Cyber Security Resiliency: Measuring the Myth & the Mission

DAVID MANZ, PHD
Pacific Northwest National Laboratory
Presentation to the University of Idaho Computer Science Colloquia March 2017
DOE’s Laboratory System is Solving America’s Toughest Challenges
PNNL leverages its science base to provide national leadership.
PNNL – FY2016 at a Glance

- $920.4M in R&D expenditures
- 4,400 scientists, engineers and non-technical staff
- 104 U.S. & foreign patents granted
- 2 FLC Awards, 2 R&D 100
- 1,058 peer-reviewed publications

- Mission-driven collaborations with government, academia and industry
- Among DOE’s top-performing labs; a premier chemistry, environmental sciences and data analytics laboratory
# PNNL’s Computing Capabilities

## Mission-Focused Technology Development

### Computing Environments

- High Performance Computing
- Quantum information science
- Large-scale data management
- Mobile and edge computing
- Embedded systems
- Cloud and streaming architectures

### Analytics

- Discrete mathematics and graph theory
- Human language technology
- Image processing
- Machine learning and recommender engines
- Social behavioral science

### Decision Support

- Information visualization
- Human-computer interaction
- Virtual and augmented reality
- Analytic tradecraft and critical thinking
- Collaboration systems

### Mission Applications

- Cyber-Physical Systems
- Biosurveillance
- Social media
- Forensics
- Emergency preparedness and response
- Biostatistics, proteomics, climate
- Power grid management
- Critical infrastructure resiliency
- Trafficking
PNNL’s Cyber Portfolio

- Cyber Security Research
- Cyber Security Operations
- Applied Cyber Security Solutions
- Cyber Analytics
Cyber Security Research

- Advancing and Formalizing the Science of Cyber Security
  - Experimentation and scientific methodology
  - Testbeds: cyberNET, powerNET
    - Dynamically reconfigurable and remotely accessible experimental environments for research, education/training, and commercial interoperability testing
    - Power, oil and gas, water, healthcare systems
  - Datasets

- Bio-inspired hypotheses
  - Digital Ants
  - MLSTONES

- Internal investments
  - Asymmetric Resilient Cybersecurity
Cyber Security Operations

- Cyber Network Defense
  - Partnership between Research and Operations
- Cyber Situational Awareness Systems
  - Cooperative Protection Program
  - Cyber Risk Information Sharing Program

March 20, 2017
CHALLENGE

A safe and reliable energy grid and network of industrial control systems requires new approaches to secure information sharing and prevention of cascading failures.

PNNL APPROACH

Wide-area situational awareness capabilities for critical infrastructures enable real-time operational response to active cyber threats.

PACRAT cyber-physical security programs include vulnerability assessments for SCADA and other control systems and secure control system protocols.
Component Security & Hardware Characterization

CHALLENGE

Ensure the integrity of mission-critical computer hardware and firmware components across the global supply chain.

PNNL APPROACH

Specialized diagnostic and monitoring tools enable identification of malicious code injection and pirated hardware.

Fingerprint mobile devices in crowded EM environment by exploiting artifacts in transmitted or emitted RF due to variability in device components.

Hardware-based CPU instruction set encryption prevents unauthorized code execution & creates unique devices to eliminate computing monoculture; minimally impacts performance, suited for embedded devices.
Cyber Analytics

CHALLENGE

Online threats evolve rapidly and are hidden in massive amounts of benign traffic; high-performance data processing and anomaly detection are needed.

PNNL APPROACH

PNNL’s behavior modeling algorithms and bio-inspired string matching have been used to search evidence of cyber compromise and malware.

A scalable visualization system for computer network communications helps analysts discover suspicious transactions.

March 20, 2017
PNNL’s cyber strategy will drive and enable a strategic national approach

- The defining security challenge of our time
- A key role for national labs
- A mandate for PNNL leadership
- Elevated PNNL leadership and substantial mission impact

SHAPE THE EMERGING CYBER BATTLEFIELD

- Reveal adversary strategy and tactics
- Counter adversary strategy and tactics at PNNL
- Control high-consequence systems
Cyber Security Problems Today

- Attribution
  - May not be an issue for you

- “Provable” security
  - Effectiveness
  - Measurability
  - Lifespan (silver bullet)

- Developing relevant security
  - Security in context

- Problem exists between chair and keyboard
  - Is the user to blame (phishing, watering hole, plugging in USB drives)?
  - Is the developer to blame?
  - What is the role of the human as a user and defender?

- Reliability vs. safety vs. security vs. resilience
Science of Cyber Security

Problem
- Treating as applied science without fundamental science foundation

Approach
- Methods for performing rigorous scientific research
- Theories for the field to begin building a body of knowledge
- Review field for successful research

Impact
- Move toward resilience for defender
- Enable metrics – ability to measure
- Support decision making
Cyber Security Science & Alchemy

- Transmute lead into Gold

$^{82}_{79}$Pb $\rightarrow$ $^{79}_{79}$Au

- Define mathematical laws for cyber phenomenology

March 20, 2017
Path Forward

- Best practices are necessary but not sufficient
  - See Verizon, Symantec, Mandiant, FBI, Tofino, GTRI, etc. reports
- Gain understanding
  - Of our own domain
  - Of the adversary
- Develop validatable and quantitative defenses and options for defender

Premise: This requires science
What Does Science Provide?

- **Experimentation**
  - Models/simulation
    - Biological examples
  - Testbeds

- **Evidence**
  - Repeatable
  - Reproducible
  - Falsifiable
  - Controlled biases

- **Observation**
  - Describe future behavior
  - Provide assurance
Attributes of cyber science:
Scientific questions

- Mechanics
  - Understanding the how and what of cyber space
  - Discrete vs continuous system modelling
  - Contextual specificity (dimensionality, ordinality, identity, speed)

- Measurements
  - Sensemaking (ascribing meaning)
  - Exploring exogenous and endogenous sensors (what is observable)
  - Significant units

- Cyber-Social Phenomenology
  - HCI
  - Techno-social cognition
  - Adversarial coevolution & competition

- Predictions (culmination)
  - Actuarial evidence
  - Cyber Forecasting (weather)
  - Quantifiable Cyber Risk
What is Resilience?

**Resilience:** The degree to which a cyber system will continue to support mission in the face of impediments

**Resilience: Characteristic of a system**
What do we measure

- Take a medium sized business that manufactures power control equipment
- Workstation “health” / security
  - Antivirus/ malware
- Network activity
  - IDS – detection
  - Firewalls -prevention
- Servers
  - SIEM
  - System Logs
- O.T.
  - Manufacturing plant
Classic Information Assurance

CIA
- Confidentiality
- Integrity
- Availability

Others could include auditing, authenticity, accountability, trustworthiness, non-repudiation, and privacy.
Availability Measures?

- Redundancy
- Diversity
- Functionality
- Restoration
- Honestly/ Trustworthiness
- Connected/ Open
- Deterministic
- Coordinated
Integrity Measures?

- reduced complexity
- simplicity (i.e. code)
- deflect (i.e. honey pot vs. firewall)
- Dynamic (moving target)
- Absorb
Confidentiality Measures?

- reduced attack surface
- deflect (i.e. honey pot vs. firewall)
- Dynamic (moving target)
- Deception
- Segmented/ Restricted
- Unpredictable
- Autonomous
Other security measures

- situational awareness
- forensic analysis
- Impact
- Cost
- Reserve Capacity (shields)
- sacrifice (retreating defense)
What about the mission/ business

- Continuity of Business CooB / operations/ planning/ missions/ government
  - Continues to perform essential functions
  - Sounds like resilience?
- How do you map from computer/ network to business
  - Assets
  - security
Human element

- Insider threat
- Espionage
- Theft
- Vandalism
- Activism
Resilience Values
Per Attack

Resilience Values

- Redundancy
- Diversity
- Functionality
- Dynamic
- Non-persistence
- Restricted access
- Reduced complexity
- Reduced attack surface
- Simplicity
- Situational awareness
- Coordinated
- Autonomous

March 20, 2017
Like any other risk

**Risk** is the probability of an event occurring in the context of the:
- Asset being protected
- Abilities of the adversary
- Vulnerabilities that can be exploited
- Harm that can be inflicted

Or is it?
- \( R \neq T \cdot V \cdot C \)
- Calculating risk is not static
Cyber resilience

- Which is cyber enabled mission resilience
- Which is a spider graph per attack, constantly updating per system
Discover fundamental science to improve effectiveness of technology

Develop and evaluate new defensive solutions

Transition technology for commercialization

Educate on issues and forthcoming R&D

Applied to:
- Cyber Analytics
- Component Security
- Control Systems Security
- Resilient Cyber Security
Questions?

Contact information:
David Manz, Ph.D.
(509) 372-5995
david@pnnl.gov