Transition to Practice Technology Guide

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) Transition to Practice (TTP) Technology Guide. This guide is the culmination of extensive foraging efforts to identify promising technologies developed at Department of Energy National Laboratories, Department of Defense-affiliated laboratories, Federally Funded Research and Development Centers (FFRDCs), and academic institutions. We're excited to share these promising cybersecurity solutions with you.

Through the TTP Program, S&T is identifying innovative, federally funded research with the goal of helping to transition this research into the Homeland Security Enterprise through partnerships and commercialization. This guide represents an important step in that process, as all the technologies included here are ready to be piloted in an operational environment or ready to be transitioned to commercially available products. Contact the DHS S&T TTP program at ST.TTP@hq.dhs.gov if you're interested in piloting, licensing, or commercializing any of these technologies.

This technology guide, which is updated and published annually, is the fifth volume and features eight new technologies, along with detailed summaries for 15 technologies still active in the three-year TTP program, and information for 17 additional technologies from previous annual cohorts. As of June 2018, 15 of 40 technologies from the TTP program's first five years have been commercialized, five have been made available as open-source software, and several others are in various stages of the licensing process. We're excited for the research teams and their licensing partners and wish them success on their journey to the marketplace. Ultimately, their success will result in better cybersecurity for the nation, the global online community and you.

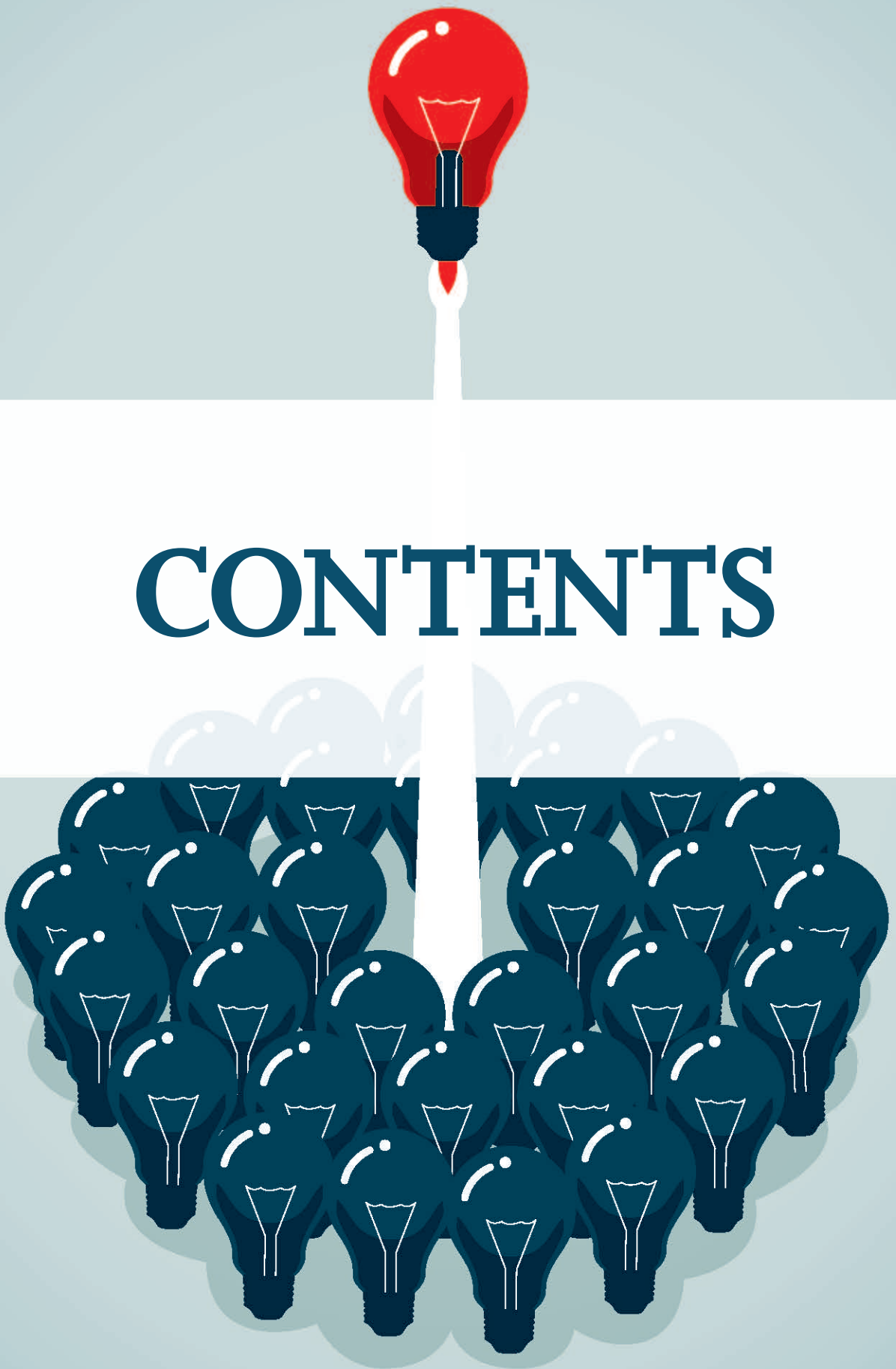
As you reflect on the cybersecurity capability gaps in your own organization, please share your thoughts with the TTP program manager (ST.TTP@hq.dhs.gov). Your input will help us identify timely solutions and inform future research efforts. Again, it's our pleasure to introduce you to the TTP program and these newly developed cybersecurity tools from the federal R&D community.

Sincerely,

Douglas Maughan
Cyber Security Division Director
DHS S&T

Nadia Carlsten
TTP Program Manager
DHS S&T

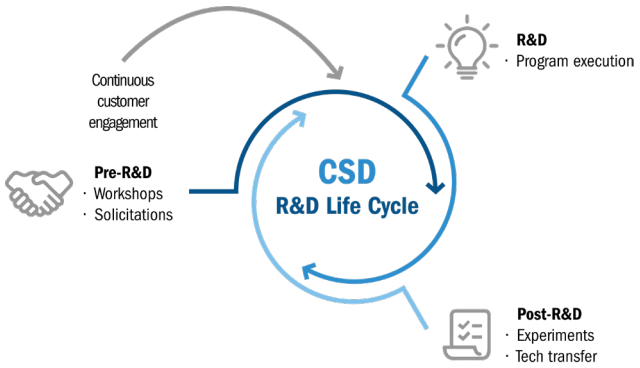
CONTENTS



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

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Leads Development of Next-Generation Cybersecurity Solutions

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



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

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

S&T's Broad Cybersecurity Technology and Capability Development Portfolio

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

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

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

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

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

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

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

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

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

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

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

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

Preparing for Emerging Cyber Threats

Through its R&D focus, 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.

Transition to Practice
Accelerating the Pace of Technology Transition

Nadia Carlsten
ST.TTP@hq.dhs.gov

Overview

Addressing rapidly evolving threats requires a better way to bridge the gap between research and the marketplace. The Transition to Practice (TTP) program addresses this critical need by identifying promising federally funded technologies and accelerating their transition into the marketplace through partnerships and commercialization. By facilitating the adoption of these solutions into broader use and creating more efficient transition processes, TTP is helping turn research into reality.

Motivation

The federal government spends more than $1 billon on unclassified cybersecurity research every year, however, very little of that research reaches the marketplace. This divide between research and commercialization, commonly called the "Valley of Death", is often the result of a lack of partnerships between the government and the private sector, insufficient resources, and inefficient processes for transferring technology out of a laboratory environment.

Since 2011, the federal government has made accelerating the transition of cybersecurity technology into widespread deployment a priority for improving the nation's cybersecurity infrastructure. The successful transition of technology continues to be a critical area in the 2016 Federal Cybersecurity R&D Strategic Plan.

TTP Goals

The TTP program's three goals are to:

- identify mature technologies that address an existing or imminent cybersecurity gap
- increase utilization through partnerships, product development efforts, and marketing strategies
- improve the long term ability of federal research laboratories to transition technology efficiently

How It Works

The TTP program targets technologies developed through federal R&D that demonstrate a high probability of successful transition to the commercial market within three years and are expected to have a notable impact on cybersecurity posture.

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 training and market research; and connecting researchers with investors and potential licensors through outreach, industry events, and Technology Demonstration Days.

The Value

20 of 40 technologies from the TTP program's first five years have already transitioned, and numerous others are in various stages of the licensing process.

The TTP program provides a unique connection point between researchers, users, and investors, maximizing the potential for wide commercial distribution and adoption, and improving alignment between the research and operational communities. Through TTP program activities, research teams are active participants in the commercialization process, gaining valuable experience. Cybersecurity professionals benefit from piloting, licensing, and commercializing a range of validated, innovative technologies that could become valuable cybersecurity solutions.

In addition, the TTP program develops technology transition processes that can be adopted by others and become self-sustaining—in essence, building a lasting bridge over the "Valley of Death".

For more information about the TTP Program, email **ST.TTP@hq.dhs.gov**.

5th COHORT OF TECHNOLOGIES:

- CHARIOT: Filtering and Enriching Relevant Content
- Keylime: Enabling TPM-Based Trust in the Cloud
- QUASAR: Strategic Decision Support for Cyber Defense Planning
- APE: A Novel Intrusion Prevention System for Android
- Akatosh: Automated Cyber Incident Verification and Impact Analysis
- CPAD: Real-Time Cyber-Physical Attack Detection
- StreamWorks: Continuous Pattern Detection on Streaming Data
- PEACE: Policy Enforcement and Access Control for End-points

CHARIOT: Filtering and Enriching Relevant Content

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Jason Matterer
jason.matterer@ll.mit.edu

This material is based upon work supported by the Department of Defense under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.

Overview

In the field of intelligence there is a truism that the information needed to thwart an attack is often available to the analysts, but lost in the mass of other, irrelevant, data. Cyber HLT Analysis, Reasoning, and Inference for Online Threats (CHARIOT) is a system that addresses this problem by filtering open-source social media to eliminate topics irrelevant to the searcher. It uses a combination of traditional machine learning along with novel transfer learning and graph partitioning techniques to first filter and then categorize and enrich the information available to analysts. CHARIOT reduces the time necessary to evaluate a document, as well as the amount of off-path research.

Customer Need

As the amount of malware and resultant cyber attacks increases, the need for analysts to find information about potential attackers, technologies, and defenses has grown beyond current capacity. Vital information about cyber attacks is being missed due to the explosion of online data and limited manpower. Manually sorting through portions of existing social media and online forums is a time consuming and expensive process.

Finding pertinent intelligence in a sea of noise is already a challenging problem, but there are additional challenges that can vary by social media platform or online forum:

- It is very difficult to know where to look online.
- Jargon may be extensively used.
- Language can vary by topic and region, sometimes in the same discussion.
- Data with relevant information already labeled is scarce.

Current state-of-the-art methods rely on user-crafted search queries that suffer from large numbers of misses and false positives. Given the volume of web text data, such methods either do not reduce the number of results to a manageable level or use overly restrictive search terms resulting in potentially useful information being lost.

Our Approach

CHARIOT leverages example documents from an analyst or, for more general use, from topically relevant social media discussions. The system is trained to distinguish documents similar to the provided samples, and to automatically filter out irrelevant content in similar sources. An analyst can refine any results using an active-learning framework that allows them to build models personalized to their task.

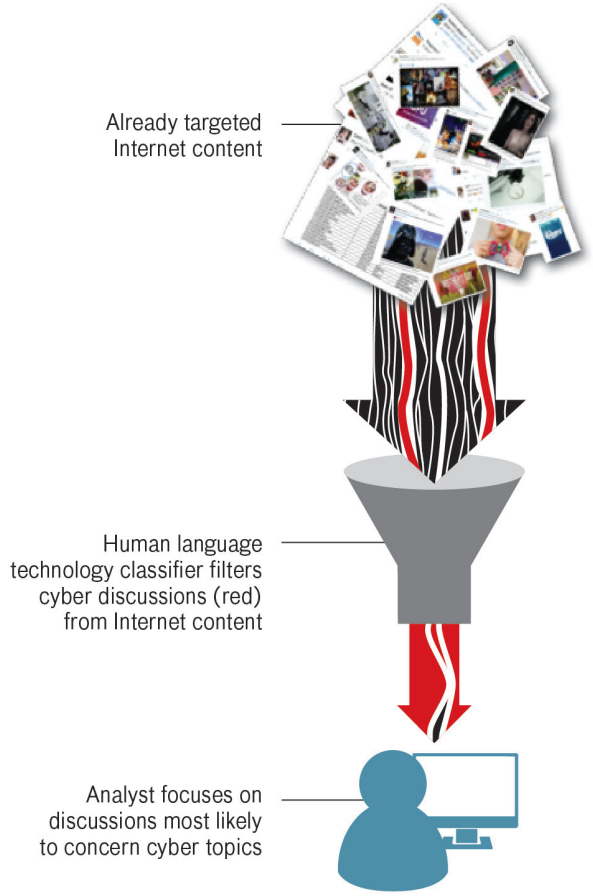


Figure 1: *Data flow from social media sources, through CHARIOT system, to analyst.*

CHARIOT's novel transfer learning algorithms enable it to repurpose a model trained on one source of documents for use with another (e.g., using a model trained on Reddit to find relevant data on Twitter). This mitigates the challenges of changing language use and jargon, as well as that of finding sufficient amounts of relevant labeled data.

Once filtered, CHARIOT enriches relevant documents with domain specific entities and topics along with links to information about each. These entities and topics are linked to a knowledge graph, providing context to the analyst, which reduces the amount of off-path research required to evaluate documents with new technologies or terminology, and consequently the average amount of time analysts require to evaluate a single document.

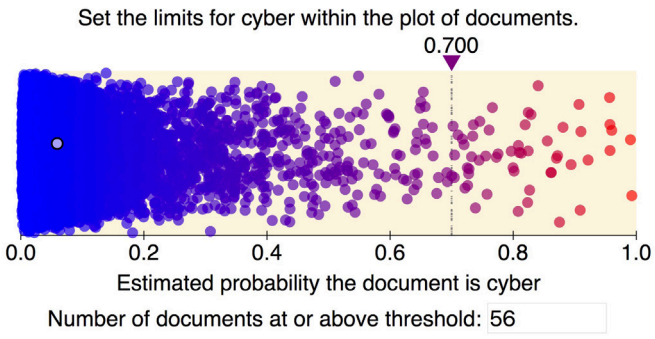


Figure 2: *CHARIOT prototype after processing 17,000 files, with a threshold set to 56 documents. More red cyber content appears to the right.*

Benefits

CHARIOT improves analyst efficiency by providing a smaller number of more relevant documents for analyst review, allowing the reuse of already trained models, and providing domain-specific context.

When used as a filter, CHARIOT reduces a corpus of 100,000 documents, of which 1,000 are relevant, to 1,148 documents, of which 900 are relevant. This reduces the volume by two orders of magnitude, and increases the proportion of relevant content from one percent to 78 percent.

The novel transfer learning algorithm increases the agility of analysts and allows them to move from source to source without bogging down in irrelevant data.

On experimental data the algorithm improved the hit rate from 10 percent (no transfer learning) to 92 percent (with our transfer learning method).

Competitive Advantage

Existing approaches, like keyword-based search tools, work best when searching for well-defined, homogeneous topics such as specific vulnerabilities or exploits. Those approaches fail when applied to more complicated, varied, or abstract topics like developing new capabilities or planning sophisticated attacks.

CHARIOT fills this gap by providing a simple method for analysts to filter massive amounts of data based on example documents. Rather than attempting to generate a perfect query (descriptive search), analysts can provide sample documents that would result from a descriptive search and allow the system to develop its own query matching relevant documents (prescriptive search).

To our knowledge, existing approaches to building domain-specific knowledge graphs rely heavily on manual processes. Our novel approach to extracting domain-specific topics and entities from existing knowledge graphs only requires the selection of a handful of initial topics, after which all relevant elements are automatically extracted.

Next Steps

The CHARIOT server and client are implemented as a Python Flask application and web page (respectively), and are ready to be deployed in a pilot program at the enterprise level. The system has been tested in a laboratory environment, and evaluated on both social media posts and other data of interest to analysts. We are seeking partners to deploy and test CHARIOT in an intelligence workflow to continue to improve the technology.

A subset of CHARIOT's features can be implemented as a standalone prototype that can run within a web browser with zero external dependencies. We are currently exploring use cases to use such a system as a portable analysis tool in environments where computing resources or connectivity are scarce.

Keylime: Enabling TPM-Based Trust in the Cloud

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Nabil Schear
nabil@ll.mit.edu

Dinara Doyle
dinara.doyle@ll.mit.edu

This material is based upon work supported by the Assistant Secretary of Defense for Research and Engineering under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Assistant Secretary of Defense for Research and Engineering.

Overview

Keylime enables users to securely bootstrap secrets (e.g., cryptographic keys, password, certificates, etc.) and continuously verify trust in their cloud computing resources without needing to trust their cloud provider. To accomplish this securely, Keylime uses the Trusted Platform Module (TPM), an industry standard hardware security chip. Keylime eliminates the complexity, compatibility, and performance issues that the TPM introduces. Using a clean easy-to-integrate abstraction, Keylime enables existing cloud security technologies such as storage and network encryption to seamlessly leverage the security of the TPM without themselves needing to be TPM-aware.

Keylime is designed from the ground-up to support cloud environments natively. It scales to secure thousands of simultaneous nodes, can detect and react to security violations in less than a second, and supports both physical and virtual cloud machines.

Customer Need

The proliferation and popularity of infrastructure-as-a-service (IaaS) cloud computing services means more cloud tenants are hosting sensitive, private, and business critical data and applications in the cloud. Unfortunately, today's IaaS cloud service providers do not furnish the building blocks necessary to establish a trusted and secure environment for hosting these sensitive resources. Tenants have limited ability to verify the underlying platform (e.g., hypervisor) when they deploy to the cloud and to ensure that the platform remains in a good state for the duration of their deployment. Additionally, current practices restrict tenants' ability to establish unique, unforgeable cryptographic identities for their cloud machines that are tied to a hardware root of trust. Often, identity is based solely on a software-based cryptographic solution or unverifiable trust in the provider.

Some organizations, for example, in the financial, biomedical, and government sectors, have not adopted IaaS cloud computing due to these security limitations. To address the needs of customers in sensitive industries, IaaS cloud providers need stronger security features.

Commodity trusted hardware, such as the TPM, has long been proposed as the solution for bootstrapping trust, enabling the detection of changes to system state that might indicate compromise, and establishing cryptographic identities. Unfortunately, TPMs have not been widely deployed in cloud environments due to their slow performance and incompatibility with existing cloud security technologies.

Figure 1: *Keylime relies upon an industry standard hardware security chip called a TPM. Keylime uses this chip to securely provision cryptographic keys that existing technology can use without needing to be "TPM-compatible".*

Our Approach

To address the challenges of deploying TPMs in the cloud, we created Keylime, an end-to-end IaaS trusted cloud key management service that supports secure identity bootstrapping, enables continuous system integrity monitoring, and seamlessly supports both virtual and physical cloud machines. The key contribution of our work is to create a trusted computing services interface that tenants can use to get the security benefits of the TPM while using existing cloud security technology that is not TPM-compatible (see Figure 1). We provide a clean and easy to use interface that can integrate with existing security technologies, including cloud servers provisioned with cloud-init, VPN secure communications, full disk encryption, and system configuration management using Puppet.

Benefits

Keylime allows users to perform two major actions while minimizing reliance on trust in the cloud provider: bootstrapping and continuous monitoring. Bootstrapping allows a user to provision secrets onto their cloud nodes. These secrets could be credentials for accessing other services, certificates for supporting HTTPS, cryptographic keys to unlock encrypted disks, and certificate authorities to root trust in other services. Continuous monitoring allows a user to be notified if one of their cloud machines has been compromised. These notifications can be triggered in a fraction of a second after the change to the machine's software integrity. Once notified, the user can take immediate action. For example, access to sensitive content can be revoked or the machine can be brought down for remediation.

Keylime can scale to handle thousands of simultaneous nodes and perform integrity checks on nodes at rates up to 2,500 integrity reports verified per second. Keylime can securely deliver secrets to cloud nodes in approximately 2s and can detect integrity measurement violations in as little as 110ms.

Competitive Advantage

The three major IaaS cloud services (Amazon EC2, Microsoft Azure, and Google Compute Engine) do not offer any means of verifying the platform on which customer code runs. These services require full and unverifiable trust in the cloud provider for security.

Cloud services like HyTrust and CoreOS Tectonic allow the cloud provider to leverage the TPM to create trusted environments for physical machines. Unfortunately, proof of this trust does not extend directly to the user. The user must still trust the provider to schedule their machines on platforms with TPMs.

Keylime offers the ability for users to verify trust in the TPM directly without having to trust the provider to do so for them. Keylime also provides seamless operation on both physical and virtual machines. We have developed a set of software patches that enable Keylime support for virtual machines with the Xen hypervisor and OpenStack cloud software stack, as depicted in Figure 2. No other product supports TPM-based security for virtual machines.

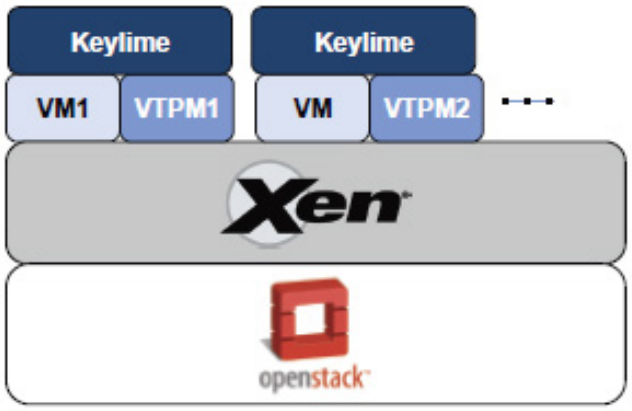


Figure 2: *Keylime integrates with the Xen hypervisor and supports secure virtual TPMs that are linked to the hardware TPM in the hypervisor. Keylime contains all the services and extensions for seamless operation as though the virtual machine were securely interacting with a physical TPM.*

Next Steps

Keylime can be used in bare metal IaaS cloud environments that support TPMs today. We are working to get the software patches we created for Keylime support in OpenStack integrated into an open source release of OpenStack. This would allow Keylime to be compatible with virtual machines in OpenStack-based IaaS environments in both public and private clouds.

We are seeking partners who are interested in implementing Keylime in their cloud environments. We are also looking for partners interested in deploying Keylime in existing bare-metal IaaS environments.

QUASAR: Strategic Decision Support for Cyber Defense Planning

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Richard Skowyra
richard.skowyra@ll.mit.edu

Steven Gomez
steven.gomez@ll.mit.edu

Hamed Okhravi
hamed.okhravi@ll.mit.edu

This material is based upon work supported under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. Air Force.

Overview

The Quantitative Attack Space Analysis and Reasoning (QUASAR) tool is a threat intelligence and decision support platform for cyber defense planners. It provides visualization and quantitative analytics for determining the security impact of deploying cyber defenses in a customer's enterprise environment. QUASAR enables intelligent, strategic decision making about what defensive investments are most valuable, how attackers may change their strategy in response, and what gaps in defense coverage remain.

Customer Need

Networks and systems, ranging from enterprise to industrial and tactical environments, are increasingly targeted by sophisticated attackers, including large criminal organizations and nation-states. These actors have access to resources that enable rapidly-evolving capabilities that not only bypass many current cyber defenses, but shift on-the-fly in order to deal with changing defensive postures.

Defense planners, such as CISOs, must choose the defenses in which to invest in order to mitigate an organization's exposure to cyber attacks. While there is a constantly growing suite of defensive cybersecurity products available in the market, their actual impact on sophisticated attackers is unclear. This makes it hard for defense planners to answer critical questions: What defenses are worth purchasing and deploying? How do they interact with one another? Are there gaps in coverage? What are attackers likely to try next and how can I best prepare? Ultimately, how can I best allocate resources to harden my organization?

Intelligent decision-making for cyber defense investment requires that defense planners have a service that provides what-if analysis of possible defense investments given all known cyber attack strategies in a particular attack domain (e.g. memory corruption). This analysis needs to be quantitative rather than qualitative, and consider not just the current state of the world but also the near-term evolution of attacker capabilities.

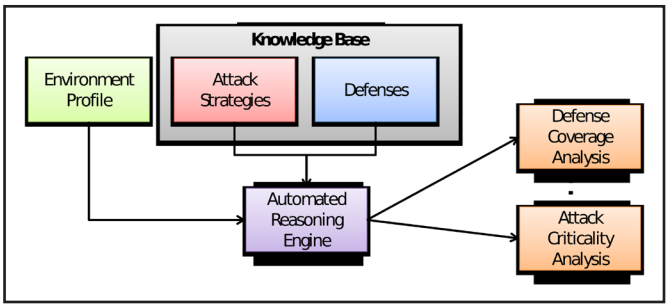


Figure 1: *QUASAR Architecture*

Our Approach

QUASAR is a software platform that enables automated reasoning and decision support about cyber attacks and defense. It has three components (shown in Figure 1): a knowledge base of cyber attack strategies and defenses, an automated reasoning engine, and a user interface for visualization and what-if analysis. The knowledge base is a mathematical model of cyber attack classes, as well as models of cyber defenses which constrain them. Operating over attack classes, as opposed to specific vulnerabilities or signatures, enables QUASAR to be both scalable, as it need not consider every version of every software program, and provide actionable results (e.g. what defenses are worth deploying). The knowledge base is populated and kept up to date by drawing on both threat intelligence data and academic cybersecurity research. QUASAR's current knowledge base –which can be easily extended to other attack domains – focuses on memory corruption attacks and defenses in particular.

QUASAR's automated reasoning engine combines this knowledge base with a high-level profile of the customer's environment (such as what operating systems are used) to create a tailor-made mathematical model using formal logic. The profile restricts results to only those attacks applicable to the customer, and only those defenses compatible with their systems. A combinatorial solver operates over this model to calculate the number of applicable attack classes that every compatible defense disrupts.

QUASAR's browser-based visualization and query front-end uses these results to display quantitative metrics

about the impact that proposed defenses will have on a customer's environment, such as the degree of defense coverage, what attack strategies remain viable even after defenses are deployed, and what additional defenses would provide the most mitigation. A variety of outputs are possible, such as the graph in Figure 2, which shows the memory corruption attack strategies to which a particular environment is most exposed. Defenses targeting these areas would thus provide the most coverage and maximally impede attackers.

A user can also explore what-if scenarios by adding or removing defenses or attacks interactively, or look at the impact of adding or removing new platforms to their enterprise environment (such as a Windows or Linux web server).

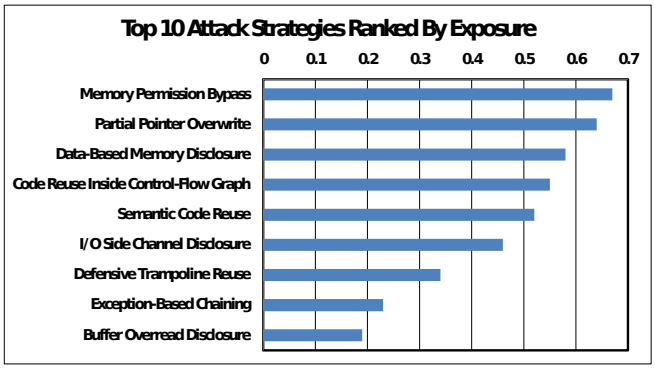


Figure 2: *Customer-specific ranking of the cyber attack strategies most effective against their environment*

Benefits

QUASAR enables intelligent hardening of deployed systems. Rather than choosing to install all possible defenses (which is both expensive and will impact performance), a defense planner can identify options that complement existing defenses and avoid overlap.

QUASAR identifies gaps in defense coverage early in the planning stage rather than later via penetration testing or when subjected to an attack. As attackers evolve new capabilities, QUASAR users can be informed of an emerging coverage gap and proactively move to close it.

QUASAR reveals when defensive techniques protect against only a narrow range of threats despite their broad claims. Users can either abandon these or augment them with complementary techniques for better coverage.

More broadly, defense planners can use QUASAR to determine which capabilities attackers are most incentivized to develop next given all modern defenses. This enables planners to anticipate and prepare for attacker strategies, rather than being forced to react once an attack is in progress.

Competitive Advantage

QUASAR provides not only reports on a customer's security posture, but also an automated reasoning and decision support system built around that data which enables interactive what-if analysis and quantitative metrics to compare current and future defenses. Its knowledge base is kept up-to-date and any query can be re-evaluated against new data at any time.

Threat intelligence and penetration testing services often only deliver static, qualitative reports and assessments against already-deployed defenses. If a customer's environment changes, or if new attack strategies appear, the recommendations may no longer be accurate. Those services that do provide continuous auditing do so at a very low level, such as tracking unpatched software vulnerabilities. This information cannot easily be used to inform high-level defense planning beyond creating, e.g., patching schedules.

Next Steps

QUASAR is currently being extended to support probabilistic and weighted attack and defense strategies. This enables customers to customize their analysis based on their environment.

We are looking for opportunities to broaden QUASAR's user base and are seeking operational partners interested in piloting the tool. It can be deployed either as a stand-alone tool that the customer uses to model their cybersecurity environment, or as a web service subscribed to by the customer. We are also looking for partners interested in licensing the QUASAR technology to provide this service to customers.

Finally, we are looking for partners interested in creating QUASAR knowledge bases for new security domains of interest to them, such as Web, mobile device, or IoT security. While QUASAR's current attacker strategy and defense model focuses on memory corruption in order combat malware, its approach to modeling attack strategies and defenses can be easily extended to many other fields of cybersecurity.

APE: A Novel Intrusion Prevention System for Android

Mark Mitchell
mmitchell@mitre.org

Overview

Unlike common laptop and desktop security products, current Android defenses are unable to proactively prevent network-based attacks. To bridge this gap, we have developed a patented, first-of-its-kind Intrusion Prevention System for Android devices (called APE) that prevents attacks before they occur. APE exists as an ordinary user space application on a device, and performs deep packet inspection and filtering of internet protocol version 4 (IPv4) traffic entering and leaving the device. APE is thus able to block malicious traffic and lower the attack profile of Android devices.

Customer Need

Android device users have a pressing need for next generation defenses against network-based attacks, because there are many ways an attacker can leverage vulnerabilities to compromise a device. From December 2016 through November 2017, there were 976 vulnerabilities disclosed for Android. Each vulnerability introduces a potential avenue for an attacker to compromise a device through malware or by simply directing a user to a malicious link or website, which can result in full device compromise. Upon compromising a device, an attacker can perform nefarious activities, such as spy on the user via the device's camera and microphone, or obtain sensitive data stored on the device, such as financial, social media, or other personal or business information. Current Android defenses are unable to prevent these network-based attacks proactively, relying instead on scans of the installed app list or monitoring of battery usage and other performance metrics. Given that antivirus apps cannot stop network attacks, there is an urgent need for a next generation intrusion prevention capability.

Our Approach

APE is a standard application that runs on an Android device and examines all IPv4 network traffic entering and leaving the device. This includes traffic using either cellular or Wi-Fi connections. The traffic is compared to a local rule set stored within the app and defines malicious behaviors. If a matching rule is found, the packet is blocked. A rule can be as simple as blacklisting a certain IP address, or disallowing a given protocol over a given port. Conversely, rules can be application-specific, such as identifying that a downloading video is attempting to execute an integer overflow. By evaluating the network traffic and blocking malicious traffic before it reaches the local apps on the device, APE prevents compromises before they occur. Figure 1 illustrates the filtering of inbound network traffic from the Internet. APE also evaluates and prevents malicious behavior in outbound network traffic, such as preventing data from being siphoned to known malware domains.

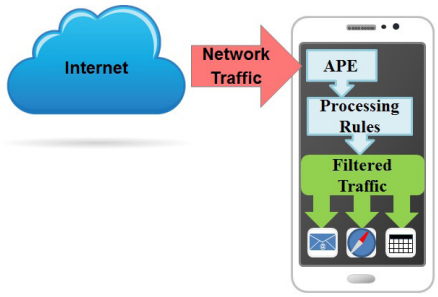


Figure 1: *APE compares all incoming traffic against a ruleset and blocks traffic matching rules that define malicious behavior. Though not illustrated here, outbound traffic is also filtered.*

Since APE exists as a normal user space app, it is simple to update the app and the associated ruleset. Updates are pushed out from the Google Play Store, similar to any other app. Updates to the rules are also pushed out as app updates.

Benefits

APE is a first of its kind Android security app that provides three major benefits:

1. Block known network attacks, completely negating the effect they would have had.
2. Mitigate newly discovered attacks by simply updating the ruleset, rather than updating the operating system (waiting for a vendor patch can takes months, if a patch is even issued at all).
3. Lower the device's attack profile by blocking unneeded ports and protocols, which makes it harder for attackers to search for vulnerabilities.

Importantly, these benefits are provided in a standard app without root access. This is crucial, as rooting a device bypasses several built-in security features.

Competitive Advantage

APE provides defensive capabilities not offered by any other Android apps. Figure 2 summarizes these competitive benefits. Specifically, APE is the only app for non-rooted devices that can examine packets before or after they are processed by an application, thus blocking attacks before compromise occurs.

In contrast, traditional smartphone antivirus apps simply scan the apps that are installed on the phone for viruses or malware, or monitor the usage of resources such as the battery. Such approaches have a number of downsides:

- Compromises are only detected after they occur. By the time a compromise is detected, sensitive data may have already been stolen.
- Once a traditional antivirus app has detected a compromise, the compromise must still be remediated, and there are cases where the app is unable to do this. This is far less effective than preventing a compromise from occurring altogether. Furthermore, a malware program may be extremely difficult to remove, and guard itself by becoming a device administrator, or by protecting itself with an unknown password.
- If an attacker can root the device, they may be able to disable or completely remove the antivirus app, before the app can take any action.

Mobile Device Management (MDM) products are also an insufficient alternative. While MDMs can configure devices to take protective measures such as disabling the camera or requiring a PIN, they are not able to inspect and block network traffic.

The only true alternative to APE is using a heavyweight VPN/IPS hardware appliance/proxy infrastructure. Such a setup is prohibitively expensive for individuals and small enterprises, significantly increases latency, and is dependent on the availability of the backend infrastructure. Since APE resides on the device as an app, it is always available, costs significantly less, and has a minimal performance impact.

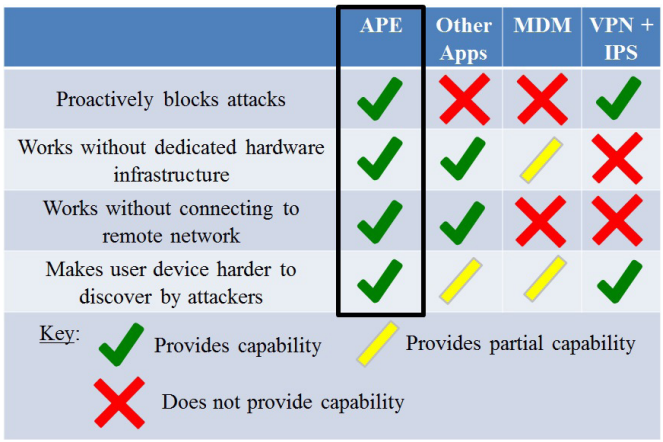


Figure 2: *APE provides a number of competitive benefits over other approaches*

Next Steps

APE has been implemented as a prototype Android app and demonstrated in a limited environment. We are seeking partners to pilot APE in their operational environments to provide feedback about desired enhancements.

The underlying technology has been submitted for a patent. APE licensees will benefit from access to the technology in the form of a reference implementation and to the IP protection afforded by the pending patent.

We are also exploring additional enhancements that could be added to APE:

- A machine learning feature to detect and block unknown attacks (i.e., 0-day exploits)
- A version of the app for Android TV and/or Android Wear (e.g., Android powered smartwatches); and a version of APE for Apple iOS
- Robust ad blocking to protect against malicious advertisements and increase performance and bandwidth.

Akatosh: Automated Cyber Incident Verification and Impact Analysis

Jared M. Smith
smithjm@ornl.gov

Aaron Ferber
ferberae@ornl.gov

Overview

Akatosh enables automated, real-time forensic analysis of endpoints after malware-attacks and other cyber security incidents by automatically maintaining detailed snapshots of host-level activity on endpoints over time. It achieves this by integrating intrusion detection systems (IDS) with forensic tools. The combination allows Akatosh to collect vast amounts of endpoint data and assists in verifying, tracking, and analyzing endpoints in real time. This provides operations personnel and analysts as well as managers and executives with continuous feedback on the impact of malicious software and other security incidents on endpoints in their network.

Customer Need

Forensic analysts and other operations personnel face two distinct and important problems. In the realm of computer security defense mechanisms, IDSs consume information like network packets, endpoint statistics, and other metrics that the IDS uses to pick out anomalous behavior, which potentially represent cyber attacks. Unfortunately, IDSs have high false alert rates and the sheer number of alerts over time can overwhelm security operations personnel, which makes correctly identifying actual cyber attacks difficult. Another problem faced by enterprises can be seen in a 2016 study by IBM and the Ponemon Institute[1], which found that among 383 companies, the cost of incident response and mitigation for a successful cyber attack accounted for 4 million USD on average per incident. over a quarter of the total cost was due to forensic activities associated with the breach. This cost largely comes from having to verify endpoint state and conduct forensic analysis after alerts from endpoints indicate that they were potentially impacted by a cyber attack or related security incident.

Our Approach

Akatosh starts by reducing the impact of false positives and the cost of incident response by enabling automated, real-time forensic analysis of endpoints when prompted by IDS alerts. This allows Akatosh to help operations personnel verify that an alert on an endpoint corresponds to a true attack. The system is comprised of small Akatosh clients, server and dashboard, as depicted in Figure 1. The clients live on network endpoints and take regularly scheduled baseline snapshots (on configurable time intervals) to record endpoint state over time.

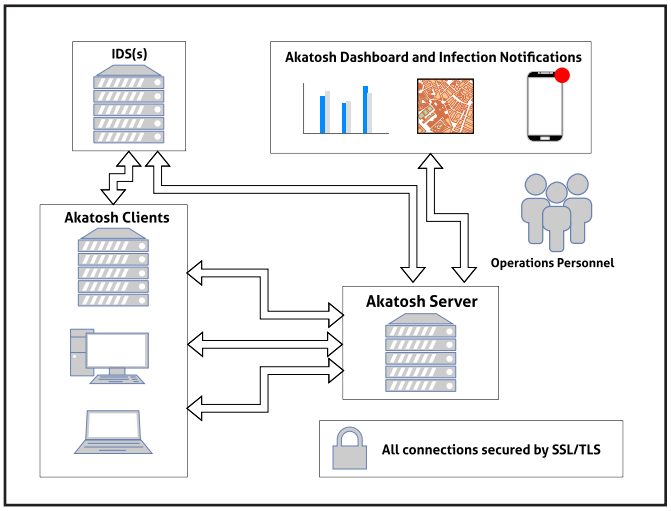


Figure 1: *The Akatosh server promptly generates and provides operations personnel with a report based on alerts on the Akatosh clients.*

These snapshots capture specific data about the endpoint, including processes, loaded drivers, registry entries, network connections, and other data. When an IDS detects anomalous behavior it alerts the Akatosh system. Depending on the nature of the alert (configured by the operators), the Akatosh client immediately takes a snapshot of the endpoint that generated the alert and sends the snapshot to the Akatosh server. The Akatosh server automatically produces a succinct incident report differentiating the post-alert snapshot from the most recent baseline snapshot. The Akatosh dashboard displays all endpoints being tracked, their status, the snapshot data being collected as the system receives IDS alerts, and the incident reports.

[1] www.ibm.com/security/data-breach

Figure 2 summarizes the underlying process described above. Akatosh automatically analyses the differences between pre-alert and post-alert snapshots in real-time and displays the results on the dashboard, showing the specific endpoint components affected by the anomalous behavior.

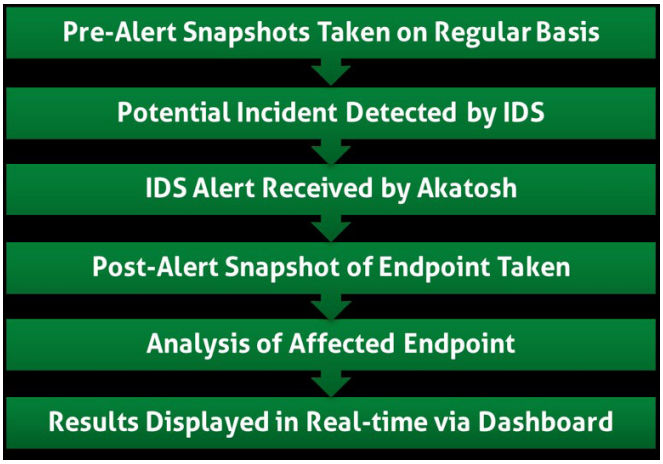


Figure 2: *Step-by-step explanation of Akatosh endpoint snapshot and real-time analysis process.*

Benefits

Akatosh reduces the time and cost of incident response activities and increases the collective strength of deployed computer security defense mechanisms.

The incident report and the specific impact results delivered to the Akatosh dashboard allow analysts and other operations personnel to quickly and easily examine the affected endpoint components and verify whether an incident truly occurred after being detected by one or more IDSs. This reduces the false alert rate and alleviates the pressure on operations personnel to respond to vast amounts of IDS alerts.

Akatosh reduces the time necessary to conduct incident response activities by automating the forensic analysis of endpoints, which removes the tedious process of manually analyzing endpoints in the wake of alerts. Akatosh guides operators directly to the endpoints affected by security incidents.

Competitive Advantage

Akatosh is the first of its kind system to integrate automated forensic analysis with IDS. Through this integration, Akatosh can perform a detailed analysis of the affected endpoints at the exact time of the incident, unlike current incident response systems, which are less reactive to immediate changes in endpoint state, at least at the level of detail that Akatosh provides.

Additionally, the Akatosh dashboard automatically provides reports showing a high level overview of affected endpoint components that operations personnel and analysts as well as managers and upper-level executives can understand and dig into. Reports are generated in real-time without shutting down endpoints to perform the tedious task of imaging the machine and analyzing the image on a separate machine. Similar products in the space don't provide differentiated endpoints states to operations personnel, and manual analysis of endpoints requires personnel to shut down machines before examining their state.

While there are products to perform endpoint history analysis for non-security related domains, such as infrastructure monitoring, these products do not transition well to verifying, tracking, and analyzing the impact of cyber attacks. By focusing on affected endpoint components, Akatosh assists in verifying incidents and automatically tracking and analyzing propagation over the components.

Benefits

The Akatosh client and server are currently implemented as cross-platform Python applications with a Python Flask web application for the Akatosh dashboard. Laboratory testing has begun on Akatosh for real-world deployments to Windows clients, and we are continuing to improve the reporting capabilities of the system, including adding more sophisticated heuristics for analyzing the impact of software and malware on enterprise networks.

We are seeking partners to deploy and test Akatosh in a realistic deployment scenario to help us improve the technology and mitigate any challenges that might occur during large-scale deployment. We are also interested in partnerships to help us further develop Akatosh for its use on Windows, Mac, and Linux, as well as for cloud deployments of the Akatosh system.

CPAD: Real-Time Cyber-Physical Attack Detection

Jason Laska
laskaja@ornl.gov

Overview

Cyber-Physical Attack Detection (CPAD) protects the operation of power transmission and distribution systems, automobiles, airplanes, manufacturing plants, nuclear facilities, and other highly sensored control systems by automatically inferring underlying physical relationships using cross-sensor analytics in order to detect sensor failures, replay attacks, and other data integrity issues in real time.

Customer Need

The successful functioning of complex cyber-physical systems depends on the reliable operation of a control loop that takes sensor data as input and produces control decisions as output. As an increasing number of cyber attacks have successfully targeted physical infrastructure and control systems, a startling pattern has emerged: almost all of the attacks blind or manipulate operators by altering the sensor data they receive.

In a power transmission system, faulty sensor data could easily lead operators to misallocate electrical power, resulting in black outs, brown outs, or power surges. In an airplane, automatic controls operating on faulty sensors could result in starving or flooding engines. In general, manipulation of sensors could allow attackers to control the system by controlling the controllers.

Additionally, sensors tend to be the least-protected components, often being accessible from cyber networks and difficult to harden or physically protect. As sensors proliferate and many new low-cost sensors come online, there is a growing need for a method to establish trust in sensors so that operators may react to bad sensor data in real time and avoid costly damages to their cyber-physical system.

Our Approach

CPAD directly addresses the problem of sensor trustworthiness by identifying readings across multiple sensors that indicate states that are not physically possible. Generally, the abundance of sensors instrumenting cyber-physical systems leads to redundancies that make it possible to cross-check sensor data for consistencies and to flag inconsistencies as data errors and possible attacks. For example, total current entering a bus must equal the total current leaving the bus (Figure 1). Further, current flow and voltage difference are proportionally related, with an often-unknown constant of proportionality. Similar relationships may exist among, for example, force, speed, position, pressure, and flow sensors.

Even when physical laws describing cyber-physical systems are known, challenges remain because many system constraints are difficult to know with suitable precision. For example, the built system may disagree with the design documents, components wear over time, and operational behavior may depend on outside factors like ambient temperature.

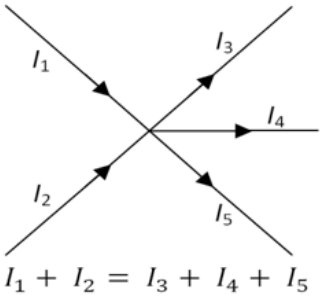


Figure 1: *Connections between sensors imply physics-based constraints, such as the current-sum relationship shown here. These constraints provide new ways to detect data spoofing.*

Rather than use given relationships, CPAD uses powerful machine learning to automatically learn constraints that sensor data must satisfy. System sensor data is fed into a comprehensive attack generation engine to construct new sensor readings having a wide range of integrity attacks and sensor failures, such as additional noise, varying sensor bias, sensor lag, data injection, and measurement replays.

Once CPAD infers the laws that govern valid sensor data, deviations from those laws indicate failures in data integrity. The resulting CPAD detectors operate on streaming sensor measurements to immediately flag any data integrity issues, allowing operators to act before the damage is done.

Benefits

CPAD helps operators by identifying if, when, and where an attack or sensor failure occurs. This information augments streaming sensor data with levels of assurance, as shown in Figure 2. The specificity of the output means operators can act quickly to minimize the effect of bad sensor data as well as to remediate the problem.

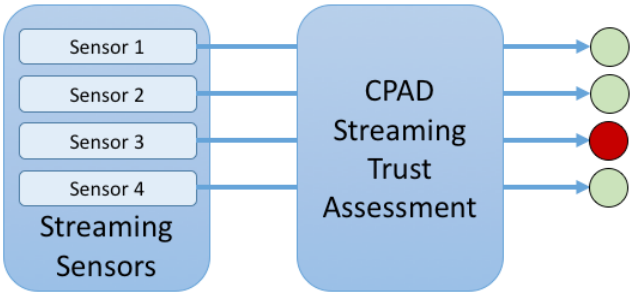


Figure 2: *After the training phase (not shown), CPAD analyzes the sensor data streams to assess trust by finding violations of the learned physical constraints. These may then be incorporated into the control process and used to initiate remediation.*

In analyses on simulated power grid data, CPAD achieved 99 percent accuracy on sensor replay attacks. Experiments demonstrated that the best approach was to automatically infer features from raw data rather than to use explicitly coded physics-based features.

CPAD trains directly on raw sensor data, which in many cases is already being collected. Consequently, the training phase of CPAD requires neither a specification of nor direct interaction with the hardware to learn the detection models. This makes CPAD very easy to deploy on new systems.

Competitive Advantage

Unlike other approaches that focus on single-sensor attack detection, CPAD uses cross-sensor analytics to exploit correlations and constraints that exist between multiple sensors. This allows CPAD to detect sophisticated attacks, like those that replay valid sensor data at a later time to produce a particular effect. On a single sensor, the data look valid, so the attack only becomes detectable when viewing related sensors simultaneously.

Another common approach focuses on anomaly detection, which identifies when the system's behavior is unusual. CPAD is not based on anomaly detection, but on *non-physicality detection*, which is the detection of combinations of sensor measurements that cannot correspond to physically realizable states. In highly complex systems, it is difficult to characterize the wide range of operating regimes required to create a robust anomaly detector. By exploiting physical constraints across multiple sensors, CPAD is expected to be more robust to previously unseen operating regimes.

Rather than finding physical constraints through laboratory equipment testing or by manually coding expert information about the systems' dynamics, CPAD infers the physical constraints from raw data. This leads to significantly less demand being placed on experts and enables the model to adapt more frequently.

Commonly, machine learning methods require a large supply of labeled normal and attack data. Because CPAD generates its own examples from raw data, there is no need to manually code information about the systems' physics. This makes it possible to apply CPAD even if there is no available labeled corpus of attack examples.

Next Steps

CPAD is currently implemented as a software tool and has been validated on both simulated and real power transmission data. Work continues to extend CPAD to a variety of real sensor data sources.

Since CPAD requires neither knowledge of physical relationships nor labeled attack data, it can be applied across a wide range of cyber-physical systems to detect data integrity attacks. CPAD could potentially be used to protect industrial plants such as manufacturing, chemical processing, and nuclear facilities. In addition, modern aircrafts, ships, and vehicles are highly instrumented and would be amenable to similar analyses.

We are seeking partners to pilot CPAD and provide feedback. Ideal partners will be interested in protecting the integrity of their data and will already be collecting from many sensors simultaneously.

StreamWorks: Continuous Pattern Detection on Streaming Data

Pacific Northwest NATIONAL LABORATORY

Sutanay Choudhury sutanay.choudhury@pnnl.gov
George Chin george.chin@pnnl.gov
Khushbu Agarwal khushbu.agarwal@pnnl.gov
Sherman Beus sherman.beus@pnnl.gov

Overview

The StreamWorks system supports continuous detection of emerging patterns in a stream of graph-structured data. Cyber data streams naturally lend themselves to a graph representation, and hence, methods for pattern detection in graph streams are very useful for detecting emerging events in massive netflow or event log data streams.

Customer Need

Real-time monitoring of cyber infrastructure is a well-established need for government and industry today. However, monitoring is mostly performed to detect behavioral anomalies in individual hosts or across an enterprise. Another form of monitoring involves querying streaming data for events of interest. Most complex queries are restricted to ad-hoc, offline querying of the data, while streaming analytics is restricted to a narrow class of aggregate queries. Even for ad-hoc queries, describing patterns of interaction between users, machines, and applications to describe sophisticated attacks in a query language can be extremely complex. Requiring cyber defenders to learn a query language limits the usability and effectiveness of the tools.

StreamWorks addresses two major problems: state of the art cyber monitoring systems do not provide sophisticated query capabilities in a streaming setting, and the usability of the query mechanism is limited by the complexity of the query language and its support for diverse classes of events.

Our Approach

The StreamWorks system is designed to support complex pattern detection of large-scale streaming data. Most cyber data sources naturally lend themselves to a graph based representation, where the data model is a collection of interactions between entities such as machines, users, and applications. Figure 1 shows how graphs can represent complex interactions that occur in cyber data as “patterns”.

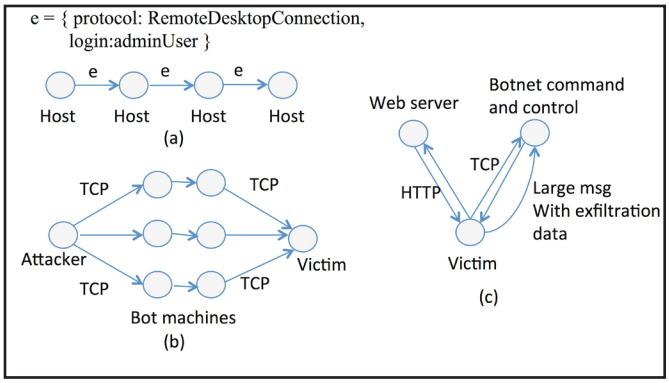


Figure 1: *Graph based descriptions of attack patterns. a) Insider infiltration b) Denial of Service attack c) Information exfiltration*

Given this setting, StreamWorks enables users to search for such patterns in streaming data. Instead of waiting for offline, ad-hoc analysis, users can issue a query such as “Tell me when X happens”. As an example, Figure 1a shows a pattern describing how an attacker may laterally move through an enterprise. Figure 1c shows a graph pattern describing an exfiltration process in which a malicious script is downloaded, enabling communication with the command and control server.

The query processing workflow in StreamWorks begins with a user submitting a visual query specification (Figure 2a on the following page). We developed visual templates for classes of events important to cyber analysts, including botnets, lateral movement, and exfiltration, among others. The user specializes a pre-populated query template and submits the query through the browser.

Next, the query optimization module analyzes the submitted query. The system uses its knowledge of stream characteristics to decompose the query into smaller sub-queries. The sub-queries are re-organized into an efficient query plan and routed to the parallel graph query-processing engine.

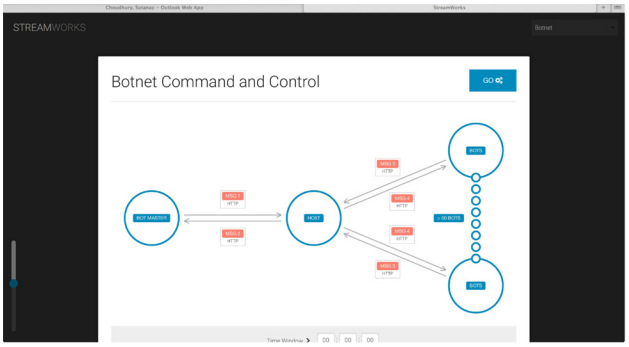


Figure 2a: *Web-based user interface for submitting pattern queries*

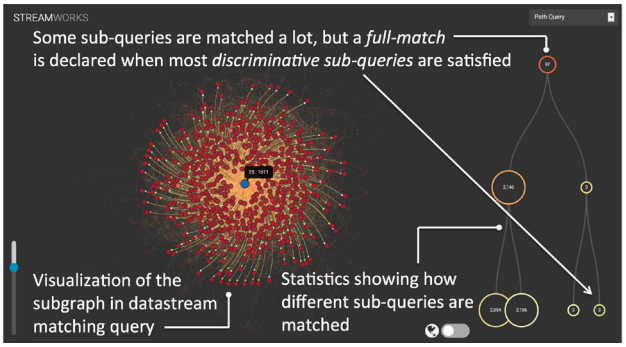


Figure 2b: *Web-based interface for visualization of query processing results*

Figure 2: *StreamWorks workflow: User selects query template for a certain event, tunes parameters and submits the query to the graph-processing engine. When a match is found in the datastream, results are sent back to the web UI.*

Key features:

- *10MEdges/second for three-edge query on streaming graph*
- *graph summaries to enable query recommendation*
- *result prioritization for handling massive numbers of matches*

A challenge with streaming query processing is that the system is constantly observing partial evidence and speculating what may occur in the future. We have developed a "lazy processing" strategy to ensure the query processor looks for the most discriminating evidence of a likely pattern match and then performs the necessary work. Once a match is found, the results are sent back to the user interface using different presentation schemes. As an example, Figure 2b shows a match with a botnet pattern. Color gradients are used to indicate confidence in various parts of the match.

Product	Streaming	Graph Search	Visual Analytics
StreamWorks	✔	✔	✔
SQRRL Enterprise	✖	✔	✔
Apache Spark	✔	✖	✖
Neo4J	✖	✔	✖

Table 1: *Comparison of StreamWorks with other applications/frameworks.*

Benefits and Competitive Advantage

StreamWorks' greatest benefit is that it allows cyber defenders to think naturally and not worry about how to express complex queries in a query language. From a monitoring perspective, StreamWorks' ability to find patterns of complex interactions between users, machines, and applications gives cyber defenders an unprecedented analytics capability.

StreamWorks' competitive advantage lies in its fundamental redesigning of query processing algorithms to enable stream processing of graph-structured data. Experiments on an internet backbone traffic dataset reveal 10-100x improvement in query runtime over approaches adapting an ad-hoc querying approach[1]. As Table 1 shows, StreamWorks' multi-disciplinary approach uniquely positions it to provide analytics capabilities that other systems do not support today.

Next Steps

We performed scalability studies and established an end-to-end workflow in the first phase of StreamWorks' development. We are actively seeking pilot opportunities to help us verify and validate the algorithms with varying data characteristics, benchmark the system to delineate its performance limits in terms of throughput, and develop support for complex queries. Such partnerships will provide partners with key insights in terms of finding low-volume, localized events or behavioral signatures that they may not be observing today.

[1] Choudhury, S., Holder, L., Chin, G., Agarwal, K., & Feo, J. "A selectivity based approach to continuous pattern detection in streaming graphs." Proceedings of the 18th International Conference on Extending Database Technology, Brussels, Belgium, March 23-27, 2015.

PEACE: Policy Enforcement and Access Control for End-points

Craig A. Shue
craig@contexsure.com

Overview

Network operators need greater control and visibility into their networks to mitigate attacks. The Policy Enforcement and Access Control for End-points (PEACE) system protects end-point devices in an enterprise network by intercepting all new network connections and vetting them at a centralized network controller. This allows network operators to enforce network policy and control access to proactively defend their networks. PEACE further provides valuable forensics and detection capabilities.

Customer Need

Operators need to understand their networks better in order to protect their organizations from cyber attacks. Such protection can be costly. One U.S. financial institution spent $500 million in 2016 alone to secure their network[1]. Cyber attacks globally cost businesses about $400-$500 billion annually. In addition to financial costs, attacks can lead to brand reputation damage, disclosure of sensitive data, and in the case of government, the loss of classified information.

Enterprise networks are often the battleground for cyber attacks, yet network operators lack detailed situational awareness, putting them at a disadvantage. In order to defend their networks, operators need the ability to see attacks that spread in local subnets and to understand why network packets are created (e.g., which application originated them and why). Further, these operators need to distinguish traffic generated by human users from traffic generated by malware processes that may be acting covertly on a computer.

Our Approach

The PEACE system runs an agent on each end-point that intercepts new network connections and requests permission to transmit from a centralized controller, as shown in Figure 1.

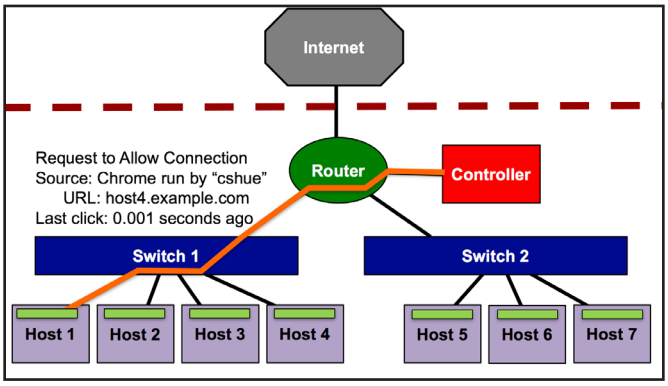


Figure 1: *End-point agents request permission to transmit from the access controller.*

The request provides a detailed justification for establishing the network connection, including the associated application, user, and the user's interactions with the graphical user interface to enable more informed access control decisions.

PEACE considers information such as text that appears on the screen and the timing and volume of information from keyboard or mouse inputs. Figure 2 shows how PEACE combines this information with network activity to determine if an application creating network activity is being actively endorsed by the user or if it is acting covertly.

Figure 2: *End-point agents provide details about usage behaviors to provide more useful context for decisions.*

Network operators can use a web interface to add new policy to the controller. In doing so, the operators will create rules that indicate what features are important for allowing or denying access. This allows the PEACE access controller to make more informed decisions.

[1] Steve Morgan, "Why J.P. Morgan Chase & Co. Is Spending A Half Billion Dollars On Cybersecurity," Forbes Article, January 2016. [Online] http://www.forbes.com/sites/stevemorgan/2016/01/30/why-j-p-morgan-chase-co-is-spending-a-half-billion-dollars-on-cybersecurity/

PEACE is easy to deploy. An organization first installs the network controller as a virtual machine image on an on-premises server. The organization then deploys the agent software on each of the organization's computers using automated software deployment tools. This approach supports incremental deployment, allowing organizations to deploy to test machines or pilot groups before rolling out organization-wide. Further, PEACE has low system overheads with only imperceptible network impacts.

Benefits

PEACE allows organizations to distinguish legitimate, user-facing applications from stealthy malware or remote access tools that attackers use to conceal their actions. Organizations will see all traffic in their networks and be able to associate it with its originating application and user.

PEACE allows network operators to craft policy that grants permission to specific applications when communicating with specific servers. This level of control allows operators to write more direct policy while limiting the opportunities for attacks to blend in with legitimate traffic. Operators will have the ability to craft precise rules, while still being high-level enough to be easily understood.

In addition, PEACE provides a forensic record of all network communication associated with end-points, regardless of whether that traffic occurs internally or with outside parties. If unauthorized activity is later detected, the PEACE controller allows network operators to reconstruct the event. PEACE can construct these records with imperceptible delays and without taxing system resources.

Competitive Advantage

PEACE is able to see traffic within subnets and definitively link this information to applications and users whereas traditional perimeter defenses such as network firewalls must make inference attempts to link traffic. Unlike traditional host-based firewalls, PEACE can dynamically respond to threats that have affected multiple machines in a network in real time, unlike traditional host-based systems which need to synchronize systems. Finally, PEACE does not rely on signatures like traditional anti-virus. Accordingly, network policies enforced by PEACE can prevent even zero-day threats from spreading within a network. By including higher-level information from the Graphical User Interface (GUI) and user actions, the forensics from PEACE are easier to understand, helping defenders isolate the root cause of attacks faster and providing more meaningful case studies to educate end users.

Next Steps

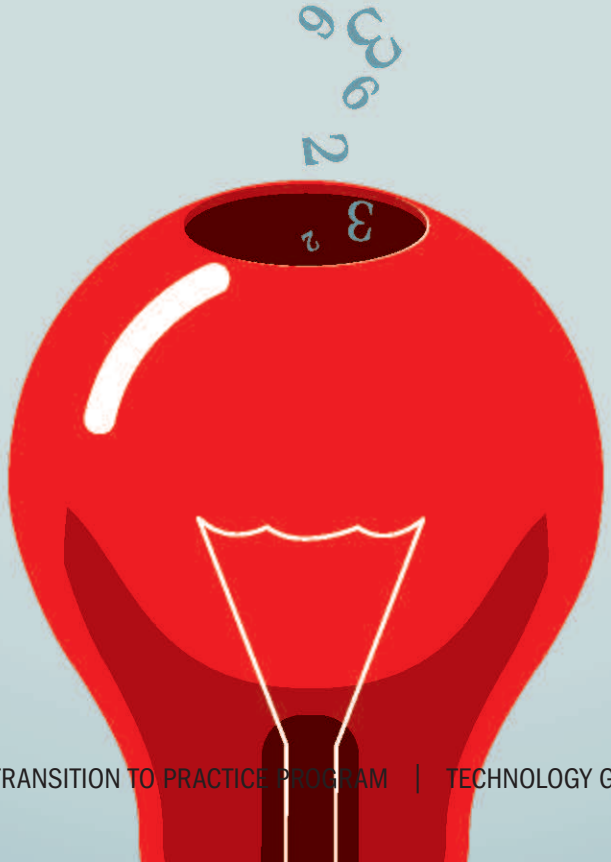
PEACE has been implemented on Linux end-points and a Linux network controller. The implementation has been tested in a laboratory environment and is ready to be piloted in external environments. We are seeking partners to deploy and test PEACE in their environments to help us improve the technology and understand issues inherent in larger deployments. We are particularly interested in pilot partners with that have end-users that run Linux desktop environments on their local machines.

The PEACE system is available for Windows 7 and 10 deployments. We are currently seeking pilot deployments for these platforms.

Funded through the National Science Foundation's (NSF) Cybersecurity Program

4TH COHORT OF TECHNOLOGIES:

- **REnigma: A Tool to Reverse Engineer Malware**
- **Socrates: Graph Analytics for Discovering Patterns and Relationships in Large Data Sets**
- **PcapDB: Optimized Full Network Packet Capture for Fast and Efficient Retrieval**
- **REDUCE: Collaborative, Statistically Guided Exploration of Malware Similarities**
- **Dynamic Flow Isolation: Adaptive Access Control to Protect Networks**
- **TRACER: Transparent Protection of Commodity Applications**
- **FLOWER: Network FLOW AnalyzER – Deep Insight Into Network Traffic**
- **SilentAlarm: Detecting Abnormal Network Traffic**



REnigma: A Tool to Reverse Engineer Malware

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Julian Grizzard
julian@dtrsec.com

James Stevens
jim@dtrsec.com

Overview

When an organization is under cyber attack, there are numerous questions that need to be answered in a timely fashion. How did the attacker get in? How bad is the damage? Who is behind the attack? How can further damage be prevented? To maximize the impact of an attack, the adversary's goal is to increase the difficulty of answering these questions. Obfuscation of executable code prevents static analysis, encrypted communication prevents network analysis, and anti-analysis techniques prevent dynamic analysis. REnigma helps malware analysts regain the upper hand against advanced malware techniques by transparently and precisely recording the execution of malware, and it enables analysis that can extract the level of detail necessary to answer the vital questions needed to understand and recover from a cyber attack quickly and accurately.

Customer Need

The analysis of malware used in a cyber attack is a very manual, time consuming, low throughput, and costly process requiring days to weeks to give the answers needed to clean up the attack and prevent further damage. Existing approaches require highly trained experts that are expensive and hard to hire or the use of automated tools that provide insufficient depth. It is critical that defenders utilize state-of-the-art techniques that provide quick, scalable, and in-depth analytic capabilities.

Our Approach

REnigma uses Virtual Machine Record and Replay (RnR) to precisely and transparently record execution of malicious code so that an analyst can then replay and analyze the execution in detail. RnR provides many powerful techniques for malware analysis that are not possible today because it enables the ability for the analyst to "rewind" to any previous state in the system without affecting the execution of the code under test. This approach enables instruction-level analysis algorithms such as exploit detection and data flow analysis to operate without being detected by anti-analysis techniques used by malware. For example, if a malicious code sample outputs encrypted data on the network, an analyst can use REnigma to backtrack to the plaintext data in memory or recover the encryption key used for exfiltration.

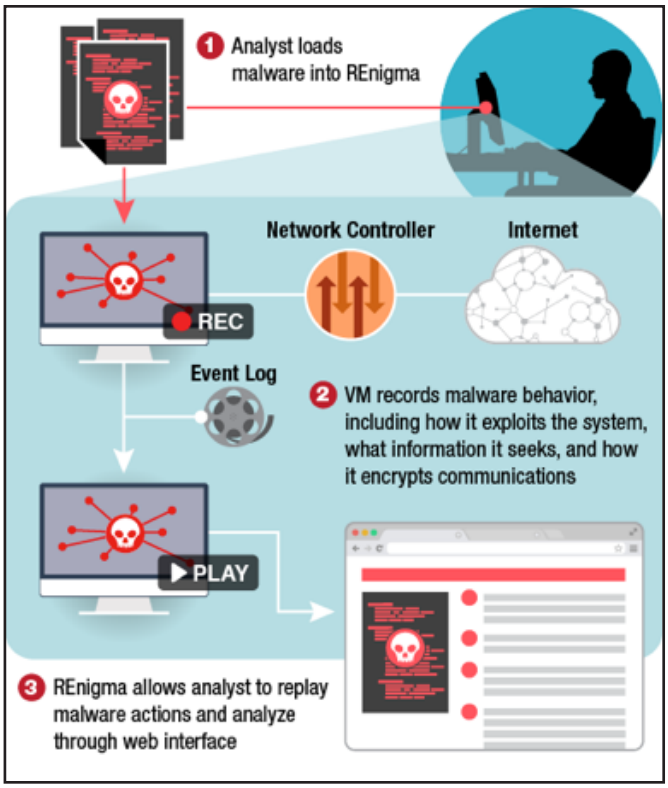


Figure 1: *REnigma analysis consists of three stages.*

REnigma analysis consist of three stages. First, the analyst loads suspect malware into REnigma. Second, REnigma launches a virtual machine, copies the malware into the virtual machine, and begins recording execution. During this stage, the malware executes inside the virtual machine exactly as it would in a normal system so that its behavior is captured. Additionally, the analyst can configure network access to the virtual machine to either expose the malware to an untethered "live" Internet connection, capturing remote command-and-control communication, or a controlled "fake" Internet connection that responds with false data. In the final stage, REnigma performs automated analysis to uncover the malware's

behavior. The analysis output includes details about exploitation methods, indicators of compromise, and decrypted command-and-control communication. The analyst can also use an indexed timeline to quickly jump to points of interest captured during recoding and manually examine the behavior in detail.

Benefits

REnigma provides an analyst with a safe and trusted place to analyze suspicious files or URLs. The capability enables analysis of malicious malware samples to understand their functionality at a level of detail not previously possible. Additionally, REnigma is designed to integrate with standard tools, allowing the analyst to retain and leverage existing skills. For example, a user can replay execution and stop at various points during replay and dump system memory. This memory image can be fed into Volatility, which is an industry standard tool for extracting key artifacts from raw memory dumps. Furthermore, REnigma incorporates a framework to create new modules that can extract arbitrary information during replay. Advanced analysts can employ REnigma's modules as well as create their own custom modules.

Competitive Advantage

The key technology behind REnigma is Deterministic Security's Virtual Machine Record and Replay (RnR) capability. Record and replay research prototypes over the past 20 years were never fully developed, were not robust, did not have high performance, or are no longer maintained. To address this gap, RnR was initially developed at the Johns Hopkins University Applied Physics Laboratory (JHU/APL) over the course of several years. In 2017, the technology was spun-off into a new company called Deterministic Security. The unique capability can record operating systems and applications running at speed with a modest 5% slowdown compared to a virtual machine that is not recorded. During replay, the precise execution of a malware sample can be recreated with instruction-level precision.

REnigma's ability to perform in-depth instruction-level analysis without disturbing the code sample reduces the need for expert reverse engineers to load the code in tools like IDA Pro and manually edit it to remove anti-analysis checks and force the malicious code to execute. REnigma allows security conscious organizations to avoid immediately resorting to manual reverse engineering as anti-analysis techniques become increasingly common, potentially saving tens of thousands of dollars per code sample analyzed.

Next Steps

Deterministic Security is actively developing and commercializing the REnigma capability. We are seeking customers that are interested in learning more about how REnigma can help solve your problems. Please contact us for more information: ***sales@dtrsec.com***.

Socrates: Graph Analytics for Discovering Patterns and Relationships in Large Data Sets

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Cetin Savkli
Cetin.Savkli@jhuapl.edu

Ryan Carr
Ryan.Carr@jhuapl.edu

Mike Lieberman
Mike.Lieberman@jhuapl.edu

Overview

SOCRATES is a flexible, easy to use graph analytics tool designed to discover patterns and relationships in large scale and complex data sets. Such data sets can be found in cyber, social, financial, energy, and biological domains. SOCRATES has been successfully used to discover previously unknown patterns in real world big data sets. Examples include detecting illegal international trade, discovering unknown associates of persons of interest from travel patterns, and detecting anomalous flight behaviors. SOCRATES can be readily applied to cyber and cybersecurity data.

Customer Need

Scope and complexity of data sets as well as evolving analytic challenges make rapid development of analytics a critical need. A key challenge in big data analysis is the human skillset required to properly store and analyze immense quantities of data. People who excel at analysis may not have the necessary computer science knowledge relevant for big data analysis and vice versa; drawing conclusions from big data requires both skill sets.

Another critical challenge is development of unsupervised methods for analysis of data. Analytic approaches based on classification or rule based techniques are unsuitable for large scale and complex data sets as data is typically high dimensional and shows great variability. Relying on past examples of bad behavior is not sufficient for detecting future threats. There is a need for development of scalable unsupervised analytics to learn patterns directly from data.

Many big data questions are domain independent. For example: determining correlations in data; discovering patterns of behavior and associated anomalies; discovering links and networks; identifying critical nodes for network resiliency, and spread of virus/information; determining central nodes, leaders, and power brokers. All of these analytic questions must be addressed in a manner that fusion of data and implementation of analytic ideas are both simple and scalable.

Our Approach

SOCRATES is flexible, easy to use graph analytics software tool designed to discover patterns and relationships in large scale and complex data sets. It features several advances in parallel computing and scalable distributed storage and uses a flexible graph model to represent complex data sets and knowledge. Every attribute of data is automatically indexed for fast random access and analytics processing.

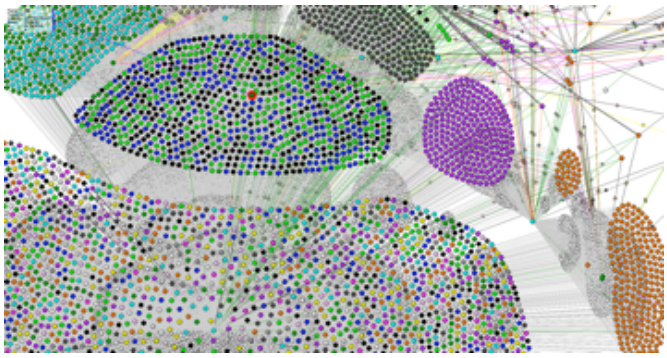


Figure 1: *Detection of anomalous activity from netflow data in a network with 2,000,000 links.*

SOCRATES' analytic capabilities are based on a probabilistic representation of data that captures a concise expression of knowledge. It uses this approach to provide anomaly detection and classification capabilities for high dimensional data including temporal behaviors. Most of the analytics and supporting correlation libraries are parallelized to take advantage of the computing power of a distributed hardware cluster.

SOCRATES also provides a library of link inference and network clustering algorithms. These algorithms work together to facilitate community based behavior analysis.

Benefits

SOCRATES provides a simple and scalable software platform and a library of unsupervised machine learning algorithms for big data analytics. Simplicity of analytics at scale allows developers and sponsors to rapidly explore ideas and leads to increased productivity both in terms of results and cost. Implementation of analytics has been

done with a focus uncovering probabilistic knowledge and patterns in large scale data into without an assumption on the availability of ground truth or categorization. SOCRATES provides a robust set of parallelized algorithms for anomaly detection in high dimensional spaces, temporal analysis, and correlation analysis.

SOCRATES' flexibility of graph representation facilitates fusion of diverse sources of data and simplifies management of data complexity. Automated indexing of attributes and advanced query capability facilitates rapid implementation of analytic ideas on complex data sets.

The combination of these benefits has led to development of analytic capabilities that have been successfully used to discover previously unknown patterns on real world data sets that can readily apply to cyber and cybersecurity data.

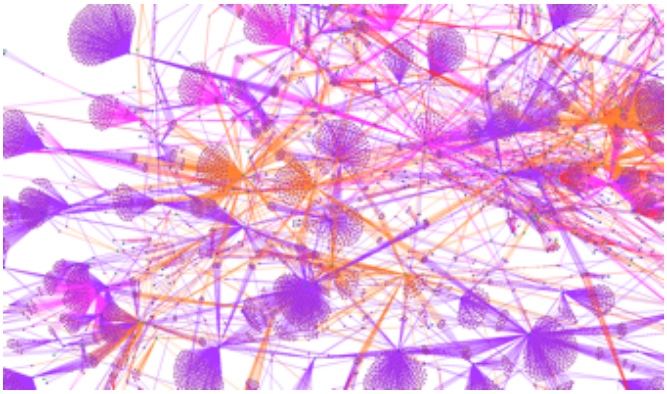


Figure 2: *Graph of global trade transactions with more than 1 billion links analyzed using Socrates to find anomalous transactions.*

Competitive Advantage

In addition to providing a robust set of analytic capabilities for behavior analysis, anomaly detection, and graph analytics, SOCRATES overcomes key issues in automated analysis of large data sets. NoSQL systems such as Accumulo & HBase face challenges that make analyzing big data difficult. SOCRATES provides secondary indexing for improved query performance, locality control to avoid unnecessary movement of data, and a schema that overcomes database maintenance challenges.

Traditional relational database management systems (RDBMS) also face challenges when dealing with big data. SOCRATES provides table structures that are flexible enough to easily support new kinds of data and better parallelization to increase scalability.

SOCRATES offers key advantages over the alternatives: a) The locality of graph elements can be controlled, a feature essential for not moving data in large scale graph analytics; b) All of the attributes of graph elements are indexed for fast query processing; c) Provides a parallelization paradigm that is close to standalone programming; and d) Cluster is not centrally managed.

The biggest competitive advantage SOCRATES provides is to make big data analysis as simple as possible and that has been the key to its success.

Next Steps

SOCRATES is a flexible, easy to use, large scale data analytics tool for use by technical users in a controlled environment. The success of analytic results using SOCRATES has sparked sponsor interest and it is being prepared for deployment at various sponsor sites. We seek additional partners who can deploy and apply SOCRATES data analytics to their large cyber and cybersecurity datasets.

PcapDB: Optimized Full Network Packet Capture for Fast and Efficient Retrieval

Shannon Steinfadt
shannon@lanl.gov

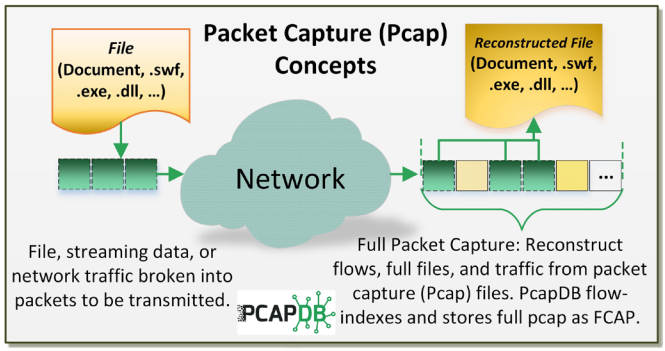
Overview

Full packet capture is an essential component to any cyber security and incident response deployment. PcapDB optimizes full network packet capture for fast, efficient search and retrieval, with packets reorganized and indexed by flow before they are ever written to disk. PcapDB provides fast results to cyber analysts and responders when speed matters most: during an incident. PcapDB is an open source software solution designed for easy deployment on low-cost, commodity hardware, allowing for large-scale and geographically distributed installations at a significantly lower cost than existing commercial solutions. PcapDB is unlike other open source tools: with storage and search optimizations as well as a scalable architecture that enables multi-site, enterprise-wide deployment, it meets both government and commercial needs.

Customer Need

Cyber security incidents are often discovered hours, weeks, or even months after they happen. On average, advanced persistent threat (APT) actors are inside networks and systems for one year before they are discovered. To fully assess the threat and scope of cyber incidents, analysts need access to full network packet capture (pcap) files for as much of the incident time frame as possible. Full packet capture gives an analyst a complete picture of network traffic during the time of the incident, similar to a black box flight recorder. With pcap, analysts can capture malware as it enters a network, monitor command and control traffic, and investigate exfiltrated data during and after a data breach, in addition to many other applications such as cyber forensics and data analytics.

To be effective, packet capture that is lossless, and line-rate is necessary. These data should be easily searchable and have the longest history (the largest amount of pcap) possible. Response time is important; while adversaries may have months to prepare an attack, analysts have comparably little time to create a comprehensive and effective response once detected. Full packet capture enables analysts to assess and respond to the current attack, and to prepare for the next one.



Our Approach

PcapDB is a new approach for packet collection, management, searching, and collaboration. Unlike other open source tools, PcapDB is designed for deployment on commodity hardware and network capture cards.

PcapDB uses the abundant CPU cycles and memory available in modern servers to optimize the captured packets for indexing and storage before they are ever written to disk. It organizes the data by the entire transfer (flow) rather than individual packets. The flow-ordered pcap (fcap) provides data in units the users expect rather than how the data happens to arrive over the wire.

The indexing structures and algorithms in PcapDB take full advantage of this flow ordering, minimizing disk interaction and greatly improving system performance. Additionally, the indexing techniques consume significantly less disk space than other solutions, leaving 99 percent of the disk available to store captured packets. This system makes the most of the physical disk investment, increasing space dedicated to store a longer pcap history with efficient indexes.

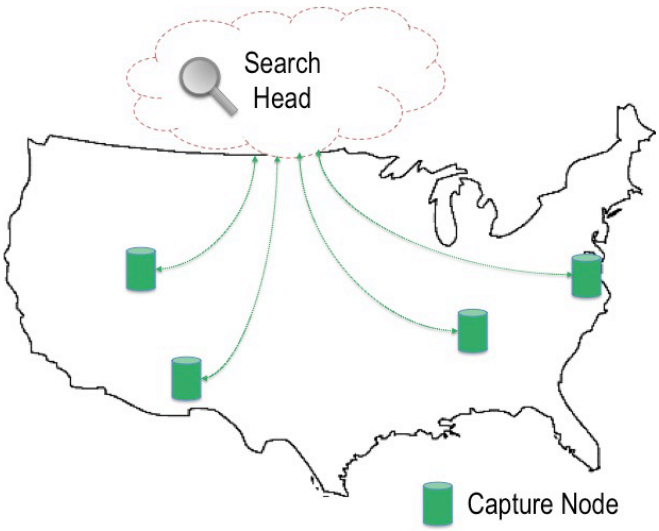
PcapDB is inherently parallel, designed to scale across multiple capture nodes to handle higher capture rates. Queries are resolved using a Map-Reduce-like model, first distributed amongst the various (local) Capture Nodes and then combined into the final result on a central Search Head. This allows for scalable, distributed capture that is able to meet different capture needs and requirements.

Benefits

PcapDB pares down the packet capture features to exactly what cyber analysts and incident responders need to do their job effectively: swift searching across the longest, logically ordered, history achievable. Users can now rapidly investigate intrusions and potential threats with a greater chance for success.

PcapDB's optimizations greatly reduce the time needed to retrieve stored packet captures. Disk reads are the slowest part of data retrieval. Eliminating wasteful disk access enables result fetching at near hardware-rate speeds.

The web-based search interface removes the need for tcpdump, improving search accuracy by avoiding search syntax errors. Integration is available via a RESTful application interface, enabling automation and pipelining of PcapDB with your existing tool set.



Competitive Advantage

PcapDB can retain over 90 percent more capture data on disk than commercial systems. PcapDB indexes are extremely efficient with precious storage space. Existing commercial packet capture technologies, while capable of high speed capture, favor increasing their feature sets to sell the capture hardware rather than improving their basic packet storage and retrieval. These "features" often result in large indexes and metadata structures that crowd out captured packets, significantly shortening the capture history.

Large-scale deployment of PcapDB is at a substantially lower cost than existing commercial solutions: less than $20K per Capture Node including ~200TB of storage (~2 weeks+ of storage at 1 GB/s). In addition, PcapDB removes the need for costly commercial capture hardware. You can build an affordable capture system using COTS hardware of your choosing on low-cost commodity Serial Attached SCSI (SAS) disks and "just a bunch of disks" (JBOD) enclosures. PcapDB includes built-in disk management utilities available though the web interface to simplify disk setup and maintenance.

PcapDB is ideal for enterprise deployment for single- and multi-site locations. Indexed packet capture data is stored locally at each Capture Node. Analysts can quickly search across all or some of the data stored across the Capture Nodes. User access, storage, and network interfaces are managed through the Search Head's native web interface.

Next Steps

The core functionality of PcapDB is complete. The user interface is rapidly nearing a deployable state for a production environment. PcapDB is currently being tested on networks with live data, up to 100 Gb/s of bandwidth. We seek partners to deploy and utilize this technology at their sites.

REDUCE: Collaborative, Statistically Guided Exploration of Malware Similarities

Juston Moore
jmoore01@lanl.gov

Overview

REDUCE is a software toolset enabling cyber security analysts to rapidly discover relationships between malware samples, to extract temporal threat intelligence, and to develop actionable signatures for known and emerging threats. REDUCE performs automated static code analysis and identifies similarities between malware samples in order to support knowledge sharing about related pieces of malware. By integrating with well-established reverse engineering tools, REDUCE speeds up both deep-dive reverse engineering efforts and custom signature generation.

Customer Need

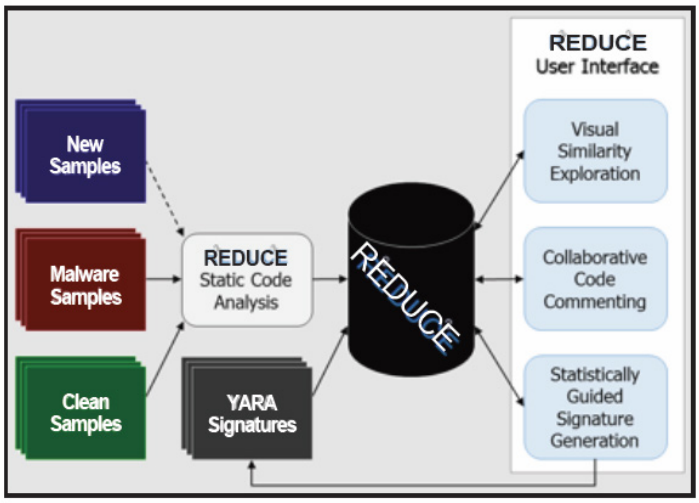
Large enterprise networks are constantly under attack by a huge number of threat actors. Each threat actor commonly deploys many variants of the same malware in order to defeat anti-virus defenses. Responding to the constant emergence of new and evolving malware threats, cyber defenders require the ability to easily compare new malware with previously seen malware samples, and to efficiently develop and deploy custom signatures to guard against targeted attacks.

Manual analysis of malware yields invaluable information, but analyzing many similar malware samples one at a time is very inefficient. Cyber security analysts currently lack tools to perform in-depth analyses of more than one or two pieces of malware at once. Analyzing similarities between sets of malware, rather than characteristics of individual samples, allows an analyst to work more efficiently and to easily transfer knowledge from previous analyses on similar pieces of malware.

Our Approach

REDUCE provides a centralized software toolset for automatically performing static analysis on a collection of malware samples. Once samples have been uploaded and processed, REDUCE uses statistical techniques to identify similar code sections across many malware samples. Identified similarities enable an analyst to leverage existing knowledge about a small set of samples in order to rapidly make inferences about the authorship and technical characteristics of new samples.

In addition to providing guidance and insight during an in-depth examination of malware, REDUCE also allows an analyst to quickly construct robust signatures for known and emerging threats. The REDUCE signature generation process is guided by information theoretic principles, which help to identify features that are distinctive to the set of interest, while eliminating features common across software samples in general. Signatures are generated in the open-source YARA format. YARA signatures can be deployed on a wide variety of security appliances and easily translated into other formats to be deployed across an enterprise.



Benefits

REDUCE is a practical toolset developed by analysts in an operational incident response environment. REDUCE helps analysts to focus on specific code patterns and threat actors rather than peculiarities of individual malware samples.

REDUCE enables a reverse engineering workflow and complements tools commonly used by security analysts. The REDUCE user interface gives analysts a big-picture view over collections of malware, while also facilitating deep-dive investigations. Using statistically guided reverseengineering, analysts can uncover similarities among a potentially large set of related malware samples.

For both experienced reverse engineers and junior analysts, REDUCE shortens the time required to construct effective signatures for new and emerging threats. REDUCE rapidly uncovers shared code between new malware samples and known samples, even if existing signatures do not detect the new samples. REDUCE also serves as an expanding knowledge resource and enhances collaboration between analysts by propagating comments between similar functions in different samples.

Competitive Advantage

The REDUCE toolset improves upon the capabilities of popular commercial and open-source binary similarity tools, such as Zynamics BinDiff, diaphora, and radare2, all of which compare only two malware samples. REDUCE identifies similarities across multiple malware samples.

Many machine learning systems, including commercially deployed solutions such as the VirusTotal, perform similarity analysis for sets of malware samples. However, these systems act as black boxes, and do not allow an analyst to directly interact in the decision-making process. In contrast to most of these systems, REDUCE displays specific similarities identified along with existing knowledge about those particular patterns. By involving analysts in critical decision-making processes, REDUCE produces information and deployable signatures that capture operational awareness criteria.

Manually constructed YARA signatures are the current de facto format for government and industry intelligence reporting. By utilizing the REDUCE signature generator, analysts at Los Alamos National Laboratory have reduced the time needed to produce quality YARA signatures from hours or days to minutes. Signatures created with REDUCE have consistently identified more malware samples of interest than commercial anti-virus or YARA signatures obtained from open source industry threat reports. REDUCE signatures also have a very low false positive rate in testing.

Next Steps

The REDUCE software is in the final phases of development and testing by security analysts within Los Alamos National Laboratory's Computer Security Incident Response Team. We seek to establish partnerships for pilot testing at other sites with in-depth reverse engineering capabilities. REDUCE can be used for malware analysis and signature generation by security practitioners with little knowledge of reverse engineering. We welcome feedback on the interpretability of the tool and its ability to work with existing reverse engineering processes.

Dynamic Flow Isolation: Adaptive Access Control to Protect Networks

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

David Bigelow
dbigelow@ll.mit.edu

Rick Skowyra
richard.skowyra@ll.mit.edu

Steven R. Gomez
steven.gomez@ll.mit.edu

This material is based upon work supported by the Assistant Secretary of Defense for Research and Engineering under Air Force Contract No. FA8721-05-C-0002. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Assistant Secretary of Defense for Research and Engineering.

Overview

Dynamic Flow Isolation (DFI) improves network security by dynamically changing access control in response to the current operational state or business need. DFI leverages Software-Defined Networking (SDN) to apply security policies on-demand to all systems on an enterprise network. Communications between individual users and services can be enabled, disabled, or rate-limited based on both automatic and human-in-the-loop decision systems.

Customer Need

Today's networks suffer from an over-connectivity problem that results in nearly all end-hosts being mutually reachable at all times. Paths that may need to exist under a particular set of circumstances are typically available under all circumstances. Leaving these unused paths in place allows adversaries to use them to move laterally within a network, often initially entering through easily compromised hosts (e.g. via phishing emails) and moving towards higher-value targets.

Improved mechanisms are required for selectively enabling and disabling paths in order to achieve the minimal connectivity demanded by the operational state or business need. For instance, at any given time a device should only be able to reach those destinations required for the current task of the actively logged in user.

Our Approach

DFI is a software-based solution that integrates with SDN controllers to align network connectivity with the operational state by changing access control in response to both automatically and manually generated events. It integrates with third-party network services such as authentication servers and intrusion detection systems (IDS) to be informed of events indicative of changes to operational state. Network connections are enabled, disabled, or rate-limited according to these events and in conjunction with a specified policy.

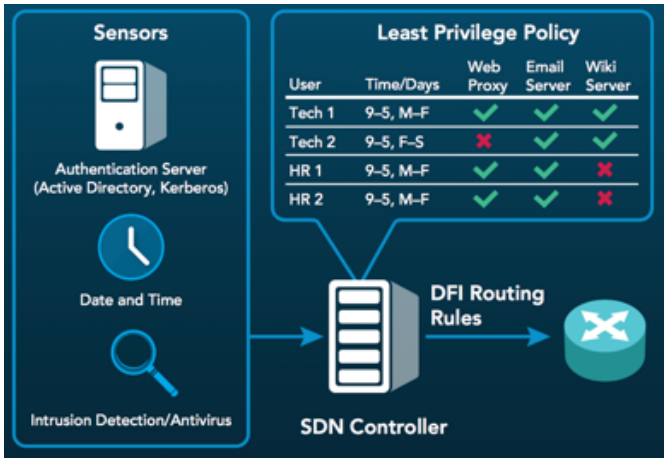


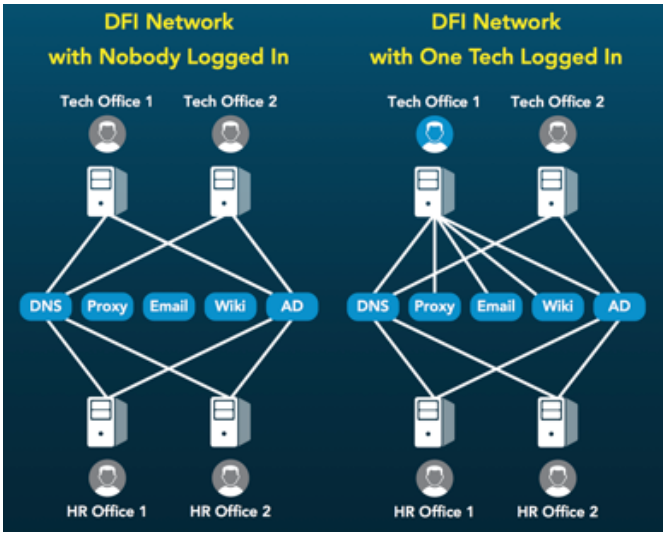
Figure 1: *DFI enforces adaptive access control in accordance with a specified policy and sensor input about the current state.*

DFI leverages recent advances in SDN to dynamically control network access in a manner that's scalable to large enterprise networks. A small policy enforcement kernel is implemented within SDN controllers that updates access rules for all switches on the network. DFI is designed to work with existing SDN hardware, be portable across SDN controllers, composable with other SDN applications, and extensible with new third-party services.

Benefits

DFI provides a means to enforce the principle of least privilege on networks and enables numerous capabilities that are impractical on existing networks.

- DFI can enforce granular connectivity changes in response to user login and logoff activity: the network can be configured to grant a device limited access to network resources until a user successfully logs in, at which point connections to specific resources are enabled, as required by that user.
- DFI can be utilized to implement contingency plans and quickly enable alternative network configurations.



Authentication-triggered network access control

- Devices can be quarantined during sensitive operations or when an intrusion has been detected via a human analyst or IDS.
- Incident response teams can take advantage of DFI to quickly alter the network in order to prevent active adversaries from accessing the most critical components while maintaining the ability to observe adversary behavior.

Competitive Advantage

Existing firewalls are effective at protecting against certain threats from external networks but do little to prevent attacks that involve lateral movement within an internal network. Additionally, firewalls are statically configured, with changes or updates requiring manual effort, on human timescales. In contrast, DFI allows for firewall-like functionality for every port on every switch, with updates that can be applied automatically at computer timescales.

Network Access Control (NAC) solutions allow enforcement of pre- and post-admission policies, primarily designed to restrict the access of non-compliant devices (e.g. unauthorized or missing patches). DFI, in addition to its broader capabilities for dynamically shaping network access, enables similar compliancy mitigations but via an entirely software-based approach that eliminates the need for proprietary hardware, is designed to be extensible and scalable, and allows for visibility into and control over policy enforcement mechanisms.

Next Steps

We're continuing to expand our integration with third-party services (e.g. IDS's) and to pilot DFI on government networks.

We're looking for opportunities to broaden the utilization of the technology and are seeking organizations interested in deploying DFI within their environment, networking or security-centric companies interested in integrating DFI into their product suites, and incident response teams seeking proactive ways to both prepare for and to shape a network during an attack.

TRACER: Transparent Protection of Commodity Applications

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Hamed Okhravi
hamed.okhravi@ll.mit.edu

This material is based upon work supported by the Assistant Secretary of Defense for Research and Engineering under Air Force Contract No. FA8721-05-C-0002. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Assistant Secretary of Defense for Research and Engineering.

Overview

Timely Randomization Applied to Commodity Executables at Runtime (TRACER) protects closed-source Windows applications against sophisticated, modern attacks by automatically and transparently re-randomizing their sensitive internal data and layout.

Customer Need

Sophisticated, large-scale attacks against popular closed-source applications such as Adobe Reader, Internet Explorer, Java, and Flash have become widespread in recent years. With such attacks, adversaries can take control of a computer remotely to exfiltrate sensitive information or steal user data. These attacks often compromise millions of machines at once.

A significant problem contributing to large-scale attacks is the homogeneity of the targets. When the attackers develop an attack against an application, since all installations of that application look alike, it will be easy for them to compromise millions of computers at once.

Another factor contributing to this problem is the closed-source nature of the applications running on the proprietary Windows operating system. According to a report, more than 90 percent of desktop computers run Microsoft Windows with closed-source applications. Many cyber protections and defenses rely on having the source code available which makes them non-applicable to such environments.

To properly protect against large-scale attacks on closed-source applications, a diversification technique is needed that changes the sensitive internal data and layout of an application.

Our Approach

TRACER automatically and transparently randomizes key internal data and layout of an application at runtime to prevent modern control hijacking attacks. Figure 1 illustrates this concept at a high level.

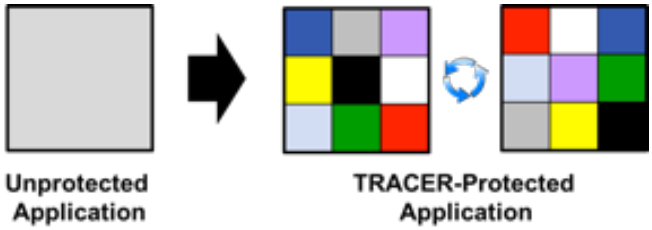


Figure 1: *TRACER frequently randomizes the sensitive internal data and layout of the application after every possible leakage point.*

The internal data and layout include stack cookies and heap metadata that protect static and dynamic memory, as well as the addresses of dynamically linked libraries (DLLs). Attackers frequently target these sensitive regions because they allow the attacker to take control of the application remotely. Figure 2 illustrates the concept of TRACER protecting DLLs.

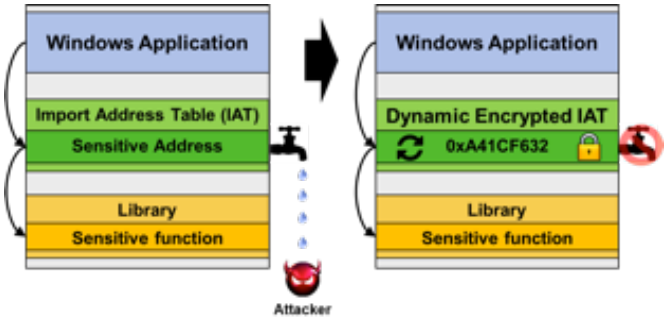


Figure 2: *TRACER prevents leakage of application's sensitive internal data or layout to attackers. The addresses of linked libraries are dynamically re-encrypted after every possible leakage point.*

TRACER re-randomizes the sensitive internal data and layout at every output from the application. Since vulnerable applications can leak how their internals have been randomized, it is crucial to continuously re-randomize these values. A time-based re-randomization would still be vulnerable because the leakage and the attack can happen within the short period of time. As

such, TRACER implements an output-based re- randomization strategy to thwart a potential attacker. With this re-randomization strategy, any information leaked by the application will be stale when attackers attempt to exploit it.

Benefits

TRACER prevents the most common and sophisticated control hijacking attacks against Windows applications. According to a survey, these attacks constitute more than 50 percent of attacks and are commonly used by Advanced Persistent Threat (APT) actors.

TRACER is implemented as a single DLL, and unlike other defenses in this domain does not require access to the source code or modification of the Windows operating system. TRACER only takes minutes to install on each machine and is seamless to operate after the initial installation. TRACER does not interfere with normal maintenance, patching, software inventory, or debugging facilities of an enterprise network.

TRACER incurs an average 12 percent increase in execution time with common Windows applications. The overhead is often masked by the normal application execution delays and is not noticeable by the users. Since most computer systems under-utilize resources such as the CPU, the incurred overhead is likely to be acceptable in most enterprise environments.

Competitive Advantage

The main competitors for TRACER are randomization techniques such as memory layout randomization (Address Space Layout Randomization), compiler-based code randomization, and instruction set randomization techniques. All these techniques employ a “one-time” randomization strategy which makes them vulnerable to information leakage attacks. Using information leakage, attackers can analyze how the application has been randomized and undo the impact of randomization. In fact, information leakage attacks are used frequently to bypass one-time randomization defenses in the wild.

By re-randomizing the sensitive internal data and layout of an application every time any output is generated, TRACER renders leaked information stale and resists attacks that can otherwise bypass randomization defenses. TRACER provides security guarantees that are stronger than all of the previously mentioned techniques.

Unlike many other defenses for closed-source applications, TRACER does not rely on emulation techniques that incur unacceptably high overhead.

Next Steps

TRACER is ready to be deployed in an enterprise to protect all commonly used Windows applications. TRACER has been tested in a laboratory environment. We are seeking partners to deploy and test TRACER in operational environments to help us improve the technology and mitigate any unknown, large-scale deployment challenges.

TRACER can alternatively be implemented within the operating system itself. We are currently exploring such deployment opportunities with operating system vendors.

FLOWER: Network FLOW AnalyzER – Deep Insight Into Network Traffic

Pacific Northwest NATIONAL LABORATORY

Darren Curtis
Darren.Curtis@pnnl.gov

Overview

FLOWER (Network FLOW AnalyzER) is a software application that performs deep IPv4/IPv6 packet header inspection in real-time to collect bi-directional network conversations between computers. It automatically combines unidirectional Internet Protocol (IP) packets into bi-directional network flows. FLOWER can be deployed anywhere in an enterprise using a passive network tap so it cannot be detected.

Customer Need

Enterprise networks, including virtual cloud networks, are under constant attack. Cyber attack tools and hacker communities give cyber-criminals an asymmetric advantage over network and system administrators acting as cyber defenders. This allows the attackers to readily breach networks, create backdoors, and infect systems, leading to costly data loss or theft of intellectual property. Some US government networks have experienced up to 25,000 attempted attacks every day.

There exists an urgent need for a novel detection system that can collect data about network activity throughout the enterprise, providing cyber-defenders insight into traffic patterns, abnormal data flows, and forensic data to study and learn about potential breaches and identify insider threats.

Our Approach

FLOWER utilizes a simple but powerful algorithm based on the IP specifications to parse and aggregate up to 1 million IPv4/IPv6 packet headers per second. FLOWER passively monitors all network traffic. Data can be collected over the same enterprise network being monitored or on a private data collection network.

FLOWER can be deployed on small inexpensive data collection appliances throughout an enterprise and at the perimeter, allowing cyber defenders to selectively target resources to monitor and incrementally deploy appliances to scale to their needs.

FLOWER produces simple CSV-formatted output files that are compatible with existing conventional data analysis tools and emerging cyber analytic research efforts. One example is Trelliscope, a public domain data visualization tool used to analyze data from the IEEE VAST 2013 challenge[1].

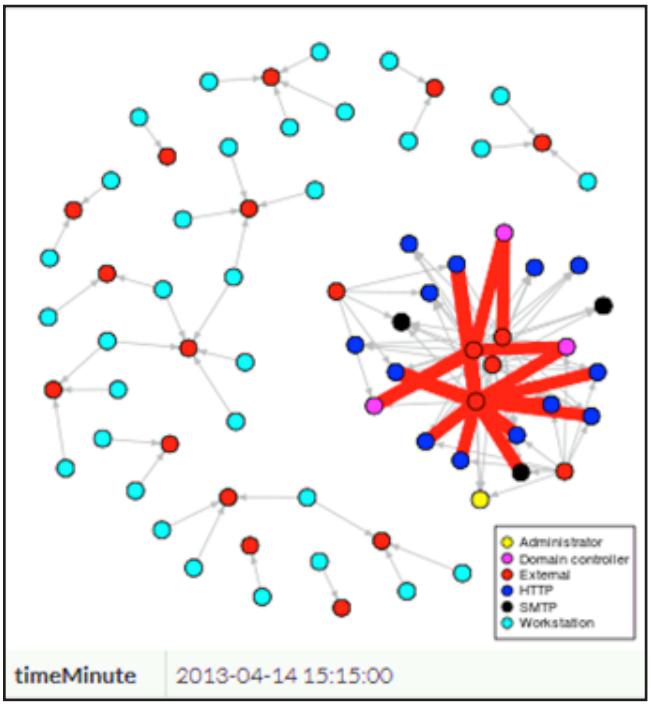


Figure 1: *Trelliscope display used to identify a breach using an Administrator account to take control of the Network Domain Controllers and modify web server configurations to redirect users to the adversary's external web server.*

Benefits

FLOWER can continue to capture network data even when the traffic exceeds the capacity of network routers and switches. It automatically handles partial or fragmented packets until all fragments have been received. In addition, FLOWER can be configured to specify the maximum number of simultaneous conversations, the number of minutes to wait to mark a conversation

[1] http://ieeevis.org/year/2013/info/call-participation/vast-challenge

complete if no packets have been seen, and the maximum number of minutes before forcing a conversation record to be written to a log file.

FLOWER can process packet capture (pcap) files generated by tcpdump, Wireshark, and other pcap generating tools.

FLOWER is a turnkey solution that can scale to meet needs of small to enterprise size networks.

Competitive Advantage

FLOWER has been deployed at over 100 US government sites and many private corporations collecting data of trillions of network flows since 2010.

Network management products from companies such as SolarWinds analyze Cisco NetFlow data to identify traffic patterns and network bottlenecks. Data collected by FLOWER data can be used for those purposes but also provide cyber security analysts more insight in the content of the network traffic to help identify unusual access patterns.

FLOWER provides the ability to recursively parse packet headers to identify the outermost network flow as well as the innermost network flow data encapsulated in a tunnel such as IPv6-in-IPv4, IPv4-in-IPv6, GRE, IPv6, and IPv6-Teredo tunnels.

Figure 2: *A representation of a tunneled network flow where the outer layer could be IPv4 and the inner layer could be IPv6 with IPv6 TCP data.*

Next Steps

FLOWER has been successfully used to detect and mitigate coordinated attacks. Cyber analysts have been able to process data and develop techniques for identifying signatures of potential attacks and modify network configurations to deter future attacks.

We are seeking partners interested in using FLOWER to learn more about their enterprise network traffic and identify potential breaches and insider attackers. We are also seeking partners willing to support a pilot of a customized FLOWER application using micro appliances and a Mobile Adhoc NETwork (MANET) in their enterprise.

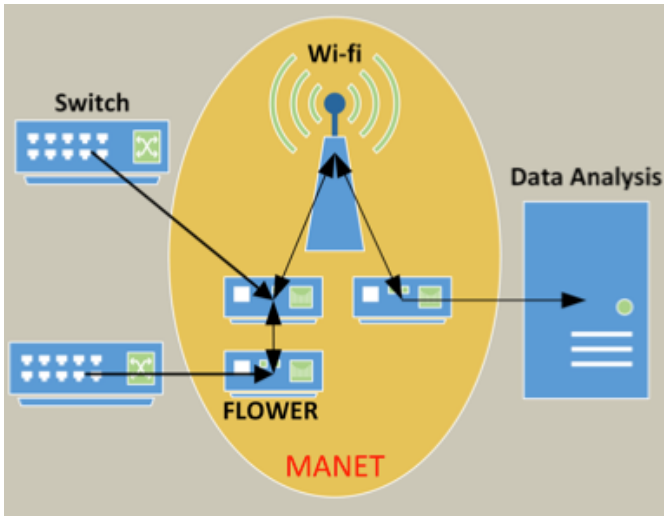


Figure 3: *Using FLOWER appliances to collect data using a secured MANET for offline data analysis.*

SilentAlarm: Detecting Abnormal Network Traffic

Pacific Northwest NATIONAL LABORATORY

Joel Doehle
joel.doehle@pnnl.gov

Overview

SilentAlarm is an inference-based technology for detecting abnormal network traffic that depends on dynamic network behavior knowledge rather than static signatures and thresholds. It characterizes network behavior as likely malicious and enables the detection of zero-day attacks and polymorphic malware without needing prior knowledge of their specific characteristics.

Customer Need

To enact effective cyber security, organizations need to be able to detect unknown malware targeting unidentified vulnerabilities. Many existing security solutions are signature-based, utilizing a detailed description of a given malware's characteristics to detect its presence on their systems and networks. These technologies require specific foreknowledge of a malware's form or function. As a result, they are incapable of detecting unknown malware or attacks exploiting as-yet undeclared vulnerabilities. This leaves organizations vulnerable to adversaries using tactics such as "zero-day" attacks and polymorphic malware. Better solutions are needed to enable organizations to identify and address these and other types of attacks without the detailed foreknowledge required to develop a signature.

Our Approach

SilentAlarm utilizes dynamic behavioral analysis to detect abnormal network traffic resulting from malware and malicious intrusions and takes action to address the malicious software behind them.

SilentAlarm provides this capability by employing a Bayesian inference model that analyzes and correlates network traffic using dynamic network behavior knowledge in order to construct hypotheses regarding likely malicious activity.

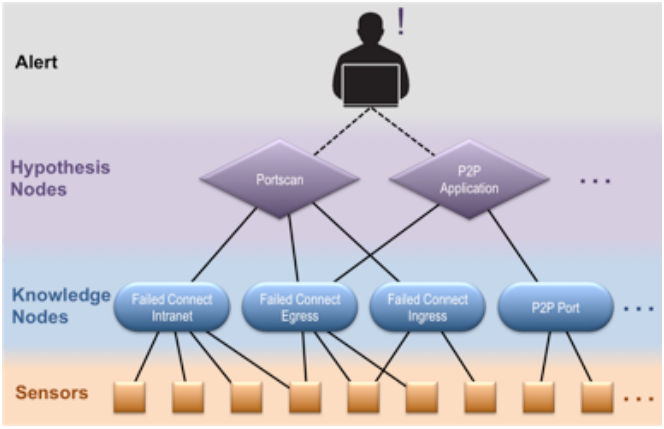


Figure 1: *SilentAlarm Inference Network Architecture*

Network events are fed into SilentAlarm through various types of sensors (e.g., network anomaly, protocol anomaly) that are already in place on a network. The traffic collected at these sensors is ingested by knowledge nodes that are associated with a particular network behavior (e.g., failed or successful SMTP, failed intranet connection). These knowledge nodes characterize the ingested traffic based on the metrics of prior network behavior.

These characterizations are pushed up to hypothesis nodes that construct hypotheses regarding the likely malicious nature of the observed traffic. Each hypothesis node conducts reasoning about one type of malicious action (e.g., port scanning). In order to do so, it subscribes to the characterizations of one or more knowledge nodes and assigns weighting values to the results of each. Collectively, these characterizations enable the hypothesis node to deduce whether the observed traffic is indicative of a particular malicious action.

When such a determination is made and the associated confidence value is greater than or equal to an alert value, a security action can be performed (e.g., sending an alert to a system administrator or disabling or restricting network access to a particular resource).

Network behavior data is continuously collected through the deployed sensors. This data – along with administrator input and feedback into the knowledge and hypothesis nodes regarding characterization and confidence values – enables SilentAlarm to "learn" and refine its understanding regarding abnormal network behavior.

Benefits

SilentAlarm is able to characterize network traffic as likely malicious based on knowledge of prior network behavior and an inferential understanding of what constitutes abnormal network behavior.

In this way, SilentAlarm is not wholly dependent on static thresholds and signatures, as many traditional malware detection methodologies are. As a result, SilentAlarm can detect previously unknown malware (including polymorphic malware and attacks against zero-day vulnerabilities) based on its behavior in a network.

This technology is device and network agnostic. It can be adapted to integrate with presently deployed sensors on an enterprise environment. It is also highly scalable across various network sizes.

SilentAlarm has been proven effective in an active enterprise environment, serving as an integral component of the security of the PNNL network for several years. Upon initial deployment, SilentAlarm correctly identified 200 machines that were infected with "zero-day" type malware, out of a network of 10,000 computers. In continued operation, SilentAlarm identified zero-day type malware on the network within three minutes of machine compromise.

Competitive Advantage

SilentAlarm is highly adaptable and extensible across varying network environments with myriad sensors. It offers proven behavioral based anomaly detection that provides an enhanced complement to signature-based solutions

Additionally, we possess a patent[1] on the technology that prevents others from developing the same type of product.

Next Steps

Several years have passed since SilentAlarm's initial development and operational use. The technology needs to be updated to reflect current network behaviors and to develop sensors for today's network event logging technology.

We would like to partner with a sponsor who is interested in renewing this technology and pursuing potential commercial opportunities for it.

[1] Goranson, Craig A., and John R. Burnette. "Methods and systems for detecting abnormal digital traffic." U.S. Patent 7,908,357, issued March 15, 2011.

3RD COHORT OF TECHNOLOGIES:

- Autonomic Intelligent Cyber Sensor (AICS): Cyber Security and Network State Awareness for Ethernet-based Industrial Control Networks
- Situ: Discovering and Explaining Suspicious Behavior
- Scalable Reasoning System (SRS): Threat Landscape Analysis for the Cyber Defender
- Dynamic Defense & Network Randomization
  - Dynamic Defense: Proactively Defending Control Systems Against Emerging Threats
  - Network Randomization: Moving Target Defense for Computer Systems
- SCOT: Turning Cyber Data into Incident Response Threat Intel
- AMICO: Accurate Behavior-Based Detection of Malware Downloads
- ZeroPoint: Advanced Weaponized Document Detection and Analytics

Autonomic Intelligent Cyber Sensor (AICS): Cyber Security and Network State Awareness for Ethernet-based Industrial Control Networks

Craig Rieger
craig.rieger@inl.gov

Tim Klett
timothy.klett@inl.gov

Overview

The Autonomic Intelligent Cyber Sensor (AICS) provides autonomous cybersecurity and state awareness for Ethernet-based industrial control networks. It employs Autonomic Computing techniques and a Service Oriented Architecture to: 1) automatically discover network entity information, 2) automatically deploy deceptive virtual hosts, and 3) automatically identify anomalous network traffic with very high accuracy.

Customer Need

Industrial Control System (ICS) networks facilitate communication among critical infrastructure and form an attack surface that must be secured. Maintaining state awareness and detecting anomalies are notoriously difficult tasks in traditional IT networks due to their inherent complexities, such as the presence of heterogeneous hardware and software, dynamic network composition and usage patterns, and decentralized control. ICS networks can have similar complexities, however the control system traffic tends to be more observable and amenable to predictive modeling.

Ensuring ICS network cybersecurity in the face of these complexities entails both real-time monitoring of network host composition and agile response to changing network conditions. Neither of these capabilities are well met by manual actions alone. A cyber sensor is needed that automatically reacts to changing network compositions and conditions, while simultaneously attaining the highest possible accuracy and lowest false positive rates in detecting anomalous traffic. Such a sensor will obviate much of the human intervention presently required to effectively monitor evolving industrial networks for anomalies.

Our Approach

AICS employs three major analysis components plus standards based communication channels to monitor and protect ICS networks:

Network Identity Identification (NEI): The NEI performs asset discovery by passively monitoring ICS network traffic. For each host discovered on the network, the NEI catalogs its IP and MAC addresses, and attempts to identify its operating system. The NEI continually updates this network model to reflect the present composition of hosts on the network, thereby providing network state awareness.

Dynamic Honeypot (DHP): The DHP utilizes the NEI's constantly evolving network model to automatically configure and deploy deceptive virtual network hosts, otherwise known as honeypots, which imitate the real hosts on the network. These honeypots serve to draw the focus of malicious intent, and thereby provide a decoy attack surface that is easily monitored for anomalous activity.

Intelligent Anomaly Assessment (IAA): The IAA selectively monitors a prescribed list of host network traffic for anomalous activity while adjusting its own sensitivity based on observed global network trends. Statistical features are extracted from the traffic of each network host into feature vectors. A fuzzy logic based anomaly detection algorithm is then used to compute an anomaly score for each vector that expresses the belief that the current window of packets contains anomalies. The anomaly score is compared against the dynamic sensitivity threshold to determine whether to raise an alert.

Communications: AICS captures control traffic by listening on the ICS network switch's SPAN ports. Network host and alert information is delivered externally over the open-standard IF-MAP protocol and syslog. IF-MAP anomaly alerts are raised through a publish/subscribe style messaging system, enabling network stakeholders to selectively receive only those types of alerts which interest them. The AICS communications approach supports flexible deployment options including the ability to deploy multiple sensors with potentially overlapping host monitoring duties.

Autonomic Intelligent Cyber Sensor (AICS): Cyber Security and Network State Awareness for Ethernet-based Industrial Control Networks

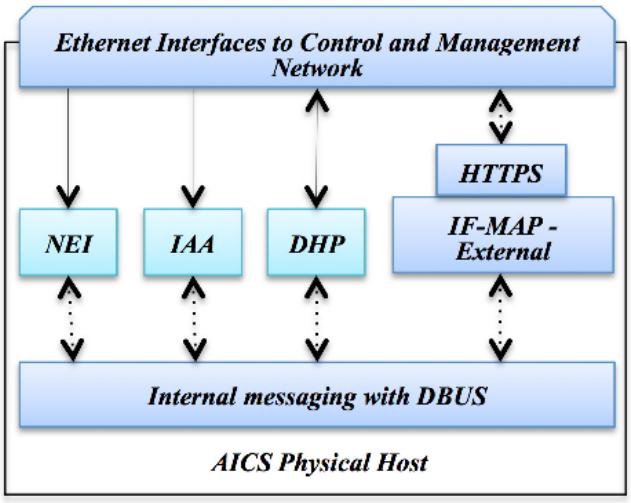


Figure 1: AICS Architecture

Benefits

AICS employs a modular framework that is deployable on commonly available hardware, and provides for automatic gathering of network host information, automatic deployment of dynamic virtual honeypots, and automatic identification of anomalous network traffic.

AICS reduces the need for human intervention in maintaining network state awareness and anomaly detection. Dynamic honeypots are automatically configured and deployed based on passive network observations, reducing dependence on human network expertise and configuration effort. AICS anomaly detection does not rely on human created rules. Instead it automatically learns normal traffic patterns directly from observation of the network. Additionally the anomaly detection algorithm is designed to minimize false alerts.

AICS has been shown to be effective in its ability to automatically configure itself and detect network anomalies within a controlled laboratory setting. For instance, while anomalous traffic was injected into a test ICS network, AICS was able to correctly label packets to specific hosts as either normal or anomalous with greater than 99.8 percent accuracy[1].

The modular nature and common communications infrastructure of AICS provides a flexible base for evolving its functionality in the future. This modular nature and common communications interface allows deployment of multiple AICS devices to achieve scalability. Further, AICS delivers alerts and other information via a common interface, which provides for easy integration with products such as system information and event managers or other data correlation solutions.

Competitive Advantage

AICS is an autonomous, intelligent cyber sensor that learns about its environment in order to maximize its own situational awareness and thereby maximize the efficacy with which it detects anomalies. This is in contrast to other state-of-the-art network awareness frameworks that often require intense intervention by skilled humans. Further, the modular design, extensibility, and standards based communication of AICS provides for quick and reliable integration with other systems.

AICS was developed by Idaho National Laboratory (INL), a Federally Funded Research and Development Center (FFRDC) whose mission includes protecting the cybersecurity of critical infrastructure. INL is internationally recognized for its expertise in providing cybersecurity for critical infrastructure, including industrial networks towards which AICS is targeted.

Next Steps

Given the acumen AICS has exhibited in experimental settings, it is ready for phased transition into real ICS networks. Thus, INL is seeking partners for Beta evaluation and commercialization of AICS for broad application to Ethernet-based ICS networks.

[1] Vollmer, T.; Manic, M.; Linda, O., "Autonomic Intelligent Cyber-Sensor to Support Industrial Control Network Awareness," Industrial Informatics, IEEE Transactions on , vol.10, no.2, pp.1647,1658, May 2014.

Situ: Discovering and Explaining Suspicious Behavior

John Goodall
jgoodall@ornl.gov

Joel Reed
reedjw@ornl.gov

Overview

Situ is a scalable, real-time platform for discovering and explaining suspicious behavior that current technologies cannot detect.

Customer Need

Despite the best efforts of cybersecurity analysts, networked computing assets are regularly compromised, resulting in the loss of intellectual property, the disclosure of state secrets, and financial damages in the billions. A 2014 report from the Center for Strategic and International Studies estimated the global cost of cyber crime at $400 billion annually. There has also been a rise of sophisticated attack groups that continually develop novel methods of penetrating networks that current technologies are typically unable to detect.

Signature-based security systems are effective at detecting known attacks, but are unable to detect novel or sophisticated attacks. Indeed, automated security systems will never be capable of detecting all malicious activity.

Network operators need tools to help identify suspicious behavior that bypasses automated security systems.

In the deluge of data in today's networks, operators cannot be expected to discover suspicious activity without better tools. Further, operators need to understand what makes an event suspicious to determine the importance and impact of the event. Highlighting such suspicious behavior helps operators focus their limited time on the most suspicious events within vast amounts of data.

Our Approach

Situ combines anomaly detection and data visualization to provide a distributed, streaming platform for discovery and explanation of suspicious behavior to enhance situation awareness.

Our novel approach to anomaly detection is based on unsupervised, probabilistic modeling. Key to our approach is modeling events in different contexts or at multiple scales; each event is modeled and scored by multiple anomaly detectors to identify different kinds of anomalous behavior. For example, a context may group events by day of the week or hour of the day to build a model of temporal behavior for each computing asset.

The anomaly detectors update the behavior models online as new data is streamed into the system. The detectors score each event for each context based on the likelihood of new events occurring given the probability model of prior behavior. Scoring the anomalousness of events for multiple contexts provides analysts with an understanding of *why* an event is anomalous. By examining these contexts, operators can understand how different event features contribute to the overall anomaly score.

The architecture of Situ is designed to scale to very high data rates on commodity hardware—hundreds of thousands of events per second. The system stores data on compute nodes for very fast updates and queries. Scored events are published to a data store for archival review and historical analysis. Scored events are also pushed immediately to a web-based visualization to allow operators to monitor the most suspicious events in real-time.

Benefits

Situ helps network operators discover and understand suspicious events that would otherwise go undetected. It reduces the huge volumes of raw network data to a smaller, manageable number of events that should be examined by human domain experts. By highlighting suspicious activity operators can find novel attacks, but can also be made aware of insider threats, policy violations, misconfigurations, and new kinds of behavior that may require some investigation. Through the application of multiple contexts, Situ can look for a wide range of activity. Different contexts perform better for different kinds of attacks. Multiple contexts can also help

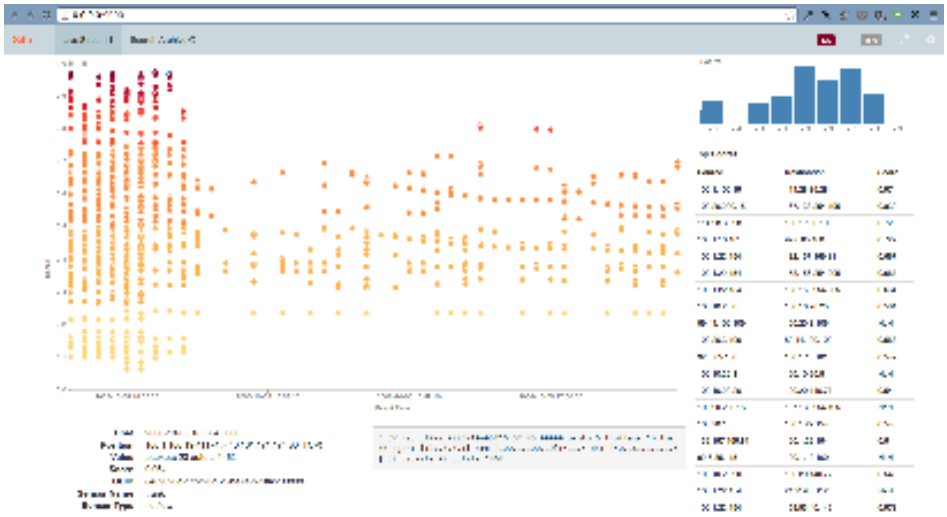


Figure 1: *Situ's streaming user interface shows the most critical events*

explain why an event is suspicious since the varying scores will point operators at certain kinds of behaviors.

Situ is generally applicable to other domains, such as intelligence analysis and cyber-physical infrastructure protection, that require real-time behavioral monitoring.

Competitive Advantage

Situ's probabilistic approach to anomaly detection has several advantages over other methods. Signature-based discovery systems can only identify *known patterns* of malicious behavior. Situ complements such systems by highlighting suspicious behavior that existing systems cannot detect.

Machine learning offers a more robust approach, but typically requires labeled training data, which is rarely available and usually out of date. Situ requires no labeled training data, making it easier to deploy in operational environments. Machine learning approaches typically train periodically offline. Situ trains online so that data models are always up to date.

Other approaches to anomaly detection in cybersecurity commonly help identify atypical events or time windows where an anomaly occurred. Situ goes further and helps operators understand *why* something is anomalous through the scoring and reporting on multiple contexts.

Many approaches to anomaly detection and attack discovery operate in batch mode (e.g. map-reduce jobs in a Hadoop store), which ignores the reality of the speed of cyber attacks. By the time detection takes place, the attacker may have come and gone. Situ operates on real-time streaming data, minimizing the time from the observation of an event by a sensor to the reporting of the event to the operator.

Finally, other approaches to attack and anomaly detection typically have large numbers of false positives, which leads operators to mistrust or ignore alerts. Situ has an adjustable false positive rate that allows an operator to define the acceptable percentage of false positives to set the threshold for discriminating anomalous from normal behavior.

Our visualization approach is unique in that it focuses on streaming data, reducing the time it takes to be notified of important events.

Next Steps

We are currently improving the user interface by creating multiple visualizations that allow analysts to seamlessly move back and forth between a view of the streaming data and a visual query interface to search through archival data.

We are looking for potential pilot and test sites, as well as commercialization and transition partners to put Situ into the hands of the operators who need it.

SRS: Threat Landscape Analysis for the Cyber Defender

Pacific Northwest NATIONAL LABORATORY

Scott Dowson
scott.dowson@pnnl.gov

Rick Riensche
rmr@pnnl.gov

Overview

Cyber defenders need to stay abreast of patterns and emerging trends in the threat landscape to effectively protect their networks. The Scalable Reasoning System (SRS) is a solution that automates data collection from various sources, analyzes the data to identify trends and hot topics, and provides a visual interface to explore the information.

Customer Need

To effectively prepare for and counter cyber threats, cyber defenders must actively survey many sources of information. Only by monitoring a broad spectrum of information resources (social media, threat reports, open source media, etc.) can the full threat landscape be pieced together. Manually discovering, harvesting, and reading data from these sources is time consuming. Tracking emerging trends against historic patterns or correlating reports across multiple sources is a taxing process that carries the risk of missing critical pieces of information. Cyber defenders need a single, consistent, and reliable collection and analysis strategy for information—a system that automatically extracts topics, themes, and trends in the data and visually presents the relevant and emerging threats.

Our Approach

SRS is a flexible framework that encompasses the 1) harvesting, processing, and management of data; 2) analytics to extract, correlate and summarize; and 3) interactive visualizations to explore and interpret the information. SRS was designed from the beginning as an extensible component-based system, so end users are empowered to customize the application to suit their needs.

Drawing from a library of data harvesting components, the system monitors and automatically retrieves data from sites using a variety of data exchange technologies. This retrieval includes pulling data from file systems, data warehouses, and web interfaces. The system can be easily adapted to new data sources as they emerge using the published software development kit.

Analytic components process, extract, and correlate categorical and topical features from the data. For unstructured text, keywords are automatically extracted, correlated, and visualized over time. This capability is used to both identify long trending patterns and detect emerging new patterns. For structured data—including temporal data— distributions and facets are calculated, providing the means to filter and pivot within the data collection.

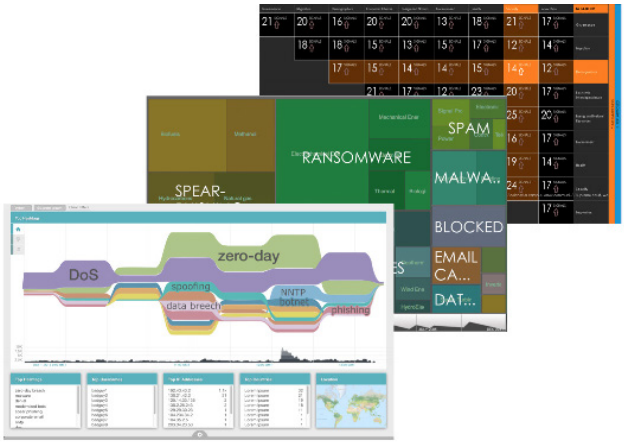


Figure 1: *Interactive visualizations of thematic trends, ontologies, and alerts detected.*

As requirements change or as new algorithms emerge, the extensible plug-and-play nature of the SRS framework allows new components to be developed and integrated to expand the collection and analysis capabilities of the system, keeping the system current and relevant.

SRS is designed to provide data and analytic products through web services and to present the information in an interactive web-based interface. This feature allows the defender to explore and interact with the data using a variety of visual widgets. Users can visually explore the breadth of information; monitor the reported trends; or drill in to focus on newly discovered information.

Figure 2: *Modular plug-and-play architecture*

Benefits

SRS provides situational awareness and alerting for both emerging threats and countermeasures as reported by the selected sources. The system is data agnostic and can be adapted to ingest most data sources. These sources are continuously monitored through a web harvesting engine that performs the arduous task of parsing and processing the data for their salient features. This frees up more time for the cyber defender to analyze the data through the interactive dashboard, which provides the visual means to explore and identify patterns in the data. The dashboard is platform independent and can be customized to meet enterprise and user needs.

Competitive Advantage

Existing tools, such as news aggregators, are useful to cast a wide net and collect information from a specific set of sources. However, these still require the user to manually read and assimilate all the data. SRS can automatically and continually ingest data from a customized set of data sources and extract the data's key features, which are then provided to the user via an interactive visualization. When appropriate, predefined analytics can be applied and presented to draw user attention to particular features.

Other services provide threat intelligence products based on meta-analysis of cyber threat data. Although these products are a very rich source of data, the threat landscape can be further broadened by incorporating other data sources. By combining threat intelligence with other data sources, SRS provides the means for cyber defenders to visually explore, discover, and monitor the full, dynamic landscape.

Next Steps

We are seeking partners interested in participating in a user study to help us learn and understand their specific needs and use cases, and in supporting a pilot of a customized SRS application in their enterprise.

Dynamic Defense: Proactively Defending Control Systems against Emerging Threats

Sandia National Laboratories

Adrian Chavez
adrchav@sandia.gov

Jason Hamlet
jrhamle@sandia.gov

Overview

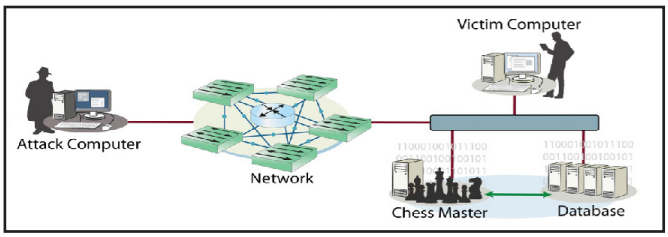
Sandia National Laboratories (SNL)[1] is investigating and developing dynamic defense techniques to better secure critical systems operating within the energy sector. Currently, it is extremely difficult to detect threats within control system networks until it is too late. Using dynamic defense techniques, SNL has developed a set of machine learning algorithms to detect system patterns that deviate from normal operation and respond in an appropriate manner depending on the scenario. Detection coupled with a set of appropriately chosen responses to mitigate malicious traffic patterns, our "chess master" engine in the diagram below, provides situational awareness to an operator and uncertainty to an adversary. We developed these security enhancements while meeting the unique time-critical constraints faced by control systems.

Customer Need

The ability to quickly recognize and appropriately respond to threats is critical to control system security. One can see from ICS-CERT alerts and advisories that critical infrastructure systems continue to be an active target for adversaries. ICS-CERT is reporting over a 20 percent increase in incidents from 2014-2015 alone[2]. Each incident is a security threat to these high-consequence, high-availability systems and deserves an appropriate response strategy that can be activated quickly.

Our Approach

SNL developed dynamic defense algorithms to detect and trigger responses that mitigate attacks on a host system. The algorithms apply an ensemble of machine learning algorithms to detect traffic that deviates from a trained baseline or resembles previously observed attacks. Once detected, a response to mitigate the specific threat is triggered or an alert is generated for operator intervention. A unique set of machine learning algorithms are employed within each host and the specifics of those sets periodically and randomly change, presenting a dynamic, difficult to predict defense posture to the adversary. Our solution works in both Windows and Linux operating systems.



Benefits

Dynamically defending systems against threats launches appropriately chosen mitigations to counter attacks quickly. Our modular implementation provides a framework to integrate new protective measures that counter past, present and future threats. New responses can easily be integrated to mitigate new threats, which is essential for maintaining high availability systems.

Competitive Advantage

Our solution has yielded higher accuracy rates and lower false-positive rates than those in published literature when compared against the same datasets. Our accuracy rates continue to improve as we refine our algorithms and train on more datasets.

Next Steps

We are currently developing our dynamic defense framework to allow for additional response modules to easily be integrated into our existing solution. We seek pilot partners to validate our detection algorithms within a laboratory environment and to transition our technology into industry.

[1] Funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE), Cybersecurity for Energy Delivery Systems (CEDS) R&D Program.

[2] www.securityweek.com/critical-infrastructure-incidents-increased-2015-ics-cert

Network Randomization: Moving Target Defense for Computer Systems

Sandia National Laboratories

Adrian Chavez
adrchav@sandia.gov

William M.S. Stout
wmstout@sandia.gov

Overview

Computer systems continue to use predictable communication paths, static configurations, and unpatched software, all of which benefit an adversary. Sandia National Laboratories (SNL) has developed a prototype implementation of a moving target defense solution that efficiently randomizes IP addresses, application port numbers, and network communication paths while maintaining network connectivity, functionality, and performance. Introducing randomness, uncertainty, and unpredictability thwart attacks and shift the advantage back to the defender. Applying these protective measures converts computer systems into moving targets, adding an additional layer of defense in the early stages of an attack.

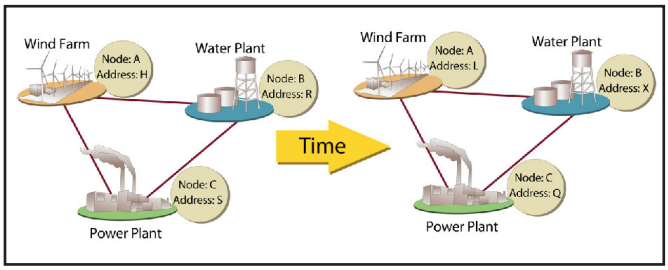
Customer Need

The first step an adversary takes is to gain reconnaissance information about a system of interest Cyber security incidents have risen dramatically, from just 5,503 in 2006 to 67,168 in 20141. In 2014 ICS-CERT found that 55 percent of incidents were APT related[1]; furthermore, 53.22 percent of all ICS-related incidents were network scanning/probing[2]. Many of these incidents are enabled by the broad availability of system information that is openly available to anyone upon request or observation. Randomization of such information is a promising solution that can protect a system against these early stages of an attack.

Our Approach

SNL's network randomization solution can be retrofitted into existing computer systems in a scalable and transparent manner. Software Defined Networking (SDN) technology allows our randomization schemes to be inserted directly into the network layer, so our solution is transparent to the end devices and scalable. We depend on an SDN controller within the network to manage the randomization of network configurations.

Each of the SDN switches is responsible for communicating with the controller to learn the random IP address, port number, and path assignments for traffic traversing the network.



Benefits

Our solution can be rapidly introduced into an existing network using OpenFlow capable hardware switches. If adding new hardware is infeasible, software-based switches, such as Open vSwitch, can be used. The randomness of network configurations provides an environment that is continuously changing and difficult for an adversary to target.

Competitive Advantage

Moving target defense strategies often involve introducing agent software onto each node in the network to randomize network configurations. This approach is effective in small environments but does not scale to large networks such as critical infrastructure networks. We are taking the next step to put research to practice and have developed a prototype that is scalable, efficient, and effective in defending against adversaries in the early stages of an attack. Latency introduced is minimal (<20ms in our test environment) and continues to improve as our development progresses.

Next Steps

We seek pilot partners to deploy our randomization algorithms at a larger scale than our test environment (300 nodes). We ultimately seek to transition our technology into industry and integrate our solution with other management systems.

[1] http://www.gao.gov/assets/680/671253.pdf

[2] https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2014_Final.pdf

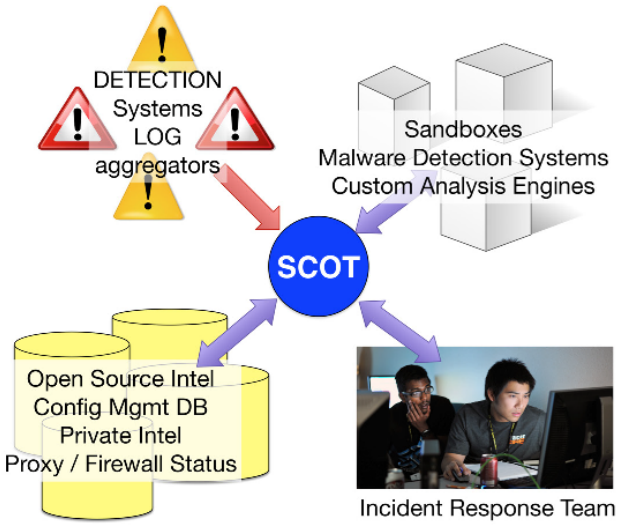
SCOT: Turning Cyber Data into Incident Response Threat Intel

Sandia National Laboratories

Todd Bruner
tbruner@sandia.gov

Overview

The Sandia Cyber Omni Tracker (SCOT) is a cybersecurity incident response management system and knowledge base. Designed by cybersecurity incident responders, SCOT provides a new approach to manage security alerts, analyze data for deeper patterns, coordinate team efforts, and capture team knowledge. SCOT integrates with existing security applications to provide a consistent, easy to use interface that enhances analyst effectiveness.

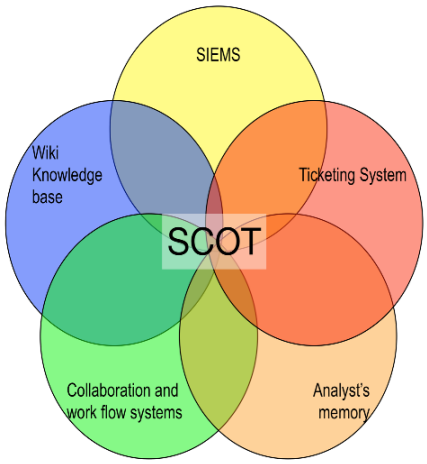


Customer Need

Incident response (IR) teams utilize many systems to detect, collect and analyze cybersecurity event data. These systems, while solving pieces of the puzzle, often fail to give the analyst a holistic view of what is happening and their team's response to those events. Many systems do not have the flexibility to work with the IR processes to research and document those activities. Research is not easily shared and searchable, so the team's effectiveness decreases, especially when key personnel are on vacation or take other positions. Without a ready corpus of examples of past events, training new team members becomes a lengthy process. Each additional tool adds cognitive load to the analyst and the tool's maintenance needs take the analyst away from the primary task of IR.

Our Approach

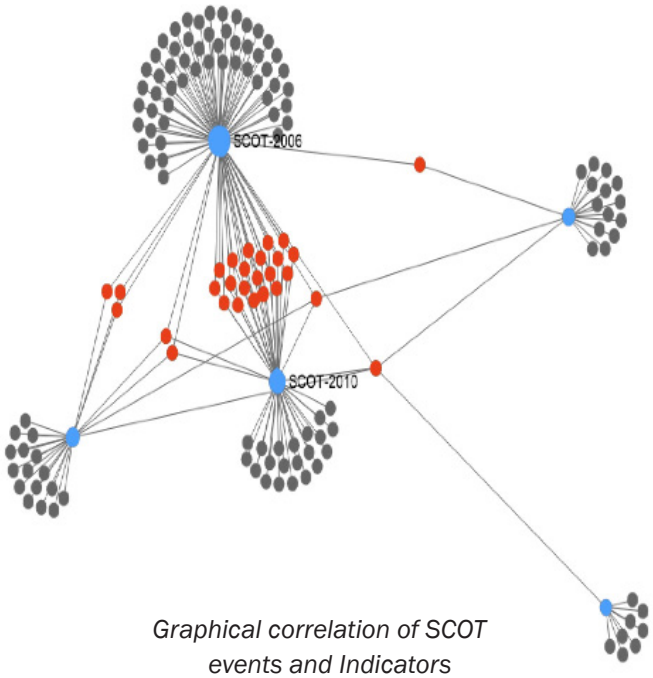
Focused on removing the friction between analysts and their tools, SCOT enables analysts to document and share their research and response efforts. As a software suite that integrates data from detectors, analysis, and other information sources, it provides real time updates of the team's work to keep the team informed and coordinated. SCOT automatically identifies indicators to help the analyst discover and respond to advanced threats. Centralization of the data reduces the contextual shifts necessary to access each detection system. Fusing detection data with the accumulated team knowledge allows the team to quickly discover that a new alert might be part of a larger campaign. In addition, SCOT automates and simplifies common analyst tasks to increase analyst's effectiveness by freeing them to concentrate on cybersecurity – not tool mastery.



Benefits

The number of alerts Sandia's IR team has seen has nearly doubled in the past several years. SCOT enabled the team to keep up with this increase without adding additional team members. As a training tool, new team members started contributing in weeks, instead of months. In just over 4 years SCOT has amassed a database of over 700K indicators from analyst and alert input. These indicators help the team spot an adversary's methods and tactics, as well as highlighting common

targets within the enterprise. SCOT processed over 1.6 million alerts since deployment, while maintaining 99.9 percent availability, and required minimal administration. SCOT is fully scalable to meet higher loads.



Graphical correlation of SCOT events and Indicators

Competitive Advantage

Sandia's incident response team realized several advantages using SCOT over other solutions. SCOT's ease of use eliminated the steep learning curve of traditional SIEMS and captured team knowledge much more effectively. Designed for cybersecurity, SCOT allows the IR team to enter data easily, instead of struggling to conform to a ticketing system designed for other purposes. While workflow systems handle linear workflows easily, SCOT is purpose built for the looping nature of cybersecurity investigations. SCOT also solves the challenges of keeping wikis, spreadsheets and documents up-to-date and accessible to an IR team. While top-notch analysts may be able to keep everything in their brains, SCOT will capture their knowledge for when they go on vacation or to other employment.

Combining the best attributes of these solutions, SCOT has been enthusiastically adopted by Sandia's IR team as an indispensible tool that enhances the productivity of the team and helps us keep an edge on our adversaries.

Next Steps

Start building your organizational memory and turn security data into intel your IR team can use. Please go to http://getscot.sandia.gov for more information on licensing and how to obtain SCOT. Sandia is actively developing SCOT and looking for ideas and contributors. We seek opportunities for collaboration and custom development. Please contact tbruner@sandia.gov for additional information.

AMICO: Accurate Behavior-Based Detection of Malware Downloads

The University of Georgia

Roberto Perdisci
perdisci@cs.uga.edu

Kang Li
kangli@cs.uga.edu

Overview

AMICO is a novel open source software system for accurate behavior-based detection of malware downloads in live web traffic. Once deployed at the edge of a network, AMICO automatically learns how to distinguish between malware and benign software downloads by observing the download behavior of the network users themselves. After the initial learning phase, AMICO is able to automatically detect new (including zero-day) malware downloads in the monitored web traffic, and can alert network security personnel with detailed incident reports about the detected events.

Customer Need

Sensitive computer networks are under constant attack. Cyber criminals can gain almost unrestricted access to a network by leveraging malicious websites to force users to download and run malicious software. This allows the attackers to implant malware into the network, and to create a backdoor that can lead to costly data breaches and loss of intellectual property.

Most networks rely on traditional antivirus software to protect themselves from malware downloads. Unfortunately, security researchers have repeatedly demonstrated that anti-virus defenses are only partially effective and may miss more than 65 percent of the latest malware threats.

Other existing malware download defenses make extensive use of URL blacklists, to prevent users from accessing known malware distribution sites. However, by nature these blacklists lag behind the new threats and fail to detect a significant number of new malware.

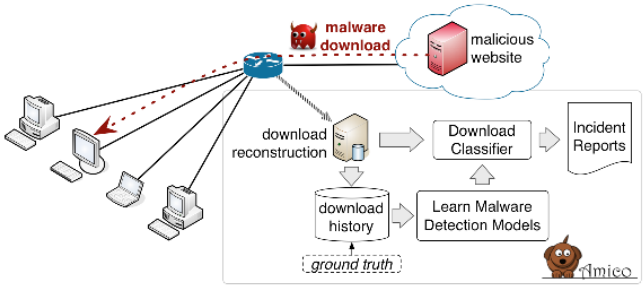
Therefore, there exists an urgent need for novel malware download detection systems that can better protect a network's perimeter by accurately detecting new, never-before-seen malware files and the related malware distribution sites.

Our Approach

AMICO's behavior-based approach to detecting malware downloads is based on the following main intuition: to evade existing defenses, malware distribution operations must be *agile*.

For example, to avoid antivirus detection, malware developers make heavy use of code obfuscation and polymorphism to frequently change their malware files. On the other hand, benign executable files usually change only when a new version is released.

Furthermore, to evade URL blacklists, malicious websites that distribute malware need to frequently relocate, for example by changing their domain name and IP addresses. On the other hand, benign executable files are typically hosted at professionally operated service providers with a stable domain name and network infrastructure.



To leverage these intuitions, AMICO combines advanced network traffic monitoring with artificial intelligence and data mining methods.

AMICO passively monitors all web traffic at the edge of a network. Every time a user downloads an executable file, the system performs an on-the-fly reconstruction of the download from the network traffic, and stores the file into a download history database, along with provenance information regarding *who* (i.e., what machines) downloaded the file and *where* (i.e., what website) the download came from.

During an initial training period, some of these download events are first labeled as either *benign* or *malware*, using the partial ground truth provided by existing antivirus tools. Given these labeled events and statistics about the download behavior of the network users collected during the training phase, AMICO automatically learns a web traffic model that can be used to accurately classify future malicious file downloads based simply on their provenance characteristics.

Benefits

AMICO is able to efficiently reconstruct and accurately classify new malware file downloads by passively monitoring web traffic from the network edge. It explicitly leverages the fact that modern malware distribution operations are highly agile, and turns the attackers' strategy into an advantage for the defenders.

AMICO automatically learns how to distinguish between malware and benign software downloads by observing the download behavior of the network users, providing a defense that can self-adapt to the deployment network and further improve detection accuracy.

Competitive Advantage

AMICO provides a fully open source and easy to deploy solution for detecting malware downloads in live web traffic.

AMICO's download classifier does not rely on signatures, and therefore is not affected by malware code polymorphism and obfuscation. Instead, AMICO leverages malware polymorphism as a feature to enable a more accurate detection of malware download events. Furthermore, AMICO does not rely on URL or domain name blacklisting, and does not need to run malware files in a sandboxed environment.

Unlike existing defenses, AMICO is able to detect never-before-seen malware download events by leveraging their provenance characteristics, and by automatically learning from the download behavior of the network users themselves. Therefore, AMICO provides an effective complement to current antivirus and malware defense solutions.

Next Steps

AMICO has been tested via pilot deployment in a large academic network serving tens of thousands of users, where it was able to detect more than 95 percent of all new malware file downloads and about 80 percent of malware files missed by existing defenses.

Pilot testing in other operational environments would provide an important opportunity to improve performance, usability, and to compare AMICO to other existing defense solutions. In addition, we are seeking partners and sponsors who are interested in fostering the widespread adoption of AMICO.

Funded through the National Science Foundation's (NSF) Division of Advanced Cyberinfrastructure (ACI), Cybersecurity Program

ZeroPoint: Advanced Weaponized Document Detection and Analytics

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Kevin Z. Snow
kevin@zeropointdynamics.com

Fabian Monrose
fabian@zeropointdynamics.com

Overview

The ZeroPoint Platform provides highly effective, high-throughput, next-generation detection and diagnostics of exploit payloads embedded in documents distributed via email and the web, content used in so-called drive-by downloads and attacks on network servers.

Customer Need

Today, the widespread proliferation of document-based exploits distributed via massive email and web-based attack campaigns is an all too familiar strategy. Attackers use this tactic to kickoff full-scale data breaches by weaponizing documents and web content to gain total access to the recipient's computer. In 2012 these data breaches cost an average of $5.5 million per incident, a figure on the rise as organizations increase their online presence and threats become more sophisticated. In August 2014, for example, several large financial institutions lost gigabytes of data to cyber criminals targeting the financial sector. Sadly, contemporary defenses have failed to keep pace with the relentless onslaught of evasive techniques that are readily available from off-the-shelf attack toolkits. In light of this ever-present threat, there is a need to empower organizations to allow end-users to safely use email and browse the web.

Our Approach

The ZeroPoint Platform is a network appliance that analyzes documents, email, web content, and server interactions collected from network border traffic and operator-submitted content. Potentially hazardous documents or web content are launched or replayed in their target application to dynamically unpack embedded exploit payloads, and then application memory is inspected to discover those payloads. The key to the ZeroPoint approach is a patented *"execution of data"* technology that uses an advanced micro-OS built into the analysis engine to enable fast, accurate inspection of data or memory to identify exploit payloads. This core technology takes advantage of hardware virtualization to inspect all data by directly *executing* it to discover what lurks within, without relying on any form of software emulation. There is no need to guess whether a resource is malicious based on trivially obfuscated file content, post-infection behavior that can easily be disguised, or out-of-date signatures. ZeroPoint hones in on the small portion of an attack the adversary cannot omit or quickly adapt – the exploit payload – by leveraging the fact that exploits operate under practical constraints that bound their operations in ways that make them detectable.

Benefits

The ZeroPoint Platform enables users to safely use email and browse the web with the confidence that attacks are promptly discovered at the first stage, before data is lost. The platform transparently provides complete network-wide protection with no downtime to deploy, inspects each document or web page in about one second, and produces virtually no false alarms. Our core technology has already been validated on the University of North Carolina Chapel Hill campus (29,000 students with 5 Gbps average load) and large-scale empirical analysis spanning 10,000 weaponized documents. ZeroPoint's diagnostic functionality also enables operators to preemptively block connections to malicious domains found in the inspected content.

Competitive Advantage

Contemporary approaches for detecting attacks have relied on antivirus *signatures* of previously observed attacks. Unfortunately, the delay between the first use of an attack and the deployment of its signature is too often measured in weeks and months. Meanwhile, the attackers continually compromise users. Moreover, signatures are widely known to produce many false alarms. A myriad of recent solutions and products–most based on sandboxing technology–claim to avoid the pitfalls of signatures and protect against zero-day attacks. However, these containment mitigations are complex and costly to deploy and manage on endpoints. Instead, ZeroPoint provides transparent and network-centric detection. Other detection solutions leverage sandboxes for behavioral analysis. Unfortunately, that behavior is easily camouflaged with benign activity, only revealing itself after an extended period of time, or is limited to the analysis of

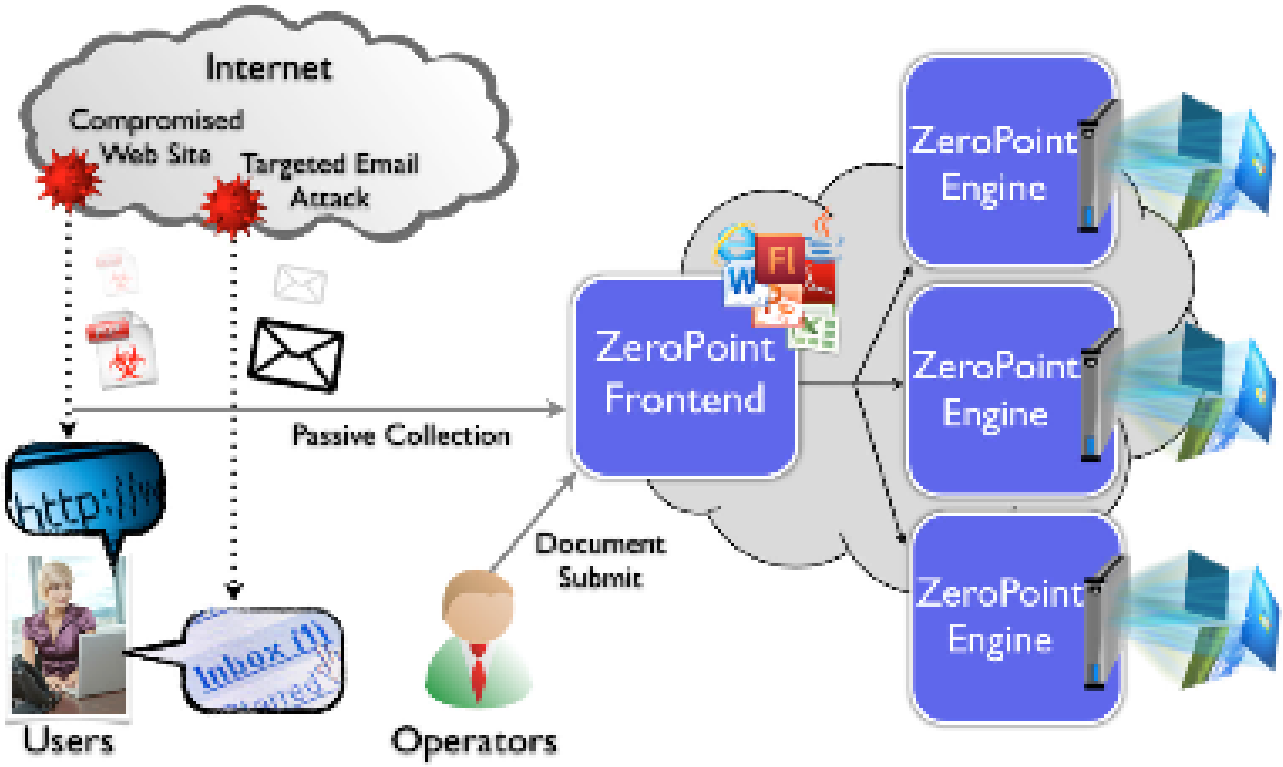


Figure 1: The deployment scales-up with multiple analysis engines in a cloud-ready model, or rolls all components into one rack-mounted server in stand-alone deployments capable of tens of thousands of inspections a day.

executable files. Rather than fruitlessly attempting to keep up with the fast pace of new attack signatures and easily disguised behaviors, our technology turns the tide by moving away from this status quo and avoiding signatures and observable post-infection behavior altogether. Our underlying technology has not required any signature, behavior, or heuristics updates over several years, and yet we continue to find weaponized documents where other solutions fail – a testament to the solid foundation on which ZeroPoint is built. In short, ZeroPoint takes a unique approach that is faster, more accurate, and more informative than other solutions.

Next Steps

Two U.S. Patents that protect the core technology are pending. We seek commercialization of our technology through partnering or licensing with a major vendor of network security products. We also seek pilot deployments with large organizations for our stand-alone or cloud-ready prototypes.

ZeroPoint is available commercially from ZeroPoint Dynamics, a network security startup.
http://www.zeropointdynamics.com/

Funded through the National Science Foundation's (NSF) Division of Advanced Cyberinfrastructure (ACI), Cybersecurity Program

2ND COHORT OF TECHNOLOGIES SUMMARY:

- CodeDNA: Scalable, High-Speed, High-Volume, Shareable Malware Detection
- Quantum Security
  - Velocirandor: Quantum Random Number Generator
  - Quantum Secured Communications: Security for the Nation's Infrastructure
- CryptAC: Securing Data for Public Clouds
- LOCKMA: Lincoln Open Cryptographic Key Management Architecture
- Digital Ants: Dynamic & Resilient Infrastructure Protection
- PACRAT: The Blended Physical and Cyber Risk Analysis Tool
- SerialTap: Enabling Complete Situational Awareness in Control Systems
- SecuritySeal: Critical Protection for Your Supply Chain
- WeaselBoard: Zero-Day Exploit Protection for Programmable Logic Controllers (PLCs)

2nd Cohort of Technologies Summary

For additional information about any of the following technologies contact the TTP program at **ST.TTP@hq.dhs.gov**

CodeDNA

Johns Hopkins Applied Physics Laboratory: CodeDNA is a scalable, shareable technology that facilitates community-based defense against malware attacks. It supports crowd-sourcing of information by providing a robust malware identifier (fingerprint) that is deterministic and repeatable for correlating reports, analyses, and other information about attackers, yet cannot be used to re-create the original malware.

For more information, contact Shaku Harshavardhana, Shaku.Harshavardhana@jhuapl.edu and Kathleen McGill, Kathleen.McGill@jhuapl.edu

Quantum Security

Los Alamos National Laboratory: Quantum Security is comprised of two technologies: *Velocirandor*, a small, low-cost, deployable solution for the generation of secret random numbers (keys) at high rates, and *Quantum Secured Communications*, which leverages Quantum Key Distribution to replace all of the key management services provided by a public key infrastructure. Velocirandor and Quantum Secured Communications are licensed and available commercially from Whitewood Encryptions Systems.

For more information, contact Raymond Newell, raymond@lanl.gov

CryptAC

Massachusetts Institute of Technology–Lincoln Laboratory: CryptAC provides cryptographic access control to enable secure storage of data in public clouds. It presents a seamless view of fine-grained access control and data organization to return control of data security to data owners and separate data security from storage management to enable interoperability with multiple cloud service providers.

For more information, contact Gene Itkis, itkis@ll.mit.edu

LOCKMA

Massachusetts Institute of Technology–Lincoln Laboratory: Lincoln Open Cryptographic Key Management Architecture (LOCKMA) is a software component that simplifies the task of adding cryptographic protections and underlying key management to software applications and embedded devices such as mobile devices, unmanned vehicles and sensors as well as larger systems. LOCKMA is licensed to several companies for use in government solutions.

For more information, contact Roger Khazan, rkh@ll.mit.edu

Digital Ants

Pacific Northwest National Laboratory: Digital Ants is a nature-inspired resilient cybersecurity technology designed to protect large enterprise networks and next-generation critical infrastructures. Digital Ants is lightweight and uses automatic learning to reduce the human cost of configuration and supervision. Digital Ants uses minimal network and computational resources.

For more information, contact tech@cynash.com

PACRAT

Pacific Northwest National Laboratory: The Physical and Cyber Risk Analysis Tool (PACRAT), a vulnerability and risk analysis software package, blends the methodology and assessment process used in physical and cybersecurity domains to provide a comprehensive assessment of the security strategy. PACRAT has been licensed to Rhino Corp adding capability to its existing products.

For more information, contact Doug MacDonald, douglas.macdonald@pnnl.gov

SerialTap

Pacific Northwest National Laboratory: SerialTap is a low-cost, embedded device for passively tapping serial line communication and transmitting it over an Ethernet network for comprehensive control system situational awareness. SerialTap is a cost-effective, nonintrusive way to enable complete situational awareness in process control systems that integrates easily with common IT enterprise security solutions.

For more information, contact ***serialtap@cynash.com***

SecuritySeal

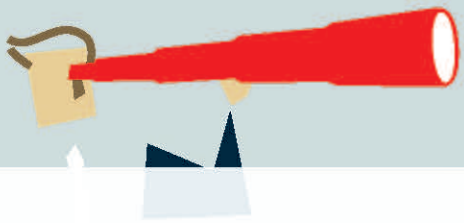
Sandia National Laboratories: SecuritySeal, a combined hardware and software solution, enables cryptographically secure authentication of a seal and any object it is affixed to, providing anti-counterfeiting protection, tamper detection and supply chain risk management for high-value assets. SecuritySeal's inability to be cloned and highly adaptable security level are valuable in a wide range of applications that require the verification of the integrity of a seal.

For more information, contact Todd Bauer, ***tmbaue@sandia.gov***

WeaselBoard

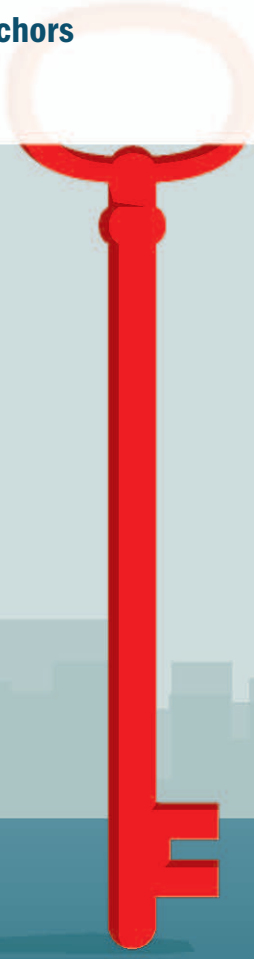
Sandia National Laboratories: WeaselBoard provides zero-day exploit protection for programmable logic controllers (PLC) by capturing and analyzing backplane traffic among PLC modules. It detects changes to process control settings, sensor values, module configuration information, firmware updates, and process control program updates.

For more information, contact John Mulder, ***jmulder@sandia.gov***



1st COHORT OF TECHNOLOGIES SUMMARY:

- NeMS (Network Mapping System): Network Characterization and Discovery Tool
- PathScan: Finding the Attacker Within
- Choreographer: A Moving Target System to Thwart Automated Network Attackers
- Hyperion: Detecting Vulnerabilities and Sleeper Code, Analyzing Malware, and Assuring Software
- USB-ARM: Architecture for USB-based Removable Media Protection
- Hone Technology: Producing Insight by Correlating Machine and Network Activities
- MLSTONES: The DNA of Cyber Security - An Organic Model for Identifying Cyber Events
- CodeLock: Tamper-proof Trust Anchors



1st Cohort of Technologies Summary

For additional information about any of the following technologies contact the TTP program at **ST.TTP@hq.dhs.gov**

Network Mapping System (NeMS)

Lawrence Livermore National Laboratory: NeMS, a software-based network characterization and discovery tool creates queryable graphs of any IP network with details of network entities, attributes, roles, and logical relationships. NeMS was licensed to Cambridge Global Advisors (CGA), which created a startup company, Quellum (http://www.quellum.com), to commercialize the technology.

For more information, contact
Celeste Matarazzo, matarazzo1@llnl.gov
or Domingo Colon, colon3@llnl.gov

Hyperion

Oak Ridge National Laboratory: Hyperion, a malware forensics detection and software assurance technology, computes the behavior of software, including malware, in all circumstances of use without the need for source code. Hyperion is commercially available from Lenvio.
https://www.lenvioinc.com

For more information,
contact Stacy Prowell, prowellsj@ornl.gov
2015 R&D 100 Award Winner

PathScan

Los Alamos National Laboratory: PathScan, a network anomaly-detection tool uses statistical models to identify network behavior. Through behavioral models, the technology detects the movement of hackers once they breach a network and allows operational teams to triage and respond to security events in real time. PathScan was licensed to Ernst & Young LLP.

For more information,
contact Ben Uphoff, Ben.Uphoff@ey.com

USB-ARM

Oak Ridge National Laboratory: USB-ARM protects the host against threats from removable media by installing an efficient and customizable layer of security that brokers device communication with the operating system. This tool blocks all communication to the device until a set of user-defined criteria are met.

For more information,
contact Stacy Prowell, prowellsj@ornl.gov

Choreographer

Oak Ridge National Laboratory: Choreographer, a moving-target system thwarts automated network attackers by constantly changing the public addresses of protected servers. This makes it challenging for attackers to guess the server's address and allows a seamless redirection of an attack to a honey pot.

For more information,
contact David Sims, simsdl@ornl.gov

Hone Technology

Pacific Northwest National Laboratory: Hone, a host-based cyber sensor, provides a new data source of correlated host and network data by forming a bridge between the networking and processing parts of monitored machines. This bridge enables the sensor to know which programs are responsible for malicious network activities. Hone has been made open source and can be found at https://github.com/HoneProject/. It also is being actively used by Google, PNNL and others as a cyber security data collection tool.

For more information,
contact Glenn Fink, glenn.fink@pnnl.gov

MLSTONES

Pacific Northwest National Laboratory: MLSTONES is a set of tools that quickly categorizes data and compares attributes of the data to determine if it poses a threat. The methodology uses the concepts of protein identification and families, inheritance and function to apply to a number of cyber-based data types.

For more information, contact tech@cynash.com

CodeLock

Sandia National Laboratories: CodeLock, a cryptographically secure code obfuscation technology, provides tamper- proof trust anchors, functional elements of which are introduced into information systems to provide unbiased measurement and unimpeded control capabilities. The trust anchors protect critical hardware and software components from malicious tampering even when operating in a compromised environment.

For more information, contact Adrian Chavez, adrchav@sandia.gov

ONLINE
http://dhs.gov/csd-ttp

FACEBOOK
Facebook.com/dhsscitech

EMAIL
ST.TTP@hq.dhs.gov

YOUTUBE
www.youtube.com/dhsscitech

TWITTER
@dhsscitech

PERISCOPE
@dhsscitech