Why Digital Systems Weaken Resilience and 6 Steps to Offset That

Richard Danzig

Resilience Week

August 2015

Good News!

Resilience is Commonly Challenged And Understood

- Capacity to Restore to Sustained Effective Operation
- Everyday & Black Swan Experiences
- Environmental, Natural, & Malevolent Experiences
- Katrina & Fukushima
- Sandy (Our Successes are Less Studied!)

Resilience Widely Recognized As a Priority

- Military Systems
- Financial Systems
- Communication Systems
- Power Systems

Digital Systems Add to Resilience

- Information Systems Assist Situational Awareness
- Communication Systems Assist Balanced Response
- Data Integration Assists Reallocation of Assets
- Digitization Abets Diagnosis and Simulation of Repair

Bad News!

So What's the Cyber Problem?

- Bugs
- Adversaries
  - State Adversaries
  - Terrorists (including Eco-terrorists)
  - Criminals (theft/ransom)
  - Ill-motivated insiders
  - Hackers/pranksters

1999: Unrestricted Warfare Qiao Liang & Wang Xiangsui

- "[R]eduction of the functions of warfare in a pure sense does not mean at all that war has ended…. It has only re-invaded human society in a more complex, more extensive, more concealed, and more subtle manner…. [W]hile we are seeing a relative reduction in military violence, at the same time we definitely are seeing an increase in political, economic, and technological violence."

The Power of the Problem

- Subverts Standard Safety and Reliability Analysis
- Previously Independent Processes Now Have a Common Failure Point
- Previously Separate Processes Now Can be Destructively Coordinated
- Warning Time May be Zero; Precedents May be Nil

This Shouldn't Be News!

Alert From ICS-CERT 12/10/14

"… a sophisticated malware campaign … has compromised numerous industrial control systems (ICSs) environments [with] BlackEnergy malware…. [T]his campaign has been ongoing since at least 2011. Multiple companies … have identified the malware on Internet-connected human-machine interfaces (HMIs)….

CS-CERT has not been able to verify if the intruders expanded access beyond the compromised HMI into the remainder of the underlying control system. However, typical malware deployments have included modules that search out … additional lateral movement within the affected environment."

Root Causes of Digital Insecurity

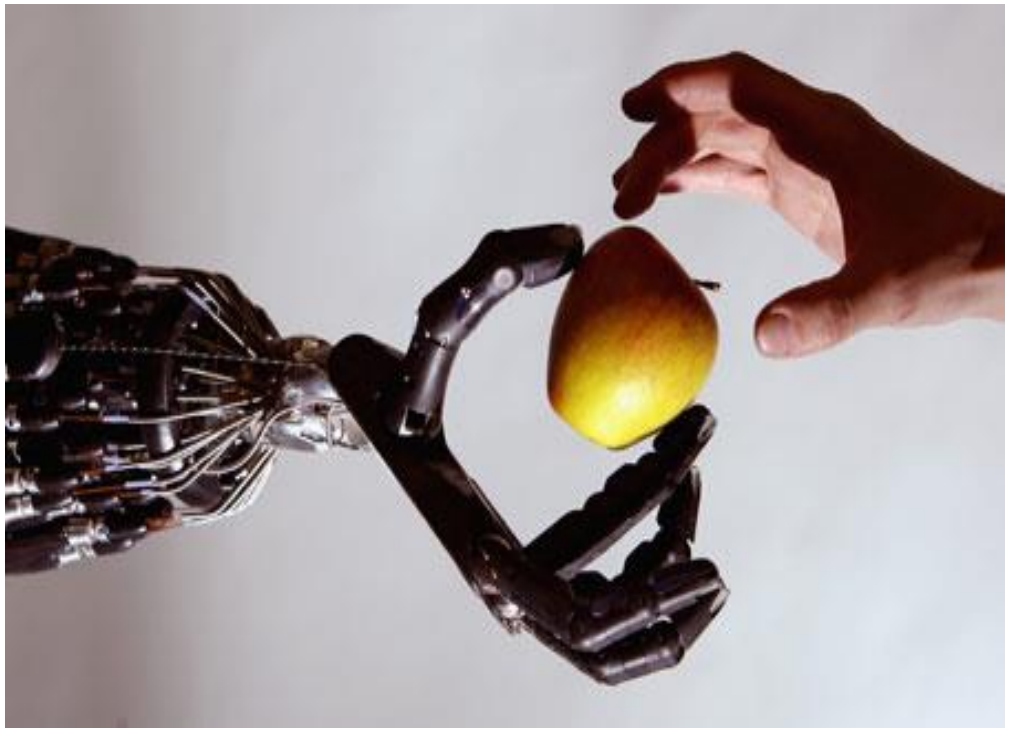
- Complexity
  - Microsoft Operating System Code – At least 50 Million Lines
  - A Major Investment House – 1 Trillion Lines of Code
- Complexity is Compounded by Extensibility
  - Integration with Other Software (eg Adobe)
  - Integration with Legacy and Future Systems

Amplifying Causes of Digital Insecurity

- Communication
- Concentration
- Collection
- Disintermediation
- Flexibility

Risk is Inherent in the Benefits of the Technology

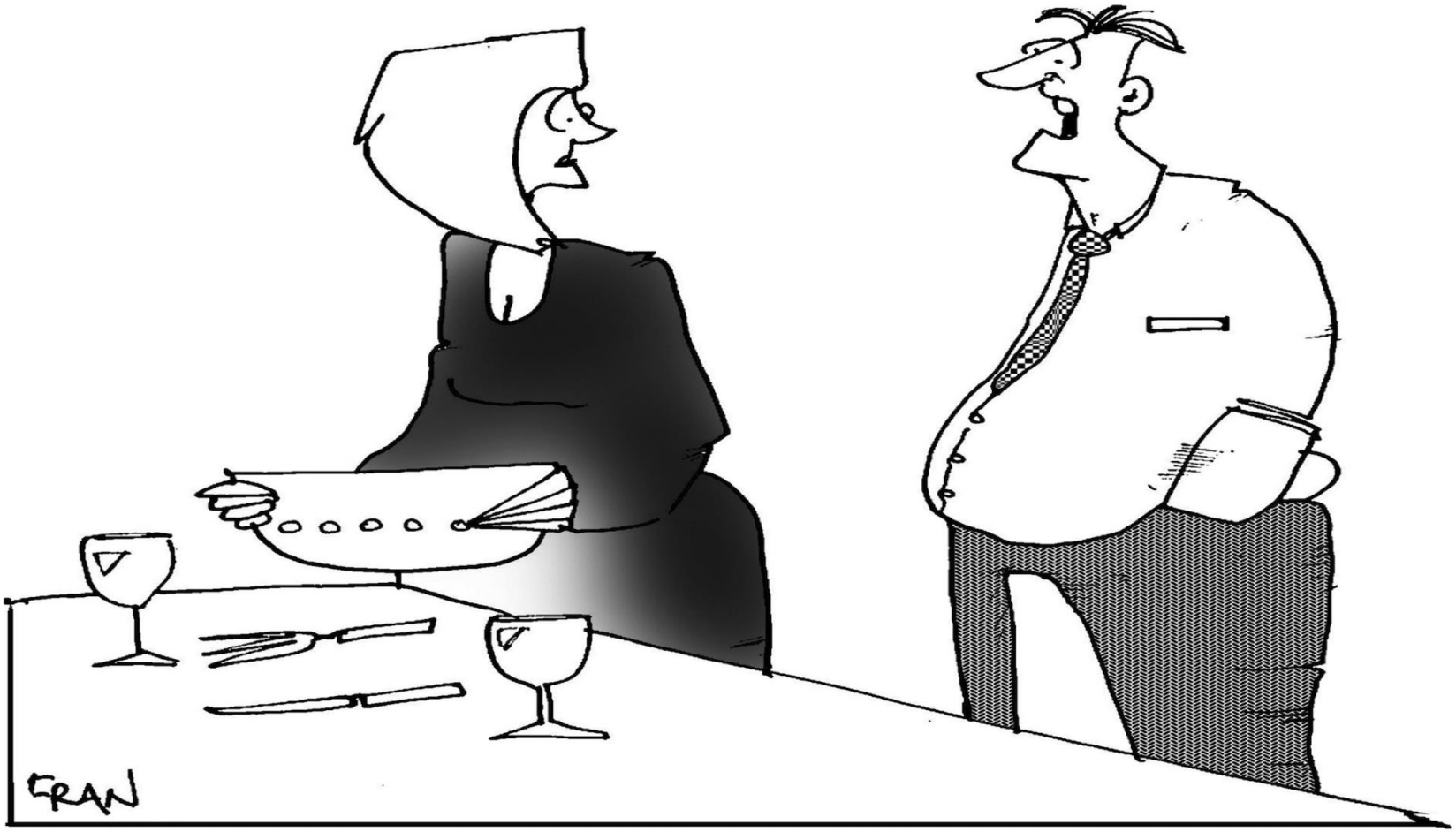
1. Concentration
2. Communication
3. Disintermediation
4. Extensibility
5. Flexibility
6. Complexity



Hardware Insecurities

- Juice Jacking
- Before Stuxnet: Corruption of Frequency Converters Bought by Iran
- Global Supply Chain

Extent of Global Supply



How Many Transistors Are Manufactured WW per Second?

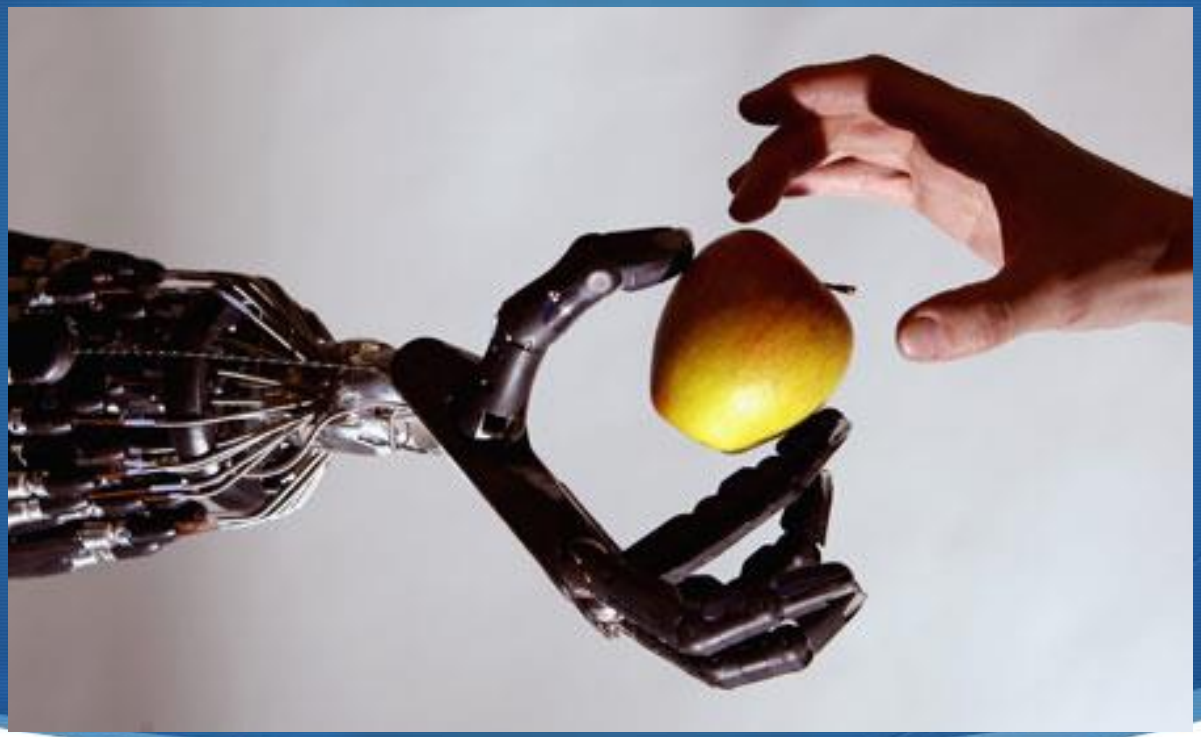
14 Trillion

(1 billion transistors used in a major graphics program)

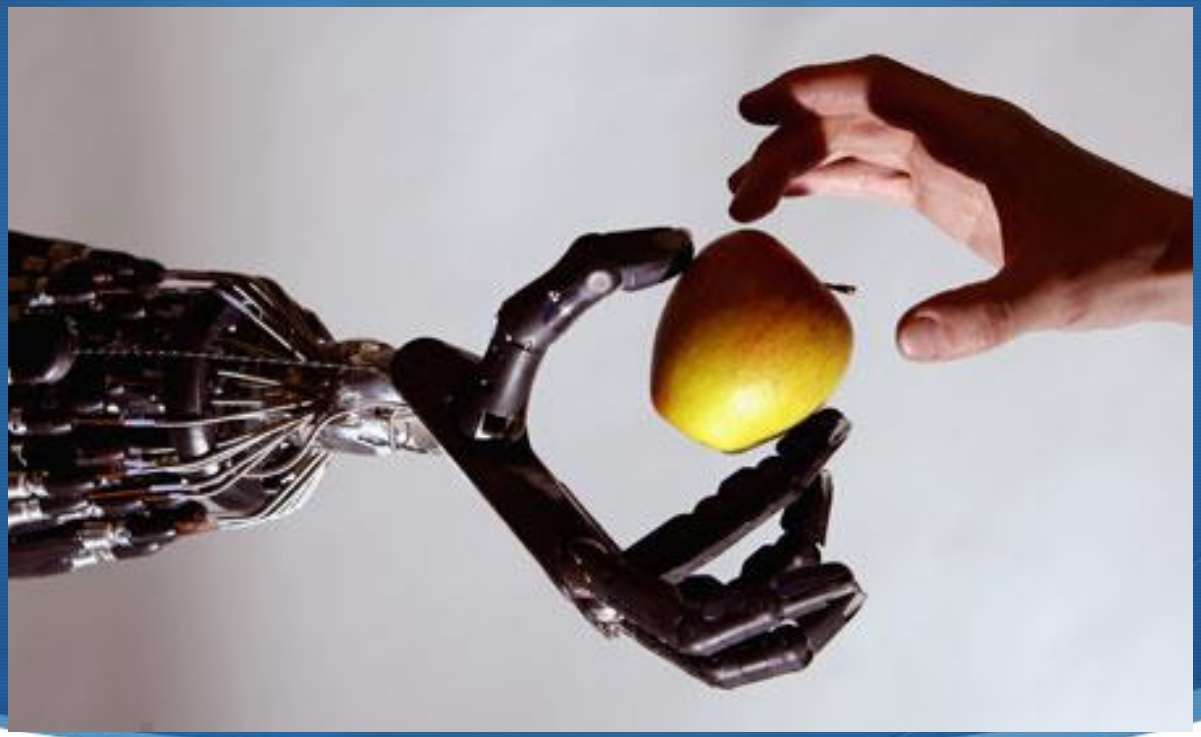
Human Risks

- Insiders
  - Snowden/Manning
  - Contractors; Third Party Counterparts
- Social Engineering
  - Read a Mitnick book!
- Mismanagement (Configuration, Password)
- "Don't Tell Anyone Your Password" – But People Will

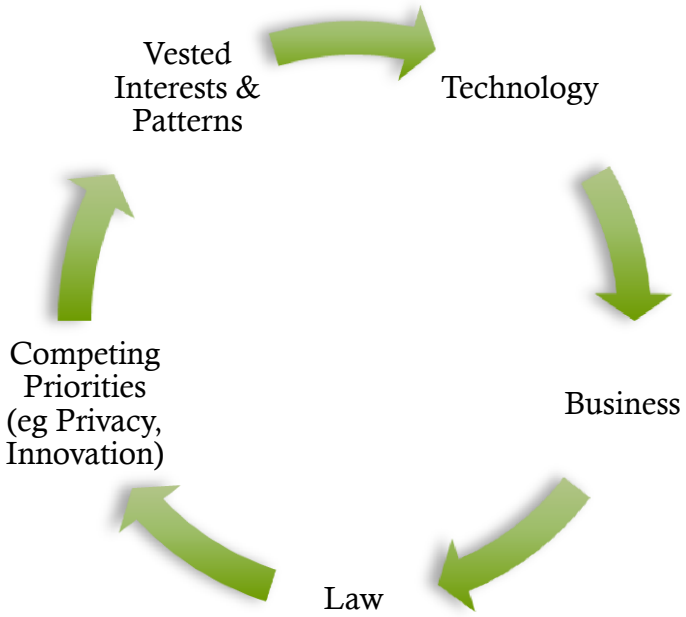
This is Poison Fruit



Improve Digital Technology?



A Wicked Problem



Speed of Change

- Gunpowder 1300-1500
- IT 1990-2015
- IT 2015 FF
- IT empowered Technologies
- Globalization

GAO, "High-Risk Series: An Update" (2/11/15)

The number of information security incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT):

FY 2006: 5,503

FY 2014: 67,168

An increase of 1,121 percent.

The Next Decade?

- Destruction of Societal Processes and Trust
  - Federal System
  - Financial System
  - Power Grid
- Individual Vulnerabilities - Hacking of Things as a Terror Weapon
  - Autos
  - Homes
  - Medical Records

Approaches to Solving our Problems

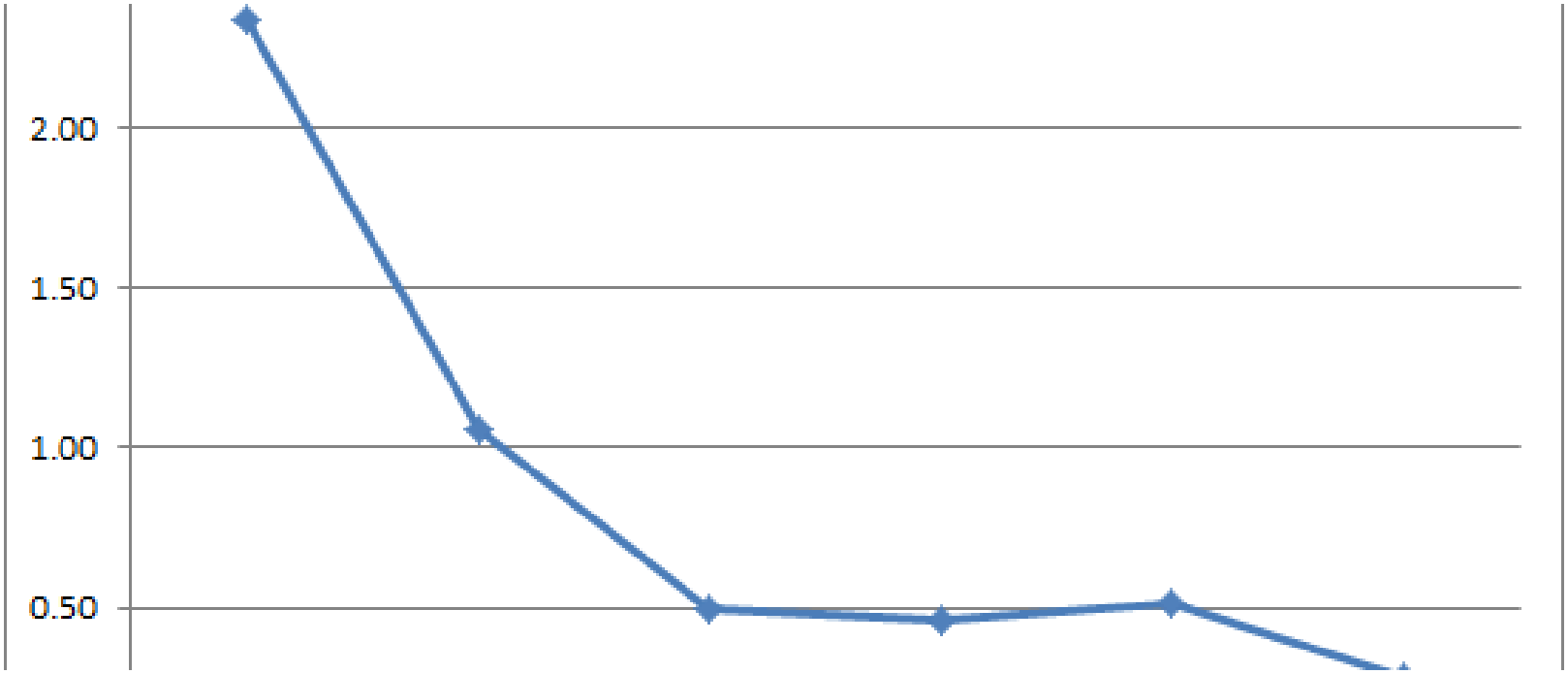
Counter-Measures

- Barriers and Training
- Screening (Anti-virals,etc.)
- Vulnerability Hunting
- Active Defense (Including Situational Awareness)
- Enclaves & Encryption
- Deterrence (Cyber & Non-Cyber Measures)
  - Segue on Attribution

Raise Costs for Attackers

- Also for Defenders!
- By How Much?
- Displacement Effects: Criminal Activity Flows to Places of Least Resistance
- Astute State Actors and Others will Prevail
  - Consider Red Team Success Histories

Vulnerabilities per Investigator 2006-11 (Sample Company)



2012 Prices for Vulnerabilities (Per Forbes Magazine)

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Cert Report 2-21-15

https://www.us-cert.gov/ncas/bulletins/SB15-061

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0313, CVE-2015-0315, CVE-2015-0320, and CVE-2015-0322.	2015-02-21	10.0	CVE-2015-0331 BID
apptha -- wordpress_video_gallery	SQL injection vulnerability in videogallerysrss.php in the Apptha WordPress Video Gallery (contus-video-gallery) plugin before 2.8 for WordPress allows remote attackers to execute arbitrary SQL commands via the vid parameter in a rss action to wp-admin/admin-ajax.php.	2015-02-24	7.5	CVE-2015-2065 CONFIRM OSVDB EXPLOIT-DB MISC
cisco -- carrier_routing_system	Cisco IOS XR 5.0.1 and 5.2.1 on Network Convergence System (NCS) 6000 devices and 5.1.3 and 5.1.4 on Carrier Routing System X (CRS-X) devices allows remote attackers to cause a denial of service (line-card reload) via malformed IPv6 packets with extension headers, aka Bug ID CSCuq95241.	2015-02-21	7.1	CVE-2015-0618 SECTRACK BID
cisco -- ips_sensor_software	Race condition in the SSL implementation on Cisco Intrusion Prevention System (IPS) devices allows remote attackers to cause a denial of service by making many management-interface HTTPS connections during the key-regeneration phase of an upgrade, aka Bug ID CSCui25688.	2015-02-21	7.1	CVE-2015-0631 BID

PC World on 2015 HP Sponsored "Pwn2Own" Contest

- "South Korean … hacker JungHoon Lee … single-handedly popped Internet Explorer 11 and Google Chrome on Microsoft Windows, as well as Apple Safari on Mac OS X….
- Lee's attack against Google Chrome earned him …$75,000 for the Chrome bug … $25,000 for a privilege escalation to SYSTEM and another $10,000 for also hitting the browser's beta version—for a total of $110,000…. The IE11 exploit earned him an additional $65,000 and the Safari hack $50,000.
- Lee's accomplishment is … impressive because he competed alone…"

Summary: 2015 Pwn2Own

- "The final count for vulnerabilities exploited this year …: five flaws in the Windows OS, four in Internet Explorer 11, three each in Mozilla Firefox, Adobe Reader, and Flash Player, two in Apple Safari and one in Google Chrome."
- "Most of the attacks demonstrated at Pwn2Own this year required chaining of several vulnerabilities together in order to bypass all defense mechanisms put in place in operating systems and browsers to prevent remote code execution."

Improving our Situation

Six Recommendations

Recommendation 1: Presume Cyber Vulnerability of Critical Systems

- Presume that all digital systems are "Contested Territory"
- Seek Lean Systems
- Use Out of Band Subsystems (Use Analog & Humans)

Challenge: Build Secure Systems from Insecure Parts

- Goal is not IT Security but Mission Achievement
- Goal: System Resilience in the Face of Component Failure
- Separate Systems, Redundant Systems
  - Avoidance of Monoculture
  - Check for Parallel Outcomes
  - Snyder & Kendrick: "Cyber Separability" for the Air Force

Recommendation 2: Recognize Private Sector "Too Important to Fail"

- Banking: Too Big To Fail
- We Regulate Airlines
- Section 9 Report
- But IT Speed of Change; Risk of Regulatory Stultification
  - Incentives
  - Collaboration
  - Focus on Ends not Means

Recommendation 3: Disaggregate the Problem

- Do Not Over-Regulate or Focus Too Broadly
- Focus on Core of Consequence to Our National Well-being
- Differentiate Industries
- Contrast, e.g., between Finance and Power
- Work Through Diverse Cabinet Departments and Regulatory Commissions

Recommendation 4: Invest in Long-Term R&D for More Robust Design

- Fund Private Sector R&D for Robustness
  - Comprehensive National Cybersecurity Initiative (CNCI)
- Map (but do not Centralize) Present Federal R&D
- Invest in One or Two Substantial Federal Projects
  - Navy Ship with Diminished Vulnerabilities
  - Power Generation/Transmission System
- Use the Model Systems to Develop Broadly Applicable Principles

Recommendation 5: Invest in Behavioral Studies

- Cyber Behavior Shaped by Economics & Norms
- Studies by Sociologists/Anthropologists/Economists
  - Our industry behaviors in business contexts
  - Attacker business models
    - Hacker
    - Criminal
    - State Sponsored

Recommendation 6: Public Private Pooling of Attack & Defense Information

- Numerous "Partnerships" Exist
- Industry Specific are Useful
- But Overview Required, without Too Much Government Control/Regulatory Risk
- Near-Miss Aviation Model (MITRE)