Cyber Security Division

FY 2012 Annual Report

Homeland Security

Science and Technology

Cyber Security Divison

FY 2012 Annual Report

Homeland Security

Science and Technology

LETTER FROM THE DIRECTOR

Douglas Maughan, Ph.D.

Cyber adversaries continue to present a full spectrum of threats not only to the U.S. government, but to private organizations and critical infrastructure sectors. This past year the Department of Homeland Security (DHS) Science and Technology Directorate's Cyber Security Division (CSD) has continued to shape cybersecurity research and development (R&D) of new technologies, tools, and techniques to protect and secure the Homeland Security Enterprise (HSE).

A goal within the division is to fund applied cybersecurity research and technologies, which can be transitioned to DHS operational components or commercialized into the marketplace. To achieve this goal, CSD applies the full technology life cycle process—research, development, test, evaluation, and transition to practice—to each technology. This successful method continues to serve a variety of stakeholders within the Department and at other federal agencies; state and municipal administrations and first responders; critical infrastructure sectors; international partners; academic institutions; and national laboratories.

CSD's major focus in fiscal year 2012 was the award of 33 new research contracts across private industry, national laboratories, and the academic community through a Broad Agency Announcement (BAA 11-02) solicitation. BAA 11-02 was a direct response to the Administration's Comprehensive National Cybersecurity Initiative, Financial Services Sector R&D Plan, and DHS's National Protection and Programs Directorate requirements. CSD received more than 1,000 white papers and 224 proposals in response to the solicitation, which included 14 technical topics areas. Awards ranged in length from one to three years depending on the maturity of the technology solution. Furthermore, CSD established numerous international agreements with Australia, Canada, the Netherlands, Sweden and the United Kingdom, to co-fund select BAA 11-02 projects.

CSD strengthened links between the cybersecurity research community, critical infrastructure sectors, and international partners, which has resulted in enhanced end-user participation in research; increased research funds; and greater awareness and use of research products across a variety of missions.

In addition to the impactful accomplishments noted above, CSD had a number of noteworthy highlights, including the following:

- The Research Data Repository project published an ethics framework for conducting information and communication technology research, which resulted in *The Menlo Report*. This report was posted to the Federal Register for comment. A companion document, *Applying Ethical Principles to Information and Communication Technology Research,* was also published and details the principles and applications more granularly and illustrates their implementation in real and synthetic case studies.
- CSD launched the Transition to Practice (TTP)

project, which targets federally funded technologies that are most likely to be successfully transitioned into the commercial market within two years and that will have a notable impact on the cybersecurity of our nation's networks or systems. This is an ambitious endeavor with enormous potential for positive impact. Additionally, TTP will provide a connection point for cybersecurity researchers, the federal government, and the private sector and ensure technology transitions from the research laboratories to the HSE.

- The Cybersecurity Forensics project funded the publication of *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector* by the CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute. The report provides a greater understanding of the behavioral, technical, and organizational factors that lead to insider threat attacks. Report results briefed to the Electronic Crimes Task Forces, which is sponsored by the U.S. Secret Service, will provide law enforcement and the private sector with recommendations to lessen or prevent insider attacks.

- The Trustworthy Cyber Infrastructure for the Power Grid project commercialized the NetAPT tool and licensed the technology to more than 20 North American Electric Reliability Corporation auditors and public utilities. NetAPT will help public utilities identify vulnerabilities in their routing hardware and software, helping them to mitigate insecure devices.

- Over 1,500 students from 131 schools participated in the CSD-sponsored National Collegiate Cyber Defense Competition (CCDC) events in 2012, making the CCDC the largest collegiate cyber defense competition program in the nation.

- CSD assisted with the R&D elements of the President's Executive Order 13636 and Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience. CSD is playing a leading role in the development of a National Critical Infrastructure Security and Resilience R&D Plan, planned for a draft release early in 2014.

This annual report will give you a high-level understanding of CSD's programs, projects, and accomplishments within fiscal year 2012.

For additional information, please visit the CSD website at www.dhs.gov/st-csd, or to reach out to the CSD program managers listed in this report.

Douglas Maughan, Ph.D.
Cyber Security Division Director
Department of Homeland Security
Science and Technology Directorate

CONTENTS

II LETTER FROM THE DIRECTOR

1 CYBER SECURITY OVERVIEW

3 RESEARCH INFRASTRUCTURE TO SUPPORT CYBERSECURITY

- 4 Experimental Research Testbed
- 5 Research Data Repository
- 6 Software Assurance Marketplace

TRUSTWORTHY CYBER INFRASTRUCTURE

- 10 Secure Protocols
  - 11 Domain Name System Extensions Deployment Initiative
  - 12 Secure Protocols for the routing infrastructure
  - 13 Internet Measurement and Attack Modeling
- 15 Process Control System Security
  - 16 Linking the Oil and Gas Industry to Improve Cybersecurity
  - 18 Trustworthy Cyber Infrastructure for the Power Grid

21 FOUNDATIONAL ELEMENTS OF CYBER SYSTEMS

- 22 Cyber Economic Incentives
- 23 Enterprise Level Security Metrics and Usability
- 24 Homeland Open Security Technology
- 26 Moving Target Defense
- 28 Software Quality Assurance
- 30 Tailored Trustworthy Spaces

33 CYBERSECURITY USER PROTECTION AND EDUCATION

- 34 Cyber Security Competitions
- 36 Cyber Security Forensics
- 38 Identity Management and Data Privacy Technologies

41 CYBERSECURITY TECHNOLOGY EVALUATION AND TRANSITION

- 42 Cybersecurity Experiments and Pilots
- 43 Transition to Practice

45 LOOKING AHEAD TO FY 2013

46 PERFORMER INDEX

CYBER SECURITY DIVISION OVERVIEW

The mission of the Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Cyber Security Division (CSD) is to

⇒ **Develop and transition new technologies, tools, and techniques to protect and secure systems, networks, infrastructure, and users, improving the foundational elements of our nation's critical infrastructure and the world's information infrastructure; and**

⇒ **Provide coordination and research and development (R&D) leadership across federal, state, and municipal governments; international partners; the private sector; and academia to improve cybersecurity research infrastructure.**

CSD serves a wide range of customers by coordinating and cooperating with partners within the Department and other federal agencies; state and municipal administrations and first response agencies; private sector companies in a wide range of industries; Internet security research organizations around the world; and universities and national laboratories.

To accomplish its mission and serve its customers, CSD has organized its work into five major program areas:

Research Infrastructure to Support Cybersecurity (RISC) — provides a research infrastructure to enable the national and international cybersecurity research community to discover, test, and analyze state-of-the-art tools, technologies, and software in a scientifically rigorous and ethical manner.

Trustworthy Cyber Infrastructure (TCI) — ensures that the nation's critical infrastructure—such as the oil and gas pipelines, information infrastructure, and Internet—become more secure and less vulnerable to malicious and natural events.

Foundational Elements of Cyber Systems (FECS) — focuses R&D activities on the characteristics that are essential to the desired end states of trustworthy cyber systems and accelerates the transition of new cybersecurity technologies into commercial products and services.

Cybersecurity User Protection and Education (CUPE) — focuses R&D activities on developing ways to improve the security and protection of user online activity, attract the next generation of cybersecurity warriors, and provide the tools needed for investigating cybercriminal and terrorist activities.

Cybersecurity Technology Evaluation and Transition (CTET) — provides a coordinated process of assessments, evaluations, and operational experiments and pilots to transition the fruits of research into practice.

RESEARCH INFRASTRUCTURE TO SUPPORT CYBERSECURITY

Cybersecurity R&D involves understanding new threats and risks and discovering solutions that will help protect our nation's cyber infrastructure. The RISC program provides a research infrastructure that mimics real-life conditions, which allows the program to accelerate the research, development, and deployment of effective defenses for U.S.-based computer networks and systems.

In fiscal year (FY) 2012, CSD carried out the RISC program through three projects:

- **Experimental Research Testbed** — CSD provides a cybersecurity testbed capable of large-scale, repeatable experiments to safely analyze cyber attacks, evaluate defense mechanisms against attacks on the cyber infrastructure, and develop attack mitigation and confinement strategies.
- **Research Data Repository** — CSD created and maintains a large-scale data set repository of real network and system traffic to support the cybersecurity research community in its mission to accelerate the design, production, and evaluation of next-generation cybersecurity solutions, including commercial products.
- **Software Assurance Marketplace (SWAMP)** — CSD established SWAMP to provide a national-level resource in software assurance for open security technologies used in civilian agencies and their communities. SWAMP can be used as both a research platform and as a core component in supporting U.S. Government software development activities.

Experimental Research Testbed

The Experimental Research Testbed Project, also known as the DETER testbed, focuses on providing cybersecurity researchers the ability to run experiments on a secure "virtual Internet." The testbed's contained environments allow researchers to safely test advanced defense mechanisms against "live" threats without endangering other research or the larger Internet. The DETER testbed is currently used to test and evaluate cybersecurity technologies by more than 200 organizations from more than 20 states and 17 countries, including major DHS-funded researchers, government, industry, academia, and educational users. Additionally, the DETER testbed has been used by 30 institutions for more than 40 classes, ultimately reaching more than 2,000 students.

The DETER testbed provides the necessary infrastructure—networks, tools, methodologies, and supporting processes—to support national testing of emerging and advanced security technologies. CSD's current efforts to further develop the testbed will support larger and more complex experiments with increased usability.

The success of the DETER testbed lies largely on collaboration with the cybersecurity research community. Annual workshops are conducted to disseminate and discuss project results and outcomes, and CSD has published reports documenting benchmarks, testbeds, data collection and analysis, and evaluations of security mechanisms that have been deployed.

FY 2012 Highlights

- Advances to the underlying DETER testbed technology to enable new scientific experimentation were realized through development and use of the DETER Containers system for virtualization at multiple scales, and the Montage Agent Interface system, a communications and control system for experimentation.
- CSD continued efforts to extend DETER to support federated experimentation for the SmartGrid as part of our work in the DETER Enabled Federated Testbeds (DEFT) Consortium. This is part of an emphasis on the SmartGrid and emerging power-based cyber-physical communities.
- All of these new technologies, facilities infrastructure, and methodologies were driven by a continuous improvement cycle of use and feedback from several active user communities. During FY 2012, the testbed supported a growing educational classroom community and a specialized sophisticated user community as part of a Defense Advanced Research Projects Agency (DARPA) program.

PROJECT PERFORMERS

- Pacific Northwest National Laboratory
- University of California, Berkeley
- University of Illinois at Urbana-Champaign
- University of Southern California, Information Sciences Institute

WEBSITE

www.deter-project.org

PROGRAM MANAGER

Luke Berndt
luke.berndt@hq.dhs.gov

Research Data Repository

The Research Data Repository, also known as PREDICT, is the only freely available, legally collected repository of large-scale datasets containing real network and system traffic. PREDICT will provide a streamlined legal framework to centralize and control the distribution of datasets while protecting researchers, data providers, and data hosts. PREDICT will help users accelerate the design, production, and evaluation of next-generation cybersecurity solutions, including commercial products. Until PREDICT was created, technology developers and evaluators often had to determine the efficacy of their technical solutions based on anecdotal evidence or small-scale test experiments. Now, a variety of real-world data sources and types are available and evaluations, so solutions may be based on more comprehensive real-world data.

PREDICT was conceived as a distributed repository with three key components: data providers, data hosts, and a Coordinating Center. Data providers legally supply the data to be shared through the repository, data hosts provide the infrastructure to store the repository data and transfer it to authorized recipients, and the Coordinating Center provides a centralized mechanism for cataloging available data while managing the submission and review of data requests. The goal of the distributed structure is to provide secure, centralized access to multiple sources of data and promote data sharing while protecting the privacy of the data producers and the security of their networks and data. A Web portal, **https://www.predict.org**, provides both public and restricted access to the repository.

In FY 2012, PREDICT entered a new phase. International participation efforts commenced, starting with Japan, and associated procedures and legal frameworks were created. Additionally, the legal framework was revised to be more flexible by providing a mechanism to address classes of datasets covered in the legal agreements, as opposed to specific enumeration of data, and agreement modification for any new data.

Additionally, in FY 2012, PREDICT developed an ethics framework for conducting information and communication technology research, which resulted in *The Menlo Report*. This report was posted to the Federal Register for comment. The report's associated disclosure control principles will be released in FY 2013.

FY 2012 Highlights

- New customers and partners were added to the project, including 45 from academia, 44 from commercial industry, 2 foreign and 18 government partners, and 3 non-profit organizations.
- 119 new datasets were added to the repository, which represented a 44 percent increase in the number of datasets available for analysis and experimentation.
- The cybersecurity research community requested 210 accounts and requested access to 340 cumulative datasets.

PROJECT PERFORMERS

- Georgia Tech Research Corporation
- Global Cyber Risk, LLC
- Merit Network, Inc.
- Packet Clearing House
- Research Triangle Institute
- University of California, San Diego
- University of Michigan
- University of Southern California
- University of Wisconsin

WEBSITE

https://www.predict.org

PROGRAM MANAGER

Manish Karir
manish.karir@hq.dhs.gov

Software Assurance Marketplace

The cost of removing a software defect or correcting software vulnerability grows exponentially for each downstream phase of the software development life cycle (SDLC) in which it remains undiscovered. It has been proven that software designed and built in with security throughout the SDLC is more resilient, costs less to sustain, and requires less to rework. To ensure the software is secure throughout the SDLC, software developers need a way to test the software iteratively for defects and vulnerabilities. However, many developers do not have the proper tools to assist them in conducting these tests.

To address these issues, CSD initiated the SWAMP project to provide a national-level R&D resource in software assurance for open security technologies used in civilian agencies and their communities. SWAMP can be used as both a research platform and as a core component in supporting U.S. government software development activities. SWAMP will provide a collaborative research environment in which software developers can test their software, software tool developers can test and fine-tune their tools against a wide range of software packages, and software researchers can interact and exchange ideas to improve software assurance tools and techniques.

By offering these services, SWAMP will reduce the number of vulnerabilities found in software, improve software quality assurance tools and technologies, advance the quality and adoption rate of software quality assurance tools, lower the threshold for using them, and make it easier to interpret the results from a range of disparate tools. SWAMP will be positioned as a national marketplace that is a core part of the software development and ownership lifecycle, offering access to a comprehensive set of software analysis tools, software testing capabilities, and documentation and training materials to improve the overall quality and reliability of software that powers our nation's critical infrastructure.

The SWAMP project began in late FY 2012. In FY 2013, CSD will build and design the SWAMP environment, which will involve the following steps:

- Develop and design the cybersecurity architecture for SWAMP
- Develop policies and procedures for intrusion/ incident response
- Establish and maintain security operations monitoring systems
- Select and install initial software packages; install and calibrate software analysis tools
- Establish strong authentication and Identity Access Managementcapabilities for SWAMP

PROJECT PERFORMERS

- Morgridge Institute for Research

WEBSITE

http://swamp.cosalab.org/index.html

PROGRAM MANAGER

Kevin E. Greene
kevin.greene@hq.dhs.gov

TRUSTWORTHY CYBER INFRASTRUCTURE

The Internet connects all our networks, including the nation's critical infrastructure. It has become the central nervous system for our government, our citizens, and our industries. When it is attacked, the effects can ripple far and wide. The Internet's address system, created in 1983, was not built with security in mind, and was not meant for services that require strict verification of users' identities, such as electronic banking. No one envisioned how vast the Internet would become. The TCI program focuses on ensuring that the nation's critical infrastructure, such as the oil and gas pipelines, information infrastructure, and Internet, becomes more secure and less vulnerable to malicious and natural events. This program engages industry, government agencies, the private sector, and academia to improve the core functions of the Internet and critical-sector information systems in order to protect their owners, operators, and users, including U.S. government networks and private citizens.

The majority of government communications utilize private-sector networks, including critical infrastructure (e.g., information technology [IT] networks, communications networks, financial services networks, the electrical grid, oil and gas systems). These networks have critical interdependencies, so a failure in one network (e.g., the electrical grid) can impact others (e.g., financial networks).

In FY 2012, CSD carried out the TCI program through three projects:

- **Secure Protocols** — CSD led efforts to develop security protocols for the existing Internet infrastructure (essential to daily Internet operations) so that users are not redirected to unsafe websites or pathways by malicious actors.
- **Internet Measurement and Attack Modeling (IMAM)** — In order to better protect and defend critical Internet infrastructure, CSD first identified which critical Internet resources were most vulnerable to attack. CSD developed capabilities to map Internet hosts, routers, and modeling and analysis to predict the effects of cyber attacks on commercial and federal infrastructures.
- **Process Control Systems (PCS) Security** — CSD led efforts to secure the information systems that control the country's critical infrastructure, including the electrical grid, oil and gas refineries, pipelines, and the financial sector, to reduce vulnerabilities as legacy, standalone systems are networked and brought online.

Secure Protocols

The National Strategy to Secure Cyberspace clearly states the need to "secure the mechanisms of the Internet by improving protocols and routing."

The Internet is made up of three key pieces: the Domain Name System (DNS), Internet Protocol (IP) addressing, and the routing infrastructure. The DNS maps IP addresses consisting of long sets of numbers to a recognizable set of letters, words, or numbers; the average Internet user recognizes these as Web addresses. IP addresses serve as unique identifiers and are critical to the construction of networks and the identification of destinations on the Internet. The routing infrastructure relies on the Border Gateway Protocol (BGP) to discover routes between the large networks that make up the Internet.

The Secure Protocols project aims to solve the lack of secure mechanisms in BGP, DNS, and IP addressing by securing the endpoints with public/private keys and protecting the path for communications to eliminate tampering. These are complex, globally distributed systems, owned and operated by a variety of organizations and companies that bear the burden of upgrading their systems and software to improve security. Because of this individual responsibility, it is critical to involve these entities in every step of the process, including the research, development, testing, evaluation, and transition activities necessary to design, implement, standardize, and deploy secure solutions for BGP and DNS.

In order to achieve its goals, the Secure Protocols project is divided into two distinct, yet interrelated initiatives: **Domain Name System Security Extensions (DNSSEC) Deployment Initiative** and **Secure Protocols for the Routing Infrastructure.**

Domain Name System Security Extensions Deployment Initiative

DNS is a critical piece of Internet infrastructure that serves as the Internet's "phonebook" by translating human-readable host names into IP addresses. Nearly all Internet applications rely on some form of DNS data and an unintentional error in the DNS can effectively deny service to Internet applications. Worse still, intentionally false DNS data can result in hijacked communications. For example, erroneous DNS data for SomeBank.com can render SomeBank.com unavailable while intentionally false data can direct the bank customer to an adversary pretending to be SomeBank.com. The security, trust, and continued functionality of the Internet will be greatly influenced by implementing a more secure, robust DNS. In recent years, the Internet community has developed a standard protocol known as DNSSEC to provide security for all DNS communications. CSD, in partnership with the National Institute of Standards and Technology (NIST), has led the DNSSEC Deployment Initiative, encouraging all sectors of the digital world to voluntarily adopt measures that will improve the security of the Internet's naming infrastructure. The initiative is part of a global, cooperative effort involving organizations in the public and private sectors.

The underlying technology of DNSSEC is now well understood. CSD's FY 2012 efforts revolve around measuring the deployment of DNSSEC technology and monitoring tools to ensure that existing deployments are working as intended. To measure growth in DNSSEC deployment, CSD developed tools to track who is providing DNSSEC data by measuring the number of signed zones and signed delegations. To understand who is making use of the signed data, aggregated summary reports were added to the DNSSEC Check tool, which are useful in measuring DNSSEC support in resolvers that are responsible for initiating DNS lookups and ultimately obtaining the DNS records desired by users. To help ensure correct operations, tools were also developed to help manage deployments. This work includes multiple troubleshooting and monitoring tools to provide better situational awareness for DNS operators, monitoring plug-ins add DNSSEC capabilities to existing network monitoring systems. New capabilities include a DNSSEC-Nodes tool that observes DNS packets "on the wire" and provides a visual representation of the steps used to validate the DNS data. Other tools add support for DNS operations, such as "out-of-band" signing, zone realms, and threshold-based auto signing.

FY 2012 Highlights

- For zone operators who provide data, new tools and enhancements to existing tools were provided for monitoring DNSSEC deployments.
- For DNS resolvers who request data, new tools for measuring and visualizing resolver behavior were provided, including extended DD-WRT and OPEN-WRT Graphical User Interfaces (GUIs) to provide status and control of the resolver.
- CSD developed open source tools and scripts that illustrate a methodology for evaluating resolvers and provide a path to resolvers for DNSSEC compliance.

PROJECT PERFORMERS

- NIST
- Shinkuro, Inc.
- SPARTA, Inc., a Parsons Company

WEBSITES

www.dnssec-deployment.org
www.dnssec-tools.org

PROGRAM MANAGER

Edward Rhyne
edward.rhyne@hq.dhs.gov

Secure Protocols for the Routing Infrastructure

In 2004, CSD started the Secure Protocols for the Routing Infrastructure effort to improve the security of Internet Addressing and Routing and make it less susceptible to disruption and misdirection caused maliciously or through misconfiguration. IP addresses serve as unique identifiers that are critical to the construction of networks and identification of destinations. The **Resource Public Key Infrastructure (RPKI)** standard provides a method for verifying the authenticity of IP addresses. The routing infrastructure relies on the BGP to discover routes between the large networks that make up the Internet. Currently, it is challenging to determine if a BGP route has been altered, allowing for the interception or misdirection of traffic. The **BGP Security (BGPSEC)** standard allows network operators to detect of changes to the routing path, while taking into consideration the scale and complexity of global Internet routing. CSD has played a leading role in the development of both standards and in promoting their adoption.

The systems that support Internet routing and addressing are complex, globally distributed, and owned and operated by a variety of organizations and companies that bear the burden of upgrading their systems and software to improve security. Because of this, these entities have been involved in every step of the standardization process.

In addition to working with the Internet community to draft the RPKI and BGPSEC standards, CSD develops tools to help encourage the deployment of these technologies by network operators. These tools include an automated test suite that makes it easier for router vendors to test implementation and a tool for creating, validating, and distributing address certificates.

FY 2012 Highlights

- In February 2012, the Internet Engineering Task Force—the open standards body for the Internet—published a suite of 14 specifications defining security protections for the global Internet Routing Infrastructure, 10 of them authored under DHS funding. These specifications have proven their worth by being implemented, accepted, and deployed.
- Five tutorials and workshops were held in operator forums worldwide, employing a platform that gave operators hands-on access to the new technology, in real time, with globally distributed routers in the Internet.
- New versions of the DHS-funded software that implements the standards were made available, including support for new standards specification and better scaling features. Two interoperability tests were conducted between these implementations and the others.

PROJECT PERFORMERS

- SPARTA, Inc., a Parsons Company
- Raytheon BBN Technologies

WEBSITE

https://www.dhs.gov/csd-spri

PROGRAM MANAGER

Luke Berndt
luke.berndt@hq.dhs.gov

Internet Measurement and Attack Modeling

The Internet has grown organically as individuals and institutions connect to obtain information, communicate, and exchange files in addition to the myriad of other needs that are dependent on cyberspace. The protection of cyber infrastructure depends on the ability to identify critical Internet resources that are subject to attack. The first step is to measure the infrastructure as it exists today, then make periodic or continuous measurements to identify changes, recognize attacks, and provide analysis.

The IMAM project is focused on the development and application of modeling and analysis capabilities to predict the effects of cyber attacks on federal government installations and other critical infrastructure. It accomplishes this through the detection of malware and botnets, situational understanding, and attack attribution. The technologies being developed are critical to national security missions—in particular, to missions that support DHS watch-center operations that conduct analyses of cyber infrastructure threats and risks, as well as missions that strengthen U.S. military and civilian communications environments that rely on the Internet.

IMAM made considerable progress in FY 2012. A powerful and versatile globally distributed measurement infrastructure—***Archipelago*** (Ark)—has now expanded to 60 monitors in 30 countries on 6 continents. Ark's capabilities include using several techniques to measure both current versions of Internet communications protocols (IPv4 and IPv6), as well as monitoring IPv6 adoption. IPv6 is an evolutionary upgrade that was developed when IPv4 address space began reaching maximum capacity; however, the two versions will coexist for many years. Ark now continuously gathers the largest set of IPv4 and IPv6 topology data ever made available to academic researchers and government agencies. Ark regularly provides richly annotated topology maps of observable Internet infrastructure, as well as a powerful measurement platform capable of performing other types of Internet infrastructure measurement experiments.

Additionally, completed versions of the ***Correlation Layers for Information Query and Exploration*** (CLIQUE) and the ***Traffic Circle*** cyber visualization tools were released in FY 2012, helping analysts identify malicious activity in high-volume computer network data through

behavior modeling coupled with interactive visual analysis. Both tools were delivered to the United States Computer Emergency Readiness Team for testing.

FY 2012 Highlights

- S&T funded the development of monitors and conducted continuous probing of BGP-announced IPv6 prefixes to map and better understand trends in the IPv6 Internet space.
- S&T funded the development of a new approach to discover anycast (used by most large DNS services), which detects masquerading (e.g., man-in-the-middle attacks).
- S&T awarded seven new R&D contracts through Broad Agency Announcement (BAA) 11-02 to six government, private sector, and academic institutions. Through these contracts, awardees will aim to make Internet infrastructure more resilient and provide measurement data that will help the research community better understand how cyber systems operate and interact. Three additional contracts will be awarded in FY 2013. Together, these 10 contracts will comprise a significant portion of the IMAM project portfolio for the next three fiscal years and will strengthen the nation's cyber health.

PROJECT PERFORMERS

- Columbia University
- Georgia Tech Research Corporation
- Merit Network, Inc.
- Naval Postgraduate School
- Oak Ridge National Laboratory
- Pacific Northwest National Laboratory
- Raytheon BBN Technologies
- University of California, San Diego
- University of Southern California, Information Sciences Institute

PROGRAM MANAGER

Ann Cox, Ph.D.
ann.cox@hq.dhs.gov

Process Control System Security

PCSs are computer-based facilities, systems, and equipment used to remotely monitor and control sensitive processes and physical functions. They are responsible for the distributed monitoring and control of much of the nation's critical infrastructure, such as the electrical power grid and oil and gas refineries and pipelines. As these traditionally stand-alone systems are being connected and brought online, vulnerabilities have been introduced with the migration to standard IT components; introduction of standard networking technology, such as Transmission Control Protocol/ Internet Protocol (TCP/IP); and integration of business and process control networks.

These vulnerabilities have increased the need for cybersecurity in PCSs, particularly in the energy sector. Critical to national interest, the electrical power grid underlies virtually all economic activity and essential government services. Because the majority of the critical infrastructure is not owned by the federal government, but rather by private companies that are often reluctant to share information due to their wish to maintain competitive advantages, it is up to the federal government to fund R&D and provide transition pathways for the vendor community to assist infrastructure owners.

To address these needs, the PCS Security project was established in 2009. Requirements for the project come from the cybersecurity requirements gathering process, internal to S&T, as well as from industry sources, including the Industrial Control Systems Joint Working Group, led by the DHS National Protection and Programs Directorate, and the Department of Energy's (DOE) Roadmap to Secure Control Systems in the Energy Sector.

In order to focus on the most critical areas, the PCS Security project is broken into two separate efforts: **Linking the Oil and Gas Industry to Improve Cybersecurity** (**LOGIIC**) and **Trustworthy Cyber Infrastructure for the Power Grid** (**TCIP-G**).

Linking the Oil and Gas Industry to Improve Cybersecurity

In 2004, DHS identified the oil and gas industry's PCSs and supervisory control and data acquisition systems as potential points of threat from terrorists seeking to destabilize the energy industry supply capabilities and the U.S. economy. Recognizing this vulnerability, industry and government came together to start the LOGIIC consortium, an ongoing collaboration between oil and natural gas companies and S&T.

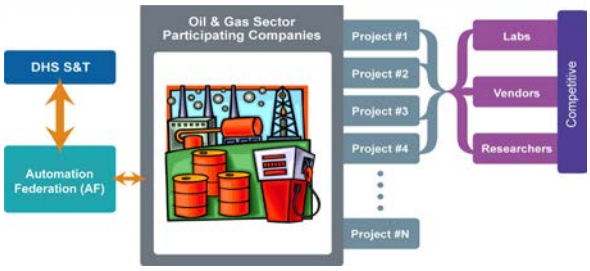


Figure 1: The LOGIIC organizational process for identifying and conducting projects

The LOGIIC consortium facilitates cooperative research, development, testing, and evaluation procedures to improve cybersecurity in petroleum industry digital control systems. The consortium undertakes collaborative R&D projects to improve the level of cybersecurity in critical systems of interest to the oil and gas sector. The objective of LOGIIC is to promote the interests of the sector while maintaining impartiality, the independence of the participants, and vendor neutrality.

LOGIIC represents a model partnership between government and industry. In this effort, oil and gas companies contributed the operational environment, expertise, and project management; vendor companies provided security expertise and products; and S&T contributed testing facilities and independent research staff with technical security expertise. Current members of LOGIIC include: BP, Chevron, Shell, Total, and other large oil and gas companies that operate significant global energy infrastructure.

FY 2012 Highlights

- The LOGIIC consortium completed a study of Host Protection Strategies (HPS) to evaluate host-based cybersecurity technologies for use in a process control environment. Host Protection is when a service is hosted on one machine but leveraged by any other networked machines. The idea is to investigate security solutions that would reside on the host to see which protection strategy is most effective in a PCS setting. The Application Whitelisting Report presents findings of the LOGIIC project regarding application whitelisting, key attributes to its use in a PCS environment, and general conclusions about its implementation. This report, and others, can be found at https://logiic.automationfederation.org.
- The LOGIIC consortium presented the findings from the Safety Instrumented Systems (SIS) project and the HPS project to industry at the International Society of Automation (ISA) Automation Week, a yearly technical conference that addresses security practices for control systems. SIS are the devices, sensors, and functions that measure and react to specific processes within a plant. The purpose of SIS is to bring a plant or control system to a safe steady state during emergencies.
- CSD received the 2012 DHS S&T Under Secretary's Award for Outstanding Collaboration in S&T.

PROJECT PERFORMERS

- SRI International

WEBSITE

www.logiic.org

PROGRAM MANAGER

Greg Wigton
gregory.wigton@hq.dhs.gov

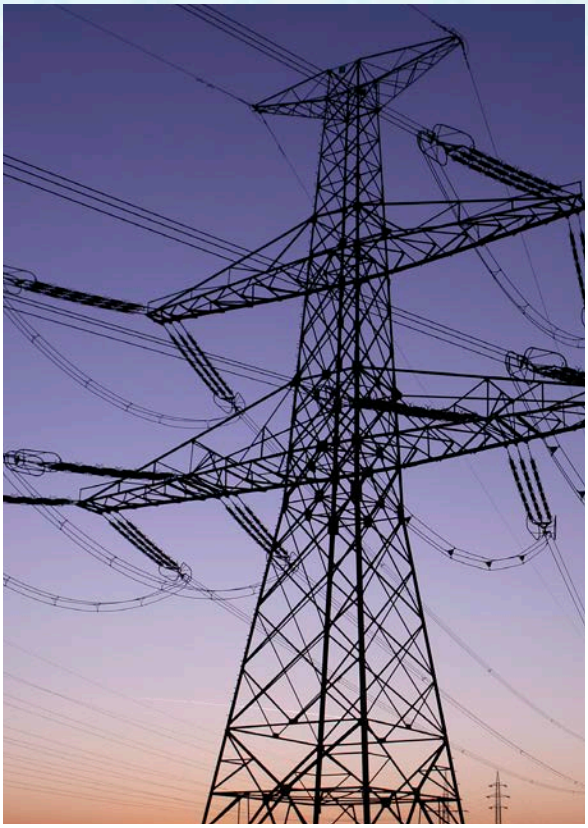
Trustworthy Cyber Infrastructure for the Power Grid

CSD and DOE jointly funded the TCIP-G effort to address the challenge of protecting the nation's power grid by significantly improving the way the power grid infrastructure is built, thus making it more secure, reliable, and safe.

Today's quality of life depends on the continuous functioning of the nation's electric power infrastructure, which in turn depends on the health of an underlying computing and communications network infrastructure that is at serious risk. These risks may come from cyber hackers who gain access to control networks or create denial-of-service attacks on the networks themselves, or from accidental causes, such as natural disasters or operator errors.

Research conducted as part of the TCIP-G effort focuses on securing the low-level devices, communications, and data systems that make up the power grid, to ensure trustworthy operation during normal conditions, cyber attacks, and power emergencies. Simulation and evaluation techniques are employed to analyze real power grid scenarios and validate the effectiveness of the TCIP-G designs and implementations. TCIP-G has also developed interactive and open-ended applets for middle-school students, along with activity materials and teacher guides to facilitate the integration of research, education, and knowledge transfer by linking researchers, educators, and students.

In FY 2012, the effort made considerable progress in several research areas, including Advanced Metering Infrastructure (AMI), or smart meters that offer advanced capabilities in the form of two-way communication between the meters and companies, but also create new vulnerabilities; security of wide-area smart grid measurement systems; detection of hardware Trojans (with implications for supply chain security); and security of embedded systems. Research in these areas is an important element in the security of the emerging Smart Grid.



PROJECT PERFORMERS

- University of Illinois at Urbana-Champaign

WEBSITE

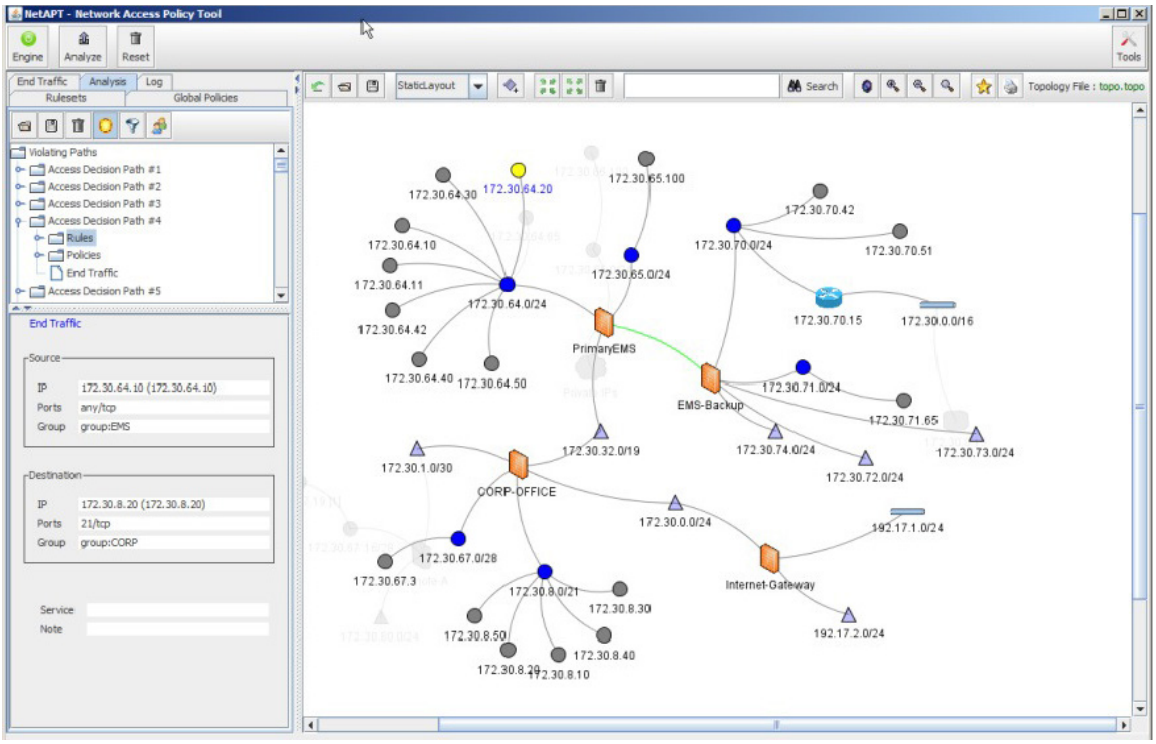
www.tcipg.org

PROGRAM MANAGER

Greg Wigton
Gregory.Wigton@hq.dhs.gov

FY 2012 Highlights

- Autoscopy, an embedded system security tool, was transitioned to Schweitzer Engineering Laboratories, a major supplier and integrator of technologies that is planning to incorporate it into upcoming product lines.
- The Network Access Policy Tool (NetAPT) tool (pictured) was commercialized and the technology licensed to more than 20 North American Electric Reliability Corporation auditors and public utilities. NetAPT will help public utilities identify vulnerabilities in their routing hardware and software, helping them to mitigate unsecure devices.
- Enhancements for the TICP-G testbed were developed, including implementing the Itron AMI testbed and federating the testbed with the DEFT framework, a collaboration to explore cyber-physical research infrastructure.
- TCIP-G research outreach included more than 130 presentations to industry groups, conferences, and individual partners, as well as more than 40 publications in journals and conferences.



FOUNDATIONAL ELEMENTS OF CYBER SYSTEMS

The only long-term solution to the vulnerabilities of today's networking and information technologies is to ensure that future generations of these technologies are designed with security built in from the ground up. The FECS program focuses R&D activities on the characteristics essential to the desired end states of trustworthy cyber systems. A system needs to have sound security requirements, and users need strong assurances that the system meets those requirements. The FECS program will accelerate the transition of safe, secure cybersecurity technologies into commercial products and services. End users of these technologies include first responders, critical infrastructure providers, the banking and finance sector, private industry, and government agencies.

In FY 2012, CSD carried out the FECS program through several projects, six of which had noteworthy accomplishments this year:

- **Cyber Economic Incentives (CEI)** — To understand the value of implementing cybersecurity measures into business operations and to get stakeholders to behave in a way that will improve overall security, CSD is studying the economic factors or conditions and incentive structure for security measures.
- **Enterprise Level Security Metrics and Usability (ELSM&U)** — CSD is leading the development of information security metrics that will finally allow system administrators to measure the progress and comparisons of security between systems. Meaningful metrics have been hard to achieve because of the rapid evolution of IT, as well as the shifting focus of adversarial action.
- **Homeland Open Security Technology (HOST)** — CSD is a driving force behind evaluating and promoting open security methods, models, and technologies and identifying viable and sustainable approaches that support national cybersecurity objectives. Through HOST, CSD led efforts of discovery, collaboration, and development in open-source software and practices that produce a measurable impact.
- **Moving Target Defense (MTD)** — Attackers have exploited the historically static environment in which our systems operate. S&T is taking a game-changing approach by building capabilities that continually shift the attack surface and more resilient hardware that functions effectively under attack.
- **Software Quality Assurance (SQA)** — S&T developed tools, techniques, and environments to analyze software, address the presence of internal flaws and vulnerabilities in software, and improve software security associated with critical infrastructure (energy, transportation, telecommunications, banking and finance, and other infrastructure types).
- **Tailored Trustworthy Spaces (TTS)** — S&T is addressing the challenge of today's subsystems that cannot maintain or verify their security conditions with a high degree of confidence, thus inhibiting a robust trust environment.

Cyber Economic Incentives

The state of cybersecurity is now, and in the future will continue to be, dependent upon multiple economic factors or conditions. For example, it has been difficult for private firms, let alone the government, to determine the amount actually invested in various cybersecurity measures and the ultimate value their cyber infrastructures and business operations have derived from such measures. In other words, the comprehensive data necessary for measuring return on investment are lacking. Furthermore, models for estimating the value of such investments do not exist. Gaining an understanding of the incentive structure for security measures is key to convincing stakeholders to behave in a way that will improve overall security.

Under the CEI project, CSD funds two distinct but complementary research areas. One is focused on reducing the challenges to making cybersecurity investments in the private sector. This effort is developing a cost-benefit framework and testable hypotheses based on that framework. Hypotheses testing, which will be conducted on critical infrastructure sector organizations, will validate or refute the proposed relationships between externalities and under investment in cybersecurity. Additional models will be developed to inform investment decisions and support policy development. The other area is focused on understanding and disrupting the economics of cybercrime by discovering and testing the use of various disincentives for engaging in cybercrime. The effort develops data interchange formats, identifies cybercrime supply chains employed by organized crime elements, and models attacker behavior psychology. The overall objective of this research area is to understand how cyber criminals operate and where intervention mechanisms would have the most impact.

The CEI project began late in FY 2012. In FY 2013, the project plans to deliver the following products:

- At least four cybersecurity investment case studies that will help validate (or refute) hypotheses on how incentives are being or could be applied and their likelihood of success in reducing losses due to cyber attacks;
- A detailed plan for a comprehensive cybersecurity investment survey that will be distributed to approximately 300 organizations from a variety of industry sectors; and
- Preliminary catalogs of cybercrime indicators and cyber criminal supply chains, data interchange formats and standards for sharing cybercrime information, and general models of cyber attack behavior. These interchange formats will help ensure that anonymized data cannot be re-identified, an important feature for conducting research.

PROJECT PERFORMERS

- Carnegie Mellon University
- University of Maryland

PROGRAM MANAGER

Joseph Kielman, Ph.D.
joseph.kielman@hq.dhs.gov

Enterprise Level Security Metrics and Usability

Defining effective information security metrics has proven difficult, even though there is general agreement that such metrics could measure progress in security measures and, at a minimum, make rough comparisons of security between systems. Metrics underlie and quantify progress in many other system security areas, such as physical security. The lack of sound and practical information security metrics is severely hampering progress both in researching and engineering secure systems. However, general community consensus regarding what types of metrics are useful and what exactly should be measured, has been hard to achieve. This is due in part to the rapid evolution of IT, as well as the shifting focus of adversarial action.

Enterprise level security metrics address the security posture of an organization. More specifically, enterprise level security metrics address the question of whether an organization's security mechanisms are enough to defend against or respond to security threats. Experts, such as system administrators, and non-technical users alike must be able to use an organization's system while still maintaining security.

This project will develop security metrics and the supporting tools and techniques to make them practical and useful as decision aids. This will allow the user to measure security while achieving usability and to make informed decisions based on threat and costs to the organization.

The ELSM&U project began in late FY 2012. In FY 2013, CSD plans to:

- ***Produce a suite of metrics tools for measuring enterprise network security risk that can be integrated into the Cauldron attack graphing tool.*** These tools will leverage data sources that are commonly deployed within enterprise networks, such as vulnerability scanners and firewall configuration files. These tools will be inexpensive to compute, unambiguous, and repeatable and will track and visualize multiple security metrics over time. This will support trend analysis, help direct resources for vulnerability remediation, and monitor enterprise security state as network configurations evolve and new vulnerabilities and threats emerge.
- ***Install the enhanced NetAPT tool in electric utility enterprise and industrial control networks and train industry users how to operate the tool.*** The current NetAPT tool analyzes a utility's control network to determine all possible connections to all possible destinations. It provides output of this analysis (and an ability to annotate it) in a spreadsheet form that is amenable for inclusion in audit documentation. The enhanced NetAPT tool will leverage these features and add more metrics features to make the tool more useful to both utilities and auditors.

PROJECT PERFORMERS

- George Mason University
- IBM
- Indiana University
- University of Houston
- University of Illinois at Urbana-Champaign

PROGRAM MANAGER

Greg Wigton
gregory.wigton@hq.dhs.gov

Homeland Open Security Technology

Open-source software, composed of source code that is available for use, modification, and redistribution, provides many innovative security solutions that are not being leveraged by the government. The shared nature of open source means that improvements made by one agency benefit the larger community, yet government acquisition and security certification can make it challenging to use these solutions. The HOST project focuses on improving awareness of open-source security solutions available to all levels of government, inventorying those that have been successfully deployed, and sponsoring development in areas where security solutions do not currently exist.

HOST is engaging thought leaders from the open-source and open-government communities. An initial group of government users of open-source software, including users from the National Aeronautics and Space Administration, Department of Defense, DHS National Protection and Programs Directorate, Office of theChief Information Officer, and Immigration and Customs Enforcement (ICE), came together to form an Executive Committee for this project. The Executive Committee will identify transition partners for technologies they prioritize for development.

Initial sponsorship focused on developing the first open-source, multithreaded intrusion-detection system, called Suricata, and supporting the Federal Information Processing Standards validation of OpenSSL, an open-source encryption library used in both open-source and commercial software. OpenSSL is one of the most popular encryption libraries and is used in a variety of Web browsers and email applications.

FY 2012 Highlights

- The HOST team cataloged more than 300 open source software relevant to security and government use that will be shared publicly through www.OpenCyberSecurity.org.
- CSD initiated collaborations and investments with key security open-source software communities including the Open Web Application Security Project and the Open Source Digital Forensics Community.
- CSD continued investments and support of Suricata during its transition from research into production applications across the cybersecurity market. This included the piloting of these commercially supported appliances to determine their ability to meet requirements.

PROJECT PERFORMERS

- Georgia Tech Research Institute
- Open Information Security Foundation
- Open Source Software Institute

WEBSITE

www.opencybersecurity.org

PROGRAM MANAGER

Luke Berndt
luke.berndt@hq.dhs.gov

```
var
  X:real;
  Y:real;
  N:integer;
procedure TForm1.Button1C
begin
with Image1.Canvas do
begin
    X := 0;
    while X<500 Do
    begin
    X:=X+0.1 ;
    Y:=200-100*(Sin(X
    Pixels[Round(X),R
    end;
    MoveTo(0,200); L
    MoveTo(250,0); L
    N:=0;                //W
    while N<500 do
    begin
    N:=N+100;
    MoveTo (N, 190)
    TextOut (N,200,
    end;

    N:=0;
    whil
```

Moving Target Defense

In the current environment, our systems are built to operate in a relatively static configuration on presumably trusted hardware. This approach is a legacy of a time when malicious exploitation of system vulnerabilities was not a concern, and thus IT system design has focused on simplicity. However, it is now clear that static systems present a substantial advantage to attackers. Attackers can observe the operation of key IT systems over long periods of time and plan attacks at their leisure. Today's hardware still only provides limited support for security and capabilities that do exist are often not fully utilized by software. Therefore, a game-changing approach to building capabilities that continually shift the attack surface is necessary, and hardware must be designed to exhibit greater functional resilience while under attack.

In FY 2012, CSD began four efforts within the MTD project. Two of these efforts focus on shifting the attack surface, and the other two focus on hardware-enabled trust.

The first effort looks at the design of secure hardware caches that do not leak sensitive information through cache-based, side-channel attacks. This effort plans to develop a Newcache hardware solution that is software- and performance-transparent and that can be integrated into the current software and hardware ecosystems. The Newcache architecture will apply MTD to cache mapping to thwart the attacker while also providing an improvement in performance over standard caches.

Another effort in MTD will result in the development of a network edge hardware device that will change IP addresses across multiple, separate enclaves at a sub-second frequency. The goal is to develop a rack-mountable network appliance that provides standard configuration interfaces and can support enterprise throughput requirements. Furthermore, the appliance will interoperate with legacy systems and have management interfaces so that it is easily usable by existing systems administrators with minimal training.

The third effort is working to develop Hardware Enabled Zero-Day Protection (HEZDP)—a comprehensive security solution utilizing Unified Extensible Firmware Interface for user space protection. HEZDP utilizes a full-spectrum approach across multiple layers with hardware being the cornerstone for thwarting attacks. The HEZDP software starts at the firmware level and is applied in the operating system kernel to provide comprehensive resilience against all forms of malicious activity.

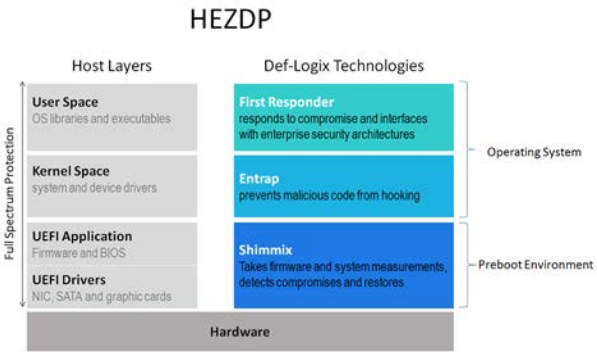


Figure 2: Multiple layers of host stack and HEZDP protection

The fourth effort is working to design and demonstrate a new hardware-enabled architecture that can provide a foundation for comprehensive malware defenses and end-to-end trust. This foundation is scalable from low-end embedded systems, like sensors and actuators used in industrial control systems, to handheld devices like smart phones and tablets, to large servers in enterprise and cloud computing data centers.

CSD also awarded five Small Business Innovation Research (SBIR) efforts in the area of MTD. Each of these efforts offers unique approaches to addressing this challenge. They include:

- An MTD Framework that efficiently manages the continuous deployment of randomized software components to change a system's attack surface over time and evade threats.

- An IP Hopping system that will use available network data and hopping algorithms to allow for constant IP address changing of both source and destination IP addresses. This IP Hopper will also utilize IPv6, which will allow up to 340 undecillion (3.4 x 10^38) different IP addresses to be utilized.
- A Multi-layer, Ever-changing, Self-defense Service that will hinder an attacker's ability to exploit a target system by removing the static network and system attributes that simplify reconnaissance, as well as continuously refresh the target system to a new virtual instance with a known, trusted state.
- A binary randomization tool called Emerald that will employ advanced binary analysis to understand a binary program's code paths and data structures, which will then allow it to comprehensively randomize the binary program at multiple levels.

The magnitude of the problem arising from the current state of our static systems and networks requires a varied and thorough approach across many technical areas. The diversity of the proposed solutions illustrates the depth of the challenge. In addition to the technical challenges, it requires a shift in mindset away from the way networks have typically been structured over the past few decades.

The MTD project began in late FY 2012. In FY 2013, CSD plans to:

- Deliver packaged Newcache test chip samples.
- Develop a behavior-level simulation model of Newcache.
- Deliver three high-performance network appliances, user guides, and a user interface.
- Complete Phase I SBIR efforts and select Phase II performers.
- Deliver a "fieldable" release of HEZDP that will have all the components of HEZDP fully integrated.
- Develop an end-to-end architecture, demonstrate it using a combination of simulated hardware and system prototypes, test its resilience against various attacks, and explore its commercialization in server processors and embedded systems.

PROJECT PERFORMERS

- Charles River Analytics
- Cybernet Systems Corporation
- Def-Logix
- Endeavor Systems
- Ensighta Security, Inc.
- IBM T.J. Watson Research Center
- Northrop Grumman Information Systems
- Princeton University
- SCIT Labs, Inc.

PROGRAM MANAGER

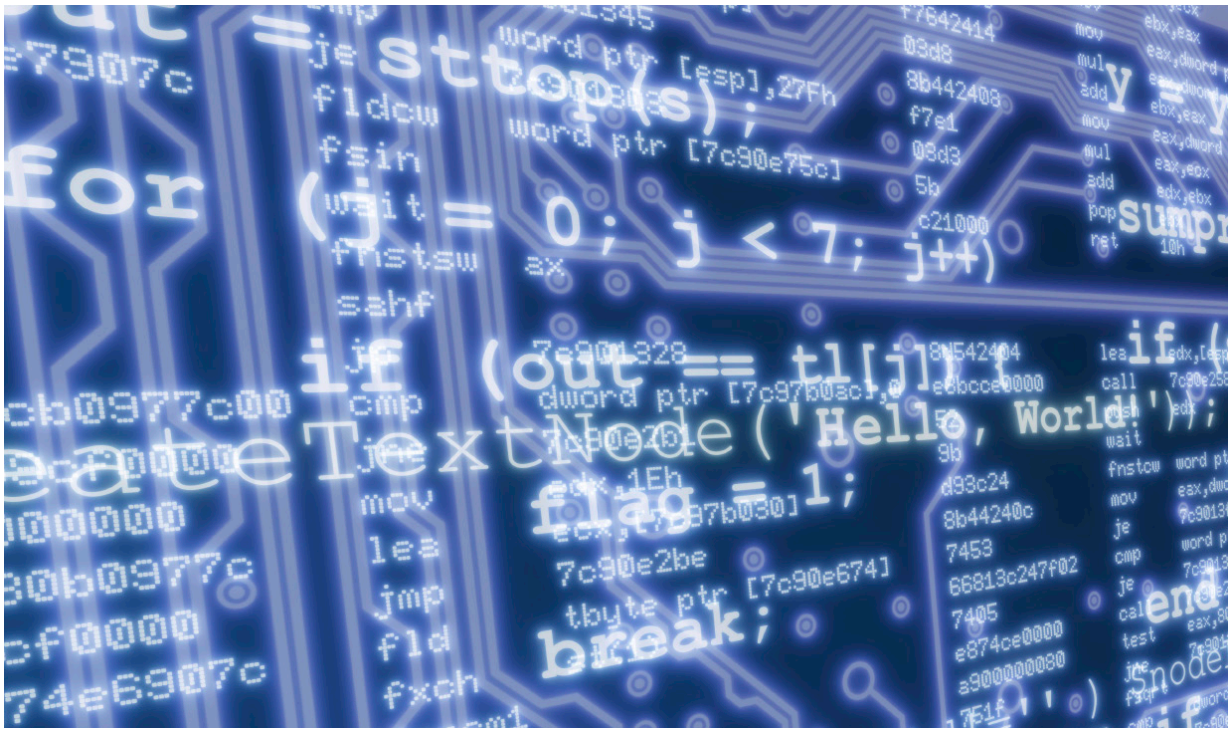
Edward Rhyne
edward.rhyne@hq.dhs.gov

Software Quality Assurance

Our nation's critical infrastructure, businesses, and services are extensively and increasingly controlled and enabled by software. Vulnerabilities in that software put our nation's critical resources at risk. Software size and complexity introduces risks and impacts the overall quality of software. The work that will be performed in this project will help improve how software systems are designed, developed, and maintained through innovative R&D in SQA tools and techniques for software analysis and testing.

In FY 2012, the SQA project initiated three new efforts to provide solutions to improve the quality and reliability of software used in the nation's critical infrastructure. These efforts will:

- Improve existing capabilities over state-of-the-art tools and provide new techniques and capabilities in testing and evaluating software, focusing on precision, accuracy, and reliability. This will involve designing a Tunable Information Flow system that combines the strengths of static analysis, a proof-carrying code framework, and runtime monitoring techniques to protect software systems from security vulnerabilities. This will allow organizations to accept (i.e., trust) software that is designed, developed, and maintained by third parties by leveraging a tunable information policy based on the security requirements of that organization.
- Provide a "Gold Standard" benchmark for SQA tools that measures the effectiveness of tools, mathematically proving software code is safe and free of critical vulnerabilities and weaknesses. This will provide the "Ground Truth" that will establish soundness (high precision) in detecting and reducing "false negatives" found in most state-of-the-art software assurance tools.



- Provide a flexible interface to ingest the results of disparate static analysis tools and normalize and correlate findings to create a single, unified view of weaknesses found by those tools. This interface will be presented as an interactive visualization to express vulnerabilities and risks in a meaningful way. This will enable software developers to prioritize findings and focus on the highest-impact weaknesses identified by tools. The goal is to provide an execution context that can be used to improve the quality and reliability of software.

The SQA tools and techniques developed in this project will be integrated into SWAMP, which is designed to provide a collaborative research environment where software developers and researchers can exchange ideas and test their tools.

These SQA efforts began in late FY 2012. In FY 2013, CSD plans to:

- Develop prototypes for the underlying theory for the Information Flow Analysis Compiler tool, a prototype for the underlying theory and design for a proof checking tool against a tunable consumer security policy, and a prototype for the underlying theory and design for runtime monitoring that will provide feedback of runtime monitoring results to the Information Flow Analysis Compiler and proof checking tools.
- Develop a precise mathematical definition and provide analysis capabilities for identifying targeted weaknesses within software code locations, implement and improve the precision and scalability of the CodeHawk tool, and establish a "Ground Truth" to benchmark and measure the effectiveness of SQA tools. CodeHawk is a high-precision static analysis tool that uses an abstract interpretation framework to provide "Ground Truth" for key vulnerabilities associated with C source code.
- Review a list of dynamic tracing tools and develop integration requirements for each. This will facilitate the ease of integration into key technologies such as CodeDx. CodeDx is a technology developed as part of an SBIR Phase II effort that is designed to normalize and correlate outputs from disparate static analysis tools.
- Develop use cases for static source code analysis by introducing runtime trace data to prioritize vulnerability findings and better manage data inefficiencies that are a result of unsound and imprecise static analysis tools.

PROJECT PERFORMERS

- Secure Decisions, a Division of Applied Visions, Inc.
- HRL Laboratories
- Kestrel Technology

PROGRAM MANAGER

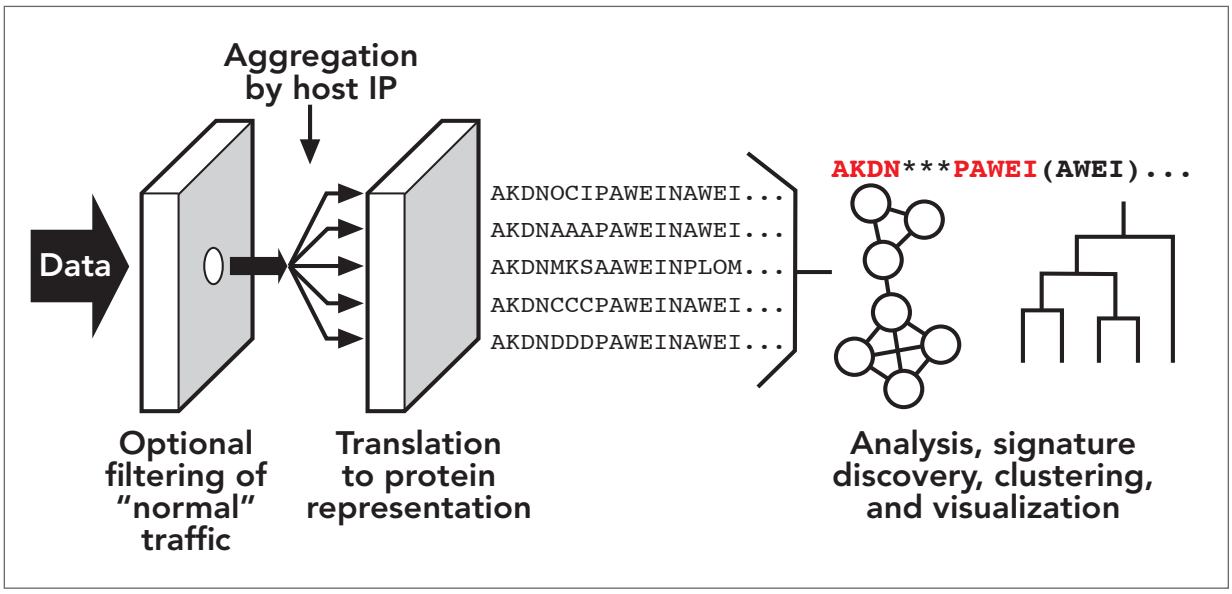
Kevin E. Greene
kevin.greene@hq.dhs.gov

Tailored Trustworthy Spaces

Today's cyberspace is composed of subsystems that cannot maintain or verify their security conditions with a high degree of confidence, thus inhibiting a robust trust environment. CSD has established the TTS project to address the challenge of creating distributed, consistently trusted environments that support both functional and operational, as well as policy requirements. The requirements for this research were derived from the Comprehensive National Cybersecurity Initiative. The National Cyber Leap Year Summit 2009 identified specific ideas around TTS, and these were further codified in the *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*, published by the National Science and Technology Council in December 2011.

Under TTS, CSD funds research in two complementary areas—Digital Provenance and Nature Inspired Cyber Health. Digital Provenance examines data that has originated from different sources and may have been transformed, processed, aggregated, or otherwise manipulated by many entities. For cybersecurity usage, "provenance" refers to having indisputable knowledge of the source and history of digital data. Work in this area includes developing a digital object tracking platform and tools, a command shell interface to fulfill legal and regulatory requirements for evidentiary handling and chain of custody, and an application that provides location provenance for mobile devices.

Nature Inspired Cyber Health relies on biological models, or adapts techniques found useful in biological science, to create secure cyber infrastructures. There are two distinct efforts being funded in this topic area. The first translates behavioral models for insect colonies into algorithms for rapidly detecting previously undetected code or malware in computer system networks. The second applies analytical techniques similar to those used in determining gene or protein sequences to discover anomalous, and potentially malicious, sets of transactions or instructions within networks (pictured below).



The TTS project began in late FY 2012. In FY 2013, CSD plans to deliver the following technologies, demonstrations, or knowledge products:

- A network baseline modeling tool (CLIQUE) to the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC). This modeling tool will allow REN-ISAC to develop a basis for identifying and removing normal traffic sequences from analysis, allowing resources to focus on anomalous sequences.
- A prototype demonstration of the command shell interface for ensuring digital chain of custody. This prototype deployment will allow for user feedback to be incorporated into the agile software development model.
- A data leakage pilot with the Secure Medical Workspace. The Secure Medical Workspace, part of the Carolina Data Warehouse for Health initiative, assesses the degree to which technology will be able to support the dual goals of sharing research information while protecting sensitive patient data.

PROJECT PERFORMERS

- ITT Exelis
- Pacific Northwest National Laboratory
- Rutgers, The State University of New Jersey
- University of Alabama at Birmingham
- University of North Carolina at Chapel Hill

PROGRAM MANAGER

Joseph Kielman, Ph.D.
joseph.kielman@hq.dhs.gov

CYBERSECURITY USER PROTECTION AND EDUCATION

People are users of systems and infrastructures. They may be everyday citizens using cyber systems to perform various tasks, they may be cybersecurity professionals, or they may be cyber criminals conducting malicious activity. The CUPE program focuses R&D activities on improving the security and protection of user online activity, attracting the next generation of cybersecurity warriors, and providing the tools needed for investigating cyber criminal and terrorist activity.

In FY 2012, CSD carried out the CUPE program through three projects:

- **Cyber Security Competitions** — CSD supported cybersecurity competitions, which focus on overcoming the shortage of technically skilled people required to operate and support deployed systems, as well as on educating young individuals who can design secure systems and create sophisticated tools needed to prevent malicious acts. CSD supported competitions including the National Collegiate Cyber Defense Competition (NCCDC) and the U.S. Cyber Challenge (USCC), both conducted in support of the National Initiative for Cybersecurity Education.
- **Cyber Security Forensics** — CSD worked to develop new cyber forensic analysis tools and investigative techniques for law enforcement officers and forensic examiners to address the full range of cyber-related crimes.
- **Identity Management and Data Privacy Technologies** — CSD made strides toward enhancing the security of information-sharing environments and the protection of users by improving authentication for persons, hardware devices, and software applications across all levels of government. The Identity Management and Data Privacy Technologies project addresses the inadequate amount of security, trust, usability, policies, and procedures that currently exists to secure interactions among stakeholders who wish to ensure that their identity is properly protected and managed.

Cyber Security Competitions

The Cyber Security Competitions project helps fulfill the challenge presented in Priority III of the National Strategy to Secure Cyberspace to "foster adequate training and education programs to support the nation's cybersecurity needs." Cybersecurity competitions focus on the overcoming the shortage of technically skilled people required to operate and support systems already deployed but also on educating young individuals who can design secure systems and create sophisticated tools needed to prevent malicious acts.

CSD provided funding to support the continued development and execution of the Collegiate Cyber Defense program (CCDC) and USCC. In FY 2012, more than 1,500 students from 131 colleges and universities participated in CCDC events. In the 2012 CCDC season, competition organizers worked with DHS to integrate other CSD-supported efforts and technologies, such as DNSSEC, into CCDC events. Integrating other research projects provides additional testing opportunities for the technologies and exposes students to advanced technologies and research efforts. Traffic logs from the 2012 NCCDC were provided to CSD for feedback into other CSD-supported research efforts and technologies. This additional data will help to improve technologies under development.

Funding from CSD also helped to support the development of training materials for teams participating in CyberPatriot, the largest high-school-level cyber defense competition. These materials were used by more than 1,000 teams and more than 5,000 students nationally and internationally. Twenty-five states and more than 1,000 students participated in the USCC CyberFoundations competitions in FY 2012. CyberPatriot also conducted four cyber camps with more than 200 students during the summer of 2012, continuing their effort of the 2011 camps. Each camp featured four days of intense instruction and culminated in a Capture the Flag competition.

FY 2012 Highlights

- 131 schools participated in CCDC events in 2012, making it the largest collegiate cyber defense competition program in the nation.
- USCC increased the number of Cyber Quests competitions in 2012, resulting in participation from more than 1,000 students and professionals over the course of three unique competitions.
- 94 scholarships were provided for continuing education and participation at the USCC summer camps.
- USCC established an initial virtual community: **http://www.cybercompex.org**

PROJECT PERFORMERS

- National Board of Information Security Examiners (USCC)
- University of Texas at San Antonio (CCDC)

WEBSITES

https://www.nbise.org/uscc/Cached
http://www.nationalccdc.org/

PROGRAM MANAGER

Edward Rhyne
edward.rhyne@hq.dhs.gov

Cyber Security Forensics

Digital evidence is frequently present at crime scenes and the forensic investigation of devices such as computers, cell phones, and global positioning system (GPS) devices is increasingly important to law enforcement. Officers and forensic examiners face a constant challenge to stay ahead of the latest technologies as their roles become more significant in criminal and terrorist investigations. In response to this challenge, CSD, working with DHS components—Customs and Border Protection, Federal Law Enforcement Training Center, ICE, and the U.S. Secret Service (USSS) — and other federal, state, and municipal law enforcement agencies, initiated the Cyber Security Forensics project in 2009.

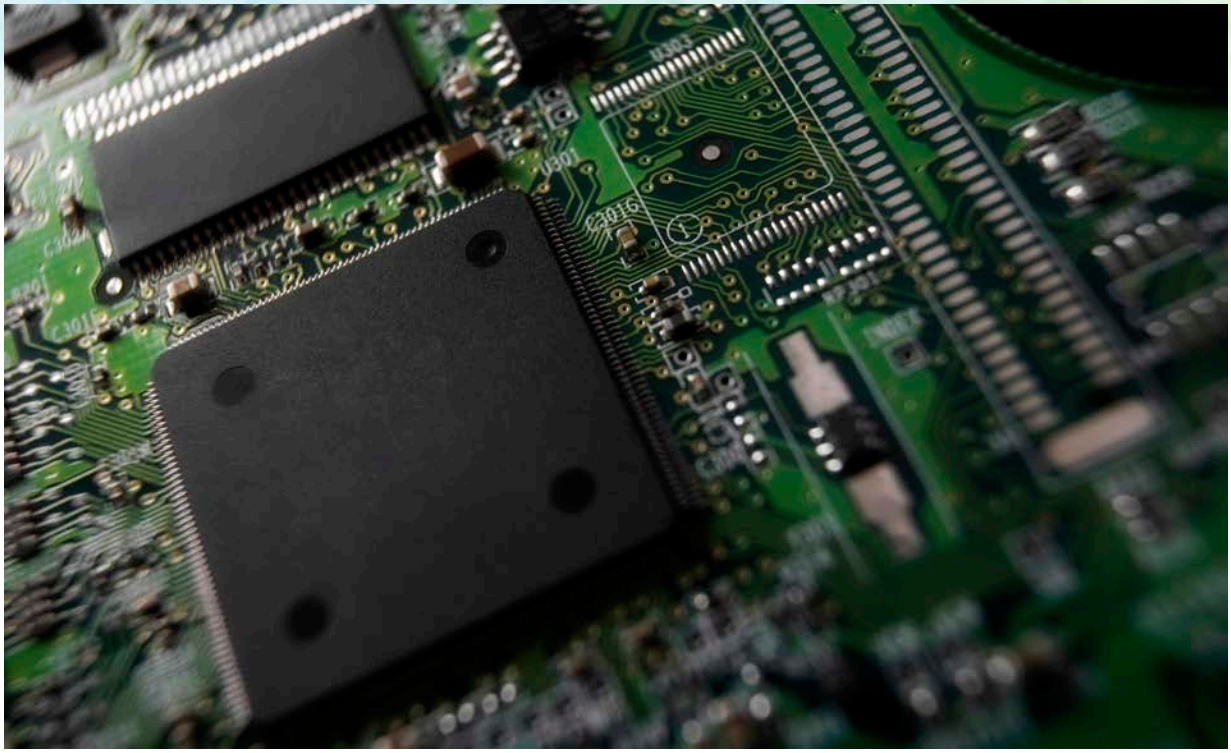
The Cyber Security Forensics project is developing new cyber forensic analysis tools and investigative techniques for law enforcement officers and forensic examiners to address the full range of cyber-related crimes. Additionally, the CSD-sponsored Cyber Forensics Working Group (CFWG) meets semiannually to discuss new requirements and ongoing work. Participation in the working group is open to all federal, state, and local law enforcement agencies.

A particularly important subset of cyber forensics, identified as a result of discussions held during CFWG meetings, is the analysis of portable media devices such as USB drives, iPods, and cell phones. The small size and versatility of portable media devices make them useful tools in the conduct of criminal and terrorist activity. Law enforcement officers require tools that can recover system files, operating system information, applications, deleted files, and unallocated space from portable digital media storage devices.

During FY 2012, the Cyber Security Forensics project funded several efforts to develop portable media examination tools. A GPS device forensic tool R&D effort concluded at the end of the year and CSD will be funding an expanded pilot training and licenses of the new technology for law enforcement in FY 2013. The project also began an effort to create a cell phone forensics tool for law enforcement investigators to forensically image NAND flash memory chips. This project will provide an innovative new solution to the problem of imaging the non-volatile rewritable memory chips found in phones and give law enforcement a less invasive and time-consuming method for mobile phone forensics.

The project also started an effort in FY 2012 focused on the development of gaming system forensic tools for law enforcement to utilize in warranted investigations. Today's typical gaming systems have processing, multimedia, and networking capabilities rivaling personal computers. Beyond standard gaming functions, wireless capabilities enable users to interact and communicate with other players, browse and purchase items over the Internet, and stream videos onto their systems. Use in criminal activity has led to the seizure of gaming systems by U.S. law enforcement agencies during court-authorized searches.

Another area of focus for the Cyber Security Forensics project is research on solutions to mitigate insider threats to an organization. Work in this area also focuses on the collection of actionable counter-intelligence and legally acceptable evidence for law enforcement. One effort concluded with the publication of *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector* by the CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute. The report provides a greater understanding of the behavioral, technical, and organizational factors that lead to insider threat attacks. The report's results and recommendations will provide law enforcement and the private sector with ways to lessen or prevent insider attacks. Additionally, a new insider threat effort started in FY 2012 focuses on the detection of threatening insiders utilizing lightweight media forensics to analyze storage profiles of users and identify anomalies.



FY 2012 Highlights

- The First Responder Cyber Field Kit R&D project concluded and the project outcomes were presented at the 2012 Crimes Against Children Conference.
- CSD funded initial research into solid state drive forensic tools.
- The CyberForensics Electronic Technology ClearingHouse went operational and is a resource for encouraging information sharing across agencies.

PROJECT PERFORMERS

- ADF Solutions, Inc.
- Berla Corporation
- Carnegie Mellon University
- ITT Exelis
- Naval Postgraduate School
- NIST
- University of Wisconsin
- viaForensics

WEBSITE

http://www.cyberfetch.org

PROGRAM MANAGER

Megan Mahle
megan.mahle@hq.dhs.gov

Identity Management and Data Privacy Technologies

The White House is committed to building a reliable, resilient, trustworthy digital infrastructure for the future. The President and Congress directed DHS to prevent and protect the nation against terrorist attacks and to respond to both man-made and natural disasters. Agencies and organizations are experiencing a lack of processes and tools to share and coordinate information effectively, not because of inadequate amounts of data and information sharing environments, but because of an inadequate amount of security, trust, usable tools, policies, and procedures. In order to achieve its goals, the Identity Management and Data Privacy Technologies projects are addressing the needs of the Homeland Security Enterprise (HSE).

Identity and Access Management (IdAM)—a key component of cybersecurity—has become more complex, dealing with all facets of storing; verifying data about individuals; and controlling their access to places, facilities, money, materials, and computer systems. IdAM has become one of the most vital and fastest-growing concerns of system owners and chief information officers The risk of cyber attacks on systems guarding sensitive information increases as more agencies and private companies engage in complex, federated digital world.

CSD partners with federal, state, local, public, private sector organizations to solve these problems. In 2007, CSD established the Identity Management (IdM) Testbed to pursue research, development, test, and evaluation (RDT&E) focused on providing solutions to manage digital identities and implementing access control strategies for the HSE, which includes federal, state, local, and private sectors. As the only federal agency funding IdAM R&D, CSD uses the IdM Testbed to participate in key proof-of-concept pilots. Developing and leveraging open standards, specifications, and current and new technologies, the Testbed seeks to identify access control solutions emphasizing cost efficiency, interoperability, and enhanced security and privacy for the HSE. Because of the growing need for access control to cyber and physical systems, the IdAM project has several research projects focusing on homeland security missions:

Federal

CSD is providing secure and cost-effective solutions for all federal agencies by supporting the research needs of the Identity, Credential, and Access Management Subcommittee (ICAMSC), under the Federal Chief Information Officer. By leveraging the CSD research efforts conducted in the IdAM Testbed, the ICAMSC is able to transition the research into operational requirements, such as the Backend Attribute Exchange profile found on http://www.idmanagement.gov.

State, Local, and Public

STATE AND LOCAL PARTICIPANTS

- All Hazards Consortium
- Colorado
- District of Columbia
- Maryland
- Chester County, PA
- Hawaii
- Missouri
- Nevada
- Pittsburgh, PA
- Pennsylvania
- Rhode Island
- Southwest Texas
- Texas
- Virginia
- West Virginia

In a partnership between S&T and the Federal Emergency Management Agency (FEMA), CSD established the Personal Identity Verification-Interoperable (PIV-I)/First Responder Authentication Credential (FRAC) Technology Transition Working Group (TTWG). The PIV-I/FRAC TTWG consists of state and local agencies as well as fusion centers who seek to increase the adoption of high-assurance, interoperable credentialing standards across jurisdictional lines for both physical and logical access control. The group meets quarterly to share lessons learned and success stories, provide policy makers with a unified emergency manager perspective, and identify technology and capability

gaps where CSD provides RDT&E support. CSD is currently laying the groundwork for a pilot, to be finalized in FY 2013, demonstrating the ability for a standards-based transmission of local jurisdiction attributes to be coordinated with the FEMA emergency responder attribute repository in an emergency operation.

Private Sector

CSD is supporting an effort with the Financial Services Sector Coordinating Council (FSSCC) to address identity theft and fraud to protect citizens and prevent financial loss by enhancing the resilience, security, integrity, and usability of financial services. The effort requires policy evaluation and technical development of architectural approaches and processes for confirming identity credentials presented when opening a bank account. This supports the National Strategy for Trusted Identities in Cyberspace (NSTIC) goal for interoperable identity solutions. This work was conducted under the White-House-facilitated Memorandum of Understanding between S&T, NIST and the FSSCC on cybersecurity R&D activities for protecting the physical and electronic infrastructures.

FY 2012 Highlights

- CSD developed the open-standard **Verification of Identity Credential Service** gateway for the finance sector requirement to improve the identity proofing process and reduce the risk of identity fraud for financial services.
- CSD developed an interoperable communications standard and cost-effective solution to improve the identity verification process of emergency response officials' entitlements, permission, and certifications for making access decisions at incident scenes (e.g., Hurricane Sandy). CSD is in the process of transitioning an end-to-end solution to FEMA and state and local agencies to verify and authenticate emergency responder smart card credentials using smart phone devices.
- CSD is transitioning open-source middleware to industry to allow commercially available physical access control systems to interoperate with cyber systems for a more secure, cost-efficient, effective access management system. This capability is sought by multiple private companies and federal facilities.
- CSD developed a proof-of-concept demonstration of a policy reasoning engine to analyze privacy policies to ensure they comply with applicable laws and regulations. The tool is a critical enabler of secure information sharing environments, fostering confidence that personal information is being used appropriately and minimizing privacy breaches.

PROJECT PERFORMERS

- American Association of Motor Vehicle Administrators
- The Johns Hopkins University, Applied Physics Lab
- Massachusetts Institute of Technology, Computer Science and Artificial Intelligence Lab
- MITRE – Homeland Security Systems Engineering and Development Institute
- Queralt Inc.

WEBSITES

https://www.dhs.gov/sites/default/files/publications/CSD-Moving-Towards-Interoperability.pdf

https://www.dhs.gov/csd-idm

www.ahcusa.org/PIV-I%20TTWG.html

PROGRAM MANAGER

Karyn Higa-Smith

karyn.higa-smith@dhs.gov

CYBERSECURITY TECHNOLOGY EVALUATION AND TRANSITION

To ensure the effective deployment and operational use of new cybersecurity innovations, the "valley of death" chasm must be bridged by technology transition through cooperative efforts and investments by both the research and acquisition communities. The CTET program conducts a coordinated process of assessments, evaluations, and operational experiments and pilots in order to transition the fruits of research into practice.

It is critical to assess and evaluate cybersecurity technologies—whether developed within or outside of CSD—prior to operationally deploying the technologies within the HSE. This includes Red Team evaluations to identify vulnerabilities and weaknesses, as well as operational assessments. Experience shows that transition plans developed and applied early in the life cycle of the research program, if accompanied by probable transition paths for the research product, are effective in achieving successful transfer from research to application and use. These transition paths are affected by the nature of the technology, the intended end user, participants in the research program, and other external circumstances.

In FY 2012, CSD carried out the CTET program's activities through the following projects:

- **Cybersecurity Experiments and Pilots (E&P)** — Through experiments and pilots, CSD developed cybersecurity technologies that were tested and evaluated in operational environments so that solutions could move from the lab to real life, securing the networks of users who need them.
- **Transition to Practice (TTP)** — As a result of CSD's successful track record in transitioning products, CSD was tasked to lead the acceleration of cybersecurity technologies into widespread deployment and use via the marketplace. By targeting technologies that are most likely to successfully transition to the commercial market within two years, CSD will have a notable impact on the cybersecurity of our nation's networks or systems.

Cybersecurity Experiments and Pilots

Technology transfer from the lab to the marketplace is a vital and unique aspect of CSD's R&D efforts. The DHS Chief Information Officer, Federal Law Enforcement Training Center, DHS Office of Cybersecurity and Communications, and other operational components need experimental deployment opportunities to investigate operational capabilities of new technologies. The Cybersecurity E&P project provides a platform for experimentation, testing, evaluation, and operational deployment to facilitate technology transfer. Deploying CSD-developed technologies allows operational components to understand cutting-edge capabilities.

The first step is to identify mature technologies that were developed by CSD and are ready for experimentation, piloting, or deployment in an operational environment. Once a list of technologies is identified, CSD meets with customers and operational components to determine which technologies could be deployed in their operational networks. The goal is to place CSD-funded technologies into the network environments of our customers and partners to enhance their security posture and receive feedback on the products. A successful deployment will lead to the adoption of the technology by the customer and full deployment.

In FY 2013, the E&P project plans to pilot the following products:

- ***Open-source technology developed under the CSD HOST project.*** The pilot testing of the nPulse network system will allow for the detection of malicious behavior on the ICE network and for the recording and examination of the communication to better determine the source and intent of the activity.
- ***Network visualization tool developed under CSD BAA 07-09.*** The VIAssist technology will be piloted by the Library of Congress. VIAssist is a CSD-funded technology that helps analyze network traffic and security event data by providing scalable, visual representations of cyber data.

CSD will identify two to three additional CSD-funded technologies in FY 2013 and work with customers to plan a pilot or experiment or to transition the technology into their infrastructure.

PROJECT PERFORMERS

- Secure Decisions, a Division of Applied Visions, Inc.

PROGRAM MANAGER

Greg Wigton
gregory.wigton@dhs.gov

Transition to Practice

The technology "valley of death" is a well-known concept in the R&D community. The term succinctly describes the historically difficult task of transitioning technology out of the research lab and into the commercial marketplace. The purpose of the TTP project is to build a bridge over the "valley of death."

In 2011, the Networking and Information Technology Research and Development (NITRD) Program of the White House named ways the federal government can rapidly improve the security of the nation's cyber infrastructure. From that list, one of the NITRD's top priorities is to accelerate the transition of cybersecurity research into widespread deployment and use via the marketplace. As one of the agencies designated to address this priority, CSD established the TTP project. TTP builds on CSD's previous successes in transitioning cybersecurity technology into commercially available products.

In accordance with NITRD's recommendations for accelerating technology transition, TTP's goals are to: (1) identify mature technologies that address an existing or imminent cybersecurity gap in public or private systems that impact national security; (2) identify and fund necessary improvements identified during pilot programs and test and evaluation activities; and (3) introduce cybersecurity technology throughout the entire HSE through partnerships and commercialization.

TTP is targeting technologies that are most likely to successfully transition to the commercial market within two years and that will have a notable impact on the cybersecurity of our nation's networks or systems. This is an ambitious endeavor with enormous potential for positive impact. Additionally, TTP will provide a connection point for cybersecurity researchers, the federal government, and the private sector and ensure technology transitions from the research lab to the HSE.

FY 2012 Highlights

In FY 2012, technology foraging efforts were focused on federally funded research conducted at the DOE National Laboratories. Technology foraging discovers, adapts, and leverages technology solutions developed by other governmental and private-sector entities to address risks to our security. In subsequent years, foraging activities will expand to Department of Defense research centers and academic institutions.

- CSD reviewed 30 federally funded cybersecurity technologies at eight DOE National Laboratories and selected eight promising technologies to transition.
- CSD initiated partnerships with numerous federal agencies, federal R&D organizations, critical infrastructure operators, and the private sector.

PROJECT PERFORMERS

- Sandia National Laboratories

R&D Partners

- Argonne National Laboratory
- Lawrence Berkeley National Laboratory
- Lawrence Livermore National Laboratory
- Los Alamos National Laboratory
- Oak Ridge National Laboratory
- Pacific Northwest National Laboratory
- Sandia National Laboratories

WEBSITES

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

http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

http://www.whitehouse.gov/the-press-office/2011/10/28/presidential-memorandum-accelerating-technology-transfer-and-commerciali

http://www.nitrd.gov/fileupload/files/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

PROGRAM MANAGER

Michael Pozmantier

michael.pozmantier@hq.dhs.gov

LOOKING AHEAD TO FY 2013

S&T is an integral player in DHS's focus on safeguarding and securing cyberspace to ensure that the nation is prepared for the cyber threats and challenges of tomorrow.

Looking into FY2013, CSD will be collaborating with several international partners. There is international interest in several major CSD project areas including Cybersecurity User Protection & Education (CUPE), Foundational Elements of Cyber Systems, Research Infrastructure to Support Cybersecurity (RISC), and Trustworthy Cyber Infrastructure (TCI). Based on international interest, CSD will be collaborating to create technical annexes (TAs) to project arrangements (PAs) with Australia, Canada, The Netherlands, Sweden, and The United Kingdom.

Presently, it is anticipated that there will be TAs covering collaboration with the following projects: Internet Measurement and Attack Modeling; the Research Data Repository; Cyber Economic Incentives; Enterprise Level Security Metrics and Usability; Leap Ahead Technologies; Moving Target Defense; Software Quality Assurance; Tailored Trustworthy Spaces; Cyber Security Forensics; and Insider Threat. In all, it is anticipated that CSD's international partners will provide more than $1.3 million toward CSD initiatives and participate in project management, technology related collaboration and the joint sharing of intellectual property.

Furthermore, as discussed earlier, CSD launched numerous new efforts during FY 2012 that spawned activities that took root and grew in FY 2013 and were noted in this report. Beyond those described above, CSD's key R&D activities for FY 2013 include:

Research Infrastructure to Support Cybersecurity

- Collaboration with the Government of Japan to share cybersecurity internet data available in the Research Data Repository.

Trustworthy Cyber Infrastructure

- Transition Symbiote software to a commercial vendor. Symbiote is a software product that protects embedded devices at the kernel level, providing much stronger security than what's found in the current state-of-the-art.
- Deploy an AMI monitoring solution in a test network with more than 40,000 meters.

Cybersecurity User Protection and Education

- Research forensic solutions for law enforcement in the new area of solid-state storage.

Cybersecurity Technology Evaluation and Transition

- Test and evaluate selected cybersecurity technologies and develop partnerships with private industry for commercialization and technology piloting activities.

Performer Index

PROJECT	PERFORMER	ROLE	PRIME CONTACT INFORMATION
Experimental Research Testbed	University of Southern California - Information Sciences Institute (USC-ISI)	Testbed Development and Operation	Terry Benzel tbenzel@isi.edu
Experimental Research Testbed	University of California - Berkeley	Testbed Development and Operation	
Experimental Research Testbed	Pacific Northwest National Laboratory (PNNL)	Process Control System Integration	
Experimental Research Testbed	University of Illinois at Urbana-Champaign (UIUC)	Process Control System Integration	
Research Data Repository	Packet Clearing House (PCH)	Data Host and Dat Provider	Bill Woodcock woody@pch.net
Research Data Repository	University of Southern California (USC)	Data Host and Dat Provider	John Heideman johnh@isi.edu
Research Data Repository	University of California - San Diego (UCSD)	Data Host and Dat Provider	Kimberly (“kc”) Claffy kc@sdsc.edu
Research Data Repository	Research Triangle Institute (RTI)	Coordination Center Operations	Charlotte Scheper cscheper@rti.org
Research Data Repository	University of Michigan	Data Host and Dat Provider	Michael Bailey mibailey@eecs.umich.edu
Research Data Repository	Global Cyber Risk, LLC	Legal Famework and Privacy Support	Jody Westby westby@mindspring.com
Research Data Repository	Merit Network, Inc.	Data Host and Dat Provider	
Research Data Repository	Georgia Tech Research Corporation	Data Provider	
Research Data Repository	University of Wisconsin	Data Provider	
Software Assurance Marketplace (SWAMP)	Morgridge Institute for Research	Lead Developer	Miron Livny miron@cs.wisc.edu
Secure Protocols - DNSSEC	Shinkuro, Inc.	Domain Name System Security (DNSSEC) Protocol Development	Steve Crocker Steve@shinkuro.com
Secure Protocols - DNSSEC	Sparta, Inc., a Parsons Company	Ubiquitous Deployment of Domain Name System Security	Russ Mundy Russ.Mundy@sparta.com
Secure Protocols - DNSSEC	National Institute of Standards and Technology	Border Gateway Protocol (BGP)	Douglas Montgomery DougM@nist.gov
Secure Protocols - SPRI	Sparta, Inc., a Parsons Company	Standards Development & System Prototyping	Sandra Murphy Sandra.Murphy@sparta.com
Secure Protocols - SPRI	Raytheon BBN Technologies	Standards Development & System Prototyping	
Internet Measurement and Attack Modeling	Raytheon/BBN	Real-time Protocol Shepherds (RePS)	Ronald Watro, PhD. Rwatro@bbn.com
Internet Measurement and Attack Modeling	Naval Postgraduate School	Methodology for Assessment of Security Properties	Cynthia Irvine, PhD. Irvine@nps.edu
Internet Measurement and Attack Modeling	Georgia Tech Research Corporation	Comprehensive Understanding of Malicious Overlay Networks	Wenke Lee, PhD. Wenke@cc.gatech.edu
Internet Measurement and Attack Modeling	Oak Ridge National Laboratory	Visually Fusing Contextual Data for Situational Understanding	John Goodall, PhD. Jgoodall@ornl.gov

Internet Measurement and Attack Modeling	Columbia University	Advanced Situation Awareness of High Impact Malware Attacks Against the Internet Routing Infrastructure	Salvatore Stolfo, PhD. Sal@cs.columbia.edu
Internet Measurement and Attack Modeling	University of Southern California	The Retrospective Future in the Internet (Retro-Future)	John Heidemann, PhD. Johnh@isi.edu
Internet Measurement and Attack Modeling	Naval Postgraduate School	High-Frequency Active Internet Topology Mapping	Robert Beverly, PhD. Rbeverly@nps.edu
Internet Measurement and Attack Modeling	University of California at San Diego	Cartographic Capabilities for Critical Cyberinfrastructure	Kimberly Claffy, PhD. Kc@caida.org
Internet Measurement and Attack Modeling	Merit Networks, Inc.	Enabling Operational Use of RPKI via Internet Routing Registries	W. Joseph Adams, PhD. Wjadams@merit.edu
Internet Measurement and Attack Modeling	International Computer Sciences Institute	Netalyzr NG: Monitoring DNS, DNSSEC, and TLS from the Edge	Nicholas Weaver, PhD. Nweaver@icsi.berkeley.edu
Internet Measurement and Attack Modeling	Pacific Northwest National Laboratory	Scalable Modeling of Network Flows for US-CERT	Daniel Best Daniel.best@pnnl.gov
Process Control Systems Security - LOGIIC	SRI International	Project Management	Ulf Lindqvist ulf.lindqvist@sri.com
Process Control Systems Security - TCIPG	University of Illinois at Urbana-Champaign (UIUC)	Project Director	Bill Sanders whs@illinois.edu
Cyber Economic Incentives	Carnegie Mellon University	Understanding and Disrupting the Economics of Cybercrime	Nicolas Christian nicolasc@cmu.edu
Cyber Economic Incentives	University of Maryland	Reducing The Challenges to Making Cybersecurity Investments in the Private Sector	Larry Gordon lgordon@rhsmith.umd.edu
Enterprise Level Security Metrics and Usability	George Mason University	Metrics Suite for Enterprise-Level Attack Graph Analysis	Sushil Jajodia jajodia@gmu.edu
Enterprise Level Security Metrics and Usability	IBM	Usable Multi-Factor Authentication and Risk-Based Authorization	Larry Koved koved@us.ibm.com
Enterprise Level Security Metrics and Usability	Indiana University	CUTS: Coordinating User and Technical Security	Jean Camp ljcamp@indiana.edu
Enterprise Level Security Metrics and Usability	University of Houston	Implicit and Continuous Mobile User Identification/ Authentication Using Smartphone Sensors	Weidong (Larry) Shi larryshi@cs.uh.edu
Enterprise Level Security Metrics and Usability	University of Illinois at Urbana-Champaign (UIUC)	A Tool for Compliance and Depth of Defense Metrics	David Nicol dmnicol@illinois.edu
Homeland Open Security Technologies	Georgia Tech Research Institute (GTRI)	Project Lead	Joshua Davis Joshua.Davis@gtri.gatech.edu
Homeland Open Security Technologies	Open Source Software Institute	Solutions Inventory	
Homeland Open Security Technologies	Open Information Security Foundation	Software Development	
Moving Target Defense	Charles River Analytics	Moving Target Defense Framework (MTDF)	Curt Wu cwu@cra.com

Performer Index

Moving Target Defense	Cybernet Systems	IP Hopper (for Moving Target Defense)	Merrill Squiers msquiers@cybernet.com
Moving Target Defense	Def-Logix	Hardware-Enabled Zero Day Protection (HEZDP)	Paul Rivera privera@def-logix.com
Moving Target Defense	Endeavour Systems	Multi-layer Ever-changing Self-defense Service (MESS)	Will Hickie will.hickie@endeavorsystems.com
Moving Target Defense	Ensighta Security	Emerald: Binary Program Randomization	Dawn Song dawnsong@gmail.com
Moving Target Defense	IBM T.J. Watson Research Center	Hardware Based Malware Defenses and End-to-End Trust	Dimitrios Pendarakis dimitris@us.ibm.com
Moving Target Defense	Northrop Grumman Information Systems	Appliance for Active Repositioning in Cyberspace (AARC)	Jeffrey Foley Jeffrey.l.foley@ngc.com
Moving Target Defense	Princeton University	Using Moving Target Defense for Secure Hardware Design	Ruby Lee rblee@princeton.edu
Moving Target Defense	SCIT Labs	Scalable MTD Based on SCIT Technology	Arun Sood asood@scitlabs.com
Software Quality Assurance	Applied Visions/Secure Decisions	Code Dx	Ken Prole - Ken.Prole@avi.com
Software Quality Assurance	Applied Visions/Secure Decisions	Code Pulse	Hassan Radwan Hassan. Radwan@avi.com
Software Quality Assurance	HRL Laboratories	Tunable Information Flow	Dr. George Kuan gkuan@hrl.com
Software Quality Assurance	Kestrel Technologies	A Gold Standard for Benchmarking C Source Code Static Analysis Tools	Dr. Henny Sipma sipma@kestreltechnology.com
Tailored Trustworthy Spaces	ITT Exelis	Evidentiary Integrity for Incident Response	Rosanne Pelli Rosanne.pelli@exelisinc.com
Tailored Trustworthy Spaces	Pacific Northwest National Laboratory	Nature Inspired Health (LINEBACkER)	Christopher S Oehmen christopher.oehmen@pnnl.gov
Tailored Trustworthy Spaces	Rutgers University	Bio-Inspired Distributed Decision Algorithms for Anomaly Detection	Nina Fefferman feffermn@dimacs.rutgers.edu
Tailored Trustworthy Spaces	University of Alabama at Birmingham	Secure Location Provenance for Mobile Devices	Ragib Hasan ragib@cis.uab.edu
Tailored Trustworthy Spaces	University of North Carolina-Chapel Hill	Efficient Tracking, Logging and Blocking of Accesses to Digital Objects	Fabian Monrose fabian@cs.unc.edu
Cyber Security Competitions	National Board of Information Security Examiners	Highshcool Cyber Security Competitions	Karen Evans KarenEvans@prodigy.net
Cyber Security Competitions	University of Texas - San Antonio (UTSA)	Collegiate Cyber Security Competitions	Greg White Greg.White@utsa.edu
Cyber Security Forensics	ADF Solutions	First Responder Field Kit - Triage Responder	JJ Wallia, CEO/Co-founder info@adfsolutions.com
Cyber Security Forensics	Berla Corporation	GPS Forensic Logical Analysis Tool - Blackthorn3	Ben LeMere blemere@berlacorp.com

Cyber Security Forensics	Carnegie Mellon University	Banking and Finance Sector Insider Threat Study	Randy Trzeciak rft@cert.org
Cyber Security Forensics	Naval Postgraduate School	Gaming Systems Forensics	Simson Garfinkel slgarfin@nps.edu
Cyber Security Forensics	Naval Postgraduate School	Insider Threat	Simson Garfinkel slgarfin@nps.edu
Cyber Security Forensics	Exelis	Law Enforcement Information Portal - CyberFETCH	Adam Hovak adam.hovak@exelisinc.com
Cyber Security Forensics	National Institute of Standards and Technology	National Software Reference Library/Cyber Forensics Tool Testing	Barbara Guttman barbara.guttman@nist.gov cftt@nist.gov nsrl@nist.gov
Cyber Security Forensics	University of Wisconsin	Vulnerability Assessment of Open Source Wireshark	Prof. Barton P. Miller bart@cs.wisc.edu
Cyber Security Forensics	viaForensics	NAND/NOR Chip Forensics	Chee-Young Kim ckim@viaforensics.com
Identity Management and Data Privacy Technologies	Johns Hopkins University - Applied Physics Laboratory	Host the Identitiy Management Testbed; Backend Attribute Exchange	Camille Schumacher Camille.Schumacher@jhuapl.edu Tom Smith tom.smith@jhuapl.edu
Identity Management and Data Privacy Technologies	Queralt	Small Business Innovation Researce effort “Attribute Based Authorization & Visitor Application”	Michael Queralt michaelq@queraltinc.com
Identity Management and Data Privacy Technologies	MITRE SEDI	Privacy Enhancing Technology Engineering and Transition	Stuart Shapiro sshapiro@mitre.org
Identity Management and Data Privacy Technologies	American Association of Motor Vehicle Administrators	Financial Institution-Verifying Identity Credentials Service	Paul Blanchard pblanchard@aamva.org
Identity Management and Data Privacy Technologies	Massachusetts Institute of Technology	Accountable Information Usage in Distributed Information Sharing Environments	Dr. Lalana Kagel lkagal@CSAIL.MIT.EDU
Cyber Security Experiments and Pilots	Applied Visions/Secure Decisions	ViAssist visualization pilot with Library of Congress	Brianne O’Brien brianne.obrien@ securedecisions.com
Transition to Practice	Sandia National Laboratories	Test and Evaluation	