Cyber Security Division Technology Guide 2017

Homeland Security

Science and Technology

Introduction

Thank you for your interest in the U.S. Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Cyber Security Division (CSD) research and development (R&D) portfolio. This 2017 CSD Technology Guide is the culmination of extensive efforts to identify and develop cybersecurity technologies for homeland security application within industry, academia and our national lab partners. Many of these technologies have been funded through Broad Agency Announcements (BAA) and Small Business Innovative Research (SBIR) programs. We're excited to share these promising cybersecurity technologies with you.

The CSD Technology Guide, which is updated and published annually, features innovative R&D technology solutions addressing Cyber Outreach, Cyber Physical Systems, Cybersecurity Research Infrastructure, Human Aspects of Cybersecurity, Law Enforcement Support, Mobile Security, Network and System Security, Open-Source Technologies, Software Assurance, and Transition to Practice.

Through partnerships and commercialization, CSD—a part of the Homeland Security Advanced Research Projects Agency (HSARPA)—is identifying innovative, federally funded research that addresses cybersecurity needs and is helping transition the tools and technologies developed by its performers into the Homeland Security Enterprise. All of the technologies included in this guide are mature and ready to be piloted in an operational environment or transitioned into a commercially available product. If you're interested in becoming an S&T partner or piloting, licensing or commercializing one of our technologies, please connect with us at SandT-Cyber-Liaison@HQ.DHS.GOV.

In addition to these technologies, we are interested in future research areas that will address cybersecurity capability gaps in your own organization. We encourage you to share your thoughts with us; your input will help us identify real-world solutions and inform future research efforts. Again, it's our pleasure to bring you the 2017 CSD Technology Guide and introduce you to these potentially groundbreaking cybersecurity tools developed through the federal government R&D community.

Sincerely,

Douglas Maughan

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

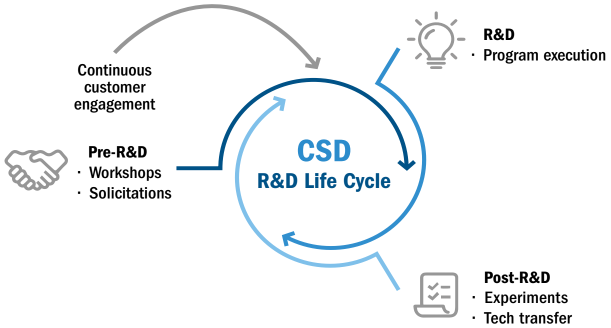
CONTENTS

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 the federal government's Federal Cybersecurity Research and Development Strategic Plan announced in February 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; delivering simulation-supported cyber exercises to critical infrastructure owners and operators; 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 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; 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

> "Computers and computer networking provide major benefits to modern society, yet the growing costs of malicious cyber activities and cybersecurity itself diminish these benefits. Advances in cybersecurity are urgently needed to preserve the Internet's growing social and economic benefits by thwarting adversaries and strengthening public trust of cyber systems."
>
> **Federal Cybersecurity Research and Development Strategic Plan, February 2016**

testing of next-generation cybersecurity technologies through the Defense Technology Experimental Research (DETER) testbed.

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; and developing intuitive security solutions that can be implemented by information technology owners and operators who have limited or no training.

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; improving the collection of network traffic information to provide scalable, real-time access to the data collected from around the globe; conducting research in attack modeling to enable critical infrastructure owners and operators to predict the effects of cyberattacks on their systems; creating technologies that can identify and alert system administrators when an attack is occurring; 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.

Secure Protocols—Adding security to the Internet's core routing protocol—Border Gateway Protocol—so communications follow the intended path between organizations.

Software Assurance—Developing tools, techniques and environments to analyze software, address internal flaws and vulnerabilities in software, 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.

CYBER PHYSICAL SYSTEMS:

- Cyber Physical Systems Security: Medical Device Risk Assessment Platform
- Cyber Physical Systems Security: Uptane

Medical Device Risk Assessment Platform

Medical Device Innovation Safety and Security Consortium

Dale Nordenberg
dalenordenberg@novasano.com

Dr. Daniel Massey, CSD CPSSEC
Program Manager
Daniel.Massey@hq.dhs.gov

Overview

Cyber vulnerabilities in medical devices and their risk controls are an asymmetric threat to patient safety, privacy and the usability of medical devices. To properly establish the scope of needed security risk management activities, a medical device must be assessed to determine which features expose a potential security risk based on its intended use and operating environment. The Medical Device Risk Assessment Platform provides health delivery organizations (HDOs) and medical device manufacturers a system to assess these cybersecurity risks. The platform allows the effective assessment of cyber risks and the implementation of appropriate policies and controls to mitigate risks.

Customer Need

Today's evolving medical device technology and increasing connectivity require HDOs to manage cyber security risk management strategies. The merging of the information technology and clinical engineering sectors has created a gap in the toolsets and processes required to implement comprehensive cybersecurity risk management practices. Because of electronic medical records, network-connected medical devices and private health information data breaches, the risks associated with threats and vulnerabilities require the medical industry to adequately consider and address cybersecurity risks as part of its overall risk-management assessment and mitigation strategy.

Approach

There are significant safety factors that must be considered when securing medical devices, paramount being the possibility of a patient's death. This cybersecurity assessment tool provides manufacturers, HDOs and medical professionals the resources needed to manage the unique risks presented by connected medical devices and helps organizations across multiple steps of the risk management process.

Benefits

By completing the platform's risk assessments of an organization's medical devices, the combined set of assessments can be used to identify the most critical threats and guide the implementation of policies to appropriately mitigate these risks. After profile implementations have been completed, the assessments can be repeated for upgraded controls and coupled with current threat intelligence from related platforms. Last, as the nature of the threat changes, existing and future risk information can be used to determine if current and planned controls still fit within an organization's business priorities, risk tolerance and resource constraints.

Competitive Advantage

The platform provides HDOs and medical device manufacturers a system for assessing the cyber security risks of the numerous and rapidly growing array of medical devices that are essential to modern health care.

Next Steps

Next steps include design implementation and managing evolving partnerships and collaborations with the National Health-Information Sharing Analysis Center, which will include a series of medical device cybersecurity workshops with a focus on risk assessment.

Uptane

New York University

Dr. Justin Cappos
jcappos@nyu.edu

Dr. Daniel Massey, CSD CPSSEC Program Manager
Daniel.Massey@hq.dhs.gov

Overview

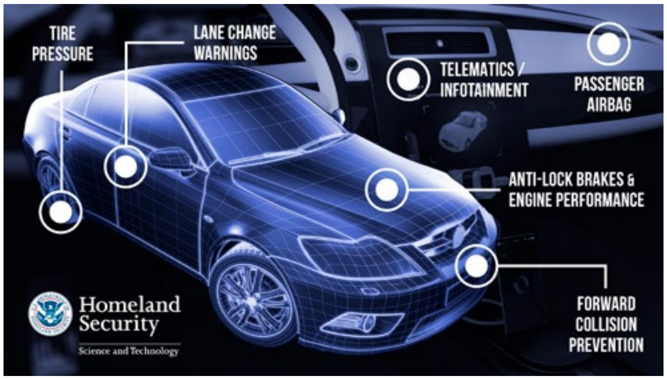
The insecurity of software update systems poses a major security risk to modern computers. Software updates often are inadequately protected, leading to substantial damage. For example, a 2013 attack on South Korean banks and media companies caused $765 million in damages. Attacks against cyber physical systems such as automobiles could cost more and potentially impact millions of lives.

Customer Need

New defensive techniques are needed that retain strong security guarantees even in the face of key compromises. Uptane, a new security solution being developed by researchers at New York University (NYU), will incorporate new techniques that will help secure vehicular software updates, but have little impact on automobile manufacturers. For example, a car manufacturer may decide to push software updates over the air within the continental United States, but in Hawaii, Puerto Rico and Alaska it may require dealerships to distribute updates via USB, the onboard diagnostic (OBD) system or Wi-Fi. The new security model will enforce these restrictions so a malicious actor who controls a dealership in San Juan, Puerto Rico, for example, cannot compromise a vehicle in San Jose, California. The technology will enable manufacturers to manage the risk for a wide array of compromise scenarios.

Approach

The technology will enhance the security of automobile update systems by adding and validating metadata to improve resilience to attacks. Because different auto manufacturers and tier 1 vendors have their own development and deployment infrastructure, this technology does not propose a universal solution. Instead, it offers flexibility to accommodate users and their unique security needs.


TIRE PRESSURE
LANE CHANGE WARNINGS
TELEMATICS / INFOTAINMENT
PASSENGER AIRBAG
ANTI-LOCK BRAKES & ENGINE PERFORMANCE
FORWARD COLLISION PREVENTION
Homeland Security
Science and Technology

Benefits

The solution will improve automobile security with little cost to manufacturers, car dealers and owners. No additional hardware is needed; updates are disseminated using existing automobile manufacturer and dealership infrastructure such as over-the-air updates. Deploying the technology will be a cost-effective method to mitigate the risk of cyberattacks on automobile software update infrastructure.

Competitive Advantage

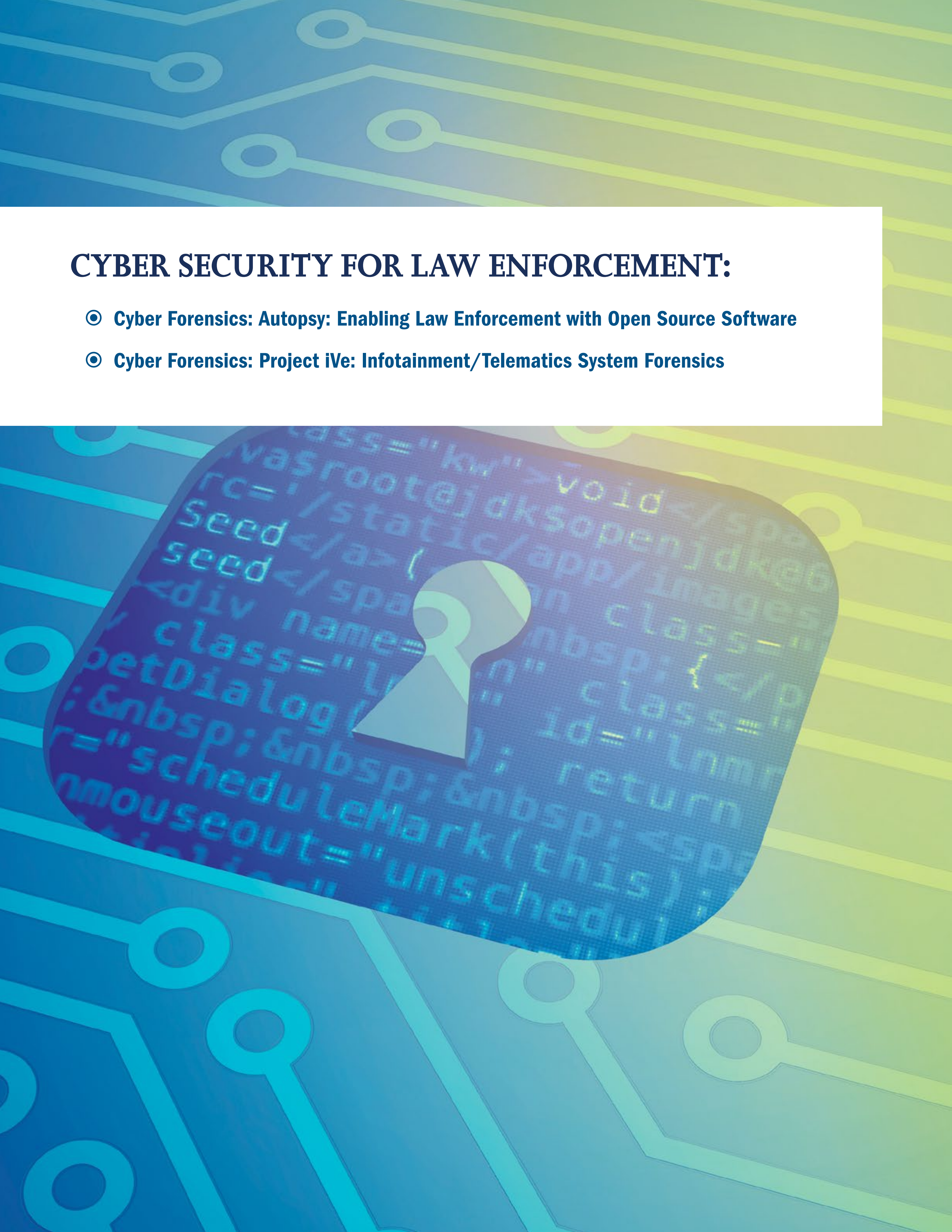
The technology will provide a flexible framework that enables different parties to configure the provided security benefits to their needs and environment. This flexibility will provide an innovative approach and competitive edge over those companies that offer one-size-fits-all automotive cybersecurity solutions.

Next Steps

NYU is producing a standards specification for the metadata format used by the secure automotive software updater. Since a substantial portion of security deals with operational issues like key management, NYU also is working with automobile manufacturers to tailor solutions that provide enhanced security with minimal usability impact.

CYBER SECURITY FOR LAW ENFORCEMENT:

- Cyber Forensics: Autopsy: Enabling Law Enforcement with Open Source Software
- Cyber Forensics: Project iVe: Infotainment/Telematics System Forensics



Autopsy

Enabling Law Enforcement with Open Source Software

Basis Technology

Laurin Buchanan
Laurin.Buchanan@securedecisions.com

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

Overview

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

Customer Need

As digital devices have become an essential part of daily life, they also have become critical to nearly every criminal investigation at the local, state and federal levels. This criminal use means enforcement organizations need to keep up with an increasing number of 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

Areas of focus during the course of this project include creating an image gallery, developing a timeline analysis capability, identifying indicators of compromise, and searching for account numbers. Each module yields different benefits.

The image gallery module allows investigators to review large numbers of images by grouping them by folder or other user-defined criteria. Autopsy prioritizes which group of files to display.

The timeline module enables investigators to establish a pattern of life. It combines events from files and application-level data into a single interface. It also clusters events together to help reduce data overload for the investigator.

The indicators of compromise module helps users find traces of known intrusions using the STIX XML descriptors. The account number module reduces false-positives and makes it easier to review searches for stolen credit card numbers.

Competitive Advantage

The project enhancements have targeted ease of use and provide results as quickly as possible as the key elements for success. Open-source modules add functionalities and promote flexibility to best suit an investigator's needs.

Next Steps

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

Project iVe

Infotainment/Telematics System Forensics

Berla Corporation

Ben LeMere
blemere@berla.co

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

Overview

iVe is a digital forensics tool for the acquisition of user data from vehicle infotainment and telematics systems. It is a new and innovative capability for law enforcement investigators to acquire data through logical and/or physical acquisition. Vehicle systems store a vast amount of data including navigation history, call logs, SMS messages and photos. Currently, iVe supports more than 5,200 makes and models of vehicles, including Ford, General Motors, Fiat-Chrysler, Toyota, BMW and Toyota.

Customer Need

Modern vehicles are complex systems, with an average of 70 computers and five networks connecting the computers, which generate a significant amount of data that potentially could be used as evidence in criminal and terrorist investigations.

Approach

iVe uses logical and/or physical acquisitions to collect connection data from phones; devices such as media players, USB drives and SD cards; and navigation data from vehicles. Additionally, iVe collects event data that captures information from vehicle operations such as gear shifts, light activations, door openings; USB attachments, Bluetooth devices and GPS systems; the odometer; phone calls made from a connected phone; Wi-Fi connections; and system reboots. iVe data collection is done through nondestructive means, ensuring the vehicle remains operational after data acquisition.

iVe Mobile, an Android app, is a field-support tool that provides first responders the information they need to determine iVe's capability for a given make and model of vehicle. It provides information about supported vehicles, supported infotainment/telematics systems, and removal instructions prior to data acquisition.

Benefits

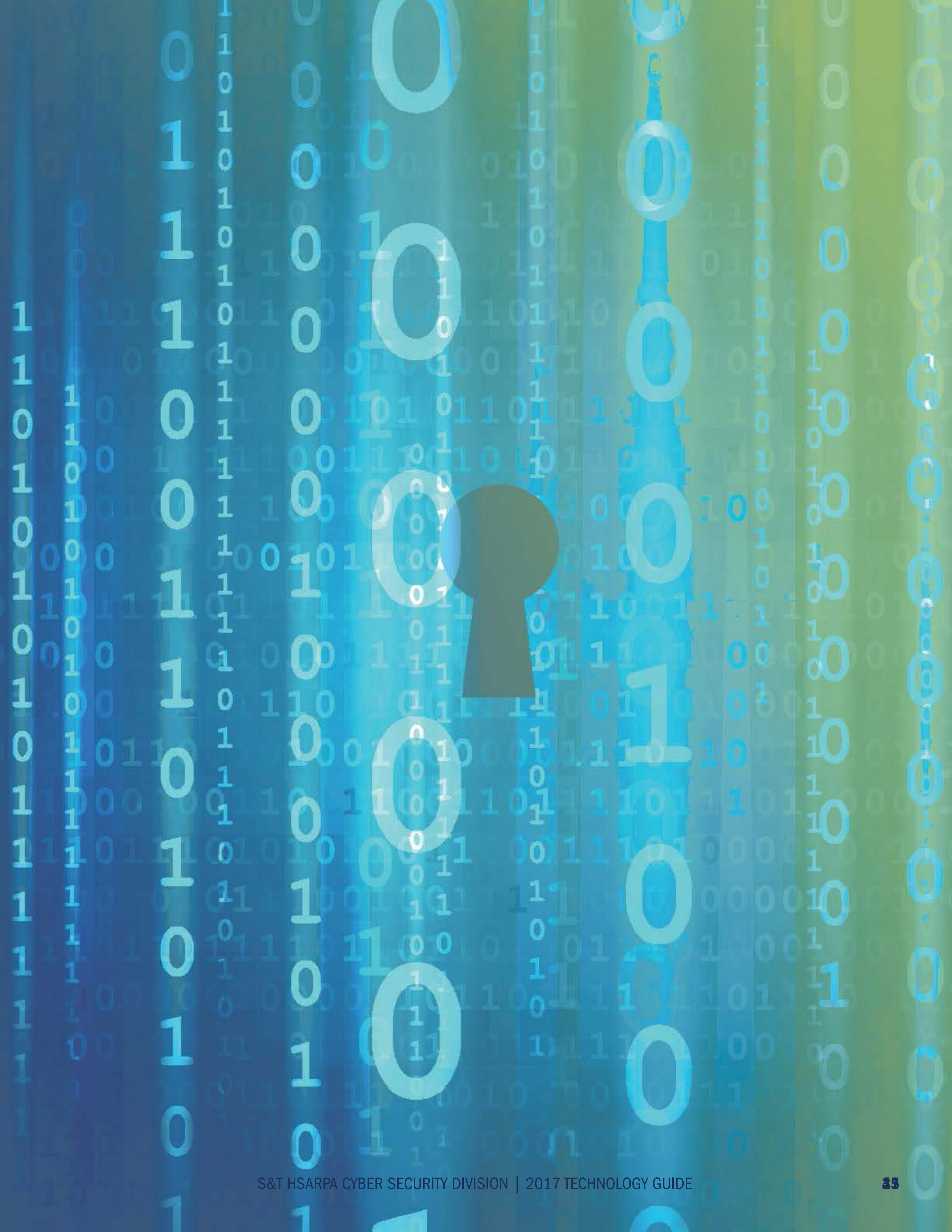
iVe provides a capability that law enforcement agencies can use to investigate crimes committed with vehicles by acquiring data that may provide supporting evidence to their investigations. Vehicle infotainment and telematics systems provide a wealth of data for investigators to determine pattern of life activities for potential suspects and their vehicles.

Competitive Advantage

DHS S&T CSD has partnered with 17 federal, state and local law enforcement agencies to guide the requirements process, to serve as testers for the tool, and provide feedback to the researchers and CSD. The partnership enables iVe to target specific law enforcement investigative needs. It also allows iVe to continuously expand the supported vehicles to add additional makes and models and additional capabilities to extract data from vehicle infotainment and telematics systems.

Next Steps

iVe is commercially available for law enforcement acquisition. iVe will continue to add additional manufacturers and infotainment/telematics systems and enhance iVe Mobile.



CYBERSECURITY RESEARCH INFRASTRUCTURE:

⦿ Information Marketplace for Policy and Analysis of Cyber-risk & Trust: Internet Atlas

Internet Atlas

University of Wisconsin-Madison

Paul Barford
pb@cs.wisc.edu

Erin Kenneally, JD
CSD IMPACT Program Manager
erin.kenneally@hq.dhs.gov

Overview

Detailed maps of the Internet are a starting point for assessing infrastructure risk and vulnerabilities, understanding routing and traffic behavior, designing and monitoring security infrastructures, and forensic investigations of attacks and intrusions. Over the last six years, University of Wisconsin-Madison researchers, supported by CSD, have developed Internet Atlas. Atlas is a geographically anchored representation of the physical Internet, including nodes (e.g., colocation facilities), conduits/links that connect nodes, and relevant meta data (e.g., source provenance). Atlas contains more than 25,000 node locations and 20,000 links for more than 1,200 networks around the world. Customized interfaces enable a variety of dynamic (e.g., border gateway protocol updates, targeted traffic measurement, Network Time Protocol measurements) and static (e.g., highway, rail, census) data to be imported into Atlas and layered atop the physical representation. Atlas is implemented in a web portal based on an ArcGIS geographic information system, which enables visualization and diverse spatial analyses of the data.

Customer Need

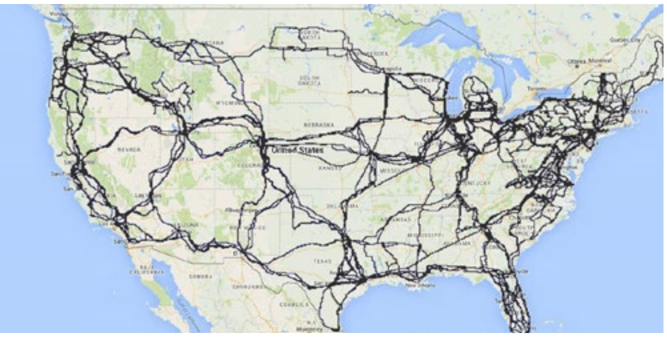
Atlas customers are owners, operators or users of Internet communication infrastructure who must ensure their infrastructures are reliable, operational and secure.

Atlas offers a global representation that can extend what is found in typical network operation centers. Atlas' detailed global perspective enables risk and vulnerability analysis; real-time monitoring that can identify performance degradation, outages, attacks and intrusions; and forensic investigation of incidents.

Approach

The Atlas data repository was built using search-to-find primary source data including maps and other public records such as conduit permits. This data is entered into the repository using a combination of manual and automated processes. Data updates and audits are ongoing. The Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT) supports the global cyber risk research community by coordinating and enabling real-world data and information-sharing capabilities.

The Internet map data serves as the base representation in the Atlas web portal. Also included is the ability to conduct targeted active probe-based measurement of Internet paths, visualize and assess Border Gateway Protocol 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 Atlas' application programming interface [API]).



Benefits

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

Atlas is the largest known 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

Atlas is expected to be deployed in an operational setting. It also is available through CSD's IMPACT at www.ImpactCyberTrust.org.

CYBERSECURITY OUTREACH:

- Cybersecurity Competitions: Comic-Based Education and Evaluation

Comic-Based Education and Evaluation

Secure Decisions

Laurin Buchanan
Laurin.Buchanan@securedecisions.com

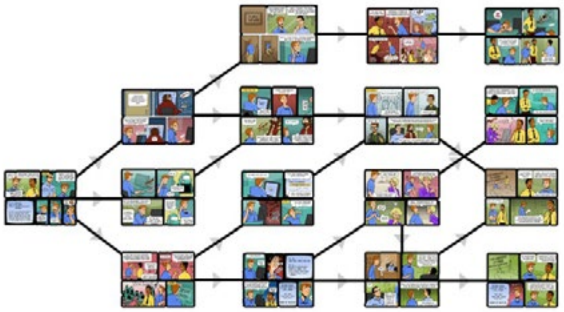
Edward Rhyne, CSD Cybersecurity Competitions Program Manager
Edward.Rhyne@HQ.DHS.GOV

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 interactive, graphic-branching stories. These branching stories—or “choose your own adventure” (CYOA) 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 stories.

Customer Need

Raising safe-computing awareness and changing risky behavior is challenging. The audience must understand how and why the risk applies to them, that the risk brings real consequences, and how they can reduce the risk. 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 graphic interactive 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.

Competitive Advantage

There are no other known solutions for the easy creation of interactive storylines for educational and training purposes. Partial solutions exist for non-programmers to create instructional comics, but they lack support for branching storylines and the creator cannot integrate lesson plans to create curricular materials. 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. Additional development is refining and enhancing the user interface, expanding the graphic library, expanding automation to create full color panels for CYOA comics, and adding scoring capabilities to allow readers to demonstrate their cyber competence by achieving a high score.

HOMELAND SECURITY OPEN SOURCE TECHNOLOGIES:

- Security Controls Compliance Server

Security Controls Compliance Server

Greg Elin
gregelin@govready.com

Dr. Daniel Massey, CSD HOST Program Manager
Daniel.Massey@hq.dhs.gov

Overview

Developers using open-source software (OSS) often struggle with getting their products and services adopted by the federal government because of the unfamiliar, expensive and time-consuming Federal Information Security Management Act (FISMA) certification and accreditation process. The mandated FISMA Risk Management Framework is a six-step process developers must go through for their system to receive an Authority to Operate certification. GovReady is developing an open-source Expert System for FISMA (ESF) called Security Controls Compliance Server that will make FISMA compliance testing easier and quicker.

Customer Need

There is a strong need to simplify and automate the complexities of tailoring federally mandated security controls. This can be done by transforming various security controls, publications and catalogs into machine-readable data and rules; applying best-fit algorithms to this knowledgebase of policies, roles, technologies and system architectures; and providing an easy-to-use interface that simplifies the experience of compliance with embedded coaching.

Approach

The primary objectives of this ESF approach is to transform the open-source software innovator's interactions from the National Institute of Standards and Technology Special Publication 800-53—Security and Privacy Controls for Federal Information Systems and Organizations—from a text-heavy experience to an intuitive and collaborative Software-as-a- Service experience. This method includes adding an early-stage version of a working open-source ESF and developing an assessment to determine if and how an expert system makes FISMA compliance easier for OSS projects.

Benefits

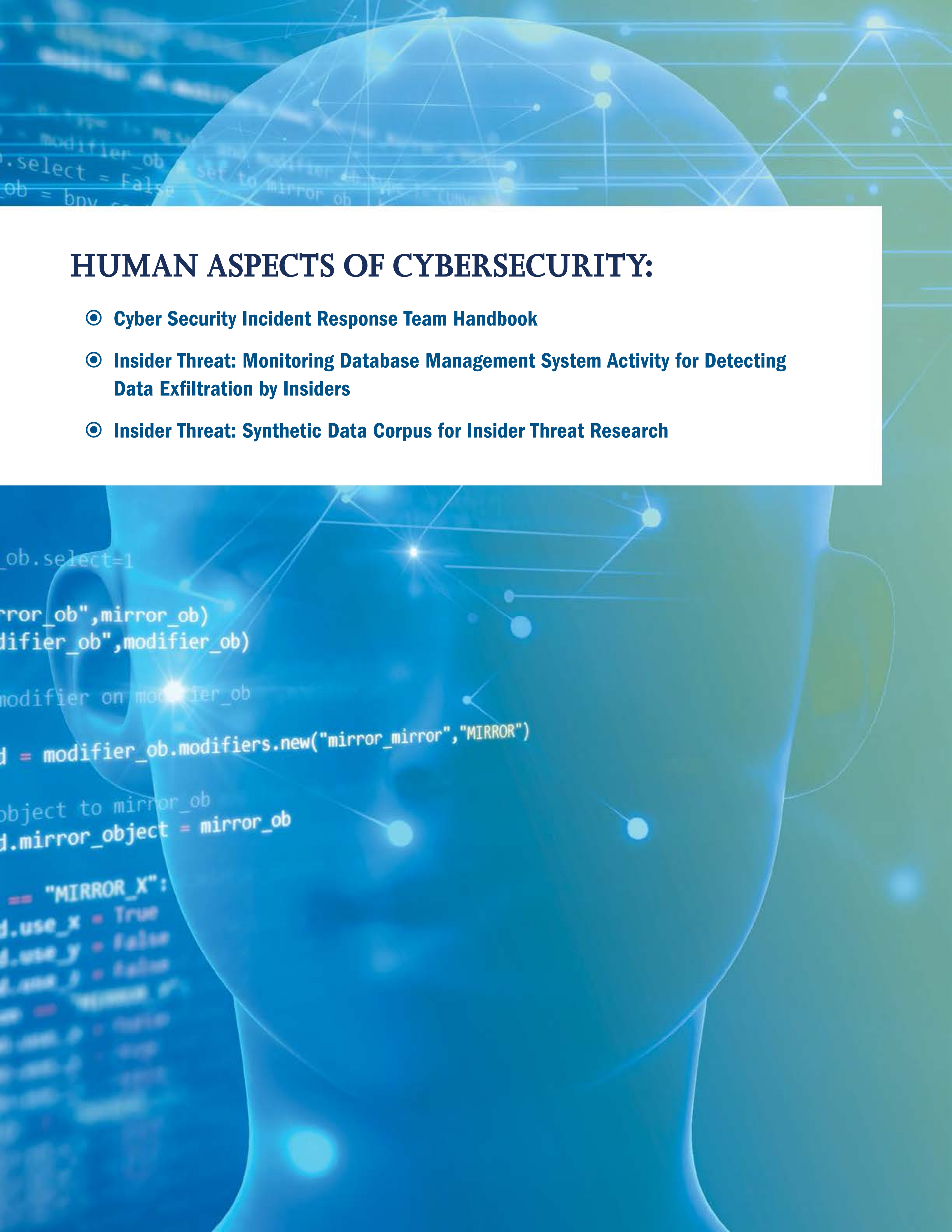
A number of benefits come with this approach. It is possible to do a one-time codification of an organization's policies, procedures, information technology roles, and tooling so the ESF can generate a complete system security plan using information about the network system that is gathered through normal processes over a day. This system security plan can be used as a guide that helps with implementation during the systems development lifecycle and generates control validation tests to continuously monitor compliance.

Competitive Advantage

An expert system that knows the 800-53 controls, different information system architectures, and IT products and services, enables adding codification of an organization's policies, procedures, tools and people and then generates specific, preferred control implementations for a given information system. This method is much simpler than what has been done by competitors and more cost efficient and less time-consuming.

Next Steps

The performer is conducting outreach to open-source technology providers, including various DHS S&T projects such as the Software Assurance Marketplace (SWAMP), launching a website to promote the use of the Security Controls Compliance Server (SCCS), and planning webinars and workshops to introduce potential end-users to the SCCS.



HUMAN ASPECTS OF CYBERSECURITY:

- Cyber Security Incident Response Team Handbook
- Insider Threat: Monitoring Database Management System Activity for Detecting Data Exfiltration by Insiders
- Insider Threat: Synthetic Data Corpus for Insider Threat Research

Cyber Security Incident Response Team Handbook

George Mason University

Reeshad Dalal
rdalal@gmu.edu

Scott Tousley, CSD CSIRT Program Manager
scott.tousley@HQ.DHS.GOV

Overview

This research project identified the key principles necessary to develop and sustain an effective Cyber Security Incident Response Team (CSIRT) through organizational science and more than 100 interviews with CSIRT organizations and individuals. The resulting CSIRT handbook describes needed knowledge, skills and abilities for CSIRT organizations—from individual, team and multi-team system (MTS) perspectives—and is a significant CSIRT leadership and training resource.

Customer Need

CSIRT organizations are growing in responsibilities and complexity and must respond to infrequent but significant security problems and incidents. Current CSIRT operations draw on technical experience and practice with little focus on principles of social science that CSIRTs should apply to their organization, training and operations. These principles are essential because the increasingly interconnected world requires organized and adaptive CSIRT teams that can respond effectively to a variety of security challenges that often occur unexpectedly.

Approach

The CSIRT research effort applied a multidisciplinary team approach to developing and validating the principles for building and operating an effective CSIRT. The project team included Dartmouth College, the George Mason University Organizational/Psychology departments, and Hewlett-Packard. Research elements included: defining CSIRT effectiveness, defining CSIRT response triggers, describing CSIRT teams/processes, developing a common performance taxonomy at individual, team and MTS levels, developing content through discussions/workshops with many different CSIRT teams and individuals, and developing a handbook of best practices and actionable recommendations for CSIRT managers that supports CSIRT training and development programs. This research was conducted in collaboration with the DHS National Cybersecurity and Communications Integration Center (NCCIC) and international partners from Sweden and the Netherlands.

Benefits

The CSIRT research effort generated recommendations for how to develop, train and sustain high-quality CSIRT organizations of any size throughout the government and private sector. These teams will support continuous development of cyber-incident response capabilities, which is a focus of Presidential Policy Directive 41.

Competitive Advantage

Several organizations have developed recommended guidance for CSIRT staffing and procedures, including maturity model approaches that address how to scale CSIRT capabilities based on size and experience. The CSIRT Handbook builds on this earlier work by combining practical CSIRT expertise with the most relevant social and organizational science, resulting in a reference and training resource that can be used by all types of CSIRT organizations.

Next Steps

The CSIRT Handbook is available to an CSIRT organization at http://tinyurl.com/CSIRTSocialMaturityHandbook. CSD is working with the DHS NCCIC organization to promote the handbook as a reference and engagement resource across the domestic and worldwide CSIRT communities. CSD also is working with key CSIRT organizations and the technical/management consulting community to build awareness and a community of practice around this CSIRT work and to support transition and continuous improvement.

Monitoring Database Management System Activity for Detecting Data Exfiltration by Insiders

Northrop Grumman

Donald Steiner, Ph.D.
Donald.Steiner@ngc.com

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

Overview

Within the Monitoring Database Management System Activity for Detecting Data Exfiltration by Insiders (MDBMS) project, Northrop Grumman and its subcontractor, Purdue University, created the DBSAFE system to identify anomalous queries to relational database management systems (RDBMS) that are indicative of insider threats such as data exfiltration or sabotage. DBSAFE uses machine-learning techniques to develop models of normal Structured Query Language statements used by groups of users. It then alerts on queries that deviate from the norm.

Customer Need

Data represents one of the most important assets of an organization. Malicious insiders pose a considerable threat to an organization by intentionally releasing or manipulating sensitive data. This type of cyberattack is hard to detect and mitigate using conventional database security mechanisms. By studying the patterns of interaction between users and an RDBMS, anomalous activity can be detected that may indicate early signs of exfiltration. Customers need an anomaly detection system that operates close to the RDBMS to prevent malicious use of data.

Approach

DBSAFE incorporates techniques for detecting and countering efforts by insiders to exfiltrate or manipulate sensitive data. The approach is comprised of the following activities:

- Profiling normal database interactions
- Detecting anomalous queries
- Deploying countermeasures

The project implemented and evaluated the techniques in prototype software systems culminating in an operational environment.

Benefits

The benefits of this approach include:

- Dynamic and automated generation of behavioral profiles based on roles, rather than individuals
- Near real-time alerts of anomalous database queries that may indicate malicious activity
- Automated responses according to predefined policies
- Logs of anomalous queries, metadata and explanation for forensic purposes

Competitive Advantage

Most existing cyber security defense tools protect an organization from external attacks, but are ineffective against insider threats. Many insider-threat detection tools focus on collecting behavioral patterns of individual users instead of monitoring data usage. Those that protect the data source use complex and have unmanageable rules. Analytic approaches use static logs causing a delay in response. DBSAFE overcomes these hurdles by providing an automated and readily adaptable mechanism to detect potential insider threats in near real-time.

Next Steps

DBSAFE is available for pilot deployment to evaluate the efficacy of machine-learning approaches in real-life enterprise environments.

Synthetic Data Corpus for Insider Threat Research

MIT—Lincoln Labs

Glenn Carl
glenn.carl@ll.mit.edu

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

Overview

A corpus of experimental data has been created to support research, development, testing and evaluation of insider threat detection tools. This data corpus consists of 12 independent, multiday, enterprise scenarios. Each scenario's instrumentation contributed more than one terabyte of rich, detailed cyber data (e.g., packet capture [PCAP] network packet traces, Microsoft [MS] Outlook Mail Data File, MS Domain Controller and File Server event logs). Half the scenarios model intentional insider threat activities such as intellectual property (IP) theft or deletion and the other half exhibits false-positive versions (e.g., system misconfiguration). This data corpus will be made available to the broader community via DHS S&T's IMPACT project.

Customer Need

High-quality evaluation of insider threat research is hampered by the lack of suitable test data. This test data should capture the behavioral activity of malicious insiders and benign enterprise users. It also should be in the format of common data sensors expected in the target operational environment (e.g., corporate enterprise).

Approach

CSD partnered with the Massachusetts Institute of Technology–Lincoln Labs (MIT-LL) to enhance the Lincoln Adaptable Real-time Information Assurance Testbed (i.e., LARIAT cyber-training, -test and -evaluation range) to be capable of emulating realistic insider threat activities such as malware installation or mail-based coordination and nominal daily activities. These insider threat activities are specified as rare, scripted actions for a small percentage of the users within the cyber range's modeled enterprise. To create the data corpus, the LARIAT cyber range is instrumented for one to two weeks while the 50+ modeled users login and logout, browse an emulated Internet, send and reply to mail, use SharePoint and social networking services, and perform insider threat actions.

Benefits

Generating realistic test data for the insider threat research community, including academia, government and industry, is time- and resource-intensive. The benefit of this approach is that a mature, repeatable test environment is used to generate synthetic, realistic insider threat data. Additionally, the data provided is in common formats (e.g., PCAP, MS event logs) for which several data analysis support tools exists (e.g., Wireshark, python data parsers).

Competitive Advantage

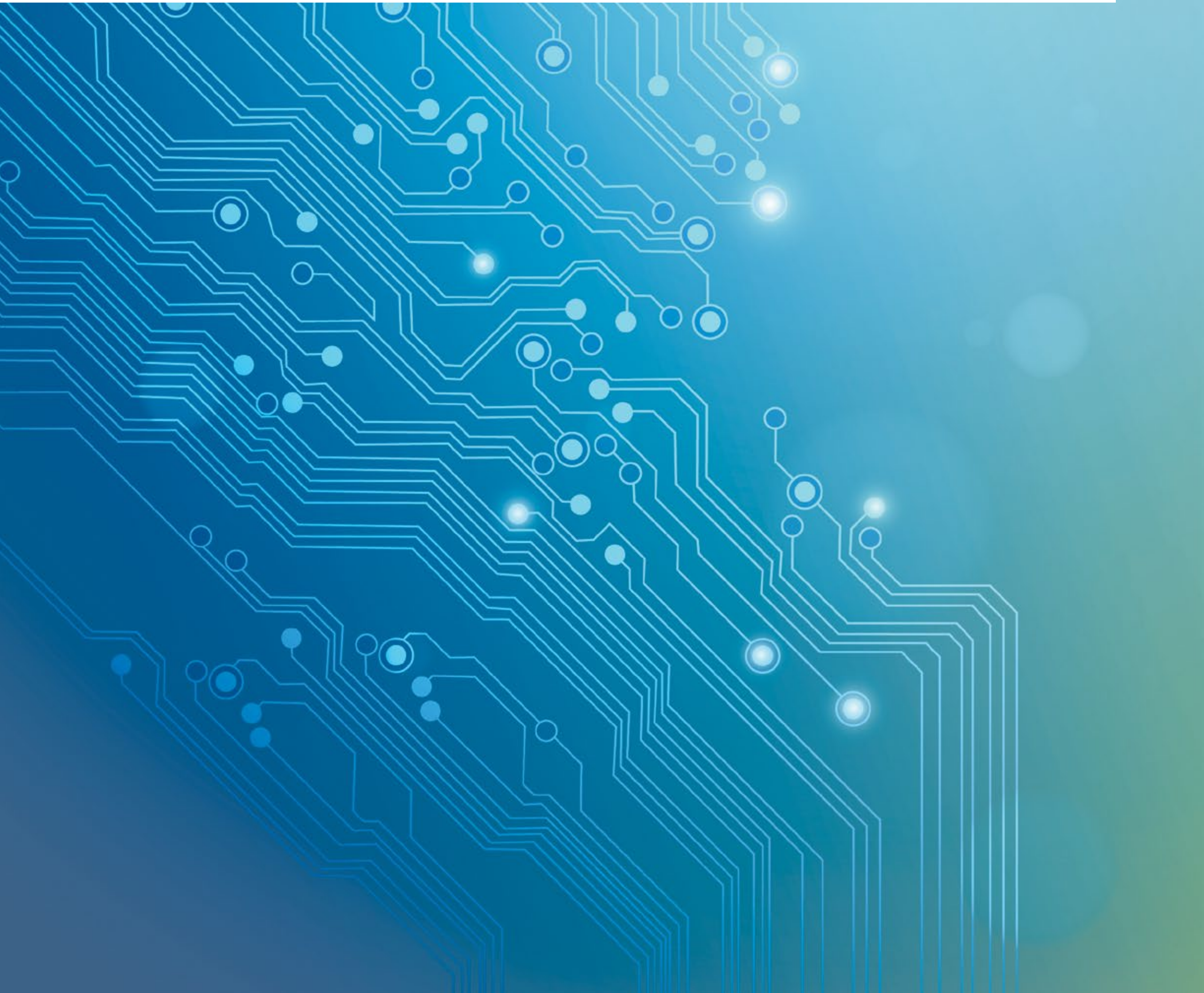
The competitive advantage is the data corpus is widely available to all insider threat researchers or developers with few restrictions. Additionally, the data corpus is in formats typically produced by data sensors in today's enterprises.

Next Steps

Once the enhancements are developed, the dataset will be migrated to the IMPACT project and disseminated for use to the insider threat research community.

MOBILE SECURITY:

- Mobile Device Security: Mobile Roots of Trust: Software-Only Roots-of-Trust for Mobile Devices
- Mobile Device Security: Mobile App Software Assurance



Mobile Roots of Trust

BlueRISC

Software-Only Roots-of-Trust for Mobile Devices

Kristopher Carver
kris@bluerisc.com

Vincent Sritapan, CSD Mobile Device Security Program Manager
Vincent.Sritapan@hq.dhs.gov

Overview

This mobile roots of trust (MRoT) technology measures and verifies a mobile device's static and runtime state to enable trust and overall device security. It can be used to detect malicious system change or activity, and the presence of ransomware and rooting. To ensure access to critical information and software, it can be performed only in a trusted state. MRoT requires no modifications to the underlying operating system kernel, manufacturer or service provider support for insertion, which greatly reduces hurdles to adoption.

Customer Need

The mobile device market has grown tremendously. Individuals, businesses and governments rely on mobile devices to access critical infrastructure and share vital information (e.g., banking, medical, intellectual property). This growth also has brought about a parallel surge in attacks. Attacks such as ransomware are gaining frequency and are highly effective. Roots-of-Trust (RoTs)—highly trustworthy, tamper-evident components—provide a foundation to build security and trust.

Our Approach

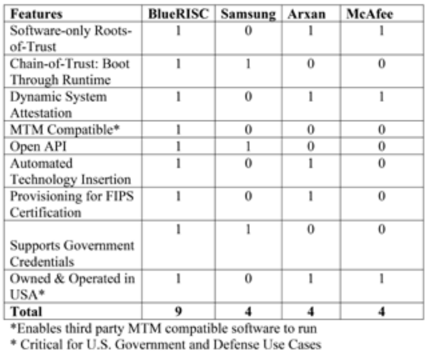
BlueRISC's MRoT solution is a software-based, mobile-security architecture, spanning both boot-time/static and runtime/dynamic RoTs, and mimicking the protection achievable through use of dedicated, security-centric hardware. At its core, MRoT uses cryptographic protections, while not requiring any plaintext persistent key storage. The solution is packaged with a Secure Vault application that enables the protection of off-the-shelf Android applications and their data. It also supports the industry-accepted Trusted Computing Group Mobile Trusted Module (MTM) specification, but goes beyond MTM by providing dynamic trust verification, enabling an open, useable application programming interface to the underlying trusted services.

Benefits

The value proposition of this MRoT product is the establishment of software-based static and dynamic RoTs that can be leveraged for application and data protection and trusted policy enforcement. The solution comes prepackaged with an Android calendar application supporting "Secure Events." It also supports automated detection of ransomware and rooting exploits. The automated installation methodology and the lack of modifications to the underlying operating system kernel drastically reduce barrier-to-entry into the commercial marketplace.

Competitive Advantage

In mobile device protection, there are two main solution types: those provided by the device manufacturer and those designed to operate on top of the operating system to provide user-land security services. Of these, the former represents the most prevalent competition. The following table provides a detailed competitive analysis.



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

*Enables third party MTM compatible software to run
* Critical for U.S. Government and Defense Use Cases

Next Steps

The performer has successfully demonstrated an MRoT prototype. Moving forward, researchers will be increasing exposure to the solution and working with existing commercialization partners. Additional use-cases with new partners will be pursued as the solution matures.

Mobile App Software Assurance

Kryptowire

Dr. Angelos Stavrou
info@kryptowire.com

Vincent Sritapan, CSD Mobile Device Security 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 applications. However, these benefits must be carefully weighed against possible security and privacy risks introduced by third-party mobile applications that have not been vetted for possible security and policy issues. Kryptowire has developed a system for assessing, analyzing, tracking and archiving mobile applications to assess adherence to U.S. federal government security standards.

Customer Need

Smartphones and tablets enable government employees to access mobile applications virtually anytime and anywhere. Third-party software developers create innovative mobile applications that can help government employees better fulfill the mission of their agency. Each agency must ensure the mobile applications used by their employees do not introduce unacceptable risks to its data and network resources. Agencies must analyze the security and privacy implications of mobile applications and verify their compliance with information technology security and privacy policies prior to deployment.

Approach

The mobile application analysis system enables the automated, large-scale analysis of mobile application binary and source code, Java or native code and libraries.

These security analysis results are presented to an analyst in a detailed application report through a web-based portal. Pass-fail evidence is provided with attribution to the code level.

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 applications based on the following standards:

- National Institute of Science and Technology (NIST) Special Publication 800-163: Vetting the Security of Mobile Applications
- National Information Assurance Partnership (NIAP) Protection Profile for Application Software
- The system reduces the time it takes an analyst to assess the security posture of an application. Also, it offers testing and protection profiles for different use-cases as defined by the testing organization.

javax crypto KeyGenerator generateKey[]
mponent com banking payment invoice TypeInCardAct
SimpleCrypto small line
Generated key value [byte representation]
java security SecureRandom setSeed[byte[]]
Seed value [byte representation]

Competitive Advantage

This mobile application analysis portal allows government agencies to have control, accountability and transparency over the vetting and risk-scoring processes, test for compliance with NIST and NIAP guidelines; and integrate the security and privacy analysis results into other mobile application management and mobile device management (MDM) technologies.

Next Steps

The next steps will be the development, certification, accreditation and piloting of an on-premises appliance. Given the initial solution was cloud-based, it is anticipated that the on-premises solution will provide customers the flexibility to vet their own and third-party applications against specific policies and requirements.

NETWORK SYSTEM SECURITY:

- Security of Cloud-Based Systems: Self-Shielding Dynamic Network Architecture
- Distributed Denial of Service Defense: Open Source Spoofer Toolset
- Distributed Denial of Service Defense: Voice Security Research for 911 and NG911 Systems
- Internet Measurement and Attack Modeling (IMAM): A Trust Platform for IoT
- IMAM: Distributed Incident Management System
- IMAM: ImmuneSoft: Software Immune System for Embedded Devices
- IMAM: Science of Internet Security: Technology and Experimental Research
- IMAM: Systemic-Risk Assessment Tools for Cyber-Physical-Human Infrastructures
- IMAM: Trinocular: Detecting and Understanding Outages in the Internet
- IMAM: TrustBase: A Platform for Deploying Certificate-Based Authentication Services

Self-Shielding Dynamic Network Architecture

Intelligent Automation, Inc.

Nicholas Evancich
nevancich@i-a-i.com

Edward Rhyne, CSD Security of Cloud-Based Systems Program Manager
Edward.Rhyne@hq.dhs.gov

Overview

The static nature of today's networks provides ample opportunity for attackers to gather intelligence, plan and execute attacks at will. To address this problem, Intelligent Automation, Inc. has developed Self-shielding Dynamic Network Architecture (SDNA), a dynamic defense that alters network architecture and behavior to stop and contain cyberattacks while remaining transparent to a legitimate user.

Customer Need

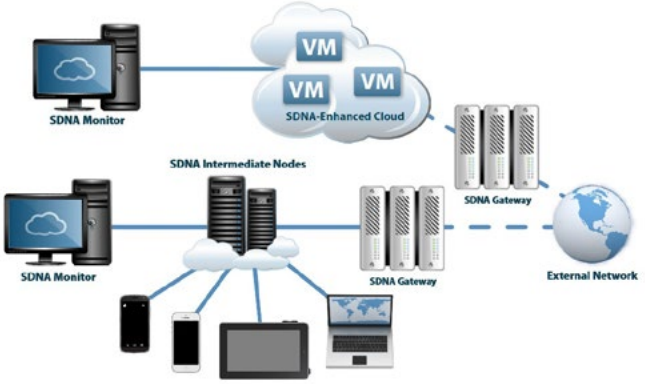
Today's networks are very vulnerable to cyberattacks. To a determined adversary, there are many ways to get inside a network, bypass current protection technologies, and attack intended targets. None of the current protection technologies stop the now-common practice of attacking a network from within using zero-day exploits, stolen credentials and other sophisticated tactics. An innovation in cybersecurity technology is needed that goes beyond the current state-of-the-art methods.

Approach

The technology prevents an attacker from targeting, entering or spreading through a network by adding dynamics that present a constantly changing view of the network over space and time. The dynamics are IPv6-based and cryptographically strong. It prevents malicious packets from even reaching the 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.



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

Competitive Advantage

Current defenses check against 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 there is no protection once an attacker gets past them. Basic randomization can improve resilience, but does not prevent against misuse of credentials.

Next Steps

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

Open Source Spoofer Toolset

University of California San Diego

KC Claffy
kc@caida.org

Dr. Daniel Massey, CSD DDoSD Program Manager
Daniel.Massey@hq.dhs.gov

Overview

The Open Source Spoofer Toolset provides an easy and secure method to determine if an organization allows users to send forged (spoofed) Internet packets. All organizations should block forged packets using well-established best practices such as BCP38. This toolset provides the capability to test whether an organization is deploying best practices and if they are deployed correctly and provide assistance to correct and identify issues or vulnerabilities.

Customer Need

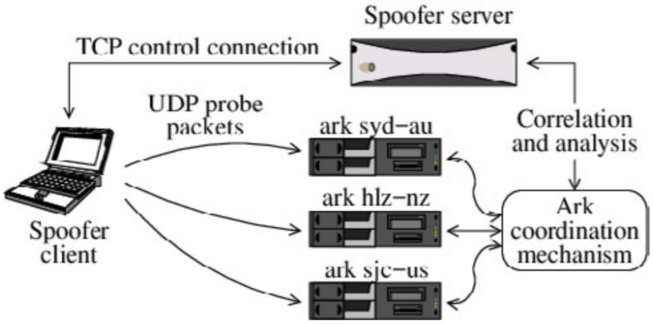
Many Internet Service Providers (ISPs) provide transit of Internet Protocol (IP) packets with forged source addresses in packet headers. This lack of filtering enables Distributed Denial of Service (DDoS) attacks and makes it complex and expensive to discover an attack source. A production-quality Source Address Validation (SAV) testing system, data analysis to inform assessment of infrastructure hygiene and effectiveness of anti-spoofing compliance efforts, and a traffic analysis system to track the deployment of SAV best practices will help solve this problem.

Approach

The research's primary goal is to measure and improve the use of SAV. Many DDoS attacks rely on the use of forged source addresses. Forged addresses make tracing the real source of attacks more difficult. SAV techniques could prevent this behavior if more broadly deployed and measured. The researchers are studying, developing, testing and demonstrating new tools and methodologies to monitor and promote SAV. If successful, the effort will increase the deployment of SAV across the Internet, making some attacks impossible and many others easier to defend.

Benefits

Several benefits result from the Spoofer toolset, including development of a measurement platform to test IP source address validation, which is targeting measurement and analysis to promote best current practices. In addition, the toolset will contain strategies for mitigating susceptibility to DDoS attacks that are a threat to national security, commerce and critical infrastructure.



Competitive Advantage

There are currently no other known open-source toolsets that measure and report the deployment of SAV, offer new client-server testing systems or user incentives for deployment of best practices. The toolset focuses on industry-developed best practices that have wide general support, but have not been adopted widely. The toolset will fill that void by promoting established best practices that if widely implemented will make the Internet more secure.

Next Steps

Researchers will develop an implementation plan based on the Autonomous Systems Rank system to detect provider-customer interconnections where the provider has not deployed SAV; update the reporting system to include a report on viability of an Internet Exchange Point SAV system; and host a series of software demonstrations.

.

Voice Security Research for 911 and NG911 Systems

SecureLogix

Mark Collier
mark.collier@securelogix.com

Dr. Daniel Massey, CSD DDoSD Program Manager
Daniel.Massey@hq.dhs.gov

Overview

Telephony Denial of Service (TDoS) is a flood of malicious inbound calls. TDoS attacks 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 also can affect financial services by denying consumers access to customer service centers. If synchronized with a Distributed Denial of Service (DDoS) attack against a financial service Internet and mobile presence, a TDoS attack could prevent customers from contacting their banks.

Customer Need

The underlying 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 very difficult to differentiate between legitimate and malicious calls. This issue makes robocalls, bomb threats and SWATing—tricking an emergency service into dispatching an emergency response based on a false report of a critical incident—more severe and difficult to mitigate. The key need is the ability to authenticate callers and detect fraudulent spoofing of a calling number. SecureLogix is working on multiple projects to solve TDoS and authentication/spoofing detection and applying the results to voice-security issues.

Approach

The goal is to shift the advantage from a DDoS 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

A number of benefits resulted from testing the model, including addressing issues of call-number spoofing and authenticating callers as well as complex forms of TDoS, robocalls, bomb threats and social engineering. In addition, the approach showed potential for the protection of key resources such as next-generation 911, emergency responders, banking and schools, and authentication of banking consumers.

Competitive Advantage

The research is based on an existing voice-security solution. This solution provides a software base to build upon, which can be deployed in complex voice networks and 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—sectors that are to be protected as part of the DHS mission.

Next Steps

Next steps include identifying a pilot to address mobile users by working with service providers, collecting data and validating initial rules, and continuing to develop countermeasures and test with pilot customers.

A Trust Platform for IoT

Power Fingerprinting

Carlos R. Aguayo Gonzalez
caguayog@powerfingerprinting.com

Dr. Ann Cox, CSD IMAM Program Manager
ann.cox@hq.dhs.gov

Overview

Power Fingerprinting (PFP) has developed a unique platform for trust and intrusion detection to secure legacy and Internet of Things (IoT) devices. The technology leverages unintended emissions (e.g., power consumption) to detect cyberattacks without impacting latency or processing overhead. Security as a Service (SaaS) is especially well-suited for protecting critical infrastructure such as industrial control systems or network infrastructure.

Customer Need

Critical infrastructure systems, including power generation, industrial control, networking and military systems, are vulnerable to cyberattacks due to their reliance on digital processors. Attacks can be introduced at multiple points throughout the lifecycle, including malicious hardware implants and tampered firmware. Additionally, critical systems often have strict safety and reliability requirements frequently paired with constrained platforms making it very difficult to support traditional intrusion detection systems.

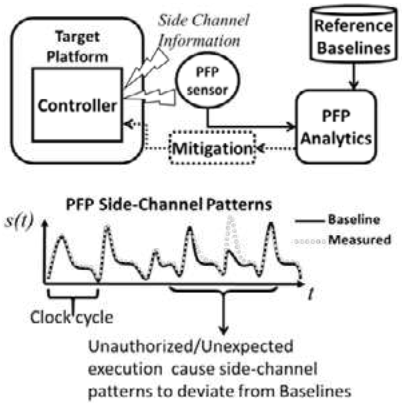
Approach

Leveraging analog, unintended emissions—known as physical side channels (e.g., power consumption)—to detect cyberattacks, the solution relies on signal processing and machine learning cluster side channel data at different scales and detects anomalies to tampered hardware, firmware, configuration or software.

The technology is especially well-suited for monitoring field operations devices, e.g., industrial control or Supervisory Control and Data Acquisition (SCADA) systems and monitoring appliances can be provided for legacy systems. When an intrusion is detected, the technology enables policy-based remediation, including bringing the device to a known state.

Benefits

If an attacker performs any operation on the target, it will reflect on the side channels and can be detected. The technology has been tested for various applications, showing it can detect and remediate in machine time. This approach is well-suited for monitoring IoT and embedded devices and low-level execution such as firmware and bootloaders.



Integrity assessment and intrusion detection using PFP.

The developer's pMon 801 rack-mount appliance monitor is optimized to detect implant attacks such as SYNful Knock in Cisco Routers. The security appliance continuously monitors and detects attacks in routers and other devices, making it ideal for server farms and data centers.

Competitive Advantage

The solution's engines are agnostic to the target platform and can be used to monitor legacy and new devices. The solution can be deployed onsite or in the cloud, providing scalability for large deployments. This versatility enables significant cost reduction with a SaaS business model.

Next Steps

The developer is seeking channel partners to go to market and is working to add the solution into GSA Schedule 70 to facilitate acquisition and actively is pursuing SaaS pilots.

Distributed Incident Management System

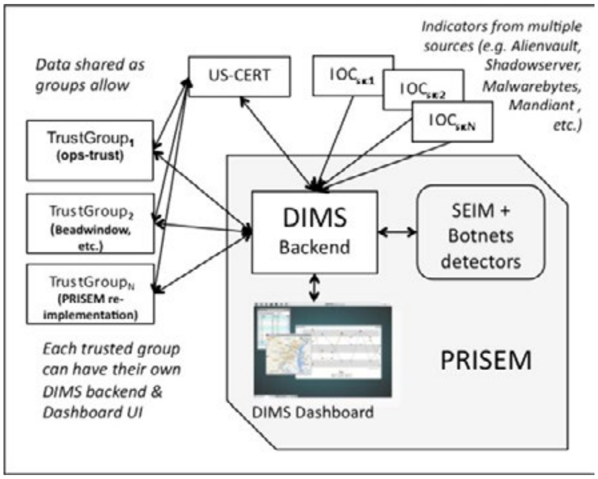
University of Washington

David Dittrich
dittrich@u.washington.edu

Dr. Ann Cox, CSD IMAM Program Manager
ann.cox@hq.dhs.gov

Overview

The 2016 Verizon Data Breach Investigation Report shows that more than 33% of security incidents are due to application and configuration errors. The budgets of state, local, territorial and tribal (SLTT) government entities are strained, yet they still are responsible for securing public data and systems. The Distributed Incident Management System (DIMS) project brings multiple open-source security and data-processing tools into an open platform by leveraging existing tools and threat information feeds to address the needs of SLTT system security administrators in a manageable and affordable way.


Indicators from multiple sources (e.g. Alienvault, Shadowserver, Malwarebytes, Mandiant , etc.)
Data shared as groups allow
US-CERT
IOC_{src1}
IOC_{src2}
IOC_{srcN}
TrustGroup_1 (ops-trust)
TrustGroup_2 (Beadwindow, etc.)
TrustGroup_N (PRISEM re-implementation)
DIMS Backend
SEIM + Botnets detectors
PRISEM
DIMS Dashboard
Each trusted group can have their own DIMS backend & Dashboard UI

Customer Need

Lower cost and more security are goals for nearly all networks. Configuration errors are a primary cause of system vulnerability. Reduced complexity of the configuration process improves security, so that fewer configuration mistakes occur, leading to lower operating costs. Through automation of installation and configuration of open-source operating systems, open-source security tools, and ongoing system administration functions, the solution reduces complexity and system administration overhead.

Approach

The technology provides a reference implementation of a small-scale distributed Linux platform using a “hybrid-cloud” model combining a bare-metal, virtual machine and containers in a scalable and securable deployment.

Benefits

Open-source software tool developers and system administrators operating the technology’s deployments will benefit from the agile software development model, development and operations support, and continuous integration mechanisms.

Competitive Advantage

More than 20 years of secure system administration of multiple Linux influences and incident-response expertise underlies the technology’s design model. No similar reference model of this scope exists in the open-source community.

Next Steps

The platform underwent red-team assessment in the fourth quarter of 2016. It is now in a pilot deployment and field-testing phase that will last the first nine months of 2017.

ImmuneSoft

Software Immune System for Embedded Devices

BlueRISC

Jeffry Gummeson
jeff@bluerisc.com

Dr. Ann Cox, CSD IMAM Program Manager
ann.cox@hq.dhs.gov

Overview

BlueRISC's 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 being made.

Customer Need

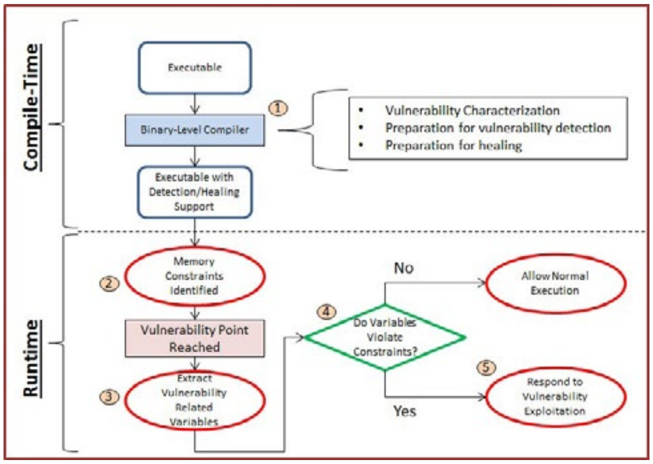
With the proliferation of the Internet of Things (IoT), the role of embedded systems has grown substantially in recent years. These systems are increasingly being used to perform critical tasks ranging from controlling critical infrastructure to managing communications to controlling medical devices. Their use in performing these sensitive tasks has incentivized a growing number of attacks against them.

Approach

Rather than following the ad-hoc mindset of traditional vulnerability patching, this technology is a hybrid approach, spanning a static binary analysis and a runtime exploitation detection and healing system. When encountered, attacks are detected prior to exploitation, preventing an attacker from leaking system data or making malicious modifications.

Benefits

Due to the generic nature of its program analysis-based vulnerability characterization, the technology is applicable to a wide range of vulnerabilities; specific knowledge of a vulnerability is not required to heal it. Its runtime detection system enables it to not only detect "silent" vulnerabilities, which do not make system modifications and otherwise go undetected, but also more traditional exploitations that result in a malicious system modification. Vulnerability characterization is performed at the binary-level, making it applicable to legacy systems where source code is unavailable.


Compile-Time
Executable
1
Binary-Level Compiler
Vulnerability Characterization
Preparation for vulnerability detection
Preparation for healing
Executable with Detection/Healing Support
Runtime
2
Memory Constraints Identified
Vulnerability Point Reached
3
Extract Vulnerability Related Variables
4
Do Variables Violate Constraints?
No
Allow Normal Execution
Yes
5
Respond to Vulnerability Exploitation

ImmuneSoft System Architecture

Competitive Advantage

The platform, while using binary-level static analyses for characterization, ultimately relies on runtime interactions to drive the healing solution. This reliance translates into a solution that is not only feasible but also has minimal performance and code-size overhead when deployed, while still successfully healing codes against future exploitation attempts.

Next Steps

The toolkit associated with the technology is being implemented. This toolkit will support autonomous healing as well as provide support for static, vulnerability-centric visualization of embedded software with specific guidance regarding the insertion of vulnerability mitigations.

Science of Internet Security: Technology and Experimental Research

University of California San Diego

KC Claffy
kc@caida.org

Dr. Ann Cox, CSD IMAM Program Manager
ann.cox@hq.dhs.gov

Overview

The Science of Internet Security: Technology and Experimental Research (SISTER) project builds on the Center for Applied Internet Data Analysis's (CAIDA) 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 measurement of security-relevant properties and behavior of the global Internet.

Customer Need

The opacity of Internet infrastructure limits the capabilities of research and development 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

The project combines a series of targeted activities that demonstrate and illuminate the capabilities of the current infrastructure to address specific articulated needs of the DHS S&T community. Researchers are focusing their 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 and Domain Name System).

Benefits

The project results will support macroscopic security and stability monitoring through 24/7 reachability probing of the entire 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, identify grey market IPv4 address transfers and produce monthly lists of candidate transferred prefixes, and enable on-demand, mapping and querying of router-level topology data.

Competitive Advantage

CAIDA, using the Ark infrastructure, has gathered the largest set of network topology data available to academic researchers. This infrastructure and data is used by SISTER for a broad spectrum of network scientific 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 cyber security vulnerabilities, from global scale to individual networks.

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

Brigham Young University

Sean Warnick
sean@cs.byu.edu

Dr. Ann Cox, CSD IMAM Program Manager
ann.cox@hq.dhs.gov

Overview

The Systemic-Risk Assessment Tools for Cyber-Physical-Human Infrastructures leverage systematic methods for evaluating cyber-physical-human systems and identifying weak points that could destabilize, hi-jack or infer critical state information about a system. Results include enhanced situational awareness, vulner-ability assessment, countermeasure development, and counterfactual exploration. Previous applications in-clude financial systems, air traffic control, water man-agement, data-driven agriculture, and manufacturing.

Customer Need

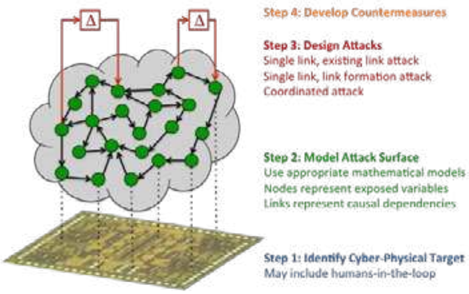
Identifying intrinsic vulnerabilities within systems or infrastructures is an unmet customer need. Critical infra-structure are typically large-scale physical systems with an essential information technology component for computation and communication for distributed deci-sion processes such as the smart grid. These systems of-ten 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 trig-gering 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 oper-ational model of the system's attack surface.

This attack surface is used to design attacks based on particular mission-focused objectives and assumed constraints. Constraints on the attack limit its operational capabilities such as restricting it to a singlelink attack on an existing link versus a multiple-link, coordinated attack


Δ
Δ
Step 4: Develop Countermeasures
Step 3: Design Attacks
Single link, existing link attack
Single link, link formation attack
Coordinated attack
Step 2: Model Attack Surface
Use appropriate mathematical models
Nodes represent exposed variables
Links represent causal dependencies
Step 1: Identify Cyber-Physical Target
May include humans-in-the-loop

This systematic attack design method for cyber-physical-human systems clearly identifies intrinsic vulnerabilities.

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 as-sumed to be available externally to outsiders such as currently known exploits supported by particular com-munications protocols or software platforms. As a result, the analysis is technology neutral, yet specific to the particular way the system processes and moves infor-mation. Early work has demonstrated this methodology on critical infrastructure systems, including water-management systems, cyber-enabled precision agricul-ture 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 IMAM Program Manager
ann.cox@hq.dhs.gov

Overview

Many factors cause Internet outages—from big events like Hurricane Sandy in 2012 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 on 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.

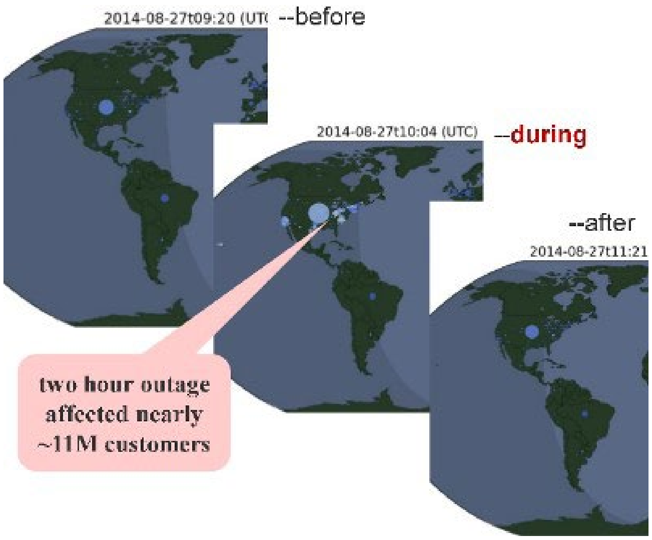
The technology detects outages across the Internet by adaptively probing all 24 address blocks where at least 15 addresses reply to pings (as of 2016 that's about 4.1 million blocks). The solution's algorithms integrate measurements from multiple sites to avoid misinterpreting local problems and cluster and visualize outages across the entire IPv4 Internet.

Benefits

Researchers are developing 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

The technology has compiled new data about Internet outages that is available without cost to researchers and industry. The research provides coverage of more than 4 million network blocks around the world. Complementing commercial services that observe website reliability, it detects outages in edge networks and provides known precision, detecting outages as early as within six minutes of occurrence.


2014-08-27t09:20 (UT(--before
2014-08-27t10:04 (UTC) --during
--after
2014-08-27t11:21
two hour outage affected nearly ~11M customers

A map depicting an Internet outage affecting 11 million U.S. users on August 27, 2014. Circle size represents numbers of affected networks at each location

Next Steps

Researchers are collaborating with the Federal Communications Commission to understand the applicability of the approach to their 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, ACM SIGCOMM, 2013 http://doi.acm.org/10.1145/2486001.2486017.

TrustBase

A Platform for Deploying Certificate-Based Authentication Services

Brigham Young University

Daniel Zappala
zappala@cs.byu.edu

Dr. Ann Cox, CSD IMAM Program Manager
ann.cox@hq.dhs.gov

Overview

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

Customer Need

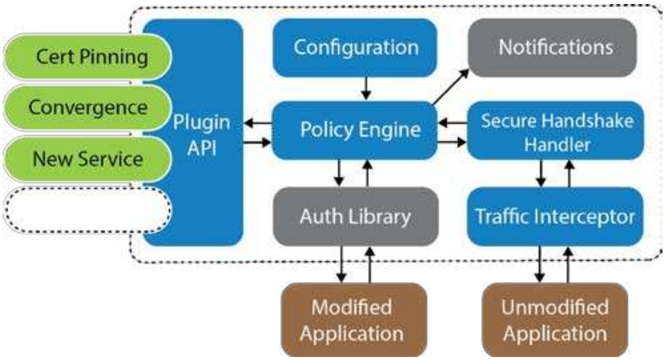
Internet infrastructure needs better ways to validate the certificates that vouch for server identities. There are two important flaws in how this validation is conducted today: first, applications often don't properly validate certificates due to developer mistakes; second, even the best applications 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 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 designed a research prototype implementation for Linux and demonstrated it has negligible overhead. They also 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 also have taken numerous steps to harden the Linux implementation.



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

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 properly followed.

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 a Windows implementation, an application programming interface for applications to call the system directly, and additional authentication services. They also are planning extensive usability testing. For code and questions, contact Ann Cox at Ann.Cox@hq.dhs.gov.

SOFTWARE ASSURANCE:

- Software Quality Assurance: CodeHawk Automated Malware Analyzer
- Software Quality Assurance: Code Ray: Hybrid Application Security Testing
- Software Quality Assurance: Hybrid Analysis Mapping: Software Assurance Enhancement Technology
- Software Assurance Marketplace

CodeHawk Automated Malware Analyzer

Kestrel Technology

Henny Sipma
sipma@kestreltechnology.com

Kevin Greene, CSD SQA Program Manager
kevin.greene@hq.dhs.gov

Overview

The CodeHawk Automated Malware Analyzer (CHAMA) is a tool for semantic static analysis of malware using abstract interpretation technology developed by Kestrel Technology. It performs a fully automatic, deep semantic analysis of an x86 PE executable and outputs a report that identifies significant data flows and type information. It provides a detailed view of the executable behavior that can be used to extract indicators of compromise and semantic features for machine learning.

Customer Need

The tool is targeted toward several user groups, including public and government entities responsible for identification and analysis of the latest malware. Other target groups include threat-intelligence companies that need to augment their "sandbox" dynamic analysis with static analysis and companies that need advanced semantic-level feature extraction to identify advanced malware. Service companies that require semantic-level analysis of advanced malware threats, and analysts who need to automate malware analysis when using disassemblers can also benefit from using this tool.

Approach

Using the CodeHawk abstract interpretation analysis engine, the analysis tool uses intra- and inter-procedural data propagation to collect information on data retrieved or received from the system or network, data sent to the network, and actions performed on the computer and peripherals. The analysis results provide host- and network-based indicators and input and output indicators. CHAMA assists in detecting suspicious activity by associating predefined and user-defined predicates to library functions that identify the call itself as suspicious or identify unusual combinations of arguments or flags.

Benefits

The tool complements current malware identification and analysis tools by automating static analysis of malware and enabling machine learning based on semantic features to allow detection of complex sophisticated malware. It also provides insight into sophisticated malware functionality using static analysis as well as detailed Chief Information Security Officer-level reporting of what data was accessed by malware and where it was sent to understand the damage done.

Competitive Advantages

The analysis is not limited by providing syntactic analysis with no behavioral analysis to understand malware functionality. The tool provides 80 percent to 100 percent code coverage, which may be missed by symbolic execution, and is capable of analyzing malware that is triggered by a specific event or is detected in a debugger.

Next Steps

CHAMA is available as an automated tool. Organizations that want to evaluate the tool may contact Kestrel Technologies about using it under an evaluation license.

.

Code Ray

Hybrid Application Security Testing

Secure Decisions

Kenneth Prole
ken.prole@securedecisions.com

Kevin Greene, CSD SQA Program Manager
kevin.greene@hq.dhs.gov

Overview

Code Ray combines the results of both static and dynamic application security testing to highlight software vulnerabilities in the source code that are exploitable by an external attacker. Developed by Secure Decisions, the technology also maps software vulnerabilities to industry standards to make it easier to find and fix highest-priority vulnerabilities.

Customer Need

To avoid vulnerabilities, software professionals must run application security tests to discover vulnerabilities before attackers. To achieve the greatest coverage, users must run several static source code analyzers, dynamic penetration testing tools and manual code analyses. It is difficult and time consuming to create a consolidated set of results that show all vulnerabilities in the source code, including the vulnerabilities that are visible to an attacker. It's also time consuming to prioritize the thousands of vulnerabilities that typically are found so the most critical are corrected.

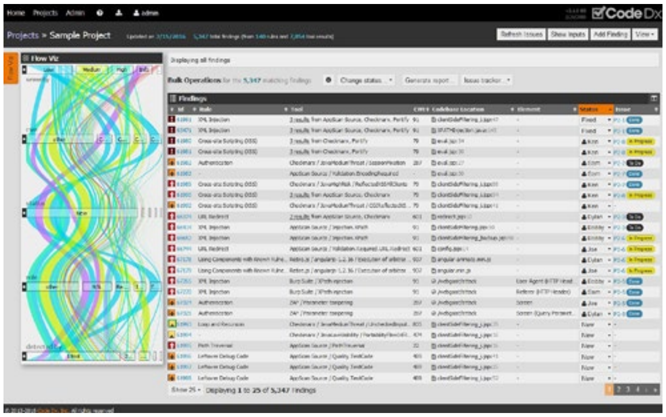
Approach

The technology engages Hybrid Application Security Testing (HAST) and correlates and normalizes the output of Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST) tools using runtime instrumentation and Common Weakness Enumeration (CWE).

Code Ray monitors an application during DAST using runtime instrumentation to store the execution path that produced the test results and uses runtime instrumentation traces to map SAST result-source locations to the observed execution paths. The correlation is enhanced by normalizing the DAST and SAST results using CWE as a common frame of reference. Using the merged DAST-to-SAST results, Code Ray maps the correlated findings to selected industry standards and widely recognized compliance standards such as the Open Web Application Security Project Top 10 and SysAdmin, Audit, Network and Security Top 25. In the last step, the results are displayed in a simplified risk-management framework.

Benefits

The technology provides software developers, testers, security analysts and auditors improved vulnerability coverage, improved accuracy, easier prioritization of the most severe vulnerabilities, remediation guidance, and improved communication through visual interface.



Competitive Advantage

The consolidated results are easier and quicker to interpret than the current state-of-the-art that requires sequential reviewing and mental correlations of disparate results from multiple application security testing techniques. The transition path to Code Dx, a software-vulnerability management system commercially available and accessible in the DHS Software Assurance Marketplace (SWAMP), jumps the hurdles that many small- to medium-size businesses face: time to learn and cost.

Next Steps

Code Ray is being transitioned into Code Dx. After this transition is completed a free educational version will be available to institutions that teach application security testing.

Hybrid Analysis Mapping

Software Assurance Enhancement Technology

Denim Group

Dan Cornell
dan@denimgroup.com

Kevin Greene, CSD SQA Program Manager
kevin.greene@hq.dhs.gov

Overview

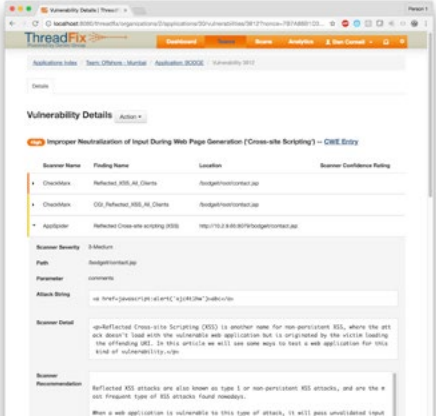
Organizations are at risk because of vulnerabilities in the software systems they develop and deploy. Static Analysis Security Testing (SAST) and Dynamic Analysis Security Testing (DAST) technologies can help software assurance teams identify potential weaknesses and vulnerabilities in software, but this approach requires the use of multiple technologies. Hybrid Analysis Mapping (HAM) technology developed by Denim Group provides software assurance teams the ability to efficiently correlate the results of different security testing technologies to provide better insight into the security state of software systems.

Customer Need

Organizations testing the security of software systems must use multiple technologies to obtain sufficient test coverage. Unfortunately, the results produced by these disparate tools are provided in incompatible formats, leaving organizations with volumes of data that require manual analysis and correlation. HAM allows security analysts to efficiently correlate and analyze this data to make decisions about vulnerability remediation. HAM also can be used to increase the quality of security testing, resulting in superior test coverage and deeper analysis.

Approach

When provided with application source code, the HAM technology works by detecting the language and application framework used by the application. HAM identifies all URLs the running application will respond to as well as all inputs that can change the behavior of the application. For each of these attack surface points, HAM tracks the location in the application source code responsible. Based on this attack surface model, HAM allows the coordination of the attack surface of DAST scanning results with the source code location of SAST scanning results.



Vulnerability Details

High Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') -- CWE Entry

Scanner Name	Finding Name	Location	Scanner Confidence Rating
CheckMarx	Reflected_XSS_All_Clients	/bodgeit/root/contact.jsp	
CheckMarx	CGI_Reflected_XSS_All_Clients	/bodgeit/root/contact.jsp	
AppSpider	Reflected Cross-site scripting (XSS)	http://10.2.9.66:8079/bodgeit/contact.jsp	

Scanner Severity: 3-Medium

Path: /bodgeit/contact.jsp

Parameter: comments

Attack String:

```
<a href=javascript:alert('xjc4tJhw')>abc</a>
```

Scanner Detail:

```
<p>Reflected Cross-site Scripting (XSS) is another name for non-persistent XSS, where the att
ack doesn't load with the vulnerable web application but is originated by the victim loading
 the offending URI. In this article we will see some ways to test a web application for this
 kind of vulnerability.</p>
```

Scanner Recommendation:

```
Reflected XSS attacks are also known as type 1 or non-persistent XSS attacks, and are the m
ost frequent type of XSS attacks found nowadays.

When a web application is vulnerable to this type of attack, it will pass unvalidated input
```

Benefits

HAM gives software assurance teams more comprehensive testing results, which enables the team to more efficiently consume the results and turn them into actionable remediation recommendations. This attack surface model also can be used for additional operations that held software assurance teams increase the fidelity of security testing as well as accelerate the remediation of identified vulnerabilities.

Competitive Advantage

HAM is included in the ThreadFix application vulnerability management platform. This allows software assurance teams to use HAM across their entire portfolio of applications. Also, making aspects of HAM technology available through an open-source license has facilitated the creation of a user's and contributor's community that is accelerating the adoption and evolution of the technology.

Next Steps

HAM is available for pilot usage via the open-source ThreadFix Community Edition and commercial ThreadFix Enterprise Edition software platforms.

Software Assurance Marketplace

Irene Landrum
llandrum@continuousassurance.org

Kevin Greene, CSD SWAMP Program Manager
kevin.greene@hq.dhs.gov

Overview

The Software Assurance Marketplace (SWAMP) is a no-cost software assurance testing platform that combines an array of open-source and commercial software assurance tools with advanced high-throughput computing. SWAMP also includes a growing library of open-source applications with known vulnerabilities to help developers improve the effectiveness of their static and dynamic analysis tools. With the computing capacity required to support continuous assurance, SWAMP provides the automation to continuously run multiple analysis tools on software packages. Software and tool developers can use an integrated results viewer to display weakness reports with integrated common weakness enumerations from multiple tools.

Customer Need

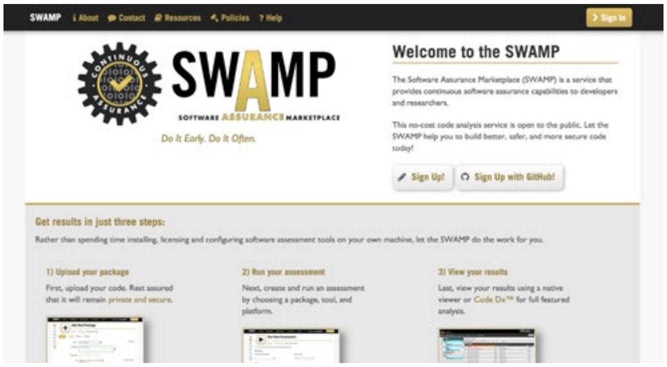
SWAMP promotes continuous assurance technologies and practices through an open and collaborative framework that protects confidential data and facilitates sharing, making it easier for software and tool developers to adopt continuous assurance practices.

Our Approach

The Morgridge Institute for Research, a private, nonprofit research institute located at the University of Wisconsin-Madison, leads SWAMP and hosts the infrastructure, core development and software-testing teams. Additional participants are the University of Wisconsin-Madison, Indiana University and University of Illinois at Urbana-Champaign. Through SWAMP's Bring Your Own Code program, developers can submit code through a secure interface, test the software, and access analysis results. SWAMP's do-it-early, do-it-often concept of continuous assurance enables developers to build security into their continuous-integration and continuous-delivery pipelines.

Benefits

SWAMP provides a powerful, flexible and secure facility for organizations and open-source developers to institute software assurance practices. The supported platforms, tools and packages are maintained by the SWAMP team, lowering the obstacles to performing software security assessments. SWAMP encourages software developers, software assurance researchers, infrastructure operators, educators, students and individuals from open-source, government and commercial groups to assess their software—developed and acquired—to promote a more stable and secure software ecosystem.



Welcome to the SWAMP

The Software Assurance Marketplace (SWAMP) is a service that provides continuous software assurance capabilities to developers and researchers.

This no-cost code analysis service is open to the public. Let the SWAMP help you to build better, safer, and more secure code today!

Get results in just three steps:

Rather than spending time installing, licensing and configuring software assessment tools on your own machine, let the SWAMP do the work for you.

1) Upload your package

First, upload your code. Rest assured that it will remain private and secure.

2) Run your assessment

Next, create and run an assessment by choosing a package, tool, and platform.

3) View your results

Last, view your results using a native viewer or Code Dx™ for full featured analysis.

Competitive Advantage

Unlike similar offerings of no-cost software assessment services by commercial entities, SWAMP is designed, built, operated and supported by a partnership of four nonprofit research institutions that have a long, demonstrated commitment to open-source, cybersecurity, privacy and software assessment. Also, the participants are driven by an underpinning vision of an open and continuous software assurance framework that facilitates easy adoption of new software analysis technologies.

Next Steps

The SWAMP team has developed SWAMP-in-a-Box (SiB), an onsite solution that's available on a GitHub repository. SiB is designed to integrate in continuous integration and delivery environments. Start using SWAMP at https://mir-swamp.org/. Learn more about continuous assurance at https://continuousassurance.org/. More information about SiB is available at https://continuousassurance.org/swamp-in-a-box/.

TRANSITION TO PRACTICE:

- Transition to Practice: Accelerating the Pace of Technology Transition

Transition to Practice

Accelerating the Pace of Technology Transition

Nadia Carlsten, CSD Transition to Practice 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 National Science Foundation-funded academic institutions. The program's goal is to transition this research into the Homeland Security Enterprise through partnerships and commercialization. Technologies selected by TTP go through a 36-month process that focuses on 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 are 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
- Cloud Security:
- CryptAC: Security Data for Public Clouds
- Keylime: Enabling Trust in the Cloud

Cryptography and Key Management:

- LOCKMA: Lincoln Open Cryptographic Key Management Architecture
- Quantum Security: Quantum Random Number Generator and Quantum Secured Communications
- 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 IoT 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 Detection on Streaming Data

ONLINE
www.dhs.gov/cyber-research

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

TWITTER
@dhsscitech

FACEBOOK
Facebook.com/dhsscitech

YOUTUBE
www.youtube.com/dhsscitech

PERISCOPE
@dhsscitech