically trusted)
- Limit breaches (reduce attackers' ability to move laterally and escalate privilege in the environment)
- Protect sensitive corporate data by using strong encryption
- Improve visibility into who is on the network, what resources are accessed and protected, and how to improve incident detection, response, and recovery
- Perform continuous, ongoing, dynamic, risk-based assessment of resources

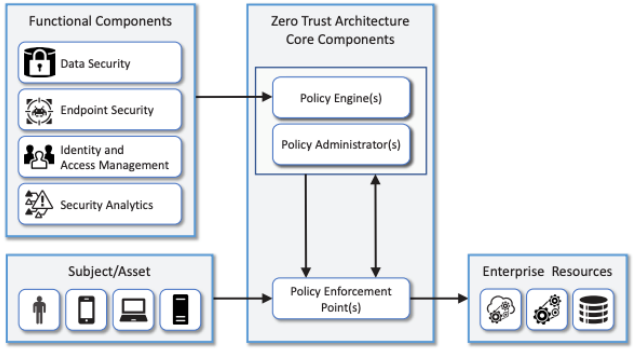
The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE ABOUT NCCOE
https://www.nccoe.nist.gov.

CONTACT US
nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE

A ZTA is designed for secure access to enterprise resources. Shown here is a high-level, notional architecture of the core components of a ZTA build for a typical IT enterprise and the functional components to support it. A detailed explanation of each component can be found within the practice guide and project description at https://www.nccoe.nist.gov/zerotrust.



TECHNOLOGY COLLABORATORS

The technology vendors participating in this project submitted their capabilities in response to an open call in the Federal Register. Companies with relevant security capabilities were invited to sign a Cooperative Research and Development Agreement with the National Institute of Standards and Technology (NIST), allowing them to participate in a consortium to build this example solution.

Technology Collaborators		
Appgate	IBM	Ping Identity
AWS	Ivanti	Radiant Logic
Broadcom Software	Lookout	SailPoint
Cisco	Mandiant	Tenable
DigiCert	Microsoft	Trellix
F5	Okta	VMware
Forescout	Palo Alto Networks	Zimperium
Google Cloud	PC Matic	Zscaler

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or the NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available.

DOWNLOAD PRACTICE GUIDE
This fact sheet provides a high-level overview of the work underway on zero trust cybersecurity. For more details, download the practice guide at https://www.nccoe.nist.gov/zerotrust

HOW TO PARTICIPATE
As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have question about this project or would like to join the Zero Trust Architecture Community of Interest, please email nccoe-zta-coi@list.nist.gov.

June 2022

Zero Trust Architecture Guide

NIST SPECIAL PUBLICATION 1800-35A

Implementing a Zero Trust Architecture

Volume A:
Executive Summary

Alper Kerman
Murugiah Souppaya
National Institute of Standards and Technology
Rockville, Maryland

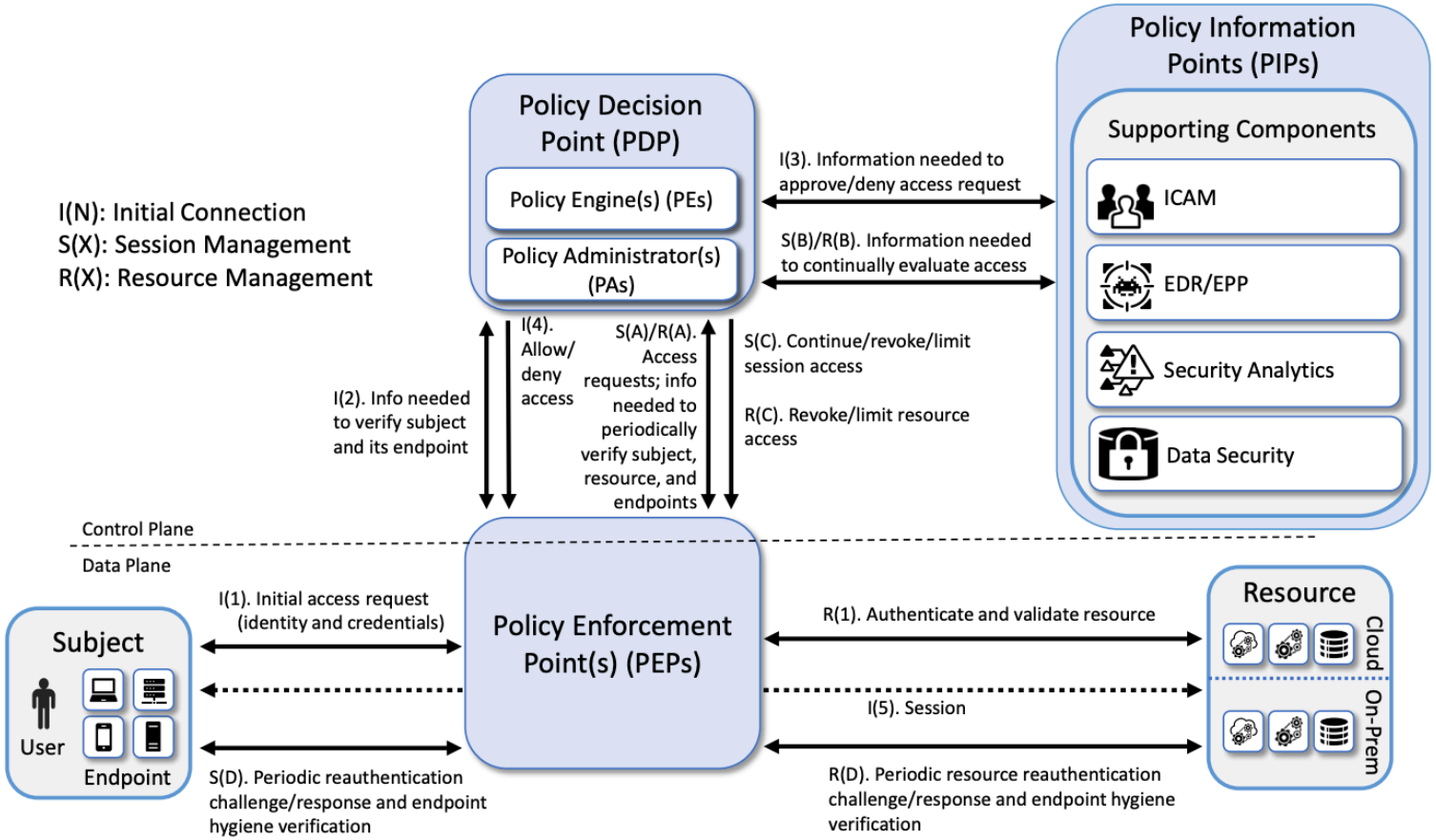
Dr. Parisa Grayeli
Susan Symington
The MITRE Corporation
McLean, Virginia

June 2022

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



NIST Resource(s): Cellular Security Guidance

Cellular Security Guidance

NIST Special Publication 800-187

Guide to LTE Security

Jeffrey Cichonski
Joshua M. Franklin
Applied Cybersecurity Division
Information Technology Laboratory

Michael Bartock
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-187

December 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

PRELIMINARY DRAFT

NIST SPECIAL PUBLICATION 1800-33A

5G Cybersecurity

Volume A:
Executive Summary

Mike Bartock
Jeff Cichonski
Murugiah Souppaya
National Institute of Standards and Technology
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

February 2021

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/building-blocks/5g-cybersecurity

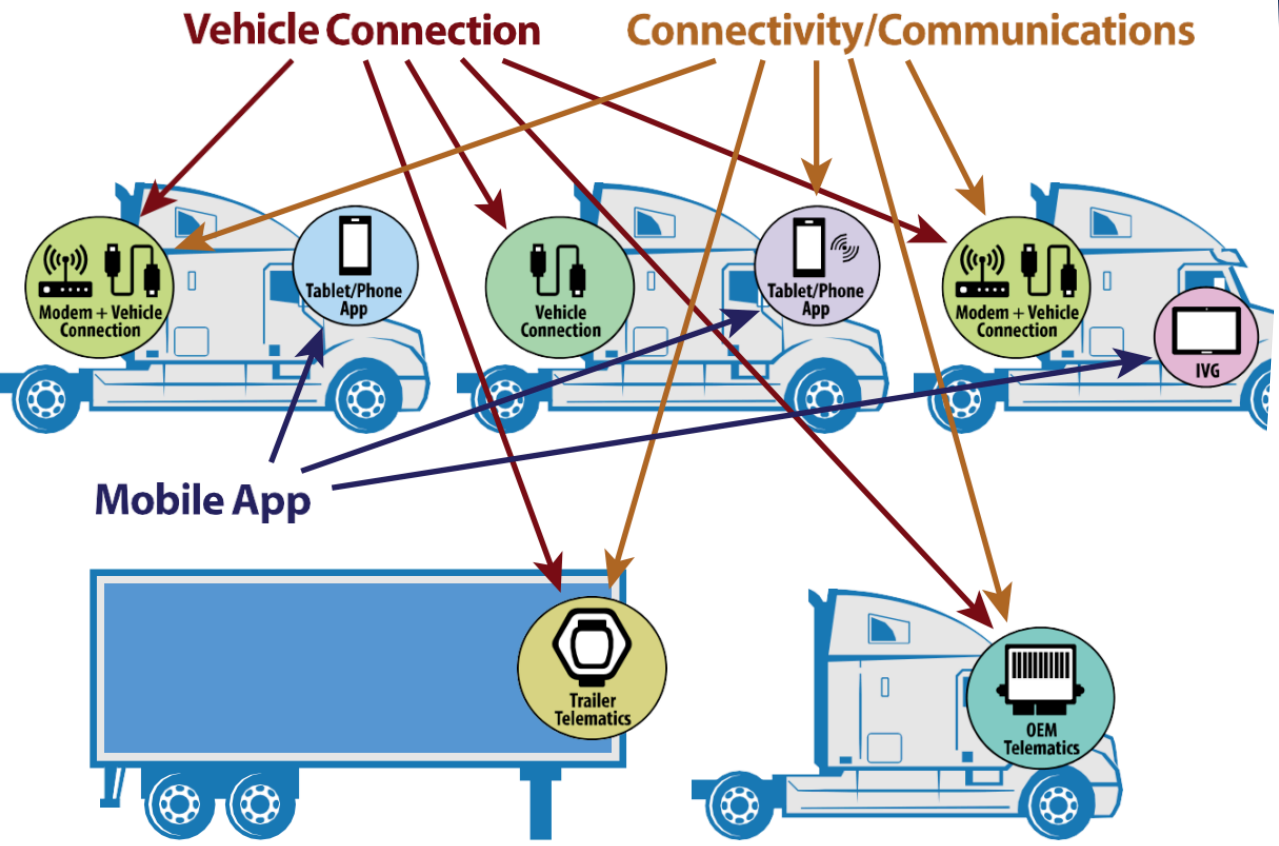
NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Relevant Highlights

A look at NMFTA's mobile use case

- Diagram from NMFTA Cybersecurity Requirements for Telematics Systems v1.5



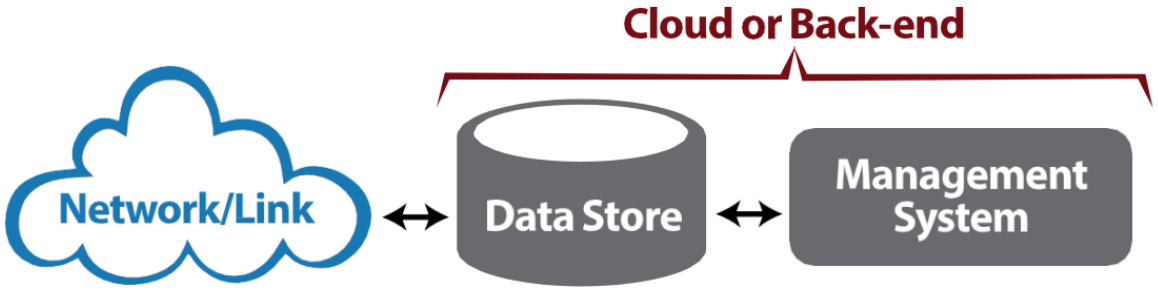
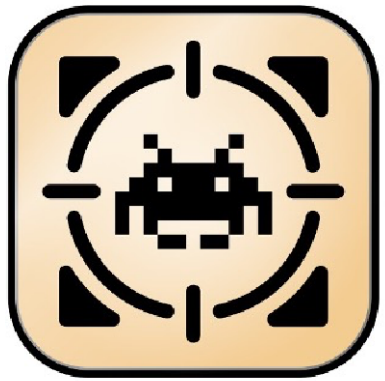


Figure 1. Abstracted Telematics, Fleet Management Information Systems (FMIS) and/or ELD

National Motor Freight Traffic Association, Inc. "*NMFTA Cybersecurity Requirements for Telematics Systems v1.5*". https://biz.nmfta.org/documents/ctsrp/NMFTA%20Cybersecurity%20Requirements%20for%20Telematics%20Systems%20v1.5.pdf?v=2. *(Nov. 2022)*

Mobile Threat Defense (MTD)



Mobile Threat Defense Agent (Zimperium)

a.k.a.

Mobile Endpoint Detection & Response (EDR)

What is it?:

MTD is an application installed on the device that provides information about the device's threat posture based on risks, security, and activity on the device.

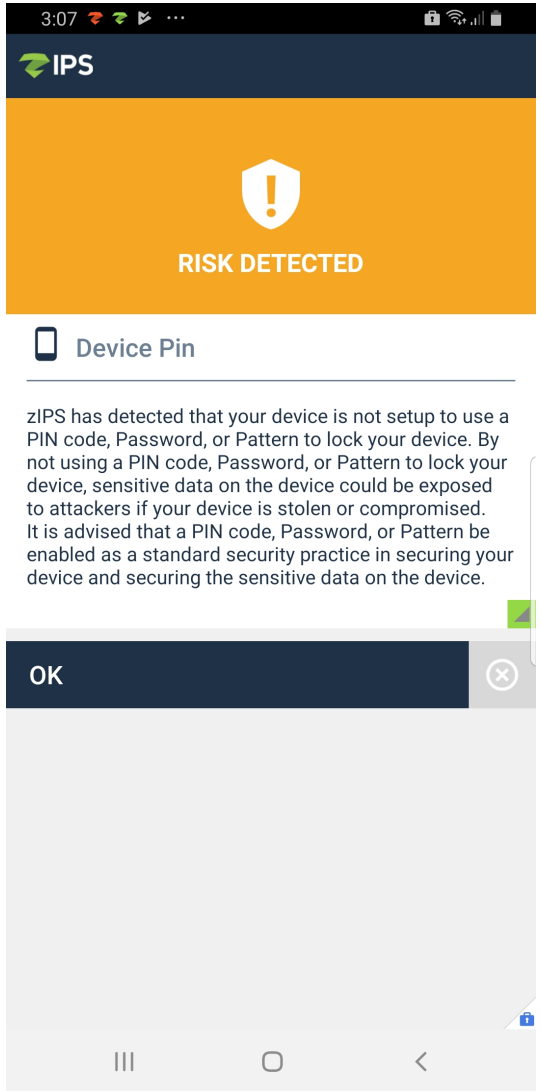
How does it work?:

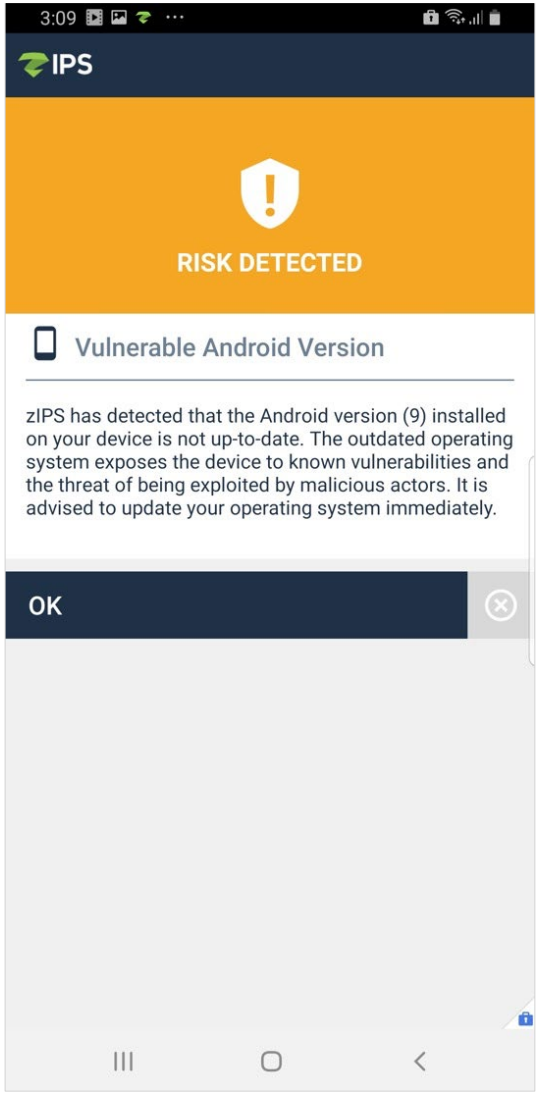
It uses device APIs to obtain risk posture information and to detect threats (e.g., phishing) and vulnerabilities.

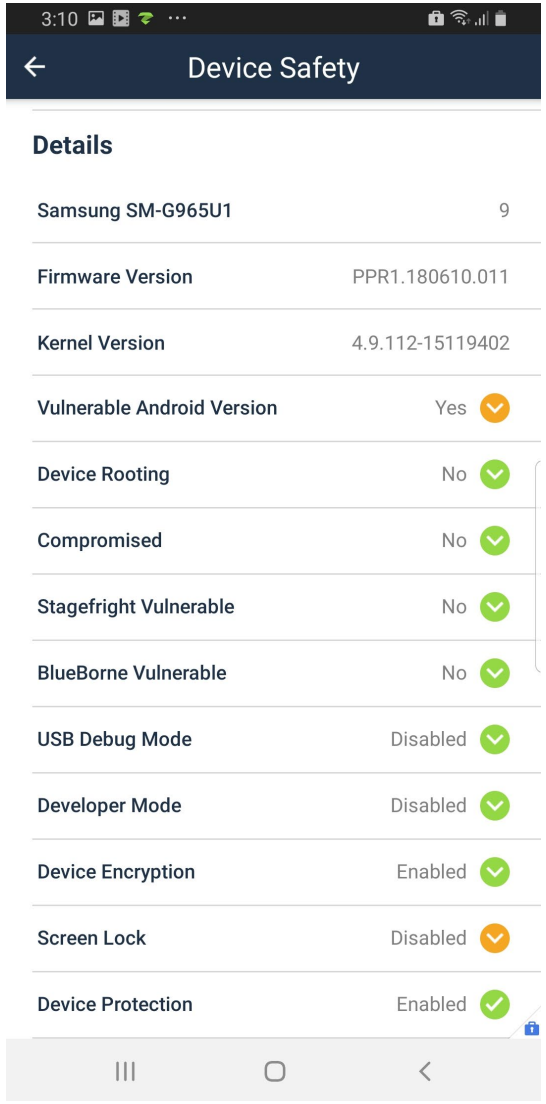
How does it address security and privacy concerns?:

The MTD analyzes and informs the user and the organization of device-based, application-based, and network-based threats so that the organization can perform mitigations.

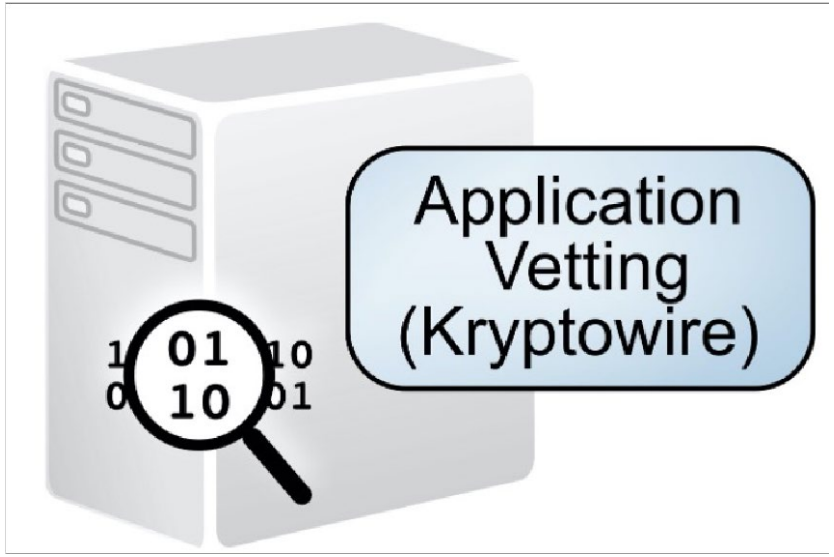
MTD/EDR Examples







Mobile Application Vetting



What is it?:

Mobile application vetting services are used to scan applications for potentially unwanted behavior.

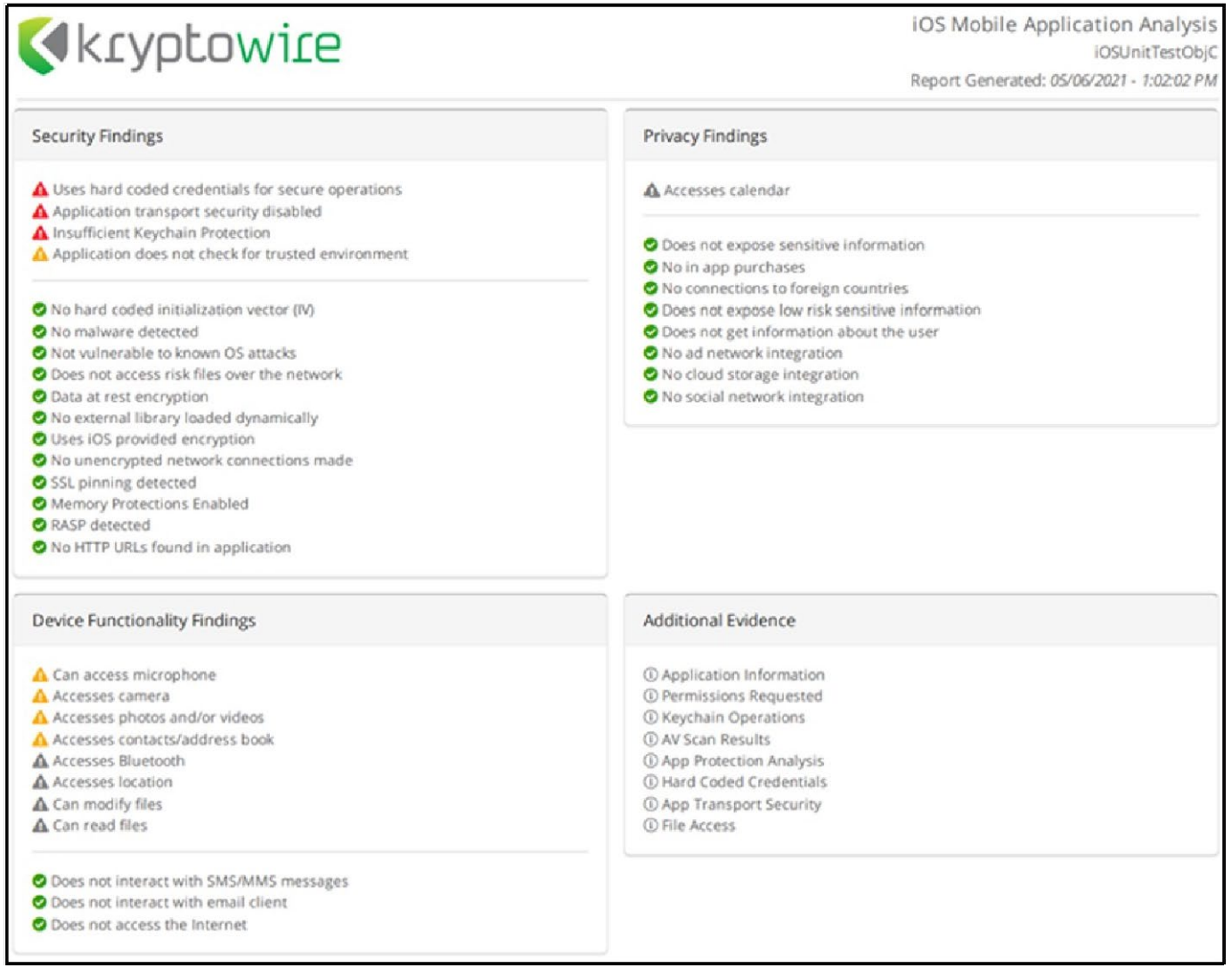
How does it work?:

Mobile application vetting services use a variety of static, dynamic, and behavioral techniques to determine if an application demonstrates any behaviors that pose a security or privacy risk.

How does it address security and privacy concerns?:

Mobile application vetting services provide organizations with the information necessary to make risk-based decisions when selecting/developing mobile applications for the organization.

Mobile Application Vetting Examples



kryptowire

iOS Mobile Application Analysis
iOSUnitTestObjC
Report Generated: 05/06/2021 - 1:02:02 PM

Security Findings

- ⚠ Uses hard coded credentials for secure operations
- ⚠ Application transport security disabled
- ⚠ Insufficient Keychain Protection
- ⚠ Application does not check for trusted environment

- ✓ No hard coded initialization vector (IV)
- ✓ No malware detected
- ✓ Not vulnerable to known OS attacks
- ✓ Does not access risk files over the network
- ✓ Data at rest encryption
- ✓ No external library loaded dynamically
- ✓ Uses iOS provided encryption
- ✓ No unencrypted network connections made
- ✓ SSL pinning detected
- ✓ Memory Protections Enabled
- ✓ RASP detected
- ✓ No HTTP URLs found in application

Privacy Findings

- ⚠ Accesses calendar

- ✓ Does not expose sensitive information
- ✓ No in app purchases
- ✓ No connections to foreign countries
- ✓ Does not expose low risk sensitive information
- ✓ Does not get information about the user
- ✓ No ad network integration
- ✓ No cloud storage integration
- ✓ No social network integration

Device Functionality Findings

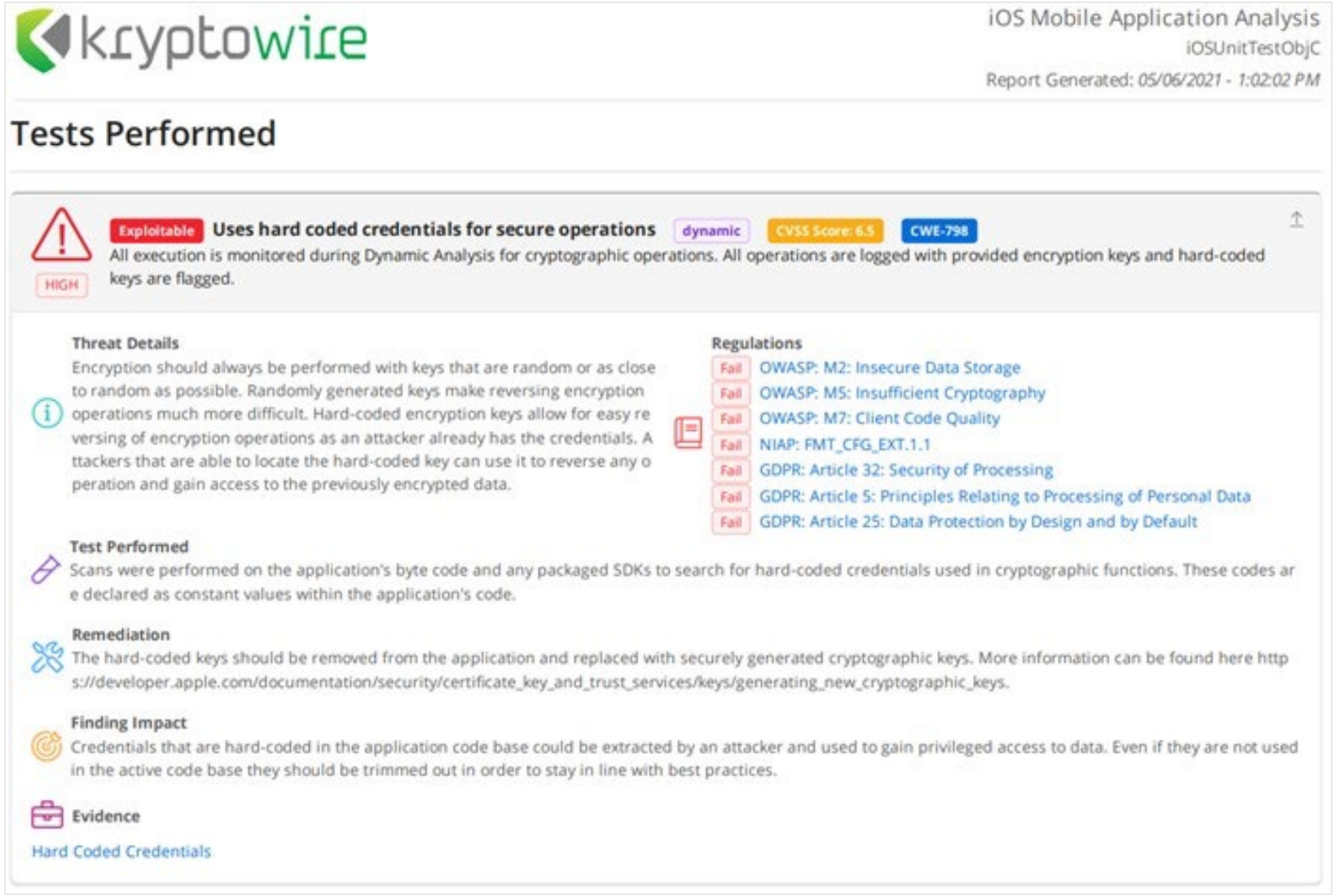
- ⚠ Can access microphone
- ⚠ Accesses camera
- ⚠ Accesses photos and/or videos
- ⚠ Accesses contacts/address book
- ⚠ Accesses Bluetooth
- ⚠ Accesses location
- ⚠ Can modify files
- ⚠ Can read files

- ✓ Does not interact with SMS/MMS messages
- ✓ Does not interact with email client
- ✓ Does not access the Internet

Additional Evidence

- ⓘ Application Information
- ⓘ Permissions Requested
- ⓘ Keychain Operations
- ⓘ AV Scan Results
- ⓘ App Protection Analysis
- ⓘ Hard Coded Credentials
- ⓘ App Transport Security
- ⓘ File Access

Mobile Application Vetting Examples



kryptowire

iOS Mobile Application Analysis
iOSUnitTestObjC
Report Generated: *05/06/2021 - 1:02:02 PM*

Tests Performed

Exploitable **Uses hard coded credentials for secure operations** dynamic CVSS Score: 6.5 CWE-798

HIGH

All execution is monitored during Dynamic Analysis for cryptographic operations. All operations are logged with provided encryption keys and hard-coded keys are flagged.

Threat Details

Encryption should always be performed with keys that are random or as close to random as possible. Randomly generated keys make reversing encryption operations much more difficult. Hard-coded encryption keys allow for easy re versing of encryption operations as an attacker already has the credentials. A ttackers that are able to locate the hard-coded key can use it to reverse any o peration and gain access to the previously encrypted data.

Regulations

- Fail OWASP: M2: Insecure Data Storage
- Fail OWASP: M5: Insufficient Cryptography
- Fail OWASP: M7: Client Code Quality
- Fail NIAP: FMT_CFG_EXT.1.1
- Fail GDPR: Article 32: Security of Processing
- Fail GDPR: Article 5: Principles Relating to Processing of Personal Data
- Fail GDPR: Article 25: Data Protection by Design and by Default

Test Performed

Scans were performed on the application's byte code and any packaged SDKs to search for hard-coded credentials used in cryptographic functions. These codes ar e declared as constant values within the application's code.

Remediation

The hard-coded keys should be removed from the application and replaced with securely generated cryptographic keys. More information can be found here http s://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/generating_new_cryptographic_keys.

Finding Impact

Credentials that are hard-coded in the application code base could be extracted by an attacker and used to gain privileged access to data. Even if they are not used in the active code base they should be trimmed out in order to stay in line with best practices.

Evidence

Hard Coded Credentials

Mapping to 800-53 Controls

Table G-1 Example Solution's Cybersecurity Standards and Best Practices Mapping

Specific product used	How the component functions in the example solution	Applicable NIST Cybersecurity Framework Subcategories	Applicable NIST SP 800-53 Revision 5 Controls	ISO/IEC 27001:2013	CIS 6	Applicable NIST SP 800-181 NICE Framework Work Roles (2017)
Mobile Threat Defense						
Kryptowire Cloud Service	Application Vetting	**ID.RA-1:** Asset vulnerabilities are identified and documented.	**CA-2, CA-7, CA-8:** Security Assessment and Authorization **RA-3, RA-5:** Risk Assessment **SA-4:** Acquisition Process	**A.12.6.1:** Control of technical vulnerabilities **A.18.2.3:** Technical Compliance Review	**CSC 4:** Continuous Vulnerability Assessment and Remediation	**SP-RSK-002:** Security Control Assessor **SP-ARC-002:** Security Architect **OM-ANA-001:** Systems Security Analyst

Mapping to Controls

Ref #	Category	Criticality:	Public Requirements References/Descriptions
RA-020	Risk Assessment	Medium	NIST 800-53 r5 RA-3 – RISK ASSESSMENT

Applicable Component Categories

Mobile App;
Vehicle Connection;
Connectivity/Communications;
Cloud or Back-end;

Requirement

The vendor shall use the results of risk assessments to influence systems development and processes.

Verification: Inspection, Demonstration, Test, or Analysis

Inspection of vendor-supplied statement of the use of risk assessments in influencing the ongoing development of their products.

Remarks

-

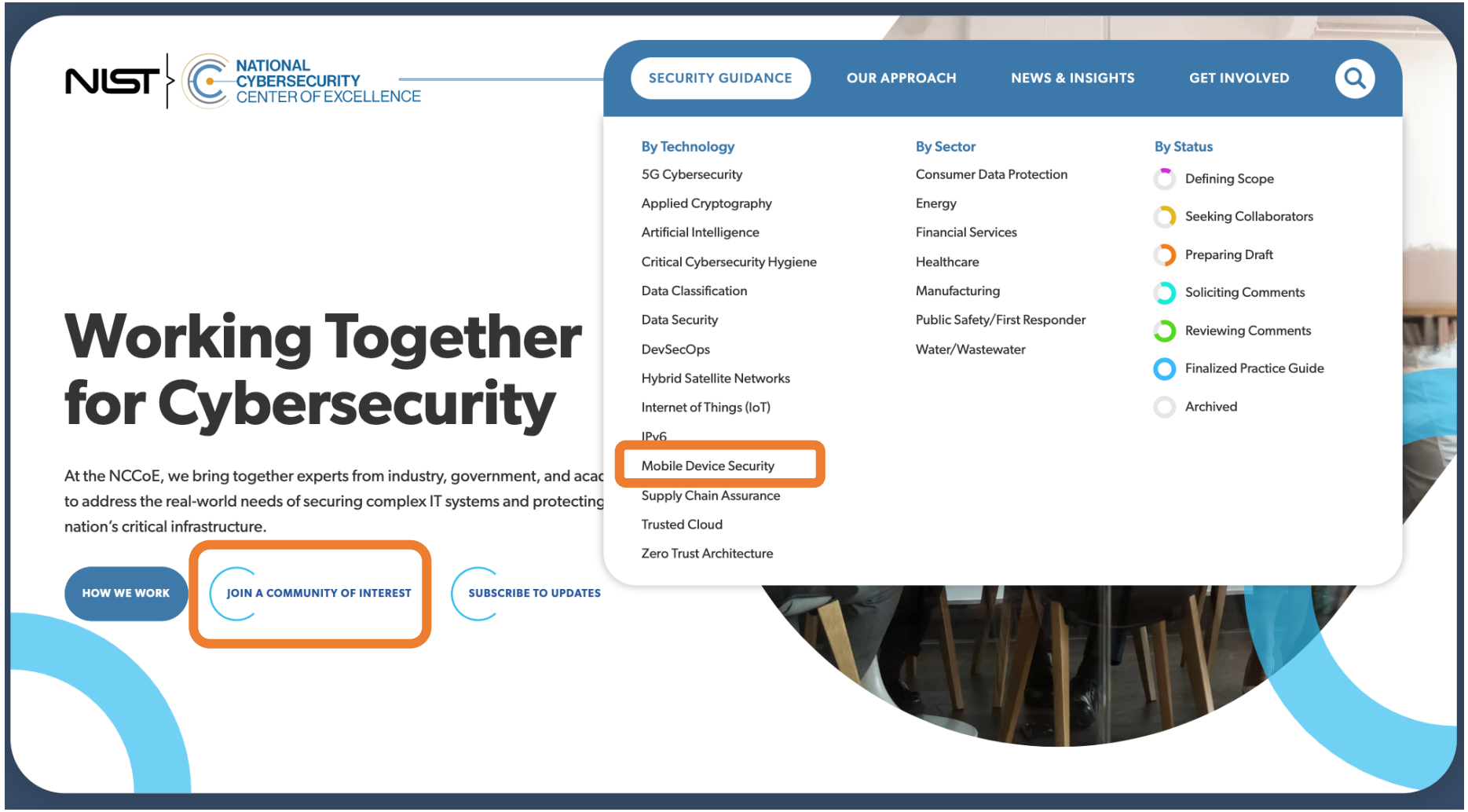
a. Conduct a risk assessment, including:
1. Identifying threats to and vulnerabilities in the system;
2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;
b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;
c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]];
d. Review risk assessment results [Assignment: organization-defined frequency];
e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and
f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

CAIQ GRM-08.1 Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?

FMCSA GDL 1 Conduct architectural analysis and/or threat modeling during system design

Closing Remarks

Check out our website: https://www.nccoe.nist.gov/



Questions?

Gema@nist.gov

We Want to Hear From You

What other topic(s) would be helpful to include in future guides?

- Share a Project Idea
- Discuss Challenges
- Contribute to Publications
- Participate in a Project
- Join a Community of Interest

mobile-nccoe@nist.gov

Mobile Project Lead:
Gema Howell
Gema@nist.gov

(Back Up Slides)

ENTERPRISE MOBILITY MANAGEMENT (EMM)

What is it?:

- A policy enforcement tool that allows organizations to secure the mobile devices of users who are authorized to access organizational resources.

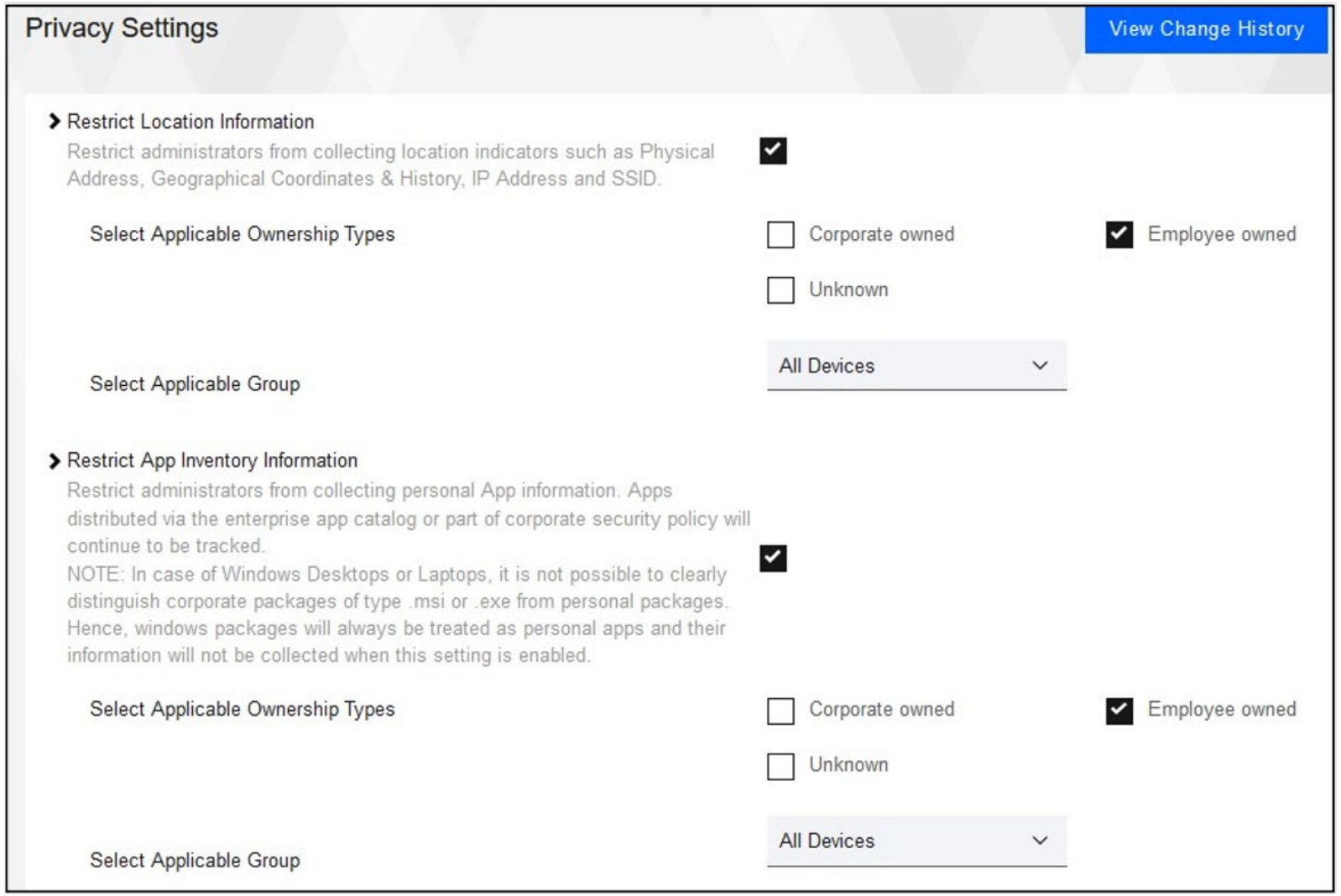
How does it work?:

- Mobile administrators use the EMM portal to manage and enforces the polices, configurations, and security actions applied to registered mobile devices.
- An EMM agent on the mobile device, usually in the form of a mobile application.

How does it address security and privacy concerns?:

- The EMM enforces organizational policies for security and privacy controls.
- The EMM also establishes the work environment for work activities and the separation from personal information.

ENTERPRISE MOBILITY MANAGEMENT (EMM)



ENTERPRISE MOBILITY MANAGEMENT (EMM)

IBM **MaaS360**

To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

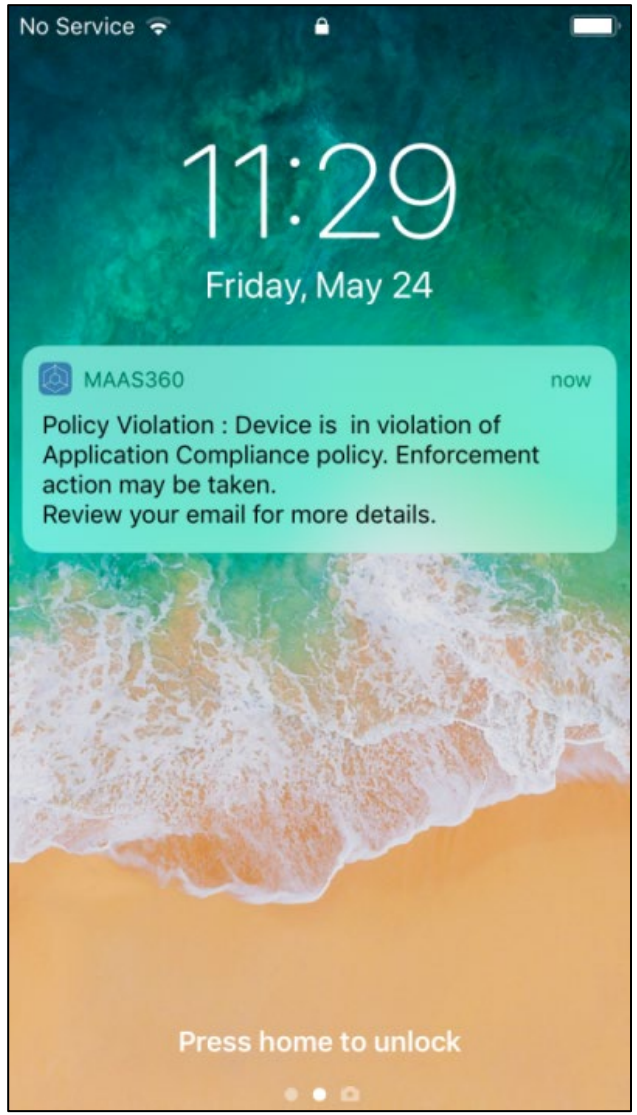
Policy Violation Alert

Device Name: iPhone
Username: o n (o @ .com)
Policy Violation: Application Compliance
Restricted App detected: PhoneCopy
Restricted App detected: My Calendar
Restricted App detected: PCalendars

Review executed and planned enforcement actions below:

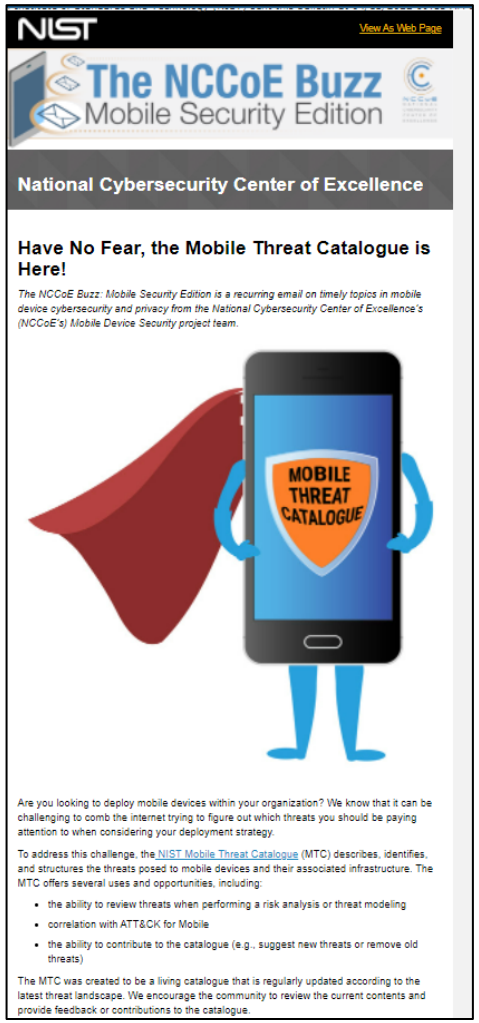
Action(s) Performed:
Remove Control. Device will stop being managed.
Action(s) Planned: None

Instructions from Admin: Enterprise Mobile Device Management control is removed from your device due to failure to comply to application requirements.

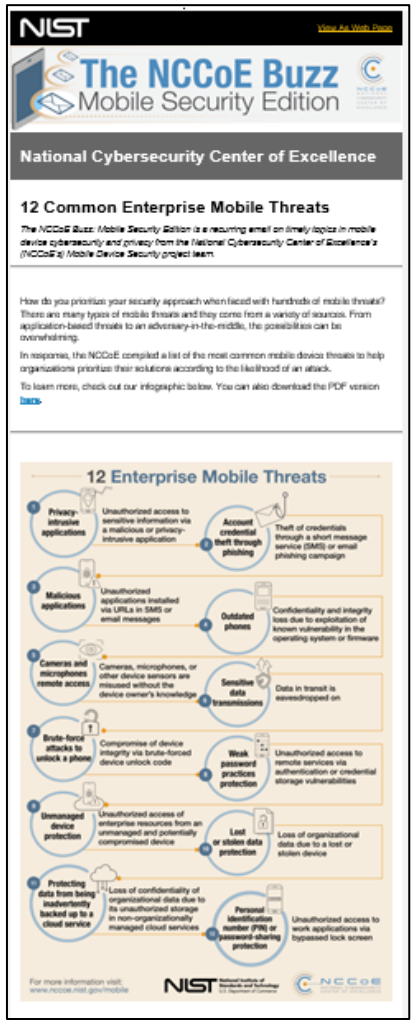


Mobile Device Security Buzzes

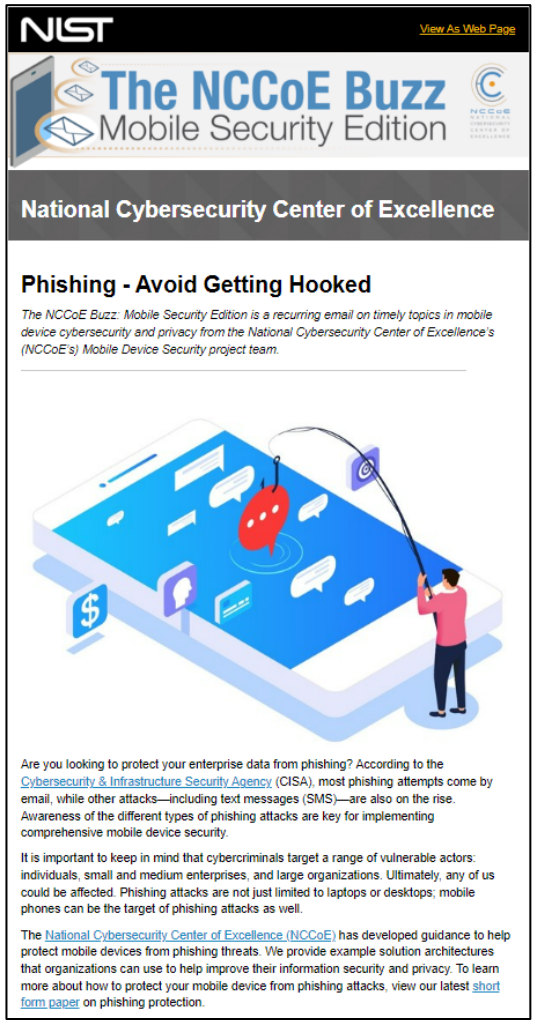
January 2022,
Privacy



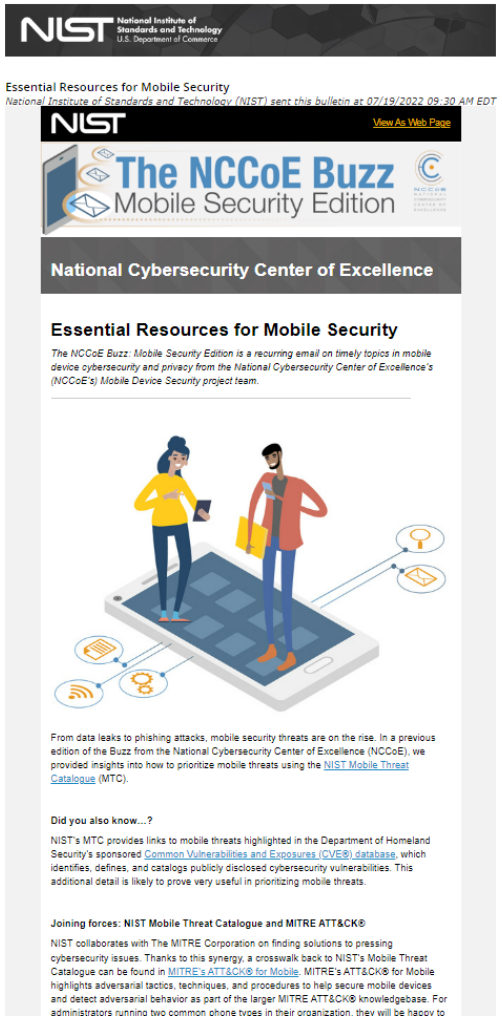
April,
Common Threats



May,
Mobile Threat Catalogue



June,
Phishing



July,
MTC and ATT&CK

Mobile Device Security Buzzes

NIST View As Web Page

The NCCoE Buzz
Mobile Security Edition

National Cybersecurity Center of Excellence

7 Privacy Challenges for Enterprise Mobility

The NCCoE Buzz: Mobile Security Edition is a recurring email on timely topics in mobile device cybersecurity and privacy from the National Cybersecurity Center of Excellence's (NCCoE's) Mobile Device Security project team.

When organizations allow employees to use mobile devices for work (e.g., Bring Your Own Device/BYOD), there are potential privacy implications that can impact employees. Privacy and cybersecurity are commonly thought of as two distinct areas, but when considering the risks of each, they often intersect.

Below is a list of 7 privacy challenges for enterprise mobile deployments, some of which arise from cybersecurity-related risks:

August,
Mobile Privacy Risks

NIST View As Web Page

The NCCoE Buzz
Mobile Security Edition

National Cybersecurity Center of Excellence

Zero Trust Applied to the Mobile World

The NCCoE Buzz: Mobile Security Edition is a recurring email on timely topics in mobile device cybersecurity and privacy from the National Cybersecurity Center of Excellence's (NCCoE's) Mobile Device Security project team.

Many professionals in the cybersecurity community are talking about zero trust architecture (ZTA), and although it is not a new concept, there is renewed interest in implementing zero-trust principles. This introduces challenges for an organization's mobile administrators. But what does zero trust *really* mean for mobile?

Due to the pandemic, many employees have transitioned to remote/telework options to accomplish their daily work activities. The portability of mobile devices makes it easier to respond promptly to emails, attend virtual meetings, and use special work apps from anywhere, even in your own home. They also serve as backup devices when the primary computing devices are not functioning properly at remote sites.

In this new environment, mobile devices are now another endpoint connected to enterprise resources and can put the entire enterprise at risk if compromised or stolen. ZTAs can minimize this impact by applying cybersecurity practices that assume no implicit trust, constant monitoring, and restricted access to the enterprise resources based on the criticality of resources and user and device identity and posture.

September,
RSA Blog Promotion

NIST View As Web Page

The NCCoE Buzz
Mobile Security Edition

National Cybersecurity Center of Excellence

Mobile Passwords--Tricks & Treats

The NCCoE Buzz: Mobile Security Edition is a recurring email on timely topics in mobile device cybersecurity and privacy from the National Cybersecurity Center of Excellence's (NCCoE's) Mobile Device Security project team.

With Halloween around the corner, the National Cybersecurity Center of Excellence (NCCoE) wants to share a few "tricks" and tips for mobile passwords that result in the "treat" of protecting your mobile device from compromise.

Potential Threats

Below is a list of several potential mobile password threats that can impact you or your organization:

- **Lost/Stolen Phone** – If an unauthorized user obtains a lost or stolen mobile phone that has no password, they may have easy access to sensitive information on the device (e.g., messages, photos, or email)
- **Brute-Force Attack** – If a mobile phone has a weak password, a malicious attacker may be able to easily obtain the password and gain access to information on the mobile phone
- **Phishing** – If a password is captured by texting or emailing to convince a user or subscriber into thinking the attacker is a verifier or reliable party, the attacker can gain access to a user's account(s) and access sensitive information

October,
Mobile Passwords Tricks and Treats