



Mobile Security R&D Program Guide

Volume 1



**Homeland
Security**

Science and Technology

This page intentionally left blank.

Welcome

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 guide introduces you to the goals and objectives for Mobile Security R&D, its alignment with DHS and federal mobile security strategies and priorities, and provides a view into S&T's exploration of new and cutting edge mobile security R&D. We are excited to share these promising mobile security technologies with you and welcome your feedback.

Through targeted mobile security R&D, S&T seeks to accelerate the adoption of secure mobile technologies by government and industry to address mobile cybersecurity needs and protect the Homeland Security Enterprise. This guide represents the important contributions of the Mobile Device Security (MDS) Program in achieving the Digital Government Strategy goal of "Building a 21st Century Platform to Better Serve the American People." Mobile security R&D is intended to address security gaps and barriers and accelerate the adoption of secure mobile technologies into the federal government. The MDS Program goals are to apply R&D to:

- Enable a secure mobile workforce
- Enable mission success through effective and efficient technologies

This technology guide, which will be updated and published annually, features 13 new technologies. To help direct future publications, please reflect on the mobile security capability gaps in your own organization, and share your thoughts with the DHS S&T MDS Program Manager ([email Vincent Sritapan](#)). Your input is critical to identify timely solutions and to inform future research efforts. It is our pleasure to introduce you to the MDS program and these newly developed mobile security tools resulting from government funding.

Sincerely,



Douglas Maughan
DHS S&T Cyber Security Division
Director



Vincent Sritapan
DHS S&T - Cyber Security Division
MDS Program Manager

MOBILE SECURITY

Contents

CYBER SECURITY DIVISION	1
MOBILE DEVICE SECURITY (MDS) PROGRAM STRATEGY	4
SOFTWARE BASED MOBILE ROOTS OF TRUST	9
<hr/>	
BLUE RISC	11
<hr/>	
GALOIS	13
<hr/>	
DEF-LOGIX	15
MOBILE INSTRUMENTATION	16
<hr/>	
HRL LABORATORIES	17
<hr/>	
KRYPTOWIRE	19
<hr/>	
NORTHROP GRUMMAN	21
<hr/>	
UNITED TECHNOLOGIES RESEARCH CENTER	25
TRANSACTIONAL SECURITY METHODS	27
<hr/>	
RUTGERS UNIVERSITY	28
NEXT-GEN MOBILE SECURITY MANAGEMENT TOOLS	30
<hr/>	
IBM	31
<hr/>	
UNIVERSITY OF NORTH CAROLINA AT CHARLOTTE	32
MOBILE DEVICE LAYER PROTECTION	34
<hr/>	
INTELLIGENT AUTOMATION INC.	35
MOBILE APP SECURITY	37
<hr/>	
KRYPTOWIRE LLC	39
CONCLUSION	41

Department of Homeland Security Science and Technology Directorate Cyber Security Division

The Cyber Security Division is a Key Component in the President's National Strategy

Threats on the Internet change fast and 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.

In the Department of Homeland Security (DHS) Science & Technology Directorate (S&T), the CSD enables and supports research, development, testing, evaluation, and transition for advanced technologies in cybersecurity and information assurance. This full lifecycle of activities evolved in response to the President's National Strategy to Secure Cyberspace and the Comprehensive National Cybersecurity Initiative (CNCI).



The CNCI establishes a multi-pronged approach the Federal government will take in identifying current and emerging cyber threats, shoring up current and future vulnerabilities in telecommunications and cyberspace, and responding to or proactively stopping entities that wish to steal or manipulate protected data on secure Federal systems.

The S&T Cyber Security Division addresses these objectives by:

- Discovering new solutions for emerging cybersecurity threats to the nation's critical infrastructure;
- Driving security improvements to close critical weaknesses in today's technologies and emerging systems; and
- Delivering new, tested technologies to defend against cybersecurity threats and making them available to all sectors through technology transfer and other methods.

CSD Focuses on Critical Vulnerabilities in the Cyber Security Landscape

Internet Infrastructure Security—Developing security protocols for the existing Internet infrastructure (browsers and routers, essential to daily Internet operation) so that users are not redirected to unsafe websites or pathways by malicious actors.

Critical Infrastructure/Key Resources—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.

National Research Infrastructure—Providing the infrastructure that enables development and testing of technologies to address cybersecurity issues including botnets, worm propagation and defense, and denial-of-service defenses that protect Internet websites against attack; providing a data repository to support the cybersecurity research community.

Leap-Ahead Technologies—Develop "leap-ahead" technologies that will achieve orders-of-magnitude improvements in cybersecurity. One of CNCI's goals is to achieve a reliable, resilient, and trustworthy digital infrastructure.



Our vision is a cyberspace that supports a secure and resilient infrastructure, that enables innovation and prosperity, and that protects privacy and other civil liberties by design. It is one in which we can use cyberspace with confidence to advance our economic interests and maintain national security under all conditions.

— Quadrennial Homeland Security Review, 2010

Cyber Security Education—Helping to foster adequate training and education programs critical to the nation’s cybersecurity needs by providing opportunities for high school and college students to develop their skills and by giving them access to advanced education and exercises through team competitions.

Identity Management—Evaluating and developing proof-of-concept solutions, and conducting pilot experiments of identity and access control architectures and technologies, as well as data privacy protection technologies for the homeland security community.

Cyber Forensics—Developing new cyber forensic analysis tools and investigative techniques to help law enforcement officers and forensic examiners address cyber-related crimes.

Software Assurance—Developing tools, techniques, and environments to analyze software, address the presence of internal flaws and vulnerabilities in software, and improve software security associated with critical infrastructure (energy, transportation, telecommunications, banking and finance, and other sectors).

S&T: Preparing for Next-Generation Cyber Threats

In the coming years, several cybersecurity challenges must be addressed. The most critical of these include Enterprise-Level Metrics, Combating Insider Threats, Combating Malware and Botnets, Digital Provenance, Situational Understanding and Attack Attribution, and Usable Security.





Mobile Device Security (MDS) Program Strategy

Mobile Device Security Program Strategy

Vision

The Department of Homeland Security (DHS) workforce has become increasingly mobile, driving the need for secure mobility solutions and a coordinated approach and framework to guide the selection and implementation of common enterprise mobility solutions. To promote the safe and secure adoption of mobile technology in DHS and the federal government, the DHS Science and Technology Directorate (S&T) Cyber Security Division (CSD) within the Homeland Security Advanced Research Project Agency (HSARPA) created the Mobile Device Security (MDS) Program, and adopted the following vision to guide its research efforts:

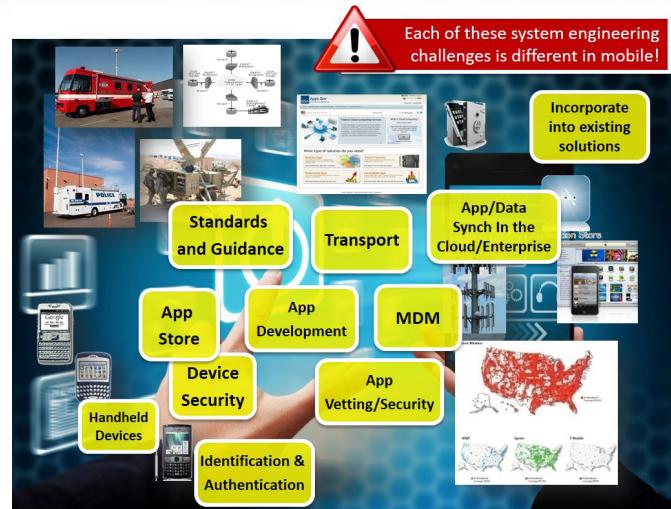
MOBILE DEVICE SECURITY PROGRAM VISION

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

Context

Mobile Technology, recognized as a cornerstone of the 2012 White House Federal Digital Government Strategy (DGS), seeks to enable “access to quality digital government information and services anywhere, anytime, on any device.” The DGS acknowledges new and unique security and privacy challenges must be met to accelerate the adoption of mobile technology into the federal government. In addressing DGS challenges, interagency efforts resulted in development of security requirements for mobile computing and identification of major barriers and gaps that impede mobile adoption. The mobile challenge areas identified were Mobile Device Management, Mobile Application Management, Identity and Access Management, and Data Protection. Though progress has been made in these areas, more needs to be done to address current and especially emerging challenges.

Two factors conspire to create the urgent need for secure enterprise solutions. First, the use of mobile solutions is rapidly increasing across the Department and the federal government. Secondly, mobile threats present an increasingly common and more sophisticated threat to data stored or processed on DHS devices. Threats to mobile devices, applications, and data have grown dramatically in the past few years. A recent analysis of threats¹ highlighted several key developments, including the following.



Elements of a Mature Mobile Ecosystem

- Malware grew substantially in the U.S., driven by an increase in threats holding devices and data hostage in exchange for payment (ransomware).
- Mobile threat sophistication is increasing. Certain malware has even entered the marketplace pre-installed on certain devices, indicating a compromised supply chain. Malware self-defense mechanisms are also gaining sophistication, evading attempts to detect and defeat the application.
- A mature mobile ecosystem comprises many elements, as shown below. Each of these areas presents security challenges and opportunities for additional study and mobile security research and development (R&D).

Objectives

To respond to the evolving threats and security challenges in the mobile space, S&T CSD has developed and will transition programs directed at several strategic objectives and initiatives. Through this work, S&T will ensure DHS is poised to bridge current capability gaps and deploy solutions that effectively, efficiently, and securely enable the mission of the Department. The MDS Program has established three overarching objectives as it seeks to achieve the program vision:

MOBILE DEVICE SECURITY PROGRAM OBJECTIVES

- 1: Partner with DHS Components and federal stakeholders to identify operational requirements and capability gaps
 - 2: Develop secure mobile solutions to enhance the DHS mission
 - 3: Partner with industry to foster innovation
-

Strategic Alignment

The objectives and initiatives of the MDS Program align with DHS, S&T, and federal strategies and priorities. The

DHS S&T 2015-2019 Strategic Plan addresses the goals and objectives necessary to deliver effective and innovative insight, methods, and solutions for the critical needs of the Homeland Security Enterprise (HSE). The plan's three strategic objectives were specifically designed to address the environment the Government operates within today, and MDS Program goals directly align with Objectives 1 and 2. These objectives and their respective initiatives are:

1. Deliver Force Multiplying Solutions:

- Identify and prioritize operational requirements and capability gaps
- Make strategic investments in high-impact, priority areas
- Partner with the HSE

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

The Program also directly aligns with two key goals and objectives of the **DHS Information Technology Strategic Plan²**:

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.

Mobile technology by its nature allows the end user access to data that might not otherwise be available. Ensuring access to data and services 'anywhere, anytime' is one aspect of the targeted mobile security R&D and aligns specifically with Objective 2.4. Mobile security R&D is heavily focused on ensuring secure delivery of data and/or services, consistent with Objective 4.2.

The Office of Management and Budget's Cybersecurity Strategy and Implementation Plan (CSIP) also addresses the need for mobile security as an imperative. This document notes that "Mobile devices have become as powerful and connected as desktop and laptop computers, requiring the same level of attention to cybersecurity. Mobile security has unique challenges that require different solutions than existing programs offer. [Potential solutions]... could address authentication, application management, device management, and encryption, and may include approved tools, best practices, and implementation support."

Finally, it should be noted that the MDS Program is directly aligned to the requirements of DHS components and missions elicited through multiple sources, as noted below.

Initiatives to Address Objectives

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

To achieve Objective 1, the MDS Program leverages the efforts of existing federal and DHS mobility working groups to gather and prioritize mobile security capability gaps preventing mobile implementations both at the federal level and across the HSE. These groups include the following federal and DHS working groups:

Federal Interagency Working Groups

- Federal Chief Information Officers (CIO) Council's Information Security and Identity Management Committee (ISIMC) Mobile Technology Tiger Team (MTTT)
- ISIMC Identity, Credential and Access Management Sub-Committee (ICAMSC)
- MTTT Mobile Application Security Vetting Working Group

DHS Mobility Working Groups

- Common Enterprise Mobility Tiger Team
- Mobility Initiative-5 (mi-5)
- Mobile Community of Practice

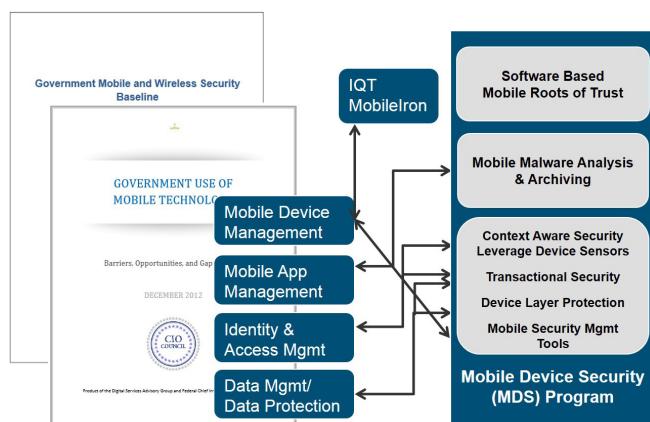
OBJECTIVE 2: Develop Secure Mobile Solutions to Enhance the DHS Mission

Collectively, these groups have identified gaps in current policy or technologies that inhibit the adoption of secure mobile solutions. From these issues, CSD has prioritized several that are appropriate targets for Mobile Security R&D, including:

- Mobile device management
- Device interface management
- Trust implementation for executables and access
- Application management and version control
- Malware and mobile app security vetting
- Identity management and authentication
- Data privacy
- OS fragmentation

The MDS Program has established several initiatives to address the primary gaps identified through its partnerships with DHS Components and other federal agencies. These efforts identified needs for secure mobile solutions in four areas:

- Mobile device management
- Mobile app management
- Identity and access management
- Data management/data protection



These areas are interrelated; for example, secure solutions for both mobile device management and mobile app management include data protection and integration with identity and access control solutions.

The MDS projects and initiatives addressing these challenges are related as illustrated above. These initiatives are broadly focused on mobile device security and mobile application security, as described below.

Mobile Device Security

One objective of this effort is to develop tamper-evident modules, or “roots of trust,” that can be continuously measured and verified to produce a chain of cryptographically strong evidence about the state of the device. This serves to verify devices are in a protected state at power-on and continue 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.

A cross-cutting effort under mobile device management seeks to leverage the mobile device’s innate capabilities (e.g., application sandboxing, camera, GPS, etc.) to sense and measure the environment, user interaction, and app interaction to gather contextual information. Situational awareness capabilities that relate contextual attributes, such as application usage, patterns of data access, and geo-location, can be used to ascertain the risk associated with the user, device, app, and network connectivity. This knowledge can be applied to any of the four categories of security management for devices, applications, users, and data to enable the ability to dynamically enforce policies and adapt service access based on threat level associated with the current context. Moreover, these continuous sources of contextual attributes also enable capabilities for behavioral-based user identification and anomaly detection.

Mobile App Security

The MDS Program is developing a framework that employs static, behavioral, and flow-based techniques to continuously vet the security posture of government-developed and commercially developed mobile apps throughout their

lifecycle – from requirements, design, and implementation through deployment, maintenance, and retirement. This capability will go beyond identifying malicious software and be able 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.

The DHS Joint Requirements Council (JRC), a component-led body focused on operational mission areas, is designed to identify, prioritize and recommend investments to address cross-department required capabilities, ensuring unity of effort among the components, and to address the highest priority needs to meet mission requirements. The JRC established the Cybersecurity Portfolio Team in 2014 to identify and develop requirements for the highest priority, cross-department capability needs for cybersecurity. The Cybersecurity Portfolio Team identified new capabilities in Mobile App Security as a high-priority, cross-department need. Future efforts under the mobile app security program seek to promote a standards-based approach (e.g., via linkage to national vulnerability databases), integrate the vetting of mobile applications with federal application stores, and enable active management of applications throughout the lifecycle by integrating the solution with mobile enterprise management solutions.

On the Horizon

OBJECTIVE 3. Partner with Industry to Foster Innovation

In addition to addressing current and emerging mobile security challenges in the four key aspects of the MDS Program (devices, apps, identity, data), additional R&D will be needed to integrate these technologies into a holistic mobile security solution that protects the HSE. Future R&D areas include integration into continuous monitoring and other elements of the network security infrastructure.

Industry partnerships and relationships enable the MDS program to engage and leverage the power of the private sector to bring innovative solutions to the marketplace sooner. The MDS Program has formed valued relationships with academic and industry performers, including the

following, by technical area:

Mobile Roots of Trust R&D

- BlueRISC, Inc., Amherst, MA
- Def-Logix, San Antonio, TX
- Galois, Inc., Portland, OR

Mobile Malware Analysis / Mobile App Archiving R&D

- University of California, Santa Barbara / Vrije Universiteit Amsterdam

- George Mason University / KryptoWire LLC

Broad Agency Announcement: Mobile Technology Security⁴

- Northrop Grumman – Mobile Device Instrumentation
- HRL Laboratories, LLC – Continuous Behavior Based Authentication for Mobile Devices
- Kryptowire LLC – Quo Vadis? A framework for Mobile Device and User Authentication
- United Technologies Research Center – CASTRA: Context-Aware Security Technology for Responsive and Adaptive Protection
- Rutgers University – Dynamic Data Protection via Virtual Micro Security Perimeters
- IBM: Multi-modal Mobile Security Management for User Behavior Anomaly Detection and Risk Estimation
- University of North Carolina at Charlotte – Theseus: A Mobile Security Management Tool for Mitigating Attacks in Mobile Networks
- Intelligent Automation, Inc. – TRUMP: Trusted Monitor and Protection for Mobile Devices

A summary of each performer's R&D technology follows.

References

[1] 2014 Lookout Mobile Threat Report, [Lookout.com Website](#).

[2] Department of Homeland Security Information Technology Strategic Plan, FY2015-2018.

[3] OMB m-16-04, Cybersecurity Strategy and Implementation Plan, [White House Website](#).

[4] See press release at: [Department of Homeland Security Science & Technology News Website](#)

Software Based Mobile Roots of Trust

» SECURITY «



110101 001001 001010

010001 001011 110100 110101 001001 001010 100110 010010 101010

110101 001001 001010 100110 010010 101010 110100 100010 010100

010100 100101 110101 001001 001010 100110 010010 101010 110100 100010 010100

110101 001001 001010 100110 010010 101010 110100 100010 010100
001001 100010 001010

010001 001011 110100 110101 001001 001010 100110 010010 101010 110100 100010 010100



01010



Mobile Roots of Trust: Software-only Roots of Trust for Mobile Devices

BlueRISC

Kristopher Carver – PI
[Email Kristopher Carver](#)

Dr. Andras Moritz – Founder
[Email Dr. Andras Moritz](#)

Jeffry Gummesson – Sr. Security Architect
[Email Jeffry Gummesson](#)

Overview

BlueRISC's MobileRoT measures and verifies a mobile device's static and runtime state to enable trust and overall device security. It can be utilized to detect malicious system change or activity and to ensure that access to critical information and software can only be performed in a trusted state. MobileRoT requires no modifications to the underlying operating system kernel, nor any manufacturer or service provider support for insertion, which greatly reduces hurdles to adoption.

Customer Need

The mobile device market has grown tremendously. Individuals, businesses, and governments rely on mobile devices to access critical infrastructure and share vital information (e.g. banking, medical, intellectual property, etc.). This growth in adoption has also brought about a parallel surge in attacks. Malware, ransomware and spyware are targeting mobile platforms to steal sensitive data, access private networks, track users and do other nefarious activities. Particularly for governments using mobile technology, mobile attacks can disrupt life-saving operations, endanger personnel and expose government systems to exploitation.

Roots-of-Trust (RoTs), which are highly trustworthy tamper-evident components, can provide a foundation to build security and trust. RoTs are usually provided as a specialized hardware chip (e.g., Trusted Platform Module) on desktop or laptop systems. However, mobile devices lack dedicated hardware mechanisms for providing RoTs. This leaves a single solution, namely to provide RoTs via software. Unfortunately, this is challenging to realize given the sophistication of current threats and the ease in which a mobile device's state and information can be extracted and altered. Moreover security specifications such as Trusted Computing Group's Mobile Trusted Module do not address how to support mobile RoTs in software nor do they address dynamic verification of device and software behavior while applications are running.

Our Approach

To overcome the array of surface attacks designed against software-based systems, MobileRoT utilizes a new architecture for enabling transitive trust based on a Core Root of Trust for Measurement (CRTM). The CRTM is hardened code that acts as the root-of-trust for reliable integrity measurements and is the foundation for additional trusted services. The MobileRoT architecture includes a layer of encrypted CRTM code that is tied to a cryptographic key that is generated at boot-time. With the CRTM established, the resulting system does not require any sensitive information to be stored persistently in an unprotected state, closely mimicking the level of security achievable via a dedicated hardware. A secure cryptographic sealing and unsealing procedure tied to the boot-time and runtime measurements performed by the solution enables application and data protection. Since all protected data and applications are sealed, they remain protected even in the case of an attacker's attempt to alter or bypass the MobileRoT technology.

Traditional solutions focus primarily on boot-time validation, establishing the validity of each component prior to a complete boot, while providing only minimal support for runtime activities. Unfortunately, it is widely known that sophisticated attacks can target applications that are already running and devices are rarely rebooted these days. To address the shortcomings of one-time static verification, MobileRoT provides dynamic verification and attestation by also performing runtime measurements of the system state of the device. These runtime agents harden themselves from attack and modification by creating a self-validating network, which can instantly respond to a threat to the system or the protection technology itself.

While cybercrime targeting mobile devices is becoming pervasive, MobileRoT can preserve and confirm the integrity of the device while at rest or in use. BlueRISC's MobileRoT technology has overcome barriers to bring RoT to a mobile platform, providing a foundation of security features to accelerate development of secure mobile devices.



Benefits

The value proposition for BlueRISC's MobileRoT product is the establishment of software-based static and dynamic RoTs that can be leveraged for providing application and data protection and trusted MDM policy enforcement. The automated installation methodology and the lack of any modifications to the underlying operating system kernel drastically reduce barrier-to-entry.

MobileRoT reliably allows all levels of software, including user applications, to have access to its trusted services through an open application programming interface (API). This enables the creation of secure off-the-shelf third-party and proprietary applications and data, and strengthens key management and policy enforcement technology, such as Mobile Device Management (MDM). MobileRoT also provides fine-grained protections integrated directly into an application. For example, BlueRISC has taken a standard Android Calendar application and modified to support the concept of a "Secure Event". This secure event is established in cooperation with the MobileRoT and persistently protected. To view a secure event, proper authorization and authentication is required and the system state must be verified.

Competitive Advantage

In the mobile device protection, there are two main types of solutions: those provided by the device manufacturers and those designed to operate on top of the OS to provide some user-land security services. Out of these two types of products, the former represent the main competition. Table 1 provides a more detailed competitive analysis between mobile protection solutions.

BlueRISC's solution complements the user-land security solutions (such as MDM), which could take advantage of the RoTs provided by MobileRoT to harden their system/approach via the open trusted services API. The provided features are valuable to traditional anti-virus/MDM companies because recent trends in security suggest that they are losing their value proposition as the attacks are becoming more sophisticated. Lastly, one of the goals of MobileRoT is to provide a U.S.-made alternative to vendor-specific technologies such as Samsung's Knox that is also open to third-party developers. This is also expanding upon the protections and trusted services while enabling flexibility.

Next Steps

We are currently finalizing implementation of the Trusted Services API to provide beta versions to our existing partners for use-case development and security evaluation. We are always interested in exploring additional use-cases with new partners.

Competitive Analysis of Mobile Protection Solutions

Features	BlueRISC	Samsung	Arxan	McAfee
Software-only Roots of Trust	1	0	1	1
Chain-of-trust: Boot through Runtime	1	1	0	0
Dynamic System Attestation	1	0	1	1
MTM Compatible+	1	0	0	0
Open API	1	1	1	0
Automated Technology Insertion	1	0	0	1
Provisioning for FIPS Certification	1	1	0	0
Supports Government Credentials	1	1	0	0
Owned & Operated in USA*	1	0	1	1
Total:	9	4	4	4

+ Enables 3rd party MTM compatible software to run

* Critical for US Government & Defense Use Cases

Mobile Roots of Trust : Next-Generation Security and Confidence

Galois

Adam Wick

[Email Adam Wick](#)

Overview

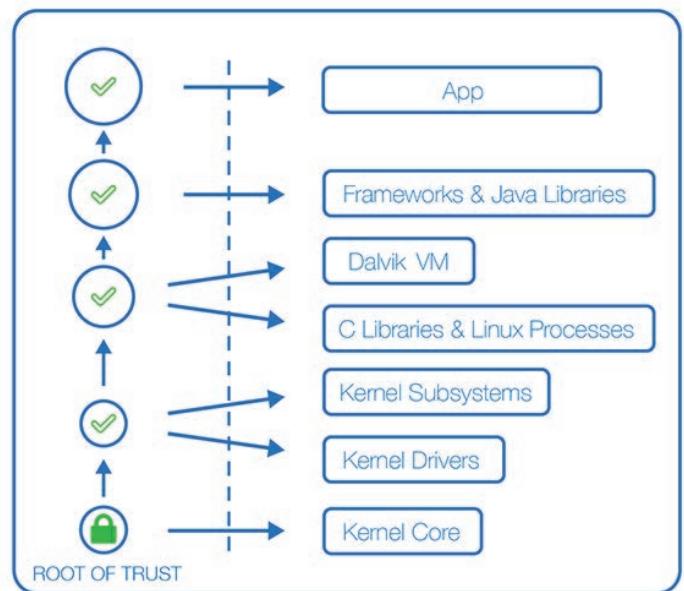
Mobile roots of trust provide a mechanism to not only have a secure device, but to prove it. While such capabilities exist in limited product lines, we focus on increasing commercial understanding of the capability to bootstrap a market that provides better and more prevalent capabilities.

Customer Need

As malware infects the mobile environment, the critical services in our lives must begin to ensure that the requests they receive from our mobile phones are actually coming from us, rather than from malware. To do this, they must have a trustworthy mechanism by which to query the state of our devices. This capability allows government and commercial entities to ensure, for example, that critical data is only transferred to devices that have been properly configured to organizational standards.

At the heart of any such mechanism is a root of trust. It provides the basis for any argument the phone makes about its state. Because of the root of trust, we trust the phone's measurement of some base service: the boot loader, for example. Because we trust the boot loader, we trust what it reports about what OS was booted. Because we trust that, we trust the OS's reports about what services are loaded. From there, we can build trust in libraries, system services, and even applications. Ultimately, at the bottom of this chain of evidence is the root of trust, see Figure 1.

While some basic roots of trust exist in current systems, they lack the strength required for truly critical systems. The reasons for this lack hearken back to a frequent paradox in technology transition: hardware manufacturers are reluctant to improve systems without user demand, software developers are reluctant to use hardware capabilities with limited penetration, and users are unwilling to demand features for software they don't have.



A measurement chain for the Android

Figure 1: Root of Trust Layering

Our Approach

Our goal is to break this paradox by introducing useful applications that government and commercial vendors can use to solve critical problems. Through these applications, we can begin to increase customer demand for related software by showing the usefulness of the technique across multiple use cases. In doing so, we thus increase the demand for strong roots of trust in off-the-shelf mobile devices.

Our first example application is an entrance-monitoring device. In this application, we can create a system that can automatically determine if a device meets the criteria of an organization for admittance: for example, if the camera is appropriately disabled, if the operating system has been updated appropriately, or if the network settings are appropriately configured. For devices that succeed, it can also provide information to the device: calendar events, site maps, or even network configuration information.

Our second example pairs a mobile device and a cloud-based service. In this example, we use a root of trust to prove to a server that the device is not running a broken version of a library. Such a capability would allow a bank, for example, to reliably determine that a user is not using a compromised or comprisable cryptography library in its communication.

Benefits

By generating applications that utilize roots of trust, we mobilize the security and mobile applications community by providing them with examples, guidance, and advice in creating their own products. As with many technologies, the early adopters pay some of the largest development costs, as they must blaze new ground. In this project, we attempt to lower this cost of early adoption with our prototypes, so as to speed up the adoption of the technology across the industry.

Competitive Advantage

Mobile roots of trust provide operators deep confidence in the integrity of a request. With most other security systems, including most Mobile Device Management (MDM) systems, operators must always be concerned that the client software has been subverted and the responses it receives are faked. With mobile roots of trust, we close this loop.

Note that this makes mobile roots of trust an assistive security technology: it does not replace MDM systems, but it can be used to ensure that the MDM software is running and operating correctly. This analogy can then be expanded across a wide variety of systems:

- It does not encrypt data, but ensures that your encryption layer is running appropriately.
- It does not authorize users, but can ensure that your authorization scheme is running appropriately and has not been bypassed.

In short, mobile roots of trust allow operators to not just write secure systems, but to verify that those systems are really running.

Next Steps

The next steps for this work are to publish information about these applications more widely, and find homes for them in commercial, government, or military venues. From there, we plan to expand the portfolio of applications even further, thus driving demand for the underlying technology even higher.

Mobile Roots of Trust : Trusted User Module (TUM)

Paul Rivera

[Email Paul Rivera](#)

Dr. Andras Moritz – Founder

[Email Dr. Andras Moritz](#)

Overview

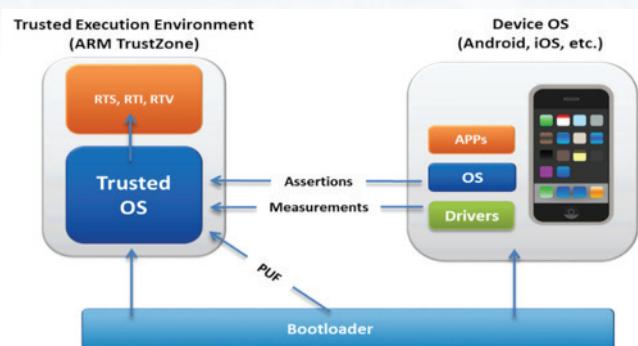
Trusted User Module (TUM), is a solution that provides a software-based root of trust for devices where a Trusted Platform Module (TPM) chip is absent. Applicable devices include mobile phones, tablets, and wearable devices. Leveraging this technology, a device can produce a unique identity for another device, measure and protect boot loader and operating system code, and utilize cryptography services and keys available only to that unique device.

Customer Need

Mobile devices, such as smartphones and tablets, are increasingly being used by the general public for sensitive tasks such as personal banking. With this increase of sensitive transactions, mobile devices are becoming attractive for hackers to break into and exploit. Although several pieces of technology exist to help protect against such intrusions, these devices lack a firm foundation upon which to build trust and security. Software-based security methods – the most common security measures found on mobile devices today – provide limited security and no secure root of trust. Hardware-based security requires a specialized piece of hardware called a TPM to provide root of trust services. Though the number of devices with this hardware is rising, it is not commonly found on today's mobile devices.

Our Approach

This technology can be employed by third party applications to provide platform integrity, encryption services, remote attestation services, secure signing services and licensing enforcement. Platform integrity includes measuring boot loader and operating system (OS) code, preventing execution of unrecognized or modified code, and restoring the original trusted code. Encryption services include disk encryption, secure password and key storage, and secure storage of other sensitive data. Remote attestation services include remote server or VPN authentication along with remote service authentication. Finally, secure signing services will allow for transaction



signing, which is something that financial institutions can use.

Benefits

The TUM will allow devices to have Smart Card-like security for VPNs, virtual wallets, and digital signatures. The approach requires no special hardware and is platform agnostic. When embedded into a wearable device, the TUM can turn it into a single sign-on device; this allows for secure connections made from other devices registered with the wearable device to be made quickly, providing two- to three-factor authentication.

Competitive Advantage

Our technology can work on multiple devices from different vendors. Knox, for example, is proprietary and only works on the Galaxy line of Android phones. The TUM is platform and OS agnostic, which allows for the technology to be embedded in wearables along with other devices. Additionally, TPM is a hardware implementation of roots of trust; however, this is currently rare and not implemented on mobile devices. This approach will be able to complement the TPM once it becomes available for mobile devices.

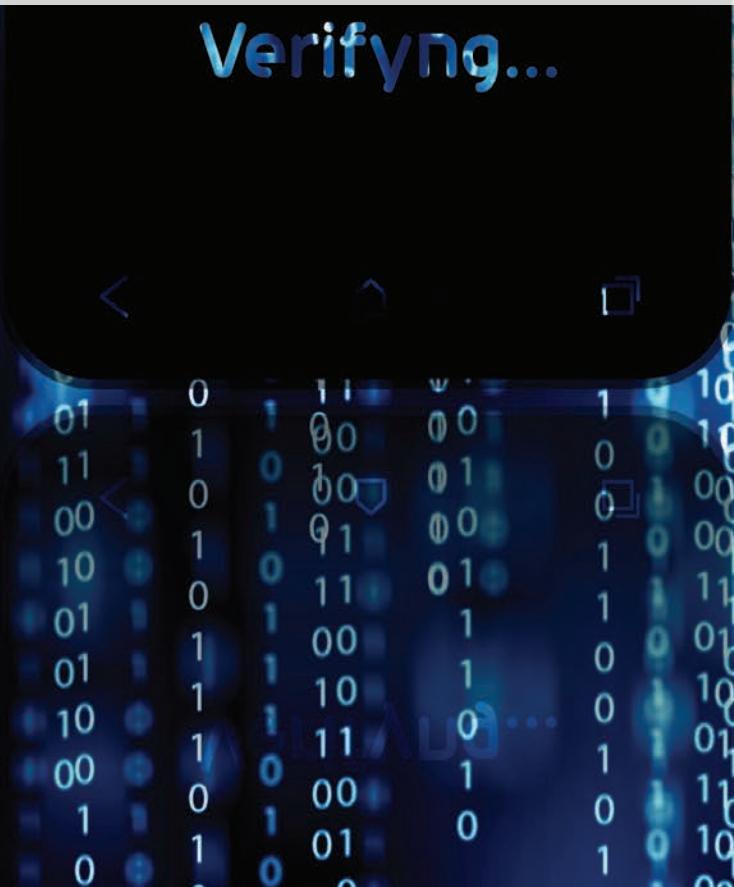
Next Steps

We are in the second phase of development and will continue to work on building additional applications on top of the TUM. We will be looking for investors to help fund the project to commercialization.



Security Login

Mobile Instrumentation



Verifying...

iSentinel: Continuous Behavior-based Authentication for Mobile Devices

HRL Laboratories

Vincent De Sario

Email Vincent De Sario

Tsai-Ching Lu

Email Tsai-Ching Lu

Overview

iSentinel is a breakthrough low-power, cascading anomaly detection system that provides unobtrusive, and continuous, behavior-based authentication for mobile devices.

Customer Need

With the ever increasing role of mobile devices in our world, significant challenges have arisen related to maintaining security of these devices. We are specifically addressing a customer need where physical access to a device is compromised.

This security threat model involves a mobile device, which has been authenticated by the authorized user and subsequently falls into the hands of another party. Whether the other party is “honest but curious” or malicious, the system needs to detect that someone else is using the phone. In this particular threat scenario continuous behavior-based authentication is required, using signatures learned from the authorized user by monitoring device sensors. Due to the continuous nature of the monitoring and authentication, low-power classification of sensor data streams is needed. This requires specialized hardware that is capable of running at much lower power than conventional mobile device processors. Finally, a sophisticated security management system is needed to execute appropriate security policies on the device.

Our Approach

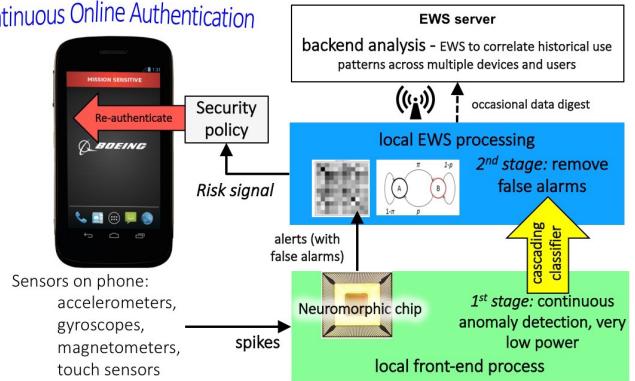
iSentinel’s power-efficient, neuromorphic hardware exploits brain-inspired plasticity in an algorithm for continuous sensor-agnostic online learning and classification of user behaviors. Security alerts from this front-end process will activate our novel early warning system (EWS) algorithms running on the local mobile device processor for improved analysis, and on a backend server for learning group norms and detecting stealthy attacks against multiple users and devices. This cascading classification approach combines the power efficiency of neuromorphic hardware with intermittent EWS classification to remove false alarms, to infer behavioral anomalies from an ensemble of mobile device sensors.

State-of-the-art approaches for mobile device security train behavioral models offline on conventional processing hardware that use much more power than HRL’s neuromorphic chip. This chip is unique among neuromorphic hardware in that it employs spike timing dependent plasticity (STDP) to automatically perform inference from online training data without supervision (by updating synaptic weights directly in hardware). In addition, our scalable sensor and model agnostic EWS algorithms require no specialized knowledge to extract unique signatures and perform behavior discovery from multiple sensor data streams.

We will implement this revolutionary system with our subcontractor The Boeing Company using a secure mobile device, a unique Android-based architecture with a foundation built upon layers of trust from embedded hardware, operating system policy controls, risk-management policies, risk-based assessment of the context in which the device is being used, and compatibility with leading mobile device management systems.

Benefits

Continuous Online Authentication



iSentinel will result in a new way to prevent unauthorized use of a mobile device, with minimal drain on power or computing resources. Re-authentications will be required only after a sophisticated multi-stage analysis that will reduce false alarms. Our methods analyze multiple streams of sensor data in real time continuously, from three different perspectives: spiking neural networks,

graph-theoretic analysis of behavior transitions, and group behavior interactions. Implementation on the secure mobile device provides DHS with continuous behavior-based authentication tied to robust risk management policies. Thus, in the face of ever-increasing use of mobile devices by DHS and other agencies, the result of our work will raise the level of security with minimal impact on the user experience.

Competitive Advantage

Finding the balance between security, privacy, and usability for mobile authentication has been an active area of research for the past five years. Unlike existing state-of-the-art technologies that train their classifiers on specific sensors for user identification and authentication, our approach adapts to inputs from any sensors, detecting anomalies independent of the specific sensors, while conducting adaptive multi-stage analyses with significantly reduced power consumption. The power efficiency of our neuromorphic chip and EWS algorithms will enable our system to continuously analyze data from multiple sensors with minimal impact on the user.

Many researchers have taken advantage of the availability of multiple sensors on mobile phones and proposed using the inputs from specific (combinations of) sensors to train their classifier(s) and to authenticate users. For example, some models utilize the notion of implicit authentication based on behavior patterns that can be identified from a combination of sensors including location, co-location, application usage, biometric measurements, continuity of interaction between the user and the phone, and possession of the phone. Some researchers focused on the factors governed by motion and posture sensors and utilized multi-staged external servers for heavy classification analysis.

Unlike existing approaches, iSentinel utilizes three stages for anomaly detection with low false alarms: (1) the neuromorphic chip for continuous online monitoring and classification, (2) our EWS algorithms run on the mobile device CPU for closer inspection of alerts, and (3) the offline backend server for group behavior analysis.

Next Steps

We are currently performing hardware testing of our neural chip consisting of 576 neurons. A neuromorphic hardware interface and configuration software has been written, and pilot studies have been completed, using publicly available accelerometer data, to demonstrate the capability to differentiate between accelerometer time-series.

Our EWS algorithms were tested on mobile sensor data collected across different users across the same scenario (phone in pocket walking down a hallway). Based on the EWS gait patterns detected from the accelerometer data a wavelet-based classifier could distinguish between the two users.

Next steps include performing tests of the operation of all 16 time-multiplexed synapses associated with a neuron in the neural chip. We also plan to perform more sophisticated neuromorphic hardware studies to determine the optimal training method. Continued testing of EWS algorithms for anomaly detection on mobile data collected from multiple users is also planned to verify our pilot results findings and to generalize these results to large mobile device data sets.

Quo Vandis: Mobile Device and User Authentication Framework

Kryptowire

Dr. Angelos Stavrou
[Email Dr. Angelos Stavrou](mailto:Dr.Angelos.Stavrou)

Overview

Quo Vandis provides continuous device and user behavioral authentication to prevent unauthorized access to mobile app functionality and sensitive enterprise data. Coupled with Mobile Device Management (MDM), or as a stand-alone solution, the Quo Vandis authentication decision engine collects live smartphone sensor data from the user, device context and environment to derive authentication confidence levels. Our approach is designed to support a robust permission model with multiple authentication levels.

Customer Need

Passwords have been proven to be ineffective in computing environments and even more challenging to work with on mobile devices, with small form factors. Multiple devices require a separate and unique password for each mobile app. This results in a high probability of failure, user frustration and ultimately weaker levels of security as user's seek work-arounds to bypass password-based security controls. Moreover, passwords alone cannot solve the impostor problem when a device is lost or temporarily misplaced and cannot take policy or mission parameters into consideration. The National Institute of Standards and Technologies is currently evaluating new approaches to remote user authentication and recommending the use of passwords only for low value assets.

Our Approach

Kryptowire's Quo Vandis collects sensor data from the user's smartphone to improve the confidence level during the device and user authentication process. The data collected includes Wi-Fi, General Packet Radio Service, Near Field Communication, Bluetooth, Power, Movement, Touch measurements while the user operates on mobile devices.

The Quo Vandis Authentication Decision Engine weighs data from all the sensor modalities, the current state of the device, ongoing user activities, existing user/device profile and historical data, the device operating environment, local

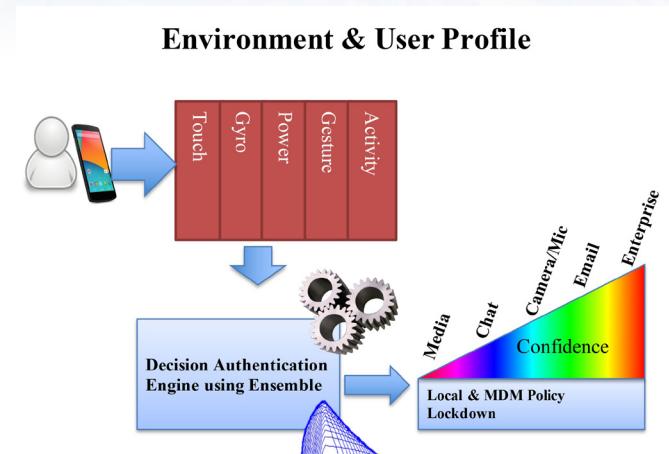


Figure 1: The Quo Vandis Framework

and MDM policies to render continuous permission and authentication decisions.

Benefits

Kryptowire's Quo Vandis addresses the limitations of a password-based device and user authentication and takes advantage of the plethora of sensor data available on today's commercial, off-the-shelf smartphones to offer seamless, robust and extensible mobile user and device authentication. The benefits of this approach include:

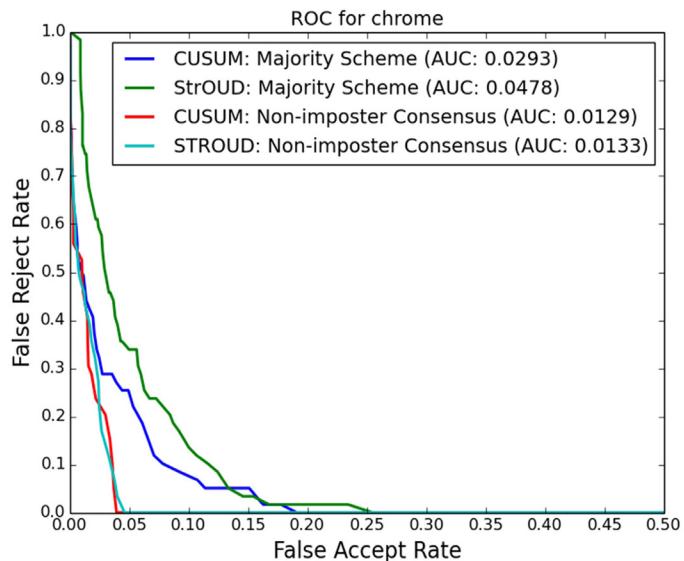
- Progressive permission model
- Multiple user access levels from non-authenticated to fully-authenticated
- Continuous authentication vs. one-time
- Unauthorized users and apps prevented from accessing sensitive functionality and data
- Policy models using location, device environment, device sensors and user input to establish trust
- Authentication level shared among devices and applications
- Remote operators situational awareness and policy enforcement via MDM application programming interfaces
- Better usability/less user frustration,

- Users and devices are seamlessly authenticated
 - no need to remember a password
- Device and user profiles can be transferred or shared among devices

Competitive Advantage

The Quo Vandis mobile device and user authentication framework can capture profiles, monitor live Android devices and lock down devices at various levels of granularity. The framework provides continuous monitoring and authentication and supports a progressive permission model. Additionally, Quo Vandis enables lockdown of mobile applications and/or device capabilities based on the combined risk derived from confidence levels, mission requirements and the mobile operating environment. The lockdown and monitoring will average less than 1% usage of device power and make imposter/non-impostor decisions within 3-5 minutes.

Preliminary Results



CARAMA: Continuous Assessment of Risk Affecting Mobile Authentication

Lap Truong

[Email Lap Truong](#)

Zadquiel Avila

[Email Zadquiel Avila](#)

Akhilesh Tyagi

[Email Akhilesh Tyagi](#)

Northrop
Grumman

Ben Draffin

[Email Ben Draffin](#)

Overview

CARAMA enables mobile authentication and continuous risk assessment based on the user's behavior. It uses touch input and device sensors to prove identity and integrates with a device and/or enterprise security policy.

Customer Need

Traditional passwords, tokens and 2-factor authentication schemes are often cumbersome and verify user identity at only a single point in time. A new approach is needed for managing security at the user level more seamlessly, allowing for multiple factors to prove identity over time. By connecting the actions users take with the identities and behaviors recorded in the past, devices and services can have both greater convenience and greater security. Any approach must not, however, compromise the benefits of mobile technology, reduce security, or hinder the user's productivity.

Our Approach uses

CARAMA leverages two unique technologies, SenSec¹ and UD-PUF², for enrolling user identity and behavior into the system. SenSec relies on a user's interaction with a mobile device to continuously authenticate them. Accelerometers and gyroscopes on the device are used to collect behavioral data, as well as touch screen interaction if data is available. Sequences of sensor data are used to build a statistical model of the user, predicting whether a new sequence of observed sensor data is likely generated by the standard user. In researching techniques for building such a statistical model, Northrop Grumman observed that human behavior is both relatively constant over time and very similar in structure to spoken or written text. Sequences of behaviors and words generally follow predictable patterns. Thus, we can apply traditional natural language processing techniques to biometric modeling based on an underlying "grammar" of human device interaction. This can be leveraged to protect the device. The second technology of our approach uses an unobtrusive highly accurate user authentication mechanism based on Physical Unclonable Functions (PUFs). These represent the

unclonable silicon biometrics of a device. Silicon fabrication foundries use steps with inherent statistical variability causing the same transistor in the design geometry to have different delays in different chips, even when they are built on the same wafer. Classically, PUFs are based on schemas that leverage variation in devices such as a ring oscillator, and they behave as a challenge/response function $R_i = f(C_i)$. The techniques from device authentication can be leveraged for user authentication as well, treating the user behavior as the "Unclonable function" and modeling from there. The response R_i of a PUF can be used as a unique biometric signature of a device for authentication.

As shown in **Figure 1**, the system collects data from sensors (global positioning system, accelerometer, camera, applications and system settings), network connections (Wi-Fi, Bluetooth, cellular) and the screen while the user interacts with the device. The system feeds these data to SenSec and UD-PUF engines to generate the result set used to establish a user profile baseline. It determines whether the set is typical or atypical based on a configurable threshold setting. Once a typical profile is established, the system saves it into the user profile database. The profile is used to authenticate the user at login and continuously assess risks during an active session.

During the active session on the device, the system continuously monitors the user's behavior and performs a real-time risk assessment based on user interactions. The results from monitoring the user will be interpreted by the mobile device management (MDM) system's policies. As shown in **Figure 2**, CARAMA's behavior analysis can influence the user's permission levels related to running applications, establishing network connections and accessing data. Higher levels of assurance are required for accessing more sensitive systems, as is common in traditional security policies today. CARAMA's security rules are a blend between the mobile user identity, behavior profile and the device security policies.

During operational use of the device, as shown in **Figure 3**, the system will authenticate the user at login using UD-PUF, as well as the user profile and security policy established during the user enrollment process. Once authenticated,

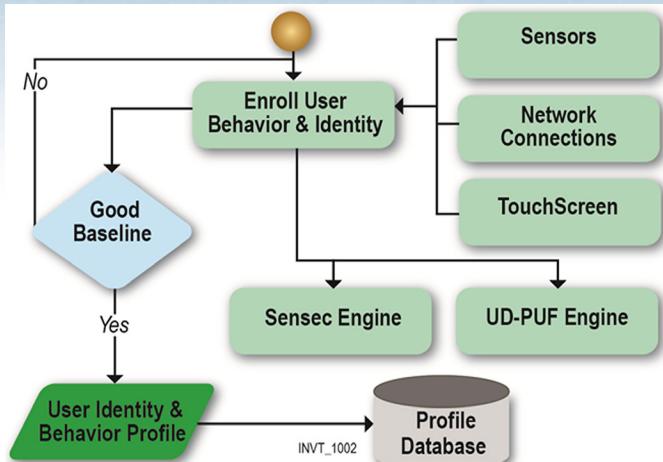


Figure 1: User Identity and Behavior Enrollment

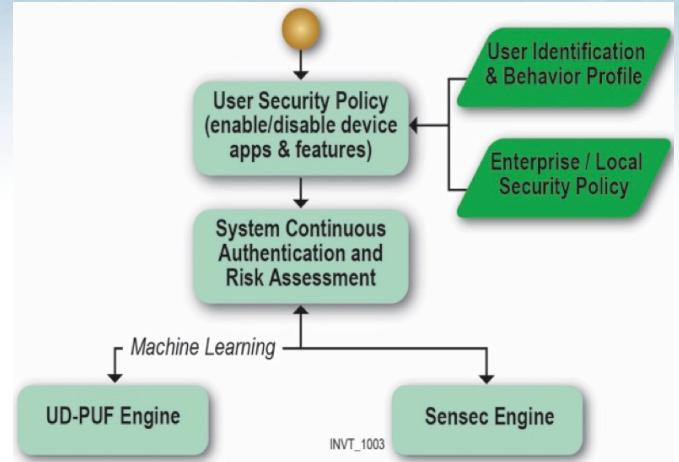


Figure 2: User-based Security Policy for Continuous Risk Management

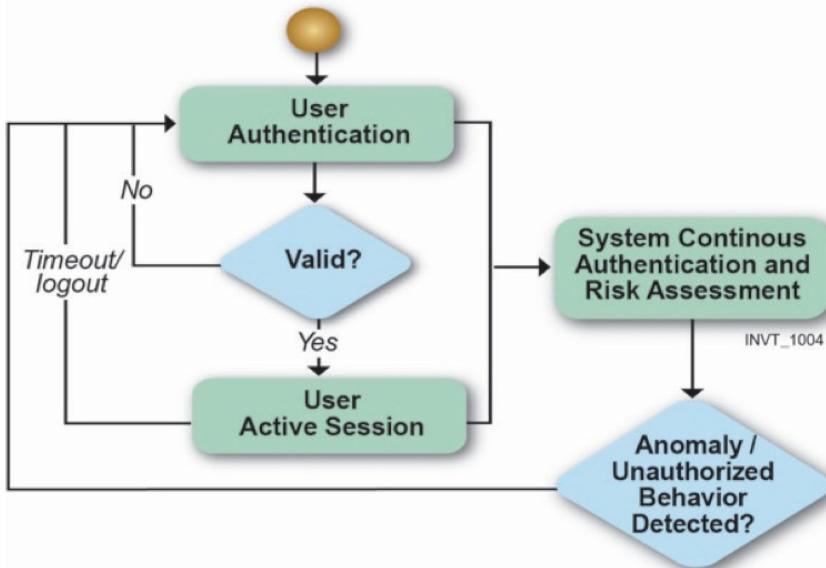


Figure 3: System Continuously Authenticates and Assesses Risks with User-based Security Policy

the continuous authentication and risk assessment component will actively assess user behavior and identity – leveraging the SenSec and UD-PUF engines. During this time, the system learns more about typical behavior and can enhance the user’s profile baseline through machine learning techniques in the two engines.

CARAMA allows protected smartphones to be both easier to use and more secure on a per-user basis. A primary disadvantage of traditional authentication techniques is the inconvenience to the user and potential credential leakage. By leveraging the user’s behavioral habits,

Northrop Grumman continuously collects proof of identity and behavior without any interruption of workflow. This saves the user time, strengthens proof of identity and reduces the security risk from hostile intrusion and stolen devices. Widespread adoption of these technologies will reduce the cost of device loss, since the devices can be automatically disabled, data-wiped, or reset automatically, minimizing sensitive data exposure.

Benefits

CARAMA focuses on providing rapid verification of authorized users and accurately identifying intruders with low false acceptance and low false rejection rates. The system also minimizes battery life impact, network traffic volume and inconvenience for the user. It emphasizes maximizing intuitiveness, responsiveness, compatibility, ease of configuration and efficacy for any enterprise tasked with proving user identity, or handling cases of lost or stolen phones.

Competitive Advantage

CARAMA offers a unique capability of aggregating two cutting edge technologies, SenSec and UD-PUF, to continuously monitor user behavior on mobile devices. It can assess and mitigate risks posed by activity of unauthorized users accessing applications. It provides for:

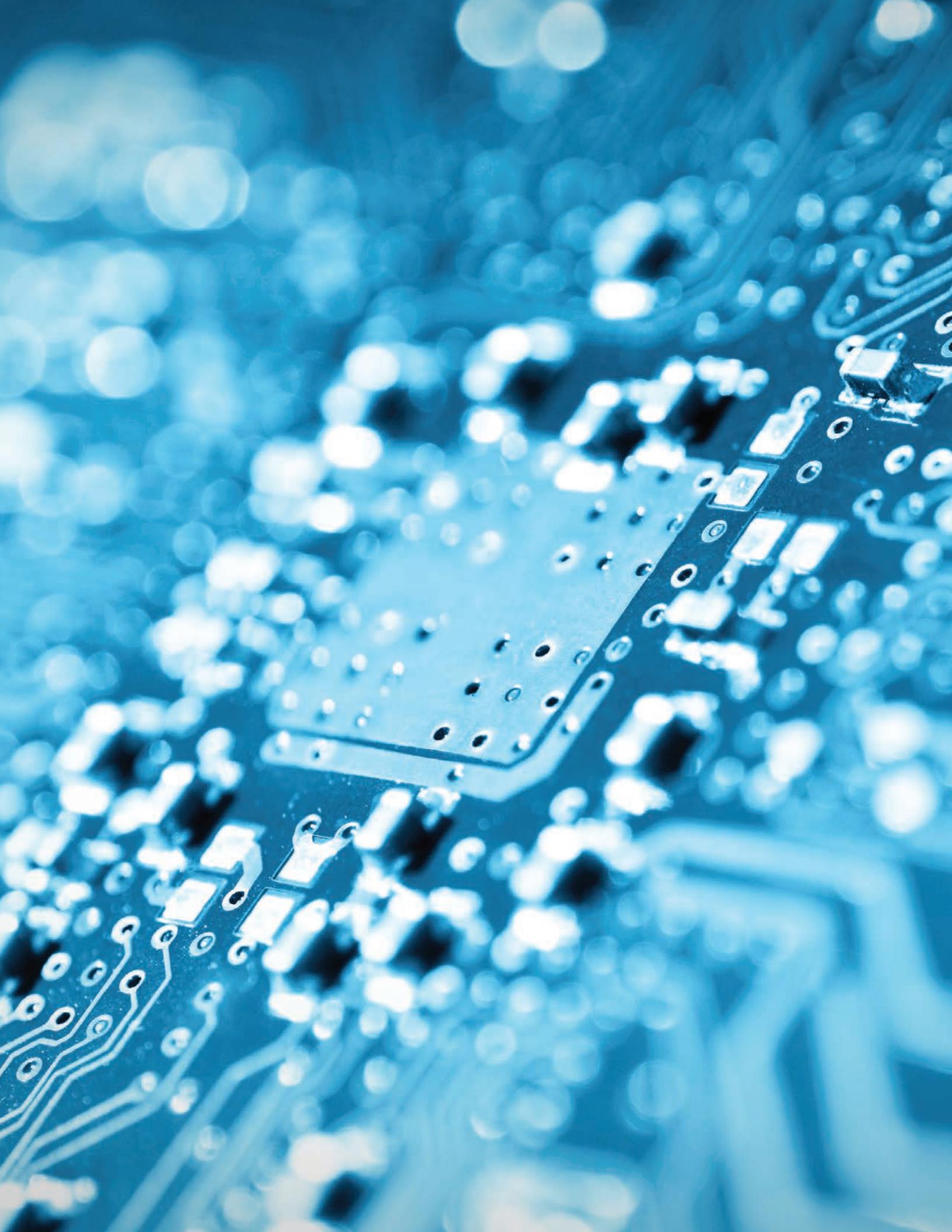
- Continuous assessment in the background about whether a user is authorized to use particular applications and access data on the device. This takes into account:
 - External factors: Where is the device being used? How recently has identity been proven? What is the security level of the networks it is connected to?
 - Internal factors: What are the active sensors? What applications are being used and what are their security policies? What data is being accessed?
- Rapid, accurate and unobtrusive verification of user identity.
 - If the risk exceeds a threshold, the user will be rapidly and accurately verified or the device will be shut down. The verification process should be simple and minimally obtrusive to the user, yet with a high degree of accuracy.

Next Steps

The next step for CARAMA will be integrating with a MDM security policy and developing a commercial-level graphical user interface (GUI) for the system. The development will include: an enhanced user enrollment GUI, an administration GUI and intuitive feedback to the user. Additional testing and evaluation with a larger end-user population will further increase the accuracy of the behavioral models, improve the user experience and streamline configuration for enterprise IT administrators.

References

- [1] SENsor SECurity
- [2] User Device Physical Unclonable Functions



CASTRA: Context Aware Security Technology for Responsive and Adaptive Protection

United Technologies Research Center

Devu Manikantan Shila
Email Devu Manikantan Shila

Overview

CASTRA is a continual, secure and user-friendly authentication platform that aims to overcome the limitations found in existing mobile authentication and application (app) access control techniques. CASTRA accomplishes this by continuously analyzing the context around the device, and by adapting application access decisions based on the perceived level of threats and context. Perceived threats such as: user identity, confidence in user's identity, sensitivity level of the application, geo-fencing (location) constraints, application trustworthiness etc. As opposed to conventional authentication schemes, CASTRA identifies the device user by means of passively analyzing user movements, location and proximity patterns. On top of these passive user patterns, CASTRA also uses an active authentication factor, like fingerprint, voice or facial detection to add an additional layer of security. Finally, CASTRA fuses all of these signals to determine to what degree the user is authentic in order to access specific app(s) (e.g., by computing a user confidence score with every positive/negative observation).

Customer Need

Mobile devices are ubiquitous in this modern age, and as such have become indispensable as enablers for collaboration and business use. However, with this added convenience there is an increased concern over the resilience of mobile devices against advanced cyber threats. This is especially true, given the increased complexity of these devices, the rise of mobile applications and importantly, the growing amount of sensitive information stored and processed on these devices. Mobile authentication is clearly one of the most crucial security controls needed for preventing unauthorized access to those sensitive services and information. However, many authentication solutions currently being used by the government and private sectors are inadequate. It can be difficult to fully realize the benefits of these mobile devices, mainly because of the degraded user experience (requiring users to authenticate every time the device is used), lack of user-specific and context-aware service access rights, poor security practices, insufficient security,

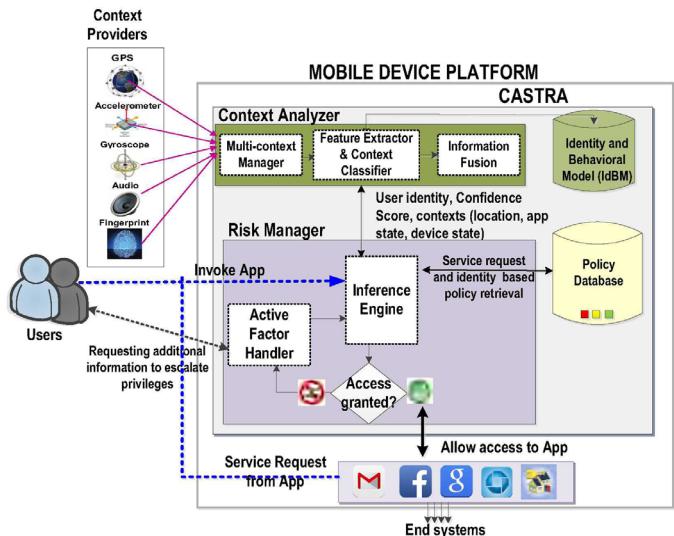
single shot authentication and presence of advanced malware in 3rd party apps that have visibility to data or resources handled by the sensitive apps. Moreover, current solutions do not completely leverage the processing and sensing capabilities of mobile devices to create the unique signatures that can enhance security without compromising the usability.

There is a strong need for secure and user-friendly authentication platforms like CASTRA for providing secure access to applications or data residing in smart devices.

Our Approach

The CASTRA solution is based on the integration of existing service access technologies with mobile device sensors, and perception systems using our techniques for segmenting and classifying multi-dimensional time series sensor signals. This will accurately infer the context around the device, fusing multiple sensor signals based on Weighted Naïve Bayesian, to estimate the confidence about user's identity and provide context-aware adaptive access to the apps. The exhibit below shows the high level architecture overview of CASTRA.

CASTRA is comprised of two major elements: a context analyzer and risk manager. Within the context analyzer module, the multi-context manager continuously gathers



information from low level mobile sensors such as GPS, accelerometer, gyroscope, proximity, pressure etc. Relevant features are then extracted and analyzed using multi-dimensional time series segmentation and classification algorithms by the feature extractor and context classifier module. From there, the context analyzer module will deduce the context (user identity, their trustworthiness score, location, list of active apps etc) around the mobile device. Secondly, the information fusion module combines multiple observations about the user (movement, proximity and location patterns) reported by the classifier module to compute the confidence level in user's identity. The inference engine, within the risk manager, uses the input from the context analyzer to decide whether an identified user/app has authorization rights for a specific resource under the given context. To prevent lock-out of a legitimate user (due to faulty sensor observations), the active factor handler will request further information (answer challenge-response or perform biometrics) from the user to boost trustworthiness.

Benefits

Enabling CASTRA will provide several benefits, such as protecting sensitive services and information residing in mobile devices from unauthorized hands, enabling multi-user authentication to devices and customizing services based on the user identity (responsive feature). It will also provide context-aware adaptive service/resource access based on the identity and trustworthiness of the user, service/resource sensitivity and threat level of the context, provide continuous user authentication and enable a user-friendly scheme without requiring the user to inconveniently authenticate every time the device is accessed.

Competitive Advantage

CASTRA provides several advantages compared to existing methods, such as context-aware authentication of device users and service provisioning, continuous user authentication and risk assessment, data (sensitive) visibility restriction to untrusted apps, fine-grained adaptive access control policy and enhanced usability.

The advantages of CASTRA are highlighted below by providing some example use cases.

Bob's smart phone (mobile device) runs several apps of varying sensitivity levels, ranging from low to high. He

is tired of authenticating to the device (using traditional techniques such as passwords, PINs, pattern locks, biometrics) whenever it is accessed, irrespective of the app he accesses. Bob will use CASTRA to create a user-friendly authentication scheme and will then set access control policies for each app.

Bob uses his smart phone to access smart devices at home (wireless locks, thermostats). Bob will use CASTRA to set access control policies to operate these devices (e.g., geo-fences, user profiles with associated confidence levels).

Bob's smart phone consists of several apps that are shared between family members. He wants to prevent unauthorized access to sensitive/personal apps such as banking, stock trade, health, SMS messages, etc. He will use CASTRA to build a multi-user authentication scheme and set access control policies for apps such that only allow Bob to access personal and sensitive apps.

Bob installs several third party apps such as gaming, news, etc. on his phone. Besides typical permission control (e.g. seen in Android phones), Bob is aware of 3rd party malware attack and likes to use CASTRA to prevent an untrusted app being active when sensitive or personal app is accessed.

Next Steps

We are currently designing machine learning models that can identify users with regard to location, gait, and device proximity patterns using public datasets. Experiments to collect various data from built-in mobile sensors such as accelerometer, gyroscope, proximity, humidity, audio, and pressure are also ongoing. In addition, we are seeking volunteers who are interested in being a part of the data collection experiments.



Transactional Security Methods

SWIRLS: Remote Access For Mobility via Virtual Micro Security Perimeters

Dr. Angelos Stavrou

Email Dr. Angelos Stavrou

Rutgers University
Electrical and Computer
Engineering Department

Overview

Smartphones are increasingly used in a variety of roles with wildly differing data-protection requirements, ranging from the access of sensitive content to the production and sharing of personal content via online social networks. SWIRLS provides a first-class data-protection architecture for mobile operating systems that uses dynamic information flow tracking and cryptographic policy enforcement technologies to isolate data instead of execution environments. SWIRLS provides formal method capabilities to simplify the guaranteed trustworthy usage of mobile phones without worrying about potential data leakage and unauthorized sensitive data access by third parties. Consequently, government and enterprise personnel could use their devices for various purposes involving sensitive data with different security requirements, while SWIRLS controls the data flow and access through the system in a very fine-grained manner and with negligible overhead.

Customer Need

Today, the only line of defense against accidental or malicious sensitive data leakage is through isolation of execution environments, (e.g., virtualization-based

techniques) that provide separate virtual phones which run on the same hardware but are otherwise completely isolated. However, the development and maintenance of multiple such environments is burdensome for both content owners and users. Content owners are burdened by having to develop apps for the sole purpose of enforcing data protection when otherwise a third-party app, perhaps with better functionalities, might have sufficed. These apps often live in siloed containers and are unable to access services provided by the rest of the mobile platform for fear of information contamination. For users, these multiple environments present a fragmented and often inconsistent experience that increases cognitive effort. Finally, in cases where system resources, such as cameras, microphones, or location are concerned, container-based approaches fail entirely.

Our Approach

SWIRLS develops a user-transparent and lightweight system-wide data isolation. It dynamically tags data based on its security context as embodied in a capsule and controls data mixing between capsules using a). system-wide multi-layer dynamic information flow tracking and b). distributed cross-application enforcement of capsule owner-specified and signed policies. SWIRLS provides

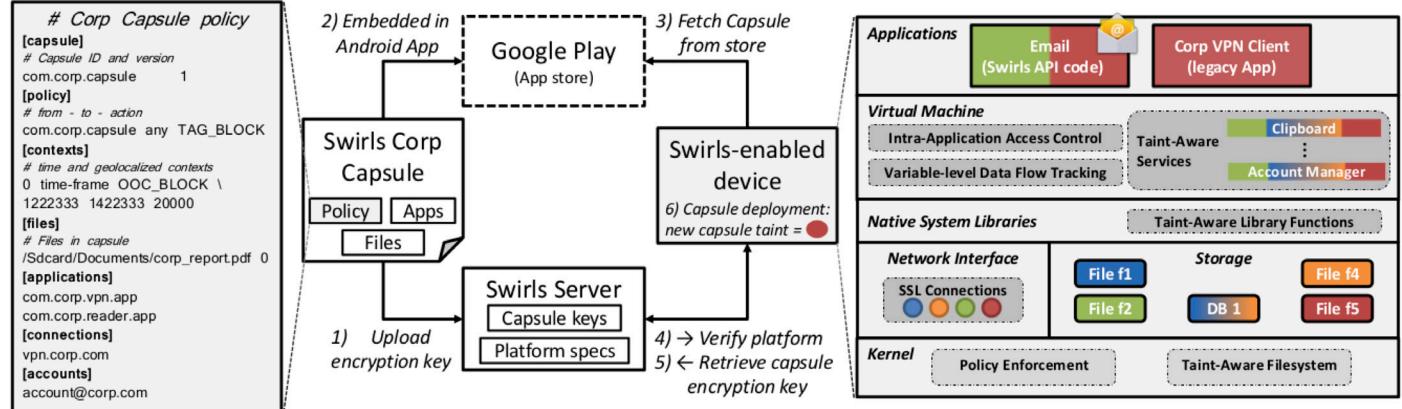


Figure 1: Smartphone clients usually use, or are asked to use, their devices for several purposes in various contexts with different security requirements on a daily basis. A context may represent a user role, a specific activity, time, location, or any combination thereof. SWIRLS enables secure realization of such scenarios through a formally verified architecture - including dynamic information flow tracking - as well as cryptographic system-wide and multi-layer policy enforcement.



users with a unified environment, and provides app developers with a programming API to construct seamless user interfaces which allows access to data with different security requirements through the same apps without fear of any malicious or inadvertent data leakage. SWIRLS provides formally proved security guarantees about its components: dynamic policy definition by the data owners, App store-based cryptographic distribution of capsules, and on-device integrity verification and installation.

Benefits

SWIRLS enables the operating system to track the flow of data on a per-capsule basis, as it is used by applications on the mobile device, and enforces the security policies associated with it.

Competitive Advantage

Swirl outperforms existing state-of-the-art solutions by addressing and eliminating the following real-world challenges:

Usability barrier. Existing solutions provide a coarse-grained interface that affects the solution's usability significantly. The user has to keep track of the contexts manually and switch among them explicitly through touch-screen swipes.

Unguaranteed security. Existing solutions are not guaranteed to maintain the data security invariants because they are heavily dependent on the users – who are susceptible to make mistakes – to ensure that unauthorized data accesses do not occur.

Architectural inflexibility. Existing solutions concentrate on the complete isolation of contexts so to keep entities related to each context absolutely separated from the others. Such isolation results in a static and inflexible architecture, which is not feasible to be reconfigured specially by non-technical users. Additionally, such an inflexible fixed architecture presents a paradoxical behavior. It does not allow any data transfer across the contexts at all (i.e., it is too restrictive) but does, however, permit every single data communication request between applications that belong to the same context (i.e., it is too permissive for practical use cases).

High-performance overhead. To guarantee context isolation, almost all of the existing solutions duplicate a full subset of system resources, such as context-specific

copies of the same application, content provider, or system service. System resource replications, as well as the usage of virtualization techniques, cause existing solutions to not only increase high-performance overhead (i.e. resulting in low battery life and poor usability), but also limit the number of contexts that each resource-limited smartphone device can handle.

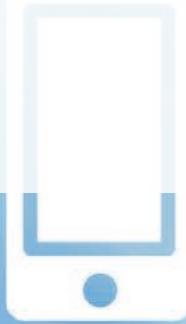
Next Steps

We are currently developing the system's architecture for secure data access control, cross-application, whole-system efficient data flow tracking, as well as cryptographic capsule distribution and installation frameworks. We are also working on the tool's user interface to facilitate use of the proposed techniques by non-technical end users without compromising any of the promised security guarantees. Furthermore, we are developing a use-case of SWIRLS for remote and secure smartphone IO access for first responders.

Additionally, we are looking for benchmarks to validate SWIRLS in real-world settings, and for commercialization and transition partners to achieve greater impact by putting SWIRLS into the hands of the operators who need it.



Next-Gen Mobile Security Management Tools



Multi-Modal Mobile Security Management for User Behavior Anomaly Detection and Risk Estimation

IBM

Ching-Yung Lin

Email Ching-Yung Lin

Overview

Mobile devices carry a number of vulnerabilities that can result in proprietary data leakage, fraudulent transactions, and even physical damage to the user and surroundings. Our solution creates novel Mobile Management Tools that understand long-term context-aware behavior anomalies on multiple devices with advanced understanding of human-device relationships and multi-modality behavior fusion.

Customer Need

Defense against malicious usage or abnormal use of mobile devices is difficult but crucial as more and more employees bring mobile devices to work. For example, employees could take pictures of proprietary documents using mobile devices and leak them out. Current mobile device security management relies on fixed rules that end users could easily get around with.

Our Approach

Our multi-layer approach discovers anomalous behaviors across multiple mobile devices. The system includes a prototype device layer of secure mobile service usage acquisition, with which the collected user activity will then be pre-processed and send to a central server hosting relationship data storage. The data storage will store, update, and retrieve the relationships among users, devices, activities, and services through novel graph technologies that make large-scale real-time activity update and analysis possible. New incoming activities trigger the risk analysis that generates an alert if the activities are anomalous. Alerts are shown in the used interface of the management tool along with the evidence in the user's activity history for the analyst to investigate. The system architecture is depicted in Figure 1, below.

Benefits

We provide an end-to-end package from unnoticeable and privacy-reserved data collection on mobile devices, advanced human behavior-based alert generation, high throughput data stores, to user-friendly management and alert user interface.

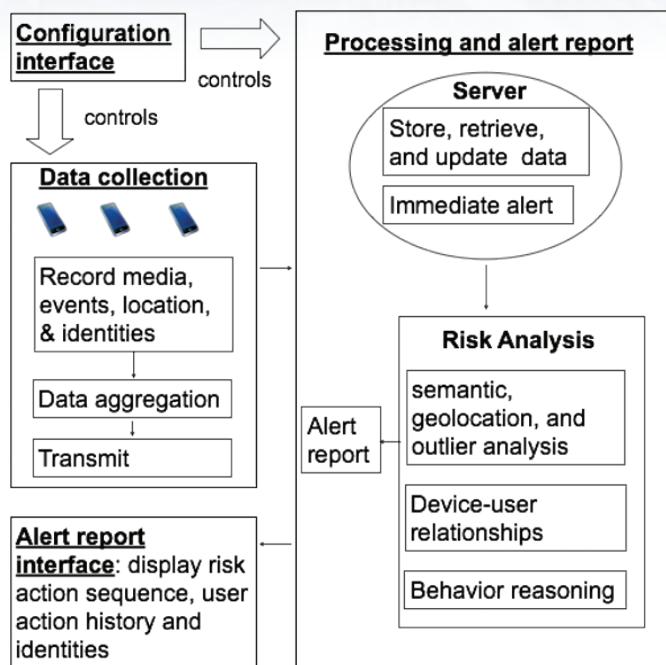


Figure 1: System Architecture

Competitive Advantage

Existing mobile security management solutions such offer a wide range of configuration and tracking features via configurable policies. However a primary feature that none of the existing solutions has context-aware anomaly detection. Moreover, the focus of existing solutions is set exclusively on the device and the installed applications, without considering the usage patterns of the human interacting with the device and users possessing multiple devices.

Next Steps

Behavior-based mobile security management is a high-impact area. We welcome opportunities to discuss how our solution can help secure the institutions' properties and work environments via identifying behavior anomalies in employees' mobile devices.

Theseus: A Mobile Security Management Tool for Mitigating Attacks in Mobile Networks

Dr. Jamie Payton

Email Dr. Jamie Payton

Dr. Leigh A. Flagg

Email Dr. Leigh A. Flagg

University of North Carolina at Charlotte

Overview

Theseus is a mobile device security management tool that monitors user activities, detects threats, and provides situational awareness for emerging first responder mobile networks.

Customer Need

The proliferation of powerful, low cost mobile devices and sensors provides attractive alternatives to traditional wired networks. Today's Wi-Fi networks will soon be augmented by the introduction of mobile, embedded, and wireless devices that are part of the Internet of Things (IoT). While these commodity devices continue to grow in power and flexibility, they are designed to be easy-to-use and quick to market. However, they are not necessarily secure. The myriad of devastating Android vulnerabilities and attacks that are increasingly designed for iOS provide evidence of the risks associated with these platforms. Such high risks are a barrier to entry for any local, state or federal government organization wishing to leverage mobile devices. This limits the potential uses of mobile devices by first responders to make the job of defending our nation and citizens safer, more coordinated, and more informed.

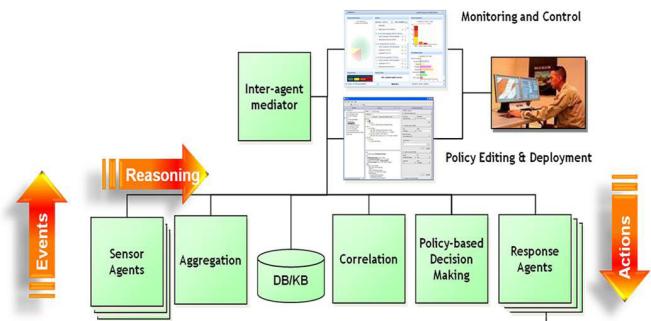
Emergency first responders need security information and event solutions that uniquely identify novel threats introduced by the use of ubiquitous devices and sensors.

Fortunately, over the years, researchers have made progress toward detecting and mitigating emerging threats for envisioned emergency response scenarios in which civilian, government, and military responders use mobile devices to support their operations. While existing threat detection and mitigation approaches focus primarily on packet-level analysis of network traffic, applying the context of device usage, in addition to communications, services and applications data has the potential to improve detection of threats in mobile settings.

Our Approach

Theseus is a proposed mobile security management tool that will extend existing threat detection approaches. This tool will provide support for detecting and mitigating emerging threats for envisioned emergency response scenarios in which civilian, government, and military responders use mobile devices to support their operations. Theseus leverages data from: sensors that detect phenomena in the surrounding environment, physiological sensors worn by emergency responders and victims, and sensors embedded on commodity mobile devices carried by emergency responders, to create a unified model of user activities and network communications.

The Theseus unified model goes beyond traditional threat detection approaches to incorporate the context of use of communications, services, and applications. By learning spatiotemporal patterns of data, communications - and application usage for first responders in given roles and scenarios - it is possible to identify anomalous behaviors that may be indicative of a threat to network security.



To provide actionable support, Theseus provides a web-based dashboard application that monitors the conditions of the mobile network, detects potential threats, and alerts personnel of detected vulnerabilities. Using a policy-based specification and an agent-based knowledge system, Theseus can present network operators with a set of recommended mitigation strategies.

Benefits

Theseus helps first responders to discover and mitigate mobile/sensor system vulnerabilities prior to compromise, and increases opportunities to expand the use of mobile devices in emerging emergency response networks. By providing aggregation and correlation of traditional cyber threat detection data streams with novel spatiotemporal events, the Theseus system will provide first responder network administrators the situation awareness they need for the unique threats to their communications. The integration of this collection of disparate data originating from collections of sensors, services, and mobile applications serves as a common semantic model of user activities, interactions, and behaviors. Integrating and analyzing data from disparate, distributed sensors that capture spatiotemporal information about the surrounding environment and the actions (both physical and operational) of emergency response personnel has the potential to reveal threats to devices and communications that were previously undetected. Given any identified threats, Theseus alerts device users and security staff quickly through a web-based interface that recommends actions for mitigation, and enables quick response to recommended mitigation actions.

Competitive Advantage

Theseus' **context of use** approach to modeling user behavior in a first responder mobile network is a unique approach that offers distinct advantages in monitoring emerging ubiquitous device networks. Network packet analysis can only identify a user's source, destination IP and their intent to do harm. Theseus complements such systems by providing temporal and spatial dimensions of data that identifies an individual's roles and intentions in the first responder network, and provides indicators of suspicious, risky and/or threatening activities which existing systems may not detect.

Theseus is an intelligent, flexible, and scalable cyber security situational awareness solution. It provides multi-level situational awareness and control through the use of a standards-based, policy-based knowledge model. That model is dynamically tunable through integrated policy management tools. Theseus has a light footprint, a distributed architecture and is easily deployed. Furthermore, it affords manual, semi-automated or

automated policy-based response allowing operators to react to security breaches rapidly.

Next Steps

Researchers at the University of North Carolina, Charlotte and Sentar Corporation are developing the spatiotemporal sensors and their associated threat models to integrate into the foundational Theseus framework.

We are working with the Madison 9-1-1 Public Safety Answering Point (PSAP) call center to elicit requirements and identify test sites. Our commercialization and transition partner, Emergency CallWorks, a Motorola Solutions division, will evaluate Theseus for use in their suite of innovative 911 dispatch solutions.

Mobile Device Layer Protection

TrustMS: A Trusted Monitor and Protection for Mobile Systems

Intelligent Automation, Inc.

Guang Jin

Email [Guang.Jin](mailto:Guang.Jin@IAI.com)

Overview

TrustMS utilizes advanced security mechanisms to address vulnerabilities on different software components. By innovatively utilizing the hardware-level security features, the key components of TrustMS are isolated from all potential attacks. Thus, no software malicious attacks can subvert the execution of TrustMS. Together, TrustMS provides a full spectrum security defense solutions for different layers of components in mobile devices.

Customer Need

Smart mobile devices such as smartphones and tablets, are playing an ever-greater role in ubiquitous information collection, dissemination and sharing. The use of mobile technology brings advantages in innovation, agility and flexibility for users. It is also known that the number of discovered malware on mobile devices keeps increasing due to insufficient security protection. As identified by the federal Chief Information Officers council, the lack of security brings immediate challenges to the adoption of mobile technologies into the government, military and sensitive commercial environments.

Like all computing devices, mobile devices are (like?) Turing machines. The state of a Turing machine is controlled by the content of variables in its memory, which can be further partitioned into code and data segments. The code segment contains the instructions to direct the computational tasks, while the data segment keeps the (temporary or final) computation results. A mobile device uses both memory segments to complete programmer specified tasks. Unfortunately, both segments are often exploited by attackers to launch malicious attacks. Current security solutions (embedded?) in mobile systems, however, offer unsatisfactory security properties against the cyber-attacks. Most solutions focus on protecting the code segment and provide a signature-based approach to monitor the data segment against a blacklist for the signature of known malicious programs and trigger an alarm once a malicious pattern is detected.

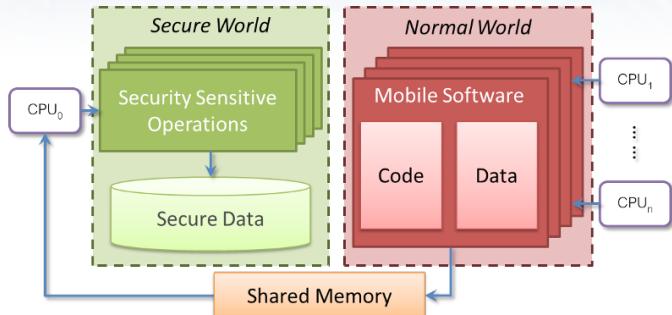


Figure 1: TrustMS Architecture

More attackers now use data-segment-targeting methods to achieve their malicious needs. Many cyber-attacks such as Return Oriented Programming (ROP) attacks, rely on exploiting vulnerable data segments of victim programs and do not tamper with the code segment. Consequently, most security solutions cannot effectively detect or prevent such a type of cyber-attacks. The security protection over the data segment faces more challenges than the code segment protection, since the data segment is much more dynamic. Mobile devices have many unique properties that are different with those on general purpose computers. For instance, they are usually built on top of resource constrained hardware and have strict time constraints. These properties require that security solutions be light-weight and have a small footprint on the Commercial Off-The-Shelf (COTS) Operating System (OS) and applications. Thus, security solutions must be tailored to these platform environments to optimize efficiency.

Our Approach

TrustMS is a trusted monitor and protection system to provide an effective and efficient security defense for mobile devices.

Figure 1 illustrates the TrustMS's architecture. TrustMS is designed for the multicore ARM platform and based on ARM's TrustZone, the hardware security extension provided by ARM. ARM's TrustZone provides the hardware-level isolation to partition the ARM-based mobile platform into two isolated execution environments, the secure and normal worlds. TrustMS dedicates a special ARM processor core (i.e., the secure core) to run in the secure world, while

other cores (i.e., normal cores) are utilized by the COTS mobile OS and applications in the normal world.

In TrustMS, the secure core maintains a shadow stack, duplicating the content of stack used by programs running in the normal world. TrustMS uses an offline code instrumentation engine to insert additional security checks and fortify target programs. The instrumented target programs will then report the content of critical program data (e.g., return addresses, indirect branch addresses, etc.) to the secure world automatically. In TrustMS, the normal cores execute target programs in the normal world. When a normal core needs to pass the program data to the secure world, the normal core simply writes the critical data content to a fast speed shared memory and continues executing the target program. In TrustMS, the secure core detects the change in the shared memory, processes the data and manages the shadow stack in the secure world in parallel with the normal cores.

To launch data-segment-targeting attacks like ROP, an attacker needs to illegally modify the return addresses in the stack used by victim programs. Once such an attack occurs, the modified normal stack will cause a mismatch with the shadow stack, which will be detected by the secure core and trigger further alerts and preventive actions.

Benefits

TrustMS has been applied to real mobile systems, including both Linux and Android systems. The experiment results show that TrustMS is effective against real-world cyber-attacks and extremely efficient to the resource constrained mobile devices.

Competitive Advantage

Isolated execution is a desired security feature, since it offers the ability to run the security critical module in absolute isolation from other software modules. TrustMS is based on ARM's TrustZone to provide the hardware-level isolated execution. By implementing the security sensitive operations in the secure world, TrustMS isolates itself from potential attacks. The hardware-based security guarantees that no malware, even the privileged ones, will be able to subvert the execution of TrustMS.

TrustMS offers an extremely efficient way for communication between the secure and normal worlds.

The innovative architecture and mechanism enable a fast, between-world communication within a few tens of nanoseconds, which significantly reduces the runtime overhead needed by TrustMS. From the in-house experiments on a quad-core ARM platform, the runtime overhead of TrustMS is negligible in most daily mobile scenarios. The experiment results show that TrustMS incurs less than 5% runtime overhead, while the state-of-art data segment protection for ARM platforms causes 10 times more runtime overhead.

While most existing security solutions focus only on the integrity of static program code segment, TrustMS provides a foundation for both static code and dynamic data segment protection of host mobile software systems. Hence, TrustMS is able to detect and prevent various types of attacks, including zero-day attacks in mobile systems.

Next Steps

The **International Association for Identification** (IAI) is currently extending TrustMS implementation onto the kernel-level programs to protect more critical COST software components, optimizing the scheduling mechanisms for the secure core to reduce power consumption.

IAI is also developing commercialization and transition strategies to apply TrustMS into real mobile devices and integrate TrustMS with real-world applications.

Mobile App Security





Mobile App Software Assurance

Kryptowire

Dr. Angelos Stavrou
[Email Dr. Angelos Stavrou](mailto:Dr.Angelos.Stavrou)

Overview

Federal, state, local and tribal government agencies can realize productivity gains and provide enhanced services through the use of mobile apps. These benefits, however, must be carefully weighed against any potential new security and privacy risks introduced by unvetted third-party mobile apps. Kryptowire will develop a scaleable enterprise system for assessing, analyzing, tracking and archiving mobile applications according to U.S. federal government security standards.

Customer Need

Smartphones and tablets enable government employees access to mobile apps virtually anytime and anywhere. Third-party software developers have created mobile apps that can support military, first responder, health care, travel, banking, finance, communications and countless other applications to help government employees better serve their agencies' mission.

Agencies must verify that the mobile apps used by their employees do not introduce unacceptable risk to agencies' data and network resources. Agencies must be able to analyze the security and privacy implications of the mobile apps and to verify their compliance with enterprise IT security and privacy policies.

Our Approach

The proposed mobile application analysis system will employ a wide range of static and dynamic analysis techniques to enable the automated, large-scale analysis of mobile application binary and source code, as well as any Java or native code and libraries.

The static and dynamic analysis results will be presented to an analyst in a detailed application report that will be accessible through a web-based portal. In case of applications with multiple versions, the system will functionally and semantically compare the application under analysis with previous versions of the same mobile application.

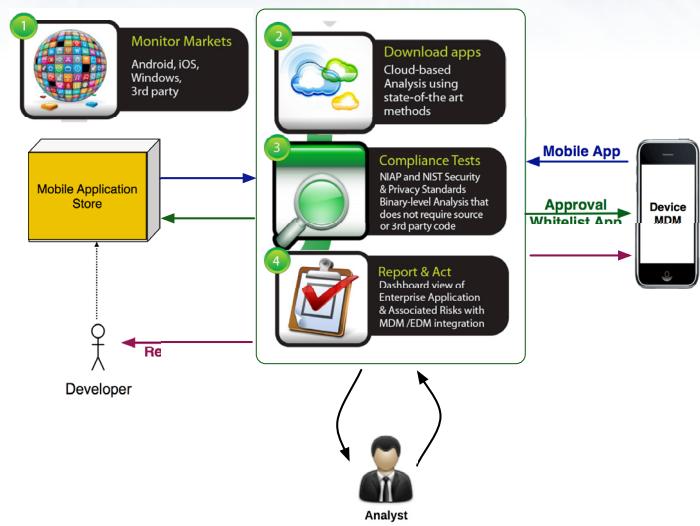


Figure 1: TrustMS Architecture

The reporting is further extended to cover market and application metadata and interactions of the application with the underlying operating system including all communications to and from the mobile device. This process will expose any potential risks stemming not only from the mobile application as a package, but also from the supply chain of the application including the application developer and the application market.

Benefits

Government agencies will be able to automatically vet their mobile applications for security and privacy compliance without access to third-party developer source code and get approved mobile applications to their user community without unnecessary delays. The IT security team will have complete visibility into the mobile applications and their metadata.

The mobile application analysis and reporting system will adhere to existing and emerging federal standards. Operationally, the system will implement the entire workflow of acquiring the mobile applications' binaries and meta-data from a configurable set of mobile markets, automatically analyzing the mobile applications' binaries, correlating the meta-data to existing versions of the mobile applications, presenting an analyst with a report, and

taking action on applications that require remediation. The system will assess third-party mobile applications' binaries and libraries including reporting based on the following standards:

- National Institute of Standards and Technology's (NIST) special publication SP800-163 Vetting the Security of Mobile Applications
- National Information Assurance Partnership (NIAP) Protection Profile for Application Software
- Mobile Technology Tiger Team (MTTT) Mobile Application Security Vetting Security Criteria

The aim of the system is to assist and reduce the time consumed by an information assurance expert in acquiring, analyzing and vetting mobile applications. Moreover, it offers testing and protection profiles for different use cases and user groups as defined by the organization that would request testing. The system will be able to support multiple analysts working in parallel and with different priorities.

Competitive Advantage

The Kryptowire mobile application analysis portal allows government agencies to pool resources, reduce the cost of manual analysis, have control, accountability, and transparency over the vetting and risk scoring process, test for compliance with NIST and National Security Agency guidelines, and integrate the results of the security and privacy analysis into other Mobile Application and Device Management technologies.

Conclusion

As the DHS S&T Cyber Security Division works to accelerate the adoption of secure mobile technologies throughout the government and industry, we must acknowledge the contributions of academia and industry in supporting our program. The ability to harness the creativity and expertise of those communities is critical to achieving our vision.

The types of R&D we invest in are aimed to solve a wide variety of technical challenges and to unleash the vast potential that mobility can bring to the Department, the government, and the global community. We have already begun transitioning new technologies and capabilities into government use and anticipate having further success with the results of current and future research efforts.

We encourage investors, researchers, and potential partners from throughout industry, government, and academia to reach out to learn more, explore our current research program, and discover how they might benefit from or participate in research and development efforts at DHS S&T.

For additional inquiries or to learn more please contact:

Vincent Sritapan

Mobile Security R&D Program Manager

Cyber Security Division

Homeland Security Advanced Research Projects Agency

Science & Technology Directorate

Department of Homeland Security

[Email Vincent Sritapan](#)

MDS Program Site: [MDS Program Website Link](#)

This page intentionally left blank.



DHS S&T Cyber Security Division Website



DHS S&T Cyber Security Division Email



DHS S&T Cyber Security
Division Twitter page



DHS S&T Cyber Security
Division YouTube page



DHS S&T Cyber Security
Division Facebook page