INTRODUCTION TO NSF CYBERSECURITY TRANSITION TO PRACTICE

Florence Hudson
Senior Vice President and Chief Innovation Officer, Internet2

Emily Nichols
Innovation Program Manager, Internet2

Introduction to NSF Cybersecurity Transition to Practice Acceleration EAGER

CONTENTS

- Goals & Approach
- Project Plan
- Project Activities Performed to Date
- Discussion

NSF Strategic Priorities in Cybersecurity

From the 2016 Federal Strategy for Cybersecurity R&D:

- …long-term investments in a wide area of ***scientific fields***, and …ensuring the **adoption and implementation of new technologies** that emerge from research
- …basis for designing, building, and operating a cyber-infrastructure with **improved resistance and improved resilience to attack** that can be tailored to … technical and policy requirements, including ...**privacy and accountability**

Federal Cybersecurity Research and Development Strategic Plan:
https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf

NSF Cybersecurity TTP EAGER Goal and Approach

Goal: accelerate Transition To Practice (TTP) of NSF funded later stage cybersecurity research into operational environments by prototyping and experimental deployments

Approach

- Develop inventory of NSF cybersecurity research awards and PI's in SaTC, CICI, CPS programs
- Determine potential for research projects for applied usage in a Research & Education environment
- Serve as a matchmaker to encourage adoption of security capabilities by operational users
- Identify security infrastructure needs/gaps with current tools, success stories, best practices, learnings, potential synergies, collaboration opportunities
- Design and develop materials, events, TTP showcase webinars, matchmaking, & researcher TTP enablement
- Explore the opportunity to develop an end-to-end innovation pipeline
- Engage the extended R&E pipeline
- Design, develop, and begin to execute the pilot program

NSF Cybersecurity Transition to Practice (TTP) Success: Bro

- Bro provides a flexible, open network monitoring platform.
  - Developed since 1995, now at ICSI & NCSA.
  - Open-source with a BSD license.
  - Fundamentally different from a traditional IDS.
- Bridges gap between academia and operations.
  - Has helped transition research into practice for almost two decades.
  - Deployed operationally by universities, research labs, Fortune 20.

Project Plan

Step	Project Activities	1Q	2Q	3Q	4Q	5Q	6Q	7Q	8Q
1	Project team in place								
2	Develop NSF Research Asset Inventory								
3	Interview NSF, researchers, practitioners, universities, industry, labs, DHS, other agencies								
4	Develop researcher/practitioner match-making showcase -online, events								
5	Develop TTP R&D showcase and technical workshops								
6	Deploy workshops				#1	#2	#3	#4	
7	Design, develop NSF TTP Portal								
8	Develop materials for NSF TTP Portal								
9	Deploy NSF TTP Portal								
10	Assess TTP program and develop recommendations								

Project Activity #1: Project team in place

- Florence Hudson, Chief Innovation Officer, Internet2
- Emily Nichols, Innovation Program Manager, Internet2
- Giselle Trent, Executive Assistant to Chief Innovation Officer, Internet2

Project Activity #2: NSF Research Asset Inventory – 914 Active SaTC Awards

Title	PI	Organization	Award Amt
TWC: TTP Option: Frontier: Collaborative: MACS: A Modular Approach to Cloud Security	Ran Canetti	Trustees of Boston University	$1,609,797
Collaborative Research: SI2-SSI: Empowering the Scientific Community with Streaming Data Middleware: Software Integration into Complex Science Environments	Tony Fountain	University of California-San Diego	$1,455,429
TWC: Medium: Micro-Policies: A Framework for Tag-Based Security Monitors	Benjamin Pierce	University of Pennsylvania	$1,200,000
TWC: TTP Option: Frontier: Collaborative: MACS: A Modular Approach to Cloud Security	Srini Devadas	Massachusetts Institute of Technology	$1,176,449
TWC: Medium: Hardware Trojans in Wireless Networks - Risks and Remedies	Yiorgos Makris	University of Texas at Dallas	$1,129,437
CPS: TTP Option: Synergy: Safe and Secure Open-Access Multi-Robot Systems	Magnus Egerstedt	Georgia Tech Research Corporation	$999,999
TWC: Medium: Collaborative: Towards Securing Coupled Financial and Power Systems in the Next Gen Smart Grid	Karl Levitt	University of California-Davis	$839,997
CPS:Synergy:Security of Distributed Cyber-Physical Systems with Connected Vehicle Applications	Pierluigi Pisu	Clemson University	$800,000
TWC: Medium: Collaborative: Towards a Binary-Centric Framework for Cyber Forensics in Enterprise Environments	Dongyan Xu	Purdue University	$800,000
TWC SBE TTP: Medium: Bringing Anthropology into Cybersecurity	Xinming Ou	Kansas State University	$715,845
TWC SBE: Option: Small: Building Public Cyber Health - Designing and Testing the Efficacy of a School-Focused, Gamification Approach to Create a Secure Computing Environment	Noel Greis	University of North Carolina at Chapel Hill	$653,975
SBES TWC: Phase: Small: Protecting the Bazaar: The Ecology of Cybersecurity in Weakly Fortified Networks	David Maimon	University of Maryland College Park	$647,804
TWC: TTP Option: Small: Differential Introspective Side Channels --- Discovery, Analysis, and Defense	Zhuoqing Mao	University of Michigan Ann Arbor	$605,282
CPS: TTP Option: Synergy: Collaborative Research: Hardening Network Infrastructures for Fast, Resilient and Cost-Optimal Wide-Area Control of Power Systems	Aranya Chakrabortty	North Carolina State University	$600,000
SBE: Medium: Collaborative: Understanding and Exploiting Visceral Roots of Privacy and Security Concerns	Alessandro Acquisti	Carnegie-Mellon University	$595,197
RET Site: Cyber Security Initiative for Nevada Teachers (CSINT)	Shamik Sengupta	Board of Regents, NSHE, obo University of Nevada, Reno	$540,000
TWC: Small: Understanding Anti-Analysis Defenses in Malicious Code	Saumya Debray	University of Arizona	$514,796
TWC: Medium: Collaborative: Towards a Binary-Centric Framework for Cyber Forensics in Enterprise Environments	Golden Richard	University of New Orleans	$511,193
TWC: Small: Quantitative Analysis and Reporting of Electromagnetic Covert and Side Channel Vulnerabilities	Alenka Zajic	Georgia Tech Research Corporation	$500,535
CICI: Data Provenance: Provenance-Based Trust Management for Collaborative Data Curation	Zachary Ives	University of Pennsylvania	$500,000
CPS: Breakthrough: Secure Telerobotics	Howard Chizeck	University of Washington	$500,000
TWC: Small: Addressing the challenges of cryptocurrencies: Security, anonymity, stability	Arvind Narayanan	Princeton University	$500,000
TWC: Small: Behavior-Based Zero-Day Intrusion Detection for Real-Time Cyber-Physical Systems	Sibin Mohan	University of Illinois at Urbana-Champaign	$500,000

Project Activity #2: Campus Pilot Projects

- **Zeropoint** – **Document Detection and Analytics**. UNC-Chapel Hill, PI – Fabian Monrose
  - Analyzes email, web content and server traffic for hazardous content. End-user will not need to guess whether a document is infected with malicious code, but is notified before data is lost.
- **Amico – Detection of Malware Downloads**. University of Georgia, PI – Roberto Perdisci
  - Automatically distinguishes between malware and benign software downloads.
- **CipherLocker – A Fully-Private Cloud Storage, Search, and Collaboration Portal for Education**: A Campus Pilot. State University of New York-Stony Brook, PI – Radu Sion
  - Functionality similar to Box and Dropbox, with additional feature of Search on Encrypted Data (SED) that makes stored files safely searchable while remaining encrypted.
- **A Kit for Exploring Databases Under the Hood for Security, Forensics and Data**. DePaul University, PI – Alexander Rasin
  - Open source tools to provide visibility into the storage of several database systems, illustrating exactly what is happening inside.
- **Named Data Networking**: Colorado State University, PI – Christos Papadapolous

Zeropoint:

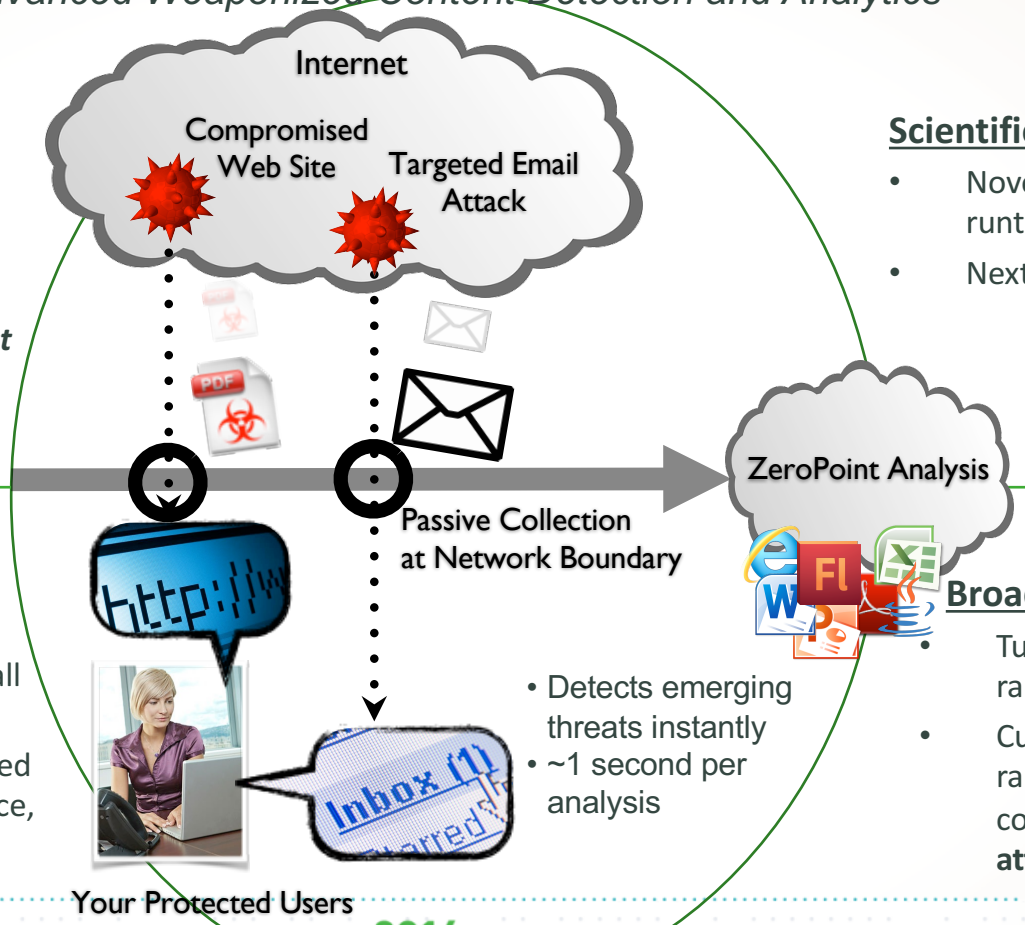
Advanced Weaponized Content Detection and Analytics

Challenge:

- **Weaponized documents** are pervasive and automatically and uniquely generated per-incident.
- Attacks take ***seconds to compromise, but months to detect*** with commodity technologies.

Solution:

- Patented ***Execution-of-Data*** technology examines data as potential code, executes it from all angles
- Malicious code, if present, is forced to run instantly in our secure space, providing operators with **concise forensic traces**.



- Detects emerging threats instantly
- ~1 second per analysis

Scientific Impact:

- Novel application of dynamic runtime analysis at scale
- Next-generation cyber defense

Broader Impact:

- Turns the tide by significantly raising the bar for the attacker
- Cuts through all the layers of randomized and obfuscated content, **illuminates intent of attacks**

Zeropoint Dynamics, LLC
http://www.zeropointdynamics.com
Contact: Kevin Z. Snow (kevin@zeropointdynamics.com)

CipherLocker

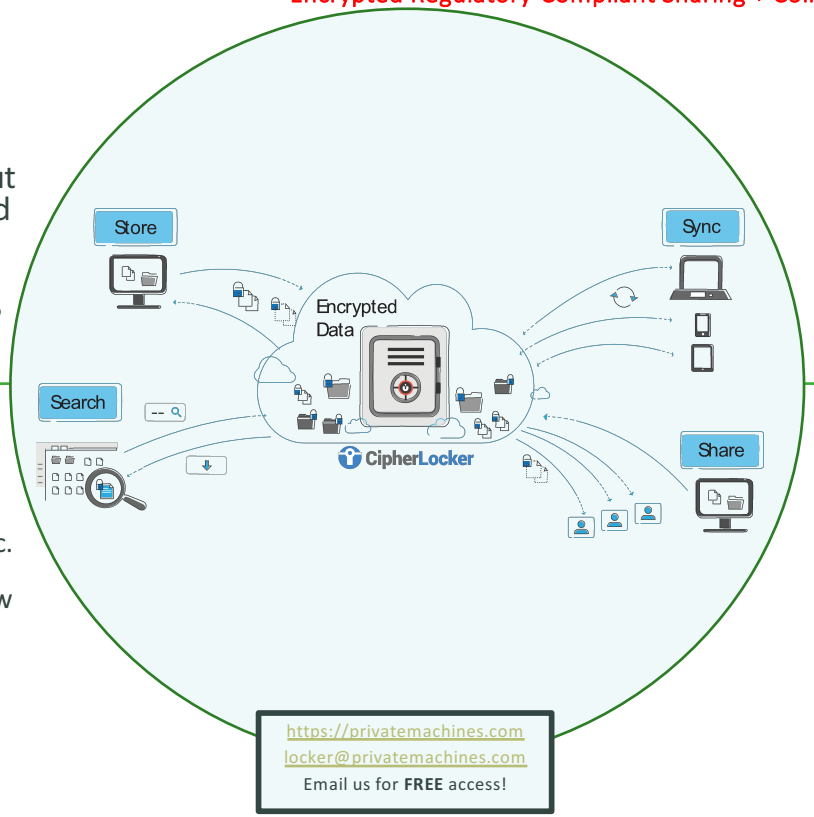
Encrypted Regulatory-Compliant Sharing + Collaboration

Challenge:

Sharing and collaborating without risk of data leaks and compromise. Regulatory compliant. NIST FIPS certified.

Solution:

Strong, transparent client-side encryption layer. Drag-and-drop share. Store. Share. Sync. Search. Everything encrypted on-prem. New innovative search on encrypted data technology.



https://privatemachines.com
locker@privatemachines.com
Email us for **FREE** access!

Scientific Impact:

Researchers and students participate and directly evaluate the platform in operation. Project sparks significant additional research into client-side driven security in cloud contexts.

Broader Impact:

Provide free secure storage to 24,500 students and 2,500 educators. Testbed for deploying secure protocols in a live environment. The project will train students and contribute to the creation of a skilled cyber-security domestic workforce available to fulfill our nation's needs.

INTERNET2 2016 TECHNOLOGY exchange MIAMI FL SEPTEMBER 25-28

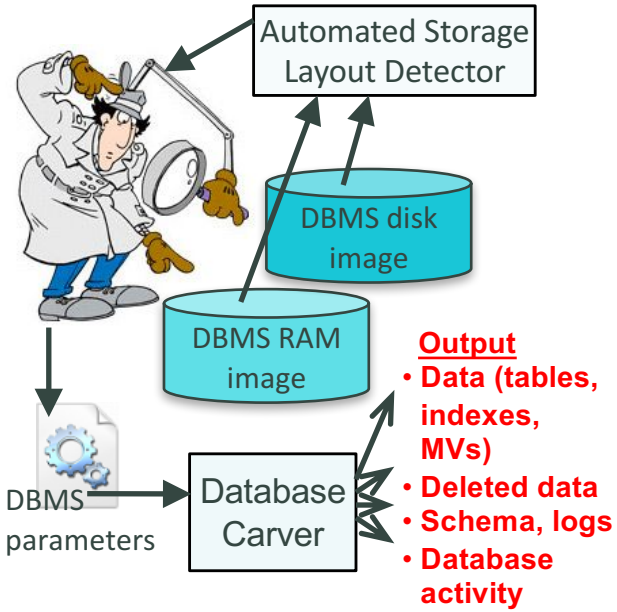
Database Reconstruction Kit: How to Capture all DBMS Data and Activity from any Disk or RAM Fragment

Challenge:

- Given an **incomplete** or **corrupt** storage with **unknown** database(s)
  1. Reconstruct **all data**
  2. Determine **database activity**

Solution:

- **Universal**, parametric model of byte-level DBMS storage
- Automate learning new DBMS parameters
- Reconstruct any storage fragment (disk or RAM)



Scientific Impact:

- A **unified** database storage model
- **Automating** reverse-engineering of DBs
- **Generalized** approach to database forensics

Broader Impact:

- Reconstruct database from **partial** or **corrupt** disk fragments or RAM
- **Determine if an attacker stole or tampered with data**

CNS Award #1656268

Alexander Rasin, Jacob Furst, Karen Heart (DePaul University)

Jonathan Grier (Grier Forensics)

INTERNET2 2016 TECHNOLOGY exchange MIAMI FL SEPTEMBER 25-28

Project Activity #3: Interview CI Experts (Network/Security Engineers, SysAdmins, DBAs, CISO, CIO) on Needs and Willingness to try Later Stage Research

1. Interview NSF TTP cybersecurity awardees & future PI's
   - Determine who is ready to enter an applied research phase
   - Identify which PI's need a campus pilot or partner to test out the concept
2. Identify & interview potential R&E Practitioners re: interest in testing/applying the research
   - Approach Internet2 member universities to determine interest
   - Roles: CIOs, CISOs, IT staff
   - Identify cybersecurity gaps and needs, interest in approach, considerations
3. Interview SMEs in the TTP process to identify best practices and learnings
   - Federal Agencies & Programs including NSF SATC/CICI/CPS, DHS, CRI, SBIR/STTR, ICORPS, IU/CRC
   - University Vice Presidents of Research and Tech Transfer Offices

Project Activity #4: Enable TTP Matchmaking

1. Develop matchmaking opportunity for ready researchers and institutions
   - Identify R&E institutions interested in participating in NSF funded cybersecurity research
   - Engage CIOs and CISOs in the potential practitioner institutions to validate interest
   - Develop plan for matchmaking events
2. Develop portfolio of cybersecurity research ready to be applied in practitioner institutions
   - Assess cybersecurity research readiness for applied research in practitioner institutions
   - Classify and present research by category: e.g., Named Data Networking, Network Security, IoT, Smart Grid, HCLS
3. Assess best practices and determine if and how to leverage them
   - From DHS TTP, SBIR/STTR, Tech Transfer programs, industry, successful TTPs

Project Activity #5 and 6: Develop and deploy TTP matchmaking showcase events, workshops, webinars

1. Kickoff and input from Internet2 membership
   - Internet2 TechEx, Miami, FL: Kickoff, September 27, 2016
2. Webinars or workshops to showcase TTP research assets with potential R&E users
   - Internet2 Collaborative Innovation Community call and Input – October 2016, perhaps ongoing TBD
   - Internet2 events: Global Summit - April 2017, May 2018; TechEx - Sept 2016, Oct 2017
   - Other calls/events, w/agencies, organizations, regionally, CIOs/CISOs, ITANA (IT Architects iN Academia)
3. Webinars and workshops to provide researcher coaching for TTP success
   - Knowing when you are ready to transition to an applied research environment for user input
   - Other potential topics: clarity of value proposition of research tool/asset
   - Identify who can do the coaching and how best to provide it

Discussion

- Are you involved in Cybersecurity TTP work – with NSF or another agency?
- Do you have cybersecurity research on campus you know of that might be interested in a TTP matchmaking opportunity in the Internet2 community?
- Would you be interested in being an applied research user?
- What would you need to make the decision to apply cybersecurity research?
- If you have been involved in applying cybersecurity or other NSF research before, what was the experience, and what can we learn from it?
- What do you think the opportunities, challenges, best practices, and critical success factors are for TTP?
- What acceleration techniques, partnership models, and other forms of enablement do you think would improve the TTP process?

Please let us know your input, interest and pilot opportunities

- **Tuesday, Sept 27 TechEx Afternoon session to continue the discussion, 3:50-4:40pm "NSF Cybersecurity Transition to Practice Acceleration EAGER – CONTINUED"**

- Email us:
  - Florence Hudson fhudson@internet2.edu
  - Emily Nichols enichols@internet2.edu
  - cino@internet2.edu

INTRODUCTION TO NSF CYBERSECURITY TRANSITION TO PRACTICE

Florence Hudson
Senior Vice President and Chief Innovation Officer, Internet2

Emily Nichols
Innovation Program Manager, Internet2