HSARPA Cyber Security Division

Internet Measurement and Attack Modeling Project

Active Internet Measurement Systems Workshop (AIMS)

February 6-8, 2013

Ann Cox, PhD.
Program Manager
Cyber Security Division

Homeland Security Advanced Research Projects Agency (HSARPA)

Homeland Security

Science and Technology

Homeland Security
Science and Technology

CSD Mission

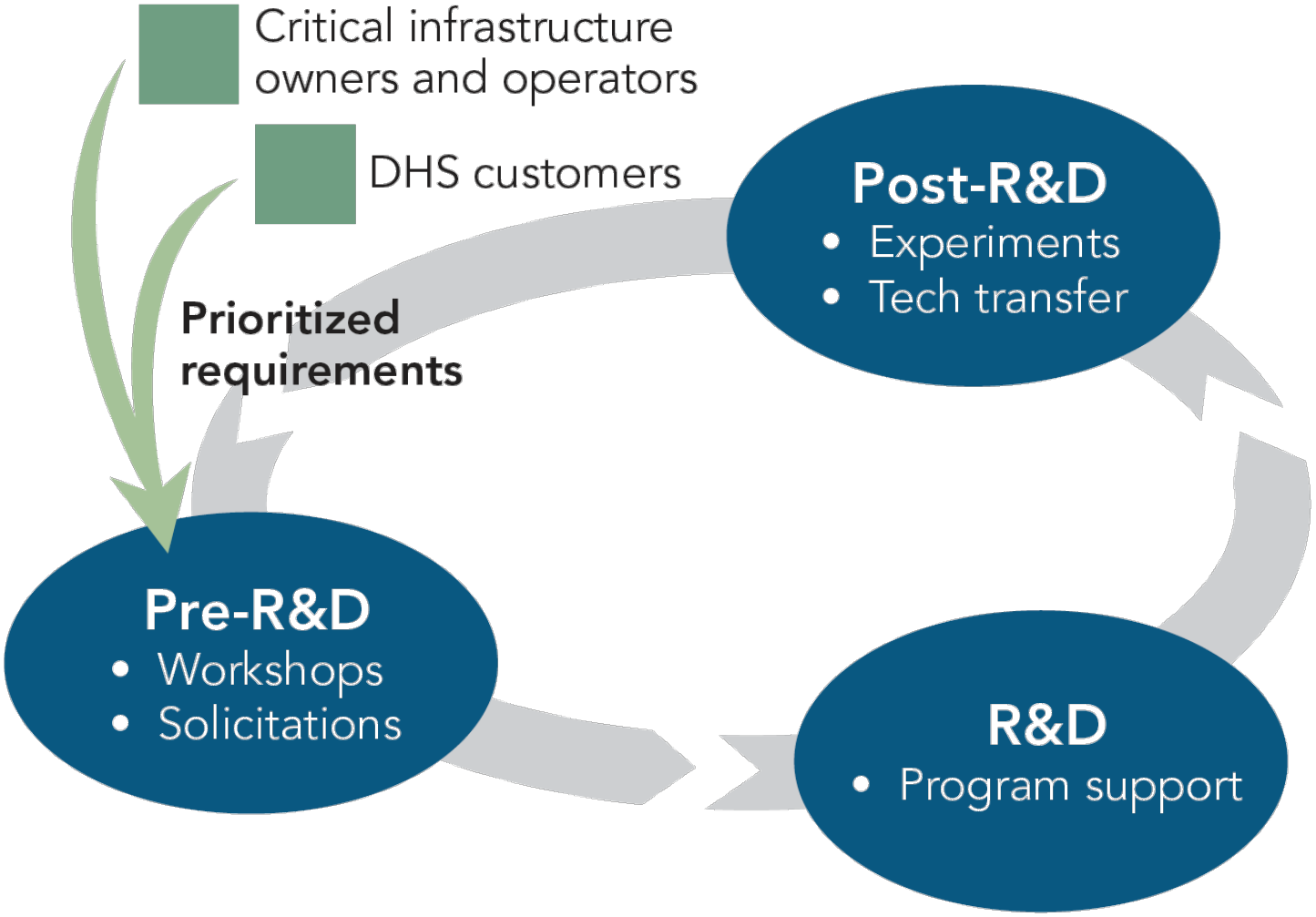
- Develop new technologies, tools and techniques to defend and secure current systems and networks, and strengthen future systems and networks, to enable DHS and the U.S. to better protect critical infrastructures and respond to attacks from our adversaries;

- Conduct and support technology transition efforts across DHS and through a full range of government, commercial and hybrid approaches;

- Provide coordination and research and development leadership for internal DHS customers, agencies of the U.S. government that conduct or sponsor research and development, academia, private sector and international partners within the cybersecurity community.

Homeland Security
Science and Technology

CSD R&D Execution Model



Homeland Security
Science and Technology

Research Infrastructure (RISC)

- Experimental Research Testbed (DETER)
  - Researcher and vendor-neutral experimental infrastructure
    - Used by over 200 organizations from more than 20 states and 17 countries since 2003
    - Used by over 40 classes, from 30 academic institutions involving 2,000+ students
  - http://www.deter-project.org
- Research Data Repository (PREDICT)
  - Repository of network data for use by the U.S.- based cybersecurity research community
    - More than 200 users (academia, industry, gov't); Over 350TB of network data; Tools are used by major service providers and many companies
    - Legal framework is US-based. Working to add international users (CA, AUS, JP, EU)
  - https://www.predict.org
- Software Assurance Market Place (SWAMP)
  - A software assurance testing and evaluation facility and the associated research infrastructure services

Homeland Security
Science and Technology

Foundational Elements (FECS)

- Enterprise Level Security Metrics and Usability
- Homeland Open Security Technology (HOST)
- Software Quality Assurance
- Cyber Economic Incentives (CNCI*)
- Leap Ahead Technologies (CNCI*)
- Moving Target Defense (CNCI*)
- Tailored Trustworthy Spaces (CNCI*)

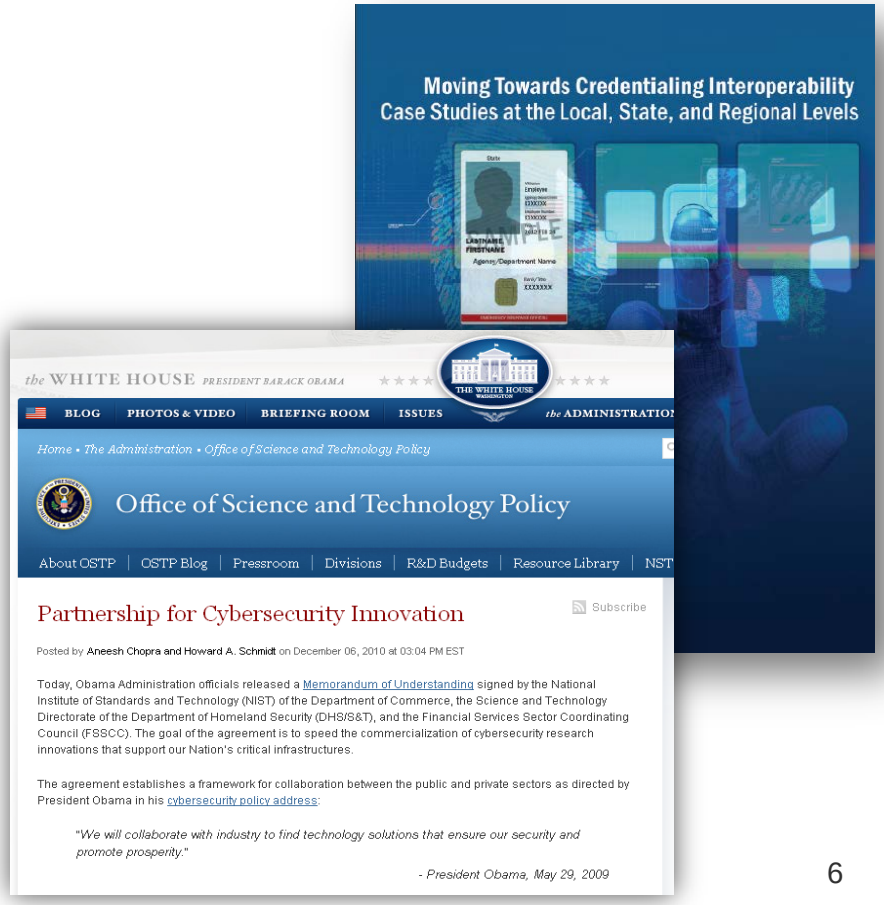
*CNCI – Comprehensive National Cybersecurity Initiative launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) in January 2008.

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

Homeland Security
Science and Technology

Cybersecurity Users (CUPE)

- Cyber Security Competitions
  - National Initiative for Cybersecurity Education (NICE)
  - NCCDC (Collegiate); U.S. Cyber Challenge (High School)
- Cyber Security Forensics
  - Support to DHS and other Law Enforcement customers (USSS, CBP, ICE, FBI, CIA)
- Identity Management & Data Privacy Technologies
  - National Strategy for Trusted Identities in Cyberspace (NSTIC)



Homeland Security
Science and Technology

Evaluation and Transition (CTET)

- Assessment and Evaluations
  - Red Teaming of DHS S&T-funded technologies
  - Support of the Security Innovation Network (SINET)
- Experiments and Pilots
  - Experimental Deployment of DHS S&T-funded technologies into operational environments
    - Partnerships with ICE, USSS, CBP, NCSD, S&T CIO
  - Distributed Environment for Critical Incident Decision-making Exercises (DECIDE) Tool for Finance Sector to conduct risk management exercises and identify improvements
- Transition to Practice (CNCI)
  - Transitioning cyber security technologies developed through federally funded research and development (R&D) into broader utilization

Homeland Security
Science and Technology

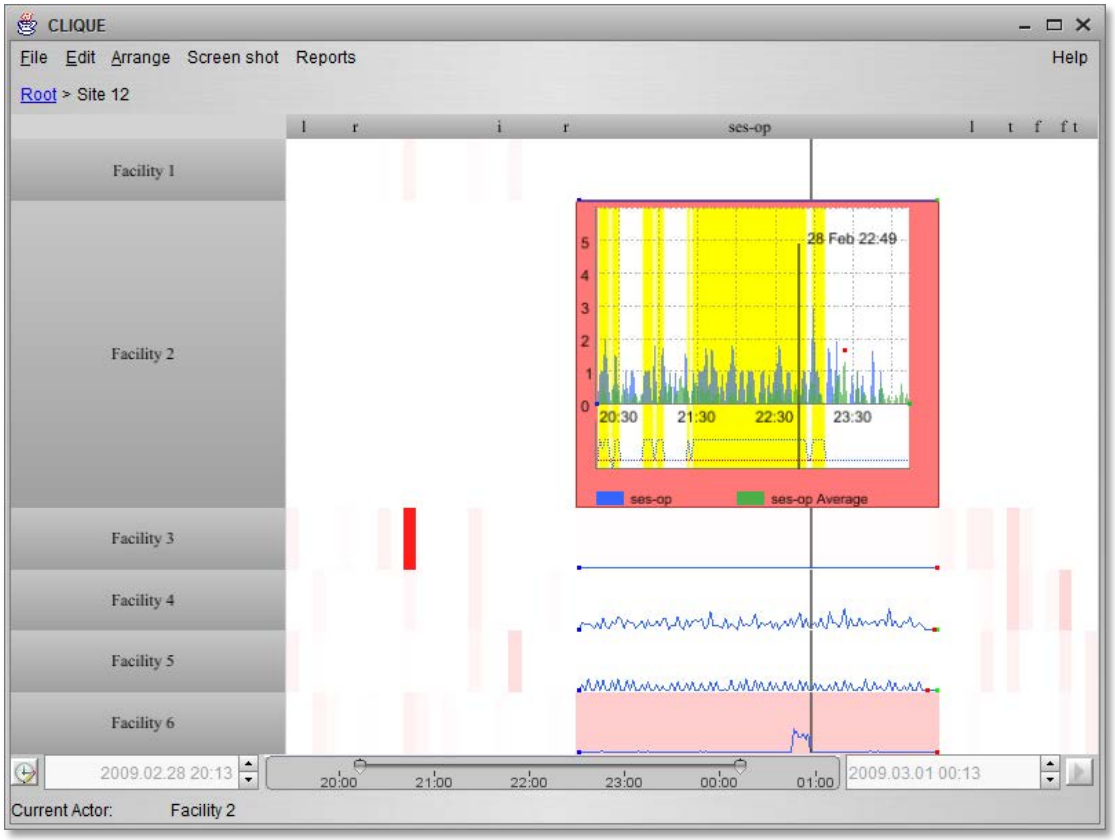
Trustworthy Cyber Infrastructure

- Secure Protocols
  - DNSSEC – Domain Name System Security
    - Started in 2004; now 35 top level domains adopted globally including the Root
  - SPRI – Secure Protocols for Routing Infrastructure
- Process Control Systems
  - LOGIIC – Linking Oil & Gas Industry to Improve Cybersecurity
  - TCIPG – Trustworthy Computing Infrastructure for the Power Grid
- ****Internet Measurement and Attack Modeling****
  - Geographic mapping of Internet resources
  - Logically and/or physically connected maps of Internet resources
  - Monitoring and archiving of BGP route information
  - Co-funding with multiple international partners

Existing Effort: CLIQUE / Traffic Circle

Correlation Layers for Information Query and Exploration (CLIQUE) (Performer: PNNL)

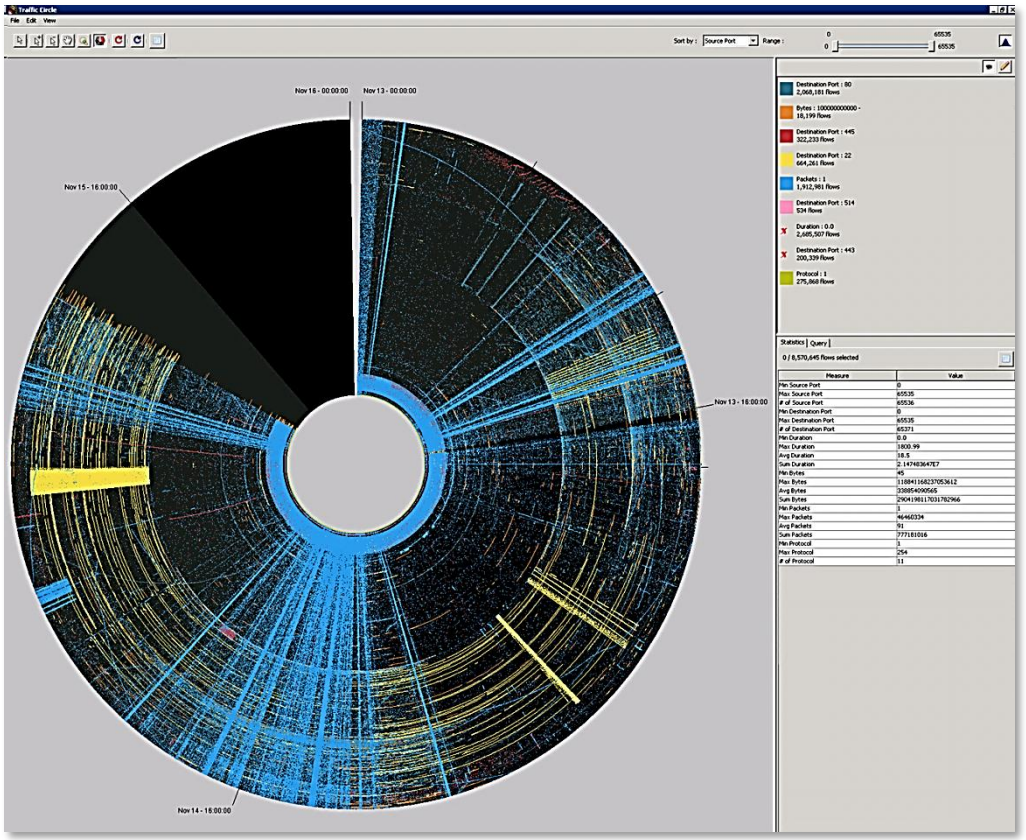
Displays high-level overviews of network traffic using a new behavioral model-based anomaly detection technique. The CLIQUE system builds models for learning and classifying expected behavior on individual hosts on a network and then compares these modeled behaviors to real-time streaming data to generate early indicators of “non-normal” network activity.



Existing Effort: CLIQUE / Traffic Circle

Traffic Circle (Performer PNNL)

- As network transactions occur, Traffic Circle displays them on a moving timeline. Via the “time wheel” analysts can dynamically zoom through data spanning months or years in just seconds. The tool allows for sophisticated filters that highlight important patterns.



IMAM Efforts under BAA 11-02

Real-time Protocol Shepherd (RePS)

Raytheon/BBN 10-month effort

- Uses real-time proactive tools with Bro and Suricata systems to actively prevent network based attacks using chained rules and flow variables in Suricata and detection modules and scripts in Bro

Methodology for Assessment of Security Properties

Naval Postgraduate School (NPS) 36-month effort

- A systematic methodology for security assessment and the construction of composite information systems, as well as a set of metrics and rules for security properties of individual components that will later be connected to such systems.

Homeland Security
Science and Technology

IMAM Efforts under BAA 11-02

Comprehensive Understanding of Malicious Overlay Networks

Georgia Tech Research Center (GTRC) 24-month effort

- (1) Prevention of botnet infections using network- and host-based defenses
  (2) Detection of infections that take hold of operator networks
  (3) Comprehensive large-scale analysis of malware
  (4) Large-scale analysis of passive DNS data
  (5) Innovation of attribution and traceback technologies
  (6) Long-term remediation of botnets through the use of next-generation sinkholes and network management technologies.

IMAM Efforts under BAA 11-02

Visually Fusing Contextual Data for Situational Understanding

Oak Ridge National Laboratory (ORNL) 36-month effort

- Contextual information integrated into STUCCO[1] to understand the significance of events, and a threat landscape service at a macro level that provides new threat indicators from social media and synthesis of open source reporting.

[1] STUCCO - Situation and Threat Understanding by Correlating Contextual Observations. STUCCO will be a scalable visual analytics solution that enables both exploration of the efficacy of potential contextual data sources and real-time monitoring of high-value contextual data.

Homeland Security
Science and Technology

IMAM Efforts under BAA 11-02

Advanced Situation Awareness of High Impact Malware Attacks Against the Internet Routing Infrastructure

Columbia University 24-month effort

- Develop and deploy an experimental system that injects intrusion detection functionality within the firmware of a (legacy) router that senses the unauthorized modification of router firmware. The technology may be developed and deployed as a sensor to detect attacks in an Early Attack Warning System, but also may be implemented to prevent firmware modifications.

Homeland Security
Science and Technology

IMAM Efforts under BAA 11-02

The Retrospective Future in the Internet (Retro-Future)

USC/ISI 36-month effort

- An Internet ‘DVR’ that will record, abstract, and replay packet traces, DNS, and routing information to enable retrospective analysis of network security events (new 0-day attacks and worms, insider threats, etc.)

High-Frequency Active Internet Topology Mapping

Naval Postgraduate School (NPS) 36-month effort

- Deployment of three recently developed discriminatory active topology primitives. These primitives maximize the utility of each individual path tracing probe, permitting additional probing within a fixed time or load budget. This will enable higher speed mapping, enumeration of load-balanced paths, and better resolution of router aliases.

Homeland Security
Science and Technology

IMAM Efforts under BAA 11-02

Cartographic Capabilities for Critical Cyberinfrastructure

CAIDA 36-month effort

Enabling Operational Use of RPKI via Internet Routing Registries

Merit Network, Inc. 12-month effort

- Integrate Resource Public Key Infrastructure (RPKI) into the Internet Routing Registry (IRR) system and in particular the largest routing registry, the RADB
  - Extend the Routing Policy Specification Language (RPSL) to include support for RPKI attributes
  - Build and operate a public RPKI validation cache
  - Modify the core routing registry software to allow it to lookup and return RPKI validity information for each route query
  - Augment existing toolsets so that they can use the RPKI information being distributed via the IRRs

Homeland Security
Science and Technology

IMAM Efforts under BAA 11-02

Netalyzr NG: Monitoring DNS, DNSSEC, and TLS from the Edge

UC-Berkeley/ICSI 24-month effort

- A set of extensions to the widely used and free Netalyzr edge network debugging, diagnostic, and network measurement suite. This free tool will add significant monitoring for DNS, DNSSEC, and TLS, enabling client to detect individual network manipulations and to debug problems as they occur.

Homeland Security
Science and Technology

Small Business Innovative Research (SBIR)

Important program for creating new innovation and accelerating transition into the marketplace

- Since 2004, DHS S&T Cyber Security has had:
  - 63 Phase I efforts
  - 28 Phase II efforts
  - 5 Phase II efforts currently in progress
  - 9 commercial/open source products available
  - Four acquisitions
    - Komoku, Inc. (MD) acquired by Microsoft in March 2008
    - Endeavor Systems (VA) acquired by McAfee in January 2009
    - Solidcore (CA) acquired by McAfee in June 2009
    - HBGary (CA) acquired by ManTech in February 2012

DHS S&T Long Range Broad Agency Announcement (LRBAA)

S&T seeks R&D projects for revolutionary, evolving, and maturing technologies that demonstrate the potential for significant improvement in homeland security missions and operations

- Offerors can submit a pre-submission inquiry prior to White Paper submission that is reviewed by an S&T Program Manager
- S&T BAA Submission Website: https://baa2.st.dhs.gov
- Additional information can be found on the Federal Business Opportunities website (www.fbo.gov)
  - **LRBAA 12-07 has been extended until December 31, 2013**
  - New topics have been added and some deleted; only topics listed in the latest amendment may be submitted at this time.
  - https://www.fbo.gov/index?s=opportunity&mode=form&id=fd7681bfcc57bae4d443fce6710279b7&tab=core&_cview=1

Homeland Security
Science and Technology

Contact

Ann Cox, Ph.D.

Program Manager

Cyber Security Division

Homeland Security Advanced Research Projects Agency (HSARPA)

Ann.Cox@hq.dhs.gov

202-254-6198

For more information, visit

http://www.cyber.st.dhs.gov

Homeland Security

Science and Technology