MC: Peter Alfonso, Vice President for Research & Economic Development, University of Rhode Island

Welcome: David M. Dooley
President, University of Rhode Island

Opening Remarks: James Langevin
U.S. Congressman

Remarks: Sheldon Whitehouse
U.S. Senator
Keynote: General Keith B. Alexander, Commander, U.S. Cyber Command (USCYBERCOM) and Director, National Security Agency/Chief, Central Security Service (NSA/CSS), Fort George G. Meade, MD.
THINKING BIG
Go Rams!
Cyber Security For the 21st Century
Deep Blue - 1997
Massive computation power

Watson - 2010
Natural language and assessment
Facebook Helps Organize Snowball Battle at Dupont Circle

Shades of ‘Snowmageddon’: Dozens turn Dupont Circle into snowball battleground

By Steve Hendrix
Washington Post Staff Writer
Wednesday, January 26, 2011, 11:24 PM

After an 11-month warm-weather truce, a snowball was hurled with hostile intent across Dupont Circle at

---

Social Media Gets Credit for Tunisian Overthrow

Facebook Helps Organize Snowball Battle at Dupont Circle

Game over in Tunisia & Egypt: Why the revolution HAS been tweeted

Forbes

---

Game over in Tunisia & Egypt: Why the revolution HAS been tweeted
Adversaries are developing destructive Advanced Persistent Threats faster than we are developing policies, authorities and technical means to protect against them.
5 Strategic Initiatives

Cyber as Operational Domain

Employ New Defense Operating Concepts – Active Defense

Extend Cyber Defenses – Critical Infrastructure

Build International Partnerships

Leverage the Nation’s Ingenuity
Extending Protection to Critical Infrastructure
We the People of the United States, in Order to form a more perfect Union, establish Justice, ensure domestic Tranquility, provide for the common Defense, and promote the General Welfare, and to secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.
GRACE HOPPER
AND THE
INVENTION OF THE INFORMATION AGE

KURT W. BEYER
Panel Session 1: *Cyber Threats to Critical Infrastructure*

**Douglas Maughan**, Ph.D., Director, Cyber Security Division, Department of Homeland Security

**Theresa Murray**, Regional Catastrophic Planner, Rhode Island Emergency Management Agency – Topic: *Cyber Disruption Efforts in Rhode Island*

**Yan Sun**, Ph.D., Associate Professor, URI Department of Electrical, Computer, and Biomedical Engineering - Topic: *Understanding Cascading Failures in the U.S. Power Grid*

Panel Q & A
CYBERSECURITY SYMPOSIUM

Douglas Maughan
Director, Cyber Security Division
Department of Homeland Security
USG Cybersecurity R&D Activities

URI Cybersecurity Symposium
Kingston, RI
April 11, 2011

Douglas Maughan, Ph.D.
Division Director
Cyber Security Division
Homeland Security Advanced Research Projects Agency (HSARPA)
douglas.maughan@dhs.gov
202-254-6145 / 202-360-3170
## 12 CNCI Projects

### Focus Area 1

- **Reduce the Number of Trusted Internet Connections**
- **Deploy Passive Sensors Across Federal Systems**
- **Pursue Deployment of Automated Defense Systems**
- **Coordinate and Redirect R&D Efforts**

### Focus Area 2

- **Connect Current Centers to Enhance Situational Awareness**
- **Develop Gov’t-wide Counterintelligence Plan for Cyber**
- **Increase Security of the Classified Networks**
- **Expand Education**

### Focus Area 3

- **Define and Develop Enduring Leap Ahead Technologies, Strategies & Programs**
- **Define and Develop Enduring Deterrence Strategies & Programs**
- **Manage Global Supply Chain Risk**
- **Cyber Security in Critical Infrastructure Domains**

---

**Establish a front line of defense**

**Resolve to secure cyberspace / set conditions for long-term success**

**Shape future environment / secure U.S. advantage / address new threats**

---

11 April 2011

CNCl = Comprehensive National Cyber Initiative
Business/IT Cybersecurity Solutions Can Break Control Systems

Different Priorities

**Control Systems**
- Availability then
- Integrity then
- Confidentiality

**Business/IT Systems**
- Confidentiality then
- Integrity then
- Availability

- Power systems must operate 24/7 with high reliability and high availability, no down time for patching/upgrades
- Control system components may not have enough computing resources (e.g., memory, CPU, communication bandwidth) to support the addition of cybersecurity capabilities
- Real-time operations are imperative, latency is unacceptable
- Real-time emergency response capability is mandatory
Open Protocols
– Open industry standard protocols are replacing vendor-specific proprietary communication protocols

Common Operating Systems
– Standardized computational platforms increasingly used to support control system applications

Interconnected to Other Systems
– Connections with enterprise networks to obtain productivity improvements and information sharing

Reliance on External Communications
– Increasing use of public telecommunication systems, the Internet, and wireless for control system communications

Increased Capability of Field Equipment
– “Smart” sensors and controls with enhanced capability and functionality, demand response communication networks
Aligning Efforts, Accelerating Solutions

- **Energy Sector’s** synthesis of critical control system security challenges, R&D needs, and milestones
- Strategic framework for aligning activities
- Catalyst for public-private collaboration
- Tool for focusing investment and accelerating solutions

**Roadmap Vision**

In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to **survive** an intentional cyber assault with no loss of critical function.
Measure and Assess Security Posture
➢ By 2015, the sector will help ensure that energy asset owners have the ability and commitment to perform fully automated security state monitoring of their control system networks with real-time remediation capability.

Develop and Integrate Protective Measures
➢ By 2015, next generation control system components and architectures that offer built-in, end-to-end security will replace many older legacy systems.

Detect Intrusion and Implement Response Strategies
➢ By 2015, the energy sector will operate control system networks that automatically provide contingency and remedial actions in response to attempted intrusions into the control systems.

Sustain Security Improvements
➢ By 2015, energy asset owners and operators are committed to working collaboratively with government and sector stakeholders to accelerate security advances.
DHS S&T Mission

Strengthen America’s security and resiliency by providing knowledge products and innovative technology solutions for the Homeland Security Enterprise
R&D Execution Model

Customers
- NCSD
- NCS
- USSS
- National Documents

Other Sectors
- e.g., Banking & Finance

Critical Infrastructure Providers

Prioritized Requirements

Pre R&D
- Workshops
- Solicitation Preparation
- CIP Sector Roadmaps

Supporting Programs
- DETER
- PREDICT

R&D
- DNSSEC
- CI / KR – Energy, B&F, O&G
- Cyber Forensics
- BAAs
- SPRI
- HOST
- Education / Competitions

Post R&D
- Outreach – Venture Community & Industry
- R&D Coordination – Government & Industry
- Experiments and Exercises

Cyber Security
R&D CENTER

11 April 2011
• DNSSEC – Domain Name System Security
  – Working with OMB, GSA, NIST to ensure USG is leading the global deployment efforts
    • http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf
  – Working with vendor community to ensure solutions
    • http://www.govsecinfo.com/the-keys-to-deploying-dnssec.html

• SPRI – Secure Protocols for Routing Infrastructure
  – Working with global registries to deploy Public Key Infrastructure (PKI) between ICANN/IANA and registry and between registry and ISPs/customers
  – Working with industry to develop solutions for our current routing security problems and future technologies
Finance Sector - DECIDE

• DECIDE (Distributed Environment for Critical Infrastructure Decision-making Exercises)
  – Foster an effective, practiced business continuity effort to deal with increasingly sophisticated cyber threats
    • Enterprises will be able to initiate their own large-scale exercises, define their own scenarios, protect their proprietary data, and learn vital lessons to enhance business continuity, all from their desktops
  – Think through sector impacts and responses to operational disruptions of market-based transactions across networks of the National Planning Scenarios
    • Enhance coordination during a large-scale disruption to key infrastructures
  – The concept has been reviewed by and developed with input from experts at ChicagoFIRST, the Options Clearing Corporation, ABN-AMRO, Eurex, Archipelago, Bank of New York, and CitiBank.
  – The Financial Services Sector Coordinating Council R&D Committee has organized a user-group of subject matter experts paid by their respective financial institutions to support the project over the next two years.
Critical Infrastructure / Key Resources

- MOU between DHS S&T, NIST, and FS Sector Coord Council (FSSCC) in coordination with WH
- Framework for public-private collaboration on R&D projects for the FS
- Initial projects
  - High Assurance Domains (e.g., DNSSEC)
  - Identity Management

Partnership for Cybersecurity Innovation

Today, Obama Administration officials released a Memorandum of Understanding signed by the National Institute of Standards and Technology (NIST) of the Department of Commerce, the Science and Technology Directorate of the Department of Homeland Security (DHS S&T), and the Financial Services Sector Coordinating Council (FSSCC). The goal of the agreement is to speed the commercialization of cybersecurity research innovations that support our Nation’s critical infrastructures.

The agreement establishes a framework for collaboration between the public and private sectors as directed by President Obama in his cybersecurity policy address.

“We will collaborate with industry to find technology solutions that ensure our security and promote prosperity.”

- President Obama, May 20, 2009

Financial services—banking and credit card transactions, insurance, trading and funds management, and many other business and consumer financial activities—are increasingly provided online. These services are essential in the daily lives of citizens, critical for the fast-paced conduct of modern business, and required for the healthy pulse of e-commerce, locally and globally. As a result, threats to these services are threats to individuals, companies, and the Nation. Ensuring these online services are reliable, accurate, safe, and secure against threats is a shared responsibility of the public and private sectors alike. Many of the innovations arising from this partnership will extend beyond financial services to online health services, the Smart Grid, and the Nation’s water, transportation, and other critical infrastructures.

This agreement will accelerate the deployment of network testbeds for specific use cases that strengthen the resiliency, security, integrity, and usability of financial services and other critical infrastructures’ functions, processes, and people by:

1. Facilitating coordination and cooperation among Federal agencies and the financial services sector in the development and delivery of innovative cybersecurity technologies and processes; and
2. Establishing testbed processes for the implementation of specific use cases.
• **LOGIIC – Linking Oil & Gas Industry to Improve Cybersecurity**
  – http://www.logiic.org

• A collaboration of oil and natural gas companies and DHS S&T to facilitate cooperative research, development, testing, and evaluation procedures to improve cyber security in Industrial Automation and Control Systems.
  – Consortium under the Automation Federation

• Industry determines the R&D projects and then government, industry, and partners help them execute the projects and promote the results to the rest of the sector
  – Raising awareness for the whole community
Electric Sector - TCIPG

• TCIPG – Trustworthy Computing Infrastructure for the Power Grid
  – Drive the design of an adaptive, resilient, and trustworthy cyber infrastructure for transmission & distribution of electric power
    • Protecting the cyber infrastructure
    • Making use of information to detect/respond to attacks
  – Support the provisioning of a new resilient “smart” power grid that
  – Advisory Board of 30+ private sector companies
Registration open for 2011 TCIPG Summer School on Cyber Security for Smart Energy Systems

The 2011 TCIPG Summer School will explore the nexus between electrical energy systems and cyber security. Power industry practitioners, researchers, and graduate students are invited to join us June 13-17, 2011 at the Q Center in St. Charles, Illinois.

Congressional Briefing on Power Grid Infrastructure Security and Resiliency

The University of Illinois has been invited to brief Congress on Power Grid Infrastructure Security and Resiliency: Protecting Critical Assets. Faculty from the TCIPG Center will discuss the challenges of protecting our nation’s power grid and the important research being conducted to make the power grid infrastructure more secure, resilient, and safe.
Analysis of Impacts of Smart Grid Resources on Economics and Reliability of Electricity Supply

Objectives

• Investigate the impacts of wind generation (WG) and demand response (DR) resources on the economics and reliability of power systems.
• Analyze the interplay between volatile WG and various types of DR.
• Develop models for planning and policy analysis so as to facilitate the integration of such resources into future power grids.

Recent Achievements

• Developed a stochastic unit commitment model for systems with integrated WG and DR resources.
• Preliminary simulation results provide a proof of concept that DR-based reserve capacity is a cost-effective mechanism to counter the volatility and uncertainty of WG. Also, studies indicate that load leveling can prove beneficial for systems with wind generation.

11 April 2011
Testbed-Driven Assessment: Experimental Validation of System Security and Reliability

Objectives

• To develop methods and tools for evaluating security mechanisms for next-generation power grid.
• Test-developed methods and tools on real or close-to-real power equipment.

Recent Achievements

• Set up the environment to emulate credential-stealing incident and corresponding detection mechanism in the testbed.
• Designing and setting up an example substation network using actual substation equipment.
Project Objectives

- Link researchers, educators, consumers, and students.
- Develop pedagogically and technologically sound curriculum materials relating math and science to power, energy, and cyber communication issues and utilize these materials to connect with middle and high school teachers and students.
- Create interest in STEM disciplines and careers.
- Illustrate issues necessary for consumer acceptance and use of smart grid technologies.

Advanced metering technologies allow two-way communication between the utility and the consumer.

tcipg.mste.illinois.edu
Our Education Problem

Problem: The U.S. is not producing enough computer scientists and CS degrees

- CS/CE enrollments are down 50% from 5 years ago\(^1\)
- CS jobs are growing faster than the national average\(^2\)

Computer Science/STEM have been the basis for American growth for 60 years
The gap in production of CS threatens continued growth and also national security
Defense, DHS, CNCI and industry all need more CS and CE competencies now

---

• National Cybersecurity Awareness (Lead: DHS).
  – Public service campaigns to promote cybersecurity and responsible use of the Internet

• Formal Cybersecurity Education (Co-Leads: DoEd and OSTP).
  – Education programs encompassing K-12, higher education, and vocational programs related to cybersecurity

• Federal Cybersecurity Workforce Structure (Lead: OPM).
  – Defining government cybersecurity jobs and skills and competencies required.
  – New strategies to ensure federal agencies attract, recruit, and retain skilled employees to accomplish cybersecurity missions.

• Cybersecurity Workforce Training and Professional Development (Tri-Leads: DoD, ODNI, DHS).
  – Cybersecurity training and professional development required for federal government civilian, military, and contractor personnel.
Toward a Federal Cybersecurity Research Agenda: Three Game-changing Themes
A Roadmap for Cybersecurity Research

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

- Scalable Trustworthy Systems
- Enterprise Level Metrics
- System Evaluation Lifecycle
- Combatting Insider Threats
- Combatting Malware and Botnets
- Global-Scale Identity Management
- Survivability of Time-Critical Systems
- Situational Understanding and Attack Attribution
- Information Provenance
- Privacy-Aware Security
- Usable Security
Summary

• Many USG efforts focused on securing critical infrastructures for the future

• DHS S&T continues with an aggressive cyber security research agenda
  – Looking at future R&D agendas with the most impact for the nation, including education

• Need to continue strong emphasis on technology transfer and experimental deployments
Cyber Disruption Efforts
In Rhode Island

Theresa C. Murray
Regional Catastrophic Planner
Rhode Island Emergency Management Agency
National Incident Management System (NIMS)

- NIMS provides a consistent nationwide template to enable:
  - federal, state, tribal and local governments, nongovernmental organizations and the private sector to work together to prevent, protect against, respond to, recover from and mitigate the effects of incidents
Guide for State’s All Hazards Response

- Revision began in 2009
  - Emergency Support Function #2, Communications
    - Coordination with telecommunications and information technology industries
    - Protection, restoration, and sustainment of cyber and information technology resources
Rhode Island Cyber Disruption Support Annex

- Outlines organizations, actions, and responsibilities
- Coordinated approach to protect against, prepare for, respond to, and recover from cyber-related incidents
- Information systems critical to the state and/or national security or economy
Rhode Island Cyber Disruption Support Annex

- Identifies stakeholder roles and responsibilities
- Coordinates rapid identification, information exchange, response, and remediation
- Mitigates damage caused by malicious or unintentional disruption of cyber activity
Rhode Island Cyber Disruption Support Annex

- Framework may be utilized in any emergency with cyber-related issues including:
  - Significant cyber threats
  - Disruptions
  - Cyber attacks against state computer networks, critical infrastructure or information systems
Rhode Island Cyber Disruption Support Annex

- Awareness Briefings
  - Chambers of Commerce
  - Emergency Management Advisory Council
  - Private Businesses
  - Rhode Island Association of Emergency Managers
  - State and local governments
Rhode Island Cyber Disruption Response Team

- Rhode Island State Police, Computer Crimes Unit
  - Rhode Island Cyber Disruption Workshop, March 3
    - Higher Education, Defense Contractors, Financial Industry and Hospital Representatives
    - Identify Possible Team Members
    - Team Selection Meeting, April 14
Partners

- Rhode Island State Police, Computer Crimes Unit, Cyber Security Task Force
- Rhode Island Emergency Management Agency
- Rhode Island Office of the Governor
- Rhode Island Army National Guard
- Rhode Island Air Force National Guard
- Rhode Island National Guard
- Rhode Island Department of Information Technology
- Rhode Island Division of Public Utilities and Carriers
- Rhode Island State Fusion Center

- Rhode Island State Department of Elementary and Secondary Education
- The University of Rhode Island, Digital Forensics Center
- Rhode Island State Agencies, Boards and Authorities
- Cox
- Full Channel
- Verizon
- Sprint/Nextel
- Tower Stream Wireless
- Information Systems Security Association

CYBERSECURITY SYMPOSIUM

Cyber Disruption Efforts in Rhode Island
Partners

- InfraGard
- Multi-State Information Sharing Analysis Center
- National Grid
- Northeast Power Coordinating Council, Inc.
- Ocean State Higher Education Economic Development and Administrative Network
- Providence Water Supply Board
- Federal Bureau of Investigation
- United States Attorney’s Office
  - Anti-Terrorism Advisory Council
- United States Coast Guard
- United States Department of Defense, National Guard Bureau
- USNORTHCOM
- United States Department of Homeland Security
- Cyber-terrorism Defense Initiative Integration Center
- National Cyber Security and Communications Security/Information Analysis and Infrastructure
- United States Computer Emergency Readiness Team
- United States Navy-Navy Emergency Preparedness Liaison Officer
- United States Secret Service, Electronic Crimes Task Force, Boston
Regional Catastrophic Grant Program

- Collaborative coordination and support in all phases of catastrophic incident prevention, preparedness, response, recovery and mitigation
  - Rhode Island, Massachusetts, New Hampshire
  - 34 local jurisdictions, including 2 Urban Area Security Initiatives (UASI)
Regional Catastrophic Grant Program

Cyber Disruption Efforts in Rhode Island
Regional Catastrophic Grant Program

- Regional Catastrophic Coordination Plan Cyber Disruption Annex
  - Addresses cyber disruption incident coordination and cooperation among Rhode Island, Massachusetts and New Hampshire
  - State Cyber Disruption Response Team Exercise, April 13
  - Regional Catastrophic Table Top Exercise, April 27
Rhode Island Cyber Resilience

- DHS Cyber Resilience Reviews
  - Conducted by Cyber Security Evaluation Program (CSEP)
  - Cyber review of an organization’s ability to manage cybersecurity
  - Designed to assist in constructive dialogue and cooperative improvement
  - Government and private industry stakeholders
  - Interview based assessment conducted in one day
  - CSE@hq.dhs.gov
Rhode Island Emergency Management Agency

Theresa C. Murray
Theresa.C.Murray@US.Amy.Mil
401-462-7336

CYBERSECURITY SYMPOSIUM

Cyber Disruption Efforts in Rhode Island
Understanding Cascading Failures in the U.S. Power Grid

Yan (Lindsay) Sun and Haibo He
Computer & Electrical Engineering
The University of Rhode Island
US Power Grid is Vulnerable

- Wall Street Journal (April 2009): Cyber spies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system,…
- An article in Nature (April 2010) demonstrated that cascading failures of two interdependent networks, the power grid and Internet communication network
An Example of Cascading Failures

Extremely Complicated Behavior of Power Grid

- Example: Blackout on August 14, 2003
  - 12:05:44 - Conesville Unit 5 (shutdown)
  - 1:14:04 - Greenwood Unit 1 (shutdown)
  - 1:31:34 - Eastlake Unit 5 (shutdown)

- Conesville plant is in central Ohio; Greenwood plant is north of the Detroit area; Eastlake Unit 5 is in northern Ohio.

→ spread to large portions of the Midwest and Northeast United States, with a total impacted area of about 50 million people and 61,800 megawatts (MW) of electric load.
Smart Grid, Smart Enough?

Understanding Cascading Failures in the U.S. Power Grid
Understanding Cascading Failures

- Attackers’ perspective: What is the best attack strategy?
Attack Strategies

- Traditional Attack Strategy
  - Attack nodes with the highest load

- New Metrics
  - Percentage-of-failure: The number of failed nodes divided the total number of nodes
  - Required Redundancy (RED): The minimum required system tolerance value such that cascading failure will not occur when one node is taken down
  - Risk if Failure (RIF): The risk of single-node failure in terms of causing cascading failure
Testing Results (I)

- New attack strategies are more dangerous

Western North American power grid network: 4941 nodes; 6594 transmission lines.

When the attacker use risk-based metric, they simply take down the node with largest RIF value, which is the optimal attack strategy.
Testing Results (II)

- Sequential Attack v.s. Non-sequential Attack
URI Innovations

- Attack Strategies

Understanding Cascading Failures in the U.S. Power Grid
Expected Outcomes

- **Defense:**
  - Smart Protection of the Smart Grid

- **Tools**
  - Test bed
  - Visualization Tools

Understanding Cascading Failures in the U.S. Power Grid
Panel Session 1: *Cyber Threats to Critical Infrastructure*

**Douglas Maughan**, Ph.D., Director, Cyber Security Division, Department of Homeland Security

**Theresa Murray**, Regional Catastrophic Planner, Rhode Island Emergency Management Agency – Topic: *Cyber Disruption Efforts in Rhode Island*

**Yan Sun**, Ph.D., Associate Professor, URI Department of Electrical, Computer, and Biomedical Engineering - Topic: *Understanding Cascading Failures in the U.S. Power Grid*

Panel Q & A
Lunch & Viewing of Student Cybersecurity Research Posters

Please return by 1pm
Panel Session 2: Cyber Forensics

Jeffrey Troy, Deputy Assistant Director, FBI Cyber Division - Topic: Cyber Threats and Responses

Daniel Dickerman, Special Agent, US Internal Revenue Service Criminal Investigation Electronic Crimes Program - Topic: The Evolution of Cyber Forensics

Alan White, Director of Network Security and Risk Consulting for North America, Dell/Secure Works Inc - Topic: Workforce Issues

Victor Fay-Wolfe, Ph.D., Professor, URI Department of Computer Science and Statistics – Topic: Cyber Forensics @ URI

Kevin Bryan, Ph.D. Candidate, URI Department of Computer Science - Topic: Research in Steganography Detection

Panel Q & A
“Short of armed conflict, nation-states are unlikely to launch cyber attacks against the United States. [...] The greatest threats remain espionage and cyber crime.”
Panel Session 2: Cyber Forensics

**Jeffrey Troy**, Deputy Assistant Director, FBI Cyber Division - Topic: *Cyber Threats and Responses*

**Daniel Dickerman**, Special Agent, US Internal Revenue Service Criminal Investigation Electronic Crimes Program - Topic: *The Evolution of Cyber Forensics*

**Alan White**, Director of Network Security and Risk Consulting for North America, Dell/Secure Works Inc - Topic: *Workforce Issues*

**Victor Fay-Wolfe**, Ph.D., Professor, URI Department of Computer Science and Statistics – Topic: *Cyber Forensics @ URI*

**Kevin Bryan**, Ph.D. Candidate, URI Department of Computer Science - Topic: *Research in Steganography Detection*

Panel Q & A
Cyber Threats and Responses

Jeffrey Troy
Deputy Assistant Director
FBI Cyber Division
Overview

- FBI Cyber Crime Program
- Cyber Threat Environment
  - Technical sophistication
  - Storage and processing capabilities
  - Increasing number of hackers
- Driving changes in forensics
  - More efficient processes
  - Better tools
FBI Cyber Division

- Threat focus strategy
- Highly cooperative
- Predictive and Preventative
Technical Sophistication

- More code + more vulnerabilities
- Porting of apps to multiple platforms
  - Mobile, desktop, tablet
  - Inherent flaws and adaptive flaws
- Encryption
- Zero Days
  - The white hat dilemma
- Kits
  - Zeus
  - Spy Eye
Capacity

- **Storage**
  - Low cost home storage
  - Virtual and cloud
    - Legal, jurisdictional, geographic issues
  - Devices with storage capacity
- **Processing**
  - Increased RAM capacity
  - RAM-based malware
  - Processing in the cloud – more processing power
Volume of Attacks

- Hactivists
  - Leaderless organizations - anonymous
- Global national security capability being developed by all nations
- Statistics
Improving Forensic Processes

- On-site triage
- Consolidation of analysis
  - Tool sharing, Malware Analysis Project
- Data sharing
  - Government -to- Government
  - Private -to- Private
  - Government -to- Private
Improving Forensics Tools

- MCARTA
- COTS
- FTK Imager
- After Life
The Evolution of Cyber Forensics

Daniel Dickerman
Technical Advisor & Director of Training
IRS Criminal Investigation, Electronic Crimes
My Background

- Career as IRS Special Agent in NY, GA, and RI (plus lot’s of time in DC)
- Have been using computers for 25+ years and doing forensics on them for the past 15 years.
  - Conducted thousands of Computer Forensic examinations
  - Developing courses & teaching Computer Forensics since 1999
- Currently manage the joint DHS/Treasury Computer Forensic Training Program
- Co-developed the URI Computer Forensic curriculum
In the Beginning…

…long before most individuals ever owned a computer, IRS had a need to capture, recover, and analyze digital evidence from business computer systems.
“Computer Forensics” is born

- Treasury Computer Investigative Specialist partnership was formed to share LE expertise & resources.
- Procedures & Tools are developed to: capture, search, recover, decrypt, analyze and authenticate digital evidence.
1980s – 1990s

- Primarily stand-alone computers
- Basic storage media
- Simple non-automated forensic tools
  - Manual analysis of very small amounts of data, with very slow computers and very simple tools….by today’s standards.
- Skills primarily within the LE community
Into the 21st Century

- Smarter automated Computer Forensic tools
- Faster computers
- Exponential growth in amounts of data to capture and analyze
- More complex data and software
- Strong encryption & full disk encryption
Evolving to “Digital Forensics”

- New technologies
  - Networks
  - Mobile Devices
  - Social Networking
  - Game Consoles
  - Etc.

- New tools & skills required
The Internet

- Social Networking
- Email
- Video/Voice over IP (Skype)
- Blogging (Twitter)

The possibilities (and forensic challenges) are endless…
Data in “The Cloud”

- Is Cloud Computing involved?
- Where is the active data & how do I get it?
- Jurisdiction?
- Historical data?
- Forensic remnants?
The APT

- Phishing
- Malware
- Hacking
- And so on…

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of $18.75. Please submit the tax refund request and allow us 5-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please [click here](https://www.irs.gov). Regards,

Internal Revenue Service

The Evolution of Cyber Forensics
Expanding to “Cyber Forensics”

- Digital evidence is no longer just “static” data
  - Real-time (live) acquisition and Analysis
- Analyze or just remediate?
- The challenge of finding the perpetrator or the evidence
  - Encryption
  - Anonymous proxies
  - Beyond jurisdictional boundaries
- Forensics will continue to evolve
  - Memory parsing
  - Wear leveling
  - Quantum computing
The Importance of Partnerships

- LE can’t do it alone
- Academic Partnerships
  - Development of academic programs (i.e. URI)
  - Industry research (i.e. ECTCOE)
- Cyber Security Partnerships
  - Professional Organizations
  - Private Industry
- Public Awareness & Education
Contact Info:

- S/A Daniel Dickerman
  - Technical Advisor & Director of Training
  - IRS Criminal Investigation, Electronic Crimes
  - Email: daniel.dickerman@ci.irs.gov
  - Phone: (401) 826-4731
Cyber Security and Forensics
Workforce Issues

Alan J. White, CISSP, GCIA, CEH, CISA, CCE, GCIH
Director of Security and Risk Consulting, North America
Dell/SecureWorks

CYBERSECURITY SYMPOSIUM
My Background

Previous and Other Roles

- **US Army Major**
  - Computer Emergency Response, Team Chief  RI Army National Guard
  - Special Forces Battalion, Signal Officer

- **Information Security Architect**
  - University of Rhode Island

- **Adjunct Faculty**
  - University of Rhode Island
  - Roger Williams University

- **Alumni BS Computer Science Department**
  - University of Rhode Island
Partnerships and Relationships

- Microsoft Active Protections Program (MAPP)
- Forum of Incident Response & Security Teams (FIRST)
- Financial Services Information Sharing and Analysis Center (FS-ISAC)
- Internet Security Alliance (ISA)
- Internet Systems Consortium (ISC)
- SANS Institute
- Zero Day Initiative (ZDI)
- Anti-Phishing Working Group (APWG)
- USSS ECTF
- FBI & FBI Citizens’ Academy
- Department of Defense
- Department of Energy
- InfraGard
- NATO
- Interpol
- CyberCop Secure Information Exchange Network
- Federal Trade Commission
- Cyber Security Forum Initiative (CSFI)
- National Cyber-Forensics & Training Alliance (NCFTA)

Cyber Security and Forensics Workforce Issues
Industry Threats

Elite Security Hackers

- Focused on
  - Malware creation
  - Cyber espionage
  - Exploit research
  - Hactivistism
  - Cybercrime
  - Financial laundering
  - Botnet Herders
Industry Threats

Adversary Computer Network Exploitation Infrastructure

- Web Hosting Compromise
- Stage 2 Exploit Sites
- Data Collection
- Command and Control
- Open Mail Relay/Web Mail
- Botnet Peer/Relay
- Spear Phishing
- USB Storage Device

- Adversaries
- Hop Points

- Malware.exe
- Victim Host
- Spear Phishing And Worms
- Open Relay Discovery and Web Mail Manipulation
- Botnets and Fast Flux Networks

- SQL and IFRAME injection
- Exploit Creation Kits
- Data Exfiltration
- Data Exfiltration

- Drive-By Exploits Payload
- Open Mail Relay/Web Mail
- Botnet Peer/Relay

- Cyber Security and Forensics
- Workforce Issues
Industry Threats

Cyber Security and Forensics Workforce Issues
Industry Threats

XLSTrojan uses Google Code for Command and Control

1. APT creates Google Account in order to create Google Code Project
2. APT actor creates Google Code Project
3. Most likely APT actor crafts Targeted Phishing Attack w/ XLSTrojan
4. Victim opens phishing payload and infected by XLSTrojan
5. Trojan checks into Project site; receiving updated configuration
6. Trojan instructed to find and exfiltrate specific data to various “Drop Sites”
7. APT actor retrieves exfiltrated data from various “Drop Sites”
Industry Threats

Operation Payback DDoS Campaign, or the “WikiLeaks War”
Industry Threats

ACH/Wire Fraud

- Focused on threat analysis and threat intelligence:
  - 1-4 victims/day
  - Avg. take $100,000/victim
  - $500K – $1Mil/week
  - $100Mil attempted in 2009
  - $40Mil+ unrecovered
  - > All US bank robberies combined

- ALL done by ONE E. European crew
Industry Needs

Elite Security and Intelligent Workforce

- Focused on threat analysis and threat intelligence:
  - Malware analysis
  - Countermeasure development
  - Reverse engineering
  - Counter intelligence
  - Forensics
  - Threat modeling
  - Trending and statistical analysis
  - Researchers
Industry Needs

Just one point of visibility

- Dell SecureWorks - CTU Facts
  - 25,000 malware specimens / day
  - Monitoring ~60 Botnets
  - ~40 vulnerabilities / business day
  - 1,000’s security events of interest / day
  - 10,000’s intelligence artifacts processed a day
  - 2,800 clients attacked / day
  - ~7,000,000 IP addresses of attackers detected / year
Industry Needs

Cloud Security

- Biz Process/Operations
- Application Development
- IT Infrastructure/Operation

- App/Svc Usage Scenarios
- Develop, Test, Deploy and Manage Usage Scenarios
- Create/Install, Manage, Monitor Usage Scenarios

- Service Layer
  - SaaS
  - PaaS
  - IaaS

- Resource Abstraction and Control Layer
- Physical Resource Layer
  - Hardware
  - Facility

- Cloud Provider

Cyber Security and Forensics Workforce Issues
Summary

Fighting the Good Fight

- Industry Threats Increasing
- Industry Needs Increasing
- What we do is important!
- Goal is to make the cost of doing business for the hackers go up!
- Universities offer the next generation of industry experts!
Cyber Forensics @ URI

Victor Fay-Wolfe, PhD
Professor, Department of Computer Science
Director, Digital Forensics Center
University of Rhode Island
URI Digital Forensics Program

- URI is one of the leading digital forensics programs in the country
- URI had the first degree programs in digital forensics through a computer science department at a major university
- URI Digital Forensics Center is the only working digital forensics lab on a campus integrated with the academic program
- URI DFC has the most funding in digital forensics research of any university nationwide
URI Teaching in Digital Forensics

- **Academic Program**
  - One of the first in the country
  - Funded by National Science Foundation Cyber Security Capacity Building Program
  - Patterned after Federal Law Enforcement Training Center curriculum (Dan Dickerman)
  - Delivered online

- **University Courses**
  - Computer Forensics
  - Network Forensics
  - Advanced Forensics
  - Network Security

- **Degrees**
  - Undergrad minor
  - Graduate Certificate
  - MS & PhD

- **Training**
  - Professional Certificate
  - RI Police first responders
  - RI Cyber Security
  - Advanced topics for RI-area law enforcement

- **Internships**
  - RI State Police
  - Naval Criminal Investigative Service
  - Federal agencies
  - Local Police
  - Local companies
  - URI Digital Forensics Center
  - National Science Foundation REU in Digital Forensics @ URI
URI Digital Forensics Center

- **Facilities**
  - On-campus lab
  - Forensic acquisition hardware and software
  - Evidence and storage data center
  - Law enforcement quality procedures
  - Staff, faculty, student interns

- **Funding**
  - Congressional earmark
  - Non-profit center charges for services

- **Services**
  - Digital evidence analysis for lawyers and companies
  - Student interns learn by working cases

- **Consulting**
  - Designed and implemented RI State Police Computer Crime lab
  - Lead partner to the U.S. National Institute of Justice Electronic Crimes Technology Center of Excellence
    - Conducting nationwide needs assessment study
    - Performing cell phone analysis tool study
URI Digital Forensics Center Cases

- Political corruption
  - Back door to town computer system

- Suicide
  - Suicide web sites, email from girlfriend

- Murder
  - Who did he know, who was he talking to?

- School sexual assault
  - IMs posted on Live Journal, edited?

- School teacher inappropriate computer use
  - Pornography on the computer – who put it there? Simply spam?

- Divorce
  - Infidelity shown in emails

- Corporate Espionage
  - Company data to competitor – how did it get there?

- Stalking
  - Physical evidence of stalking, emails confirm?
RI State Police Support

- URI DFC designed and built RI State Police Computer Crimes Lab
  - Innovative design being considered as a national model
- URI DFC partner with RI State Police and RI FEMA on Cyber Terrorism Task Force and Strike Force
- URI DFC Staff resident at RI State Police Computer Crimes Lab
- RI State Police first civilian analyst in computer crime hired from URI DFC
URI Research

- Real world case work yields real research problems
- Funded by the U.S. Dept of Justice and U.S. National Science Foundation
- Example current research projects
  - Child pornography detection
  - Data Security
  - Cloud Forensics
  - Steganography detection

Research posters on display in the lobby
Commercial/Workforce Transitions

- Research transitioned to commercial products that are tools in wide-spread use in forensics and security. Examples:
  - URI Data security patent to Trap Data Group
  - URI Software write blocking and forensics tools to ForensicSoft
  - URI Steg detection techniques and software to Wetstone Technologies
  - URI Search String support and RedLight (porn scanner) tool to ECTCoE

- URI graduates are in key positions in forensics and network security
New URI Cyber Security Center

- Establish URI Cyber Security Center
- Leverage strength in digital forensics program
- Create integrated cyber security program
  - Teaching and professional training
    - Courses/degree programs
    - Workforce development
  - Service
    - Community cyber security education and support
      - You’re only as strong as your weakest link
    - State Cyber Terrorism Strike Force
  - Research
    - Critical infrastructure protection
    - Trust-based cyber security
- Many pieces in place – initial steps toward URI Cyber Security Center this year
Dr. Victor Fay-Wolfe
University of Rhode Island
Director, Digital Forensics Center
wolfe@cs.uri.edu

http://dfc.cs.uri.edu

URI Digital Forensics Program

Teaching  Service  Research
Steganalysis:
Detecting Hidden Evidence in Digital Media Files

Kevin Bryan
PhD Student
Department of Computer Science
University of Rhode Island
Threat

- Steganography
  - Hides a message “in plain sight”
  - Looks like normal communication
  - Obscures Sender/Recipient
  - Free, easy to use programs

- Example uses:
  - Stolen credit card numbers
  - Foreign Intelligence
  - Trade secrets
An Example

- Which of these flowers has a hidden message in it?
How is Image Data Stored?

- Could be just color values
- JPEG/MPEG use DCT transform to reduce data size
- Performed on blocks of 8x8 pixels

```
-12  4  0  0  0  0  0  0  0  0  0  0  0  0  0  0
 18 -2  0  1 -2  0  0  0  0  0  0  0  0  0  0  0
  0 -4 -2 -2  0  0  0  0  0  0  0  0  0  0  0  0
- 3  0  1  1  0  0  0  0  0  0  0  0  0  0  0  0
- 2  2  0  0  0  0  0  0  0  0  0  0  0  0  0  0
  2  0 -2  0  0  0  0  0  0  0  0  0  0  0  0  0
  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
```

```
-41  0  0 -2  0  0  0  0  0  0  0  0  0  0  0  0
  4  1  0 -1  0  0  0  0  0  0  0  0  0  0  0  0
  2  1  0 -2  0  0  0  0  0  0  0  0  0  0  0  0
  2  1  0  0  0  0  0  0  0  0  0  0  0  0  0  0
  0  1  0  0  0  0  0  0  0  0  0  0  0  0  0  0
  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
```
Image Steganography

- Changing the DCT values by ±1 does not significantly alter the look of the image.

![Image before and after DCT value change](image.png)
Steganalysis

- Various statistics of the DCT coefficients can give an indication of embedding
  - Distribution of values
    - Globally in the image
    - In particular DCT modes
  - Distributions of pairs of values
    - Across blocks
  - Difference of values between blocks
Video Steganalysis

- Similar to Images
- More data to work with
  - Each frame of video is an image
- Can exploit data self-similarity to make detection easier
  - Consecutive images in video are highly correlated
Steganalysis - Steps

- Preprocessing:
  - Embed images with steg tool
  - Collect stats from clean and steg file
  - Build a statistical model of the data

- For investigation:
  - Collect statistics from “suspect file”
  - Use the model to predict stegged or not
    - Can approximate amount of data embedded
Impact

- Detect steg with >95% accuracy down to 20% embedding rate
- Effectively requires 5 times the overhead for the same amount of "hidden data"
- Transitioned JPG and MP3 detection engine to Wetstone Technology's StegoSuite product
Panel Session 2: Cyber Forensics

Jeffrey Troy, Deputy Assistant Director, FBI Cyber Division - Topic: Cyber Threats and Responses

Daniel Dickerman, Special Agent, US Internal Revenue Service Criminal Investigation Electronic Crimes Program - Topic: The Evolution of Cyber Forensics

Alan White, Director of Network Security and Risk Consulting for North America, Dell/Secure Works Inc - Topic: Workforce Issues

Victor Fay-Wolfe, Ph.D., Professor, URI Department of Computer Science and Statistics – Topic: Cyber Forensics @ URI

Kevin Bryan, Ph.D. Candidate, URI Department of Computer Science - Topic: Research in Steganography Detection

Panel Q & A
Panel Session 3: Network Security and Trust

Peiter "Mudge" Zatko, Program Manager, Information Innovation Office, DARPA -
Topic: Analytic Framework for Cyber (digest)

Marcus H. Sachs, P.E., Vice President of Government Affairs for National Security Policy, Verizon - Topic: Lessons Learned from Large Data Breach Investigations

Yan Sun, Ph.D., Associate Professor, URI Department of Electrical Engineering – Topic: Theoretical Foundation of Building Trust in Distributed Networks

Lisa DiPippo, Ph.D., Associate Professor, URI Department of Computer Science and Statistics - Topic: Utilizing Trust to Secure Wireless Routing Protocols

Yuhong Liu, Ph.D. Candidate, URI Department of Electrical Engineering – Topic: Safety Assurance of Neural-controlled Artificial Legs

Panel Q & A
Analytic Framework For Cyber (digest)

Peiter “Mudge” Zatko
Program Manager
Information Innovation Office
DARPA

PowerPoint slides are not available for this speaker
Lessons Learned from Large Data Breach Investigations

Marcus H. Sachs, P.E.
Verizon
Marcus.sachs@verizon.com

PowerPoint slides are not available for this speaker please refer to this complete report for information: http://www.verizonbusiness.com/databreach
Theoretical Foundation of Building Trust in Distributed Networks

Prof. Yan (Lindsay) Sun
Computer Engineering
University of Rhode Island
Trust in Cyber Space

- Trust
  - A well studied concept in sociology and psychology.
  - Known as the **driving force** for collaboration in social communities.

- Distributed computing and communication system
  - Examples: networked sensors, cognitive radios, cyber-physical systems, and online social networks
  - Rely on **collaboration** among network participants.
Trust and Security

- When network participants do not know how to trust each other, network operations suffer.
- Participants that naively trust will be victimized.
- Mistrustful participants will ignore opportunities and their resources will be wasted because of inefficiency.
The Role of Trust (I)

Prediction and Diagnosis

When a network entity establishes trust in other network entities, it can *predict* others' future behaviors and *diagnose* their security properties.
The Role of Trust (II)

Simplification and Abstraction

- The design of many network protocols and applications must consider the possibility that some participants will not follow the protocols honestly.
- Currently, this issue is considered by individual protocols or applications
  - Repetitive monitoring, high complexity, non-compatibility
- Ideally, a trust infrastructure can help to Integrate piecemeal defense solutions
The Role of Trust (III)

Integrating Social Needs into System Design

“The most vexing security problems today are not just failures of technology, but result from the interaction between human behavior and technology”

Trust-based Solutions do not replace traditional security services, such as data integrity, confidentiality, authentication, etc.
Research Overview (I)

- Theoretical Foundations
  - What is Trust?
  - How to quantitatively evaluate trustworthiness?
  - Mathematical properties of trust values?
  - Is trust evaluation vulnerable to attacks?
Research Overview (II)

- Trust-based Security Solutions
  - Wireless Networks: securing routing, time synchronization, etc.
  - Biomedical Systems: user safety assurance
  - Social Computing: dishonest information sources (human users)
Research Overview (III)

- Analysis and Evaluation Tools
  - Which trust model is better in what circumstances?
  - How real users will attack trust evaluation?
Our Trust Management System

<table>
<thead>
<tr>
<th>Trust Record</th>
<th>direct</th>
<th>indirect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Relation type 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust Relation type 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>........</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Definition**
Quantitative Representation

**Record Maintenance**
- Initialization
- Update according to time
- Update according to records relationship
- Adjustment of forgetting factor

**Trust Establishment**
- Update direct recom. trust
- Calculate indirect Trust
- Update direct action trust
- Generate Trust Graph

**Malicious Node Detection**

**Trust Request Management**
- Process query from local applications
- Process other nodes' recom. query
- Request for Recom and Process replies

**Applications that provide observations**

**Network communication components**

**Local applications**

Theoretical Foundation of Building Trust in Distributed Networks
Attacks Against Trust Management

- Example 1: **Bad mouthing attack**: malicious nodes providing dishonest recommendations.
- Example 2: **On-off attack**: malicious nodes behave well and badly alternatively in time domain.
- Example 3: **Conflicting behavior attack**: malicious nodes behave well to one group of users and behave badly to another group of users.
- More Advanced Attacks: **RepTrap** etc.
Preview of Student Posters

Under the supervision of URI Cyber Security Team:

- **Cross-layer concept**

- **Wireless Network Security**
  - [Poster] Dynamic Sliding Window against On-Off attack

- **Security & Human Factors**
  - [Poster] Securing Reputation Systems in the Cyber Space
  - [Poster] Secure Smart-Phone Based Campus Reporting System
Utilizing Trust to Secure Wireless Routing Protocols

Lisa DiPippo, Computer Science
Yan Sun, Computer Engineering
mZeal Communications, Inc.
Overview

- Wireless sensor networks
- Security issues in WSNs
- Trust applied to routing
- Impact of the work
- How it fits into Cybersecurity program at URI
Wireless Sensor Networks

- Network of sensors collecting data
- Send data to base station wirelessly
- Devices have constraints
  - Small
  - Low-power
  - Low cost
- Applications
  - Habitat monitoring
  - Military surveillance
- Routing based on distance
Security Issues in WSN Routing

- Encryption only handles data confidentiality
- Attacks on routing
  - Imitating valid node (a)
  - Redirecting transmission (b)
  - No forwarding (c)
  - Selective forwarding (d)
Tusting Routing for WSNs

- Various types of trust for different behaviors
  - Forwarding trust
  - Reporting trust
  - Predictability trust

- Overall trust
  - Combination of all trust metrics

- Routing decision
  - Based on trust and distance
Impact and Future Work

- Assurance of delivery of critical and sensitive data in WSNs
- Detection of sophisticated attacks on routing
  - *Dynamic Sliding Windows* poster outside
- Application of trusted routing to other types of networks
  - Autonomous Systems – attacks on transmission of data
- Application of trust to any type of system where behaviors can be monitored
URI Cybersecurity Program

- Trust is unique feature of cybersecurity research at URI
- Applied to various areas
  - Posters outside
  - Yuhong Liu’s talk coming up
- Foundation of research piece of Cybersecurity Center
- Combine with teaching and service
Safety Assurance of Neural-Controlled Artificial Legs

Yuhong Liu, Yan (Lindsay) Sun
Department of Electrical, Computer and Biomedical Engineering
University of Rhode Island
Challenge: Safety Assurance

Sensor failures, Disturbance, .... Errors in user intention identification Tumble, Fall, Injury

Safety Assurance of Neural-Controlled Artificial Legs

CYBERSECURITY SYMPOSIUM
Trust Sensor Interface (TSI) - Approach

- Abnormal Detector
- Sensor Level Trust Evaluation
- System Level Trust Evaluation

Safety Assurance of Neural-Controlled Artificial Legs
Demonstration

- TSI for Subject sitting and standing
Panel Session 3: Network Security and Trust

Peiter "Mudge" Zatko, Program Manager, Information Innovation Office, DARPA - Topic: Analytic Framework for Cyber (digest)

Marcus H. Sachs, P.E., Vice President of Government Affairs for National Security Policy, Verizon - Topic: Lessons Learned from Large Data Breach Investigations

Yan Sun, Ph.D., Associate Professor, URI Department of Electrical Engineering – Topic: Theoretical Foundation of Building Trust in Distributed Networks

Lisa DiPippo, Ph.D., Associate Professor, URI Department of Computer Science and Statistics - Topic: Utilizing Trust to Secure Wireless Routing Protocols

Yuhong Liu, Ph.D. Candidate, URI Department of Electrical Engineering – Topic: Safety Assurance of Neural-controlled Artificial Legs

Panel Q & A
Arthur W. Coviello, Jr., Executive Vice President, EMC Corporation & Executive Chairman, RSA, The Security Division of EMC
Closing Remarks

James Langevin, U.S. Congressman