CyberSci Summit 2015

October 14-15, 2015 | Fairfax, Virginia | ICF International Conference Center

Proceedings Report

January 2015

icfi.com

Table of Contents

Contact

cybersci@icfi.com

Introduction

This document summarizes ICF International's CyberSci Summit 2015, the theme of which was "Resilience: Survival and Recovery in an Age of Cyber Weapons." The summit brought together experts from industry, government, and academia to share the important developments in cyber security research and development (R&D). The event took place October 14 and 15 at ICF's headquarters in Fairfax, VA.

The summit's agenda is provided, along with summaries of the keynote speeches and recaps of the breakout sessions. Copies of available individual presentations may be requested by contacting cybersci@icfi.com.

Executive Summary

Building on the success of its three previous predecessor events, CyberSci Summit 2015 brought together industry, government, and academia for a unique gathering. Designed with size and scope to foster the sharing of ideas, the summit allowed participants to interact and build on those shared ideas together, both in real-time and upon return to their respective institutions.

Four keynote speakers addressed the shared cyber security context for all participants. Twenty-six breakout sessions offered in-depth information about issues facing the cyber security R&D and about current research and development work.

In his opening remarks, ICF International Senior Vice President and General Manager, Cyber security, Samuel Visner gave an overview that touched on key points that later presenters would revisit:

- IT Infrastructure—changes are happening quickly and concurrently, often connecting enterprise and cloud resources. Cloud orchestration causes IT workloads to move from infrastructure to infrastructure as cloud processes and infrastructure become commoditized.
- Mobility—convenience has driven a cultural shift, and users now expect the ability to be untethered.
- Target Surface—when the need to protect industrial control systems and the implications of IPv6 are considered, the global attack surface is growing exponentially.
- Privacy vs. Security—balancing these two forces is an overwhelming issue for lawmakers.
- Attacker Capabilities—cyber criminals are increasingly informed with resources and capabilities that previously had been restricted to state-level players.
- Behavioral Norms—our thinking must shift to an understanding that cyber threats are not going away. State players must have offensive and defensive expectations.

Keynote Presentation Summaries

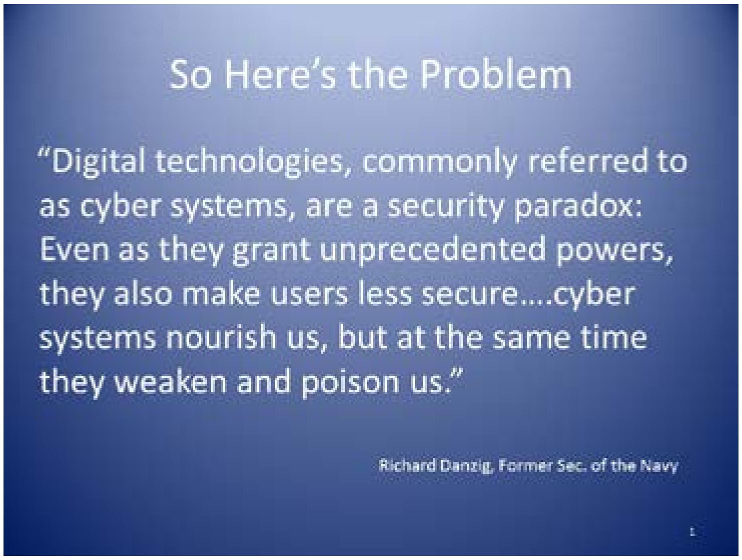
Cyber Security: Why Is This (Still) So Hard?

General Michael Hayden, Former Director, Central Intelligence Agency;
U.S. Air Force, Retired

General Michael Hayden

General Hayden presented cyber security in a broader context to illustrate the growing importance of setting boundaries and defining the bigger issues we are trying to solve. He reviewed the evolution of the Internet from its initial purpose in academia to the fully integrated "fifth domain" we rely on in every aspect of our lives. Among General Hayden's key points:

- Cyber systems "feed" us as never before, replacing the trained individuals and institutions upon whom we used to rely.
- "Cyber" is officially recognized as the fifth domain of warfare: land, sea, air, space, and cyber.
- The Internet was built for speed, scale, and ease of use. Security was not a consideration.
- Corrupting information is more of a concern than is destroying it.
- Cyber crime trend is moving toward more destructive acts.
- Cyber criminals include nation states, criminal gangs, and "hactivists," but the lines blur as some may act in the service and sponsorship of others.
- Our government has been late to need for cyber security because we still need clarity around some big ideas. Our government will be permanently late to need because of political and cultural pressures, especially around privacy.
- Considering the traditional risk equation R=T x V x C, where R=Risk, T=Threat, V=Vulnerability, and C=Consequence. We have focused historically on V. Now we are more focused on resilience to C. In the future our focus should shift to T.
- We need intelligence about specific threats because applying abstract defenses to every abstract threat will become even more impossible.
- Cyber insurance is a growing field that may drive improvement of cyber security by imposing standards baked into its business model.

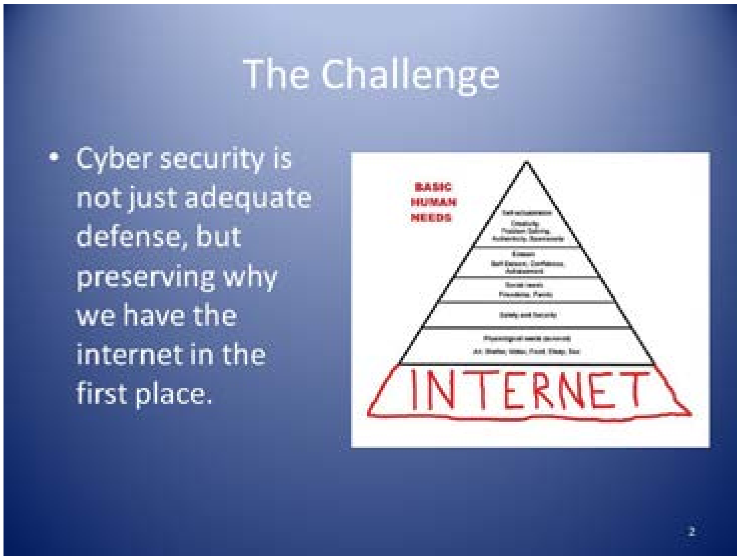


So Here's the Problem

"Digital technologies, commonly referred to as cyber systems, are a security paradox: Even as they grant unprecedented powers, they also make users less secure....cyber systems nourish us, but at the same time they weaken and poison us."

Richard Danzig, Former Sec. of the Navy

1



The Challenge

- Cyber security is not just adequate defense, but preserving why we have the internet in the first place.

BASIC
HUMAN
NEEDS
Self-actualization
Creativity
Problem Solving
Authenticity, Spontaneity
Esteem
Self Esteem, Confidence, Achievement
Social needs
Friendship, Family
Safety and Security
Physiological needs (survival)
Air, Shelter, Water, Food, Sleep, Sex
INTERNET

2

- Our security solutions cannot undermine the overriding purpose of the Web: free movement of ideas.

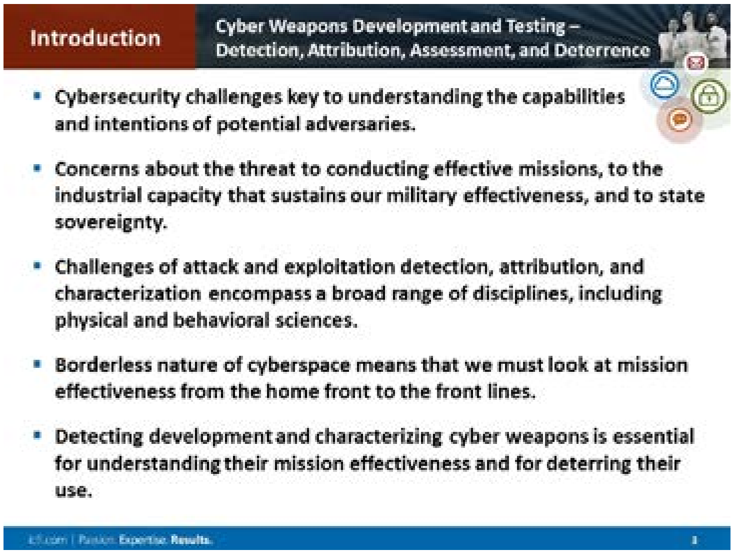
Cyber Weapons Development and Testing—Detection, Attribution, Assessment, and Deterrence: An Important Challenge to R&D Community

Samuel Visner

Samuel Visner, Senior Vice President and General Manager, Cyber Security, ICF International

Samuel (Sam) Visner emphasized how reliable detection and accurate characterization of foreign cyber weapons development and testing represent key cyber security challenges that will be important to understanding the capabilities and intentions of potential adversaries. These challenges must be met to assess real or intended effects on mission effectiveness as well as to help us understand what responses are appropriate for such attacks and how, if possible, to deter them. Work in the physical and behavioral sciences is required. Among the key points Mr. Visner presented:

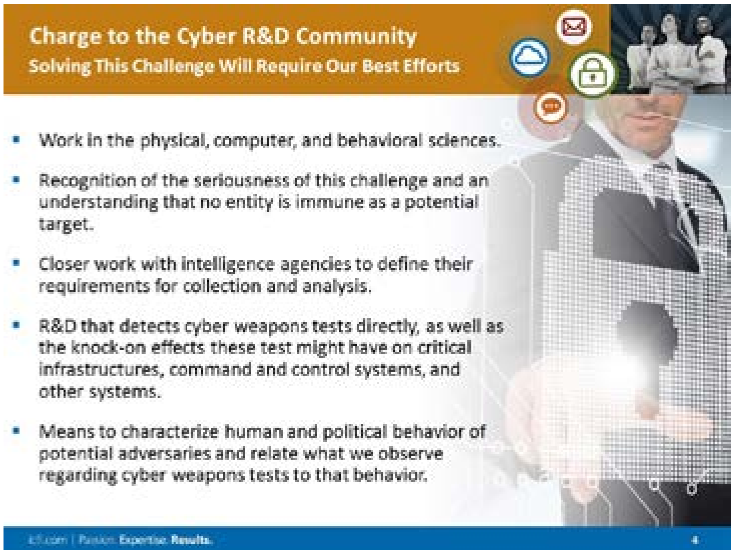
- We can look to nuclear deterrence as a model for deterrence: Would it really work and how much from that model would apply? Barriers to entry certainly are much lower in the cyber domain.
- The need for transparency among actors in the international system was demonstrated during the Cuban Missile Crisis. Does that transparency exist for cyber?
- Sony is a good example of what weapons testing actually looks like—effectively demonstrating the existence of capabilities with little fear of retribution.
- Distinguishing weapons testing from actual use of force could be difficult.
- We must understand our networks well enough to recognize anomalous behavior.
- If we equate the today's cyber situation to the Cuban Missile Crisis and nuclear era, much work must be done in the social and physical sciences. This work begins with recognition of the vastness of the requirement.
- We are moving toward a normative state in which cyber security is considered a cost doing business among nations.


Introduction

Cyber Weapons Development and Testing – Detection, Attribution, Assessment, and Deterrence

- Cybersecurity challenges key to understanding the capabilities and intentions of potential adversaries.
- Concerns about the threat to conducting effective missions, to the industrial capacity that sustains our military effectiveness, and to state sovereignty.
- Challenges of attack and exploitation detection, attribution, and characterization encompass a broad range of disciplines, including physical and behavioral sciences.
- Borderless nature of cyberspace means that we must look at mission effectiveness from the home front to the front lines.
- Detecting development and characterizing cyber weapons is essential for understanding their mission effectiveness and for deterring their use.

icf.com | Passion. Expertise. Results. 3


Charge to the Cyber R&D Community

Solving This Challenge Will Require Our Best Efforts

- Work in the physical, computer, and behavioral sciences.
- Recognition of the seriousness of this challenge and an understanding that no entity is immune as a potential target.
- Closer work with intelligence agencies to define their requirements for collection and analysis.
- R&D that detects cyber weapons tests directly, as well as the knock-on effects these test might have on critical infrastructures, command and control systems, and other systems.
- Means to characterize human and political behavior of potential adversaries and relate what we observe regarding cyber weapons tests to that behavior.

icf.com | Passion. Expertise. Results. 4

- Advances in technology could enhance our security, but they also could represent new vulnerabilities.

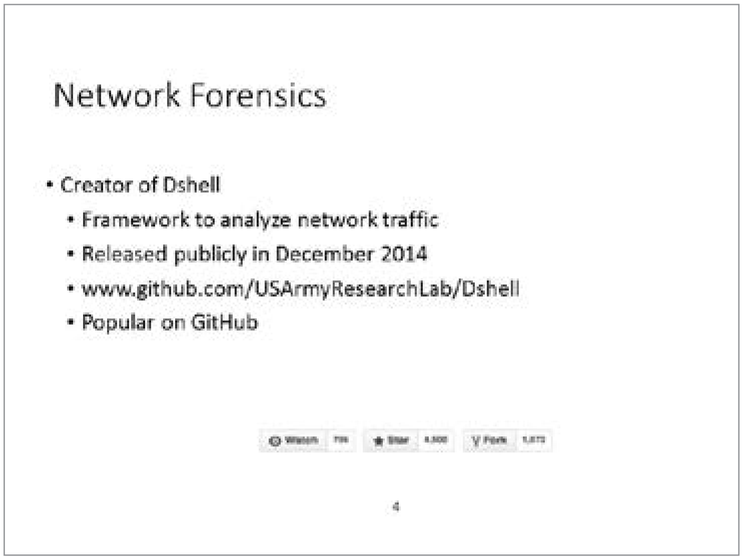
Transitioning Cyber Security Research

William J. (Billy) Glodek, Former Network Security Branch Chief, U.S. Army Research Laboratory

William J. Glodek

Mr. Glodek brought focus to basic and applied research in some specific areas of cyber protection and the importance of transforming "raw data into actionable information for analysts and decision makers." His expertise in network forensics, threat analysis, and machine learning led to the development and sharing of Dshell, the most popular U.S. Department of Defense (DoD) open source tool in existence. Key points from Mr. Glodek's presentation include:

- Focus research on transforming "raw data into actionable information for analysts and decision makers" through network forensics, threat analysis, and machine learning.
- Created Dshell (Decoder Shell), a Python-based framework to analyze network traffic with features including IP-to-Geo and IP-to-ASN mapping.
- Released Dshell publically on GitHub to benefit from outside technical expertise and validate use.
- Attribution of a breach is essential. You must be right in order to deter which can be very difficult, especially if one attacker is trying to emulate another.
- Implanting obfuscated command and control, then parsing and de-obfuscating, to learn about the difference between detecting and understanding breach. Getting into the network is easier than getting out.
- Leverage Dshell to improve the community's ability to verify and validate network forensics research.
- Use other technology enablers for transition, including Docker, an open platform for easy "Build, Ship, Run" at GitXiv.org, a space to share collaborative open computer science projects.

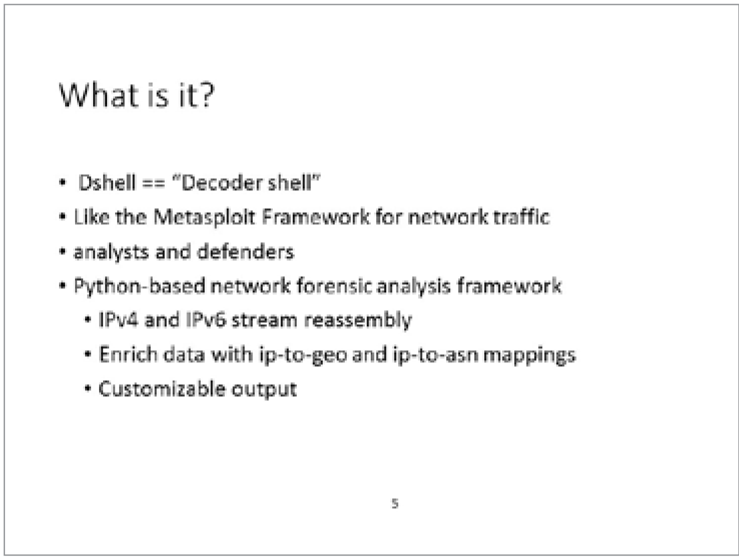


Network Forensics

- Creator of Dshell
  - Framework to analyze network traffic
  - Released publicly in December 2014
  - www.github.com/USArmyResearchLab/Dshell
  - Popular on GitHub

Watch
Star
Fork

4



What is it?

- Dshell == "Decoder shell"
- Like the Metasploit Framework for network traffic
- analysts and defenders
- Python-based network forensic analysis framework
  - IPv4 and IPv6 stream reassembly
  - Enrich data with ip-to-geo and ip-to-asn mappings
  - Customizable output

5

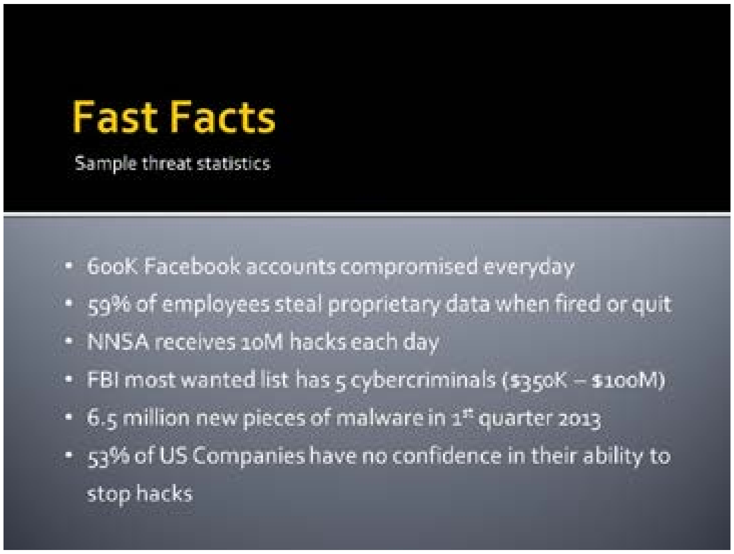
Turning the Tide on Cyber Defense

Dr. Michael Wertheimer, Former Research Director, National Security Agency

Dr. Michael Wertheimer

Dr. Wertheimer presented data to offer perspective on the size and scope of our cyber security challenges. He addressed aspects of those challenges that are increasing our vulnerability—size of target surface, reaction time, hardware limitations, over-reliance on software. He emphasized that solutions will require new collaborations between academia and industry, and the public and private sectors. Among Dr. Wertheimer's key points:

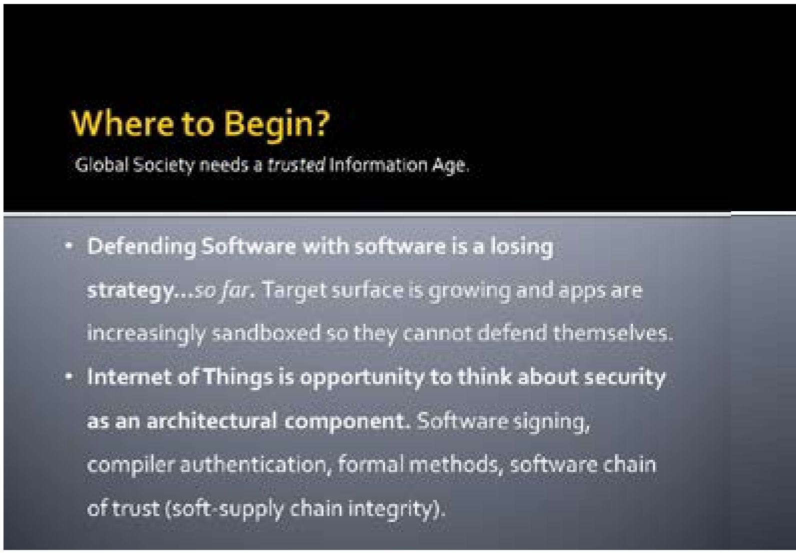
- Threat statistics and software complexity are growing faster than our ability to build protections.
- Using software to protect software fails.
- Open source did not make things better. Vulnerability has been constant since 2007.
- IT administrators and users are slow to react to known vulnerabilities while attackers act quickly.
- An active market exists for zero-day vulnerability exploitation. A supply and demand situation can yield up to $250,000 for an iOS breach.
- New thinking may include liability for companies that lose an organization's data and improved authentication of data integrity.
- The target surface is growing, especially with the Internet of Things. Current hardware limits protection.
- We need security rooted in hardware, including authentication at layers 1 and 2, which are currently ignored.
- Modularity of hardware would offer more control and less vulnerability to hacking.
- New collaborations are part of the solution, e.g., academia and industry, public and private sectors.



Fast Facts

Sample threat statistics

- 600K Facebook accounts compromised everyday
- 59% of employees steal proprietary data when fired or quit
- NNSA receives 10M hacks each day
- FBI most wanted list has 5 cybercriminals ($350K – $100M)
- 6.5 million new pieces of malware in 1st quarter 2013
- 53% of US Companies have no confidence in their ability to stop hacks



Where to Begin?

Global Society needs a *trusted* Information Age.

- **Defending Software with software is a losing strategy…***so far*. Target surface is growing and apps are increasingly sandboxed so they cannot defend themselves.
- **Internet of Things is opportunity to think about security as an architectural component.** Software signing, compiler authentication, formal methods, software chain of trust (soft-supply chain integrity).

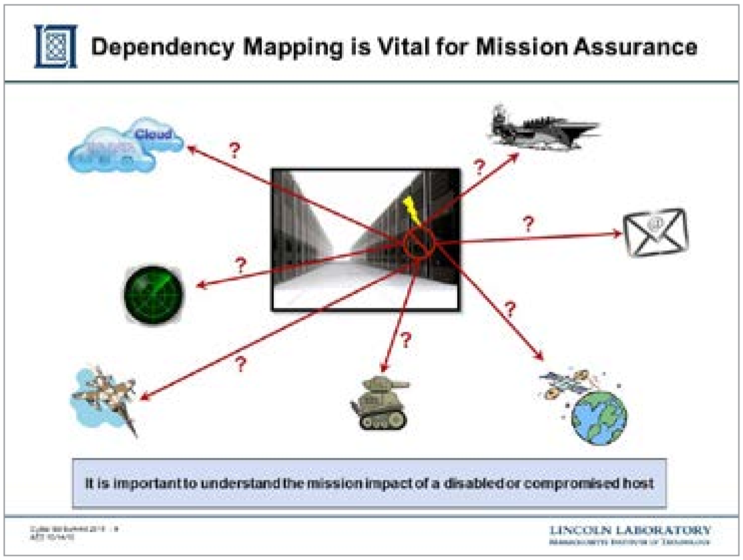
Mission Assurance as a Function of Scale

Alexia Schulz, MIT Lincoln Laboratory

Because all DoD missions depend on cyber-assets and capabilities, a dynamic and accurate cyber dependency analysis is a critical component of mission assurance. Mission analysis aims to identify hosts and applications that are "mission critical" so they can be monitored and resources preferentially allocated to mitigate risks. For missions limited in duration and scale (tactical missions), dependency analysis is possible to conceptualize in principle although difficult to realize in practice. However, for long-duration and large-scale missions (strategic missions), the situation is murkier. In particular, because a typical strategic DoD mission might expect to leverage a large enterprise network, cyber-researchers struggle to find technologies that will scale up to large numbers of hosts and applications. Dr. Schulz argued that the difficulty is fundamental: As the mission timescale becomes increasingly longer and the number of hosts associated with the mission becomes increasingly larger, the mission encompasses the entire network. Mission defense becomes indistinguishable from classic network defense. Concepts generally associated with mission assurance such as fight-through are not well suited to these long timescales and large networks. This train of thought leads us to reconsider the concept of "scalability" as applied to mission assurance and suggests application of a hierarchical abstraction approach. Large-scale, long-duration mission assurance then may be treated as the interaction of many small-scale, short-duration tactical missions.

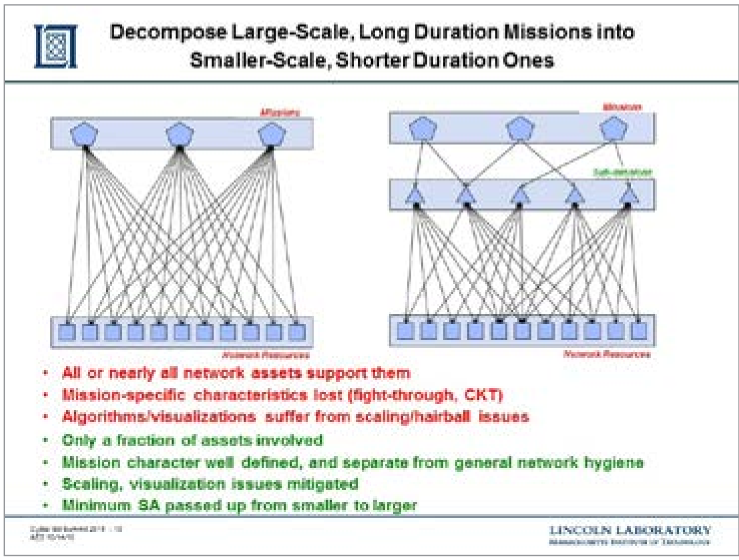
Dr. Schulz presented the following conclusions:

- Mission assurance constructs such as Cyber Key Terrain and fight-through
  - Are meaningful for tactical missions involving limited time and a small fraction of the total network resources.
  - Lose their meaning for strategic missions of indefinite time that require a significant fraction of total network resources.
- Larger missions can be decomposed into smaller tactical ones in both spatial and temporal domains.
- Mission assurance software need not scale to the size of a global enterprise.
  - Network-wide visualizations or a common operating picture may not be as useful for mission assurance as is generally believed.
- Future research agendas should emphasize:
  - Developing technology for the swift, dynamic, and accurate mapping of tactical missions.
  - Modeling the complex interactions of tactical building blocks to ensure larger scale strategic missions.



Dependency Mapping is Vital for Mission Assurance

It is important to understand the mission impact of a disabled or compromised host



Decompose Large-Scale, Long Duration Missions into Smaller-Scale, Shorter Duration Ones

- All or nearly all network assets support them
- Mission-specific characteristics lost (fight-through, CKT)
- Algorithms/visualizations suffer from scaling/hairball issues
- Only a fraction of assets involved
- Mission character well defined, and separate from general network hygiene
- Scaling, visualization issues mitigated
- Minimum SA passed up from smaller to larger

The Ugly Truth About Certificate Revocation

Dave Levin, Research Scientist, University of Maryland

Authentication—i.e., being able to verify with whom one is communicating—is a critical component to secure communication and is traditionally made possible by a public key infrastructure (PKI). A necessary primitive feature in any PKI is the ability for a certificate authority to verifiably revoke a certificate it has issued and to disseminate these revocations to all users who may have cached the certificate. This process requires human action and thus leads us to ask, "Are administrators doing what they must to ensure a secure Web?" He presented a measurement study on how administrators of the most popular one million websites reacted to the widespread Heartbleed vulnerability. The study revealed that popular websites are surprisingly slow and incomplete in revoking potentially compromised certificates. For example, three weeks after the announcement of Heartbleed, 87 percent of vulnerable certificates had not been revoked. These results motivate a slew of open problems that, if answered, would ultimately lead to a more secure, more reliable PKI for all users.

High-assurance Hardware: Is It Possible?

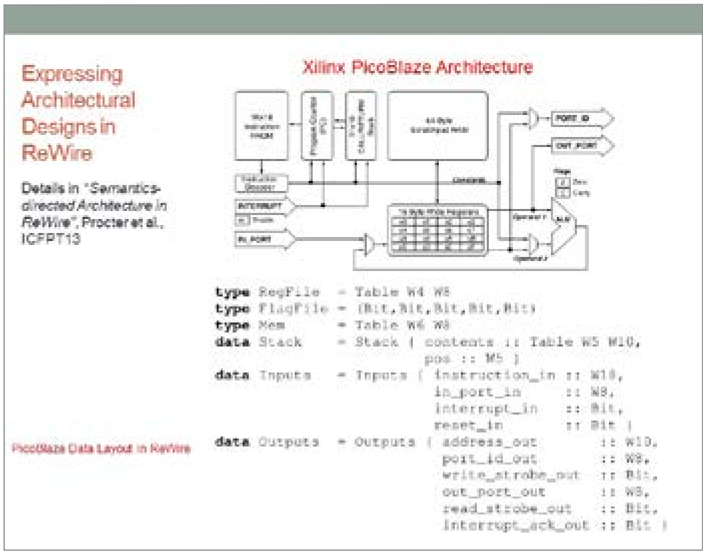
William Harrison, Associate Professor, University of Missouri (MU)

There is no such thing as high assurance without high-assurance hardware. High-assurance hardware is essential, because all high-assurance systems ultimately depend on hardware that conforms to, and does not undermine, critical system properties and invariants. Yet, high-assurance hardware development is stymied by the conceptual gap between formal methods and hardware description languages used by engineers. In his presentation, which represented joint work with Dr. Gerry Allwein of the U.S. Naval Research Laboratory and Dr. Michela Becchi, Dr. Adam Procter, and Ian Graves of MU, Dr. Harrison discussed ReWire. ReWire is a Haskell-like functional programming language that provides a suitable foundation for formal verification of hardware designs and a compiler for the language that translates high-level, semantics-driven designs directly into working hardware.

Dr. Harrison showed that the ReWire language and Toolchain:

- Inherit Haskell's good qualities:
  - Pure functions, strong types, monads, and equational reasoning
  - Formal denotational semantics. [HarrisonKieburtz05, Harrison05]
- Feature language design identifying HW representable programs
  - Mainly restrictions on recursion in functions and data
  - Built-in types for HW abstractions, including clocked and parallel computations

He presented ReWire's design and implementation along with a case study in the design of a secure multicore processor based on the Xilinx PicoBlaze. He demonstrated both ReWire's expressiveness as a programming language and its power as a framework for formal, high-level reasoning about hardware systems.



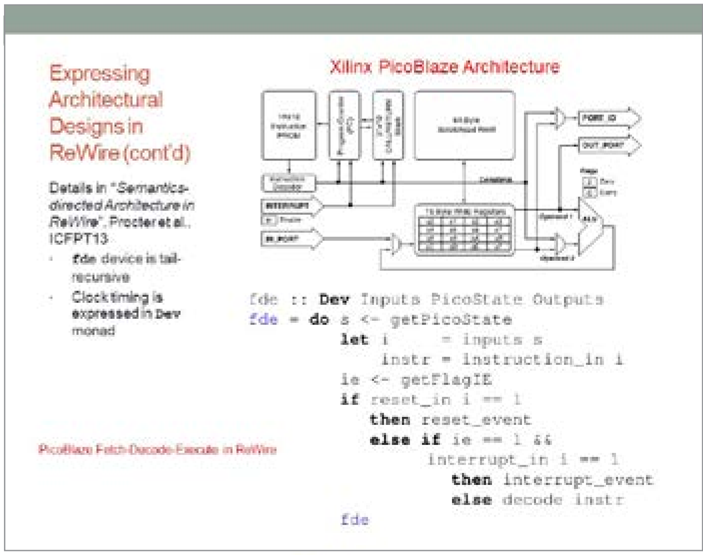
Expressing Architectural Designs in ReWire

Details in "Semantics-directed Architecture in ReWire", Procter et al., ICFPT13

Xilinx PicoBlaze Architecture

```
type RegFile  = Table W4 W8
type FlagFile = (Bit,Bit,Bit,Bit,Bit)
type Mem      = Table W6 W8
data Stack    = Stack { contents :: Table W5 W10,
                        pos :: W5 }
data Inputs   = Inputs { instruction_in :: W18,
                         in_port_in     :: W8,
                         interrupt_in   :: Bit,
                         reset_in       :: Bit }
data Outputs  = Outputs { address_out      :: W10,
                          port_id_out      :: W8,
                          write_strobe_out :: Bit,
                          out_port_out     :: W8,
                          read_strobe_out  :: Bit,
                          interrupt_ack_out :: Bit }
```

PicoBlaze Data Layout in ReWire



Expressing Architectural Designs in ReWire (cont'd)

Details in "Semantics-directed Architecture in ReWire", Procter et al., ICFPT13

- fde device is tail-recursive
- Clock timing is expressed in Dev monad

Xilinx PicoBlaze Architecture

```
fde :: Dev Inputs PicoState Outputs
fde = do s <- getPicoState
         let i     = inputs s
             instr = instruction_in i
         ie <- getFlagIE
         if reset_in i == 1
            then reset_event
            else if ie == 1 &&
                     interrupt_in i == 1
                       then interrupt_event
                       else decode instr
         fde
```

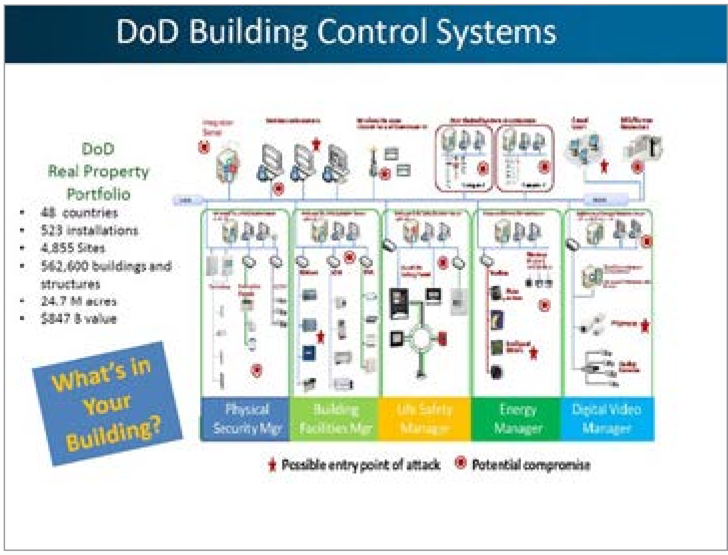
PicoBlaze Fetch-Decode-Execute in ReWire

Cyber Securing Building Control Systems

Michael Chipley, President and Chief Executive Officer, The PMC Group, LLC.
Matt Albertsen, Director of Engineering, Chinook Systems, Inc.

The nation's buildings rely increasingly on building control systems (otherwise known as operational technology) that are Internet-enabled. These systems provide critical services that allow a building to meet the functional and operational needs of its occupants but become easy targets for hackers and others with malicious intent. Attackers can exploit these systems to gain unauthorized access to facilities, cause physical destruction of building equipment, be used as an entry point to traditional IT systems and data, and expose an organization to significant financial obligations to contain and eradicate malware or recover from a cyber-event. This presentation explored topics that spanned facility control systems vulnerability, alert and advisories overview, exploiting control systems demos, industrial control systems security guide, cyber security evaluation tool demo, and General Services Administration and DoD control systems cyber policy and strategy. Mr. Albertson concluded with a review of key plans and documents that every building owner should include when building a cyber security strategy for IT and OT assets:

- System Security Plan (SSP)
- Plan of Action and Milestones (POAM)
- Information Technology and Concept of Operations Plan (ITCP)
- Incident Communications Procedures (ICP)
- Security Auditing Plan (SAP)



DoD Building Control Systems

DoD Real Property Portfolio

- 48 countries
- 523 installations
- 4,855 Sites
- 562,600 buildings and structures
- 24.7 M acres
- $847 B value

Cybersecuring Buildings Workshops

National Institute of Building Sciences
News & Press: News Releases

http://www.nibs.org/news/166752/Institute-Workshops-to-Focus-on-Cybersecurity-of-Building-Control-Systems.htm

Toward the Information Theoretic Limits of Anomaly Detection

Michael Tope, Engineering Researcher, U.S. Department of Defense

Anomaly detection and network deception detection are important components of network defense systems. One popular approach is to use Bayesian methods to model the expected activity and behaviors, and then send alerts on outliers. Factors that impede the construction of Bayesian and similar statistical models include (1) unknown underlying statistical distributions, (2) unknown dependencies among data samples (invalidating common independence assumptions), and (3) difficulty ascertaining the complexity of such unknowns to prevent overfitting of models. In addition, we seek agile online detection algorithms. Such online adaption increases the number of parameters that must be learned from the input data (environment), which in turn inherently slows the response. What is the limit? Are there conditions under which such algorithms become hopelessly blind? Using relatively simple information, Mr. Tope outlined Theoretic PAC-Bayesian (PAC = Probably Approximately Correct) methods that mitigate many of the problems described while yielding some small loss of statistical power with high probability. Further, this approach bounds the learning rate (dynamically estimated from the input data) with very few statistical assumptions. The learning rate then bounds detection performance. Mr. Tope discussed performance results from testing this approach to detect network topology deception within traceroute measurements.

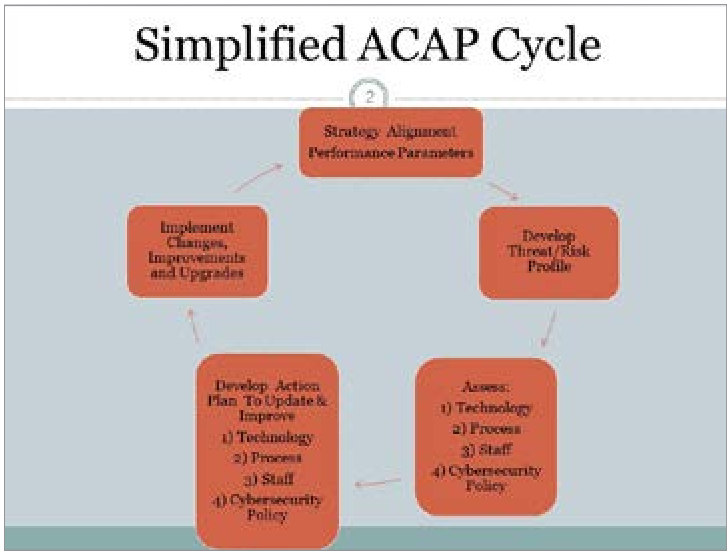
He concluded his presentation by discussing the following points:

- PAC-Bayesian methods hold promise (but are too conservative).
  - In decision processes, the convergence rate can be O(n) optimal.
- PAC-Bayesian methods are well suited for cascaded and nested decision processes.
  - Incorporating robustness (high probability bounds) is relatively easy.
  - Identify and remove outliers and samples with "too" much influence.
- Results show that the performance is close to expectation.

Outthinking the Barbarians: The Agile Cyber Threats Action Plan (ACAP)

Jo Lee Loveland Link, President, VOLVOX Inc.
John Link, Director of Operations, VOLVOX Inc.

ACAP is a cyber security strategy process the presenters developed that focuses on creating an iterative 80 percent + solution strategy to emergent cyber threats and risks. The process fuses several fields: risk management, strategic planning, creative collaboration, process improvement, and information sharing. ACAP moves cyber security strategy and culture from being compliance oriented—unable to manage the threat complexity and tempo—to a proactive and adaptive approach. It takes advantage of a team's creative thinking to counter the full range of cyber threats in a one- to three-day process during which a cross-functional technical and leadership team shares information, surfaces insights, and makes decisions. These decisions are 1) create and continuously update the evolving threat and risk profile; 2) rapidly assess the organization's cyber security infrastructure for real-time effectiveness and adaptability; 3) examine the threat and risk profile against its technology, monitoring, and response processes and plans; staff capacity; and cyber security policies; 4) define process and system deltas and problems before they fail; and 5) create a robust action plan for an adaptive cyber-response to remedy the deltas through user alerts, cyber security policy, innovative staffing, and the required technology and process upgrades. The ACAP process then is iterated in one- to six-month "Agile" cycles or as needed.



Simplified ACAP Cycle

2

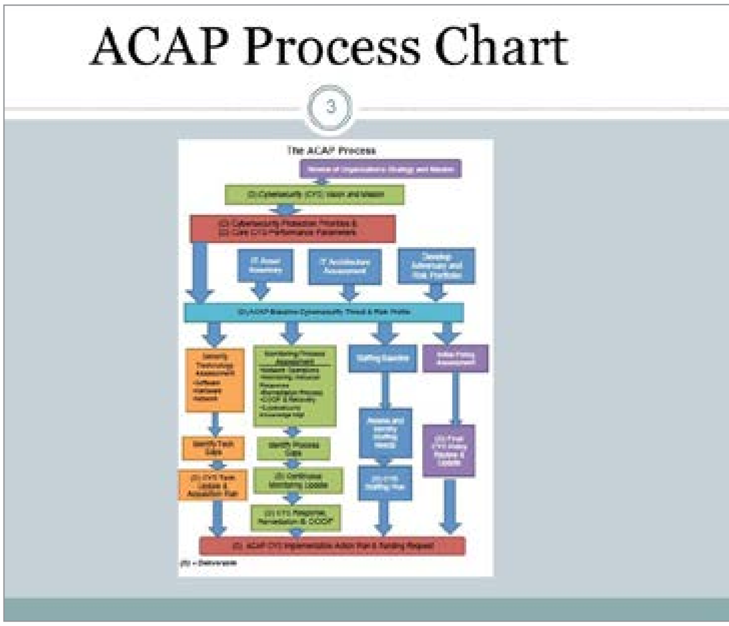
Strategy Alignment
Performance Parameters

Develop
Threat/Risk
Profile

Assess:
1) Technology
2) Process
3) Staff
4) Cybersecurity
Policy

Develop Action
Plan To Update &
Improve
1) Technology
2) Process
3) Staff
4) Cybersecurity
Policy

Implement
Changes,
Improvements
and Upgrades



ACAP Process Chart

3

The ACAP Process

(D) Cybersecurity (CYS) Vision and Mission
(D) ACAP Baseline Cybersecurity Threat & Risk Profile
Staffing Baseline
(D) ACAP CYS Implementation Action Plan & Funding Request
(D) = Deliverable

The presentation concluded with a summation of next steps:

- We are looking for:
  - Agencies, nonprofits, and corporations to pilot ACAP.
  - Academic partners to collaborate in building pilots and researching outcomes.
  - Together we create foundation for ACAP capacity building.
  - The community continues further improvements to the ACAP process.

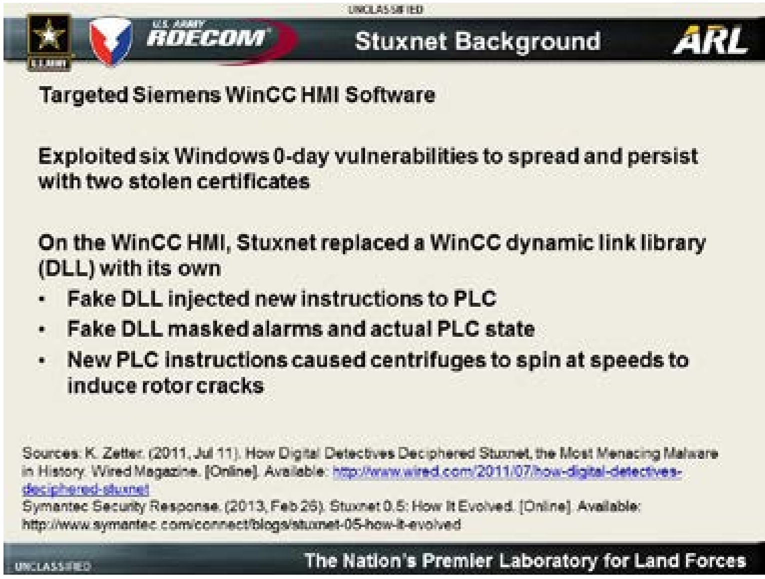
- Looking ahead:
    - Congress should consider an ACAP as a due diligence for acquisition purposes to expedite Cyber security resource pipeline.

Demonstration of Cyber Threats to Legacy Industrial Control System (ICS) Protocols

Dan Sullivan, Senior Principal Software Engineer, Raytheon

In his presentation, which represented joint work with Ed Colbert, Ph.D., Chuck Smith, and Steve Hutchinson, Mr. Sullivan demonstrated a cyber-attack against an industrial control system programmable logic controller (PLC) by exploiting the vulnerabilities of the legacy Modbus protocol. In particular, exploiting Modbus to affect industrial devices in the same way as Stuxnet affected centrifuges. His discussion also explored what an attacker can learn about a network through passive reconnaissance and reviewed legacy ICS protocols security vulnerabilities, which included:

- Security was not designed in many legacy protocols.
    - **Examples:**
        - **Modbus**—common fieldbus protocol
        - **CAN Bus**—used in cars
        - **Inter-Control Center Protocol (ICCP)**—used in electrical grid
- Attack Vectors: From Internet through corporate network through:
    - Phishing
    - "Waterhole attack"
    - Compromised firmware/patches
- From vendors or contractors with external access (e.g., Target hack)
- Wireless and mobile devices



UNCLASSIFIED

U.S. ARMY RDECOM Stuxnet Background ARL

Targeted Siemens WinCC HMI Software

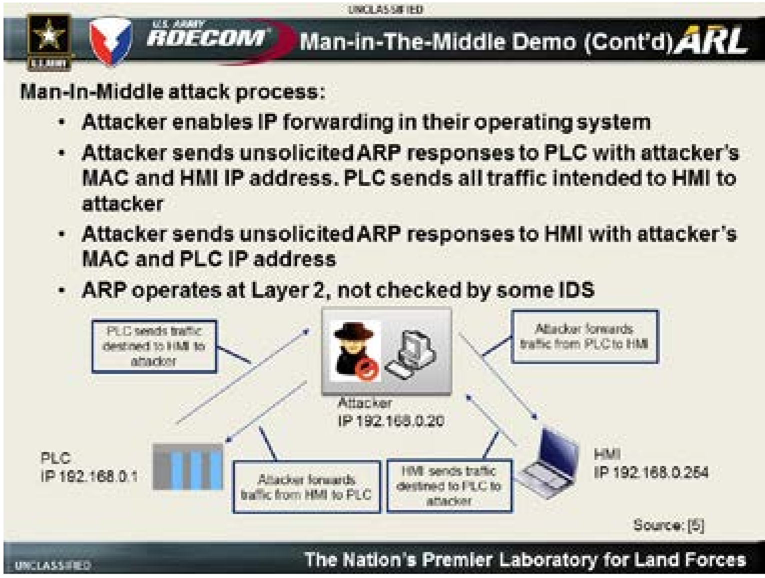
Exploited six Windows 0-day vulnerabilities to spread and persist with two stolen certificates

On the WinCC HMI, Stuxnet replaced a WinCC dynamic link library (DLL) with its own

- Fake DLL injected new instructions to PLC
- Fake DLL masked alarms and actual PLC state
- New PLC instructions caused centrifuges to spin at speeds to induce rotor cracks

Sources: K. Zetter. (2011, Jul 11). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. Wired Magazine. [Online]. Available: http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet
Symantec Security Response. (2013, Feb 26). Stuxnet 0.5: How It Evolved. [Online]. Available: http://www.symantec.com/connect/blogs/stuxnet-05-how-it-evolved

UNCLASSIFIED The Nation's Premier Laboratory for Land Forces



UNCLASSIFIED

U.S. ARMY RDECOM Man-in-The-Middle Demo (Cont'd) ARL

Man-In-Middle attack process:

- Attacker enables IP forwarding in their operating system
- Attacker sends unsolicited ARP responses to PLC with attacker's MAC and HMI IP address. PLC sends all traffic intended to HMI to attacker
- Attacker sends unsolicited ARP responses to HMI with attacker's MAC and PLC IP address
- ARP operates at Layer 2, not checked by some IDS

PLC sends traffic destined to HMI to attacker

Attacker forwards traffic from PLC to HMI

Attacker
IP 192.168.0.20

PLC
IP 192.168.0.1

Attacker forwards traffic from HMI to PLC

HMI sends traffic destined to PLC to attacker

HMI
IP 192.168.0.254

Source: [5]

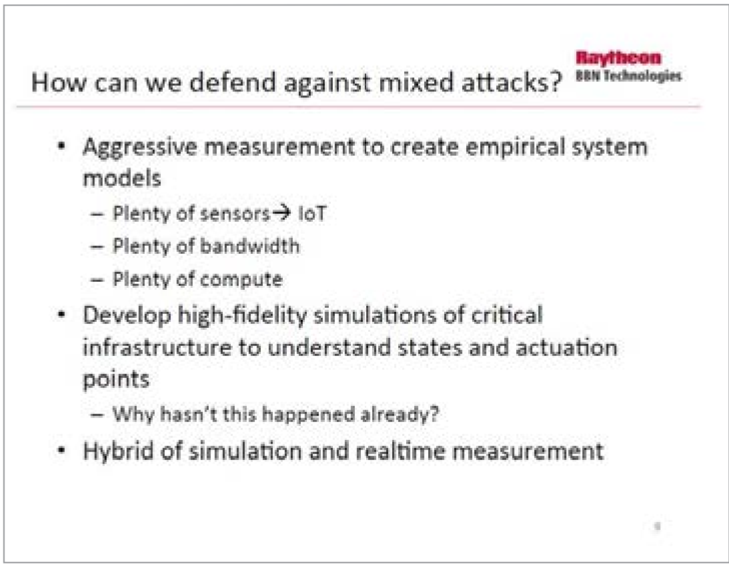
UNCLASSIFIED The Nation's Premier Laboratory for Land Forces

Mr. Sullivan also demonstrated how an attacker can send rogue Modbus messages to a PLC. He additionally demonstrated a man-in-the middle attack that showed how an attacker can send false messages to a human machine interface (HMI) while sending rogue messages to the PLC and the plant operator being unaware of the attack.

Opportunity Knocks: Defending Against Mixed Cyber + Physics Attacks Against Critical Infrastructure

Joshua Edmison, Senior Scientist, Raytheon BBN Technologies

Critical infrastructure ranging from water and power distribution to roadways and railways are a complex mixture of sensors, actuators, and processing that span many different environments. While there are several examples of cyber-only threats against critical infrastructure (e.g., Turkey 2008 gas pipeline) and physical-only attacks (e.g., 2014 shooting of substation transformers), Dr. Edmison detailed in his presentation that the threats combining mixed cyber-attack and system physical attack to achieve the attacker's objective are an important area for developing defensive capabilities. Cyber threats can be initiated without warning, may offer precision, and can be performed at a distance, but they are limited/bounded by parts of the infrastructure that are controlled or sensed. In contrast, physical-only threats usually occur within a focused geographical footprint (close physical proximity) while typically offering less precision and some early warning. By combining cyber-attack and physical attack simultaneously, an adversary could amplify the effectiveness of an attack. For example, physically damaging a small element or component could place a system in a degraded state (e.g., tipping point) that would enable more limited cyber-based actuation to push the system to failure. Combined attacks necessitate the development of new defensive capabilities for critical infrastructure. His presentation used examples, suggested potential defenses, and identified areas for future investigation of mixed cyber/physical attacks, including:



How can we defend against mixed attacks?

Raytheon BBN Technologies

- Aggressive measurement to create empirical system models
  - Plenty of sensors→ IoT
  - Plenty of bandwidth
  - Plenty of compute
- Develop high-fidelity simulations of critical infrastructure to understand states and actuation points
  - Why hasn't this happened already?
- Hybrid of simulation and realtime measurement

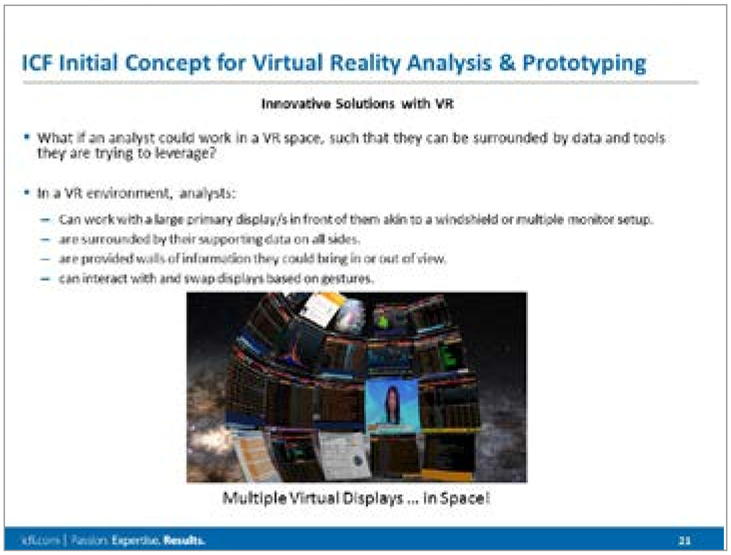
- Collection and processing of opportunistic sensor data
  - Non-ideal sensors in every way but numerous
- Domain-specific simulations of system state
  - Must align with real data
- Inventory and logistics for reconstitution
  - How do you know what I have where? How can I move the materials or people when a problem occurs?

Virtual Reality for Cyber-analysis and Investigation

Lee Trossbach, Senior Project Manager, ICF International
Garrett Payer, System Architect, ICF International

Products that facilitate users to immerse themselves in virtual reality constructs have taken a huge leap forward with the introduction of the Oculus Rift peripheral (and similar products) since its Kickstarter Initiative in 2012. The Oculus Rift has revolutionized the virtual reality industry and provided a catalyst for research, development, and commercialism. As Mr. Trossbach detailed in the presentation, ICF pursued and created an elementary demonstration virtual cyber-analysis space that included some interactive capabilities. Virtual 3D cyber-analysis environments have the opportunity to provide a cyber-analyst or researcher with a unique work environment such that the analyst or researcher would be surrounded by his or her work (custom-sized and custom-placed display objects of interest) to facilitate unique insight and understanding. ICF believes that these environments will increase productivity, reduce the cognitive load, and provide a greater opportunity for the human sense-making process. In conclusion, Mr. Payer, co-presenter, discussed possible directions for future work, including:

- Adapt existing research and technology.
- Engage the community and apply existing work for use in creating a more engaging, more effective analyst experience.
  - We are not experts in Neuro-linguistic programming (NLP), voice recognition, or gesture controls. We will adapt our cyber-expertise to existing work in these areas.
  - Where existing technology does not meet expectations, rather than investigate these areas ourselves, we will collaborate with academia and Industry to push the boundaries forward. We will adapt this work for use in cyber space.
- Add additional capabilities to the existing prototype.
  - Add primitive voice recognition and command translation.
  - Add additional gestures for controlling the environment.
- Integrate with existing Intrusion Detection System to display alerts in real time.



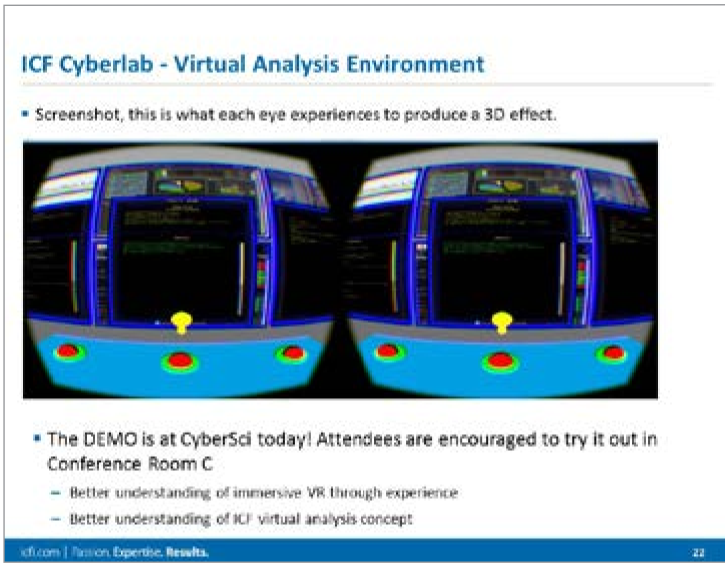
ICF Initial Concept for Virtual Reality Analysis & Prototyping

Innovative Solutions with VR

- What if an analyst could work in a VR space, such that they can be surrounded by data and tools they are trying to leverage?
- In a VR environment, analysts:
  - Can work with a large primary display/s in front of them akin to a windshield or multiple monitor setup.
  - are surrounded by their supporting data on all sides.
  - are provided walls of information they could bring in or out of view.
  - can interact with and swap displays based on gestures.

Multiple Virtual Displays ... in Space!

icfi.com | Passion. Expertise. Results. 21



ICF Cyberlab - Virtual Analysis Environment

- Screenshot, this is what each eye experiences to produce a 3D effect.

- The DEMO is at CyberSci today! Attendees are encouraged to try it out in Conference Room C
  - Better understanding of immersive VR through experience
  - Better understanding of ICF virtual analysis concept

icfi.com | Passion. Expertise. Results. 22

Protecting Critical Infrastructure from Cyber-attack Through Technical Isolation

Nate Cimo, Managing Partner, Bowler Pons Solutions Consultants

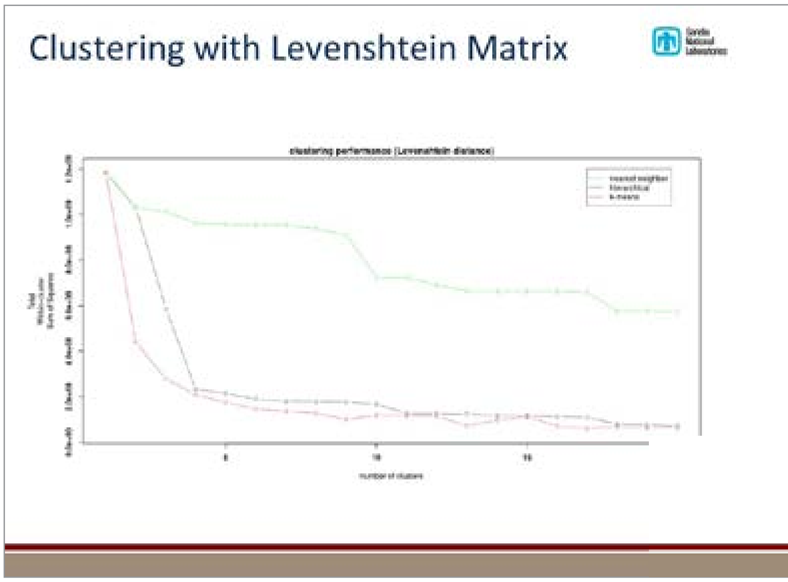
Cyber threats are increasingly transgressing from the cyber world to the physical world. Most commonly seen motivators for this shift are the ease of attack and the impact of the attack. Mr. Cimo said that with current critical infrastructure technologies, securing the inherent technology is either impossible or nearly impossible. He asserted that the best method for securing critical infrastructure is through secured logical segregation with controlled communications between segments. This controlled communications should consist of multiple defenses and in-depth technologies to ensure all seven layers are inspected and protected. He also provided details on this architecture and examined a case sample of its current implementation in the real world during his presentation.

Dimension Reduction for Cyber-attack Detection and Analysis

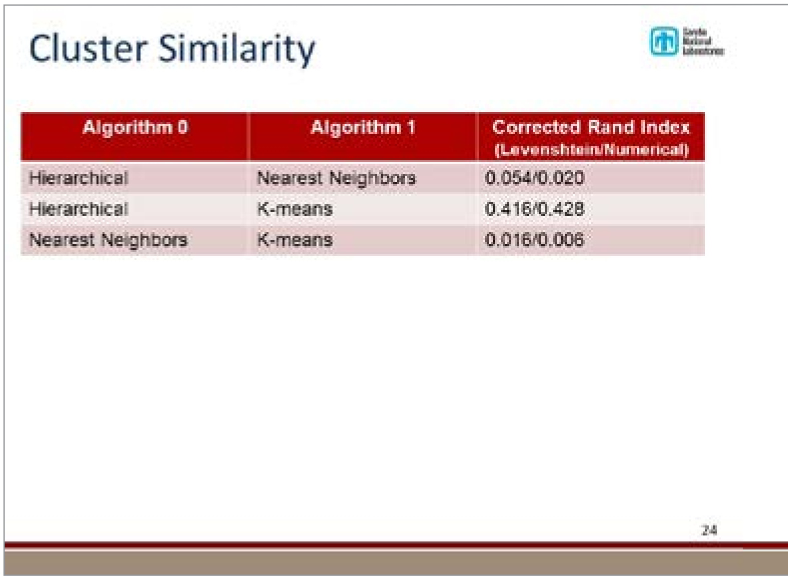
Robert Mitchell, Scientist, Sandia National Laboratories

State-sponsored, terrorist, criminal, and recreational attacks on high-visibility cyber systems have become prevalent. The increase in frequency and effectiveness of these attacks inspires the cyber defense community to improve its defensive tools. In his presentation, which represented joint work with Josh Maine, Andrew Fisher, and John Jarocki, Mr. Mitchell said that prevention mechanisms ideally stop attacks. However, given insider threats and well-funded cyber-attack activities, robust detection and analysis must reinforce prevention techniques. The event logs used in detection and analysis techniques have many features, which overwhelm human and artificial consumers. He proposed and evaluated machine-learning models for reducing the dimension of these datasets.

Mr. Mitchell discussed the consideration of the many features that comprise decoded back door data (that is, commands typed by an adversary) and metadata as a machine-learning dimension-reduction problem. Specifically, he presented the feature selection (best subset and stepwise selection) and feature extraction (principal component analysis and partial least squares) approaches. He illustrated how to create four machine-learning dimension-reduction models and to measure the quality (using proportion of variance explained and KL divergence) of their results, which will boost future cyber-attack detection and analysis research that uses machine learning.



Clustering with Levenshtein Matrix



Cluster Similarity

Algorithm 0	Algorithm 1	Corrected Rand Index (Levenshtein/Numerical)
Hierarchical	Nearest Neighbors	0.054/0.020
Hierarchical	K-means	0.416/0.428
Nearest Neighbors	K-means	0.016/0.006

24

Mr. Mitchell summarized the presentation of the team's work regarding dimension reduction for cyber-attack detection and analysis with the following conclusions:

- Prepare the Dataset.
- Validate Results.
- Avoid Overfitting.
- Allow Machine Learning to Guide Your Theory, Not Provide a Black Box.

Automotive Security: Securing Communications Within and Between Cars

Massimiliano Albanese, Associate Director, Center for Secure Information Systems, George Mason University

Securing critical infrastructure—including modern transportation systems—poses new and interesting challenges because of the potential impact of security breaches. For Dr. Albanese and his research partner, Sushil Jajodia, the goal of their proposed research is to investigate the security of communications within the network infrastructure of modern vehicles, between vehicles, and between vehicles and a fixed infrastructure.

As Dr. Albanese explained during his presentation, modern vehicles are equipped with a bus based on the controller are network (CAN) protocol and multiple electronic control units (ECUs) that control all vital functions of the vehicle. Currently, this infrastructure is completely unsecured in most cars. A few car manufacturers, including General Motors and Tesla

Motors, have recently initiated efforts to secure the communications infrastructure of their vehicles. Such efforts are still in their infancy, and security features are available only in high-end models. To address security concerns in the automotive industry, Dr. Albanese explored several approaches to protect the communications infrastructure of a wide variety of existing vehicles in a practical and cost-effective way.

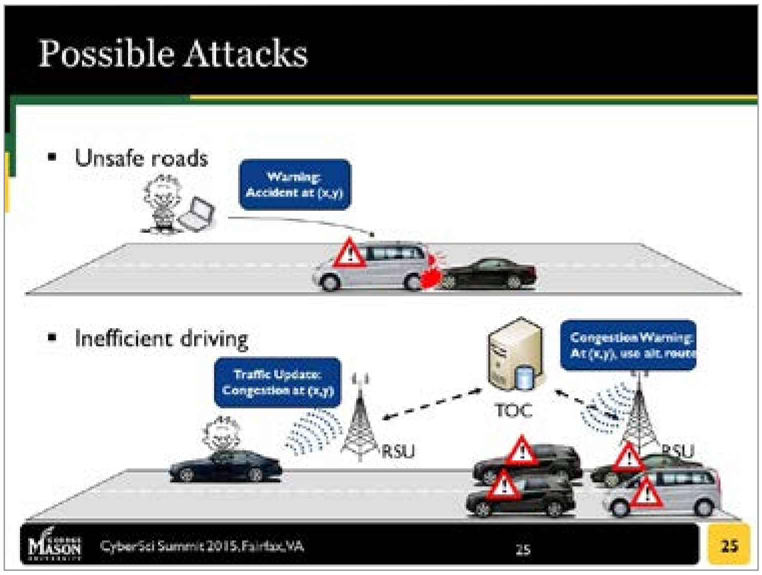
Key stages of the proposed protocol, as he outlined during his presentation, include:

- Key exchange and crypto protocol negotiation
- Initiation of update / authentication
- Firmware transfer and installation

The problem we seek to address is the trade-off between resource consumption and security. The protocol must be flexible and use multiple techniques:

- A powerful ECU might use Diffie-Hellman to exchange keys, AES-256 to encrypt update packets, and SHA-512 to authenticate each packet.
- A weaker ECU might use challenge-response to demand proof of knowledge of existing firmware and then permit the update, unencrypted.

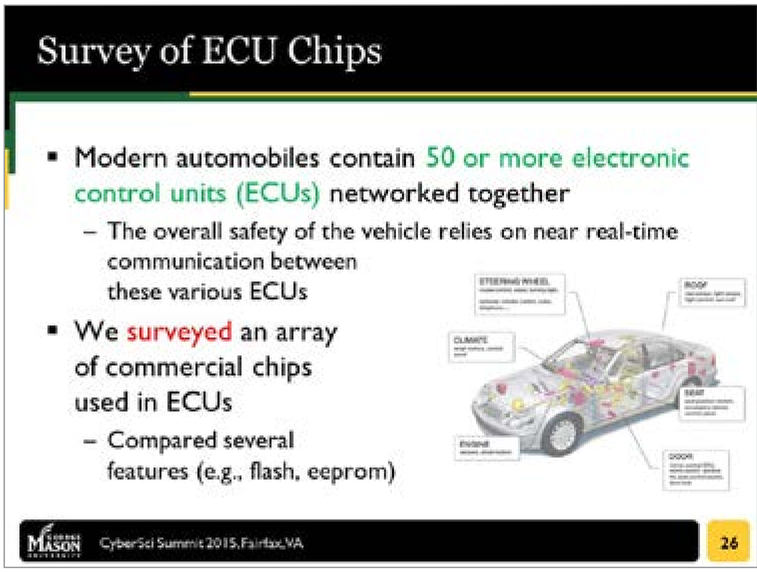
His team's ultimate goal is to develop an array of novel capabilities, including but not limited to intrusion prevention and detection, secure software updates, and self-remediation. The initial research plan consists of four main phases: (1) modeling a vehicle's attack surface, (2) defining the threat model, (3) defining mechanisms to secure firmware updates, and (4) implementing and evaluating the proposed approach on a real car.



Possible Attacks

- Unsafe roads
- Inefficient driving

Warning: Accident at (x,y)
Traffic Update: Congestion at (x,y)
TOC
Congestion Warning: At (x,y), use alt. route
RSU
RSU
MASON
CyberSci Summit 2015, Fairfax, VA
25
25



Survey of ECU Chips

- Modern automobiles contain 50 or more electronic control units (ECUs) networked together
  - The overall safety of the vehicle relies on near real-time communication between these various ECUs
- We surveyed an array of commercial chips used in ECUs
  - Compared several features (e.g., flash, eeprom)

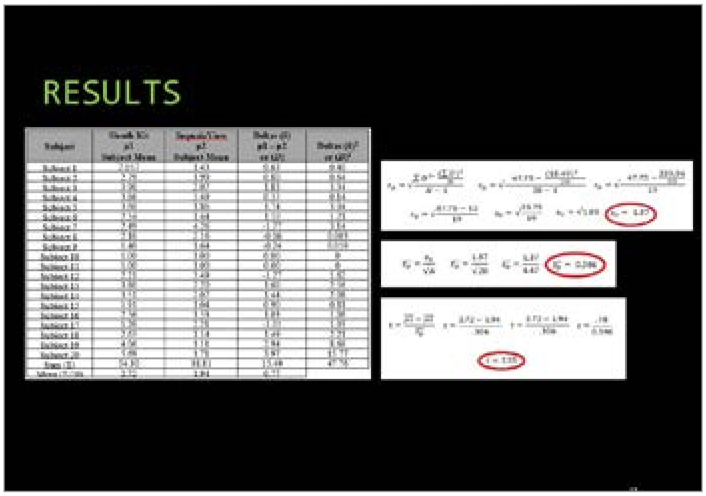
Digital Forensics Tool Interface Visualization

Robert Altiero, Researcher and Owner, Robert Altiero

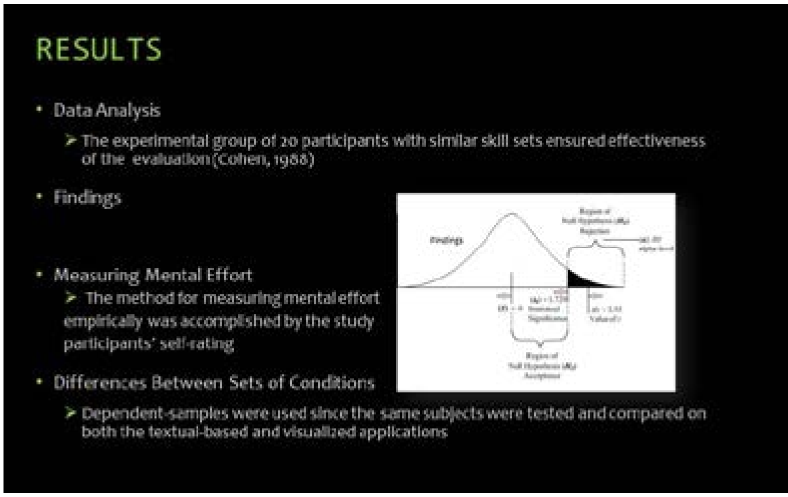
Recent trends show that digital devices are used with increasing frequency in most crimes. Investigating crimes involving these devices is labor intensive for the practitioner, applying digital forensics tools that present possible evidence and display results in tabular lists for manual review. This research investigates how enhanced digital forensics tool interface visualization techniques can be shown to improve the investigator's cognitive capacities to discover criminal evidence more efficiently. Dr. Altiero presented visualization graphs and contrasted their properties with the outputs of The Sleuth Kit digital forensic program. Exhibited is the textual-based interface proving the effectiveness of enhanced data presentation. The potential of the computer interface to present to the digital forensic practitioner an abstract, graphic view of an entire dataset of computer files was also demonstrated. Enhanced interface design of digital forensic tools means more rapid linking of suspicious evidence to a perpetrator. A t-test correlating the dependent samples' mean tested for the null hypothesis of less than a significant value between the applications' comparative workloads of the operators. Results of the study indicate a significant value and affirm the hypothesis that a visualized application would reduce the cognitive workload of the first-responder analyst.

He concluded his presentation of the material with the following implications and recommendations:

- Implications
  - With digital evidence playing a constant role in criminal investigations, according to Regional Computer Forensics Laboratories (RCFL) (2013), this study is both timely and relevant.
- Recommendations
  - Determine the most efficient way to present file-centric data visually to the digital forensics practitioner.
  - Improve the digital forensics tool for optimum demographic analysis.
  - Incorporate findings from this work and those of future projects into open-source and commercial digital forensics tool developers' tool sets.
  - Acquire funding for testing commercial tool sets.



RESULTS



RESULTS

- Data Analysis
  - The experimental group of 20 participants with similar skill sets ensured effectiveness of the evaluation (Cohen, 1988)
- Findings
- Measuring Mental Effort
  - The method for measuring mental effort empirically was accomplished by the study participants' self-rating
- Differences Between Sets of Conditions
  - Dependent-samples were used since the same subjects were tested and compared on both the textual-based and visualized applications

ICS Monitoring: Model Drift Paradigm

Steve Hutchinson, Researcher, ICF International

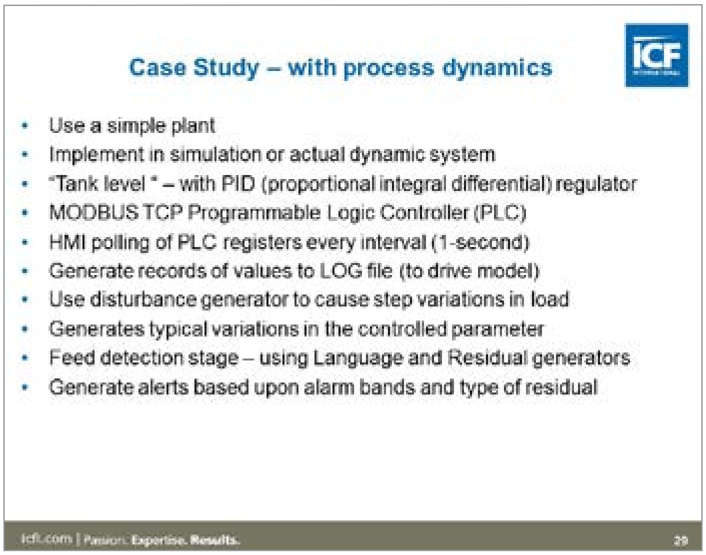
There are increasing concerns and a growing need to perform effective monitoring of infrastructure systems, often called industrial control systems (ICS) and supervisory control and data-acquisition systems (SCADA). Mr. Hutchinson illustrated that ICS monitoring is remarkably similar to computer network defense (CND) both in theory and in practice.

He described a pragmatic approach using best practice from CND (as practiced within DoD) Mr. Hutchinson stated that effective monitoring starts with a definition and knowledge of acceptable policy before monitoring the target (plant or network) to ascertain whether the target is operating within proper specifications (policy) at the times of observation. If one or more operating parameters are observed to be out-of-normal range, this difference can be used to drive a decision process. As with CND, one observed parameter value excursion does not prove that a problem, a compromise, or a security incident exists. Policies used in the decision process must have sufficient specificity to allow evidence and observations to drive the decision outcome deterministically.

Mr. Hutchinson summarized with the following points:

- Adaptation of FDI from control theory can be used for ICS SSM.
- Monitoring alert language.
- Case study to explore typical control parameters.
- Model to estimate state (current, and past).

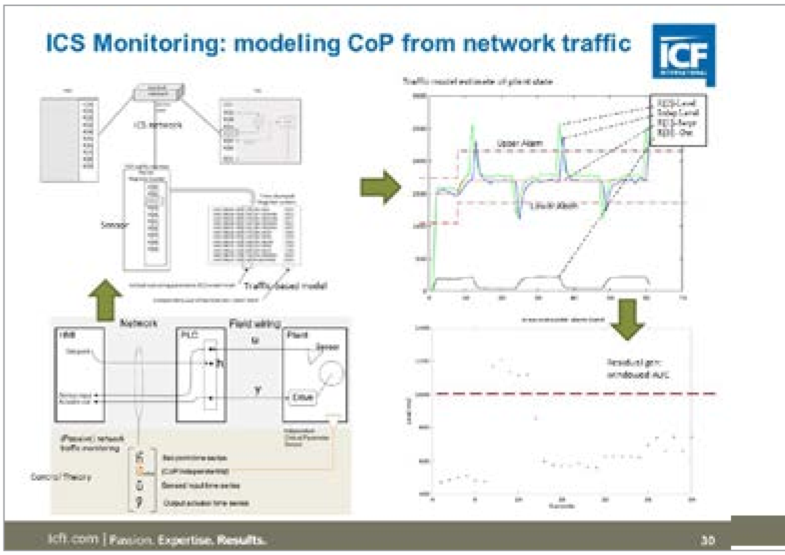
- Generate specific alerts – with semantically accurate messages.
- Collaboration with process/plant SME to define alert conditions.
- Alert language similar to Snort™.
- Define notifications, priorities, and message content.
- Integration with IT security monitoring operations



Case Study – with process dynamics

- Use a simple plant
- Implement in simulation or actual dynamic system
- "Tank level " – with PID (proportional integral differential) regulator
- MODBUS TCP Programmable Logic Controller (PLC)
- HMI polling of PLC registers every interval (1-second)
- Generate records of values to LOG file (to drive model)
- Use disturbance generator to cause step variations in load
- Generates typical variations in the controlled parameter
- Feed detection stage – using Language and Residual generators
- Generate alerts based upon alarm bands and type of residual

icfi.com | Passion. Expertise. Results. 29



ICS Monitoring: modeling CoP from network traffic

icfi.com | Passion. Expertise. Results. 30

Nation State Threats to ICS Through the Schmitt Analytical Framework

Frank Honkus, Command Post Technologies

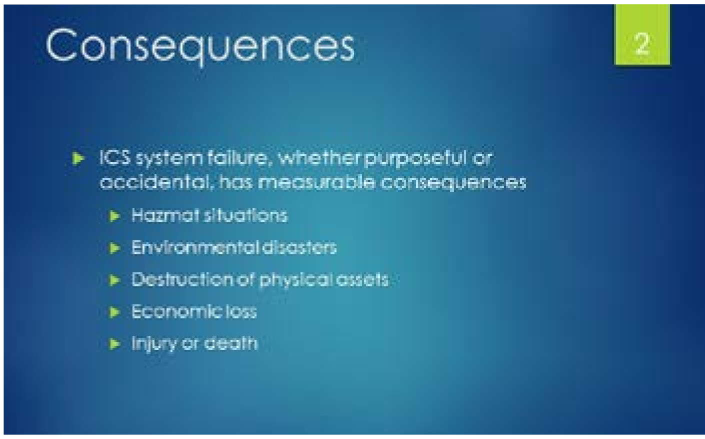
Mr. Honkus explored different political and cyber security issues centering on nation state threats to U.S. critical infrastructure, with emphasis on ICS networks. He began with a brief discussion regarding background on vulnerabilities to ICS, the concept of jus ad bellem (right to war) and use of force, and the Schmitt Analytical Framework. He applied the framework to nation state actors and malware using three case studies of China, Iran, and Havex.

Mr. Honkus concluded with recommendations on how to react and mitigate in both the IT and nation state realms. He proposed that mitigation and response are proportional to production of the target and the impact of the attack:

- Some infrastructure is less critical than others.
    - Someone would not buy a $5,000 firewall to protect the PLC that controls the on/off valve of a public water fountain.

For the case studies analyzed, responses were as follows:

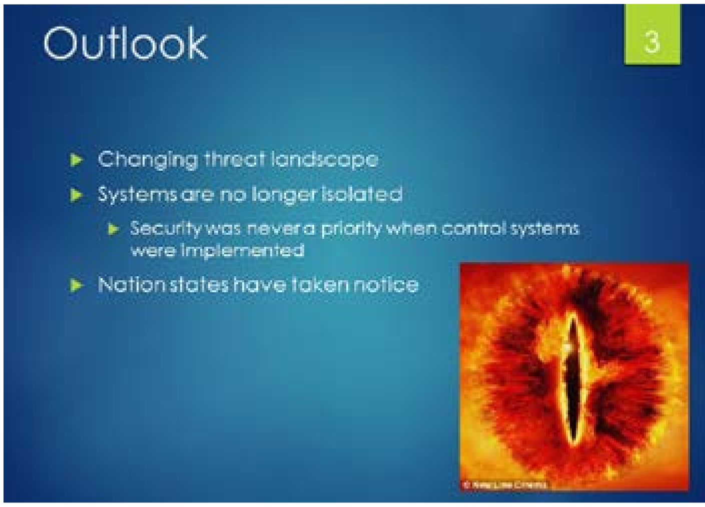
- Nation State Response: China
    - Persona non grata
    - Demarche
- Nation State Response: Iran
    - Sanctions
- Nation State Response: Havex
    - Demarche



Consequences

2

- ICS system failure, whether purposeful or accidental, has measurable consequences
    - Hazmat situations
    - Environmental disasters
    - Destruction of physical assets
    - Economic loss
    - Injury or death



Outlook

3

- Changing threat landscape
- Systems are no longer isolated
    - Security was never a priority when control systems were implemented
- Nation states have taken notice

© New Line Cinema

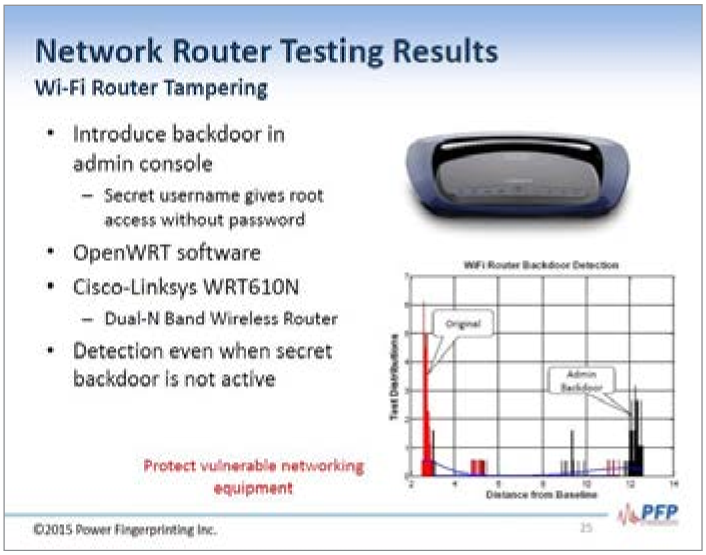
Physics-based Endpoint Intrusion Detection for Critical Infrastructure Devices

Carlos Aguayo Gonzalez, Founder and CTO, PFP Cyber Security
Thurston Brooks, VP Product Marketing, PFP Cyber Security

Critical infrastructure such as industrial control systems (ICS) presents a unique challenge from the cybersecurity perspective. ICS devices are extremely difficult to protect because they have limited processing resources, operate under strict timing constraints, are often based on legacy platforms, and typically have no mechanism to install security software. Dr. Gonzalez presented PFP, an integrity assessment approach that uses physical measurements from side channels (e.g., dynamic power consumption) to detect malicious intrusion in critical ICS endpoints. This revolutionary approach monitors the power consumption of digital systems to see distinctive patterns that uniquely identify the logic being executed within the device to detect, with extreme accuracy, when an unauthorized execution has co-opted the normal operation of critical embedded systems. Using DC, AC, or electromagnetic emanations, PFP can protect systems with constrained resources. It does not require the loading of any software artifacts on the target platform and provides an extra layer of protection complementary to traditional cyber security approaches. He presented results from real-world applications, including an Allen-Bradley PLC, a Siemens S7 PLC, and a smart grid SEL (Schweitzer Engineering Laboratories) feeder protection relay and illustrated the ability of power fingerprinting/analysis to successfully detect and defend against cyber-attacks.

Dr. Gonzalez concluded:

- PFP enables end-point intrusion detection using air-gapped side-channel analysis in ICS field devices.
- Technology fundamentals have been demonstrated.
  - Response is very promising.
  - There is work to do.
- Leveraging physics to change the asymmetry of cyber-attacks.



Network Router Testing Results

Wi-Fi Router Tampering

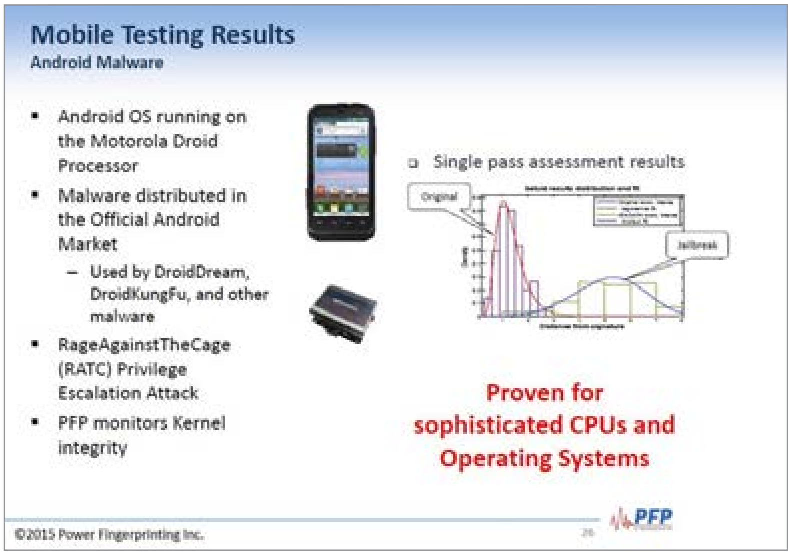
- Introduce backdoor in admin console
  - Secret username gives root access without password
- OpenWRT software
- Cisco-Linksys WRT610N
  - Dual-N Band Wireless Router
- Detection even when secret backdoor is not active

Protect vulnerable networking equipment

©2015 Power Fingerprinting Inc.

25

WiFi Router Backdoor Detection
Original
Admin Backdoor
Test Distributions
Distance from Baseline
2
4
6
8
10
12
14
PFP



Mobile Testing Results

Android Malware

- Android OS running on the Motorola Droid Processor
- Malware distributed in the Official Android Market
  - Used by DroidDream, DroidKungFu, and other malware
- RageAgainstTheCage (RATC) Privilege Escalation Attack
- PFP monitors Kernel integrity

❑ Single pass assessment results

Proven for sophisticated CPUs and Operating Systems

©2015 Power Fingerprinting Inc.

26

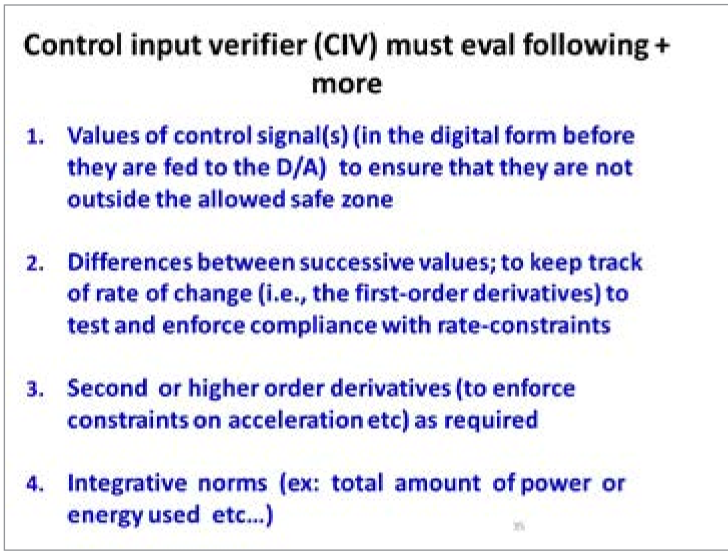
Toward Provable Security: Stopping CPS Attacks at the Interface Between Cyber and Physical

Dhananjay Phatak, Associate Professor, Computer Science and Electrical Engineering Department, University of Maryland, Baltimore County

Dr. Phatak identified the roadblocks to realizing provably secure systems and suggested strategies for circumvention. The findings included the key observation that excess capacity in the form of Turing Equivalence provides one of the main hurdles. As a result, he proposed a "dumb-down/restrict" strategy to implement computing systems as Finite Automata whenever possible. Additionally, for cyber physical systems, he illustrated that tackling the security issues in the physical portion/domain/subsystem is easier than in the cyber domain. Dr. Phatak outlined his Bounding, Integrals, Derivatives, and Signals (BIDS) framework that can detect and mitigate cyber-attacks at the interface between the cyber and the physical parts/domains of the system BEFORE physical damage occurs. In summary, characteristics of the BIDS framework include:

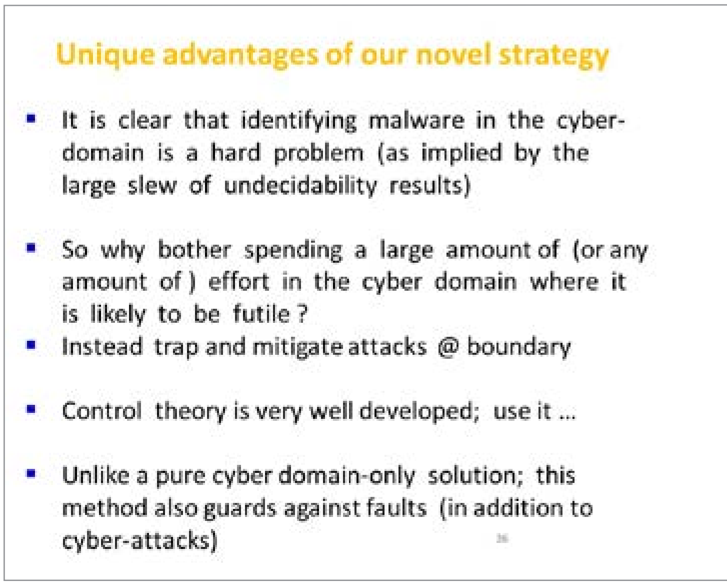
- Bounding, Integrals, Derivatives, and Signals to secure a cyber-physical system
- Analogous to the BIBO stability paradigm from classical control theory
    - Also uses other concepts such as PID control etc. from classical control theory.

He concluded, "Interface between the cyber and physical entities is potentially the optimal place to identify and mitigate cyber-attacks on a cyber-physical system."



Control input verifier (CIV) must eval following + more

1. Values of control signal(s) (in the digital form before they are fed to the D/A) to ensure that they are not outside the allowed safe zone
2. Differences between successive values; to keep track of rate of change (i.e., the first-order derivatives) to test and enforce compliance with rate-constraints
3. Second or higher order derivatives (to enforce constraints on acceleration etc) as required
4. Integrative norms (ex: total amount of power or energy used etc...)



Unique advantages of our novel strategy

- It is clear that identifying malware in the cyber-domain is a hard problem (as implied by the large slew of undecidability results)
- So why bother spending a large amount of (or any amount of) effort in the cyber domain where it is likely to be futile ?
- Instead trap and mitigate attacks @ boundary
- Control theory is very well developed; use it ...
- Unlike a pure cyber domain-only solution; this method also guards against faults (in addition to cyber-attacks)

Protecting Against Sensory-channels Threats in Cyber-physical Systems

A. Selcuk Uluagac, Professor, Florida International University

Cyber-physical system (CPS) is a relatively novel computing paradigm that has a tight integration of communications, computation, and the physical environment. An important feature of CPS devices is their ability to interact with each other and the physical world around them. With CPS applications, engineers monitor the structural health of highways and bridges, farmers check the health of their crops, and ecologists observe wildlife in their natural habitat. Nonetheless, current security models consider protecting only networking components of the CPS devices by using traditional security mechanisms (e.g., an intrusion detection system for the data that traverse the network protocol stacks). These protection mechanisms are not sufficient to protect CPS devices from threats emanating from sensory side channels. Using sensory side channels (e.g., light, temperature, infrared, and acoustic), an adversary can successfully attack a CPS. Specifically, the adversary can (1) trigger existing malware, (2) transfer malware, (3) combine multiple side channels to increase the impact of a threat, or (4) leak sensitive information. Dr. Uluagac described how these threats can occur and discussed what security mechanisms could be used to protect against them.

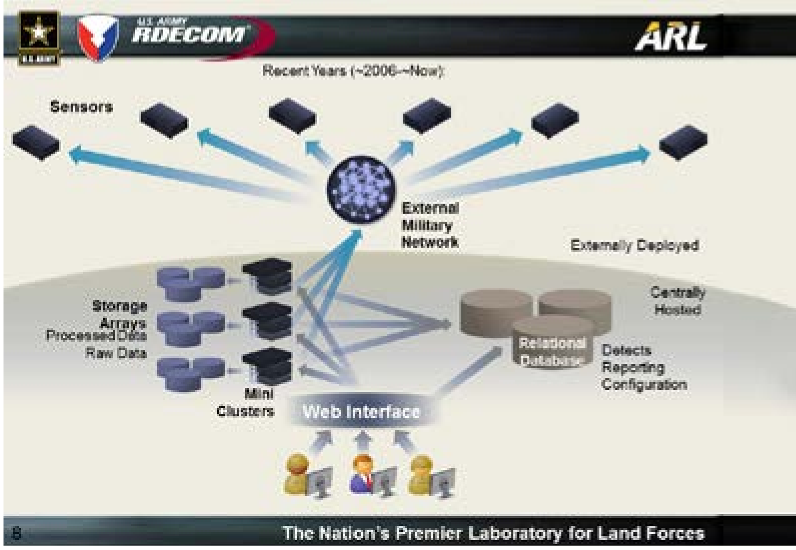
IDS Architectural Design for High-volume Environments and Research

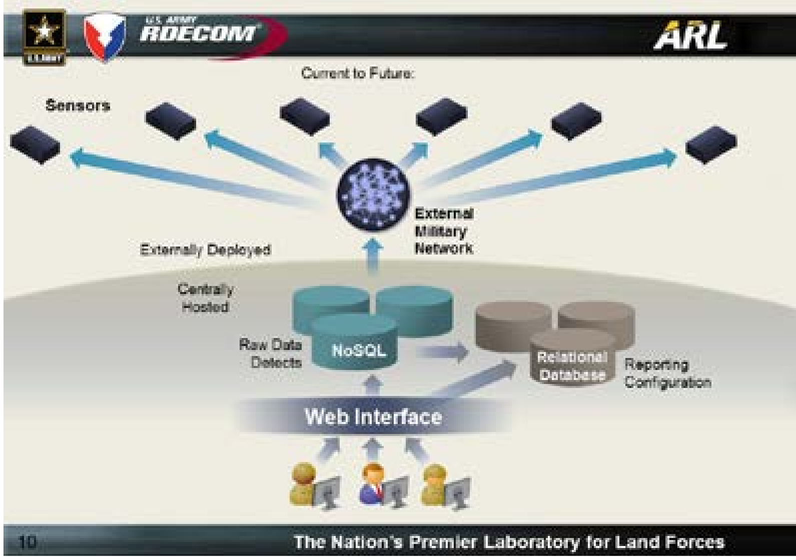
Paul Ritchey, Senior Project Manager, ICF International

With ever-increasing utilization of networks by new devices and increasing bandwidth speeds, designing future-facing intrusion detection system (IDS) architectures becomes quite challenging for large-scale, enterprise-wide deployments and research. The ICF team has significant experience in this area, having designed, implemented, and maintained such a system for the U.S. Army Research Laboratory. Mr. Ritchey discussed the architecture and its evolution over time, including the lessons learned with each iteration and where he is looking for the next implementation.

In discussing the current to future work, Mr. Ritchey projected:

- Needs will not change.
  - Continued scaling
  - Network bandwidths and utilization
- Additional processing power for new tools.
- Flexibility to add remove tools
- Support R&D
- Architectural design remains same.
  - NoSQL replaces relational database.
- NoSQL benefit
- Elimination of current Achilles heel
- More robust distributed processing and querying
- Easier to upgrade hardware over the long term





- Scale processing power and storage concurrently
- Scale without bulk investment
- Ability to integrate different, large data sources

Toward Secured Energy-based Critical Infrastructure

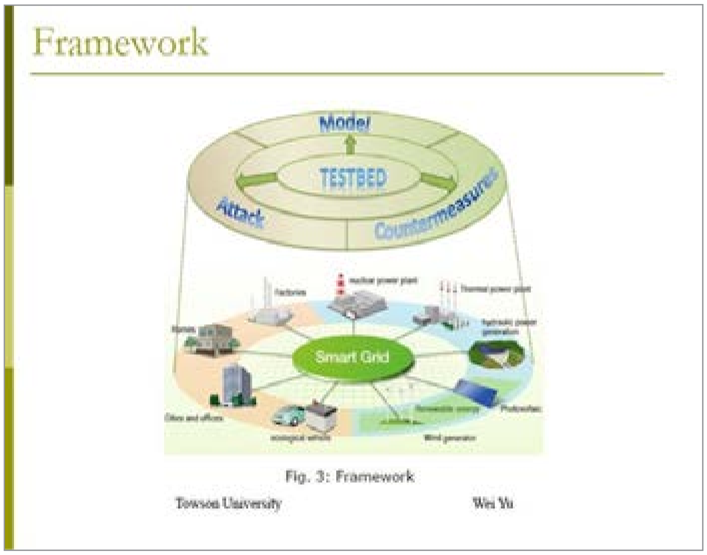
Wei Yu, Associate Professor, Towson University

The smart grid, a typical energy-based cyber-physical system (CPS), uses modern communications and computation technologies to make the power grid more efficient, reliable, and secure. Nonetheless, the smart grid may operate in hostile environments. Lacking tamper-resistance hardware for sensors and meters, for example, increases the risk to be compromised by cyber-adversaries. Dr. Yu introduced a modeling framework to systematically explore threats in the smart grid and to understand their impacts on system operations and end users. He also discussed the development of effective mitigation schemes to defend against these attacks. This research provides a scientific foundation for designing a secured and efficient energy-based critical infrastructure.

During his presentation, Dr. Yu reviewed some challenges for the Smart Grid:

- Smart Grid must be dependable, cost-effective, secure, and efficient, and operate in real time.

- High-volume data streams associated with smart grid operations need to be quickly processed and analyzed.
- Collected massive streaming data will be generated from the power grid to the energy management system (EMS) to enable efficient system operation.

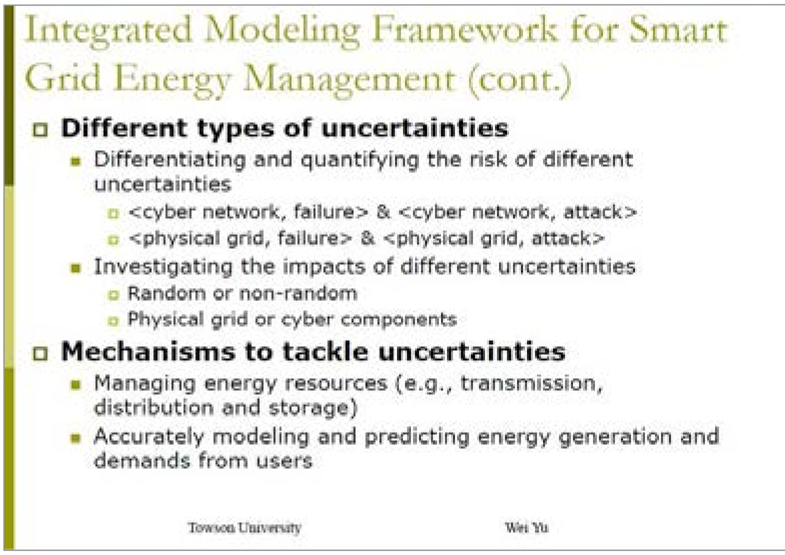


Framework

Fig. 3: Framework

Towson University

Wei Yu



Integrated Modeling Framework for Smart Grid Energy Management (cont.)

- **Different types of uncertainties**
  - Differentiating and quantifying the risk of different uncertainties
    - <cyber network, failure> & <cyber network, attack>
    - <physical grid, failure> & <physical grid, attack>
  - Investigating the impacts of different uncertainties
    - Random or non-random
    - Physical grid or cyber components
- **Mechanisms to tackle uncertainties**
  - Managing energy resources (e.g., transmission, distribution and storage)
  - Accurately modeling and predicting energy generation and demands from users

Towson University

Wei Yu

Cnetmon: A Low-resource Network Interface Activity Monitor for Situational Awareness

John Wittkamper, Developer and Researcher, ICF International

As industry searches for silver-bullet solutions to solve computer security, personnel awareness still seems to be the most viable solution. Mr. Wittkamper observed that the only way what SHOULD be happening can be known is by becoming aware of what is normally happening. As a result, the most important aspect of system understanding for security purposes is monitoring the local interfaces for "strange" traffic. Mr. Wittkamper presented Cnetmon, an approach that demonstrates how to develop a program that will run on ANY Linux platform by any user without any significant performance impact. It allows a broad picture of the network activity, so that anomalous activity could be quickly identified.

An Experimental Exploration of the Impact of Sensor-level Packet Loss on Network Intrusion Detection

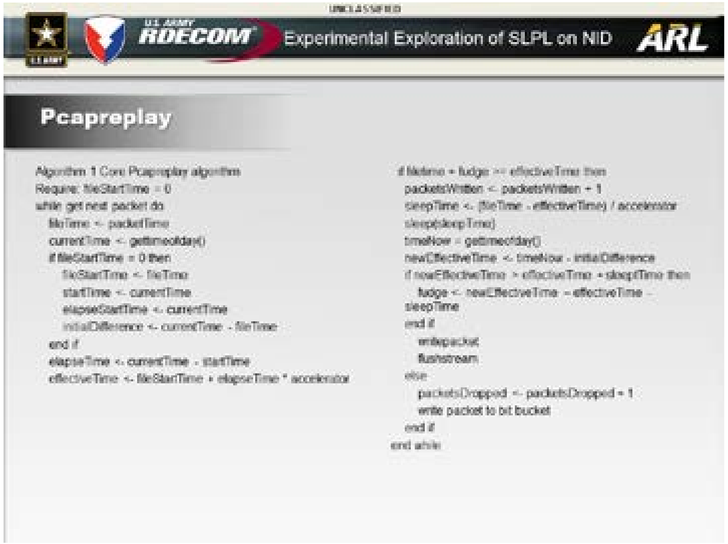
Sidney (Chuck) Smith, Computer Scientist/Team Leader Product Integration and Testing Team, U.S. Army Research Laboratory

Mr. Smith discussed the problem of sensor-level packet loss as it applies to network intrusion detection. He presented two research questions: Is there sufficient regularity in sensor-level packet loss to allow an algorithm to be developed to model it? Additionally, is the impact of sensor-level packet loss on network intrusion detection performance sufficiently regular to allow a formula to be developed that will accurately predict the effect?

To address these questions, Mr. Smith and his partner, Robert J. Hammell, II, developed and validated the Pcapreplay program. As explained in the presentation, the Pcapreplay program allowed them to characterize the manifestation of sensor-level packet loss. Mr. Smith described experiments using Pcapreplay and Snort to explore the impact of sensor-level packet loss. The team graphed and analyzed this impact against their previous theoretical work. They conducted other experiments using Pcapreplay and Snort to measure the impact on network intrusion detection (NID). Here, the alert-loss rate was graphed against the packet-loss rate, and the team compared these graphs with their previous theoretical work. Nonlinear regression analysis was applied to produce a formula with r-squared and reduced chi-squared values close enough to 1 for the team to answer both initial research questions in the affirmative.

His conclusions included the direction of future work:

- There is sufficient regularity in SLPL to allow an algorithm to be developed to model it.
- The impact of SLPL on NID performance is sufficiently regular to allow a formula to be developed that will accurately predict the effect.
- The ultimate goal is to discover the general function y = f(x) where x is the PLR and y is the ALR.
- We will complete a study of the combined effect of Network-level Packet Loss, Host-level Packet Loss, and Sensor-Level Packet Loss.
- We will validate the packet dropper developed in our theoretical work.
- Use the validated packet dropper to validate our general formula.

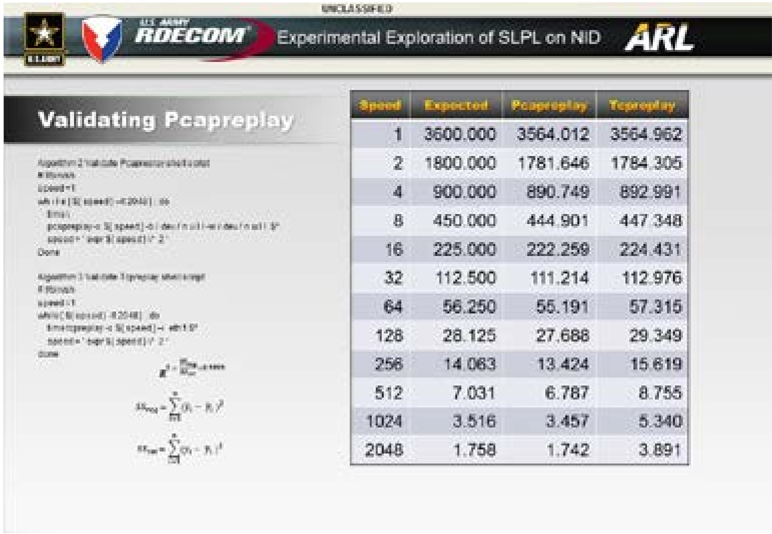


UNCLASSIFIED

RDECOM Experimental Exploration of SLPL on NID ARL

Pcapreplay

```
Algorithm 1 Core Pcapreplay algorithm
Require: fileStartTime = 0
while get next packet do
  fileTime <- packetTime
  currentTime <- gettimeofday()
  if fileStartTime = 0 then
    fileStartTime <- fileTime
    startTime <- currentTime
    elapseStartTime <- currentTime
    initialDifference <- currentTime - fileTime
  end if
  elapseTime <- currentTime - startTime
  effectiveTime <- fileStartTime + elapseTime * accelerator
  if fileTime + fudge >= effectiveTime then
    packetsWritten <- packetsWritten + 1
    sleepTime <- (fileTime - effectiveTime) / accelerator
    sleep(sleepTime)
    timeNow = gettimeofday()
    newEffectiveTime <- timeNow - initialDifference
    if newEffectiveTime > effectiveTime + sleepTime then
      fudge <- newEffectiveTime - effectiveTime -
    sleepTime
    end if
      writepacket
      flushstream
    else
      packetsDropped <- packetsDropped + 1
      write packet to bit bucket
    end if
end while
```



UNCLASSIFIED

RDECOM Experimental Exploration of SLPL on NID ARL

Validating Pcapreplay

```
Algorithm 2 Validate Pcapreplay shell script
#!/bin/sh
speed=1
while [ $( speed) -le 2048 ] ; do
  time \
  pcapreplay -s $[ speed] -b / dev / null -w / dev / null [illegible]
  speed=`expr $[ speed] \* 2`
Done

Algorithm 3 Validate Tcpreplay shell script
#!/bin/sh
speed=1
while [ $( speed) -le 2048 ] ; do
  time tcpreplay -x $[ speed] -i eth1 [illegible]
  speed=`expr $[ speed] \* 2`
Done
```

$$R^2 = \frac{SS_{reg}}{SS_{tot}} [illegible]$$

$$SS_{reg} = \sum_{i=1}^{n} (\hat{y}_i - \bar{y}_i)^2$$

$$SS_{tot} = \sum_{i=1}^{n} (y_i - \bar{y}_i)^2$$

Speed	Expected	Pcapreplay	Tcpreplay
1	3600.000	3564.012	3564.962
2	1800.000	1781.646	1784.305
4	900.000	890.749	892.991
8	450.000	444.901	447.348
16	225.000	222.259	224.431
32	112.500	111.214	112.976
64	56.250	55.191	57.315
128	28.125	27.688	29.349
256	14.063	13.424	15.619
512	7.031	6.787	8.755
1024	3.516	3.457	5.340
2048	1.758	1.742	3.891

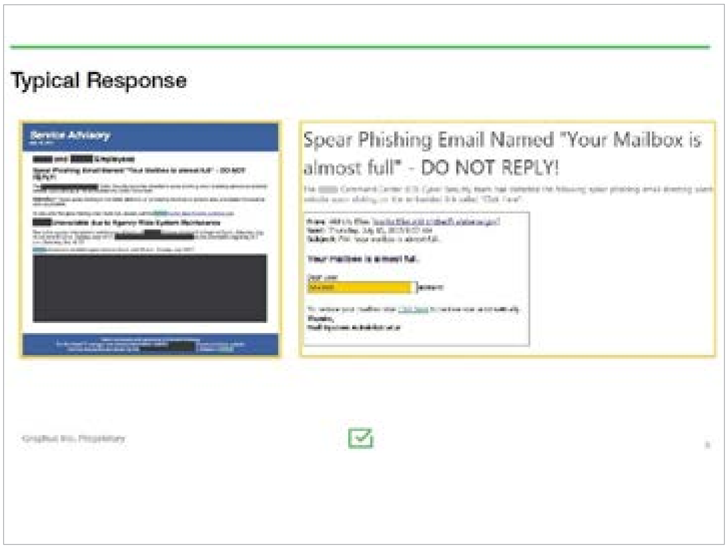
Spear Phishing: The Greatest Threat to Cyber Defenses

Manoj Srivastava, Co-founder and CEO, Graphus Inc.

The director of research at SANS Institute stated that according to a FISMA 2014 report, 69 percent of cyber-incidents reported by the private sector to U.S. CERT are phishing related. Ninety-five percent of all attacks on enterprise networks are the result of successful spear phishing. Why has email emerged as the favorite attack vector of cyber criminals and nation states? According to Mr. Srivastava, answer is simple: Email allows asynchronous, yet direct, contact with the person at the other end, exposing the enterprise to exploitation of human vulnerability to social engineering. With the availability of high-fidelity data from social media sites like LinkedIn and Facebook, mapping the "employee threat surface" of an organization is easy. Among LinkedIn, Facebook, and open Internet protocols, it is straightforward to identify high-value targets, customize the communications, and launch spear phishing that sails past all email security measures in place today. For this reason, every major data breach in the recent past has been traced back to a spear phishing email. Mr. Srivastava described how big data, security analytics, and threat intelligence could be leveraged for defending against spear phishing via Graphus.

Mr. Srivastava outlined several issues with the typical response as:

- Lack of visibility and control into email channel
- Longer response time for mitigation
- Ineffective threat detection and protection



Typical Response

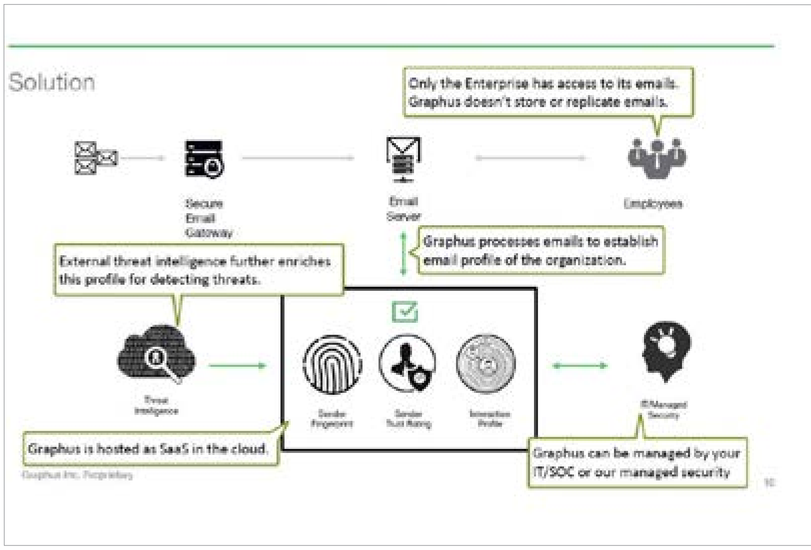
Service Advisory

[redacted] and [redacted] Employees

Spear Phishing Email Named "Your Mailbox is almost full" - DO NOT REPLY!

Your Mailbox is almost full.

Graphus Inc. Proprietary



Solution

Only the Enterprise has access to its emails. Graphus doesn't store or replicate emails.

Graphus processes emails to establish email profile of the organization.

External threat intelligence further enriches this profile for detecting threats.

Graphus is hosted as SaaS in the cloud.

Graphus can be managed by your IT/SOC or our managed security

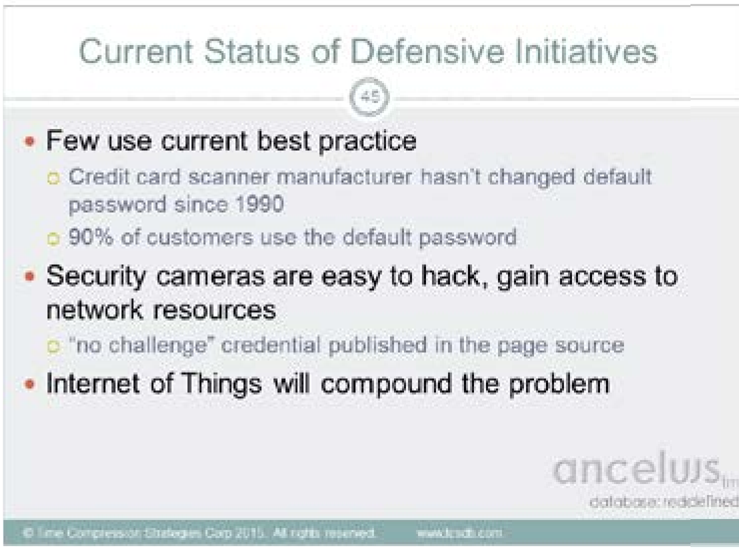
Graphus Inc. Proprietary

Rebuilding a Hardened Industrial Control Infrastructure

John Layden, President and Chief Executive Officer, Time Compression Strategies

Cyber security for industrial control systems (ICS) is more critical than traditional IT. Attacks on IT systems aim to steal stored information. Attacks on ICS systems aim to control or destroy critical infrastructure—including everything from the electrical grid to the food supply chain. They imply a major security and economic threat. Mr. Layden proposed a three-phase program to improve ICS security. Moving from passive defense, to active defense, to offense, his team maps a bridge from available technology to things needing to be invented. His analysis reveals the need to replace much of today's standard software practice. In particular, he proposes:

- Eliminate the ICS—make it unnecessary.
- Disconnect the ICS—non-networked or isolated net.
- Eliminate remote access to the ICS (or whitelist MAC ID).
- Eliminate all wireless access.
- Restrict physical access.
    - Computer room
    - Server
- No thumb drives allowed.
- Immediately implement Phase I.
- Begin moves to Phase II.



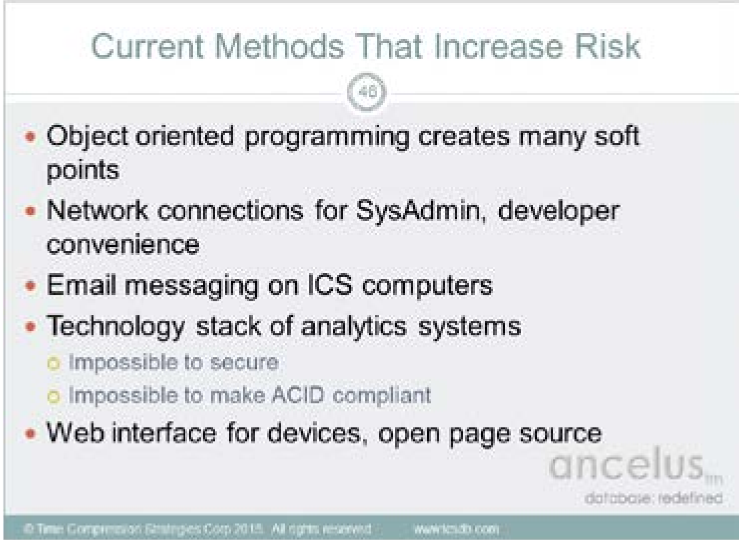
Current Status of Defensive Initiatives

45

- Few use current best practice
    - Credit card scanner manufacturer hasn't changed default password since 1990
    - 90% of customers use the default password
- Security cameras are easy to hack, gain access to network resources
    - "no challenge" credential published in the page source
- Internet of Things will compound the problem

ancelus™ database: redefined

© Time Compression Strategies Corp 2015. All rights reserved. www.icsdb.com



Current Methods That Increase Risk

46

- Object oriented programming creates many soft points
- Network connections for SysAdmin, developer convenience
- Email messaging on ICS computers
- Technology stack of analytics systems
    - Impossible to secure
    - Impossible to make ACID compliant
- Web interface for devices, open page source

ancelus™ database: redefined

© Time Compression Strategies Corp 2015. All rights reserved. www.icsdb.com

Characterizing Phishing Threats Using Natural Language Processing (NPL)

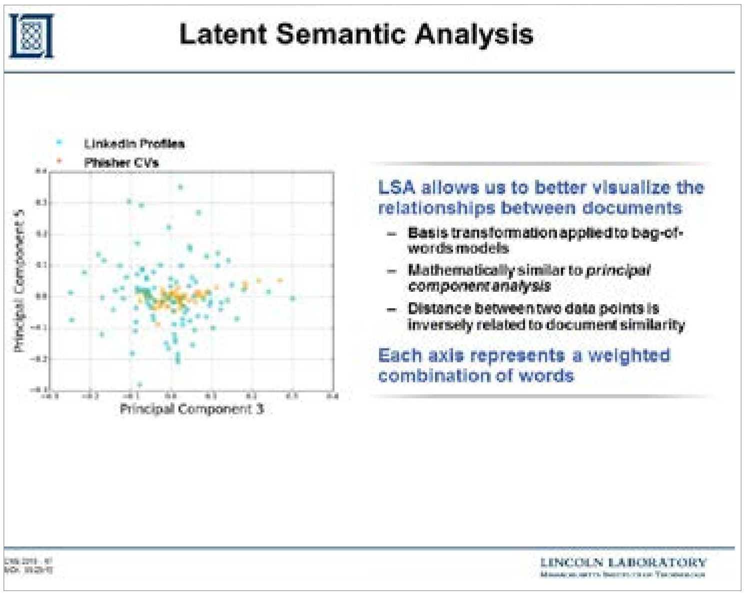
Michael Kotson, Technical Staff, Cyber Systems and Operations, MIT Lincoln Laboratory

Spear phishing is a widespread concern in the modern network security landscape. Few metrics measure the extent to which reconnaissance is performed on phishing targets. Spear phishing emails closely match the expectations of the recipient—based on details of their experiences and interests—making them a popular propagation vector for harmful malware. In his work with Dr. Alexia Schulz, Mr. Kotson used natural language processing techniques to investigate a specific real-world phishing campaign and to quantify attributes that indicated a targeted spear phishing attack. Their phishing campaign data sample comprised 596 emails—all containing a Web bug and a curriculum vitae (CV) PDF attachment—sent to their institution, MIT Lincoln Laboratory, by a foreign IP space.

The campaign exclusively targeted specific demographics within the institution. Performing a semantic similarity analysis between the senders' CV attachments and the recipients' LinkedIn profiles, the researchers concluded with high statistical certainty (p < 10-4) that the attachments contained targeted rather than randomly selected material. Latent semantic analysis further demonstrated that individuals who were a primary focus of the campaign received CVs that were highly topically clustered. These findings differentiated this campaign from those that leverage random spam.

Mr. Kotson wrapped up his presentation with a summary, including future work:

- The adversaries are targeting only researchers and lab leaders—no support staff, interns, or IT professionals.
- The probability that phisher/target pairs were randomly chosen is negligible (p-value < 10-4). This case study likely represents a spear phishing attack.
- The adversaries tend to "gang up" on targets of elevated interest. High-volume phishers seem to attack uncorrelated subgroups. CVs sent to a specific target tend to share similar vocabularies.
- NLP provides versatile tools for characterizing phishing attacks. These techniques could be generalized to study other spear phishing scenarios. If the phisher/target data are available, all analysis is automatic.
- Expand the interest profile data sample. A larger set of phisher CVs from similar campaigns is available. Possibly obtain official employee records from Human Resources?
- Analyze the development of phishing efforts over time. Do attacks become more or less targeted? Does the plan of attack evolve?
- Determine the likelihood that employees will be targeted in the future. Can we set a document similarity threshold? Could help inform an early warning system, lead to more effective employee training.
- Develop an effective counter to spear phishers' increasing reconnaissance.



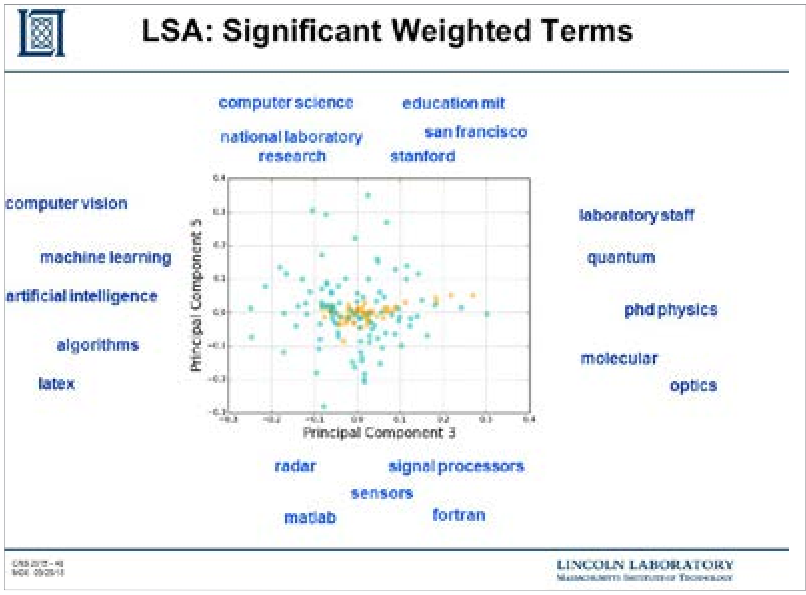
Latent Semantic Analysis

LSA allows us to better visualize the relationships between documents

- Basis transformation applied to bag-of-words models
- Mathematically similar to *principal component analysis*
- Distance between two data points is inversely related to document similarity

Each axis represents a weighted combination of words

LINCOLN LABORATORY
Massachusetts Institute of Technology



LSA: Significant Weighted Terms

computer science
education mit
national laboratory research
san francisco
stanford
computer vision
machine learning
artificial intelligence
algorithms
latex
laboratory staff
quantum
phd physics
molecular
optics
radar
signal processors
sensors
matlab
fortran

LINCOLN LABORATORY
Massachusetts Institute of Technology

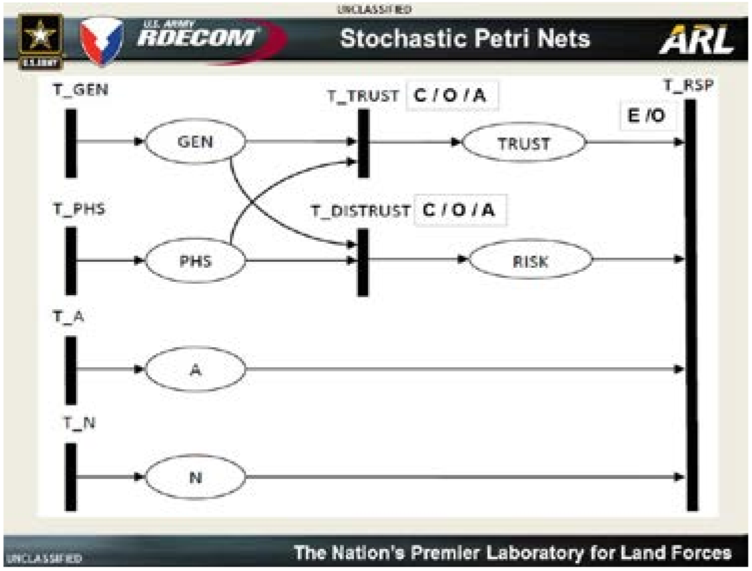
Effect of Personality Traits on Trust and Risk to Phishing Vulnerability: Modeling and Analysis

Jin-Hee Cho, Computer Scientist, U.S. Army Research Laboratory

In cyber space, various types of social engineering attacks have made humans in a system more vulnerable than ever. One of the popular social engineering attacks is a phishing attack that exploits humans' vulnerability in order to obtain individuals' private or credential information. Recently many studies investigate that the so called "phishing susceptibility," the likelihood of being phished, is closely co-related with the individuals' personality traits. In particular, the co-relationships between phishing susceptibility (i.e., vulnerability) and Big Five personality traits (i.e., openness, neuroticism, extroversion, agreeableness, and conscientiousness) have been analyzed through empirical studies in various domains, including psychology, computer science, management, and information technology. However, little prior work proposed a mathematical model investigating the effect of an individual's personality traits on perceived trust or risk and decision performance (i.e., correctness). In her presentation, Dr. Cho proposed a probability model using Stochastic Petri Nets (SPN) to investigate the effect of an individual human's personality traits on perceived trust and risk and decision performance. In conjunction with a team that included Hasan Cam and Alessandro Oltramari, Dr. Cho conducted comprehensive sensitivity analysis of key personality trait-related parameters through the evaluation of the developed SPN model. The results showed that agreeableness and neuroticism have significant effect on perceived trust and risk and decision performance, particularly when openness and conscientiousness are very low.

In her summation of the project, Dr. Cho explored the applicability and potential future directions for the SPN model:

- Use as a tool to predict phishing vulnerability in order to identify target personality people for security training or to create personality-focused security training content.
- Refine the model based on more aspects of co-relationships between key parameters based on empirical studies.
- Develop a Web-based application that evaluates a person's vulnerability and resilience to phishing attacks.


UNCLASSIFIED

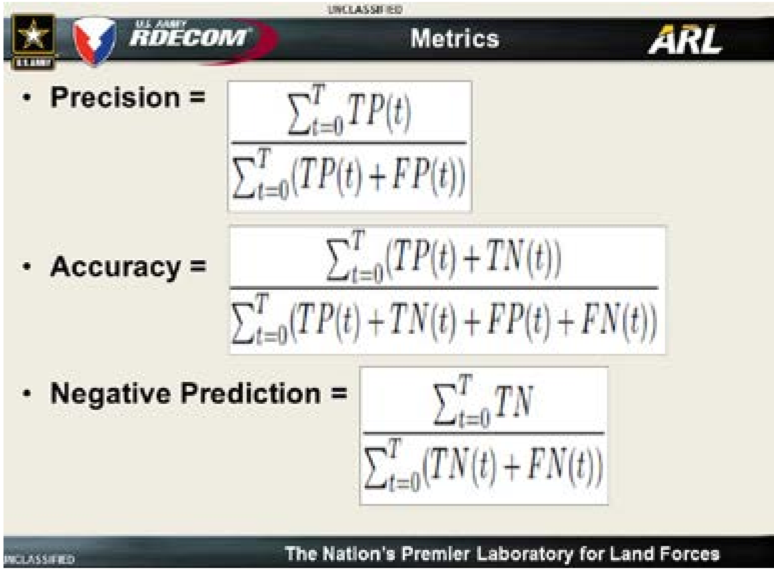
U.S. ARMY RDECOM

Stochastic Petri Nets

ARL

UNCLASSIFIED

The Nation's Premier Laboratory for Land Forces


UNCLASSIFIED

U.S. ARMY RDECOM

Metrics

ARL

- Precision = $\dfrac{\sum_{t=0}^{T} TP(t)}{\sum_{t=0}^{T} (TP(t) + FP(t))}$
- Accuracy = $\dfrac{\sum_{t=0}^{T} (TP(t) + TN(t))}{\sum_{t=0}^{T} (TP(t) + TN(t) + FP(t) + FN(t))}$
- Negative Prediction = $\dfrac{\sum_{t=0}^{T} TN}{\sum_{t=0}^{T} (TN(t) + FN(t))}$

UNCLASSIFIED

The Nation's Premier Laboratory for Land Forces

Speaker List

Massimiliano Albanese, Associate Director, Center for Secure Information Systems, George Mason University

Automotive Security: Securing Communications Within and Between Cars

Robert Altiero, Researcher and Owner, Robert Altiero

Digital Forensics Tool Interface Visualization

Michael Chipley, President and Chief Executive Officer, The PMC Group, LLC.
Matt Albertsen, Director of Engineering, Chinook Systems, Inc.

Cyber Securing Building Control Systems

Jin-Hee Cho, Computer Scientist, U.S. Army Research Laboratory

Effect of Personality Traits on Trust and Risk to Phishing Vulnerability: Modeling and Analysis

Nate Cimo, Managing Partner, Bowler Pons Solutions Consultants

Protecting Critical Infrastructure from Cyber-attack Through Technical Isolation

Joshua Edmison, Senior Scientist, Raytheon BBN Technologies

Opportunity Knocks: Defending Against Mixed Cyber + Physics Attacks Against Critical Infrastructure

William J. (Billy) Glodek, Former Network Security Branch Chief, U.S. Army Research Laboratory

Transitioning Cyber Security Research

Carlos Aguayo Gonzalez, Founder and Chief Technical Officer, PFP Cyber Security
Thurston Brooks, Vice President, Product Marketing, PFP Cyber Security

Physics-based Endpoint Intrusion Detection for Critical Infrastructure Devices

William Harrison, Associate Professor, University of Missouri

High-assurance Hardware: Is It Possible?

General Michael Hayden, Former Director, Central Intelligence Agency; U.S. Air Force, Retired

Cyber Security: Why Is This (Still) So Hard?

Frank Honkus, Command Post Technologies

Nation State Threats to ICS Through the Schmitt Analytical Framework

Steve Hutchinson, Researcher, ICF International

ICS Monitoring: Model Drift Paradigm

Michael Kotson, Technical Staff, Cyber Systems and Operations, MIT Lincoln Laboratory

Characterizing Phishing Threats Using Natural Language Processing (NPL)

John Layden, President and Chief Executive Officer, Time Compression Strategies

Rebuilding a Hardened Industrial Control Infrastructure

Dave Levin, Research Scientist, University of Maryland

The Ugly Truth About Certificate Revocation

Jo Lee Loveland Link, President, VOLVOX Inc.
John Link, Director of Operations, VOLVOX Inc.

Outthinking the Barbarians: The Agile Cyber Security Action Plan

Robert Mitchell, Scientist, Sandia National Laboratories

Dimension Reduction for Cyber-attack Detection and Analysis

Dhananjay Phatak, Associate Professor, Computer Science and Electrical Engineering Department, University of Maryland, Baltimore County

Toward Provable Security: Stopping CPS Attacks at the Interface Between Cyber and Physical

Paul Ritchey, Senior Project Manager, ICF International

IDS Architectural Design for High-volume Environments and Research

Alexia Schulz, MIT Lincoln Laboratory

Mission Assurance as a Function of Scale

Sidney (Chuck) Smith, Computer Scientist/Team Leader Product Integration and Testing Team, U.S. Army Research Laboratory

An Experimental Exploration of the Impact of Sensor-level Packet Loss on Network Intrusion Detection

Manoj Srivastava, Co-founder and CEO, Graphus Inc.

Spear Phishing: The Greatest Threat to Cyber Defenses

Dan Sullivan, Senior Principal Software Engineer, Raytheon

Demonstration of Cyber Threats to Legacy ICS Protocols

Michael Tope, Engineering Researcher, U.S. Department of Defense

Toward the Information Theoretic Limits of Anomaly Detection

Lee Trossbach, Senior Project Manager, ICF International

Garrett Payer, System Architect, ICF International

Virtual Reality for Cyber-analysis and Investigation

A. Selcuk Uluagac, Professor, Florida International University

Protecting Against Sensory-channels Threats in Cyber-Physical Systems

Samuel Visner, Senior Vice President and General Manager, Cyber Security, ICF International

Cyber Weapons Development and Testing—Detection, Attribution, Assessment, and Deterrence: An Important Challenge to the R&D Community

Wei Yu, Associate Professor, Towson University

Toward Secured Energy-based Critical Infrastructure

Dr. Michael Wertheimer, Former Research Director, NSA

Turning the Tide on Cyber Defense

John Wittkamper, Developer and Researcher, ICF International

Cnetmon: A Low-resource Network Interface Monitor for Situational Awareness

For questions, or to learn more, contact us at:

cybersci@icfi.com

About ICF International

ICF International (NASDAQ:ICFI) provides professional services and technology solutions that deliver beneficial impact in areas critical to the world's future. ICF is fluent in the language of change, whether driven by markets, technology, or policy. Since 1969, we have combined a passion for our work with deep industry expertise to tackle our clients' most important challenges. We partner with clients around the globe—advising, executing, innovating—to help them define and achieve success. Our more than 5,000 employees serve government and commercial clients from more than 70 offices worldwide. ICF's website is www.icfi.com.

CONNECT WITH US