Full Scope Cybersecurity

Dr. Robert Templeman, SSTM
Distinguished Engineer for Cybersecurity

CAPT Mark Oesterreich, USN
Commanding Officer
NSWC Crane

Dr. Brett Seidle, SES
Technical Director
NSWC Crane
Naval Research & Development Establishment

Quick Facts
- Diverse and highly educated workforce with 25,000 scientists, engineers, and technicians (with more than 2,000 Ph.Ds).
- 20 commands across the NAVAIR/NAVSEA Warfare Centers, SPAWAR Systems Centers, ONR and NRL.
- Conducts RDT&E for the DoN to discover, develop, transition and field technologically superior naval warfighting capabilities.
- Unique Naval RDT&E facilities including laboratories, test facilities and test ranges.
- Serves as principal R&D agents for Navy and Marine Corps Program Executive Offices.
- Organizationally aligned to Naval Systems Commands and ONR:
  - Naval Sea Systems Command (NSWCs, NUWCs)
  - Naval Air Systems Command (NAWCS)
  - Space and Naval Warfare Systems Command (SSCCs)

Aggressive Research, Development, Test & Evaluation for reliable real world solutions.
Naval Surface Warfare Center, Crane Division

**QUICK FACTS**

3238 NSWC Crane Employees

67% Scientists, Engineers & Technicians

2 DoD Executive Agent Assignments

$1.3B Business Base

1 Mission

3 Focus Areas

- Electronic Warfare
- Strategic Missions
- Expeditionary Warfare

5 Technical Warrant Holders

87 PhD

584 Masters

1401 Bachelors
“There are three professions that beat their practitioners into a state of humility: farming, weather forecasting, and cybersecurity”

- Dan Geer
Challenging environments
Navy got woke

The 2014 Navy Cyber Awakening was the realization of a new risk calculus in cyber

Cybersecurity is a mission priority in the NAVSEA Campaign Plan

The Navy is embarking on a year-long effort to protect hardware and software across the service.

By Aliya Sternstein

The Navy is embarking on a year-long effort to protect hardware and software service-wide, as the Internet of Things takes hold of everything from ship speakers to missile launchers.

“Task Force Cyber Awakening” will draw from U.S. Cyber
Many organizations hold a limited view of cyber, often limited to threats against software and networks.
Many organizations hold a limited view of cyber, often limited to threats against software and networks.

Full-scope cyber recognizes the entirety of the computation stack as terrain that is contested (Talbot 2011).

Cyber terrain is entangled in the other warfighting domains.
Full Scope Cyber Attacks

**Computation stack**
- policy
- humans
- cultural norms
- societal norms
- organizational roles
- applications
- middleware
- data
- operating system
- firmware
- system hardware
- integrated circuits
- transistors
- atoms

**ANTHEM DATA BREACH**
- States where Anthem operates, including Indiana
- 14
- 80 million
  - People whose data was on the hacked server

**Leaked**
- Ashley Madison
  - Life is short. Find out who’s been cheating on you.
  - Over 38,855,000 anonymous members!
- Equifax
  - Personal information exposed
  - As many as 143 million customers
Full Scope Cyber Attacks

Computation stack
- policy
- humans
- cultural norms
- societal norms
- organizational roles

Software
- applications
- middleware
- data
- operating system

Hardware
- firmware
- system hardware
- integrated circuits
- transistors
- atoms

Build and Operate a Trusted DoDIN

Cybersecurity-Related Policies and Assessments Developed by the DOD
HARNESSING THE POWER OF TECHNOLOGY FOR THE WARFIGHTER
Full Scope Cyber Attacks

Computation stack
- policy
- humans
- cultural norms
- societal norms
- organizational roles

software
- applications
- middleware
- data
- operating system

hardware
- firmware
- system hardware
- integrated circuits
- transistors
- atoms

HARDWARE TROJAN - Attack of Doping

- Doping is a process for modifying the electrical properties of silicon by introducing tiny impurities like phosphorous, boron and gallium, into the crystal.

- By switching the doping on a few transistors, parts of the integrated circuit no longer work as they should. Because the changes happen at the atomic level, the stuff is hard to detect.
Our adversaries are maneuvering over the cyber terrain to exploit weaknesses in systems and organizations.

Critical systems require a full scope approach to cybersecurity.

Naval Surface Warfare Center Crane Division and other NAVSEA warfare center divisions have numerous efforts underway to develop capabilities where gaps currently exist.
Securing Hardware
Counterfeit microelectronics

“Experts have estimated that as many as 15 percent of all spare and replacement semiconductors purchased by the Pentagon are counterfeit. Overall, we estimate that counterfeiting costs US-based semiconductor companies more than $7.5 billion per year, which translates into nearly 11,000 lost American jobs.”

SIA President Brian Toohey SASC Hearing
November, 2011
Detecting counterfeits

The technology exists to photograph or x-ray components at scale (100% collection), but requires manual inspection.

Addressing supply chain risks through computer vision
- 3-year Navy contract with Indiana University (Professor David Crandall, SICE)
- Computationally inferring hardware configurations
- Detecting counterfeit devices
Enter deep learning

Securing Meatware

*protecting our systems from our users*
Phishing

“Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers’ personal identity data and financial account credentials (APWG 2017, Lastdrager 2014).”

- World Wide Threat (APWG 2017)
  - Lowest infection rate: Sweden – 20.03%
  - Highest infection rate: China – 47.09%

- Affects governments, industry, and individuals
  - “IRS Paid $5.8 Billion in Fraudulent Refunds, Identity Theft Efforts Need Work (Forbes 2015)”
  - Average estimated cost per attack per employee is $188.4 (Ponemon Institute 2015)
    - 48% of that loss comes from productivity loss
Mitigating phishing

- Email filtering
- Deactivating hyperlinks
- Preventing drive-by downloads
- User literacy and training
  - But how well does training work?
  - Measuring educational outcomes is complex, programmatic, and context dependent (Rychetnik, Frommer, Hawe, and Shiell 2002)
Mitigating phishing

Measuring Phishing Education: A Protocol

- Indiana University, Army, and Navy collaboration
- A study was performed
  - **Threat Detection Task**: Participants categorize web sites as malicious or benign by utilizing technical knowledge and familiarity with affected websites
  - **Methods**:
    - **Sample size**: 172 participants; Data collected with Amazon’s Mturk
    - **Procedure**: Visit 3 spoof and 3 no-spoof websites; decide whether to login or leave website by clicking on login or back buttons; bonus pay is dependent on response speed & accuracy
    - **Measures**: Survey data (Demographic, practical and technical security knowledge); accuracy scores based on logins to secure sites; and real-time measures of decision making (mouse tracking and response time)
  - **Area Under the Curve (AUC)**: area formed by connecting the mouse trajectory and the straight-line trajectory beginning at the start and finishing at the end points of the observed trajectory
  - **Sample Entropy**: Variability in the trajectory measures the disorder of a time series
Securing Systems
A brief history of (DoD) Cyber

- TCSEC/CC
- DITSCAP
- DIACAP
- RMF (NIST-based)

In general, we use compliance regimes to authorize operation.

Policy and controls are often additive devolving to large checklists.
As-applied problems

1. **Expensive / Time-Consuming.** The SANS 2016 IT Security Spending Trends Survey reported regulatory compliance as a much more significant driver for spending than, e.g., reducing attack surface, improving visibility (detection), new, advanced threats and techniques, and improving incident response.

2. **Distracting.** Defenders’ focus becomes compliance, not security.

3. **Inflexible.** Good security needs to imbue experts and decision makers with flexibility/discretion based on specific context.

4. **Stifles innovation.** Strict compliance regimes discourage any variance from “checking the box.” There’s a cost to tailoring with “compensating controls.

Credit: Craig Jackson, Indiana University Center for Applied Cybersecurity Research
Information Security Practice Principles

Comprehensivity ("Am I seeing the whole field, playing the long game?")
Identify and account for all relevant systems, actors, and risks in the environment.

Opportunity ("Am I taking advantage of my environment?")
Take advantage of the actor relationships, material resources, and strategic opportunities available in the environment.

Rigor ("What is correct behavior, and how am I ensuring it?")
Specify the expected state, behavior, and evaluation and accountability criteria of the relevant systems and actors, then enforce the same.

Minimization ("Can this be a smaller target?")
Minimize the size and quantity of what is to be protected, system complexity, and the number and proliferation of externally facing points of attack.

Compartmentation ("Is this made of distinct parts with limited interfaces?")
Isolate and control system elements to allow only the accesses and functions essential for their intended purposes.

Fault Tolerance ("What happens if this fails?")
Anticipate and address the potential compromise of system elements and the failure of security controls.

Proportionality ("Is this worth it?")
Tailor security strategies to the magnitude of the risks, accounting for the practical constraints imposed by the mission and the environment.
Summary

• We must adopt a full scope cybersecurity approach for our critical systems

• There are great improvements to be made in the areas of hardware assurance and behavioral cybersecurity

• NSWC Crane is working actively with government, industry, and academia to expand our Navy’s advantage by securing national defense systems