Archived Content

Cyber Security Division Technology Guide 2018

Homeland Security

Science and Technology

Introduction to the 2018 CSD Technology Guide

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Cyber Security Division (CSD), part of the Homeland Security Advanced Research Projects Agency (HSARPA), is charged with enhancing the security and resilience of the nation's critical information infrastructure and the internet. This 2018 Technology Guide is a compilation of mature, CSD-funded research and development (R&D) projects meeting that goal and ready for operational pilots or commercial transition.

This is the third annual CSD Technology Guide, updated to feature the latest innovative R&D technology solutions within the CSD portfolio. The technologies in this guide cover areas such as Software Assurance, Mobile Security, Identity Management, Distributed Denial of Service Defense, Data Privacy, Cybersecurity Research Infrastructure, Cyber Physical Systems Security, Cyber Outreach, Cyber Forensics as well as technology solutions from CSD's Transition to Practice program.

Each project is the culmination of extensive work to identify and develop cybersecurity technologies for Homeland Security Enterprise uses. These technologies—developed by our industry, academia and national lab partners—all underwent a thorough vetting process to ensure the proposed research addresses a pressing cybersecurity gap and possesses a high level of potential for success. The number and breath of R&D projects included in this guide speaks to the importance we place on transition of our developed technologies to end-users.

If you are interested in piloting, licensing or commercializing any of the technologies in this guide, please email us at SandT-Cyber-Liaison@hq.dhs.gov. Additionally, CSD is interested in engaging with you to discuss emerging cybersecurity capability gaps you foresee impacting your organization in the future. Your input will help us tie our R&D portfolio to real-world cybersecurity gaps and tailor our out-year research efforts to ensure more successful transitions in the future.

On behalf of the entire CSD team, it is my distinct pleasure to present to you the 2018 CSD Technology Guide. In its pages you will read about groundbreaking cybersecurity tools developed within the federal government R&D community. We encourage you to take a closer look at the technologies that most interest you and to reach out to us to discuss next steps.

Sincerely,

Dr. Douglas Maughan

DHS S&T HSARPA Cyber Security Division Director

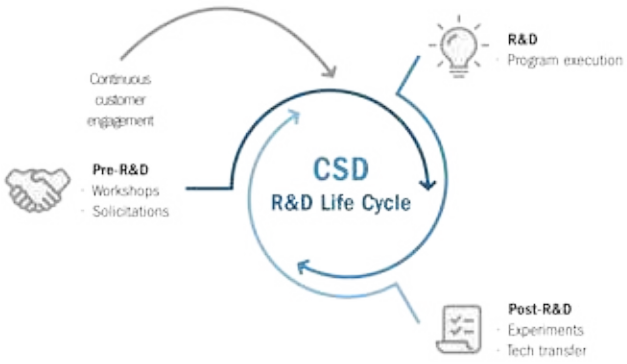
CONTENTS

Department of Homeland Security Science and Technology Directorate Cyber Security Division

THE CYBER SECURITY DIVISION LEADS DEVELOPMENT OF NEXT-GENERATION CYBERSECURITY SOLUTIONS

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

CSD supports the approaches outlined in the Federal



Cybersecurity Research and Development Strategic Plan by:

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

CSD'S BROAD CYBERSECURITY TECHNOLOGY AND CAPABILITY DEVELOPMENT PORTFOLIO

CSD's work is focused on the following programmatic areas, many of which are comprised of multiple projects targeting specific aspects of the broader program area:

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

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

Cybersecurity Outreach—Helping to foster training and education programs critical to the nation's future cybersecurity workforce needs by providing opportunities for high school and college students to develop their skills and giving them access to advanced education and exercises through team competitions.

Cybersecurity Research Infrastructure—Supporting the global cyber-risk research community by coordinating and developing real-world data and information-sharing capabilities, tools, models and methodologies through the Information Marketplace for Policy and Analysis of Cyber-risk and Trust (IMPACT) and developing the infrastructure needed to support the development and experimental testing of next-generation cybersecurity technologies through the Defense Technology Experimental Research (DETER) testbed.

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

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

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

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

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

Mobile Security—Developing innovative security technologies to accelerate the secure adoption of mobility in four areas: software-based mobile roots of trust, mobile malware analysis and application archiving, mobile technology security, and continuous authentication; and identifying and developing innovative approaches that extend beyond mobile device application deployment to provide continuous validation and threat protection as well as to enable security through the mobile application lifecycle.

Network Systems Security—Developing technologies to mitigate the security implications of cloud computing; building technologies to mitigate new and current distributed denial of service attack types; developing decision aids and techniques that enable organizations to better gauge and measure their security posture and help users make informed decisions based on threats and cost; launching an Application of Network Measurement Science project to improve the collection of network traffic information from around the globe, conduct research in attack modeling to enable critical infrastructure owners and operators to predict the effects of cyberattacks on their systems and create technologies that can identify and alert system administrators when an attack is occurring; enhancing security of the internet's core routing protocol so communications follow the intended path between organizations; and developing capabilities that continually modify attack surfaces as well as technologies that enable systems to continue functioning while a cyberattack is occurring.

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

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

Software Assurance—Developing tools, techniques and environments to analyze software, address internal flaws and vulnerabilities in software; creating a Unified Threat Management system to monitor and analyze software systems and applications for security threats; modernizing and advancing the capabilities of static analysis tools to improve coverage and integrate it seamlessly in the software development and delivery processes; and improve software security associated with critical infrastructure (energy, transportation, telecommunications, banking and finance, and other sectors).

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

S&T: PREPARING FOR EMERGING CYBER THREATS

Through its R&D focus, CSD is contributing to the nation's long-term security and reinforcing America's leadership in developing the cybersecurity technologies that safeguard our digital world. As new threats emerge, CSD will continue to be at the forefront of actions at all levels of government, in the R&D community and throughout the private sector to protect data privacy, maintain economic and national security, and empower citizens to take control of their digital security.

DHS Science and Technology Directorate

MISSION

Established by Congress in 2003, S&T's mission is to deliver effective and innovative insight, methods and solutions for the critical needs of the Homeland Security Enterprise (HSE). As DHS's primary research and development (R&D) arm, S&T manages science and technology research—from development through transition—for the Department's operational components, the nation's first responders and critical infrastructure sectors. S&T's engineers, scientists and researchers work closely with industry and academic partners to ensure R&D investments address the high-priority needs of today and the growing demands of the future.

From border security and biological defense to cybersecurity and explosives detection, S&T is at the forefront of integrating R&D across the public and private sectors and the international community. By working directly with responders and component partners across the nation, S&T strives to provide advanced capabilities and analytics to better prevent, respond to and recover from homeland security threats and high-consequence events.

FOCUS AREAS

S&T works with the broader R&D community to identify and adapt existing investments to meet operator needs and challenges in four general areas:

- S&T creates technological capabilities that address DHS operational and strategic needs or that are necessary to address evolving homeland security threats.
- S&T conducts systems-based analysis to provide streamlined, resource-saving process improvements and efficiencies to existing operations.
- S&T's technical expertise to improve project management, operational analysis and acquisition management helps DHS achieve more effective and efficient operations while avoiding acquisition failures and costly delays.
- S&T's relationships across DHS and the HSE contribute to the strategic understanding of existing and emerging threats and recognition of opportunities for collaboration across departmental, interagency, state and local and international boundaries.

Partnerships across the diverse R&D landscape—federal, state, local, tribal and territorial agencies; private industry; and academia—are the foundation for S&T's successful technology foraging efforts and adaptation of existing R&D investments to homeland security mission needs. S&T's understanding of the ever-changing threat environment and its relationships with the men and women who confront those threats every day make the organization an effective catalyst for improving the security and resilience of our nation.

DOING BUSINESS WITH S&T

Whatever the scenario, whatever the threat, S&T's mission is to strengthen America's security and resilience by providing innovative technology solutions, procedures and guidance for the HSE, which consists of DHS Components and first responders across the country. Small businesses are a vital part of our national strength and key contributors to developing solutions to better securing our country. At S&T, we ensure small companies have a fair opportunity to compete and be selected for DHS contracts.

You can learn more about government contracting, DHS S&T business networking and information about finding contracts, teaming or subcontract opportunities from the directorate's website. There also are tips and answers to frequently asked question about how to best position your company for success in working with DHS S&T. Go to www.dhs.gov/how-do-i/work-dhs-science-and-technology to learn more.

DHS S&T Homeland Security Advanced Research Projects Agency

WHO WE ARE

DHS S&T strengthens America's security and resiliency by providing knowledge products, innovative technology solutions, methods and insights for the critical needs of the Homeland Security Enterprise (HSE). S&T's HSARPA focuses on identifying, developing, and transitioning technologies and capabilities to countering chemical, biological, explosive, cyberterrorism, and unmanned aerial threats as well as protecting our nation's borders and infrastructure.

WHAT WE DO

HSARPA's functional organizations work directly with DHS components to better understand and address their high-priority requirements and define operational context by conducting analyses of current missions, systems, and processes. This process ultimately identifies operational gaps where S&T can have the greatest impact on operating efficiency and increasing capabilities.

HOW WE WORK—HSARPA GOALS

Working collaboratively within S&T, HSARPA delivers usable, scalable, cost-effective, mission-focused capabilities to DHS components and other HSE partners. The team also advises partners on science, technology, and industry developments with respect to mission, threats, and opportunities. HSARPA creates and matures a broad set of relationships across the DHS components and the HSE, which promotes open exchange of ideas and joint collaboration. In order to achieve these goals, HSARPA cultivates a knowledgeable workforce that is empowered to innovate, perform and streamline management execution processes to maximize impact.

SEVEN FUNCTIONAL ORGANIZATIONS

- Borders and Maritime Security Division: Prevents contraband, criminals, and terrorists from entering the United States, while permitting the lawful flow of commerce and visitors.
- Chemical and Biological Defense Division: Detects, protects against, responds to, and recovers from biological or chemical threats and events.
- Cyber Security Division: Creates a safe, secure, and resilient cyber environment.
- Explosives Division: Detects, prevents, and mitigates explosives attacks against people and infrastructure.
- Program Executive Office Unmanned Aerial Systems: Leads DHS's approach for guiding, assessing, advising, and enabling technical solutions for using small unmanned aerial vehicles (sUAS) and national efforts to counter sUAS misuse in the homeland.
- Apex Technology Engines: A matrixed team that powers open innovation to realize the S&T Visionary Goals. Their primary role is to provide a centralized suite of reusable products and support services individually tailored to the Apex program needs by identifying and sharing best practices, subject matter expertise, knowledge products, and technical services.
- Integrated Product Team: Provides prioritized technological capabilities that are a key driver of the research and development agenda.

To learn more about HSARPA and its initiatives, visit https://www.dhs.gov/science-and-technology/hsarpa or send an email to HSARPA@hq.dhs.gov.

INNOVATION PROJECTS

Next Generation Cyber Infrastructure Apex Program

The Next Generation Cyber Infrastructure Apex program addresses cybersecurity challenges facing our nation's critical infrastructure. Cyber Apex finds, tests and transfers proven solutions to fill cybersecurity gaps and protect these critical systems and networks.

Currently, Cyber Apex is working to harden the cyber-defenses of the financial services sector (FSS), which is a frequent target of cybercriminals. The Cyber Apex Review Team (CART), sponsored by CSD and made up of FSS institution and Treasury Department representatives, identifies gaps and evaluates solutions. While some gaps can be resolved by mature technology, others require novel ideas. This finding led Cyber Apex to establish two development paths: a consortium to test existing solutions and a partnership with the DHS Silicon Valley Innovation Program (SVIP) for early-stage solutions.

The consortium focuses on operational testing of mature technologies to determine if they meet FSS needs. Cyber Apex Solutions, the consortium manager, oversees the process of foraging and bringing technology owners together.

SVIP focuses on finding novel solutions from startups whose technologies are not mature enough for rigorous operational testing and evaluation. Solutions with promise are piloted and evaluated. The Cyber Apex solicitations under SVIP—the Financial Services Cyber Security Active Defense—seek startups that have novel solutions in the areas of moving-target defense, isolation and containment, and cyber-intrusion deception. Several performers have been selected.

DHS Silicon Valley Innovation Program

The DHS S&T Silicon Valley Innovation Program (SVIP) is keeping pace with the innovation community to tackle the hardest problems faced by DHS's operational missions and the Homeland Enterprise System. SVIP is expanding DHS S&T's reach to find new technologies that strengthen national security, with the goal of reshaping how government, entrepreneurs and industry work together to find cutting-edge solutions. SVIP, based in California's Silicon Valley, connects with innovation communities across the nation and around the world to harness the commercial R&D ecosystem for government applications, co-invest in ideas and accelerate transition-to-market.

Through a streamlined application and pitch process, SVIP is seeking solutions to challenges that range across the entire spectrum of the homeland security mission, including cybersecurity and technology solutions for Customs and Border Protection and first responders. SVIP can award a maximum of $800,000 (up to $200,000 per phase) across four phases spanning a 24-month period.

Since launching in December 2015, the SVIP has:

- Received more than 250 applications
- Made awards to more than 25 companies
- Leveraged more than $400 million in private-sector investments

For more information, visit https://scitech.dhs.gov/hsip or send an email to: DHS-Silicon-Valley@hq.dhs.gov.

CYBER PHYSICAL SYSTEMS

Side-Channel Causal Analysis for Design of Cyber-Physical Security

HRL Laboratories LLC

David Payton
dwpayton@hrl.com

Chase Garwood, CSD Cyber Physical Systems Security Program Manager
Chase.Garwood@hq.dhs.gov

OVERVIEW

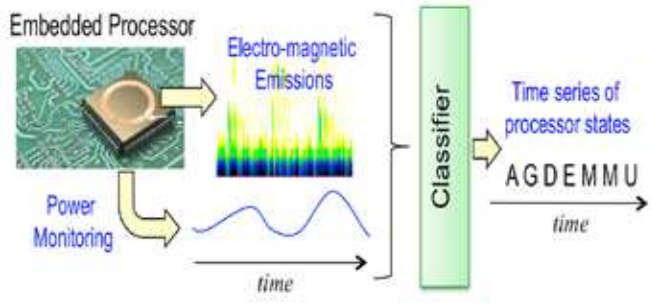
If compromised by a cyber-attack, automobiles and other cyber-physical systems could put people's lives at risk. This risk can be reduced by detecting inconsistencies between physical and cyber events that appear when an attacker attempts to take over. Using unconventional analog side-channel observations that are beyond the direct control of an attacker, this method detects when the intricate causal ties between system physics and cyber components are altered by a cyber intruder so such attacks can be prevented at an early stage.

CUSTOMER NEED

The need for enhanced vehicle cybersecurity extends to government, commercial and civilian vehicles. For government vehicles, the potential terrorist threat to first responders and law enforcement is a high-level concern since the severity of an attack could be dramatically compounded by interference with rescue efforts. Commercial trucking faces the potential for disaster caused by an attack on a single vehicle carrying hazardous materials. A coordinated attack on civilian vehicles could be used to create a severe disruption of essential services.

APPROACH

Side-channels such as power, thermal or electromagnetic emissions are used to reveal the presence of a hidden attacker by correlating computation with its effects in the physical realm. To detect attacks using both conventional and side-channel data, this method uses an information-theoretic measure that captures causal relationships from multiple time-series measurements. This approach provides a directed graph of system variables, reflecting an overall cause-and-effect structure within the system. The graph's deviation from the known causal system relationships serves as an effective early warning signal of a possible attack.



As they operate, embedded processors produce electromagnetic emissions and create time-varying demands on power that can be identified and uniquely associated with distinct processor states. A time-series of processor states can be identified from these signals and correlated with physical vehicle activity.

Benefits

By monitoring physical side-channel signatures that cannot be controlled by an attacker, and by detecting deviations from known causal interactions, auto manufacturers will be able to incorporate cyber-defenses into their vehicles that can detect and respond to attacks early, before serious damage has occurred. These defenses may be included with minimal added cost to consumers because the software can run on existing vehicle hardware and yet remain isolated from other potentially compromised modules.

COMPETITIVE ADVANTAGE

This solution goes beyond methods that look exclusively at side channels of individual processors by also looking at interactions between processors to combine the cyber with the physical to obtain a systems-level view of potential intrusions.

NEXT STEPS

Moving forward, researchers will gather data from multiple vehicles to evaluate the consistency of side-channel signals between vehicles across different mileage and use patterns. Potential application to other cyber-physical domains such as medical devices and aircraft also will be pursued.

Uptane: Secure Over-the-Air Updates for Ground Vehicles

University of Michigan Transportation Research Institute

Sam Lauzon
slauzon@umich.edu

Chase Garwood, CSD Cyber Physical Systems Security Program Manager
Chase.Garwood@hq.dhs.gov

OVERVIEW

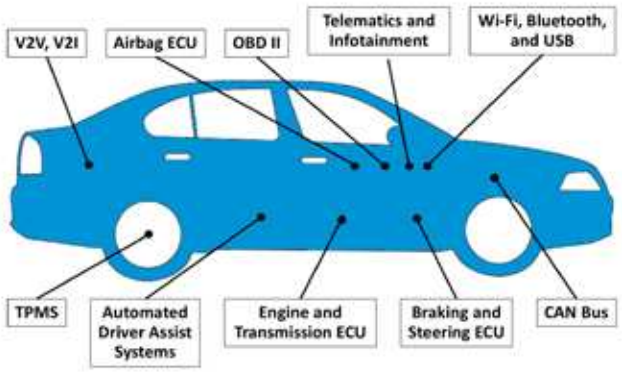
Known as "Uptane," this project is a collaboration between the University of Michigan Transportation Research Institute (UMTRI), Southwest Research Institute and New York University Tandon School of Engineering. The trio is working to solve the security and complexity issues related to the over-the-air distribution of software updates for major automotive manufacturers, suppliers and peripherally related companies.

CUSTOMER NEED

Many companies struggle with keeping software up to date, as many people have noticed while using their personal computers and mobile phones. Updates are provided frequently to ensure devices are reliable, bug-free and secure. However, software updates are a particularly useful attack vector for malicious individuals because it's far easier to manipulate update data stored in a distribution system that could then affect thousands of individual vehicles than focus on a single device. Automobile software security is critical because motor vehicles are part of the daily lives of millions of people worldwide.

APPROACH

The Uptane project's participants have met with representatives from more than 80 percent of the North American auto market and hold quarterly workshops to address issues and concerns. Additionally, a web forum was created to advance the industry discussion, accumulating more than 1,000 posts on more than 130 topics. The result of this outreach is a refinement on traditional update security designs and methodologies that innovate on the automotive software update security process by implementing new strategies such as compromise resilience.



Embedded ECUs and external connectivity in modern automobiles increases the risk of cybersecurity vulnerabilities.

BENEFITS

The Uptane solution is completely open and transparent—from design to sample source code. All output from the project may be fully reviewed and critiqued by interested parties. All concerns and comments are fed back into the design using an iterative process allowing for a maximum level of applicability across all plausible use cases within the automotive industry.

COMPETITIVE ADVANTAGE

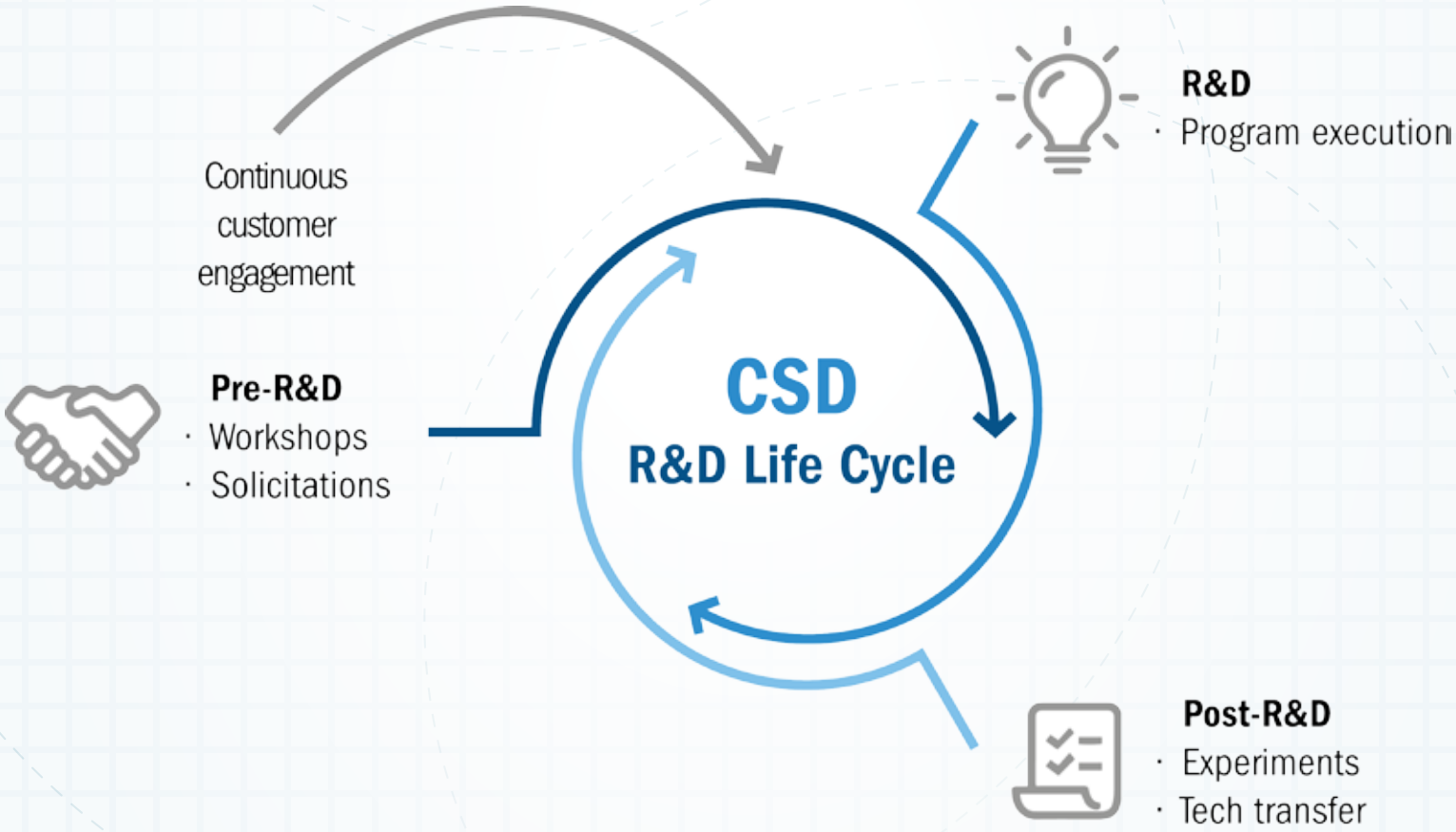
The Uptane workgroup also has begun the arduous process of standardization, allowing for professional review and collaborative refinement that provides further industry impact and the opportunity to have the results placed alongside all other industry-accepted technologies.

NEXT STEPS

Currently, Uptane is undergoing further testing by professional industry hacking teams to ensure sample source code and design implementations are functional and secure. Further deployment considerations such as the implications of using IT-related cloud providers, key provisioning, and logistics issues are being ironed out. For more information, visit https://uptane.org/.

GLOBAL CYBER CHALLENGES... AND THE SOLUTIONS WE PROVIDE

CSD is a leader in the federal government's efforts in funding cybersecurity R&D projects that solve hard problems and result in transforming an idea into a deployable solution. Through an aggressive cybersecurity R&D lifecycle process CSD produces solutions that address tomorrow's complex challenges and can be implemented in both Federal networks and the larger internet. The model comprises a continuous cycle of customer engagement, pre-R&D, R&D, and post-R&D activities oriented toward transition to practice.



CYBERSECURITY FOR LAW ENFORCEMENT

Autopsy: Enabling Law Enforcement with Open Source Software

Basis Technology

Brian Carrier
brianc@basistech.com

Megan Mahle, CSD Cyber Forensics Program Manager
Megan.Mahle@hq.dhs.gov

OVERVIEW

Autopsy is an open-source, digital forensics software that investigators use to determine how a digital device was used. The software has thousands of users around the world and supports all types of investigations—from fraud to terrorism to child exploitation. DHS S&T is funding development focused on building advanced analytic and framework features for law enforcement to use in conducting investigations. The results to date have been released to the public as features in the open-source program.

CUSTOMER NEED

Digital devices play a role in nearly every criminal investigation at the local, state and federal levels. This use means law enforcement organizations need an easy-to-use solution that can keep up with quickly changing devices at a time when their budgets are decreasing.

APPROACH

Basis Technology first surveyed state, local and federal law enforcement officials to identify their biggest challenges and where they spend the bulk of their investigative time. Several areas were identified and the development team worked with users to better understand their workflow and behaviors to automate that process. These features were incrementally released into the software. In addition to standard features that an investigator needs, the software offers a modular design for optimal flexibility.

BENEFITS

Current areas of focus are building a plug-in framework and analytics to support accounts and messaging, scaling the previously developed timeline and image gallery capabilities for multi-user environments, and collecting additional end-user feedback.

The new messaging framework is essential to allow investigators to more easily view data from the variety of messaging apps that are being used. The framework allows third-party module writers to make parsers for the various applications and easily integrate them into the Autopsy data model. This work also will build a link-analysis interface to make it easy to identify connections between individuals.

The timeline and image gallery modules were developed previously with funding from DHS S&T to establish a pattern of life and view large numbers of images. The additional work will enable collaboration among examiners in a multi-user lab.

COMPETITIVE ADVANTAGE

The project enhancements target ease of use and extensibility. Open-source modules add functionalities and promote flexibility to best suit an investigator's needs.

NEXT STEPS

Autopsy continuously is adding new features and other enhancements by engaging with a multitude of users to understand their needs and incorporate their feedback. By continuing to release these updates as open-source software, Autopsy's capabilities will be received by potential users far beyond the original focus group.

CYBERSECURITY OUTREACH

Comic-Based Education and Evaluation

Secure Decisions

Laurin Buchanan
Laurin.Buchanan@securedecisions.com

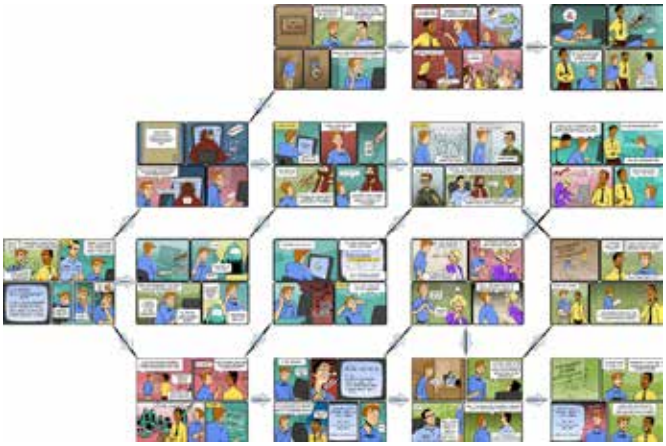
Edward Rhyne, CSD Cybersecurity Competitions Program Manager
Edward.Rhyne@hq.dhs.gov

OVERVIEW

Comic-Based Education and Evaluation (Comic-BEE) is a tool for educators, students, employers, subject matter experts and non-experts to teach or evaluate cybersecurity knowledge using branching, interactive stories. These branching stories, also known as web-comics, allow readers to make choices that determine a character's actions and the story's outcome. Readers can make decisions on topics related to cybersecurity and explore the consequences in the safe environment of a comic; no artists or programmers are needed to develop the branching interactive web comics.

CUSTOMER NEED

Building a cyber workforce demands new ways to teach, practice and evaluate cyber-skills. Users at all levels—from students to decision makers in the workplace—need to learn basic cyber concepts and strategic thinking about cyber-risks and tradeoffs. Explaining the causes and effects of cyber events is difficult because they do not occur in a context that is easily visualized. What is needed is a way to help people of all ages and backgrounds explore both risky and safe cyber-behaviors and see the consequences of choices made in a safe environment.



This illustration shows storylines branching from an initial decision. Readers start at the first panel and their decisions dictate which direction the story goes, allowing them to experience the varied outcomes and consequences of their choices.

APPROACH

Comic-BEE uses visual storytelling to help people comprehend the interaction of cause and effect of cyber events. Learners read the story and then make a choice that affects the storyline. To simplify and accelerate the creation and delivery of these interactive educational materials, the tool provides a unique system that enables those without programming or drawing skills to easily develop branching storylines using advanced automation technologies and pre-rendered art assets.

BENEFITS

Developing interactive graphic stories the traditional way is costly and time-consuming and requires specialized skills that present barriers to creation and dissemination. This tool automates the technically and artistically intensive aspects of production—from initial concept generation to the creation of graphical multi-path storyboards. Comic-BEE has integrated the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework, making it easy to align curricular materials with specific work roles and related tasks with knowledge, skills and abilities.

COMPETITIVE ADVANTAGE

There are no other known solutions for the easy creation of interactive cybersecurity storylines for educational and training purposes. This approach offers an advantage over traditional education and training methods because the interactive nature allows users to explore options and experience the consequences of their choices.

NEXT STEPS

Comic-BEE is available for piloting, testing and evaluation. Current development is refining and enhancing the user interface, expanding the graphic library, expanding automation to create full-color panels for web comics, and adding scoring capabilities to allow readers to demonstrate their cyber competence by achieving a high score.

CYBERSECURITY RESEARCH INFRASTRUCTURE

Internet Atlas

University of Wisconsin-Madison

Paul Barford
pb@cs.wisc.edu

Erin Kenneally, CSD Information Marketplace for Policy and Analysis of Cyber-risk & Trust Program Manager
Erin.Kenneally@hq.dhs.gov

OVERVIEW

Over the last seven years, University of Wisconsin-Madison researchers have developed Internet Atlas, a repository of geographically anchored representations of the physical internet infrastructure including nodes (e.g., colocation facilities), conduits/links and relevant meta data (e.g., source provenance) for more than 1,400 networks around the world. Internet Atlas also includes maps of other communications infrastructure systems such as data centers and cell towers. Customized interfaces enable a variety of dynamic (e.g., Border Gateway Protocol [BGP] updates, targeted traffic measurement and Network Time Protocol measurements) and static (e.g., highway, rail and census) data to be imported and layered atop the physical representation. Internet Atlas is implemented in a web portal based on an ArcGIS geographic information system, which enables visualization and diverse spatial analyses.

Map of the Internet's long-haul fiber optic infrastructure in the U.S. This map was extracted from the Internet Atlas repository.

CUSTOMER NEED

Internet Atlas customers are owners, operators or researchers of internet communication infrastructure who must ensure their infrastructures are reliable, performant, operational and secure. Internet Atlas offers a global representation that can extend what is found in typical network operation centers.

APPROACH

The Internet Atlas data repository was built using web-search to find primary source data, including maps and other public records such as conduit permits. This data is entered using a combination of manual and automated processes. The internet map data serves as the base representation in the Internet Atlas web portal. Also included is the ability to conduct targeted active probe-based measurement of Internet paths, visualize and assess BGP routing information, visualize other kinds of static data that is geocoded, and visualize and analyze other types of dynamic data (including customer-specific data imported via Internet Atlas's application programming interface [API]).

BENEFITS

Detailed maps of the internet are a unique starting point for assessing infrastructure risk and vulnerabilities, understanding routing and traffic behavior, designing and monitoring security infrastructures, and conducting forensic investigations of attacks and intrusions. Other benefits include a large, geocoded repository of internet physical infrastructure, an easy-to-use web portal for visualization and analysis, and a robust API for connections to other data sources.

COMPETITIVE ADVANTAGE

Internet Atlas is the largest repository of internet infrastructure maps. It features careful data curation and validation and a web portal for visualization and analysis of diverse data associated with internet maps.

NEXT STEPS

Internet Atlas is expected to be deployed in an operational setting and is seeking commercial partners. It also is available at www.ImpactCyberTrust.org.

DATA PRIVACY & IDENTITY MANAGEMENT

ReCon

Northeastern University

David Choffnes
choffnes@ccs.neu.edu

Erin Kenneally, CSD Data Privacy Program Manager
Erin.Kenneally@hq.dhs.gov

OVERVIEW

The combination of rich sensors and ubiquitous connectivity make mobile and internet of things (IoT) devices perfect vectors for invading end-user privacy and exfiltrating their data. ReCon addresses these problems by analyzing network traffic in real time to identify and block or change privacy leaks using machine learning without needing to know user personal information in advance.

CUSTOMER NEED

Applications extensively track users and leak their personally identifiable information (PII). This problem only will worsen as IoT devices are integrated into our daily lives. Improving privacy requires trusted third-party systems that enable auditing and control over PII leaks from devices that monitor users. However, previous attempts to address PII leaks fall short because they face challenges of a lack of visibility into network traffic generated by mobile devices and the inability to control the traffic.

APPROACH

A key observation is that a privacy leak must—by definition—occur over the network, so interposing on network traffic is a natural way to detect and mitigate PII leaks. Based on this insight, we use interposition on network traffic to improve visibility and control for PII leaks. ReCon analyzes network traffic in real time using machine learning to reliably infer when a flow contains PII, then allows users to block or change the leaked data.

Screenshots of the ReCon web app. The first screenshot shows the main ReCon page, the second shows what PII has been leaked and the third shows location leaks on a map.

BENEFITS

ReCon allows researchers to explore the potential of detecting privacy leaks from network flows without needing privileged access to devices, apps or Internet Service Providers. Rather, it uses software middle-boxes that run atop trusted servers (e.g., in a user's home network, in an enterprise network, on a mobile device or on a trusted cloud platform). ReCon allows individuals and enterprises to regain visibility into and control over the personal information leaking across their networks.

COMPETITIVE ADVANTAGE

Several efforts systematically identify PII leaks from mobile devices and develop defenses against them.

However, ReCon is the only one that relies only on network traffic, does not require a priori knowledge of PII that could be leaked, and is resilient to changes in PII leak formats over time. ReCon is the only solution that works independently of what device is used and can extend to cover IoT devices.

NEXT STEPS

The system already runs in cloud and enterprise environments and researchers are currently developing software that runs on home routers and mobile devices. In addition, they are evolving its PII detection to include leaks from IoT devices and are seeking partners for large-scale deployments.

Decentralized Key Management System

Evernym Inc.

Drummond Reed
drummond.reed@evernym.com

Anil John, CSD Identity Management Program Manager
Anil.John@hq.dhs.gov

OVERVIEW

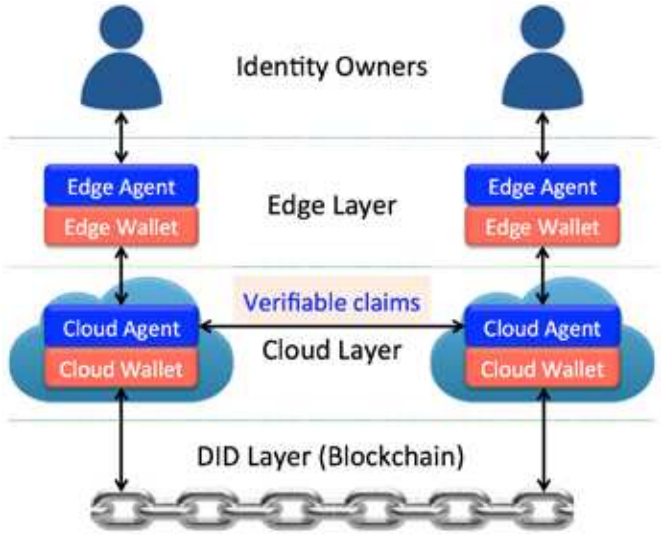
The Decentralized Key Management System (DKMS) is a new approach to cryptographic key management for blockchain and distributed ledger technologies (DLTs) that lack centralized authorities. DKMS inverts the assumption of conventional public key infrastructure (PKI) through which public key certificates are issued by centralized certificate authorities. With DKMS, the starting root-of-trust is any DLT that supports a decentralized identifier (DID).

CUSTOMER NEED

An X.509 public key certificate that is used for HTTPS-secure Web browsing is the most widely adopted PKI in the world. Yet the difficulty obtaining and managing these certificates means only a small fraction of internet users can use public-private key cryptography for identity, security, privacy, and trust management. A new infrastructure is needed that makes it easy for both individuals and organizations to generate, register, verify, rotate, retire, and recover public-private key pairs.

APPROACH

DKMS uses a three-layer architecture as depicted in the following diagram. The DID layer is based on the World Wide Web Consortium (W3C) specification for DIDs: cryptographically generated, globally unique identifiers that are self-registered on a compatible public or private blockchain (e.g., Bitcoin, Ethereum, Sovrin, Hyperledger). DIDs resolve to JavaScript Object Notation for Linked Data documents containing the public key(s) and endpoint(s) required to bootstrap secure communications. Trust in a DID is developed through the private, off-ledger exchange of verifiable claims: the W3C standard for digitally signed credentials verified by using the issuer's DID. Verifiable claims are exchanged using encrypted Peer-to-Peer (P2P) connections bootstrapped between DKMS agents at the cloud layer. Identity owners interact with DKMS at the edge layer, where most private keys are generated and stored in an edge wallet.



DKMS's three-layer architecture.

BENEFITS

DKMS removes central points of failure and creates a highly resilient and adaptable distributed key management infrastructure. DKMS enables broad cross-platform interoperability—any two entities can perform key exchange and create encrypted P2P connections without reliance on proprietary software or service providers. DKMS also enables robust key recovery, including agent-automated encrypted backup, key escrow services, and social recovery of keys from trusted DKMS connections.

COMPETITIVE ADVANTAGE

DKMS offers the same interoperability advantage as the internet. The project will leverage this advantage as an early vendor of DKMS-compliant products and services.

NEXT STEPS

DKMS is being developed as a community specification following the requirements set forth in NIST Special Publication 800-130, "A Framework for Designing Key Management Systems." The project is developing a prototype of edge agents and cloud agents in the open-source Hyperledger Indy project. The prototype will be available for proof of concept deployment in early 2018.

Verifiable Claims and Fit-for-Purpose Decentralized Ledgers

Digital Bazaar

Manu Sporny
msporny@digitalbazaar.com

Anil John, CSD Identity Management Program Manager
Anil.John@hq.dhs.gov

OVERVIEW

While distributed ledger technology (DLT, a.k.a. blockchain) holds promise in addressing problems with identity management, most have been rigidly coupled to financial applications. This rigidity makes it challenging to repurpose existing DLTs to address identity management use-cases. The Verifiable Claims and Fit-for-Purpose Decentralized Ledgers project has developed a modular and standards-based approach, building a technology stack that is capable of producing many instances of fit-for-purpose DLTs to solve a wide variety of problems at scale.

Credential information is issued to digital wallets and ledgers and its authenticity and status verified at a later date.

CUSTOMER NEED

This project addresses the need to issue digital credentials such as employee badges or customer ID cards and securely store and access the credentials via a mobile device. Customers also need to share data among groups of organizations in a way that is both tamper-proof and auditable. Both needs can be achieved with this ledger application platform.

APPROACH

The software ecosystem can be narrowly tailored toward a particular use-case, including or excluding various modules or feature sets such that domain-specific solutions can be rapidly generated and deployed. The software is built on international web standards, ensuring that it has been thoroughly vetted and that customers are not locked into the solution.

BENEFITS

The modular nature of the technology produces solutions that are more effective and secure. Modularity enables systems to be readily adapted to the task at hand, while reducing the product's attack surface. Customers can securely issue digital credentials using Web-based technologies that are available on almost all smartphones without the need for application installation and then record the status of credentials (e.g., revocation information) in a blockchain thus eliminating the need to provide 24-7 uptime guarantees for issuing systems.

COMPETITIVE ADVANTAGE

The project's Ledger as a Service (LaaS) platform is capable of storing a wide variety of information via the use of Linked Data technology. Its modular architecture results in simpler and more robust solutions that are less susceptible to problematic hacks and dangerous dependencies compared to public blockchains like Bitcoin and Ethereum.

NEXT STEPS

The performer is using its LaaS platform to execute multiple pilots. The next step is to commercialize the technology across multiple market verticals. The platform site can be viewed at https://veres.io/.

Mobile Device and Attributes Validation

Lockstep Technologies LLC

Stephen Wilson
swilson@lockstep.com.au

Anil John, CSD Identity Management Program Manager
Anil.John@hq.dhs.gov

OVERVIEW

Mobile Device Attributes Validation (MDAV) helps first responders prove their bona fides in the field. First responders usually must present permits, licenses or certifications on plastic or paper cards. Mobile technology has long been a possibility for digital credentials, but integrity and authenticity—in other words, provenance—have been missing, until now.

CUSTOMER NEED

First responders need to present robust digital versions of their qualifications in demanding circumstances with little or no network bandwidth. And, their credentials need to be validated quickly and accurately by field officers. Provenance is vital. Field officers need to know that a visitor's credentials are genuine, issued by a recognized organization, and safeguarded in a DHS-approved device.

APPROACH

Digitally mimicking traditional credentials is a challenge. Visual signs of a plastic card's integrity must be replaced by cryptographic provenance. To do this, MDAV uniquely reconfigures regular public key infrastructure (PKI) certificates to encapsulate attributes and presents them securely and directly from one mobile application (app) to another. Standard public key cryptography is used in the secure elements of approved devices. Each credential issuer is faithfully identified in the capsule, allowing for fine-grained, attributes-based access control in the field.

BENEFITS

MDAV capsules replicate conventionally issued credentials, including their issuers, but cannot be cloned, counterfeited, tampered with or loaded to unapproved devices. The capsules are customized certificates, but unlike traditional PKI MDAV places no new demands on an issuing organization's processes. Capsules are presented directly from one MDAV app to another and cryptographically verified locally, quickly and accurately. If appropriate, capsules can be entirely anonymous for application in sensitive applications like e-health and voting.

The MDAV app holds a digital wallet of first responder capsules, each holding a validated attribute or credential specifying the issuer.

COMPETITIVE ADVANTAGE

MDAV is the only solution that preserves the provenance of attributes in mobile devices. The origins of credentials and other personal details are assured as is the approval status of the devices. The simple fact that someone has a certain credential is accurately replicated by MDAV without any change to the trusted processes of the issuing organization.

NEXT STEPS

MDAV will complete internal testing by the end of 2017 and commercialization is planned through 2018. The technology is applicable to many use-cases to carry the bona fides of individuals in mobile devices. Major opportunities for this capability include electronic travel documentation, driver licensing, e-health, online payments, national ID, and the internet of things.

NFC4PACS: NFC and Derived Credentials for Access Control

Exponent, Inc.

John Fessler, Ph.D., P.E. CSCIP
jfessler@exponent.com

Anil John, CSD Identity Management Program Manager
Anil.John@hq.dhs.gov

OVERVIEW

The performer has implemented a rapid-encryption protocol called Opacity to quickly, conveniently and securely derive a credential on a mobile phone that is bound to a user's personal identity verification (PIV) card. This credential is used to quickly authenticate to a PIV-compliant Physical Access Control System (PACS) or other near-field communication (NFC)-enabled phones.

CUSTOMER NEED

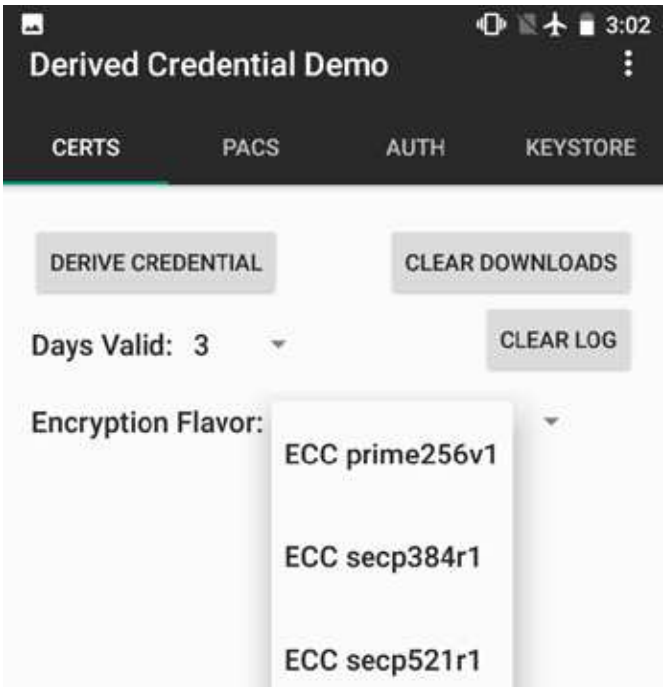
Federal employees have been using PIV cards for many years, but with the widespread use of smart phones and the desire to work remotely, employees want to replace their PIV card with their phone for day-to-day uses for both remote logical access and physical access.

APPROACH

The protocol uses a mobile phone's NFC interface to pull information from the PIV card and then uses that same card to digitally sign the new credential on the phone, thus binding the new credential to the original card. The Opacity protocol is used to establish a secure, encrypted communication channel in 300 milliseconds (ms). The entire credential-generation process takes about 2.2 seconds or less. The new credential is authenticated over the encrypted Opacity tunnel by either a NFC-capable PACS reader or another NFC phone. The user simply holds the phone with the credential up to the reader device and communications are automatically directed to the derived credential in the native Android key-store for authentication via public key infrastructure (PKI) challenge-response in approximately three seconds. For convenience, service runs in the background and the user does not need to select any application for the authentication to occur.

BENEFITS

Compelling benefits and use-cases for generating and authenticating derived credentials include such situations as a lost or stolen PIV card, denied physical access for those without PIV cards (e.g., visitors or volunteers) and mobile-to-mobile authentication where a PACS reader is not installed (e.g., at a checkpoint).



Screen capture from the Derived Credential generation portion of the demonstration app illustrating the different versions of encryption available to the user when creating the new derived credential.

COMPETITIVE ADVANTAGE

By using Opacity, contactless authentications can be performed quickly and securely. It requires only about 300 ms to establish an encrypted Opacity tunnel, after which all subsequent communications are secure. Opacity is codified in standards (American National Standards Institute Code 504 and National Institute of Standards and Technology Special Publication 800-73-4) and is available without royalties.

NEXT STEPS

The next step will be to extend the Opacity protocol and authentication process to Bluetooth. This step will expand the ecosystem to non-NFC mobile devices and enable authentication across all platforms and bring-your-own-device applications. The source code for all demonstrations is available as open source at: https://github.com/pivopacity, so agencies and vendors can quickly adopt the technology into their programs.

HOMELAND OPEN SECURITY TECHNOLOGY

Security Control Compliance Server

GovReady PBC

Greg Elin
gregelin@govready.com

Vincent Sritapan, CSD Homeland
Open Security Technology Program Manager
Vincent.Sritapan@hq.dhs.gov

OVERVIEW

The Security Control Compliance Server does for cybersecurity compliance paperwork what tax preparation software does for filing taxes. It provides a self-service portal to help teams build, authorize and operate secure and compliant IT systems. The innovative "compliance apps" map IT system components to security controls to automatically generate System Security Plans (SSP) and Authority to Operate (ATO) artifacts.

CUSTOMER NEED

Current compliance processes aren't keeping pace with the velocity of modern software development and delivery. Handwriting documents is too slow and interpreting National Institute of Standards and Technology (NIST) Special Publication 800-53 controls for IT systems takes too long. Small businesses and fast-moving innovators need a faster, more automated way to navigate the complexities of the NIST Risk Management Framework and ATO process.

APPROACH

The Security Control Compliance Server uses the familiar metaphor of an app marketplace to make compliance easier and more automated. Compliance apps are reusable data components that link together to form a complete picture of the IT system and the steps needed to obtain an ATO. Compliance apps represent both technical system components like software products and data centers and organizational processes like policy and training. A user can select a Drupal website app, an Amazon Web Services app, or a privacy policy app and then answer questions in each app to have their ATO artifacts generated automatically.

BENEFITS

The benefits of the compliance server include easier tailoring of NIST 800-53 controls to specific types of IT systems, guiding teams step-by-step through the ATO process without having to read jargon-laden government documents, automatically generating and maintaining SSP and ATO artifacts, aligning with the devops continuous integration and continuous delivery pipeline, and collecting information automatically from system components to update artifacts continuously.

Each app in the Security Control Compliance Server app marketplace is a data package that maps an IT system component onto a set of security controls of a compliance framework.

COMPETITIVE ADVANTAGE

The performance team consists of data management and user-experience experts who build tools that are easier to use and offer more productive information management. Unlike most compliance automation software that simply aggregates control descriptions or scans technical controls and still requires individuals to spend hours interpreting controls and writing implementation descriptions, the Security Control Compliance Server app prewrites the controls and guides teams through the process, including preparing various documents like continuity of operations and incident response plans. The software is open-source to make customization and community contribution easier.

NEXT STEPS

The next step is using feedback from early customers in government and the private sector to improve the software and begin outreach to technology vendors to develop more compliance apps.

HUMAN ASPECTS OF CYBERSECURITY

Lightweight Media Forensics for Insider Threat Detection

University of Texas San Antonio

Nicole Beebe
Nicole.Beebe@utsa.edu

Megan Mahle, CSD Insider Threat Program Manager
Megan.Mahle@hq.dhs.gov

OVERVIEW

This research pioneers a new approach for detecting hostile insiders by looking for individuals whose information browsing and data handling behavior diverges from their prior behavior and/or that of their coworkers. A host-level, lightweight service collects a forensic, privacy-preserving profile and securely transmits it to the analytics server. Novel anomaly detection algorithms and advanced analytics identify unusual statistical properties, prompting further monitoring and/or analysis. The key advantages of this approach are its abilities to detect preparatory actions before exfiltration and insider behavior independent of whether files are saved to disk.

CUSTOMER NEED

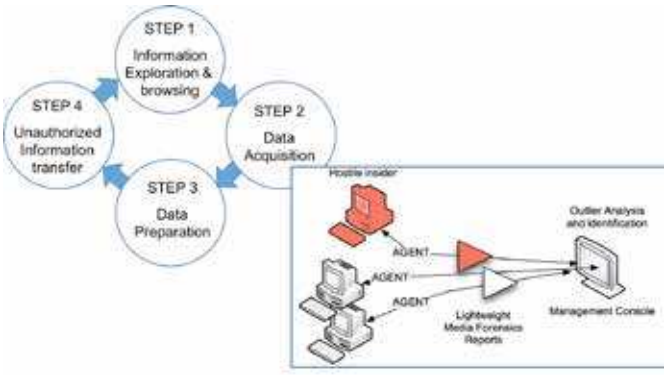
Insiders frequently browse and collect sensitive information prior to exfiltration, particularly in cases involving espionage and theft of intellectual property. Organizations need an indication and warning of such activity much earlier than currently is possible with prevailing data loss prevention (DLP) and security information and event management (SIEM) tools. Too often, data exfiltration becomes known after the fact, at which time the compromise already has occurred and the damage is done.

APPROACH

This project pioneers a new approach that profiles forensic traces of data browsed and/or collected by a user to detect users in the process of curating data before exfiltration. It looks for forensic traces that result from user interaction with various file types, file classes, data types and string classes. It integrates several open-source tools and is built on an ElasticSearch, Logstash, Kibana (ELK) stack framework. The system creates a privacy-preserving profile of user behavior and leverages new, robust anomaly detection algorithms to determine when user behavior deviates from a prior norm or from peers.

BENEFITS

Benefits over existing approaches are it is data-focused, not quantity- or quota-dependent. The forensic traces are not limited to saved data; it can recover forensic traces in free space. This approach is highly scalable and employs privacy-preserving protections. Perhaps most importantly, it is anomaly-based, not signature-based, so it can detect insiders who perpetrate their crimes in new ways.



Many insiders follow a common four-step process to curate data in preparation for exfiltration (shown as the upper graphic, Maasberg 2014). The proposed system detects hostile insiders by detecting anomalous amounts of forensic traces from the data curation process, alerting organizations to impending exfiltration before it occurs (shown as the lower graphic).

COMPETITIVE ADVANTAGE

Its competitive advantage over prevailing DLP- and SIEM-based insider threat detection approaches is it neither relies on fragile file hashes, nor computationally expensive similarity hashes. It transcends string matching and regular expressions as well as business heuristics and cumbersome, unreliable policy discovery.

NEXT STEPS

The technology has undergone operational testing and evaluation in two real-world organizations: one a critical infrastructure entity and one financial institution. It will be ready for commercialization midyear 2018. The approach could be extended with additional research and development to monitor other data transport mechanisms (e.g., web and email) or include other forensic trace "signals" such as knowledge-access mapping.


MOBILE SECURITY
CYBER SECURITY

iSentinel: Mobile Device Continuous Authentication

HRL Laboratories LLC

Dr. Vincent De Sapio
vdesapio@hrl.com

Vincent Sritapan, CSD Mobile Security R&D Program Manager
Vincent.Sritapan@hq.dhs.gov

OVERVIEW

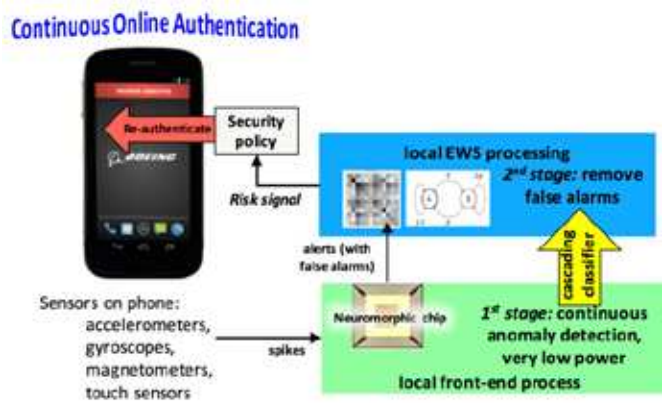
With the ever-increasing role of mobile devices in the government workplace and general U.S. population, significant challenges have arisen related to maintaining device physical security. To address these challenges, the performer is developing iSentinel—a breakthrough, low-power, cascading, anomaly-detection system that provides unobtrusive and continuous, behavior-based authentication for mobile devices. The combination of these features provides an easy-to-use, breakthrough platform for government and commercial use.

CUSTOMER NEED

Maintaining security of mobile devices to prevent loss or theft is of paramount importance for government employees and the general population. Security lapses include when a device has been authenticated by the authorized user and subsequently falls into the hands of another party. A secure system is needed to detect if someone else is using the device. To achieve this, continuous, behavior-based authentication using signatures learned from the authorized user by monitoring device sensors is required. Due to the continuous nature of the monitoring and authentication, low-power classification of sensors streams also is needed.

APPROACH

The technology's power-efficient, neuromorphic hardware exploits brain-inspired adaptation for continuous sensor-agnostic online learning and classification of user behaviors. Security alerts from this frontend process activate the novel early-warning system (EWS) algorithms running on the local mobile device processor for improved analysis. This cascading classification approach combines the power efficiency of neuromorphic hardware with intermittent EWS classification to eliminate false alarms.



iSentinel Architecture

BENEFITS

ISentinel represents a significant new way to prevent unauthorized use of a mobile device with minimal drain on power or computing resources. Re-authentications are required only after a sophisticated multi-stage analysis. The methods continuously analyze multiple streams of sensor data in real-time from two different perspectives: spiking neural networks and analysis of behavioral transitions. Thus, the system raises the level of security with minimal impact on user experience.

COMPETITIVE ADVANTAGE

Unlike existing state-of-the-art technologies that train their classifiers on specific sensors for user identification and authentication, the iSentinel approach adapts to inputs from many sensors, conducting adaptive multi-stage analyses with significantly reduced power consumption. This power efficiency enables the system to continuously analyze data from multiple sensors with minimal user impact.

NEXT STEPS

The next steps will involve developing a miniaturized version of the first-generation neuromorphic board and interface backplane so these adhere to the form factor of a smart-phone. Additionally, the performer will port the development EWS code to the Android operating system for integration with a smartphone.

Mobile App Software Assurance

Kryptowire LLC

Dr. Angelos Stavrou
info@kryptowire.com

Vincent Sritapan, CSD Mobile Security R&D Program Manager
Vincent.Sritapan@hq.dhs.gov

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 security and privacy risks introduced by third-party mobile apps that have not been vetted. Kryptowire has developed a technology for automatically testing mobile applications for compliance with the highest federal government and industry security standards.

CUSTOMER NEED

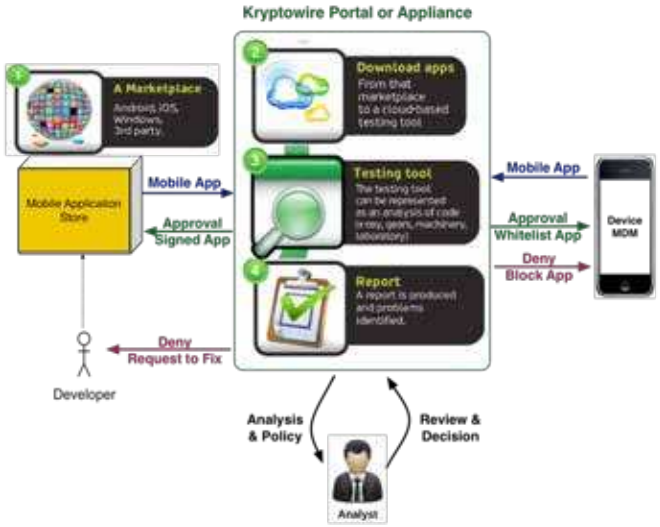
Smartphones and tablets enable government employees to access and process sensitive data through proprietary and third-party mobile apps. While apps help government employees better serve their agency's mission, government agencies must ensure mobile apps do not introduce unacceptable risk to sensitive data and network resources. They also must be able to analyze the security and privacy implications of the mobile apps and to verify compliance with enterprise IT security and privacy policies.

APPROACH

The mobile application analysis system enables the automated, large-scale analysis of mobile application binary and source code as well as any Java or native code and libraries. The security analysis results are presented in a detailed application report that is accessible through a web-based portal. Pass-fail evidence is provided with attribution to the code level. The results also are available through an application programming interface for direct integration with major Mobile Device Management (MDM) systems and other security technologies.

Benefits

Government agencies can automatically vet mobile applications for security and privacy compliance without access to third-party developer source code. The system will assess mobile applications based on the following internationally recognized standards:



Overall system operations.

- National Institute of Standards and Technology (NIST) Special Publication SP800-163, "Vetting the Security of Mobile Applications"
- National Information Assurance Partnership (NIAP) Protection Profile for Application Software

The technology assists and reduces the time for an analyst to assess the security posture of an app. Moreover, it offers testing and protection profiles for different use-cases and user groups as defined by the testing organization.

COMPETITIVE ADVANTAGE

The mobile application analysis portal allows government agencies to have control, accountability and transparency over the mobile app vetting and risk-scoring process; test for compliance with NIST and National Security Agency guidelines; and integrate the analysis results into other mobile application and device management technologies.

NEXT STEPS

Kryptowire is working with MDM vendors to further automate the remediation of mobile applications that do not meet relevant security and privacy policies.

Quo Vandis: Mobile Device and User Authentication Framework

Kryptowire LLC

Dr. Angelos Stavrou
info@kryptowire.com

Vincent Sritapan, CSD Mobile Security R&D Program Manager
Vincent.Sritapan@hq.dhs.gov

OVERVIEW

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

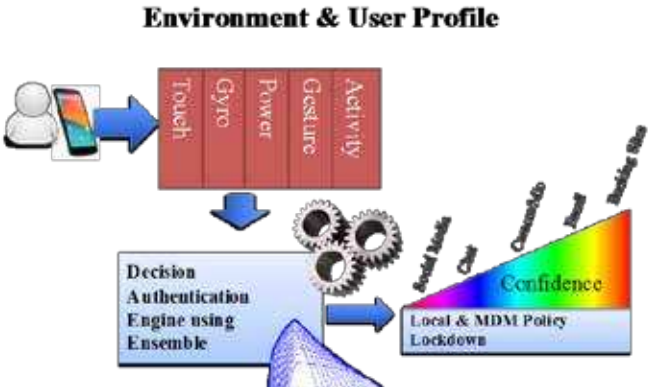
CUSTOMER NEED

Passwords have been proven to be ineffective in computing environments and even more challenging to work with on mobile devices. 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 security levels as a user seeks work-arounds to bypass password-based security controls. Moreover, passwords alone cannot solve the impostor problem when a device is lost and cannot take policy or mission parameters into consideration. The National Institute of Standards and Technologies (NIST) currently is evaluating new approaches to remote user-authentication and recommending the use of passwords for only low-value assets.

APPROACH

This technology 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 communications, Bluetooth, power, movement and touch measurements while the user operates a mobile device.

Its Authentication Decision Engine weighs data from all the sensor modalities, the current device state, ongoing user activities, existing user-device profile and historical data, the device operating environment, local and MDM policies to render continuous permission and authentication decisions.



The Quo Vandis framework.

BENEFITS

Quo Vandis addresses the limitations of password-based device user-authentication and takes advantage of wide-raging sensor data available on today's commercial off-the-shelf smartphones to offer seamless, robust and extensible mobile device user-authentication.

COMPETITIVE ADVANTAGE

This 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, it 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.

NEXT STEPS

The company will begin piloting the technology with commercial partners for Department of Defense customer use-cases. The company currently is partnering with Qualcomm to demonstrate the integration of the technology with a platform on which mobile application security can be anchored in mobile device hardware. This joint effort will demonstrate the continuous validation of the security of third-party mobile apps and services.

Remote Access for Mobility via Virtual Micro Security Perimeters

Rutgers University

Dr. Saman Zonouz
saman.zonouz@rutgers.edu

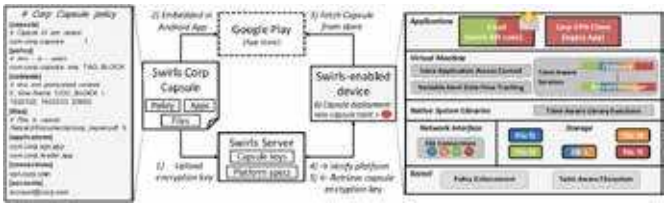
Vincent Sritapan, CSD Mobile Security R&D Program Manager
Vincent.Sritapan@hq.dhs.gov

OVERVIEW

This project provides first-class data protection for applications and operating systems that uses a novel value-based information flow-tracking and cryptographic policy enforcement to isolate data instead of execution environments. This solution does not require a modified operating system or apps. Consequently, government and enterprise personnel can use their devices for various purposes involving sensitive data with different security requirements. The solution has been submitted for a patent, released as a working prototype and published at top conferences.

CUSTOMER NEED

The only line of defense against accidental or malicious sensitive data leakage is through isolation of execution environments, e.g., virtual smartphones. For users, these multiple environments present a fragmented and often inconsistent experience that increases cognitive effort. In cases where system resources such as camera, microphones or location are concerned, container-based approaches fail entirely.



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. the solution 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.

APPROACH

The research team has developed a user-transparent and lightweight system-wide dynamic data isolation. It dynamically tags data based on its security context as embodied in a capsule and controls data mixing between capsules using dynamic information flow tracking and cross-application policy enforcement. Our prototype delivers 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

The solution 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

It outperforms existing solutions by addressing two key considerations: First, 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. Second, high-performance overhead—guarantees context isolation; almost all existing solutions duplicate a full subset of system resources.

NEXT STEPS

The researchers have implemented a fully operational prototype and the patent application has been accepted by the U.S Patent & Trademark Office. The source code for the solution is released via open-source license and available on Bitbucket (https://bitbucket.org/androidswirls/) for use by researchers internationally. The next step is to take the necessary steps toward transfer of the prototype to industry and government clients. The researchers will talk with industry partners regarding potential adoption of the solution for their data-security and privacy-compliance purposes.

TrustMS: A Trusted Monitor and Protection for Mobile Systems

Intelligent Automation, Inc.

Dr. Guang Jin
gjin@i-a-i.com

Vincent Sritapan, CSD Mobile Security R&D Program Manager
Vincent.Sritapan@hq.dhs.gov

OVERVIEW

The state of a mobile software program is determined by its code and data segments. While many mobile security solutions only protect the integrity of a static code segment, TrustMS protects the dynamic data segment. Based on hardware-level security features, the key components of the technology are isolated from potential software-based attacks. The solution has been applied to enhance the security level of software components running at different privilege levels. The benchmark results confirmed TrustMS is effective against real-world cyber-attacks with indiscernible performance differences.

CUSTOMER NEED

Most mobile security issues are rooted in software vulnerabilities (i.e., flaws made by developers). Since current software programs are large and complex, a manual or semi-automatic vulnerability-finding approach is typically error-prone and cannot fix all vulnerabilities. A fully automatic method is needed to enhance the security of mobile programs to ensure each program is free from software flaws (or when a software vulnerability is being exploited, the exploit can be easily detected and mitigated).

APPROACH

The technology consists of two major components. Its offline instrumentation engine inserts security check code into target-vulnerable programs and optimizes the instrumented code through the static analysis. A runtime, multi-core security monitor dedicates a Central Processing Unit (CPU) core to monitor instrumented programs executed by other CPU cores to reduce overheads. The solution also leverages ARM's TrustZone to increase the security level.

BENEFITS

Mobile system developers can use TrustMS to automatically enhance the security of produced mobile software. As normal cores execute the instrumented programs, the inserted security code instructs the normal cores to report the security properties to the secure core. If a software program is being exploited, the secure core can detect the attack and take further mitigation actions.

COMPETITIVE ADVANTAGE

TrustMS provides a fully automatic security enhancement and avoids error-prone manual or semi-automatic vulnerability finding methods. The solution has been applied to software programs running at different privilege levels with indiscernible runtime overheads. For example, it protected the control-flow integrity of an Android/Linux kernel running on actual ARM platforms.

NEXT STEPS

The next steps will be the development, certification, accreditation and piloting of TrustMS onto a commercial-off-the-shelf mobile system. The performer will seek commercialization and collaboration opportunities to apply it to other software systems as well. Given that the solution has been applied to the complicated Android/Linux kernel, it is anticipated the technology's transition to other platforms will be smooth and flexible.

Virtual Mobile Infrastructure

Hypori

Sanjay Challa
Support@hypori.com

Vincent Sritapan, CSD Mobile Security R&D Program Manager
Vincent.Sritapan@hq.dhs.gov

OVERVIEW

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

CUSTOMER NEED

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

APPROACH

The technology's unique approach is to avoid deploying sensitive assets to the mobile device entirely. Instead, with a virtual mobile smartphone that runs in a secure datacenter, users can rely on a simple thin client mobile app to connect and stream data to the screen of the secure virtual smartphone. With this virtual mobile infrastructure, organizations can enable mobile access while keeping all sensitive data and apps safe in a secure datacenter.

BENEFITS

This approach enables:

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

COMPETITIVE ADVANTAGE

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

NEXT STEPS

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

Ho eland Security
Science and Techn l y

DHS S&T Cyber Security Division

Securing YOUR Cyber Future

Our Mission is to:

DEVELOP & DELIVER

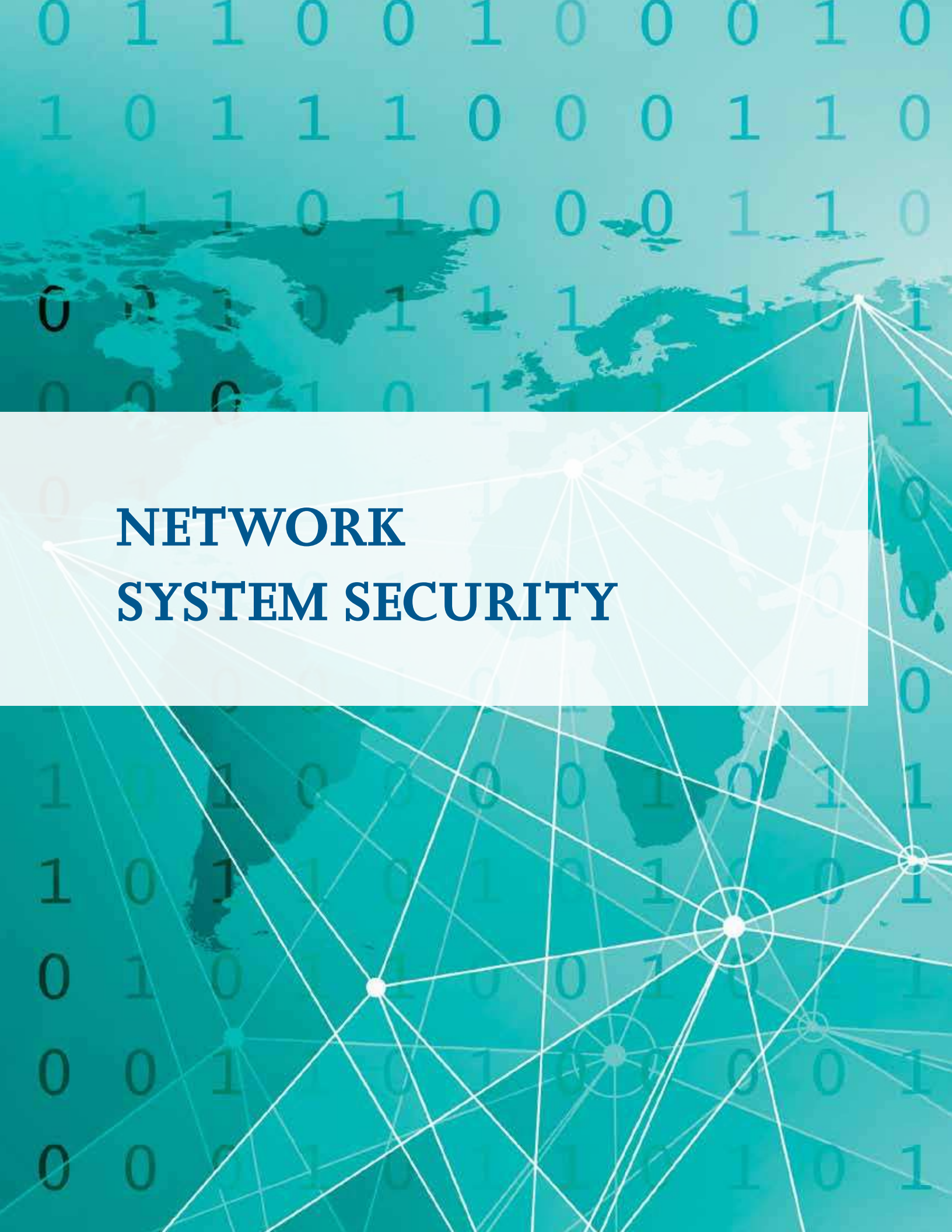
Develop and deliver new technologies, tools, and techniques to enable customers to defend, mitigate, and secure current and future systems, networks, and critical infrastructure against cyber attacks.

TRANSITION

Conduct and support technology transition and approaches across the HSE by identifying mature technologies that address existing or imminent cybersecurity gaps.

LEAD & COORDINATE

Lead and coordinate research and development among DHS components and customers, other government agencies, academia, private sector, and international partners within the cybersecurity community.



NETWORK SYSTEM SECURITY

ImmuneSoft

BlueRISC

Jeff Gummeson
jeff@bluerisc.com

OVERVIEW

ImmuneSoft is a hybrid static-and-runtime approach to detecting and healing vulnerabilities in embedded systems. A static vulnerability-centric characterization is performed offline and used to drive detection and healing at runtime. Attempts to attack protected systems are detected prior to exploitation, preventing sensitive data from being leaked or malicious modifications from being made.

CUSTOMER NEED

With the proliferation of the internet of things, the role of embedded systems has grown substantially in recent years. These systems increasingly are used to perform critical tasks—ranging from controlling critical infrastructure to managing communications to controlling medical devices. The use of embedded systems in performing these tasks has incentivized a growing number of attacks against them. Their defensive capabilities, however, are limited due to their embedded nature.

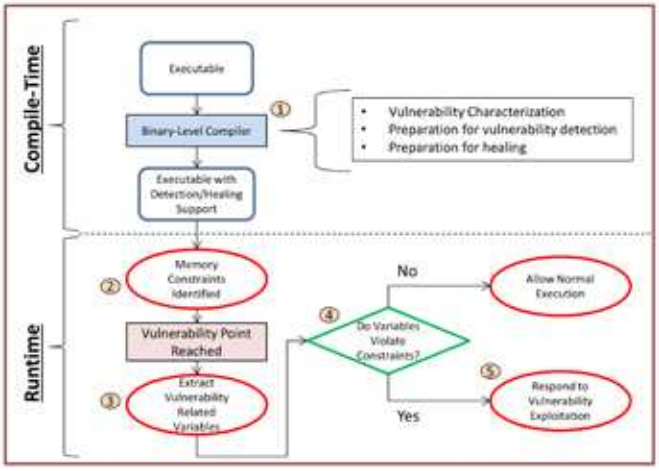
APPROACH

The technology is a hybrid approach spanning both static binary analysis and a runtime healing system. It relies on generic program analyses to perform a vulnerability-centric characterization of embedded software at the binary level based on requirements for carrying out an exploit against the system. This vulnerability characterization is tightly coupled with a runtime exploitation detection and healing system that identifies when vulnerable codes are attacked and heals them prior to exploitation.

BENEFITS

Due to the generic nature of its program-analysis-based vulnerability characterization, the technology is applicable to a wide range of vulnerabilities—no specific knowledge about a vulnerability is required to heal it. Its runtime system enables detection of "silent" vulnerabilities, which do not make system modifications and otherwise go undetected. Its vulnerability characterization is performed at the binary level and is fundamental and conceptually generic, making it applicable to a wide range of embedded central processing units as well as legacy systems.

Dr. Ann Cox, CSD Application of Network Measurement Science Program Manager
Ann.Cox@hq.dhs.gov



ImmuneSoft's system architecture.

COMPETITIVE ADVANTAGE

By using a hybrid approach based on fundamental characterization, it does not suffer from the deficiencies of static-only (e.g., unaware of runtime dataflow) or runtime approaches (e.g., based on integrity validation). This approach translates into a solution that is not only feasible but applicable to modifying and silent vulnerabilities, while having minimal performance and code-size overhead.

NEXT STEPS

A toolkit associated with the technology currently is being implemented. This toolkit will support healing and provide a vulnerability-centric visualization of embedded software as well as reporting identified potential exploitation paths. The performer is seeking partners to evaluate the approach and exploring use-case and piloting opportunities.

Science of Internet Security Technology and Experimental Research

University of California San Diego

KC Claffy
kc@caida.org

Dr. Ann Cox, CSD Application of Network Measurement Science Program Manager
Ann.Cox@hq.dhs.gov

OVERVIEW

The Science of Internet Security: Technology and Experimental Research (SISTER) project builds on the DHS- and National Science Foundation-funded Archipelago (Ark) secure-measurement platform that supports large-scale, active measurement studies of the global internet. This project is enhancing both scientific understanding and technical capabilities in the measurement of security-relevant properties and behavior of the internet.

CUSTOMER NEED

The opacity of internet infrastructure limits the capabilities of research and development (R&D) efforts to model network behavior and topology, design protocols and/or new architectures, and study real-world properties such as robustness, resilience and economics. Overcoming these limitations is impossible without realistic and representative datasets and measurement infrastructure on which to support sustained longitudinal measurements as well as new experiments.

APPROACH

This project combines a series of targeted activities that demonstrate and illuminate the capabilities of the current infrastructure to address specific articulated needs of the extended DHS Science and Technology Directorate R&D community. Researchers are focusing current efforts on inferring and analyzing internet security and stability problems, e.g., connectivity disruptions and route hijacking. For each activity, they leverage the current platform's flexibility, versatility and coordination functionality combined with key external data sources (e.g., Border Gateway Protocol, Domain Name System and geolocation data).

BENEFITS

The project results will support macroscopic security and stability monitoring through 24/7 reachability probing of the entire Internet Protocol version 4 (IPv4) routed address space, map peering interconnections at the router and facility levels, improve inference of ownership of border routers, measure Transmission Control Protocol (TCP) behavior to understand and report on security vulnerabilities, infer grey market IPv4 address transfers, and enable on-demand mapping and querying of internet router-level topology data.

COMPETITIVE ADVANTAGE

Using the Ark infrastructure, the Center for Applied Internet Data Analysis (CAIDA), has gathered the largest set of network topology data available to academic researchers. This infrastructure and data is used by networking and security researchers for a broad spectrum of research—from internet vulnerability assessments to theory of complex networks.

NEXT STEPS

SISTER will apply the results of previously developed technologies and measurement capabilities. It will study, document, analyze and explain structural and dynamic aspects of the internet infrastructure relevant to cybersecurity vulnerabilities—from global scale to individual networks.

Locations of 181 Ark vantage points in 60 countries (July 2017), with 135 Raspberry Pis (blue) and 83 nodes running Internet Protocol version 6. Tables show node distributions by region and organization type.

Systemic-Risk Assessment Tools for Cyber-Physical -Human Infrastructures

Brigham Young University

Sean Warnick
sean@cs.byu.edu

Dr. Ann Cox, CSD Application of Network Measurement Science Program Manager
Ann.Cox@hq.dhs.gov

OVERVIEW

This project leverages systematic methods for evaluating cyber-physical-human systems and identifying weak points that could destabilize, hijack or infer critical state information about a system. Results include enhanced situational awareness, vulnerability assessment, countermeasure development and counterfactual exploration.

CUSTOMER NEED

Critical infrastructure is typically large-scale physical systems with an essential information technology component for computation and communication for distributed decision processes such as the smart grid. These systems often are connected to the internet with a human-in-the-loop integral in system operation. Because of this complexity, it is difficult to understand what information within these systems is most influential to its core functionality. Knowing where an enemy would target a system if they could access anything—attacks ranging from operating less profitably than a competitor to critically damaging components and triggering cascading failures—helps management know what parts of the system need to be protected and why those protections are necessary.

APPROACH

The methodology determines mission impact by design and begins by targeting a particular cyber-physical-human system and identifying system variables that may be exposed and vulnerable to attack. The dynamic, causal relationships between variables are identified using sophisticated system-identification or machine-learning techniques when necessary, producing an operational model of the system's attack surface. This attack surface is used to design attacks based on particular mission-focused objectives and assumed constraints. Objectives may include destabilization, state hijacking or inference. Constraints on the attack limit its operational capabilities such as restricting it to a single-link attack on an existing link versus a multiple-link, coordinated attack. Countermeasures are identified and counterfactual scenarios also can be explored.

BENEFITS

This method enables design-for-security instead of security-as-an-afterthought. Future designs can be analyzed before they are built and redesigned to change the system's inherent security properties if necessary. The analysis is completely intrinsic, depending only on the system's information architecture, not technologies assumed to be available externally to outsiders such as currently known exploits supported by particular communications protocols or software platforms. As a result, the analysis is technology-neutral, yet specific to the particular way the system processes and moves information. Early work has demonstrated this methodology on critical infrastructure systems, including water-management systems, cyber-enabled precision agriculture systems, multi-agent vehicular swarms, air traffic control systems, chemical processing, manufacturing and order-book manipulation in equity markets.

NEXT STEPS

Systemic-risk assessment tools for cyber-physical-human infrastructures are available for pilot deployment as well as alpha testing on a specific critical infrastructure system.

Trinocular: Detecting and Understanding Outages in the Internet

University of Southern California/Information Sciences Institute

John Heidemann
johnh@isi.edu

Dr. Ann Cox, CSD Application of Network Measurement Science Program Manager
Ann.Cox@hq.dhs.gov

OVERVIEW

Many factors cause internet outages—from big events like Hurricane Sandy in 2012, Hurricane Harvey in 2017, and the Egyptian internet shutdown in 2011 to small, unpublicized outages. Reliable methods are needed to detect internet outages, report them and understand their causes and trends so network reliability can be improved. Outage detection allows us to judge the reliability of the internet directly and report real-world status following major outages.

APPROACH

Trinocular Outage Detection is developing new methods to provide near-real-time detection of internet outages, build understanding of what outages mean and provide reports of outages. The technology detects outages across the internet by adaptively probing all /24 address blocks where at least 15 addresses reply to pings (as of 2016, that's about 4.1 million blocks). The solution's algorithms integrate measurements from multiple sites to avoid misinterpreting local problems and clusters and visualizes outages across the entire Internet Protocol version 4 (IPv4) internet.

BENEFITS

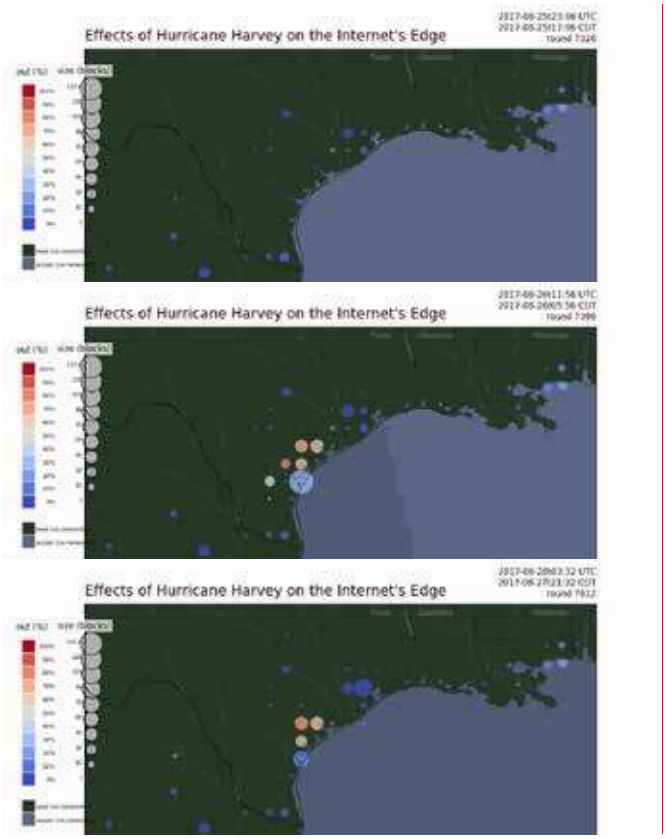
The technology generates datasets that identify network outages around the world, new methods to view and classify outages, and a deployed system that reports outages within minutes to hours of onset, instead of a retrospective report months later.

COMPETITIVE ADVANTAGES

Trinocular provides new data about internet outages that is available without cost to researchers and industry. The data includes coverage of more than 4 million IPv4 network blocks around the world over a period of more than two years to date. Complementing commercial services that observe website reliability, the technology detects outages in edge networks and provides known precision, detecting outages in as quickly as six minutes of an occurrence.

NEXT STEPS

The project team is collaborating with the Federal Communications Commission to understand the applicability of the technology to assessments of the reliability of critical U.S. infrastructure. Visit https://ant.isi.edu/duoi/ for datasets, papers, software and contact information. Animations of sample outages are at https://ant.isi.edu/outage/ani/. Technical details are at https://ant.isi.edu/outage/ and in the paper "Trinocular: Understanding Internet Reliability Through Adaptive Probing," Association for Computing Machinery SIGCOMM, 2013 http://doi.acm.org/10.1145/2486001.2486017.



Observing Hurricane Harvey with Trinocular. Before landfall (above). After landfall (right), showing outages north of Corpus Christi (red dots). Two days after landfall (far right), outages pick up in Houston (large blue dots) as flooding increases. More information: https://ant.isi.edu/outage/ani/harvey/

TrustBase: A Platform for Deploying Certificate-Based Authentication Services

Brigham Young University

Daniel Zappala
zappala@cs.byu.edu

OVERVIEW

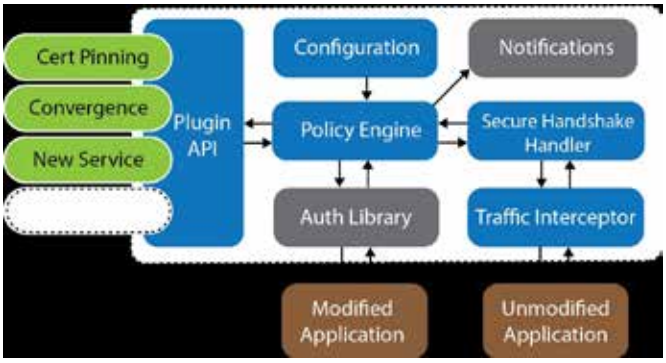
Researchers at Brigham Young University are developing TrustBase to repair and strengthen certificate-based authentication to improve online security.

CUSTOMER NEED

Internet infrastructure needs better ways to validate the certificates that vouch for server identities. There are two important flaws in how this validation is conducted today. First, applications often don't properly validate certificates due to developer mistakes. Second, even the best applications must rely on a certificate authority (CA) system that is vulnerable to hijacking. Because any CA can sign certificates for any site, the system is only as strong as the weakest CA. Additionally, CAs may not follow best practices or may be owned by adversarial governments.

OUR APPROACH

TrustBase provides certificate-based authentication as an operating-system service. It is designed to secure existing applications, strengthen the CA system and provide simple deployment of improved authentication systems.



The TrustBase architecture, showing traffic interception for existing applications, a set of handlers to extract authentication information and a policy engine to choose among installed authentication services.

Dr. Ann Cox, CSD Application of Network Measurement Science Program Manager
Ann.Cox@hq.dhs.gov

The system intercepts all network traffic, isolates certificate exchanges and ensures all certificates are properly validated. System administrators may configure a variety of authentication services and establish a system-wide policy for authentication.

Researchers have developed a prototype implementation for Linux and Windows and are continuing development to improve stability and usability. They have conducted a threat analysis and demonstrated how the architecture can protect against the following attacks: a hacked or coerced certificate authority; faked certificates inserted into a local root store; revoked certificates that are not checked properly; applications that do not properly perform validation and are subject to validation attacks; and start transmission layer security (STARTTLS) downgrade attacks. They demonstrated the Linux implementation has negligible overhead and are in the process of extending this analysis to Windows implementation.

BENEFITS

The system protects against insecure applications, forcing them to do proper certificate validation. It transparently enables existing applications to be strengthened against failures of the CA system. It also enables a system administrator to ensure best security practices are followed properly.

COMPETITIVE ADVANTAGE

The system provides coverage of all applications, enables administrator control over authentication policies, provides protection against local adversaries and enforces STARTTLS usage.

NEXT STEPS

The researchers are developing an application programming interface for applications to call the TrustBase system directly and greatly simplify development of applications that use Transport Layer Security. They also are developing additional authentication services and conducting usability testing. For code and questions, go to owntrust.org.

NetBrane: A Software-Defined DDoS Protection Platform for Internet Services

Colorado State University

Christos Papadopoulos
christos@colostate.edu

Dr. Ann Cox, CSD Distributed Denial of Service Defense Program Manager
Ann.Cox@hq.dhs.gov

OVERVIEW

The NetBrane project is developing a detection-and-mitigation system to defend against internet Distributed Denial of Service (DDoS) attacks. The system combines high-speed packet capture (more than 100 Gigabits per second [Gbps]) with machine learning to detect traffic anomalies, even if they are obscure; Software Defined Networking (SDN) to deploy fine-grained filtering rules that can be pushed instantly; and proactive defenses using network structural information and tips from hacker activities.

CUSTOMER NEED

DDoS attacks are in the top-five of network threats to the internet and cost billions of dollars in damages and expended effort. DDoS attacks have the potential to cripple large parts of or the entire internet infrastructure. DDoS is difficult to defend against because it requires a distributed solution with precise and timely communication to achieve very low false-positives.

APPROACH

Using techniques such as the Data Plane Development Kit and configurable hardware, NetBrane can use Commercial Off-The-Shelf (COTS) hardware to deploy high-speed packet capture at several Internet Exchange Points (IXPs) to gain visibility over most internet traffic. The technology uses machine learning to create fine-grained temporal traffic models that allow anomaly detection without the need to preset thresholds and with low false-positives. It uses SDN technology to deploy thousands of rules instantly to defend against complex attacks at very high speeds. Finally, the defensive technology uses network structural information such as Border Gateway Protocol (BGP) routing, internet maps, the location of vulnerable services such as Network Time Protocol, Domain Name System, etc., as well as hints from hacker forums to preemptively construct defenses so each is ready to deploy if an attack occurs.

BENEFITS

The technology offers a small footprint (up to 30 percent of IXPs); high-speed capture and machine learning for low false-positives; distributed detection and response; continuous reconnaissance to anticipate new attacks; integration of existing information to design, build and deploy proactive defenses; as well as the ability to deploy strategically thousands of rules to protect customers.

COMPETITIVE ADVANTAGE

NetBrane is the first system to take advantage of the convergence of multiple technologies such as machine learning, SDN, global internet routing, network maps and natural language processing to build a global DDoS defense system. Other solutions are either too expensive (cloud defenses), ineffective (firewalls) or may cause collateral damage (redirecting attack traffic to scrubbers).

NEXT STEPS

The project has demonstrated its ability to mitigate attacks at several hundred Gbps using COTS hardware. Two test deployments are planned: one at a local institution to defend smaller customers and another at a local internet service provider to defend dozens of institutions and big data repositories.

Open Source Address Validation Measurement

University of California San Diego

K.C. Claffy
kc@caida.org

Dr. Ann Cox, CSD Distributed Denial of Service Defense Program Manager
Ann.Cox@hq.dhs.gov

OVERVIEW

The Open Source Address Validation Measurement project provides the capability to measure whether a network is compliant with one of the most critical and longstanding, yet still elusive best practices—BCP38/84. This best practice supports source address validation, i.e., ensuring all packets leaving a network use only source addresses belonging to that network.

CUSTOMER NEED

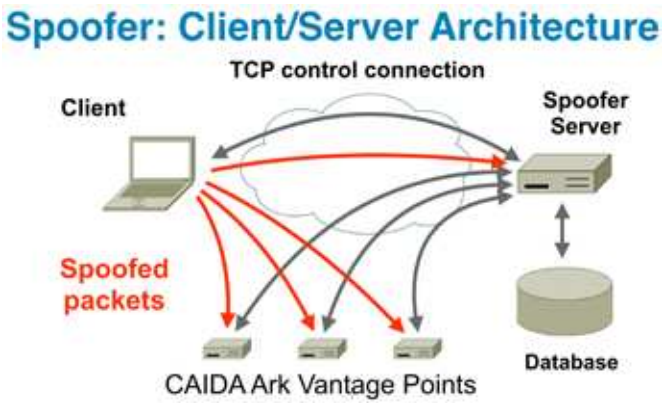
Networks that allow forged (or spoofed) source addresses enable a powerful vector for launching Distributed Denial of Service attacks that are difficult to attribute to their original source. Operators as well as any organization pursuing remediation efforts need a system to provide trustworthy measurements and analysis to track the deployment of source address validation (SAV) best practices and to inform anti-spoofing compliance efforts.

APPROACH

The project's primary goal is to measure and increase the deployment of SAV across the global internet. To enable testing and monitoring of individual networks, an open-source client-server system was developed for Windows, MacOS, and UNIX-like platforms. This system periodically tests a network's ability to send and receive packets with forged source addresses. Reports and visualizations are produced to enable prioritization of SAV-compliance attention where it will have the highest benefit.

BENEFITS

This project yields several benefits: a production-quality, client-server SAV testing system; a reporting and analysis system that optimizes compliance attention and assesses its impact; and a trace-route-based SAV-analysis system that gauges SAV deployment using trace-route data and autonomous system (AS) relationship inference.



The Spoofer client-server architecture. From the client host (far left), spoofed packets (red) travel over the internet to Ark vantage points and to the Spoofer server. The vantage points communicate with the Spoofer server regarding which spoofed packets reached the vantage points. A backend database stores results and serves data for a variety of reports useful to network operators and remediation authorities.

COMPETITIVE ADVANTAGE

There are currently no known open-source toolsets that measure and report the deployment of SAV.

NEXT STEPS

The performer is connecting with industry organizations Reseaux IP Europeens, Asia-Pacific Network Information Centre, North American Network Operators Group and National Cable & Telecommunications Association and helping internet service providers understand test results. It also is automating the upgrade path for the client software and porting the testing functionality to the OpenWRT platform to encourage wider adoption.

Voice Security Research for 911 and NG911 Systems

SecureLogix

Mark Collier
mark.collier@securelogix.com

Dr. Ann Cox, CSD Distributed Denial of Service Defense Program Manager
Ann.Cox@hq.dhs.gov

OVERVIEW

Telephony Denial of Service (TDoS) is a flood of malicious inbound calls—attacks that have targeted public-safety numbers such as 911 and emergency responders. If coordinated with a physical terrorist attack, a TDoS attack would be particularly disruptive, resulting in a large number of victims not connecting with emergency services. TDoS attacks also can affect financial services entities by denying customers access to telephone-service centers. If synchronized with a Distributed Denial of Service (DDoS) attack against a financial services firm's internet and mobile presence, a TDoS attack likely would prevent customers from contacting their banks.

CUSTOMER NEED

The enabler for TDoS attacks is the ability to cheaply and easily use automation to generate hundreds or thousands of simultaneous calls. It also is easy to spoof calling numbers and other attributes, making it difficult to differentiate legitimate and malicious calls. This issue makes robocalls, bomb threats and SWATing—or tricking an emergency service into dispatching an emergency-response team based on a false report of a critical incident—more severe and difficult to mitigate. The key need is the capability to authenticate callers and detect fraudulent number spoofing.

APPROACH

The goal is to shift the advantage from a TDoS attacker to the network administrator by developing the capability to authenticate callers and detect fraudulent call spoofing. These solutions—based on a series of filters that assign a risk-threat score to every call—will enable 911 systems administrators to better respond to and manage TDoS threats.

BENEFITS

Several benefits resulted from project testing, including addressing issues of call-number spoofing and authenticating callers as well as complex forms of TDoS, robocalls, bomb threats and social engineering. The model also showed potential for protecting key resources such as next-generation 911, emergency responders, banks and their customers, and schools.

COMPETITIVE ADVANTAGE

The research is based on an existing voice-security solution that provides a software base to build upon and can be deployed in complex voice networks. It also has an integrated Business Rule Management System and machine-learning engine that is easily extended with limited software modifications. This research will result in benefits to state and local 911 emergency operations and financial entities—critical infrastructure sectors protected as part of the DHS mission.

NEXT STEPS

Next steps include completing the research and working with pilot partners, including Palm Beach County 911, Greater Harris County 911 and a large financial entity's contact center, to validate the solution in operational environments.

A Federated Command and Control Infrastructure

Florida Institute of Technology

Tom Eskridge
teskridge@fit.edu

Edward Rhyne, CSD Federated Security Program Manager
Edward.Rhyne@hq.dhs.gov

OVERVIEW

The goal of the Federated Command and Control (FC2) project is to improve enterprise-level, cyber-defense capabilities by automatically enabling contextual and policy-controlled sharing of cyber intelligence and cyber operations. FC2 provides this capability by automatically creating and maintaining federations of enterprises based on contextual interests or operational domains. FC2 federations provide a seamless, policy-controlled automated way of information sharing, including threat indicators and defensive maneuvers.

CUSTOMER NEED

Prior research on command-and-control infrastructures for cyber operations have focused primarily on enterprise cyber-sensors and -defenses. Advanced defenses that detect and mitigate new threats can be made more effective if their information is shared with other organizations. FC2 fills this federation-building and information-sharing gap to enable coordinated operations across multiple enterprises by understanding and controlling how the organization depends on and interacts with other organizations and their supporting infrastructure systems.

APPROACH

The FC2 approach to information-sharing across diverse participating members creates an architecture that uses a common vocabulary to integrate a wide range of sensors and defenses. This approach separates the specification of federation-level defense postures from implementation within the organization, making them generally applicable throughout. New command and control mechanisms can be plugged into FC2 to enable federation involvement from numerous members. Organizations define the policies under which they agree to federation membership. The construction and maintenance of the federations are performed automatically by the FC2 infrastructure. Cross-domain reasoning, coordination and control algorithms are implemented to extend new protections throughout the federation.

BENEFITS

The FC2 approach has a number of benefits that stem from the design and implementation choices made during the project. Its extensible architecture facilitates the integration of a number of prior research efforts that enable the deployment of new capabilities through their coordination and control. It also enables participation in federation without manual intervention through automatic information-sharing policy negotiation and enforcement, ensuring that only approved information is shared. These policies are context-dependent and can be changed at any time to suit the changing needs of federation members.

COMPETITIVE ADVANTAGE

The competitive advantage of the FC2 technology comes from open architecture, extensible representations of sensors and defenses, and a common and extensible messaging format that encompasses existing messaging systems such as OpenC2 and STIX.

NEXT STEPS

The next steps include outreach to the security community and easing the adoption of FC2 technology. The key components are in the process of being open-sourced and publicly available, allowing researchers and companies to enable federation capabilities with a low threshold to adoption.

Self-Shielding Dynamic Network Architecture

Intelligent Automation, Inc.

Nicholas Evancich
nevancich@i-a-i.com

Edward Rhyne, CSD Federated Security Program Manager
Edward.Rhyne@hq.dhs.gov

OVERVIEW

The static nature of today's networks provides ample opportunity for attackers to gain intelligence, plan and execute attacks at will. To address this challenge, Intelligent Automation, Inc. (IAI), with the support of the Florida Institute of Technology (Florida Tech), is working to integrate its Self-Shielding Dynamic Network Architecture (SDNA)—a network layer Moving Target Defense—with Florida Tech's Federated Command and Control (FC2) Framework. The resulting technology will be a SDNA-FC2 prototype system with the potential to protect global cyber-operations. The combined technologies will provide a new set of advanced defense capabilities that will enable runtime obfuscation of segments in the protected network with a fully automated or human-assisted decision engine, defining the mission requirements and security objectives.

CUSTOMER NEED

To a determined adversary, there are many ways to get inside a network, bypass current protection technologies and attack intended targets. No current protection technologies stop the now-common practice of attacking a network from within using zero-day exploits, stolen credentials and other sophisticated tactics.

APPROACH

SDNA prevents an attacker from targeting, entering or spreading through a network by adding dynamics that present a constantly changing view of the network. The dynamics are Internet Protocol version 6-based and cryptographically strong. It prevents malicious packets from reaching their intended hosts. The defense mechanism increases the attacker's effort, risk of detection and time required to successfully conduct an attack. For example, if an attacker gains a foothold inside a network via a malicious insider or host compromised by a phishing attack, the defense limits the attacker's ability to spread by constraining each host to an abstract, modified view of the network.

BENEFITS

To protect against compromise, the defense mutates the network's "DNA" through packet manipulation, policies and rules to manage the competing goals of securing the network while providing legitimate users transparent access to needed services. Through this approach, attackers—even with unlimited resources—cannot send traffic directly into a protected enclave.

COMPETITIVE ADVANTAGE

Current defenses check for signatures, behaviors and artifacts of known attacks, but do not protect against unknown attacks. Firewalls are good for stopping attacks from entering the network, but provide no protection once an attacker gets past them. Basic randomization can improve resilience, but does not prevent misuse of credentials. SDNA provides several advantages over traditional defenses, including constantly manipulating the appearance of the network and keeping the attack in the reconnaissance phase as long as possible.

NEXT STEPS

SDNA is available for piloting, testing and evaluation. Additional development is underway to integrate the technology with a FC2 framework and develop a prototype that can protect various federated global enterprise networks.

A high-level overview of the SDNA architecture. SDNA-enabled gateways protect the internal SDNA-enabled architecture.

THE CSD INNOVATION ECOSYSTEM/ADVANTAGE

> “Collaboration is without a doubt essential when it comes to cyber R&D. Common pain points and threat vectors identified across government, industry, academia, and with partners around the world require a new way of thinking about how we set priorities and solve some of the most complex cybersecurity challenges of today and beyond. We recognize that a single organization cannot do this alone, and hope to lead a shift toward fully collaborative and transformative R&D.”
>
> *– Cyber Security Division*

SOFTWARE ASSURANCE

Hybrid Analysis Mapping Engine/Dynamic Application Security Testing Pre-Seeding Tool

Secure Decisions

Ken Prole
ken.prole@securedecisions.com

CSD Software Assurance Program Manager
SandT-Cyber-Liaison@hq.dhs.gov

OVERVIEW

The Dynamic Application Security Testing (DAST) Pre-Seeding Tool extends an attack surface calculation model to provide a complete picture of the exposed attack surfaces of web applications. A plugin to the DAST tools OWASP-ZAP and Portswigger-BurpSuite Professional is being created that consumes attack surface data to pre-seed an application's site mapping for DAST scanning. This enhanced capability will provide more thorough dynamic security testing.

CUSTOMER NEED

Gaps in an application's attack surface must be identified. Black-box penetration testing can miss unlinked endpoints without extensive endpoint brute forcing. Also, identifying optional parameters during black-box testing is time consuming and misses valid parameters that affect software execution. A more thorough parameters list would allow for more comprehensive testing.

APPROACH

This pre-seeding approach provides DAST scanners with a complete picture of an application's exposed attack surface so an application can be more thoroughly scanned, thus reducing false-negatives. This is achieved by using data structures from the previously developed Hybrid Analysis Mapping (HAM) technology. It extends the HAM attack surface calculation model to include—where possible—parameter types and an extension to the ZAP and BurpSuite tools to consume this attack surface and pre-seed application DAST scans. This calculated attack surface includes URLs and parameters that may be missed by traditional spidering approaches.

BENEFITS

This tool is unique since no other known systems pre-seed web application penetration tools like ZAP and BurpSuite with site endpoints and parameters that the endpoints accept. Understanding where unlinked endpoints in software are and finding optional parameters without guessing or brute forcing will help focus and expedite manual and automated penetration assessments and reduce testing costs.

COMPETITIVE ADVANTAGE

DAST scanners using spidering can fail to completely map an application's attack surface. When this occurs, directed fuzzing of the testing process fails to fully exercise an application. Using a calculated attack surface, DAST scanners are pre-seeded with a more complete application attack surface, resulting in more thorough directed fuzzing and a decrease in false-negatives. This approach produces a more complete picture of an application's security state.

NEXT STEPS

The next steps are to foster community awareness and increased use of this pre-seeding tool through open sourcing. Further exposure is envisioned through inclusion in free tool platforms such as Kali-Linux, Pentoo-Linux and Parrot Security OS. Plugins can be developed to support commercial tools IBM-AppScan and HP-WebInspect. The tool is targeted for release within the first three months of 2018.

Cyber Quantification Framework—Community Edition

Secure Decisions

Ken Prole
ken.prole@securedecisions.com

CSD Software Assurance Program Manager
SandT-Cyber-Liaison@hq.dhs.gov

OVERVIEW

The Cyber Quantification Framework—Community Edition (CQF—CE) automatically builds penetration testing and application environments and launches cyber-attacks. The workflow consists of "archetype" input for attacker and target application models through a representational state transfer (REST) application programming interface (API). Input is translated into a standardized, repeatable experiment where virtual machines (VMs) are automatically provisioned and attack sequences launched. Upon experiment completion, attack success-failure results are returned.

CUSTOMER NEED

Organizations facing serious human resource constraints in software security testing seek to use commercial and open-source tools to help them scale. However, most out-of-the-box security tools require days or weeks of manual configuration to perform well. After configuration, significant false-positives can arise, so manual or strict automated triage processes are necessary. Since manual activities are resource-intensive, testing time is shortened, resulting in disappointing scan results. This new testing platform addresses these shortcomings by automatically running a suite of application security tests within the software development lifecycle. The created test environment is isolated, automatically provisioning test environments; repeatable, ensuring new vulnerabilities aren't introduced during development; scalable, leveraging ESXi software in application testing environments; and extensible, capable of adding attacks, applications and configurations and customizing test suites.

APPROACH

CQF—CE executes test-environment automation by enabling attack simulator archetypes input ingestion through a REST API and translation into actionable experiments for testing. VMs are spun up, attacker (or penetration testing) and application (or webserver) environments are configured. The test suite is then defined and configured to automatically run a suite of attacks when code is pushed. Execution feedback is available through the REST API. Upon experiment completion, results are presented. The platform creates a reusable catalog of attacks and applications, designed for expansion so new attacks and application types can be added.

BENEFITS

The platform abstracts application security testing complexity. It saves time by eliminating manual processes, automating VM setup, connecting networks, configuring IP-addresses, installing/configuring software and attack tools, configuring/running attacks and verifying attack status. It significantly reduces the required expertise for application and penetration testing. Once attacks are implemented, they can be reused to improve application-security testing consistency and reliability.

COMPETITIVE ADVANTAGE

This testing platform provides advantages over other technologies by implementing application-security testing environment automation. Current tools require manually driven testing and individuals well-versed in application-security testing environment setup/execution. It also enables testers to automatically reassess and reconfirm the security profile of their applications.

NEXT STEPS

Next steps are to foster community awareness and increased use of the tools developed through open sourcing of CQF-CE, helping to enhance application-security testing effectiveness.

Penetration Test Automation

Secure Decisions

Ken Prole
ken.prole@securedecisions.com

CSD Software Assurance Program Manager
SandT-Cyber-Liaison@hq.dhs.gov

OVERVIEW

The Penetration Test Automation (PTA) platform is an orchestration service that facilitates the automation of existing, manually driven, command-line penetration testing tools. Automating these tools will enable the creation of automated security testing suites and increase the productivity of manual testing. Initially, the platform is equipped with plugins for three tools: SQLMap, Hydra and a new cross-site scripting (XSS) proof-of-concept. Developers can add security tools to the platform by creating straightforward wrapper plugins.

CUSTOMER NEED

Manual penetration testing is expensive and the tools used cannot be integrated readily into application security testing automation systems. Improving the quality and productivity of manual penetration testing and enabling test automation is crucial. Today, manual-penetration testers spend too much time wrangling tools. Automated security testing is uncommon because the tools are not able to be readily integrated.

APPROACH

The platform defines a standard interface that attack tool plugins implement. The interface defines how to assemble commands and parse tool output for a particular attack tool. This approach allows an automated execution platform to run different tools without having to separately integrate with each one; it must only integrate with the standard interface. This approach enables communities to build and share an attack tool library. This XSS tool detects the context of reflection and chooses correct escape strings, reducing the number of queries needed by as much as 98 percent.

BENEFITS

Automation can be used to increase the productivity of manual penetration testers—enabling more repeatable, complete and/or lower-cost testing. Automation can be used to create testing suites that can provide DevSecOps and DevOps teams a way to repeatedly and reliably verify application security testing at scale.

COMPETITIVE ADVANTAGE

Existing testing platforms support security testing of operating systems and third-party packaged software, not first-party application software. The PTA platform—in conjunction with its plugin attack tools—is easier to use for application security testing than developing a custom solution or adapting existing, non-security-focused testing frameworks.

NEXT STEPS

The research team is planning an open-source release of the PTA platform and the XSS proof-of-concept attack tool. They also want to contribute core tool enhancements back to the SQLMap and Hydra open-source projects. The team also is seeking partners to pilot the platform and its associated application-security-testing tools and provide feedback on its operational utility.

Code Ray: Better Software Vulnerability Management through Hybrid Application Security Testing

Secure Decisions

Ken Prole
ken.prole@securedecisions.com

CSD Software Assurance Program Manager
SandT-Cyber-Liaison@hq.dhs.gov

OVERVIEW

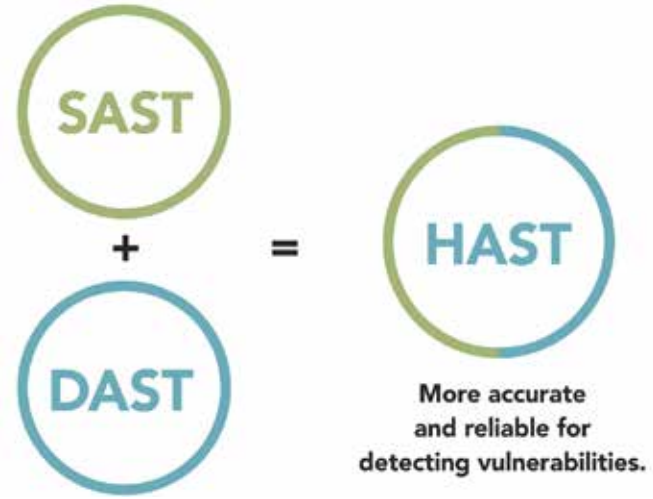
Code Ray is a technology that combines the results of static and dynamic application security testing. It highlights software vulnerabilities that are present in the source code and exploitable by external attackers without access to source code. This technology will be transitioned into use with the Code Dx software vulnerability discovery and management system and into the Software Assurance Marketplace (SWAMP).

CUSTOMER NEED

Up to 90 percent of computer security incidents are traceable to vulnerabilities in software exploited by an attacker. To avoid this situation, software developers, testers and security analysts must run application security tests to discover vulnerabilities before attackers do. To find most of the vulnerabilities in an application and to maximize vulnerability coverage, users must run several static source code analyzers alongside dynamic penetration testing tools and manual code analyses. Unfortunately, each tool presents its results in a different format and severity scale. This lack of uniformity makes it difficult and time consuming for users to create a consolidated, useful set of results that show all the vulnerabilities in the source code and which ones are visible to an external attacker. It is also time consuming to prioritize the thousands of vulnerabilities that are typically found so the most critical vulnerabilities are fixed first.

APPROACH

The technology engages in Hybrid Application Security Testing (HAST). It correlates and normalizes the output of Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST) tools, using runtime instrumentation and the Common Weakness Enumeration (CWE). The output is a consolidated set of results from all tools—duplicate results are removed—identifying which source code vulnerabilities are accessible by the software's end-users.



Code Ray's HAST combines SAST and DAST for improved security testing coverage and accuracy.

BENEFITS

The technology provides software developers, testers, security analysts and auditors better vulnerability coverage by combining several analysis techniques, improved accuracy with reduced false-positives by confirming exploitability, easier prioritization that highlights the vulnerabilities considered the most severe based on industry standards, guidance that pinpoints where to fix the code to remediate vulnerabilities, and improved communication from its visual interface that fosters collaboration between development and security teams.

COMPETITIVE ADVANTAGE

Code Ray's consolidated results are easier and quicker to interpret than the current state of the art, which requires sequential reviewing and mental correlations of disparate results from multiple application security testing techniques.

NEXT STEPS

The performer is transitioning the technology into a software vulnerability management system called Code Dx, which is commercially available. It will also be accessible in SWAMP.

ThreadFix: Hybrid Analysis Mapping

Denim Group

Dan Cornell
dan@denimgroup.com

CSD Software Assurance Program Manager
SandT-Cyber-Liaison@hq.dhs.gov

OVERVIEW

Software is integral to critical infrastructure. However, software systems have significant vulnerabilities that expose critical infrastructure to exploitation. Nation-states, organized crime, chaotic actors and other threats target software. Therefore, finding and fixing software vulnerabilities is critical for security-conscious organizations.

CUSTOMER NEED

To fully assess software security, multiple types of analysis are required. Hybrid Analysis Mapping (HAM) allows software assurance analysts to combine static application security testing (SAST) and dynamic application security testing (DAST), providing more sophisticated analysis and better results triage.

APPROACH

HAM uses application source code to create an attack surface model of an application, mapping the software code "at rest" to the dynamic behavior it will exhibit when operational. Based on this model, deeper security analysis can be performed and the results of both SAST and DAST testing can be correlated, providing the analyst a full view of the software system's security state.

BENEFITS

Using HAM, security analysts gain deeper insight into the security state of software systems and can more easily manage the volume of data that comes from sophisticated software assurance testing. In addition, the HAM attack surface model can be used to better guide DAST to help avoid false-negatives. The resulting vulnerability data is richer and helps software developers more efficiently remediate identified vulnerabilities. Embedding HAM into the software developer's toolbox helps to increase the ease of remediation so more vulnerabilities get fixed faster.

ThreadFix takes the results of the wide range of software assurance activities and normalizes them to provide analysts a comprehensive view of the security state of the software in an organization. In addition, ThreadFix communicates these results to other stakeholders in the tools they already are using, allowing organizations to successfully remediate vulnerabilities and report on progress in their software assurance program.

COMPETITIVE ADVANTAGE

This HAM technology relies only on access to source code, DAST and SAST testing results and does not require the instrumentation of running systems or the use of an agent. As a result, it is easier for organizations to deploy versus other approaches that have been used in the past.

NEXT STEPS

HAM technology is embedded in the ThreadFix application vulnerability management platform (www.threadfix.it), allowing organizations running sophisticated software assurance programs to scale to meet enterprise demands. ThreadFix allows organizations to manage large portfolios of software and make sense of data coming from the most popular and powerful SAST and DAST tools and services. In addition, ThreadFix's DevOps capabilities allows organizations to embed software assurance testing into Continuous Integration/Continuous Delivery pipelines, further reducing the time to discover, assess and remediate critical software vulnerabilities.

Real-Time Application Security Analyzer

RAM Laboratories, Inc.

Robert McGraw
rmcgraw@ramlabs.com

CSD Software Assurance Program Manager
SandT-Cyber-Liaison@hq.dhs.gov

OVERVIEW

The Real-Time Application Security Analyzer (RASAR) detects, locates and ranks vulnerabilities in binary executables compiled from software written in C/C++ even when the source code is not available. Its compliance dashboard enables visualization of vulnerabilities and compliance issues for the binary executable with regard to Common Weakness Enumeration (CWE), detected Open Web Application Security Project vulnerabilities, Defense Information Systems Agency Security Technical Implementation Guides compliance violations and violations of secure coding rules in cases where source code is available. The technology is being integrated into the Software Assurance Marketplace (SWAMP) to more widely enable its use for vulnerability detection and reporting.

CUSTOMER NEED

New software systems can be unpatched, counterfeit or contain zero-day vulnerabilities. A typical organization uses 78 percent open-source software. A 2016 HP/Ponemon study of 237 organizations showed that the average large company experienced $9.5M in cyber-crime costs per year. Sixty-one percent of these costs are associated with malicious code. In these cases, the cost per incident was $92,000 and the average time to report the incident was 50 days.

APPROACH

This approach takes the binary executable—instruments that binary—and then applies CWE checks on the instrumented binary as it executes. It then ranks and prioritizes the detected vulnerabilities by weighing CWE priority and severity metrics along with deployment factors. In the event source code is available, RASAR applies secure coding checks to the source code and then correlates the secure coding violations with the vulnerabilities detected in the binary executable through the instrumentation process. The result is a vulnerability report in SWAMP Common Assessment Result Format that has been further filtered through available source code to reduce false-positive detections and refine CWE categorization.

RASAR Concept of Operation. RASAR provides CWE-based vulnerability reports for binary executables, with additional correlation with secure coding violations if source code is available.

BENEFITS

The technology detects software vulnerabilities and identifies software supply chain compliance threats in cases where source code is not available. It prioritizes threats through the use of CWE and deployment factors. It also mitigates threats and educates developers by locating and correlating the identified binary vulnerability with those found in source code.

COMPETITIVE ADVANTAGE

In comparison with static analysis tools, RASAR greatly reduces false-positive detections by concretely executing and detecting vulnerabilities. In comparison with dynamic analysis tools, RASAR provides improved run-time performance along with CWE-based ranking and prioritization.

NEXT STEPS

RASAR will be integrated with Continuous Integration/Continuous Delivery frameworks along with supporting integration with test frameworks in SWAMP. An additional step will be enhancing the technology's capability with application layer vulnerability detection.

RevealDroid

University of California, Irvine

Sam Malek
malek@uci.edu

CSD Software Assurance Program Manager
SandT-Cyber-Liaison@hq.dhs.gov

OVERVIEW

The amount of malicious software has been growing rapidly on desktop, mobile and other platforms. Malware increasingly uses obfuscations to evade detection. To determine appropriate strategies to mitigate damage caused by malware, analysts should determine the family to which a malware belongs. To that end, a prototype for Android called RevealDroid was developed by drawing on a technology that leverages machine learning and program analysis of native, managed and reflective code to identify malicious apps and the family to which those malware apps belong. RevealDriod can detect malicious Android apps with 98 percent accuracy and detect the family to which they belong with 95 percent accuracy on a dataset of more than 54,000 apps.

CUSTOMER NEED

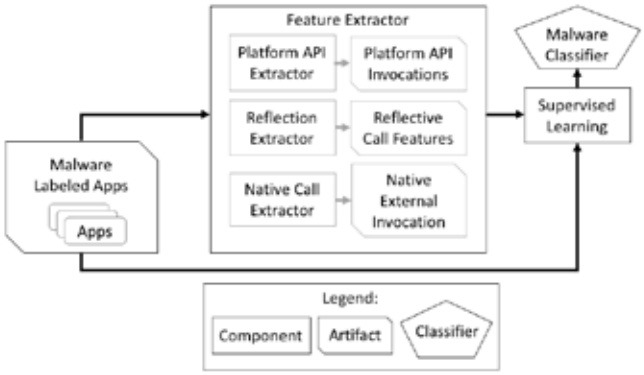
Malicious software attempts to avoid detection by using obfuscations and can rely upon managed code, native code or reflective code. Furthermore, determining the family to which a malware belongs can help analysts mitigate damage caused by such malware.

APPROACH

The technology uses machine learning and program analysis to examine managed code, native code and reflective code to identify malicious apps and their malware families. This approach can identify malicious apps and the malicious code family that was used to create them.

BENEFITS

By using machine learning and program analysis, the solution automatically can learn to detect zero-day malware by identifying the specific malicious behaviors of existing Android malware. It inspects code at multiple levels—managed code, native code and reflective code—each of which is used by malicious software to evade detection. The developer's implementation of RevealDroid corroborates its ability to detect zero-day malware. Also, it obtains accuracy improvements of up to 70 percent greater than other approaches.



RevealDroid Approach Overview

COMPETITIVE ADVANTAGE

The technology is the first approach that statically analyzes software at all levels, i.e., managed code, native code and reflective code. Time-aware experiments demonstrate its ability to detect zero-day malware with high accuracy.

NEXT STEPS

The developer intends to use functionality developed as part of the project to detect vulnerabilities and generate exploits for them. Using such functionality along with RevealDroid, the goal is to automatically monitor software for security purposes, automatically repair vulnerabilities and protect software in real-time.

Software Assurance Marketplace

Morgridge Institute for Research

James Kupsch
kupsch@cs.wisc.edu

CSD Software Assurance Program Manager
SandT-Cyber-Liaison@hq.dhs.gov

The Software Assurance Marketplace (SWAMP) logo with the continuous assurance gear-shaped icon.

OVERVIEW

The Software Assurance Marketplace (SWAMP) project pioneered the concept of "continuous assurance" by evaluating software and remediating weaknesses throughout the software-development lifecycle. SWAMP offers a no-cost, continuous-assurance platform that combines an array of open-source and commercial software analysis tools with advanced high-throughput computing (HTC) capabilities. SWAMP also is available as an open-source, on-premise platform called SWAMP-in-a-Box.

SWAMP supports Continuous Integration/Continuous Development (CI/CD) frameworks, integrated development environments (IDEs), software repositories and federated identity management. SWAMP easily integrates with existing CI/CD tools such as Jenkins and IDEs like Eclipse, offering developers continuous-assurance capabilities powered by multiple tools in their DevOps/Agile processes. The versatile HTC backend will enable future SWAMP versions to support dynamic tools that assess the operational stage of software deployment.

CUSTOMER NEED

Software is integrated into nearly every aspect of our lives and is used on multiple devices by government, business and individuals. Security breaches are regular news headlines. Software applications must be built securely at the code level and tested regularly to ensure security and protect privacy. SWAMP promotes continuous assurance technologies through an open, collaborative platform that facilitates continuous integration, making it easier for developers to adopt continuous assurance practices.

APPROACH

SWAMP is a collaboration of four research institutions—The Morgridge Institute for Research, Indiana University, University of Illinois at Urbana-Champaign and University of Wisconsin-Madison—each providing expertise to enhance the security and robustness of the project.

BENEFITS

SWAMP is a no-cost resource available to the global software community that provides a powerful, flexible and open platform for organizations and developers to institute continuous software assurance practices. SWAMP encourages software developers, assurance researchers, infrastructure operators, educators, students and individuals from open-source, government and commercial groups to assess their software—both developed and acquired—to promote a more stable and secure software ecosystem. SWAMP-in-a-Box can be deployed locally to maintain higher software security and compliance requirements.

COMPETITIVE ADVANTAGE

SWAMP is unique in offering vendor-neutral access to multiple software assurance tools, automation and the HTC capacity needed to support continuous assurance and CI/CD pipelines. Unlike similar offerings of no-cost software assessment services by commercial entities, SWAMP is designed, built, operated and supported by four institutions with a long, demonstrated commitment to open-source, cybersecurity, privacy and software assurance and driven by an underpinning vision of an open, continuous software-assurance platform that facilitates easy adoption of new software analysis technologies. All software technology that the SWAMP develops is open-source.

NEXT STEPS

- Download SWAMP-in-a-Box at https://continuousassurance.org/swamp-in-a-box/
- Use SWAMP at https://mir-swamp.org/
- Learn more about continuous assurance at https://continuousassurance.org/

DHS S&T Cyber Security Division:

Leaders in Federal Cybersecurity R&D

*Go to **www.dhs.gov/cyber-research** to learn more about CSD's work and how your organization can partner with us.*

TRANSITION TO PRACTICE

TTP: Accelerating Technology Transition

Dr. Nadia Carlsten, CSD TTP Program Manager
ST.TTP@hq.dhs.gov

The Transition to Practice (TTP) program identifies promising federally funded cybersecurity technologies through technology foraging from sources that include Department of Energy and Department of Defense laboratories, Federally Funded Research and Development Centers, and universities, with a goal of transitioning them through partnerships and commercialization. Technologies selected by TTP go through a structured process to increase market readiness, including validating the technology through testing, evaluation and pilot deployments; accelerating time-to-market by providing researchers training and market research; and connecting them with investors and potential licensors through outreach, industry events and TTP-hosted Technology Demonstration Days.

The following 40 promising cybersecurity technologies are part of the TTP program and available for piloting and/or licensing. For additional information about the TTP program and descriptions of TTP technologies, please refer to the Transition to Practice Technology Guide at https://www.dhs.gov/publication/ttp-tech-guide.

APPLICATION SECURITY:

- APE: Android Intrusion Prevention
- Hyperion: Detecting Vulnerabilities and Sleeper Code, Analyzing Malware, and Assuring Software
- TRACER: Transparent Protection of Commodity Applications

The Transition to Practice program is helping to bring cyber technology to the marketplace.

ENDPOINT SECURITY:

- CodeSeal: Tamper-Proof Trust Anchors
- Hone: Producing Insight by Correlating Machine and Network Activities
- USB-ARM: Architecture for USB-Based Removable Media Protection

INDUSTRIAL AND INTERNET OF THINGS SECURITY:

- AICS: Cyber Security and Network State Awareness for Ethernet-Based Industrial Control Networks
- CPAD: Cyber-Physical Attack Detection
- DDNR: Dynamic Defense & Network Randomization
- SerialTap: Enabling Complete Situational Awareness in Control Systems
- WeaselBoard: Zero-Day Exploit Protection for Programmable Logic Controllers

MALWARE DETECTION:

- AMICO: Accurate Behavior-Based Detection of Malware Downloads
- CodeDNA: Scalable, High-Speed, High-Volume, Shareable Malware Detection
- MLSTONES: The DNA of Cyber Security—An Organic Model for Identifying Cyber Events
- ZeroPoint: Advanced Weaponized Document Detection and Analytics

NETWORK SECURITY:

- Choreographer: A Moving Target System to Thwart Automated Network Attackers
- DFI: Adaptive Access Control to Protect Networks
- FLOWER: Network FLOW AnalyzER—Deep Insight into Network Traffic
- NEMS: Network Characterization and Discovery Tool
- PathScan: Finding the Attacker Within

- PCapDB: Optimized Full Network Packet Capture for Fast and Efficient Retrieval
- PEACE: Policy Enforcement and Access Control for End-Points
- SilentAlarm: Detecting Abnormal Network Traffic

RISK AND COMPLIANCE:

- PACRAT: The Blended Physical and Cyber Risk Analysis Tool
- SecuritySeal: Critical Protection for Your Supply Chain
- Security Operations and Incident Response:
- DigitalAnts: Dynamic & Resilient Infrastructure Protection
- Akatosh: Real-Time Incident Verification and Automated Impact Tracking and Analysis
- SCOT: Turning Cyber Data into Incident Response Threat Intel

THREAT INTELLIGENCE AND ANALYSIS

- CHARIOT: Filtering and Enriching Relevant Content
- QUASAR: Strategic Decision Support for Cyber Defense Planning
- REDUCE: Collaborative, Statistically Guided Exploration of Malware Similarities
- REnigma: A Tool to Reverse Engineer Malware
- Situ: Discovering and Explaining Suspicious Behavior
- Socrates: Graph Analytics for Discovering Patterns and Relationships in Large Data Sets
- SRS: Threat Landscape Analysis for the Cyber Defender
- StreamWorks: Continuous Pattern Dete


CYBERSECURITY
R&D
MARKET:
PLACE
TTP

Notes and Bits

ONLINE
www.dhs.gov/cyber-research

FACEBOOK
Facebook.com/dhsscitech

EMAIL
SandT-Cyber-Liaison@hq.dhs.gov

YOUTUBE
www.youtube.com/dhsscitech

TWITTER
@dhsscitech

Periscope
@dhsscitech

LINKEDIN
www.linkedin.com/company/dhsscitech