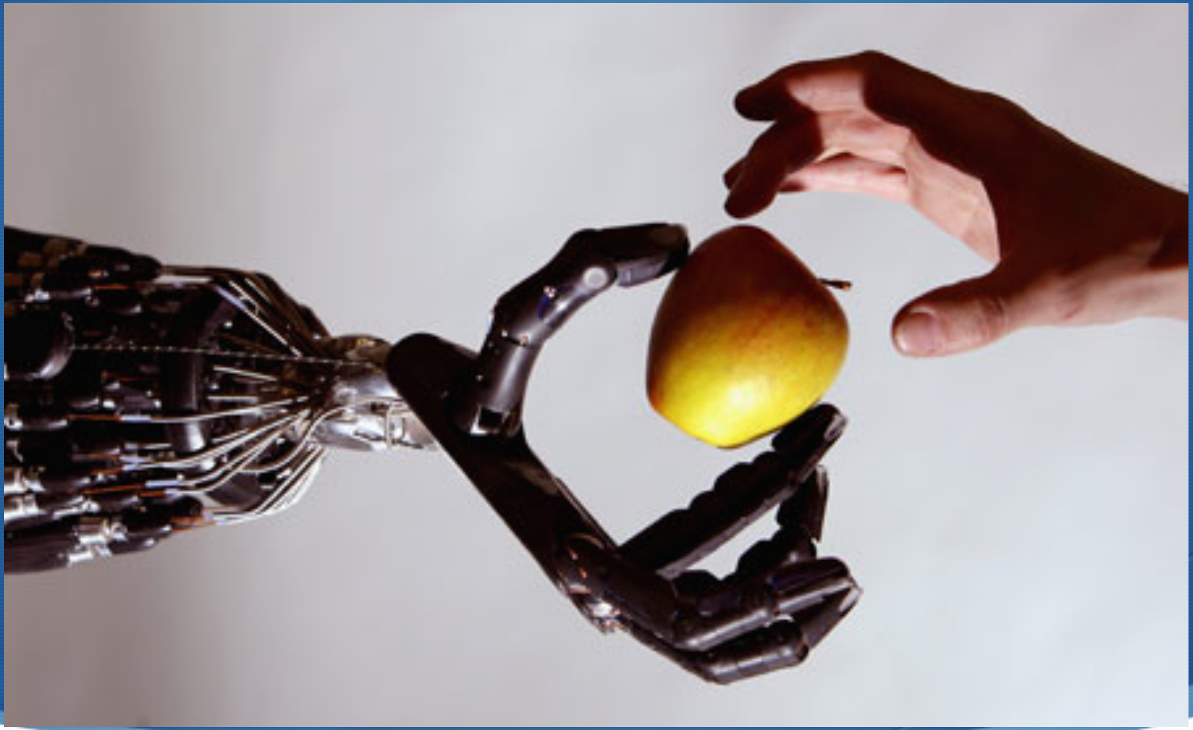
Surviving on a Diet of Poisoned Fruit

Richard Danzig

USENIX

August 2015

www.cnas.org



Overview of This Briefing

I. Admiring the Problem

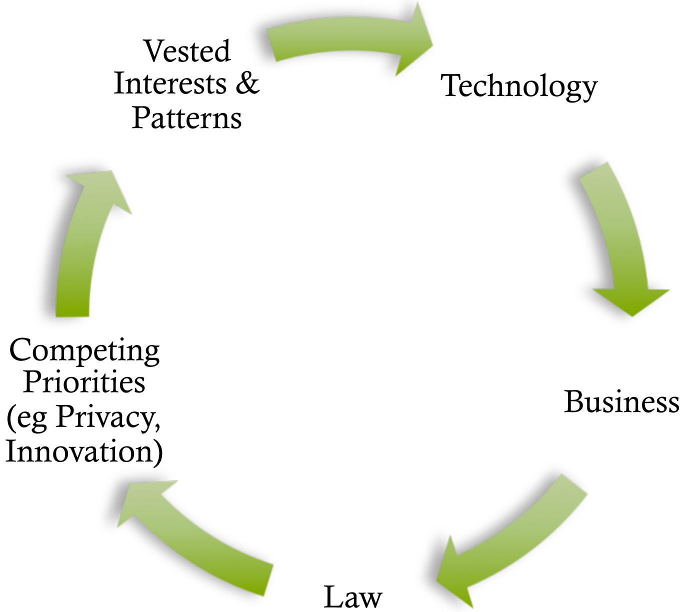
II. Analyzing and Explaining the Problem

III. Recent Approaches to Solving the Problems

IV. Improving our Situation

Admiring the Problem

A Wicked Problem



Vested Interests & Patterns

Technology

Business

Law

Competing Priorities (eg Privacy, Innovation)

Speed of Change

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

“The Past is Not Dead. It is Not Even Past”

- Espionage from the Cold War to Present
  - Less Restrained than Kinetic
  - Few Red Lines
  - Heavy Investment in US Offense/Secrecy of Exploits
  - No Equivalent to Legal Review of Title 10 Weapons
- US: Government-Private Sector US Distinction
- USG: Un-clarity about Relations to Its Own Private Sector

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."

Old & New Concept Weapons

- Old: “Weapons whose immediate goal is to kill and destroy, and which are still related to military affairs, soldiers, and munitions.”

- New: “Everything that can benefit mankind can also harm him. This is to say that there is nothing in the world today that cannot become a weapon, and this requires that our understanding of weapons must have an awareness that breaks through all boundaries….”

New Concept Weapons

- “As we see it, a single man-made stock-market crash, a single computer virus invasion, or a single rumor or scandal that results in a fluctuation in the enemy country's exchange rates or exposes the leaders of an enemy country on the Internet, all can be included in the ranks of new-concept weapons.”
- “[T]he best way to achieve victory is to control, not to kill.”

“Political, Economic, and Technological violence.”

- “The new concept of weapons will cause ordinary people and military men alike to be greatly astonished … commonplace things that are close to them can also become weapons with which to engage in war…. [S]ome morning people will awake to discover with surprise that quite a few gentle and kind things have begun to have offensive and lethal characteristics.”

Experience:
The Last Decade

- Business Transparency
  - IP Theft
  - Revelation of Processes, Products, Personnel
  - Economic Espionage (Bids, Pricing, Suppliers)

- Individual Visibility
  - All Records: Medical, Financial
  - Relationships

- “NEW Warfare” (Danzig: 1998)
  - Stuxnet
  - Sony Hack

Experience to Come?
We are Driving in the Dark

- Blinkered Prediction
- Pace of Technological Innovation
- Variety of Actors (E.g. Eco-terrorists)
- Interaction with Societal Evolution
- But …

The Next Decade?

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

Analyzing The Problem

Root Causes of Digital Insecurity

- Complexity
  - Microsoft Operating System – 50 Million Lines of Code
  - A Major Investment House – 1 Trillion Lines of Code
- Complexity 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

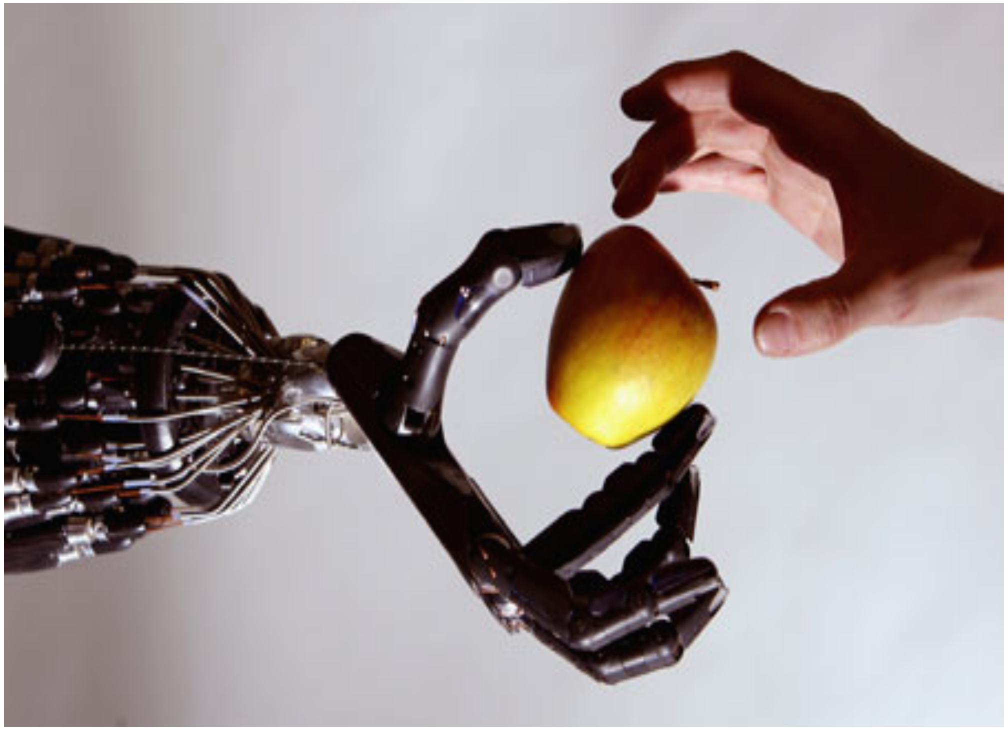
② Communication

③ Disintermediation

④ Extensibility

⑤ Flexibility

⑥ Complexity



Hardware Insecurities

- Juice Jacking
- Before Stuxnet: Corruption of Frequency Converters Bought by Iran
- Global Supply Chain
- Test Your Grasp of the Magnitude & Complexity of the Supply Chain with the Following Question (“How Many Children Have we Got?”)

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

Approaches to Solving our Problems

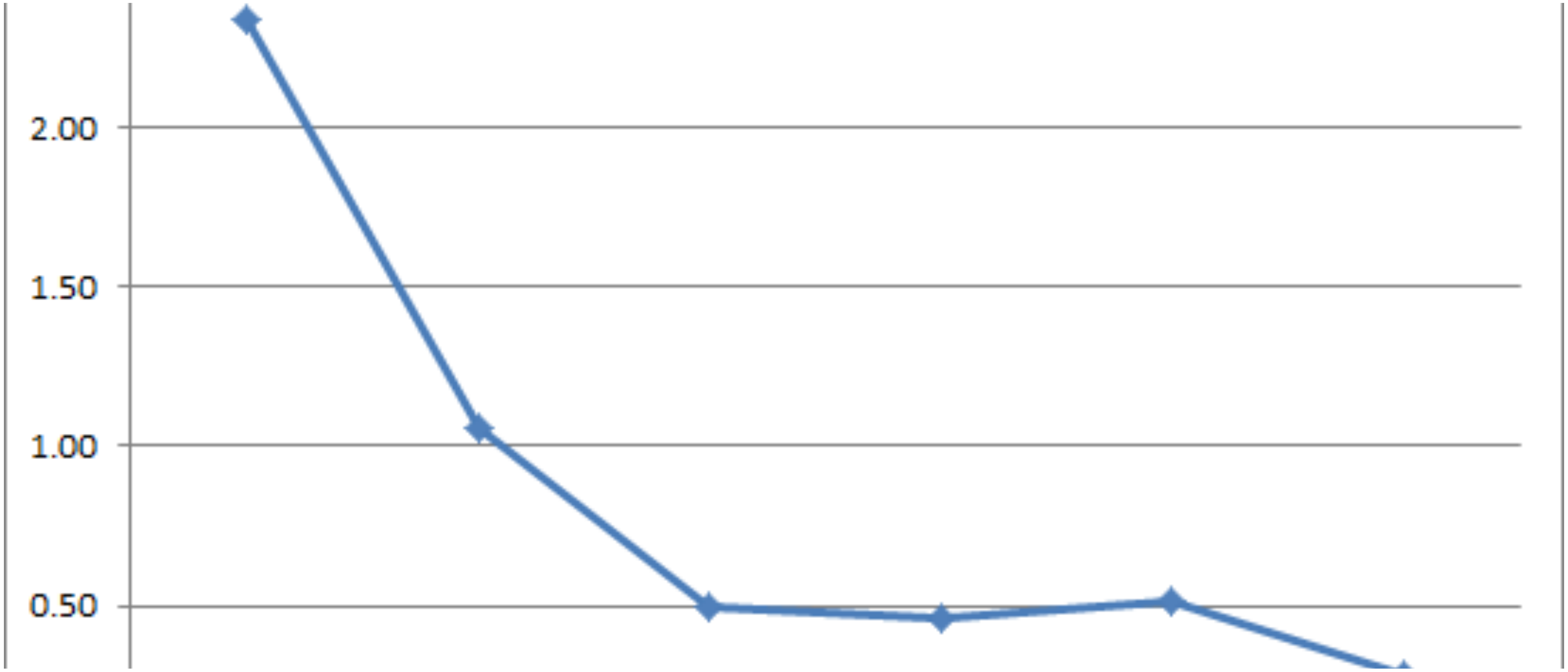
Counter-Measures

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

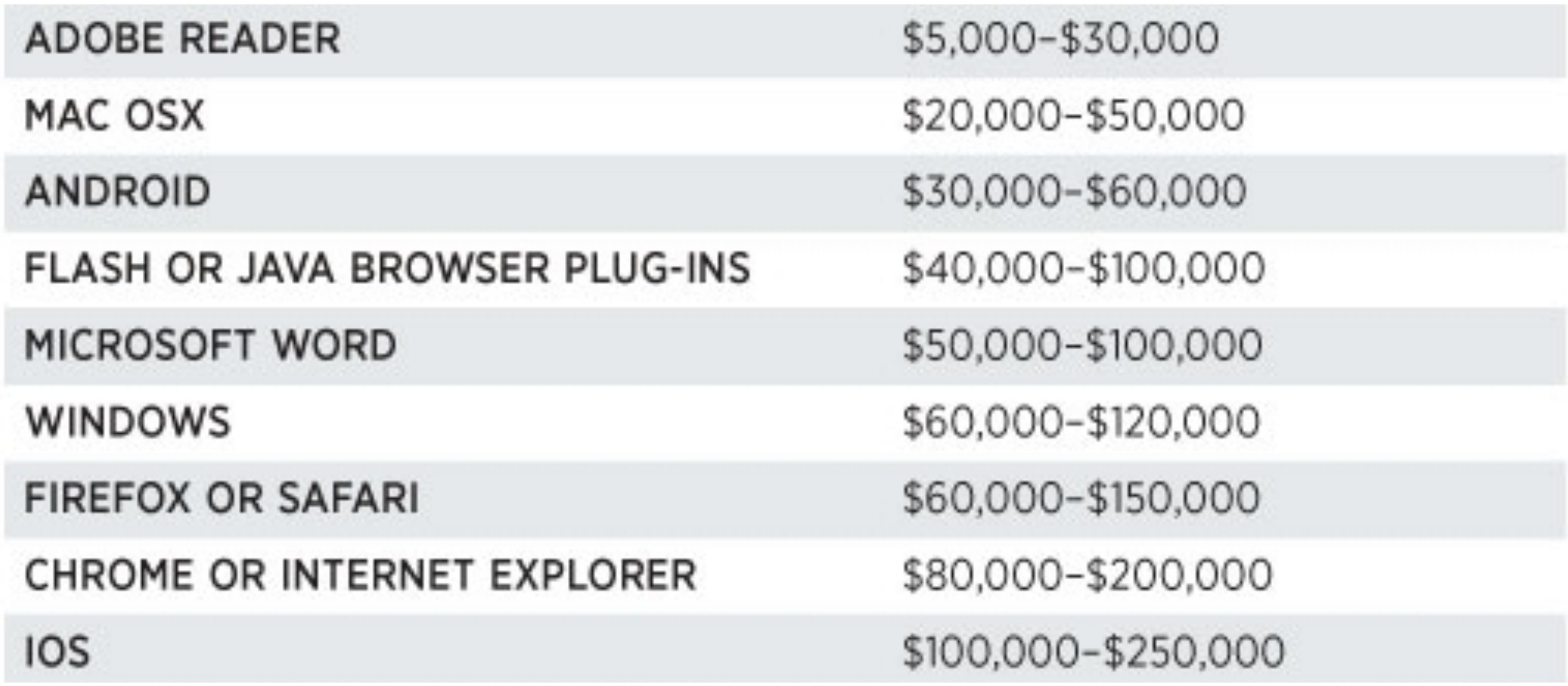
Raise Costs for Attackers

- 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)

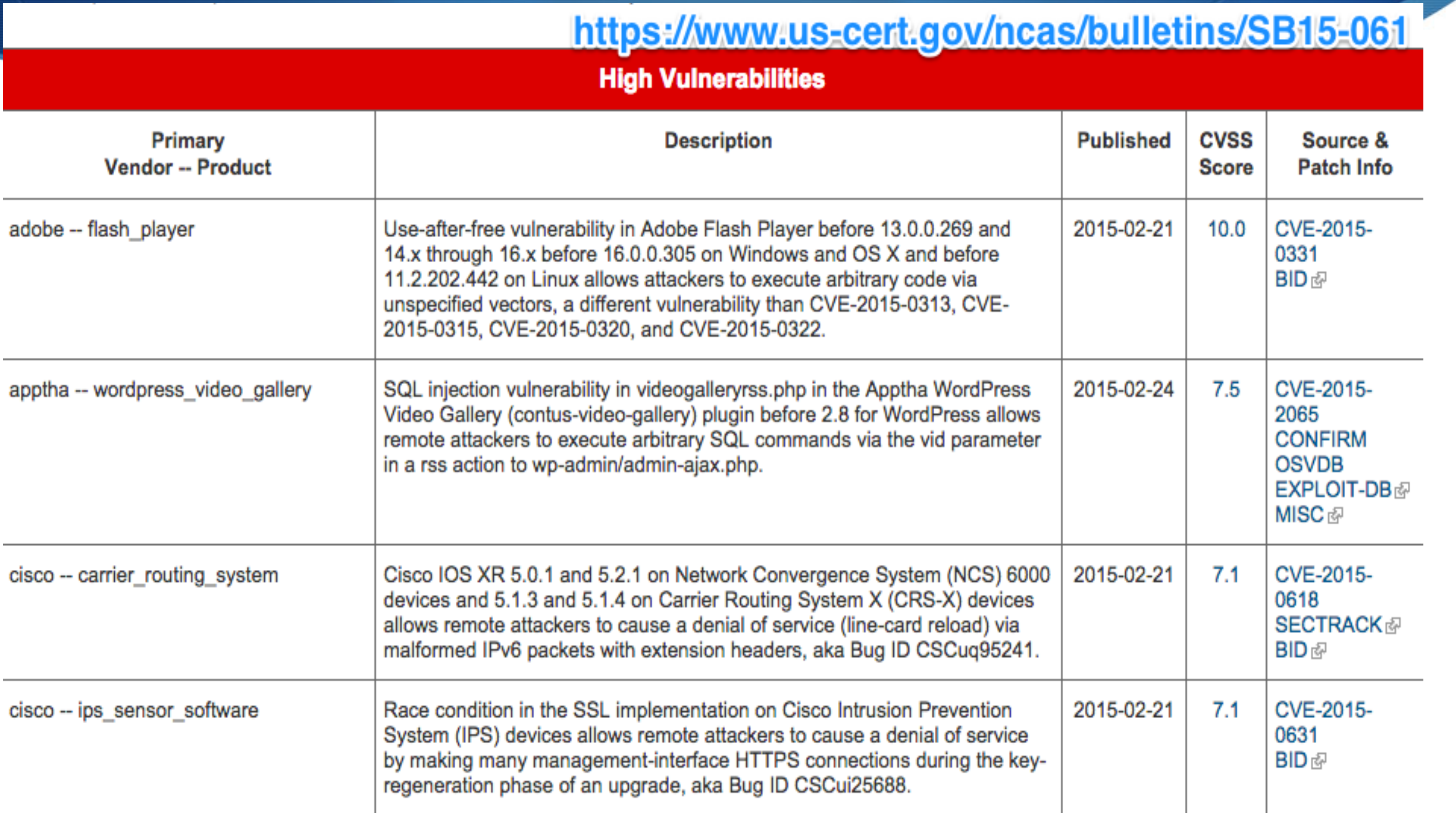


2012 Prices for Vulnerabilities (Per Forbes Magazine)



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 videogalleryrss.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

Eight Recommendations

Recommendation 1: Presume Cyber Vulnerability of Critical Systems

- "Contested Territory"
- Lean Systems
- Out of Band Subsystems (Use Analog & Humans)
- Separate & Uncouple
- Resilience

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/Focus Too Broadly
- Focus on Core of Consequence to Our National Security
- Differentiate Industries
- Contrast, eg, between Finance and Power
- Work Through Diverse Cabinet Departments and 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: Sponsor 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)

Recommendation 7: Create a Federal FFRDC

- Create a Pool of Skilled Cyber Workers
- Innovate in Hiring
  - Avoid Traditional Credentialing
  - Hiring by Competition
  - Silicon Valley Location
- Create Better Training (OJT/Peers)

Recommendation 8: Norms & Deterrence

- Some Strategic Stability Now Exists
- Emergent/Not Articulated
- But Fragile
  - US←→Iran per newspaper reports
  - Less Control Over Weapons
  - Blurring of Weapons' Purposes
  - Anonymity/Spoofing

Foundation of Mutually Assured Deterrence

- Want to allow others (eg China) to have an assured 2nd strike ability
  - Otherwise they will can panic to 1st strike
- They want us to have an assured 2nd strike capability
- Don't we both then have an interest in staying out of the cyber underpinnings of each others' nuclear arsenals?
- Otherwise we move from MAD to MUD