SYSTEMS ENGINEERING RESEARCH CENTER

SERC TALKS

WELCOME

"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.sercuarc.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.

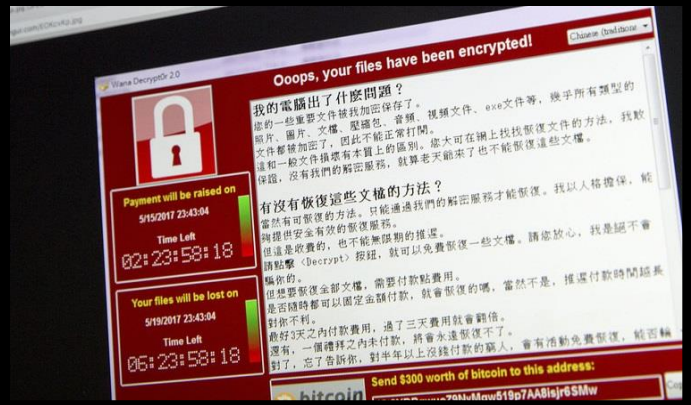
This material has been approved for public release and unlimited distribution.

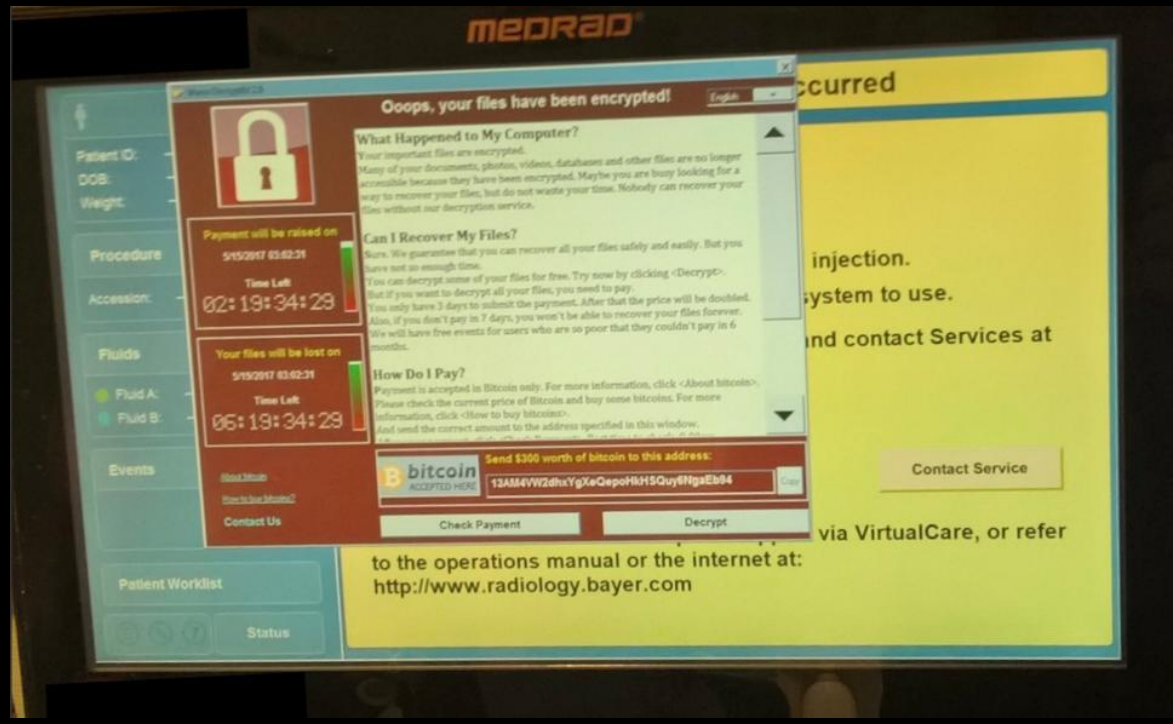
The Dilemmas of Cybersecurity
—
Why is Everything Broken?

Bill Scherlis
CMU School of Computer Science
SERC Talks – 1 November 2017

What to wear

WannaCry ransomware





From:john.podesta@gmail.com

To: peter_huffman@yahoo.com

Date: 2015-09-19 02:50

Subject: Re: Risotto

Yes and no

From: Charles[redacted]
Date: March 19, 2016 at 9:54:05 AM EDT
To: Sara[redacted]nton.com>, Shane H[redacted].com>
Subject: *Re: Someone has your password*

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[redacted]

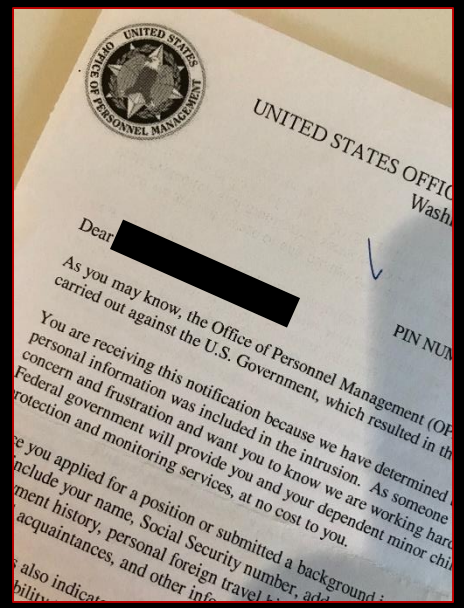
. . .

--
-Charles[redacted]
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>.

SASC hearing [May 9, 2017]:
Rogers states that NSA had warned French officials … that Russian hackers had compromised some elements of the election.

https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/

OPM Breach



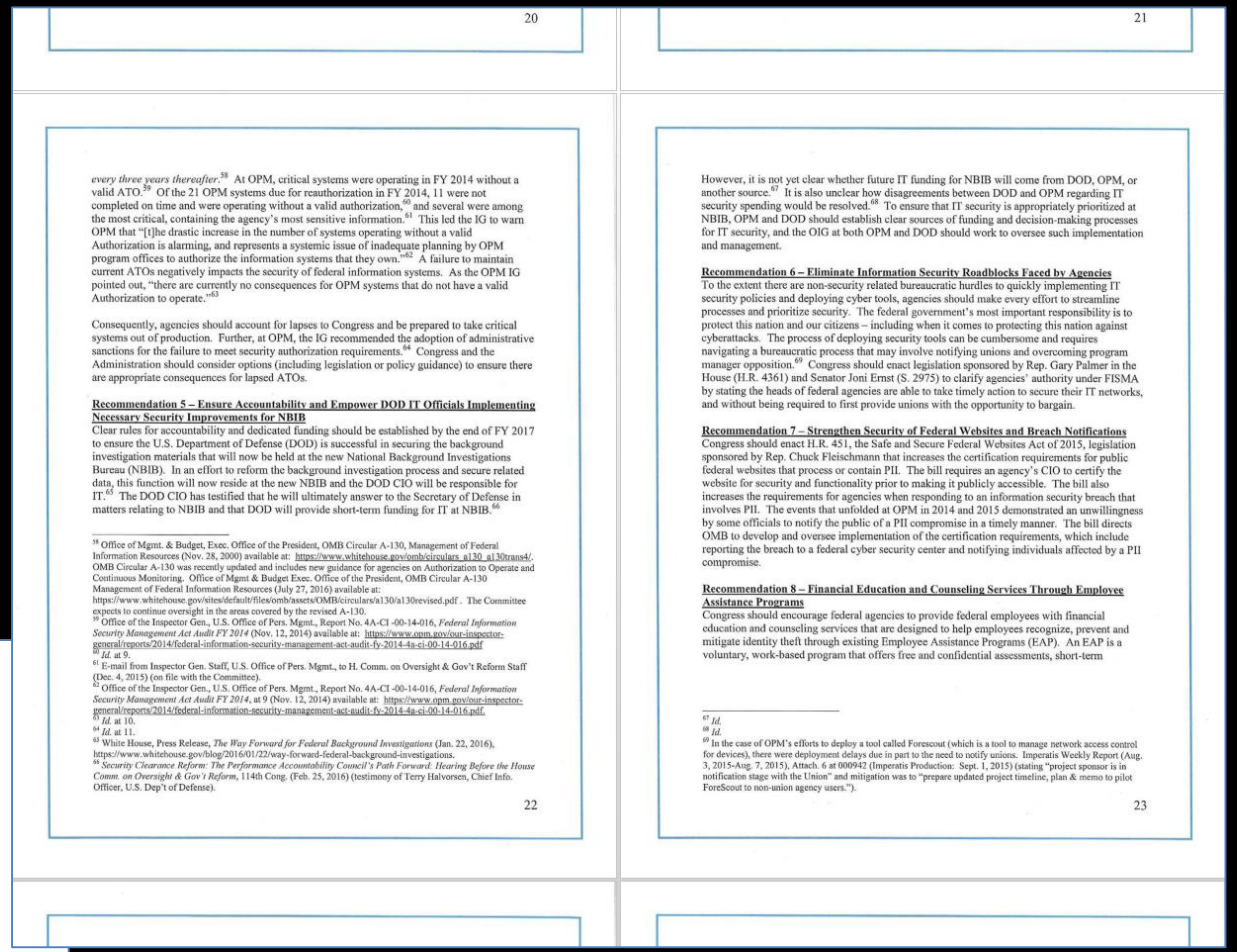
Committee on Oversight and Government Reform

U.S. House of Representatives

114th Congress

OVERSIGHT & GOVERNMENT REFORM EST 1814

The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation



20

21

every three years thereafter.[58] At OPM, critical systems were operating in FY 2014 without a valid ATO.[59] Of the 21 OPM systems due for reauthorization in FY 2014, 11 were not completed on time and were operating without a valid authorization,[60] and several were among the most critical, containing the agency's most sensitive information.[61] This led the IG to warn OPM that "[t]he drastic increase in the number of systems operating without a valid Authorization is alarming, and represents a systemic issue of inadequate planning by OPM program offices to authorize the information systems that they own."[62] A failure to maintain current ATOs negatively impacts the security of federal information systems. As the OPM IG pointed out, "there are currently no consequences for OPM systems that do not have a valid Authorization to operate."[63]

Consequently, agencies should account for lapses to Congress and be prepared to take critical systems out of production. Further, at OPM, the IG recommended the adoption of administrative sanctions for the failure to meet security authorization requirements.[64] Congress and the Administration should consider options (including legislation or policy guidance) to ensure there are appropriate consequences for lapsed ATOs.

Recommendation 5 – Ensure Accountability and Empower DOD IT Officials Implementing Necessary Security Improvements for NBIB

Clear rules for accountability and dedicated funding should be established by the end of FY 2017 to ensure the U.S. Department of Defense (DOD) is successful in securing the background investigation materials that will now be held at the new National Background Investigations Bureau (NBIB). In an effort to reform the background investigation process and secure related data, this function will now reside at the new NBIB and the DOD CIO will be responsible for IT.[65] The DOD CIO has testified that he will ultimately answer to the Secretary of Defense in matters relating to NBIB and that DOD will provide short-term funding for IT at NBIB.[66]

[58] Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-130, Management of Federal Information Resources (Nov. 28, 2000) available at: https://www.whitehouse.gov/omb/circulars_a130_a130trans4/. OMB Circular A-130 was recently updated and includes new guidance for agencies on Authorization to Operate and Continuous Monitoring. Office of Mgmt & Budget Exec. Office of the President, OMB Circular A-130 Management of Federal Information Resources (July 27, 2016) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf . The Committee expects to continue oversight in the areas covered by the revised A-130.

[59] Office of the Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI -00-14-016, *Federal Information Security Management Act Audit FY 2014* (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf

[60] *Id.* at 9.

[61] E-mail from Inspector Gen. Staff, U.S. Office of Pers. Mgmt., to H. Comm. on Oversight & Gov't Reform Staff (Dec. 4, 2015) (on file with the Committee).

[62] Office of the Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI -00-14-016, *Federal Information Security Management Act Audit FY 2014*, at 9 (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.

[63] *Id.* at 10.

[64] *Id.* at 11.

[65] White House, Press Release, *The Way Forward for Federal Background Investigations* (Jan. 22, 2016), https://www.whitehouse.gov/blog/2016/01/22/way-forward-federal-background-investigations.

[66] *Security Clearance Reform: The Performance Accountability Council's Path Forward: Hearing Before the House Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 25, 2016) (testimony of Terry Halvorsen, Chief Info. Officer, U.S. Dep't of Defense).

22

However, it is not yet clear whether future IT funding for NBIB will come from DOD, OPM, or another source.[67] It is also unclear how disagreements between DOD and OPM regarding IT security spending would be resolved.[68] To ensure that IT security is appropriately prioritized at NBIB, OPM and DOD should establish clear sources of funding and decision-making processes for IT security, and the OIG at both OPM and DOD should work to oversee such implementation and management.

Recommendation 6 – Eliminate Information Security Roadblocks Faced by Agencies

To the extent there are non-security related bureaucratic hurdles to quickly implementing IT security policies and deploying cyber tools, agencies should make every effort to streamline processes and prioritize security. The federal government's most important responsibility is to protect this nation and our citizens – including when it comes to protecting this nation against cyberattacks. The process of deploying security tools can be cumbersome and requires navigating a bureaucratic process that may involve notifying unions and overcoming program manager opposition.[69] Congress should enact legislation sponsored by Rep. Gary Palmer in the House (H.R. 4361) and Senator Joni Ernst (S. 2975) to clarify agencies' authority under FISMA by stating the heads of federal agencies are able to take timely action to secure their IT networks, and without being required to first provide unions with the opportunity to bargain.

Recommendation 7 – Strengthen Security of Federal Websites and Breach Notifications

Congress should enact H.R. 451, the Safe and Secure Federal Websites Act of 2015, legislation sponsored by Rep. Chuck Fleischmann that increases the certification requirements for public federal websites that process or contain PII. The bill requires an agency's CIO to certify the website for security and functionality prior to making it publicly accessible. The bill also increases the requirements for agencies when responding to an information security breach that involves PII. The events that unfolded at OPM in 2014 and 2015 demonstrated an unwillingness by some officials to notify the public of a PII compromise in a timely manner. The bill directs OMB to develop and oversee implementation of the certification requirements, which include reporting the breach to a federal cyber security center and notifying individuals affected by a PII compromise.

Recommendation 8 – Financial Education and Counseling Services Through Employee Assistance Programs

Congress should encourage federal agencies to provide federal employees with financial education and counseling services that are designed to help employees recognize, prevent and mitigate identity theft through existing Employee Assistance Programs (EAP). An EAP is a voluntary, work-based program that offers free and confidential assessments, short-term

[67] *Id.*

[68] *Id.*

[69] In the case of OPM's efforts to deploy a tool called Forescout (which is a tool to manage network access control for devices), there were deployment delays due in part to the need to notify unions. Imperatis Weekly Report (Aug. 3, 2015-Aug. 7, 2015), Attach. 6 at 000942 (Imperatis Production: Sept. 1, 2015) (stating "project sponsor is in notification stage with the Union" and mitigation was to "prepare updated project timeline, plan & memo to pilot ForeScout to non-union agency users.").

23

Equifax

SECTIONS HOME SEARCH

The New York Times

SUBSCRIBE NOW LOG IN

How Floyd Mayweather Helped Two Young Guys From Miami Get Rich

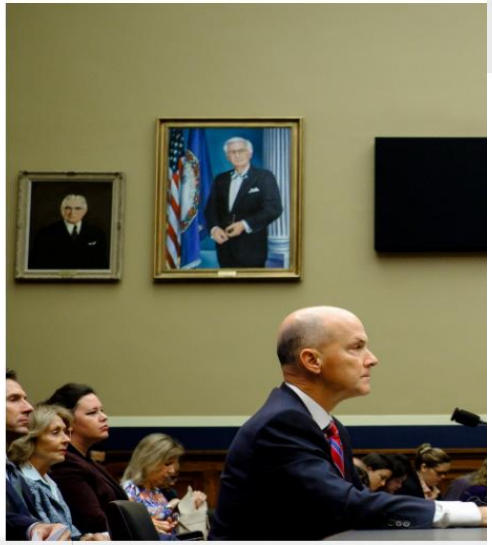
CORNER OFFICE
How to Be a C.E.O., From a Decade's Worth of Them

Hearing Amazon's Footsteps, the Health Care Industry Shudders

BUSINESS DAY

Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says

By TARA SIEGEL BERNARD and STACY COWLEY OCT. 3, 2017



the two-way BREAKING NEWS FROM NPR

MUST READS

After Massive Data Breach, Equifax Directed Customers To Fake Site

September 21, 2017 · 5:13 PM ET

MERRIT KENNEDY

Equifax is facing criticism because after the security incident it chose to create an entirely new domain for customers to check

9

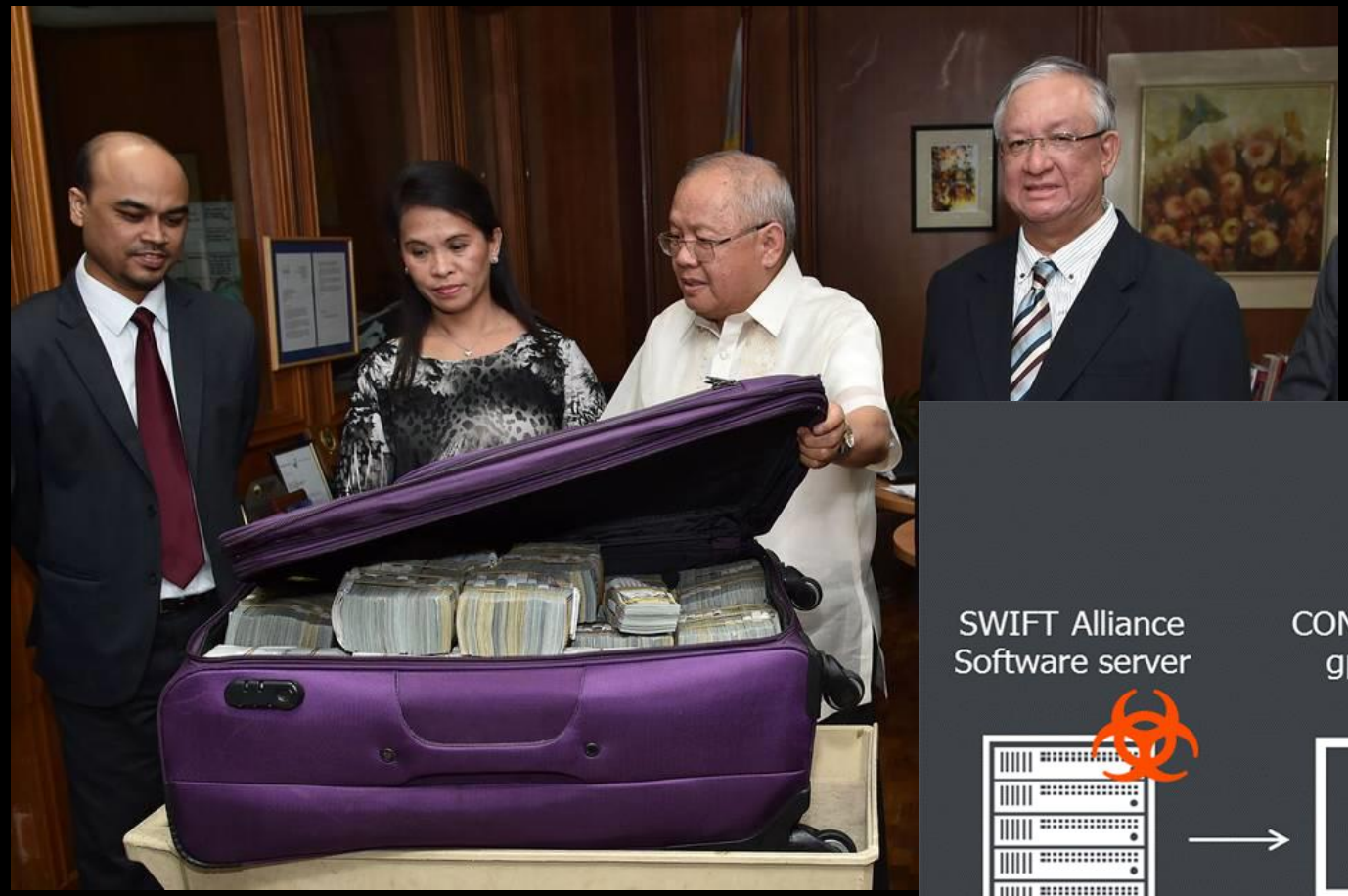
MARKETS CHART OF THE DAY

SOURCE: Markets Insider

BUSINESS INSIDER

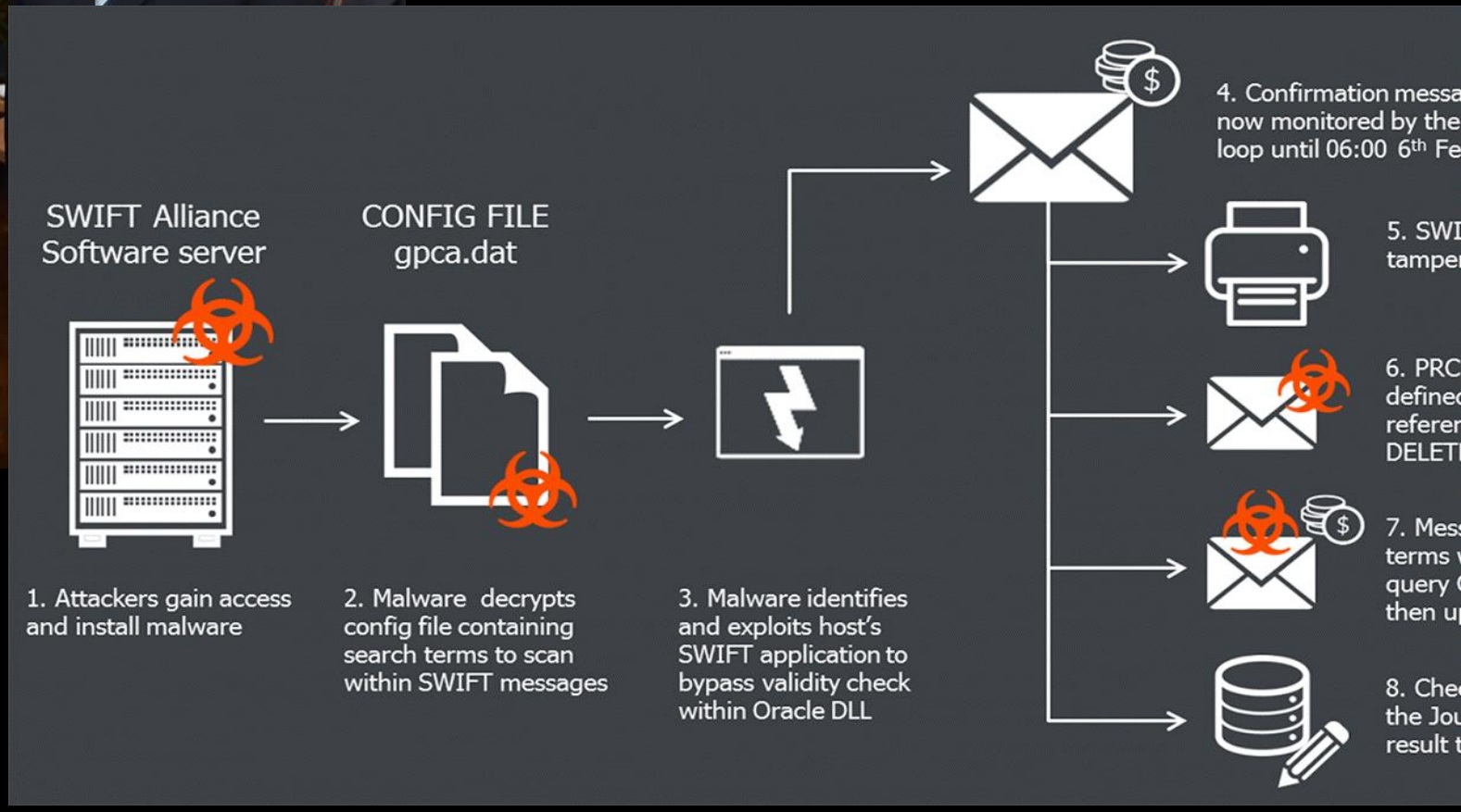
Equifax Inc.
NYSE: EFX - Oct 27, 4:39 PM EDT

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]

Bangladesh SWIFT theft



http://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html

Ukraine power grid disruptions

How Cyberattack Shut Down Ukrainian Power Companies

Phishing Emails

BlackEnergy 3

VPN & Credential Theft

Network & Host Discovery

Malicious Firmware Development

SCADA Hijack (HMI/Client)

Breaker Open Commands

UPS Modification

Firmware Upload

KillDisk Overwrites

Power Outage(s)

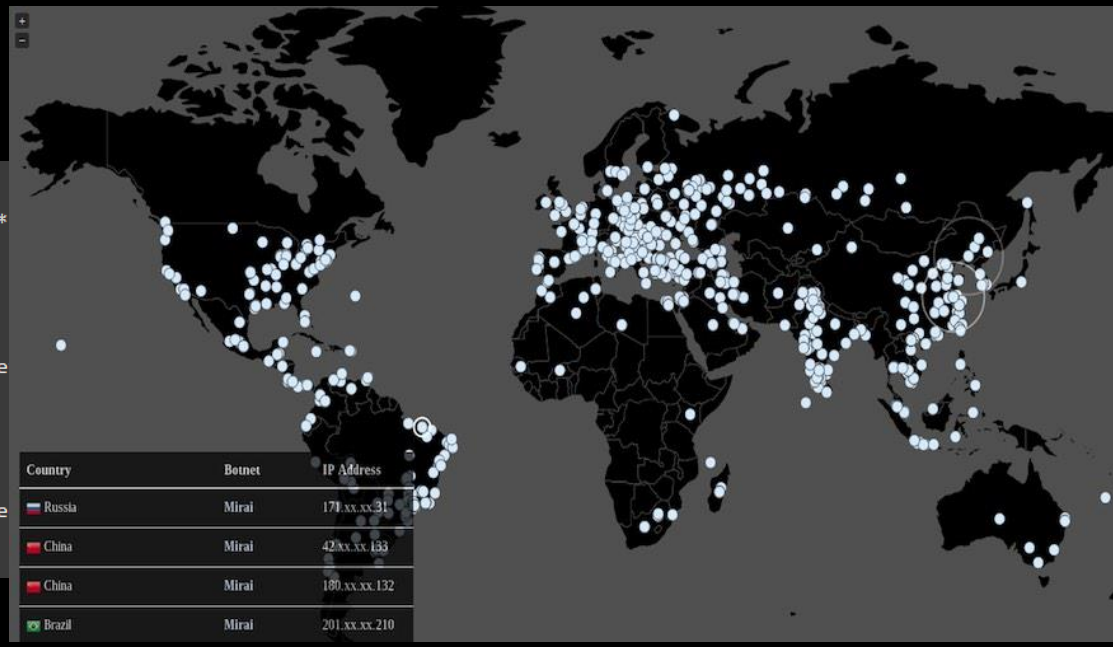
Source: NERC Electricity Information Sharing and Analysis Center, SANS Industrial Control Systems

http://foreignpolicy.com/2016/01/08/did-russia-knock-out-ukraines-power-grid/

Mirai DDoS botnet attack

- IoT devices target DNS
- Source code on github

```
#define ATK_VEC_UDP         0  /* Straight up UDP flood */
#define ATK_VEC_VSE         1  /* Valve Source Engine query flood *
#define ATK_VEC_DNS         2  /* DNS water torture */
#define ATK_VEC_SYN         3  /* SYN flood with options */
#define ATK_VEC_ACK         4  /* ACK flood */
#define ATK_VEC_STOMP       5  /* ACK flood to bypass mitigation de
#define ATK_VEC_GREIP       6  /* GRE IP flood */
#define ATK_VEC_GREETH      7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY       8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN   9  /* Plain UDP flood optimized for spe
#define ATK_VEC_HTTP        10 /* HTTP layer 7 flood */
```




```
8\x6F\x49\x4D\x12\x43\x46\x4F\x4B\x4C", 1); // root     7ujMko0admin
1\x56\x47\x4F", 1);                        // root     system
5\x40", 1);                                // root     ikwb
7\x43\x4F\x40\x4D\x5A", 1);                // root     dreambox
7\x50", 1);                                // root     user
3\x4E\x56\x47\x49", 1);                    // root     realtek
2\x12\x12\x12\x12", 1);                    // root     00000000
3\x13\x13\x13\x13", 1);                    // admin    1111111
0\x11\x16", 1);                            // admin    1234
0\x11\x16\x17", 1);                        // admin    12345
6\x11\x10\x13", 1);                        // admin    54321
0\x11\x16\x17\x14", 1);                    // admin    123456
7\x48\x6F\x49\x4D\x12\x43\x46\x4F\x4B\x4C", 1); // admin    7ujMko0admin
1\x10\x13", 1);                            // admin    1234
3\x51\x51", 1);                            // admin    pass
7\x4B\x4C\x51\x4F", 1);                    // admin    meinsm
1\x4A", 1);                                // tech     tech
```

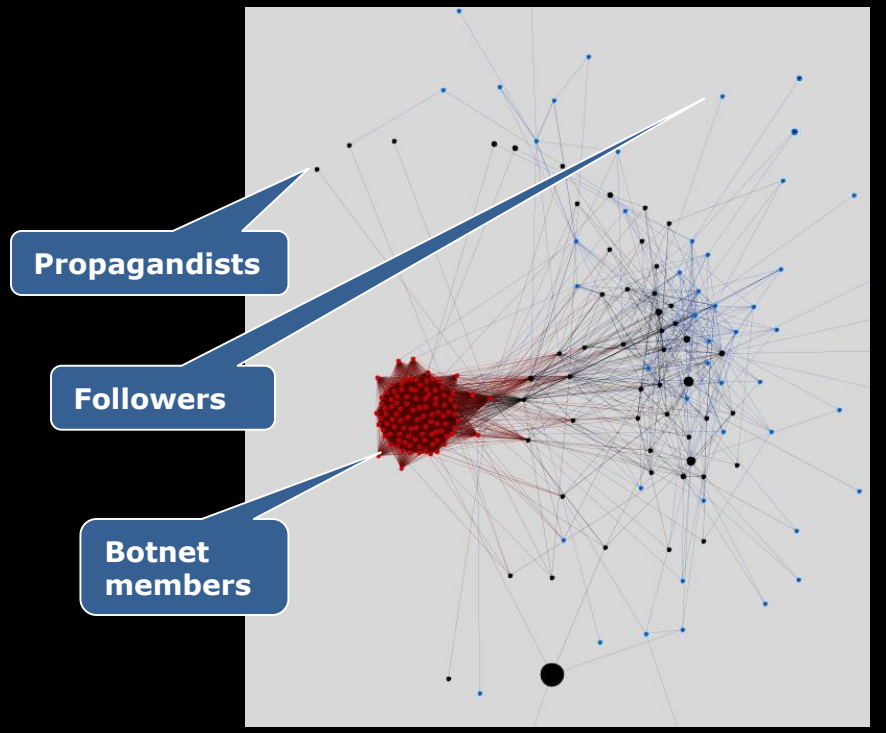
```
148     cleanup:
149     if (targs != NULL)
150         free(targs);
151     if (opts != NULL)
152         free_opts(opts, opts_len);
153 }
154
155 void attack_start(int duration, ATTACK_
156 {
157     int pid1, pid2;
158
159     pid1 = fork();
160     if (pid1 == -1 || pid1 > 0)
161         return;
162
163     pid2 = fork();
164     if (pid2 == -1)
165         exit(0);
166     else if (pid2 == 0)
167     {
168         sleep(duration);
169         kill(getppid(), 9);
170         exit(0);
171     }
172     else
173     {
174         int i;
175
176         for (i = 0; i < methods_len; i
177         {
178             if (methods[i]->vector ==
```

https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/mirai-botnet/
http://wccftech.com/who-what-why-fridays-brutal-ddos-attack-destroying-internet/
https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/attack.c

Twitter echo chamber bots

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.



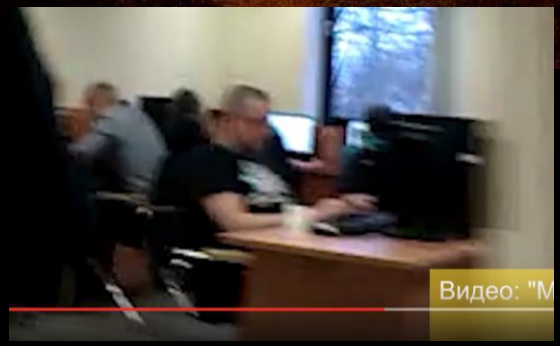
Russian Active Measures

“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!”

The Internet Research Agency
55 Savusahkina Street, St. Petersburg



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

http://www.telegraph.co.uk/news/worldnews/europe/russia/11656043/My-life-as-a-pro-Putin-propagandist-in-Russias-secret-troll-factory.html
http://www.dailykos.com/story/2017/3/30/1648777/-The-Russian-troll-army-that-swung-the-election-for-Trump

https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Six Dilemmas

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

http://www.eucom.mil/media-library/article/20010/avalanche-forecasting-group-provides-critical-data-for-commanders-during-cold-res

Threats

Vulnerabilities

Consequences

Business norms

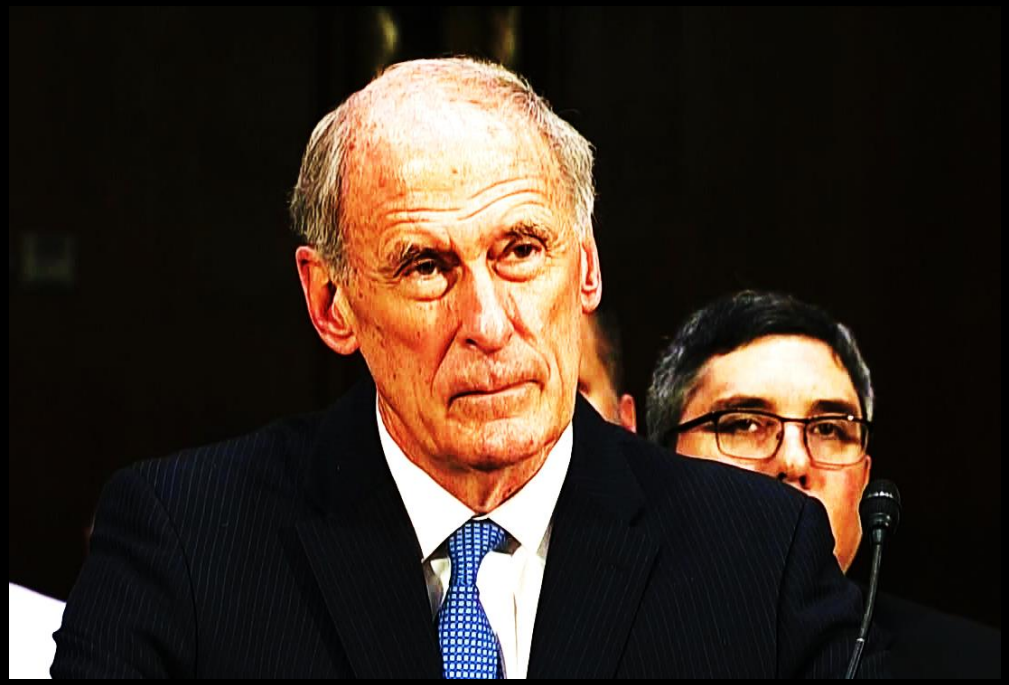
Policy influences

Public good

National advantage

Former DNI **James Clapper**

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



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]

http://www.washingtontimes.com/news/2015/feb/26/james-clapper-intel-chief-cyber-ranks-highest-worl/
https://federalnewsradio.com/hearingsoversight/2017/03/dni-nominee-plans-evaluate-streamline-intelligence-community-operations/

[Apr 2017]


Leaders

The myth of cyber-security

Computers will never be secure. To manage the risks, look to economics rather than technology

COMPUTER security is a contradiction in terms. Consider the past year alone: cyber-

of expertise will always hamper the ab
ers to protect themselves. So govern
"public health" for computing. They c

Computer security is a contradiction in terms.

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.

Economist 8-14 April 17

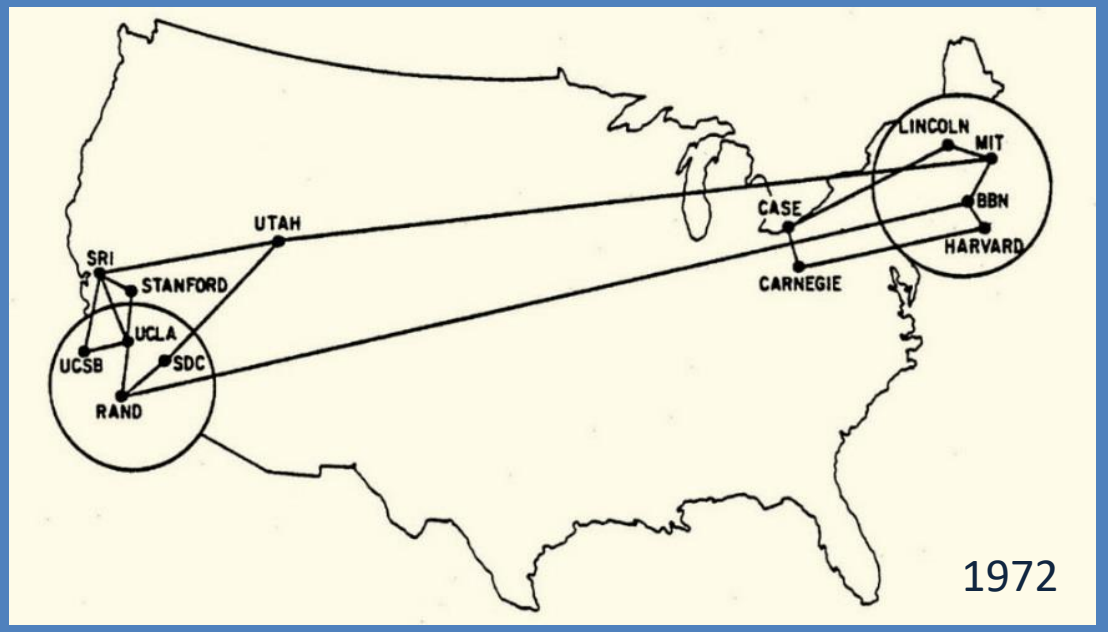
1. Is the fatalism justified?

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?*
    - *User / operator human actions? Supply chain exposure? Insider exposure?*
  - 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 awesome Walt Kelly

https://clipartfest.com/download/ANd9GcQaTCBXUu1FtxYAXsicpL3n79_U0sU15uKi6uOeRbthBJii8BmHC-iL8Q4S.html

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:*
  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

Addressing the Dilemmas – Some Thoughts, 1 of 2

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

- **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

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

- **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
  - **Insurance risk** models: Hidden correlations. Adversaries. Evidence and analysis.
  - **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
    - Framework design. Intermediate languages. Encapsulation / isolation.
  - 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

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

SERC TALKS

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!