



Mobile Security R&D Program Guide

Volume 2



**Homeland
Security**

Science and Technology

Introduction to the Mobile Security R&D Program Guide

Thank you for your interest in the U.S. Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Mobile Security Research and Development (R&D) program. This technology guide introduces you to the goals and objectives for the Mobile Security R&D program and its alignment with DHS and federal mobile security strategies and priorities and also provides a view into S&T's development of new and cutting-edge mobile security solutions. We are excited to share these promising mobile security technologies with you and welcome your feedback.

Through targeted mobile security R&D that addresses mobile security gaps and barriers, S&T is helping to accelerate the adoption of secure mobile technologies by government agencies and the mobile industry and protect the Homeland Security Enterprise (HSE). This guide represents the important contributions of the overall program's Mobile Application Security (MAS) and Mobile Device Security (MDS) projects in supporting DHS component requirements as well as broader federal government and HSE mobile security needs. The Mobile Security R&D program goals are to apply R&D to:

- Enable the mobile workforce to support the homeland security mission
- Enable mission success through effective, efficient and secure mobile technologies

This technology guide, which will be updated and published periodically, features 12 new and innovative technologies. To help direct future publications, please reflect on the mobile security capability gaps in your organization and share your thoughts with us. Your input will help us identify timely solutions and inform future research efforts. Again, it is our pleasure to introduce you to the Mobile Security R&D program and its newly developed and enhanced mobile security technologies.

Sincerely,



Dr. Douglas Maughan
DHS S&T Cyber Security Division Director



Vincent Sritapan
DHS S&T Mobile Security R&D Program Manager



CONTENTS



1 DHS SCIENCE AND TECHNOLOGY DIRECTORATE (S&T) CYBER SECURITY R&D

3 MOBILE SECURITY R&D PROGRAM STRATEGY

11 MOBILE APPLICATION SECURITY

- 12 Orchestration Platform and Correlation for Mobile Software Assurance Tools
- 13 Advancing Mobile Endpoint Security
- 14 Android Security Toolkit
- 15 Hardware-Anchored Continuous Validation and Threat Protection of Mobile Applications
- 16 Assured Mobile Application Lifecycle using Red Hat Mobile
- 17 COMBAT: Continuous Monitoring of Behavior to Protect Devices from Evolving Mobile Application Threats

19 MOBILE DEVICE SECURITY

- 20 Trusted User Module
- 21 Virtual Mobile Infrastructure
- 22 SENSor Secure Enterprise Infrastructure
- 23 Persistent Implant Finder
- 24 Prepositioned Cyber-Threats

25 MOBILE SECURITY GUIDANCE

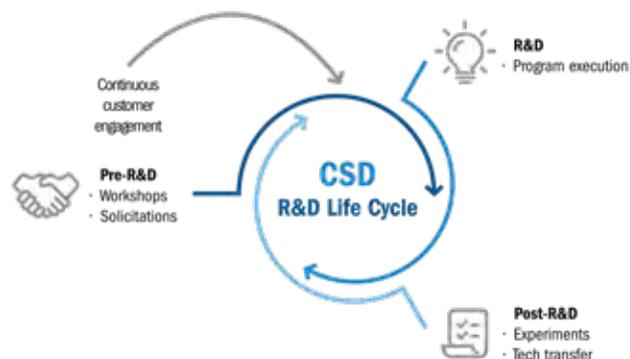
- 26 Table of Mobile Security Guidance

33 CONCLUSION

Department of Homeland Security Science and Technology Directorate: Cyber Security R&D

THE DEPARTMENT OF HOMELAND SECURITY (DHS) SCIENCE AND TECHNOLOGY DIRECTORATE (S&T) LEADS DEVELOPMENT OF NEXT-GENERATION CYBERSECURITY SOLUTIONS

Threats to the internet are constantly changing. As a result, cybersecurity is one of the most challenging areas in which the Federal government must keep pace. Next-generation cybersecurity technologies are needed to enhance the security and resilience of the nation's current and future critical infrastructure and the internet. S&T is enabling and supporting research, development, testing, evaluation and transition of advanced cybersecurity and information assurance technologies. This comprehensive approach is aligned with several federal strategic plans including the Federal Cybersecurity Research and Development Strategic Plan announced in February 2016, National Critical Infrastructure Security and Resilience Research and Development Plan released in November 2015, and the National Privacy Research Strategy unveiled in June 2016.



S&T's research and development programs support the approaches outlined in the Federal Cybersecurity Research and Development Strategic Plan by:

- developing and delivering new technologies, tools and techniques to enable DHS and the nation to defend, mitigate and secure current and future systems, networks and critical infrastructure against cyberattacks
- leading and coordinating research and solution development among the R&D community, which includes Department customers, government agencies, the private sector, academia and international partners
- conducting and supporting technology transition to the marketplace

S&T'S BROAD CYBERSECURITY TECHNOLOGY AND CAPABILITY DEVELOPMENT PORTFOLIO

S&T's work is focused on the following programmatic areas, many of which are comprised of multiple projects targeting specific aspects of the broader program area:

Cyber for Critical Infrastructure—Securing the information systems that control the country's energy infrastructure, including the electrical grid, oil and gas refineries, and pipelines, to reduce vulnerabilities as legacy, standalone systems are networked and brought online; creating innovative approaches to plan and design adaptive performance in critical infrastructure systems; and collaborating with DHS, industry and other federal and state agencies on the Critical Infrastructure Resilience Institute (CIRI) Center of Excellence, which conducts research to address homeland security critical infrastructure challenges.

Cyber Physical Systems—Ensuring cyber-physical systems and internet of things (IoT) security vulnerabilities are identified and addressed before system designs are complete and the resulting devices are widely deployed by developing cybersecurity technical guidance for critical infrastructure sectors; developing technology solutions for automotive, medical devices and building controls with an increasing focus on IoT security; addressing security, trust, context-awareness, ambient intelligence and reliability of cyber-enabled networked physical systems; and engaging through coordination with the appropriate sector-specific oversight agency, government research agencies, industry engagement and support for sector-focused innovation, small business efforts and technology transition.

Human Aspects of Cybersecurity—Researching incentives for the adoption of cybersecurity measures by infrastructure owners, the reputations of commercial network operators for preventing attacks and understanding criminal behaviors to mitigate cyber-risks; developing intuitive security solutions that can be implemented by information technology owners and operators who have limited or no training; and developing decision aids to help organizations better gauge and measure their network's security posture and undertake appropriate upgrades based on threats and costs.

Identity Management and Data Privacy—Providing customers the identity and privacy R&D expertise, architectures and technologies needed to enhance the security and trustworthiness of their systems and services.

“Special attention should be paid to R&D that can support the safe and secure integration into society of new technologies that have the potential to contribute significantly to American economic and technological leadership.

—OMB Memo M-17-30, Fiscal Year 2019 Administration Research and Development Priorities

Law Enforcement Support—Developing new cyber-forensic analysis tools and investigative techniques to help law enforcement officers and forensic examiners address cyber-related crimes and investigate the use of anonymous networks and cryptocurrencies by criminals.

Mobile Security—Developing innovative security technologies to accelerate the adoption of secure mobile technologies by DHS, the entirety of the federal government, and the global community. Current areas of development underway spanning mobile device security and mobile application (“app”) security are: mobile software roots of trust, firmware security, virtual mobile infrastructure, continuous validation and threat protection for mobile apps, and tools to integrate security throughout the mobile app development lifecycle. DHS also has identified a need for a new R&D project focused on security and resilience of mobile network infrastructure. S&T currently is developing requirements for this new program area.

Network Systems Security—Developing technologies to mitigate the security implications of cloud computing; building technologies to mitigate new and current distributed denial of service attack types; launching an Application of Network Measurement Science project to improve the collection of network traffic information from around the globe; conduct research in attack modeling to enable critical infrastructure owners and operators to predict the effects of cyberattacks on their systems and create technologies that can identify and alert system administrators when an attack is occurring; and enhancing security of the internet’s core routing protocol so communications follow the intended path between organizations.

Next Generation Cyber Infrastructure Apex—Addressing cybersecurity challenges facing the financial services sector by providing the technology and tools to counter advanced adversaries when they attack U.S. cyber systems and financial networks.

Open-Source Technologies—Building awareness of open-security methods, models and technologies that provide sustainable approaches to support national cybersecurity objectives.

Software Assurance—Developing tools, techniques and environments to analyze software, address internal flaws and vulnerabilities in software; modernizing and advancing the capabilities of static analysis tools to improve

coverage and integrate it seamlessly in the software development and delivery processes; and improve software security associated with critical infrastructure (energy, transportation, telecommunications, banking and finance, and other sectors).

Transition to Practice—Transitioning federally funded cybersecurity technologies into broader use and creating an efficient transition process that will have a lasting impact on the R&D community as well as the nation’s critical infrastructure.

PREPARING FOR EMERGING CYBER-THREATS

Through its R&D focus, S&T is committed to ensuring the nation’s long-term internet security and reinforcing America’s leadership in developing the cybersecurity technologies that safeguard our digital world. As new threats emerge, S&T will be at the forefront of actions at all levels of government, in the R&D community and throughout the private sector to protect data privacy, maintain economic and national security, and empower citizens to take control of their digital security.



MOBILE SECURITY R&D PROGRAM STRATEGY

Mobile Security Research and Development Program Strategy

VISION

The Federal government workforce has become increasingly reliant on mobile technologies to facilitate its mission and elevate productivity. As use of mobile technologies becomes more pervasive in the government, solutions are needed to secure mobile devices, for a coordinated approach to lifecycle management, and policies to guide the selection and operational use of mobile solutions. To promote the adoption of safe and secure mobile technology within the Department of Homeland Security (DHS) and across the entirety of the Federal government, the DHS Science & Technology Directorate (S&T) has established the Mobile Security Research and Development (R&D) program. Presently, this program is composed of the Mobile Device Security (MDS) and the Mobile Application Security (MAS) projects. DHS also has identified a need for a new R&D project focused on security and resilience of mobile network infrastructure. S&T currently is developing requirements for this new program area.

- 77 percent of U.S. adults own and use smartphones[3] and almost 40 percent of DHS employees have government-issued mobile devices.[4]
- The official mobile app stores (Google Play[5], Apple App Store[6], Amazon Appstore[7]) collectively offer nearly 7 million unique mobile apps.
- More than 1.5 million app publishers/developers provide apps to official app stores.[8]

Two converging factors help to create the urgent need for secure enterprise solutions. First, mobile solution use is rapidly increasing across the federal government. Second, mobile threats are increasingly common and more sophisticated, which puts data stored or processed on these devices at risk and exposes backend systems and networks to attacks via mobile malware.

As documented in the DHS Study on Mobile Device Security[9], threats exist across all elements of the mobile ecosystem—from mobile devices, applications and

GUIDING VISION FOR MOBILE SECURITY R&D

Accelerate the adoption of secure mobile technologies by the Department, the federal government and the global community.

BACKGROUND

The government's increasing reliance on mobile technology has made it an attractive and lucrative target for cyberattacks. The enhanced capabilities mobile technologies provide, the ubiquity and diversity of mobile applications and devices, and the typical use of the devices outside agencies' traditional network boundaries requires a security approach that differs substantially from the protections developed for desktop workstations.

The following statistics tell the scope and scale of the mobile industry:

- 5 billion subscribers globally[1], 395.9 million subscribers in the U.S.[2], and 1.5 million subscribers within the federal government.
- Wireless revenues: \$1.06 trillion globally[1], \$235.6 billion in the U.S.[2] and almost \$1 million in federal mobile and wireless services contracts.

data to the underlying infrastructure of carrier networks, mobile operating system providers, mobile device vendors, and enterprise systems and infrastructure. As shown in Figure 1, a mature mobile ecosystem comprises many elements. In addition to the mobile device, it includes the environment that connects the device to other devices, mobile applications, mobile application marketplaces and information systems. Each area presents security challenges and opportunities for additional study and mobile security R&D.

OBJECTIVES

To respond to the evolving threats and security challenges with mobile technologies, S&T has established an approach for the Mobile Security R&D program to identify and meet customer-driven needs. The approach starts with establishing strategic DHS component/customer and stakeholder partnerships, which are the basis for gathering

requirements and generating ideas for targeted R&D efforts. After a competitive acquisition process, innovative technologies to meet the requirements are researched, developed and made available to customers for pilots and refinement. In parallel, the Mobile Security R&D program maintains landscape awareness of technical trends as well as policy and procurement issues to ensure integration needs are understood and mechanisms are in place after the R&D phase ends that enables customers to acquire the new technologies and policies are in place to support operational use. The Mobile Security R&D program follows a three-pronged approach to achieve its R&D vision:



1. Partner with DHS components and federal stakeholders to identify operational requirements and capability gaps
2. Develop secure, innovative mobile solutions to support the DHS and overall Federal government missions
3. Champion the solutions to support transition into operational use

STRATEGIC ALIGNMENT

To respond to the evolving threats and security challenges with mobile technologies, S&T has established an approach for the Mobile Security R&D program to identify and meet customer-driven needs. The approach starts with establishing strategic DHS component/customer and stakeholder

The Mobile Security R&D program objectives and initiatives align with DHS, S&T and Federal government strategies and priorities. Within DHS in particular, the Mobile Security R&D program has sought to acquire technologies and

capabilities identified by the DHS Integrated Product Team (IPT), Secure Cyberspace–Mobile Security Sub-IPT. Broader alignment to DHS S&T priorities is as follows:

- Study on Mobile Device Security, April 2017[9]
- S&T Strategic Plan 2015-2019[10], Visionary Goal, Objectives 1 and 2:
 - Objective 1: Deliver Force Solutions:
 - Identify and Prioritize Operational Requirements and Capability Gaps
 - Make Strategic Investments in High-Impact, Priority Areas
 - Partner with the Homeland Security Enterprise (HSE)
 - Objective 2: Energize the Homeland Security Industrial Base (HSIB):
 - Optimize Markets by Pooling Demand and Developing Standards
 - Engage the HSIB through a Deliberate, Continuous and Transparent Approach
 - Improve Programs Designed to Increase Collaboration with Innovative Companies
- DHS Information Technology Strategic Plan 2015-2018[11]:
 - Goal 2: Innovative Technology, Objective 2.4: Enable end-to-end delivery of mobile solutions that enhance enterprise-wide mobile computing capabilities for successful mission outcomes.
 - Goal 4. Cybersecurity, Objective 4.2: Enable secure communications to effectively support the mission of DHS and its partners.
- National Security Telecommunications Advisory Committee (NSTAC) Report to the President on Emerging Technologies Strategic Vision-DRAFT[12]:
 - Security of the Fifth Generation (5G) infrastructure should receive great priority and the shift to 5G represents another opportunity to get cybersecurity right.

INITIATIVES TO ADDRESS PROGRAM OBJECTIVES

OBJECTIVE 1. Partner with Components and Federal Stakeholders to Identify Operational Requirements and Capability Gaps

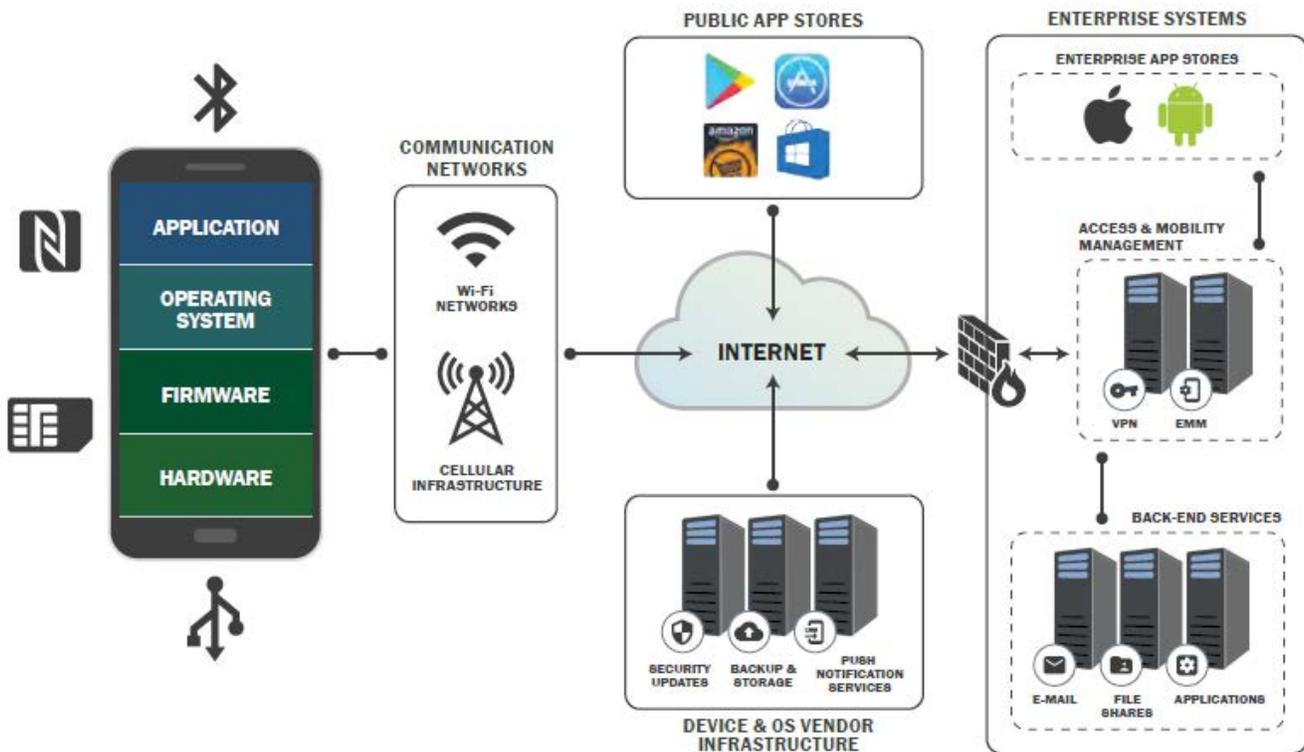
The Mobile Security R&D program leverages the efforts of existing federal and DHS mobility working groups to gather and prioritize remediation of mobile security capability gaps that prevent implementation of mobile technologies at the federal level and across the HSE. These groups include the following federal and DHS working groups:

- DHS Integrated Product Team (IPT), Secure Cyberspace—Mobile Security Sub-IPT
- Federal Chief Information Officers (CIO) Council's Information Security and Identity Management Committee (ISIMC) Mobile Technology Tiger Team (MTTT)
- Mobile Services Category Team (MSCT)
- DHS Joint Requirements Council (JRC)

OBJECTIVE 2: Develop Secure Mobile Solutions to Support the DHS Mission

The Mobile Security R&D program funds a number of solution development initiatives with private industry and academia to address gaps in mobile security technology and policy, as identified through its partnerships with other DHS components and federal agencies (under Objective 1). These R&D efforts are applied across the mobile ecosystem depicted in Figure 1 and build on existing technologies. R&D solution development is acquired through myriad flexible acquisition mechanisms, including targeted Broad Agency Announcements (BAAs), the S&T Long-Range BAA, Small Business Innovation Research (SBIR) funding, and Other Agencies Technology Solutions (OATS) SBIRs. The current Mobile Security R&D project efforts are organized into the following R&D project areas, which are described in detail below:

- Mobile Application Security
- Mobile Device Security



The Mobile Ecosystem

Mobile Application Security Project

The Mobile Application Security (MAS) project is developing innovative approaches that extend beyond deployment of an app to provide continuous assurance of mobile app security throughout an app's lifecycle. The MAS project has two primary R&D foci. One focus is continuous monitoring, vetting and security assurance of mobile apps to safeguard against vulnerabilities and future threats. The second focus is establishing a security framework and integrated development environments that will result in mobile app development platforms that enable developers to transparently ensure security and functionality throughout the mobile application lifecycle.

The MAS project industry and academia initiatives across the two R&D thrust areas are:

- Mobile App Security Orchestration Platform/Certification Tool, Apcerto Inc.
- A Framework for Assessing, Analyzing, and Archiving Mobile Applications, Kryptowire
- Continuous Validation and Protection for Mobile Devices, Lookout
- Hardware-Anchored Continuous Validation and Threat Protection of Mobile Applications, Qualcomm Technologies
- Assured Mobile Application Lifecycle using Red Hat Mobile, Kryptowire/Red Hat, Inc.
- Android Security Toolkit, Progeny Systems/Microsoft/Xamarin
- COMBAT: COntinuous Monitoring of Behavior to protect devices from evolving mobile Application Threats, United Technologies Research Center

The MAS thrusts are expanded upon below.

Continuous Validation and Threat Protection for Mobile Apps

The MAS project is funding efforts to monitor device and app execution against the security criteria established by the Federal Mobile Application Security Vetting Working Group and currently maintained by the National Information Assurance Partnership (NIAP)[6]. MAS also is developing capabilities specific to the mobile device operating environment that will respond to current known threats and vulnerabilities including the identification of malware and vulnerable code. This R&D entails developing the capability to anticipate and—if needed—respond to future threats and vulnerabilities

while continuously monitoring a mobile device's security posture. These capabilities go beyond identifying malicious software to pinpoint undesirable behavior that violates user-defined risk criteria. By providing a standard evaluation score and analysis report that provides actionable information for decision-makers to remediate problems, this effort also promotes information sharing across components and federal agencies, potentially reducing cost and avoiding duplication of analysis efforts.

Integrated Security Throughout the Mobile Application Lifecycle

The MAS project is funding R&D efforts to augment mobile app development tools with functionality that—transparently to the developer—incorporates secure mechanisms as mobile apps are developed. To make a more immediate impact, efforts in this area are building on existing mature mobile app development platforms to include requirements that will ease government use.

Mobile Device Security Project

The Mobile Device Security (MDS) R&D project focuses on securing mobile devices that can be used by adversaries to physically track device owners, to access sensitive information, to negatively impact government services, and for other nefarious objectives. The MDS project focuses on three high-priority gap topics: mobile device management, trust implementation for mobile executables, and firmware security.

The MDS project industry and academia R&D initiatives and performers are:

- Trusted User Module, Def-Logix
- Prepositioned Cyber Threats, University of Illinois at Urbana-Champaign
- Persistent Implant Finder, Red Balloon Security, Inc.
- Virtual Mobile Infrastructure, Intelligent Waves, LLC
- SENSsEI: SENSor Secure Enterprise Infrastructure, Metronome

MDS funds initiatives in the following R&D areas to address these gaps:

Mobile Software Roots of Trust

This area seeks to develop tamper-evident modules—or “roots of trust”—that continuously can be measured and verified to produce a chain of cryptographically strong evidence about the state of the device. This approach verifies devices are in a protected state at power-on and continues



to bootstrap trust to verify software (e.g., operating system, apps, security management software, etc.) before and during execution. This root of trust can be queried and measured to attest to the state of the device to provide greater assurance to security mechanisms such as software verification, application and data isolation, and data protection, which are at the heart of security enforcement technologies such as mobile device management.

Firmware Security

There are many risks to the mobile ecosystem that originate in the supply chain. Firmware design and the firmware update process are known avenues of security risks. For example, there have been documented cases where commercially available smartphones contain preloaded software that collects sensitive user data and sends it overseas[13]. To address these risks, S&T has embarked on two projects that explore supply-chain security risks of embedded functionality that accesses user information without obtaining user consent or circumvent security controls.

Virtual Mobile Infrastructure Extensions

Depending on security and regulatory requirements, infrastructure virtualization may provide security controls necessary to enable critical operations via mobile devices. To facilitate customer operations where virtualization provides an essential separation of data from mobile devices, S&T is funding virtual mobile infrastructure technology development.

OBJECTIVE 3. Champion Program-Developed Technology to Support Transition into Operational Use.

Transitioning the program-developed technology into operational use is a priority for and an integral part of the Mobile Security R&D program. S&T engages stakeholders early to inform the research and identify customers that are willing to be involved. During and after research execution, the program conducts outreach to educate and raise awareness of the innovative technologies it is developing. Outreach activities include hosting technology showcases, engaging directly with federal CIOs, expediting solution matchmaking and facilitating pilot projects to accelerate adoption of technologies.

Mobile Network Infrastructure

As described in the DHS Study on Mobile Device Security[10], threats to the mobile network infrastructure are real and will require R&D as well as evolving policies and strategies to manage risks to the security of the mobile

ecosystem. S&T is planning to initiate a mobile network infrastructure project that will seek to develop technologies to mitigate the highest security risks to the mobile network infrastructure identified in the HSE by DHS stakeholders. The following three preliminary focus areas have been identified:

Current and Legacy Protocol Security

This initiative would seek approaches and implementations to protect U.S. government personnel and citizens from being tracked or their calls or text messages from being snooped or hijacked due to inherent vulnerabilities in Signaling System Seven (SS7) and Diameter, which are rogue cellular tower threats, or vulnerabilities in Cloud-Radio Access Network (RAN) virtualized infrastructure.

5G Security

This project area will seek innovative approaches that leverage 5G virtual functions/network slicing to define methods and approaches to achieve:

- Flexible 5G security architecture tailored for a government environment
- Government-controlled security policy
- End-to-end security for the mobile device to the core
- Approaches to implement interoperable secure unclassified voice across Federal government departments and agencies.

Mobile Network Traffic Visibility for the Enterprise.

This R&D area will focus on development of new or enhanced approaches to increase visibility into mobile network traffic and to improve protection for mobile devices and enterprise backend systems by independently monitoring traffic from mobile devices. Developed approaches must be scalable to meet the increasing demands and needs of the mobile workforce.

Program Manager Contact Information:

For more information about the overall Mobile Security R&D program or its project areas, contact the program manager at:

Vincent Sritapan
S&T Mobile Security R&D Program Manager
Vincent.Sritapan@hq.dhs.gov

REFERENCES

- [1] GSMA Intelligence, “Definitive data and analysis for the mobile industry,” [Online]. Available: <https://www.gsmaintelligence.com/>. [Accessed 11 September 2017].
- [2] CTIA, “2016 Wireless Industry Survey,” [Online]. Available: <https://www.ctia.org/docs/default-source/default-document-library/annual-year-end-2016-top-line-survey-results-final.pdf?sfvrsn=2>. [Accessed 15 June 2017].
- [3] Pew Research Center, “Mobile Fact Sheet,” [Online]. Available: <http://www.pewinternet.org/fact-sheet/mobile/>. [Accessed 11 September 2017].
- [4] Department of Homeland Security, “DHS Enterprise MDM Baseline Initiative Report,” 2015.
- [5] Statista, “Number of available applications in the Google Play Store from December 2009 to September 2017,” [Online]. Available: <https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/>. [Accessed 11 September 2017].
- [6] Statista, “Number of available apps in the Apple App Store from July 2008 to January 2017,” [Online]. Available: <https://www.statista.com/statistics/263795/number-of-available-apps-in-the-apple-app-store/>. [Accessed 11 September 2017].
- [7] Statista, “Number of available apps in the Amazon Appstore from March 2011 to April 2016,” [Online]. Available: <https://www.statista.com/statistics/307330/number-of-available-apps-in-the-amazon-appstore/>. [Accessed 11 September 2017].
- [8] Business of Apps, “App Download and Usage Statistics 2017,” [Online]. Available: <http://www.businessofapps.com/data/app-statistics/>. [Accessed 11 September 2017].
- [9] Study on Mobile Device Security, April 2017, [prepared by the Department of Homeland Security (DHS) in consultation with the National Institute of Standards and Technology (NIST) <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>]
- [10] DHS S&T, “DHS Information Technology Strategic Plan FY2015-2019,” 2015 [Online]. Available: [S https://www.dhs.gov/sites/default/files/publications/ST_Strategic_Plan_2015_508.pdf](https://www.dhs.gov/sites/default/files/publications/ST_Strategic_Plan_2015_508.pdf). [Accessed 13 February 2018].
- [11] “DHS Information Technology Strategic Plan FY2015-2018,” 2015 [Online]. Available: https://www.dhs.gov/sites/default/files/publications/DHS_ITStratPlan_508.pdf. [Accessed 11 September 2017].
- [12] National Security Telecommunications Advisory Committee, “NSTAC Report to the President on Emerging Technologies Strategic Vision,” [Online]. Available: <https://www.dhs.gov/sites/default/files/publications/Draft%20NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20%287-10-17%29%20v3%20%281%29-%20508.pdf>. [Accessed 2 October 2017].
- [13] “Amazon suspends sales of Blu phones for including preloaded spyware, again.” The Verge, July 31, 2017. Available: <https://www.theverge.com/2017/7/31/16072786/amazon-blu-suspended-android-spyware-user-data-theft> [Accessed 13 February 2018].





MOBILE APPLICATION SECURITY

Orchestration Platform and Correlation for Mobile Software Assurance Tools

Apcerto

Robert Shaw

bshaw@apcerto.com

OVERVIEW

This platform orchestrates mobile application (app) development and app vetting. The team is developing solutions for normalizing and rating mobile apps based on predefined standards and embedding these security steps throughout a mobile app development platform.

CUSTOMER NEED

We live in an era of ubiquitous connectivity, real-time information-sharing and unrestricted mobility. This environment provides a range of endpoint devices, mobility platforms, mobile devices management systems and often disjointed mobile app development and security implementations. The holistic orchestration platform called the Mobile App Factory will integrate the above components and enable secure mobile app development at scale with consistency, efficiency and ease.

APPROACH

For security, the solution uses machine-learning (i.e., a Bayesian risk-detection algorithm) to perform a selective creation of logical groupings of attack vectors to assign an aggregated risk-score. This approach enables normalization of app-vetting results to different standards such as the National Information Assurance Partnership (NIAP), Open Web Application Security Project, and Health Insurance Portability and Accountability Act.

For mobile app development, the risk-scoring developed will be an input into the Mobile App Factory that houses a structured collection of related software assets, operational models and methodologies that aid in the production of mobile applications at scale.

BENEFITS

The Mobile App Factory enables federal agencies to build secure mobile apps at scale with efficiency, ease, delivers the benefits of a holistic mobile app security and development platform and has the following advantages:

- Governance, compliance and highest security credentials available
- Synergy and automation between app development and security
- Designed with the government for use by government
- Customizable to agency-specific needs
- Related software assets, operational models and methodologies tailored to customers' needs

COMPETITIVE ADVANTAGE

The platform provides a framework for seamless and automated workflow from app conception to development, to testing and distribution through continuous monitoring. Compared to others, this solution is more cost-efficient, less time consuming, simplified by automation and verified to meet baseline mobile app security standards.

NEXT STEPS

The performer will integrate with other commercial and open-source security tool vendors and translate their respective outputs to a scoring system to further enhance its security measures. The project roadmap also includes integration with Enterprise Mobility Management (EMM) platforms, increased automation in mapping app-vetting analysis to the NIAP mobile application protection profile criteria and completion of the solution's app-testing capabilities to iOS and other mobile platforms.



Apcerto Mobile App Factory—App Development and Security Platform throughout a mobile application lifecycle.

Advancing Mobile Endpoint Security

Lookout

Daemon Morell

daemon.morrell@lookout.com

OVERVIEW

In this project, Lookout is advancing new mobile endpoint security capabilities that alert device users, mobile enterprise administrators and security personnel to security threats and provide the ability to remediate vulnerabilities.

CUSTOMER NEED

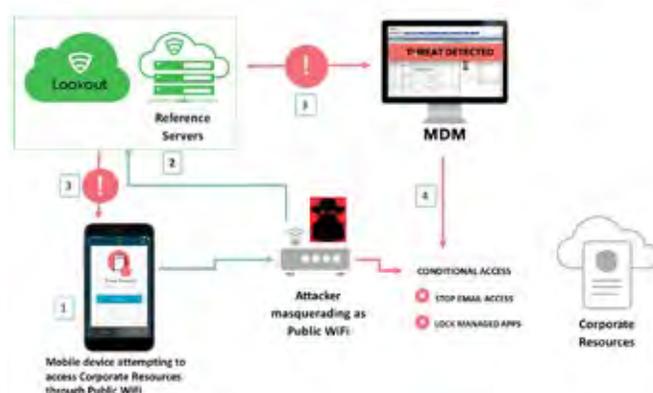
Given the proliferation of mobile device and application (app) use and the expanding mobile infrastructure, identifying and responding to threats to the mobile ecosystem is essential. To secure mobile endpoints, mobile enterprise management solutions must protect data on mobile devices and data in motion. Network-based attacks can exfiltrate corporate sensitive data despite enterprise managers and application developers following security best practices. For example, employees travel and use Wi-Fi hotspots that may be prone to network attacks at coffee shops, airports and other public places. These endpoint security capabilities will provide confidence to the end-user that their communications are not being intercepted or modified.

APPROACH

The performer is developing new app-threat, -risk and -vulnerability detection and protection capabilities and enhancing existing capabilities in its cloud-based Mobile Endpoint Security platform to protect mobile devices. These enhancements will strengthen the ability of government and enterprise to securely enable the use of mobile technologies for mission-critical activities. The work will enhance visibility into:

- Malicious and risky applications
- Phishing attacks
- Detection of side-loaded applications and non-app store signers
- Network-based threats
- Mobile device and application vulnerability detection/management
- Certificate Authority reputation system

The enhanced solution will be available for iOS and Android devices. An example of protection for network-based threats is shown below:



The endpoint app workflow for detecting and remediating against network-based threats targeting mobile devices.

BENEFITS

The benefits are to focus on threats that put mobile devices at risk. The Man-in-the-Middle approach minimizes false-positive alerts and by using safer networks, enables users to be more productive, with less risk to the misappropriation of sensitive information. Administrators also will have visibility into the capabilities and functions of all apps within their environment. This capability will allow them to identify apps that may pose significant risk based on the permissions they have on a device, the types of data they collect and where data may be exfiltrated.

NEXT STEPS

The performer is developing a localized remediation solution that will control a network connection if a threat is detected on a mobile device—whether app, operating system or network-based. This solution can deny access to corporate resources, lock apps that are leaking data or block all network traffic (i.e., place the device in “airplane mode”) until the threat is resolved. This solution will be valuable when a Mobile Device Management system is unavailable.

Android Security Toolkit

Progeny

Greg Laurent

glaurent@progeny.net

OVERVIEW

Progeny is using Microsoft's Xamarin platform, security enhancements and mobile devops best practices to enable the government to build a secure mobile application (app) framework that supports the needs of DHS and other federal agencies. Xamarin provides the capability to write cross-platform native mobile apps from a single code base for Apple, Android and Microsoft operating systems. Apps developed can run on-premises or in any cloud platform, including government-only clouds that meet critical regulatory compliance requirements.

CUSTOMER NEED

In today's operating environment, organizations need flexibility to manage their mobile platforms. Organizations and individuals routinely use a particular operating platform. Preferences frequently change as requirements or budgets shift. The solution is to develop a secure cross-platform framework that allows software to be written once into a common format and be deployed across each mobile environment. Developing a cross-platform environment provides flexibility, while preventing the app and organization from being locked into a particular platform, potentially causing implications as technology lifecycles advance. Another significant advantage is the cross-platform security approach. Threats to agency use of mobile devices exist across all elements of the mobile environment. These threats require a security approach that differs from the protections developed for PCs.

APPROACH

The project will establish enterprise-wide mobile security practices through mobile app development governance standards, best practices and tooling.

BENEFITS

This approach significantly enhances information security in mobile app development, testing, deployment and integration. Added benefits include increased development speed, efficiency and scalability, lowering development costs and improving the quality of mobile apps across the government.



The system under development is a cross-platform solution that continuously integrates security and mobile devops best practices throughout the app development and deployment lifecycle from established government and industry sources. The solution will provide government agencies the capability to write cross-platform, native mobile applications from a single codebase for Apple, Android and Microsoft operating systems.

COMPETITIVE ADVANTAGE

The capability to write cross-platform, native apps from a single codebase makes the features provided by the platform-specific Application Programming Interfaces (APIs) accessible within the Xamarin development tools. With mobile security, both device security and application security need to be considered. The performer has investigated and implemented device and mobile app security and identified requirements and best practices, while developing a methodology using Samsung KNOX to deliver security hardened, Security Technical Implementation Guide (STIG) compliant, Samsung Android devices. The performer also is expanding the methodology to iOS.

NEXT STEPS

The performer is working with government agencies to identify and develop mobile app use-cases, including users, devices, on-premise and cloud-based back-end integration, security and authentication requirements, push notifications, network routing, logging and auditing across organizations.

Hardware-Anchored Continuous Validation and Threat Protection of Mobile Applications

Qualcomm Technologies, Inc.

Kabir Kasargod

kabirk@qti.qualcomm.com

OVERVIEW

Today's mobile security solutions attempt to address continuous validation and protection for mobile applications (apps) and devices by focusing on developing capabilities that operate within the High Level Operating Systems (HLOS). These efforts include technologies for multi-factor authentication and malware detection. While these approaches have merit, they are not sufficient to fully address zero-day threats. Attackers often undermine or disable HLOS-based security by modifying the kernel and installing rootkits, thereby compromising government and industry security. This project will demonstrate the use of a hardware-anchored Mission-Critical-Grade Security Layer (MCGSL) to address zero-day attacks on commercial mobile devices by leveraging the Qualcomm® Snapdragon™ Security Platform and extending commercial capabilities to a military-grade mobile app security testing platform.

CUSTOMER NEED

Intelligent adversaries can craft attacks by moving deeper down the mobile device stack to attack the root of the device to disable HLOS and app defenses. Government and enterprise IT groups need security solutions that provide enhanced visibility into advanced mobile threats as well as increased trust that the user of the mobile device is the genuine user. However, combatting this level of threat requires a security solution that operates at a deeper execution level.



Attacks are moving deeper down the device stack and the visibility into these levels are limited. To address the challenge of a continuous application and user validation, a deep and broad foundational approach is required.

APPROACH

An MCGSL framework will provide application programming interfaces to the mobile app platform, allowing continuous validation and monitoring of third-party apps, run-time integrity checking of the device and continuous authentication of the user leveraging multiple biometric and contextual factors. These solutions operate at a deeper execution level, resulting in improved resilience to rootkit evasion and disablement.



The MCGSL is engineered to enable SoC-level access to device health, app behavior and user authentication to third parties via an extensible API. Kryptowire's Apps & Cloud will collect & analyze the data from the MCGSL.

BENEFITS

By leveraging device utilization context, app behavioral profile information and user authentication information, this approach offers coverage against a wide range of threats, reduces false-positives of security incidents and uncovers previously unseen advanced persistent threats. It also demonstrates enhanced security and increased usability that can be extended to enable an array of government and industry use-cases. Organizations also can quickly isolate compromised devices, eliminate malicious apps with real-time updates to on-device threat models and strengthen the user-authentication process.

NEXT STEPS

The research team will demonstrate the effectiveness of these solutions in a pilot program conducted by DHS.

Assured Mobile Application Lifecycle using Red Hat Mobile

Kryptowire LLC & Red Hat, Inc.

Tom Karygiannis
tkarygiannis@kryptowire.com

Steve O'Keefe
sokeefe@redhat.com

OVERVIEW

There is a significant gap in the mobile application (app) development lifecycle where the developer can introduce insecure code or code that could allow behavior that could violate management policies. These instances can either represent vectors of attack or issues that will fail security testing, requiring rework and delays. Red Hat, Inc. and Kryptowire LLC will integrate code-scanning technology into the mobile app development lifecycle, develop new capabilities and enhance the Red Hat Mobile Application Platform (RHMAP), while leveraging the mobile app information assurance software testing by Kryptowire for iOS and Android platforms.

CUSTOMER NEED

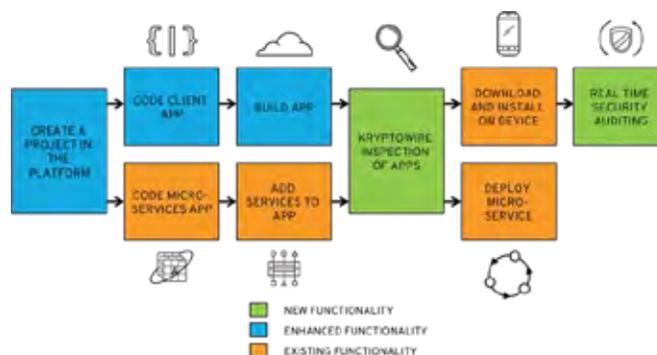
Resolving insecurities or policy violations in code after an app has been built requires considerable time and cost and can introduce delays in its release. Addressing these issues requires the introduction of secure-code scanning earlier in the development lifecycle.

APPROACH

The performers will build an integrated platform that enforces end-to-end security for mobile solutions and reduces the cost of maintaining mobile security policies—during the development process and while the apps are in use. The solution will automatically enforce checks to ensure all code and third-party libraries comply with U.S. mobile security standards before releasing it for deployment. When new security or privacy vulnerabilities are discovered that affect a deployed app, this approach can quickly push security updates to address the issue. The enforcement of the update can be accomplished through user notification or exclusion from use of back-end services.

BENEFITS

This unique capability will deliver continuous security assurance in mobile app development and result in automated governance of apps that comply with stringent government standards, thus minimizing the likelihood of human error when releasing apps. It will support mobile



This project will introduce new and enhanced functionality to the mobile app development lifecycle to make development more secure. New functionality includes inspection of apps and real-time security auditing while enhanced functionalities include creating the secure project, coding the client app and building the app.

app development and updates in compliance against the highest federal government mobile security requirements, to include National Information Assurance Partnership (NIAP) and National Institute of Standards and Technology (NIST) standards.

COMPETITIVE ADVANTAGE

This will be the first integrated commercial offering that enforces an end-to-end security model in the mobile app lifecycle. It will reduce the cost of maintaining mobile security policies during the app development process and while apps are in use. It will increase the velocity of secure mobile app development and updates.

NEXT STEPS

The performers will provide secure templates for Swift for iOS, Java for Android, and JavaScript for Apache Cordova cross platform framework. They also will provide an initial integration of their respective code-scanning capabilities using the operating-system-specific templates, followed by automation of the workflows.

COMBAT: COntinuous Monitoring of Behavior to Protect Devices from Evolving Mobile Application Threats

United Technologies Research Corporation

Devu Manikantan Shila

manikad@utrc.utc.com

OVERVIEW

COMBAT (COntinuous Monitoring of Behavior to Protect Devices from Evolving Mobile Application Threats) is a mobile app security vetting system that will be capable of preventing unauthorized access to sensitive information on mobile devices through robust identification of malware and vulnerable code. Current systems that rely on static analysis, dynamic analysis and machine learning approaches face a number of drawbacks, including information overload, a lack of solid risk-assessment baselines that prevent security analysts from making educated decisions, and an increased number of misclassified applications (apps). There also is a shortage of robust techniques for discovering vulnerable code or errors inadvertently introduced by the device developers.

CUSTOMER NEED

The development of software and algorithms to enable continuous monitoring of mobile devices to prevent malicious attacks and data theft will reduce the risk of misuse for all users of mobile devices. Third-party app stores increasingly are being used as an avenue for propagating malware because they do not police for malicious apps. Malware also can be delivered into a device via drive-by download, social engineering or phishing attacks. Even apps available via official app stores may not be safe. Importantly, solutions designed to detect malware lack the ability to detect unintentional security flaws in apps.

APPROACH

COMBAT uses artificial intelligence on diverse sources of information extracted from apps and public stores to detect malicious and vulnerable apps. COMBAT also evaluates the risk of an app and produces a detailed risk-assessment report. An in-device-based behavior monitoring service that will dynamically track the behavior of positively vetted apps in real time to enforce chosen policies will be also designed and developed.

BENEFITS

The success of this project will enable development of new algorithms and techniques for holistic and efficient detection of malicious apps as well as continuous protection of devices from emerging mobile application threats.

COMPETITIVE ADVANTAGE

COMBAT will enhance the state-of-the-art of malicious app evaluation and detection systems by predicting the risk associated with using an app for a given operational domain by reasoning over the outputs of detection classifiers. COMBAT may be used as a standalone tool or integrated with existing application vetting systems.

NEXT STEPS

The next steps include building a repository of malicious and benign applications and the third-party Software Development Kit/Integrated Development Environment and libraries used by developers. Once the task is completed, various features distinguishing malware and benign apps that will be used to train the machine learning classifiers, will be extracted.



MOBILE DEVICE SECURITY



Trusted User Module

Def-Logix

Paul Rivera

privera@def-logix.com

OVERVIEW

Trusted User Module (TUM) is a solution that provides software-based roots-of-trust for mobile devices such as mobile phones, tablets and wearable devices where a Trusted Platform Module (TPM) chip is absent. A key component to TUM is the use of a static random-access memory Physically Unclonable Function (PUF) and a Trusted Execution Environment (TEE) such as ARM TrustZone to interface them. The PUF and TEE will be used to securely store and generate keys similar to a TPM. By leveraging this technology, a device can produce and use cryptography services and keys available only to that unique device.

CUSTOMER NEED

Mobile devices like smartphones and tablets increasingly are being used by end-users for sensitive tasks such as personal banking. This trend makes end-users increasingly attractive targets for cybercrimes. These devices lack a firm foundation upon which to build trust and security. Software-based security methods provide limited security and no secure root-of-trust. Hardware-based security typically requires a TPM—a specialized piece of hardware—to provide root-of-trust services.

APPROACH

TUM uses a wearable as the software-based core root-of-trust. When paired with one or more devices, it supports apps that require verification of unique identity. The project's approach is a system using a PUF and TEE from Arm

TrustZone to interface them. The PUF is used to generate keys similar to the Endorsement Key (EK) and Storage Root Key (SRK) inside a TPM. The TEE is used as a location to securely employ these keys. A zero-knowledge proof is used to securely transmit the PUF to the TEE.

BENEFITS

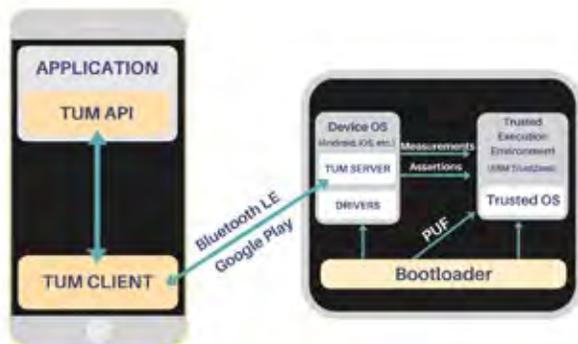
TUM is capable of securing multiple devices using single sign-on from a wearable device. It provides smartcard-like security, encryption, multifactor authentication, access control and identity management. The solution does not require special hardware, is platform agnostic and is easy to install.

COMPETITIVE ADVANTAGE

TUM improves on competitor solutions by implementing secure generation, storage and use of cryptographic keys on physically separate hardware. This allows mobile platforms to take advantage of TPM security practices previously only available on desktop systems. TUM can be easily installed from the Google and Apple app stores. In addition, TUM provides an Application Programming Interface (API) for third-party developers. This API allows numerous applications to be secured by TUM.

NEXT STEPS

The next steps for TUM development will be additional support for iOS devices and desktop computers, certification through the Fast Identity Online Alliance and growing the TUM app ecosystem. As TUM development continues, the expanded capabilities will continue to be updated and added to the Google and Apple app store offerings.



TUM Security Partitions and Data Flow diagram.

Virtual Mobile Infrastructure

Intelligent Waves, LLC

Matthew Stern

matthew.stern@intelligentwaves.com

OVERVIEW

Mobile devices have revolutionized business processes, allowing workers to be more productive, stay more connected and react to incidents in near real-time. Unfortunately, mobile devices also bring tremendous risk to organizations as sensitive data and apps are at risk on devices that can easily be lost, stolen or hacked. The technology developed in this project enables organizations to virtualize mobile devices so sensitive apps and data can be made available to mobile devices virtually, while maintaining appropriate security controls for the data on back-end servers.

CUSTOMER NEED

Many regulated industries and various parts of state, local and federal governments have strict policies to protect digital assets. With users increasingly relying on mobile devices for work, these industries and governments have been pressed to come up with answers. While traditional enterprise mobility solutions have focused on managing the apps, data and mobile device itself, attackers have continued to find ways to compromise mobile devices. There is a strong need—especially in regulated industries and government—for enabling users with mobile access without putting sensitive assets at risk.

APPROACH

The technology's unique approach is to avoid deploying sensitive assets to the mobile device entirely. Instead, with a virtual mobile smartphone that runs in a secure datacenter, users can rely on a simple thin client mobile app to connect and stream data to the screen of the secure

virtual smartphone. With this virtual mobile infrastructure, organizations can enable mobile access while keeping all sensitive data and apps safe in a secure datacenter.

BENEFITS

This approach enables:

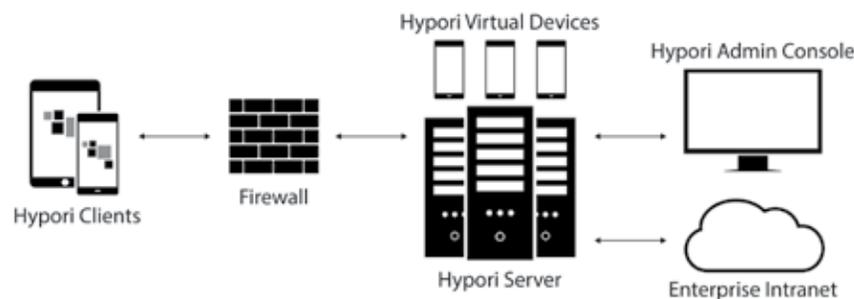
- A zero data-at-rest approach to mobile access, where no sensitive information is ever stored on the mobile endpoint
- Complete oversight and management of all virtual mobile devices, enabling much simpler app and data deployment, threat remediation and more
- Increased privacy for the end-user

COMPETITIVE ADVANTAGE

Traditional approaches to secure mobility focus heavily on the mobile device. Unfortunately, there are many ways for attackers to compromise mobile endpoints, which already are highly susceptible to being lost or stolen. Other virtual mobile infrastructure vendors have all chosen to architect their mobile virtualization solutions with one large terminal server, where multiple users can access their own set of mobile apps and data. The competitive advantage of this new approach is in its product architecture, which ensures that there is no data on the physical mobile device and where, in multiple user situations, each user has a dedicated virtual device to protect his or her data separately.

NEXT STEPS

The next step is to deploy the technology at production scale across government agencies.



The Hypori Virtual Mobile Infrastructure Components

SENsor Secure Enterprise Infrastructure

Metronome Software, LLC

Chieu Nguyen

chieu.nguyen@metronome-software.com

OVERVIEW

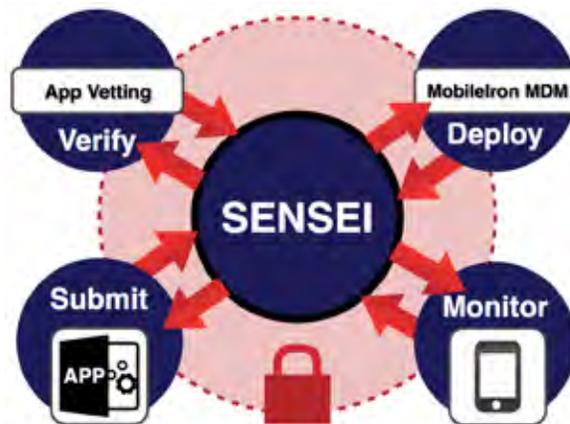
While mobile devices are the predominant consumer product for accessing the internet, internet of things (IoT) devices and sensors are flooding the landscape of essential electronics at home, work and public spaces. They are exposed to the same cyber-threats and are prime targets for adversaries attempting to disrupt sensitive operations or steal proprietary, personal or financial data. Metronome, along with its technology partners, is developing SENSEI, which provides existing systems complete security overlay for mobile, IoT devices and their applications (apps).

CUSTOMER NEED

The government's workforce—including members of the military and first responders—quickly is becoming cyber-enabled with cutting-edge mobile technology and sensors aiding their daily operations. If left unprotected, these devices are at risk to attacks by malicious actors. Malware has multiple attack vectors such as installing a faulty app containing zero-day exploits. This approach introduces a weak point in typically secure communications and operations, leading to compromised systems and even other apps.

APPROACH

Using mobile-device attestation and profiling technology combined with an app vetting and enterprise Mobile Device Management (MDM) software, SENSEI provides an existing system with capabilities and a lifecycle for device monitoring, detecting vulnerable apps prior to installation and taking corrective action should a compromise occur. End-user apps are first uploaded to SENSEI and dynamically scanned for exploitable vulnerabilities. Vetted apps are further security-wrapped by the MDM before deployment; all devices and their wrapped apps are actively monitored and managed. Furthermore, mobile devices can be configured to perform scheduled device health testing, yielding usage metrics gathered by SENSEI for evaluation.



SENSEI Secure Lifecycle Diagram (Submission, App Vetting, MDM, Monitoring).

BENEFITS

Using SENSEI integrated with an MDM to protect cloud-based infrastructures from backend to mobile endpoints (e.g., smartphones, IoT, hubs and sensors) gives existing systems the assurance that their operators have equipment resilient against malware. With this added security, the danger of system components going dark, data being compromised and lost communications is greatly reduced. Additionally, SENSEI provides a policy-based infrastructure that enables the government to enforce interaction and data management policies between cooperating organizations at many levels.

COMPETITIVE ADVANTAGE

SENSEI leverages enterprise-level MDM technology that is FEDRamp-ready, currently being evaluated for use by the Defense Information Systems Agency and already being used by large companies worldwide. With this approach, SENSEI provides a certified, well-supported product experience for government end-users and system administrators.

NEXT STEPS

The performer will conduct pilot testing with the DHS S&T Next-Generation First Responders Apex program to integrate select parts of its mobile software systems with SENSEI and evaluate the impact it has on system security and overall performance.

Persistent Implant Finder

Red Balloon Security, Inc.

Nathaniel Boggs

nathaniel@redballoonsecurity.com

OVERVIEW

Mobile device firmware typically is treated as a black box with organizations having little to no visibility into the code running on their devices. This code can contain malicious implants added in the supply chain. To find malware embedded in firmware, a Persistent Implant Finder is being developed. The Persistent Implant Finder will leverage Firmware Reverse Analysis Konsole (FRAK), Red Balloon Security's proprietary firmware manipulation framework that automates the unpacking, modification, analysis and repacking of firmware to create new FRAK analyzer modules capable of identifying a variety of implants providing detailed reports for further human analyst investigation.

CUSTOMER NEED

Currently, customers have limited visibility into the firmware running on their devices. Modern supply chains have numerous suppliers for a single device, any one of which could be malicious or compromised and lead to malicious implants being injected into the firmware. Without visibility into the firmware, customers have little idea of the true security posture of their devices.

APPROACH

The Persistent Implant Finder will have a modular design integrated for use with FRAK analyzers. Both device-family-specific analyzers and generic analyzers will be created. The process of unpacking firmware sufficiently to be analyzed will be performed by FRAK using either existing unpackers for known device firmware formats or with new FRAK unpackers created for the device family to be analyzed. These FRAK analyzers will search for a variety of implants such as password backdoors, active malware rootkits and network service backdoors.

BENEFITS

The finder will provide organizations the tools needed to gain visibility into the firmware that their devices run. This visibility will specifically be used to discover suspicious code or data in the firmware images that may be malicious implants and improve security of mobile devices.



FRAK with proposed new Persistent Implant Finder modules to assist in discovering firmware backdoors and malware implants.

COMPETITIVE ADVANTAGE

The performer will leverage expertise in firmware manipulation and FRAK, an automated firmware unpacking, analyzing, modifying and repacking framework. FRAK will allow the finder to scale quickly both in terms of analyzing more device families and in terms of creating new analyzers to find more types of implants.

NEXT STEPS

After the Persistent Implant Finder proves its capability to find malicious implants, the next step is to integrate and scale it into a comprehensive firmware analysis tool capable of generating detailed reports to present the security posture of any firmware image.

Prepositioned Cyber-Threats

University of Illinois

Michael Bailey
mdbailey@illinois.edu



OVERVIEW

The DHS S&T Critical Infrastructure Resilience Institute (CIRI), led by the University of Illinois, and Kryptowire have partnered to research and develop an automated system for the detection of prepositioned cyber-threats in mobile applications, internet of things (IoT), embedded systems and critical infrastructure technologies.

CUSTOMER NEED

Consumers, enterprises and government agencies must be able to independently and automatically detect prepositioned cyber-threats in mobile and IoT devices to prevent the loss of confidential information and protect against cyber and physical attacks. As new software and firmware is continuously introduced into the marketplace and automatically updated over the air (OTA), poor programming, intentional backdoors and security vulnerabilities have been inserted into consumer, enterprise and critical infrastructure mobile and IoT devices. Researchers have discovered data exfiltration and undisclosed back doors that can enable adversaries to collect data and surveil individuals and IoT devices.

APPROACH

This effort will develop a comprehensive framework that enables analysts to automatically determine possible threat vectors stemming from prepositioned threats. This framework will cover the collection of personally identifiable information, software backdoors, inconsistent validation checks, ineffective security checks, and debug modes for mobile operating systems. The threat vectors will be codified into the prototype that will automatically apply

concolic and forced-path execution analyses to determine the existence of a threat. The effort will scale to thousands of firmware images and cover as many vendors and firmware versions as possible.

BENEFITS

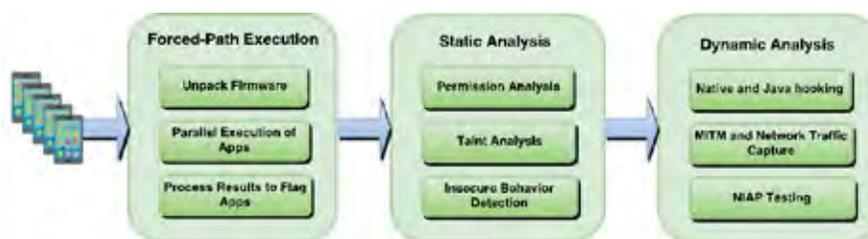
This approach is suitable for whole-firmware testing and standalone apps. The scalable, forced-path execution examines behavior without requiring a device and flagged apps and firmware are processed on an instrumented device for further analysis.

COMPETITIVE ADVANTAGE

Monitoring the mobile and IoT marketplace using arduous and non-repeatable manual reverse engineering, vulnerability assessment and penetration techniques is simply not scalable or even feasible in many devices due to the complexity and size of their code. Moreover, device firmware images can be on the order of 2GB, software is updated rapidly OTA, adversaries continue to improve their techniques by employing obfuscation and anti-reversing defenses, and devices use root detection and integrity checks. The proposed approach will automate the analysis and discovery of prepositioned threats.

NEXT STEPS

The next steps are to identify examples of prepositioned cyber-threats and develop methods for automated testing and protection technologies for incorporation into mobile, IoT and embedded systems. Then a prototype to implement the framework will be created.



Prepositioned Cyber-Threat Analysis Prototype.



MOBILE SECURITY GUIDANCE

Table of Mobile Security Guidance

There is a large and growing number of informational and guidance resources and best practices available to mobile enterprise managers to help them learn about and implement the latest security safeguards and attain the highest current state of security for their mobile ecosystem. But where can a busy mobile enterprise manager learn about all these informative resources in one place?

A great starting point is the following Table of Mobile Security Guidance compiled by the S&T Mobile Security R&D program. It is a one-stop, comprehensive reference tool you can use to conduct research of the latest developments in mobile security, identify potential upgrade matches, learn more about the new solutions and launch in-depth vetting of each applicable security solution.

If you learn of a new mobile security informational or guidance resource or best practice, please share it with us at SandT-Cyber-Liaison@hq.dhs.gov so we can add it to the guidance document.

DOCUMENT	AUTHOR	SYNOPSIS	AUDIENCE
Study on Mobile Device Security	DHS, NIST, and Interagency Working Group	This report to Congress describes threats and vulnerabilities across the mobile ecosystem, identifies mitigations to defend against the threats as well as gaps in defenses, and provides recommendations to close the gaps. The recommendations include standards, best practices, need for policy changes, gaps in DHS authorities, and the need for continued and new R&D to address the threats.	CIOs, Chief Information Security Officers (CISOs), system owners, senior managers, system engineers, system architects, cybersecurity professionals, government users, and consumers.
Navigating the Future of Mobile Services Report to American Technology Council & Federal CIO Council	MSCT, Advanced Technology Academic Research Center (ATARC)	A compilation of 12 mobile documents spanning a diverse set of topics, including mobile application vetting, enterprise mobility management, mobile identity management, mobile device-as-a-service, mobile threat protection, mobile backend-as-a-service, and mobile strategy development. Developed as a collaborative effort between government and private industry representing 75 agencies, bureaus and companies.	CIOs, CISOs, system owners, senior managers, system engineers, system architects, cybersecurity professionals
Mobility Program Guidance			
Mobile Computing Decision Framework (MCDF)	MTTT	The MCDF provides a holistic decision-making process that assists organizations in determining which mobile solution, if any, will support their missions.	CIOs, CISOs, system owners, senior managers, system engineers, system architects, cybersecurity professionals

DOCUMENT	AUTHOR	SYNOPSIS	AUDIENCE
Federal Mobile Computing Security Baseline	DHS, Department of Defense (DoD), NIST	The Federal Mobile Computing Security Baseline contains the moderate baseline for the most common federal mobility use case: federal employees operating agency-controlled mobile devices to access moderate impact systems on a Federal network. It includes the core controls for mobile device management (MDM) and mobile application management, as well as notional controls for identity and access management and data management.	CIOs, CISOs, system owners, senior managers, system engineers, system architects, cybersecurity professionals
Mobile Security Reference Architecture (MSRA)	DHS, DoD, NIST	The MSRA is a flexible architecture designed to be adapted to fit the needs of any department or agency. Readers of the MSRA document should understand the role of each component in an architecture and the associated controls and management functions. This knowledge will enable a department or agency IT architect to design a “best fit” solution for their enterprise and provide a solid set of security principles and controls to secure that solution.	CIOs, CISOs, system owners, senior managers, system engineers, system architects, cybersecurity professionals
NIST Interagency Report (NISTIR) 8144: Assessing Threats to Mobile Devices & Infrastructure Draft	NIST	This document outlines a catalogue of threats to mobile devices and associated mobile infrastructure to support development and implementation of mobile security capabilities, best practices, and security solutions to better protect enterprise IT.	CIOs, CISOs, senior managers, system engineers, system architects, cybersecurity professionals
Security Guidance for Critical Areas of Mobile Computing—Mobile Working Group	Cloud Security Alliance	This document discusses the top threats to mobile security and organizational maturity in mobile computing and provides best practice recommendations in the areas of bring your own device, Mobile Authentication, App Store Security, and MDM.	CIOs, CISOs, senior managers, system engineers, system architects, cybersecurity professionals
HiMSS— Mobile Security Toolkit	Healthcare Information and Management Systems Society (HiMSS)	This toolkit provides health care organizations resources to control and secure their mobile computing and storage devices as a part of their overall mobile security program.	CIOs, CISOs, senior managers, system engineers, system architects, cybersecurity professionals
Privacy Policy for DHS Mobile Applications, Instruction O47-01-003	DHS	This policy provides baseline privacy requirements for DHS mobile applications. Additional privacy protections may be necessary depending on the purpose and capabilities of each individual mobile application.	Privacy Officers, CIOs, CISOs, senior managers, system engineers, system architects, cybersecurity professionals

DOCUMENT	AUTHOR	SYNOPSIS	AUDIENCE
Mobile Enterprise Best Practices Guidance			
NIST Special Publication (SP) 1800-4 Practice Guide: Mobile Device Security	NIST National Cybersecurity Center of Excellence (NCCoE)	This document proposes a reference design on how to architect enterprise-class protection for mobile devices accessing corporate resources. The example solutions presented can be used by any organization implementing an EMM solution on premise or in the cloud.	Executives, cybersecurity managers, cybersecurity professionals, engineers, administrators
NIST SP 800-124r1: Guidelines for Managing the Security of Mobile Devices in the Enterprise	NIST	This publication helps organizations centrally manage the security of mobile devices. It provides recommendations for selecting, implementing, and using centralized management technologies, and explains the security concerns inherent in mobile device use and provides recommendations for securing mobile devices throughout their lifecycles.	Executives, cybersecurity managers, cybersecurity professionals, engineers, administrators
Commercial Solutions for Classified Mobile Access Capability Package	National Security Agency (NSA)	This document discusses the top threats to mobile security and organizational maturity in mobile computing and provides best practice recommendations in the areas of bring your own device, Mobile Authentication, App Store Security, and MDM.	CIOs, CISOs, senior managers, system engineers, system architects, cybersecurity professionals
Mobile Device Best Practices Guidance			
NIST SP 800-164 (Draft): Guidelines on Hardware-Rooted Security in Mobile Devices	NIST	This document provides a common baseline of security technologies that can be leveraged across multiple device types to provide device integrity, isolation and protected storage through the use of hardware-based roots of trust.	OS vendors, device manufacturers, security software vendors, carriers, application software developers, cybersecurity professionals
NIST SP 800-88 Rev. 1: Guidelines for Media Sanitization	NIST	This document provides media sanitization guidelines for mobile devices based on type and intended disposition.	System owners, property managers, legal, privacy, IT professionals, cybersecurity professionals, device users
NISTIR 7981 (Draft) Mobile, PIV (Personal Identity Verification), and Authentication	NIST	This document analyzes various current and near-term options for remote electronic authentication from mobile devices that leverage both the investment in the PIV and PIV-I infrastructures and the unique security capabilities of mobile devices.	IT professionals, cybersecurity professionals, system architects

DOCUMENT	AUTHOR	SYNOPSIS	AUDIENCE
NIST SP 800-121 Rev1 Guide to Bluetooth Security	NIST	This publication provides information on the security capabilities of Bluetooth technologies and offers recommendations to organizations employing Bluetooth technologies for securing them effectively.	CIOs, CISOs, senior managers, system engineers, system architects, auditors, cybersecurity professionals, researchers, analysts
Mobile Device Security a Comparison of Platforms	Gartner	This assessment aids security professionals by comparing and analyzing the security controls of the most popular mobile device operating systems.	CIOs, CISOs, senior managers, system engineers, system architects, cybersecurity professionals
Mobile Device Best Practices Guidance			
NIST SP 800-163: Vetting the Security of Mobile Applications	NIST	This document defines the app vetting process. App vetting comprises two main activities: app testing and app approval/rejection. The app testing activity involves testing an app for software vulnerabilities using services, tools, and humans to derive vulnerability reports and risk assessments. The app approval/rejection activity involves the evaluation of these reports and risk assessments along with additional criteria to determine the app's conformance with organizational security requirements and ultimately the approval or rejection of the app for deployment on the organization's mobile devices.	CIOs, CISOs, senior managers, system engineers, system architects, cybersecurity professionals, mobile application developers, mobile application testers
NISTIR 8136: An Overview of Mobile Application Vetting Services for Public Safety	NIST	This document is a high-level investigation of app vetting services with the goal of enumerating the traits they exhibit that may be useful to public safety.	CIOs, CISOs, senior managers, system engineers, system architects, cybersecurity professionals, app developers, app testers
Mobile Application Single Sign-On for Public Safety and First Responders	NIST NCCoE	The vast diversity of public safety personnel, missions, and operational environments magnifies the need for a nimble authentication solution for public safety. This project will explore various multifactor authenticators currently in use or potentially offered in the future by the public safety community as their next-generation networks are brought online. The effort will not only build an interoperable solution that can accept various authenticators to speed access to online systems while maintaining an appropriate amount of security, but the project also will focus on delivering single sign-on (SSO) capabilities to both native and web-/browser-based apps.	CIOs, CISOs, System owners, senior managers, system engineers, system architects, cybersecurity professionals, app developers

DOCUMENT	AUTHOR	SYNOPSIS	AUDIENCE
Open Web Application Security Project (OWASP) - Mobile Security Project	OWASP	The OWASP Mobile Security Project is a centralized resource intended to give developers and security teams the resources necessary to build and maintain secure mobile applications. Through the project, the goal is to classify mobile security risks and provide developmental controls to reduce their impact or likelihood of exploitation.	CIOs, CISOs, system owners, senior managers, system engineers, system architects, cybersecurity professionals, app developers, app testers
Cloud Security Alliance (CSA) Mobile Application Security Testing Initiative	Cloud Security Alliance	This initiative seeks to create a more secure cloud computing ecosystem that focuses on addressing endpoint security issues on mobile applications. It establishes secure engineering approaches to application architecture, design, testing and vetting.	CIOs, CISOs, system owners, senior managers, system engineers, system architects, cybersecurity professionals, app developers, app testers
Cellular Networks Guidance			
NIST SP 800-187 Guide to LTE (Long Term Evolution) Security	NIST	This document serves as a guide to the fundamentals of how LTE networks operate and explores the LTE security architecture. It also provides an analysis of the threats posed to LTE networks and supporting mitigations.	Telecommunications engineers, system administrators, cybersecurity professionals, security researchers
Signaling System 7 (SS7) Interconnect Security Monitoring Guidelines (Global System for Mobile Association (GSMA) FS.11)	GSMA	This document serves as a guide for MNOs on current mitigations for SS7/Diameter threats specifically related to interconnection fraud.	Telecommunications engineers, system administrators, cybersecurity professionals, security researchers
Mobile Application Standards			
NIAP Protection Profile for Application Software	NIAP	This assurance standard specifies information security functionality requirements for application software, including mobile applications. This standard specifies requirements to ensure that applications correctly implement security functionality and conform to norms of application behavior.	CIOs, CISOs, senior managers, system engineers, system architects, cybersecurity professionals
Requirements for Vetting Mobile Apps from the Protection Profile for Application Software	NIAP	This document presents functional and assurance requirements found in the Protection Profile for Application Software which are appropriate for vetting mobile application software outside formal Common Criteria evaluations.	CIOs, CISOs, senior managers, system engineers, system architects, cybersecurity professionals

DOCUMENT	AUTHOR	SYNOPSIS	AUDIENCE
Mobile Device Technology Stack and Device Physical Access Standards			
NIAP Protection Profile for Mobile Device Fundamentals	NIAP	This assurance standard specifies information security requirements for mobile devices for use in an enterprise. A mobile device in the context of this assurance standard is a device that is composed of a hardware platform and its system software. The mobile device provides essential services such as cryptographic services, data-at-rest protection, and key storage services to support the secure operation of applications on the device. Additional security features such as security policy enforcement, application mandatory access control, anti-exploitation features, user authentication, and software integrity protection are implemented to address threats.	CIOs, CISOs, senior managers, system engineers, system architects, cybersecurity professionals
Global Platform Specification for Trusted Execution Environment/ Global Platform Specification for Secure Element Management	GlobalPlatform	GlobalPlatform identifies, develops and publishes technical specifications and market configurations that facilitate the secure and interoperable deployment and management of multiple-embedded applications on secure chip technology. Its proven technology is regarded as the international industry standard for building a trusted end-to-end solution that serves multiple users and supports several business models.	Product vendors, original equipment manufacturers (OEM), testers
Trusted Computing Group Specifications for Trusted Platform Module	Trusted Computing Group	Trusted Platform Module (TPM) is an international standard for a secure crypto-processor, which is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.	OEM, mobile network operators, mobile service providers
Mobile Enterprise Standards			
NIAP Protection Profile for Mobile Device Management	NIAP	MDM products allow enterprises to apply security policies to mobile devices such as smartphones and tablets. The purpose of these policies is to establish a security posture adequate to permit mobile devices to process enterprise data and connect to enterprise network resources. This protection profile specifies baseline requirements for MDM systems.	CIOs, CISOs, senior managers, system engineers, system architects, cybersecurity professionals
NIAP Protection Profile - Extended Package for Mobile Device Management Agents	NIAP	This extended package describes baseline security requirements for MDM agents. An MDM agent is the mobile device-resident component of an MDM product.	CIOs, CISOs, senior managers, system engineers, system architects, cybersecurity professionals



ACRONYM	DEFINITION
ATARC	Advanced Technology Academic Research Center
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSA	Cloud Security Alliance
DoD	Department of Defense
GSMA	Global System for Mobile Association
HiMSS	Healthcare Information and Management Systems Society
IT	Information Technology
LTE	Long Term Evolution
MCDF	Mobile Computing Decision Framework
MDM	Mobile Device Management
MSCT	Mobile Services Category Team
MSRA	Mobile Security Reference Architecture
MTTT	Mobile Technology Tiger Team
NCCoE	National Cybersecurity Center of Excellence
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NSA	National Security Agency
OEM	Original Equipment Manufacturer
OWASP	Open Web Application Security Project
PIV	Personal Identity Verification
SP	Special Publication
SS7	Signaling System 7
TPM	Trusted Platform Module



CONCLUSION

Conclusion

Mobile technologies evolve rapidly to meet increasing consumer demand and maintain competitive edge. The high adoption of mobile devices, apps and services by consumers and government has made the technologies a new target for attackers, who take advantage of this rapid pace of change to identify vulnerabilities or introduce malware into the ecosystem. The Mobile Security R&D program was established to address the technical, operational and policy challenges that inhibit the government's adoption of secure mobile technologies. Since its inception, the program has had significant impact across the Federal government and has successfully demonstrated and transitioned new technologies and capabilities for government use.

MOBILE SECURITY R&D PROGRAM SUCCESSES:

- **Delivery of the Study on Mobile Device Security report to Congress in May 2017. In addition to bringing Congress's attention to the threats and vulnerabilities of mobile technologies, the report's recommendations already are impacting government policy and programs.**
- **Kryptowire's mobile application ("app") vetting technology has transitioned from research and development (R&D) to commercialization.**
- **Bluetooth access control is part of Hypori's Virtual Mobile Infrastructure product by Intelligent Waves, LLC.**
- **Inclusion of 12 mobile-specific metrics in the Fiscal Year 2018 CIO Federal Information Security Modernization Act metrics.**
- **Collaboration with the National Institute of Standards and Technology (NIST) to update relevant special publications (SP) to reflect changes in technologies, technical capabilities and policy (e.g., NIST SP 800-124 revision 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise, and NIST SP 800-163: Vetting the Security of Mobile Applications).**
- **DHS and its partners jointly published a whitepaper, "Securing Mobile Applications for First Responders", following a successful mobile app vetting pilot project with the Association of Public Safety Communications Officials.**

The program's initial investment in Mobile Security R&D—automated app security vetting technology that examines mobile apps against government standards—has been successfully piloted and transitioned to the marketplace. The goal for this project was to accelerate adoption of secure mobile applications into missions with increased efficiency and reduced cost through development and fielding of a consistent, repeatable, standards-based approach to vetting mobile apps. Presently, the Kryptowire app vetting technology is available for purchase by departments and agencies on General Service Administration (GSA) IT Schedule 70.

The success of the Mobile Application Security project app vetting technology would not have been possible without the active participation of dedicated federal customers and stakeholders, who provided requirements and guidance for all Mobile Security R&D program projects and then piloted and adopted the technology in their environments. We extend our appreciation and thanks to these customers and look forward to their continued engagement in Mobile Security R&D projects.

- Defense Information Systems Agency
- Department of Defense
- Department of Justice
- DHS Customs and Border Protection
- DHS Federal Emergency Management Agency
- DHS Headquarters
- DHS Transportation Security Administration
- Federal CIO Council
- General Services Administration
- Library of Congress
- National Information Assurance Partnership
- National Institute of Standards and Technology
- U.S. Army



Conclusion

Through customer partnerships, cross-agency collaborations and coordination with federal mobile working groups, and the contributions of the industry and academic research community, the program has met its goals for new/enhanced approaches for mobile device security and standards-based security vetting of mobile apps. Mobile Security R&D investments will help spur development/enhancement of technologies and approaches for mobile security and influence further development of government and industry standards and policy.

Current program R&D projects seek to further improve the security of mobile applications to meet the goals of integrated security throughout the mobile application lifecycle, enhanced information-sharing on attributes of mobile application security (malware and vulnerabilities), and continuous monitoring of mobile applications and app behavior to detect security vulnerabilities and anomalies and enable remediation actions. Successful accomplishment of ongoing Mobile Device Security projects will provide alternative methods to secure government data through virtualization and improve understanding of firmware security—impacting government supply-chain risk-management policies and practices. Future activities will expand R&D to improve the security of the mobile network infrastructure that is fundamental to communications and delivery of information and services.

We encourage investors, researchers and potential partners from DHS, other government departments and agencies, industry, and academia to reach out to learn more, explore the current Mobile Security R&D program and discover how they might benefit from or participate in the program's R&D efforts. For additional inquiries or to learn more please contact:

Vincent Sritapan

Mobile Security R&D Program Manager

Vincent.Sritapan@hq.dhs.gov

Notes





ONLINE

www.dhs.gov/cyber-research



FACEBOOK

Facebook.com/dhsscitech



EMAIL

SandT-Cyber-Liaison@hq.dhs.gov



YOUTUBE

www.youtube.com/dhsscitech



TWITTER

[@dhsscitech](https://twitter.com/dhsscitech)



Periscope

[@dhsscitech](https://periscope.tv/@dhsscitech)



LINKEDIN

www.linkedin.com/company/dhsscitech