“The Dilemmas of Cybersecurity – Why is Everything Broken?”

Dr. William Scherlis, Institute for Software Research, Carnegie Mellon University

November 1, 2017 | 3:00 pm ET

- Today’s session will be recorded.
- An archive of today’s talk will be available at: www.sercuar.org/serc-talks/
- Use the Q&A box to queue questions, reserving the chat box for comments, and questions will be answered during the last 5-10 minutes of the session.
- If you are connected via the dial-in information only, please email questions or comments to Ms. Mimi Marcus at mmarcus@stevens.edu.
- Any issues? Use the chat feature for any technical difficulties or other comments, or email Ms. Mimi Marcus at mmarcus@stevens.edu.
The Systems Engineering Research Center (SERC) is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

Any views, opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense, ASD(R&E), nor the SERC.

No Warranty. This Stevens Institute of Technology Material is furnished on an “as-is” basis. Stevens Institute of Technology makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of the material. Stevens Institute of Technology does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

This material has been approved for public release and unlimited distribution.
The Dilemmas of Cybersecurity
—
Why is Everything Broken?

Bill Scherlis
CMU School of Computer Science
SERC Talks – 1 November 2017
What to wear
WannaCry ransomware
Sara,

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this is done ASAP.

If you or he has any questions, please reach out to me at 410.

--

-Charles

HFA Help Desk
The HFA Operations Team is here to support you. Let us know how we’re doing by filling out a brief survey <http://bit.ly/1gL3oMk>.
Rogers states that NSA had warned French officials ... that Russian hackers had compromised some elements of the election.

[SASC hearing [May 9, 2017]:](https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/)
OPM Breach
Equifax Breach Caused by Lone Employee’s Error, Former C.E.O. Says

The New York Times

BUSINESS DAY

MUST READS

After Massive Data Breach, Equifax Directed Customers To Fake Site

September 21, 2017 5:12 PM ET

MERRIT KENNEDY

Equifax Inc.

NYSE: EFX - Oct 27, 4:39 PM EDT

109.39 USD 0.43 (0.39%)

After-hours: 109.45 0.05%
Second Secretary and Chancery of the Bangladesh Embassy Probash Lamarong, Philippines Anti-Money Laundering Council Executive Director Julia Abad, AMLC member and Insurance Commissioner Emmanuel Dooc and, Attorney Inocencio Ferrer at the counting and verification of the turned-over money at the Central Bank of the Philippines headquarters in Manila Thursday [WSJ 1 Apr 16]
Ukraine power grid disruptions
Mirai DDoS botnet attack

- IoT devices target DNS
- Source code on github

https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/mirai-botnet/
https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/attack.c
How to promote your tweets:
Build “echo-chamber” networks to amplify Twitter presence.

Social influence bots used by ISIS and others:
The “echo chamber” model – a near-complete-graph of retweet bots on Twitter.
"A powerful explosion heard from miles away happened at a chemical plant in Centerville, Louisiana #ColumbianChemicals

"Is this really ISIS who is responsible for #ColumbianChemicals?

"Tell @Obama that we should bomb Iraq!"

Savchuk: **They get work specifications.**
*There are several main topics, Ukraine, USA and the EU.*
Six Dilemmas

1. Identity
2. Assessment
3. Engineering
4. Accountability
5. Deterrence
6. Commonality
Avalanche forecasting group provides critical data for commanders during cold res
Current DNI, retired Senator Dan Coats

... sailed through his nomination hearing to be the next Director of National Intelligence, promising to make **cybersecurity his top priority** [March 2017]

Former DNI James Clapper

“**Cyber ranks highest on worldwide threats to the U.S.**” [Feb 2016]

A modern car is a computer on wheels.

An aeroplane is a computer with wings.

The arrival of the “Internet of Things” will see computers baked into everything from road signs and MRI scanners to prosthetics and insulin pumps.

Hackers have already proved that they can take remote control of connected cars and pacemakers.

Computer security is a contradiction in terms.
1. Is the fatalism justified?
2. What is inhibiting decisive action?
3. What might that action be?
Six Dilemmas

1. Identity
2. Assessment
3. Engineering
4. Accountability
5. Deterrence
6. Commonality

Internet historical roots
- Small and mutually trusting community
- Eventually scale overtook trust

http://www.vox.com/a/internet-maps
1. Why is it so hard to attribute attacks?

- Diverse dimensions of identity on the Internet:
  - *Individuals* – Guccifer 2.0?
  - *Organizations* – Fancy Bear?
  - *Systems* – Tokelau phish host (myaccount.google.com-securitysettingpage.tk)?

- In practice: technical means + gumshoe work
  - Affirmed identity vs. cloaked identity vs. spoofed identity (false flag)

- The dilemma of identity and attribution:
  **How to accommodate the full spectrum of identity exposure and affirmation?**
  - Some goals
    - Operate across the gradient of exposure and affirmation:
      - Tax refund >> Online purchase >> Reviewing medical literature >> Human rights activists
    - Support affirmed identity when needed for transactions, etc.
    - Respect personal privacy as a societal value, enshrined in HIPAA, FERPA, etc.
      - Anonymous discourse has social benefit, also enables bad behavior
      - National/cultural norms vary
2. Why do we still struggle to assess our cyber risk?

- The dimensions of cyber risk are difficult to assess
  - Threat?
    - Nation-state and terror groups, criminal gangs, ...
  - Vulnerability?
    - Attack surface? Network exposure? Design weaknesses?
  - Consequences?
    - Direct: Financial, physical, etc.
    - Indirect: Reputational/intangible, privacy, etc.

- The dilemma of risk assessment:
  How to allocate resources to mitigate cyber risk when we cannot assess it effectively?

- Some goals
  - Measure these dimensions to enable prioritization of preparation
  - Develop useful actuarial models
    - Assess: Threats, knowledge, correlation, probabilities
    - Assess: Supply chain structure and potential hidden correlations (e.g., OpenSSL, zlib)
The aim of any testing scheme is to ensure that the customer gets substantially the software that he ordered and it must provide the customer with convincing evidence that this is so.

— NATO Software Engineering report 1968
3. Why can’t we build systems that are more secure?

• We don’t fully understand the software and systems that we build
  – Software is not reaching a technical plateau – the tide of abstraction continues to rise
    • Routine and repeatable activity gives way to automation
    • Hence, more creative work, engineering uncertainty, and measurement challenge
  – Assurance capability and confidence are advancing at a similar rapid pace
    • Production of evidence to support assurance claims is not routine practice
  – Software has become the most critical building material of our age (and materiel of cybersecurity)

• The dilemma of secure systems engineering:
  The dilemma of secure systems engineering: How to better integrate security into systems engineering practice?
  – Kinds of evidence: models, analyses, tests, etc.
  – Some goals
    • Architecture and requirements practice to integrate security
    • Tooling and team practice to integrate evidence production
    • Rapid evolution/re-evaluation
    • Living with bugs, through resiliency and robust design
    • Rapid innovation
4. Why is accountability so diffuse?

• How can we fairly allocate accountability and liability?
  – Software-based systems have tool chains and supply chains that are rich, diverse, and complex
    • **Components**: Computing infrastructure, networks, services, frameworks, libraries, components, intermediate langs
    • **Tools**: IDEs, analysis, testing, process support, managing engineering data
    • **Models and analyses**: to support evaluation and assurance judgments
  – Commercial norms – typical?
    • No guarantees regarding errors, performance, security
    • No reverse engineering – often construed to include security evaluation

• **The dilemma of accountability:**
  **How to allocate accountability to drive higher levels of security?**
  – Some goals
    • Specific promises regarding software-based systems
    • Business incentives
    • Architectural constraints to enable effective evaluation (cf. flight controls)
    • Progress for vehicle software, AI-based systems, etc.
5. Why is it difficult to deter attacks?

• Are there safe ways to retaliate when attacked?
  – “Active defense” is offense
  – Government can do this
    • Military doctrine: When to jump from cyber to kinetic
  – Individuals and firms cannot
    • Government can partner with firms in major attack response

• The dilemma of deterrence:
  What is the potential to respond actively to attacks in progress?
  – Some goals
    • More confident attribution: accountability, deterrence
    • Control over attribution for attacks we launch
6. Do we have too much commonality?

• How do we retain national leadership in computing technology?
  – There are multiple world-wide monocultures
    • Most major commercial and open source application platforms and frameworks
    • The synthetic terrain of the Internet, its services, and its architectures
  – Common platforms
    • Business benefits – go to market channels, etc.
    • Monoculture vulnerabilities
    • Benefits of innovation diffuse rapidly worldwide

• **The dilemma of commonality and diffusion:**
  How to operate when computing innovation diffuses world wide?
  – Some goals
    • Advantage over potential cyber adversaries
    • Monoculture benefits
    • Market leadership
• **Model the interactions among these issues**
  – Example (from a national perspective):
    • Accountability+ → Engineering+ → Assessment+ → Accountability+
    • Identity+ → Deterrence+, Accountability+

• **Address potential technical disruptors – examples:**
  – AI and autonomy in cyber-defense and cyber-offense (fast battle rhythm)
  – IoT security architectures and root of trust
  – Vehicle architectures that isolate safety critical and analog of flight controls
  – Evidence production in government acquisitions, even incrementally

• **Create S&T focal point to aggressively advance secure systems engineering**
  – Address linkage of cybersecurity with AI and autonomy
  – Address linkage of cybersecurity advancement with software advancement
  – Improve technical capacity for assessment and accountability
Addressing the Dilemmas – Some Thoughts, 2 of 2

• **Evolve business practices to drive enhanced security**
  – **Cost/benefit models** for assurances and supporting evidence
    • Business case models for long-term risk
    • Building-code models that support evolving engineering norms
  – **Supply chain** models identifying long-term benefits and risks
  – **Acquisition pivots**: Architecture. Evidence. IID. Managed evolution

• **Advance make-a-difference technical areas – examples:**
  – **Architectural** enablers for security
  – **Modeling, analysis, tooling, and data** capabilities
    • Evidence capture and dependency management
    • Technical modeling / analysis, with emphasis on composability
    • Languages and embedded DSLs with first-class assurances: typing, etc.
  – **Bolt-on** security capabilities for existing systems

1. Identity
2. Assessment
3. Engineering
4. Accountability
5. Deterrence
6. Commonality
Thank you

scherlis@cmu.edu
SERC 2017 Annual Events

6 days away…

REGISTER NOW

For more information or any questions regarding this event, please contact:

Ms. Monica Brito or Ms. Megan Clifford
UPCOMING TOPICS:

Successfully Applying Agile Methods for High-Criticality Systems

Talk Dates:
February 7, 2018 | Tentatively 11:00 AM ET
April 4, 2018 | 1:00 PM ET
June 6, 2018 | 1:00 PM ET

Presenters:
• Jan Bosch, Professor of Software Engineering, Director Software Center, Chalmers University of Technology
• Phyllis Marbach, INCOSE LA Chapter President; Senior Software Engineer at Boeing – Retired
• Robin Yeman, Lockheed Martin Fellow, Lockheed Martin (LM) Information Systems and Global Solution, Agile/evOpSec SME

Thank you for joining us!
Please check back on the SERC website for today’s recording and future SERC Talks information!