



Calhoun: The NPS Institutional Archive
DSpace Repository

Faculty and Researchers

Faculty and Researchers' Publications

2013-05-16

The Cyber Security Mess

Garfinkel, Simson L.

Monterey, California. Naval Postgraduate School

<https://hdl.handle.net/10945/44315>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



The Cyber Security Mess

Simson L. Garfinkel
Associate Professor, Naval Postgraduate School

May 16, 2013

DISCLAIMER:

“The views expressed in this document are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.”

NPS is the Navy's Research University.

Monterey, CA — 1500 students

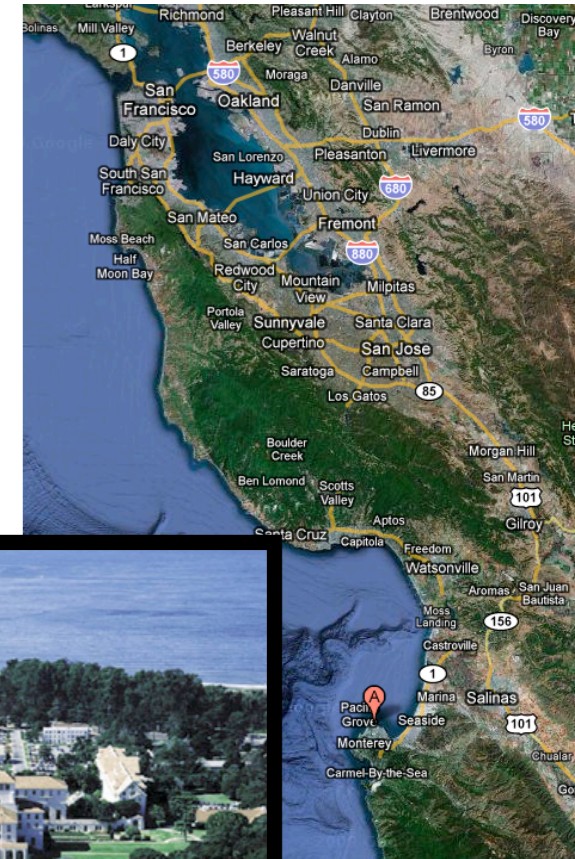
- US Military & Civilian (Scholarship for Service & SMART)
- Foreign Military (30 countries)

Graduate Schools of Operational & Information Sciences (GSOIS)

- Computer Science
- Defense Analysis
- Information Sciences
- Operations Research
- Cyber Academic Group

National Capital Region (NCR) Office

- 900 N Glebe (Ballston)/Virginia Tech building



“The Cyber Security Risk”, *Communications of the ACM*, June 2012, 55(6)

V viewpoints

00132.1145/1184328.1284330 Simon L. Garfinkel

Inside Risks The Cybersecurity Risk

Increased attention to cybersecurity has not resulted in improved cybersecurity.

The risk of being “hacked”—whatever that expression actually means—is at the heart of our civilization’s chronic cybersecurity problem. Despite decades of computer security research, billions spent on security operations, and growing training requirements, we seem incapable of operating computers securely.

There are weekly reports of penetrations and data thefts at some of the world’s most sensitive, important, and heavily guarded computer systems. There is good evidence that global interconnectedness combined with the proliferation of hacker tools means that today’s computer systems are actually less secure than equivalent systems a decade ago. Numerous breakthroughs in cryptography, secure coding, and formal methods notwithstanding, cybersecurity is getting worse as we watch.

So why the downward spiral? One reason is that cybersecurity’s goal of reducing successful hacks creates a large target to defend. Attackers have the luxury of choice. They can focus their efforts on the way our computers represent data, the applications that process the data, the operating systems on which those applications run, the networks by which those applications communicate, or any other area that is possibly subverted. And faced with a system that is beyond one’s technical hacking skills, an attacker can go around the security perimeter and use a range of other techniques, including social engineering, supply-chain insertion, or even kidnapping and extortion.

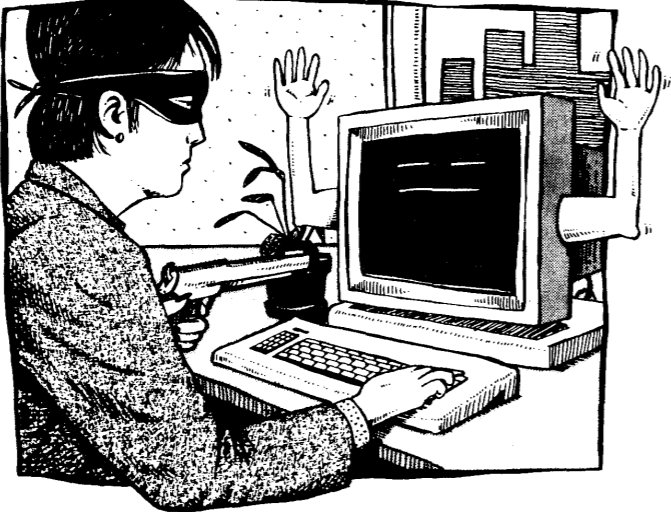
It may be that cybersecurity appears to be getting worse simply because society as a whole is becoming much more dependent upon computers. Even if the vulnerability were not increasing, the successful hacks can have significantly more reach today than a decade ago.

Views of Cybersecurity

The breadth of the domain means many different approaches are being proposed for solving the cybersecurity problem:

- Cybersecurity can be viewed solely as an insider problem. What is needed, say advocates, are systems that prevent

I have spent 25 years trying to secure computers...



An Introduction to Computer Security
[Part 1]

Simson L. Garfinkel

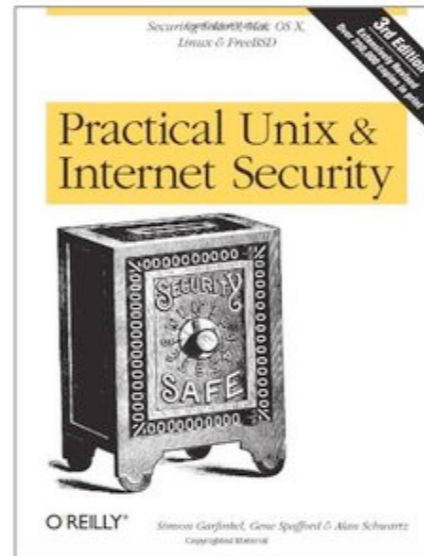
"Spies," "vandals," and "crackers" are out there, waiting to get into—or destroy—your databases.

LAWYERS MUST UNDERSTAND issues of computer security, both for the protection of their own interests and the interests of their clients.

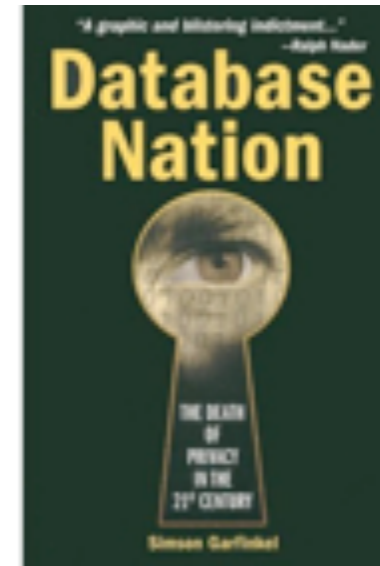
Lawyers today must automatically recognize insecure computer systems and lax operating procedures in the same way as lawyers now recognize

39

Sept. 1987



1991



2000



2006

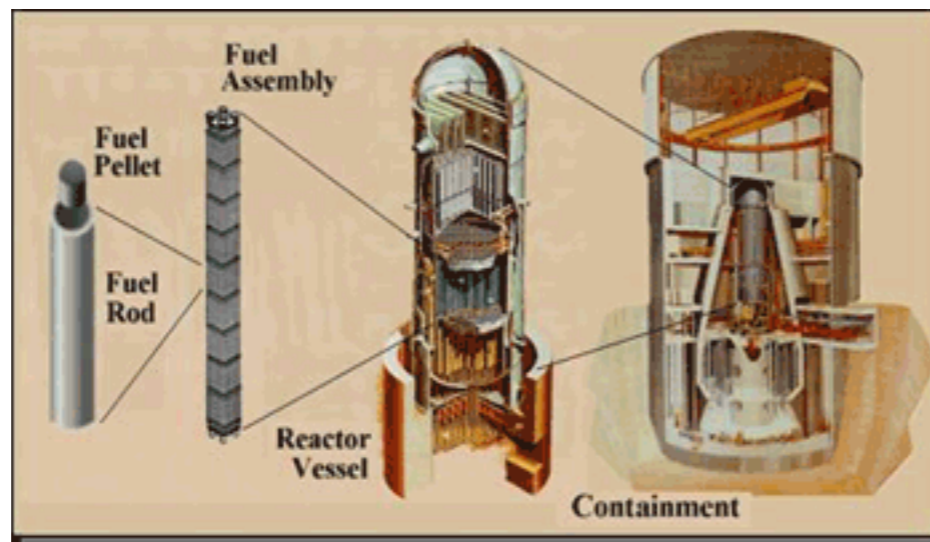


2006

Today's systems are less secure than those of the 1970s.

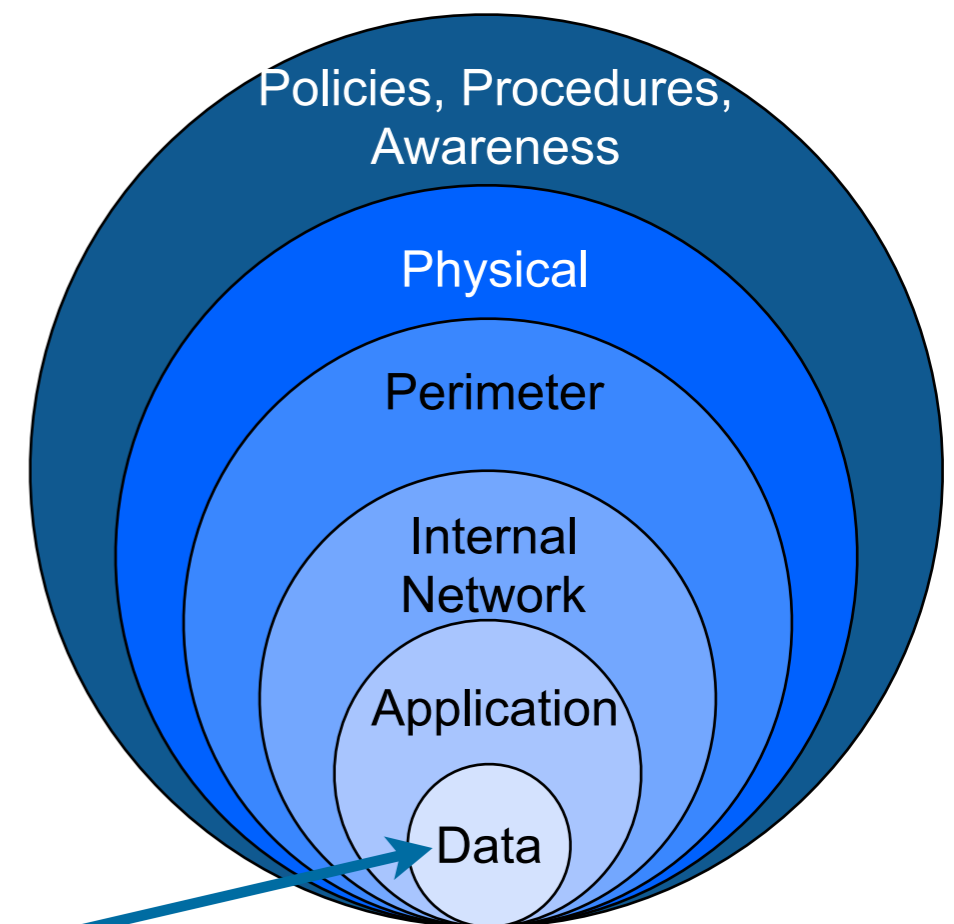
The lack of security is **inherent** in modern information systems.

- Attack is **easier and cheaper** than defense.
- Cyber “Defense in depth” does not work
— *a single vulnerability compromises.*



Defense in depth of nuclear reactors

<http://www.nrc.gov/about-nrc/regulatory/research/soar/soarca-accident-progression.html>



**Cyber can directly target
inner defenses**

It's easier to break things than to fix them.

Windows

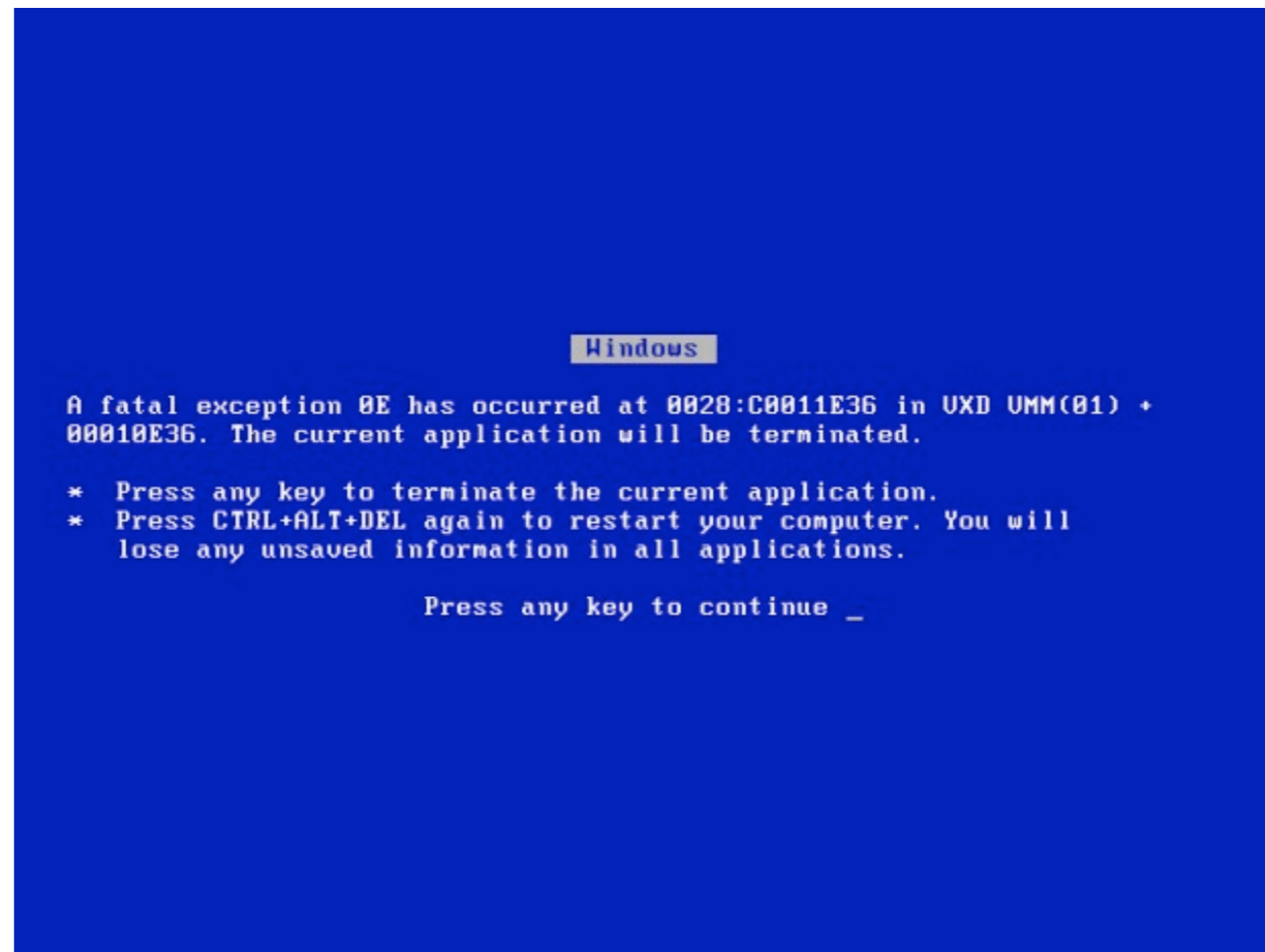
A fatal exception 0E has occurred at 0028:C0011E36 in UXD UMM(01) + 00010E36. The current application will be terminated.

- * Press any key to terminate the current application.
- * Press CTRL+ALT+DEL again to restart your computer. You will lose any unsaved information in all applications.

Press any key to continue _

Today we expect computers to crash

We should also expect them to be hacked.



The solution is not better security



I start every day with...

[ISN]
Internet Security
News



[ISN] — infosecnews.org

The screenshot shows a Gmail search results page for the query 'from:infosec news'. The browser address bar shows the URL 'https://mail.google.com/mail/ca/u/0/#search/from%3Ainfosec+news'. The search results are displayed in a list format, with each entry including a checkbox, a star icon, a folder icon, the sender 'InfoSec News', the subject line, and the time received. The list includes various news items such as 'Amy's Baking Company Says 'We Were Hacked!'' and 'U.S. Cyber Command Head General Alexander To Keynote Black Hat USA 2013'. The left sidebar shows the 'COMPOSE' button and navigation links for 'Inbox (2)', 'Sent Mail', 'All Mail', 'Spam (2,131)', and 'Trash'. The bottom of the page shows storage usage ('43% full Using 4.4 GB of your 10.1 GB'), copyright information ('©2013 Google - Terms & Privacy'), and account activity ('Last account activity: 0 minutes ago').

Sender	Subject	Time
InfoSec News	[ISN] Amy's Baking Company Says 'We Were Hacked!' Following Yesterday's Scorched Earth ... - Visit the InfoSec New	2:23 am
InfoSec News	[ISN] U.S. Cyber Command Head General Alexander To Keynote Black Hat USA 2013 - Visit the InfoSec News Security	2:21 am
InfoSec News	[ISN] Saudi Telecom Sought U.S. Researcher's Help in Spying on Mobile Users - Visit the InfoSec News Security Book:	2:19 am
InfoSec News	[ISN] Stolen laptop could contain important patient information - dpp/news/local/stolen-laptop-could-contain-important-pat	2:17 am
InfoSec News	[ISN] Too much infosec regulation undermines security, warns NAB - Visit the InfoSec News Security Bookstore Best S	2:15 am
InfoSec News	[ISN] Legal Showdown on Cybersecurity - Visit the InfoSec News Security Bookstore Best Selling Security Books and M	May 13
InfoSec News	[ISN] Bank Muscat mulls options to recover card fraud money - com/News/Article-15279.aspx By AE James Times of C	May 13
InfoSec, Simson (2)	[ISN] Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment... - 2 When news of Stuxne	May 13
InfoSec News	[ISN] SC hacking solution could cost \$15 million next year - Visit the InfoSec News Security Bookstore Best Selling Sec	May 13
InfoSec News	[ISN] Privacy Breach on Bloomberg's Data Terminals - that Bloomberg News reporters had extracted subscribers' privat	May 13
InfoSec News	[ISN] Is 'fear the auditor' holding back real IT security? - Visit the InfoSec News Security Bookstore Best Selling Securit	May 10
InfoSec News	[ISN] The Onion explains how its Twitter account was hacked - com/news/2013/051013-the-onion-explains-how-its-2696'	May 10
InfoSec News	[ISN] 'Deleted' Snapchat photos saved in phone data, can be examined as evidence - Visit the InfoSec News Security B	May 10
InfoSec News	[ISN] How hackers allegedly stole "unlimited" amounts of cash from banks in just hours - Visit the InfoSec News Securit	May 10
InfoSec News	[ISN] 100 of UK's richest people concealing billions in offshore tax havens - Visit the InfoSec News Security Bookstore l	May 10
InfoSec News	[ISN] MAPCO warns of payment card security breach - Visit the InfoSec News Security Bookstore Best Selling Security	May 9
InfoSec News	[ISN] A National Security Imperative: Protecting Singapore Businesses From Cyber-Espionage - Visit the InfoSec News	May 9
InfoSec News	[ISN] Bush, Powell hacker hits 'Sex and the City' author - com/news/2013/may/8/bush-powell-hacker-hits-sex-and-city-at	May 9
InfoSec News	[ISN] Theft at DFSS in Chicago could lead to health data breach - While Chicago News Affairs Office Joshua Purkiss dir	May 9
InfoSec News	[ISN] Feds Drop Hacking Charges in Video-Poker Glitching Case - Visit the InfoSec News Security Bookstore Best Selli	May 9



May 2013 — \$45 million stolen from US banks with phony ATM cards

RISK ASSESSMENT / SECURITY & HACKTIVISM

How hackers allegedly stole “unlimited” amounts of cash from banks in just hours

Feds accuse eight men of participating in heists that netted \$45 million.

by Dan Goodin - May 9 2013, 3:45pm EDT

BLACK HAT HACKING 55



Wikipedia

Federal authorities have accused eight men of participating in 21st-Century Bank heists that netted a whopping \$45 million by hacking into payment systems and eliminating withdrawal limits placed on prepaid debit cards.

The eight men formed the New York-based cell of an international crime ring that organized and executed the hacks and then used fraudulent payment cards in dozens of countries to withdraw the loot from automated teller machines, federal prosecutors alleged in court papers unsealed Thursday. In a matter of hours on two separate occasions, the eight defendants and their confederates withdrew about \$2.8 million from New York City ATMs alone. At the same times, "cashing crews" in cities in at least 26 countries withdrew more than \$40 million in a similar fashion.



April 2013 — AP Twitter feed reports White House bombing

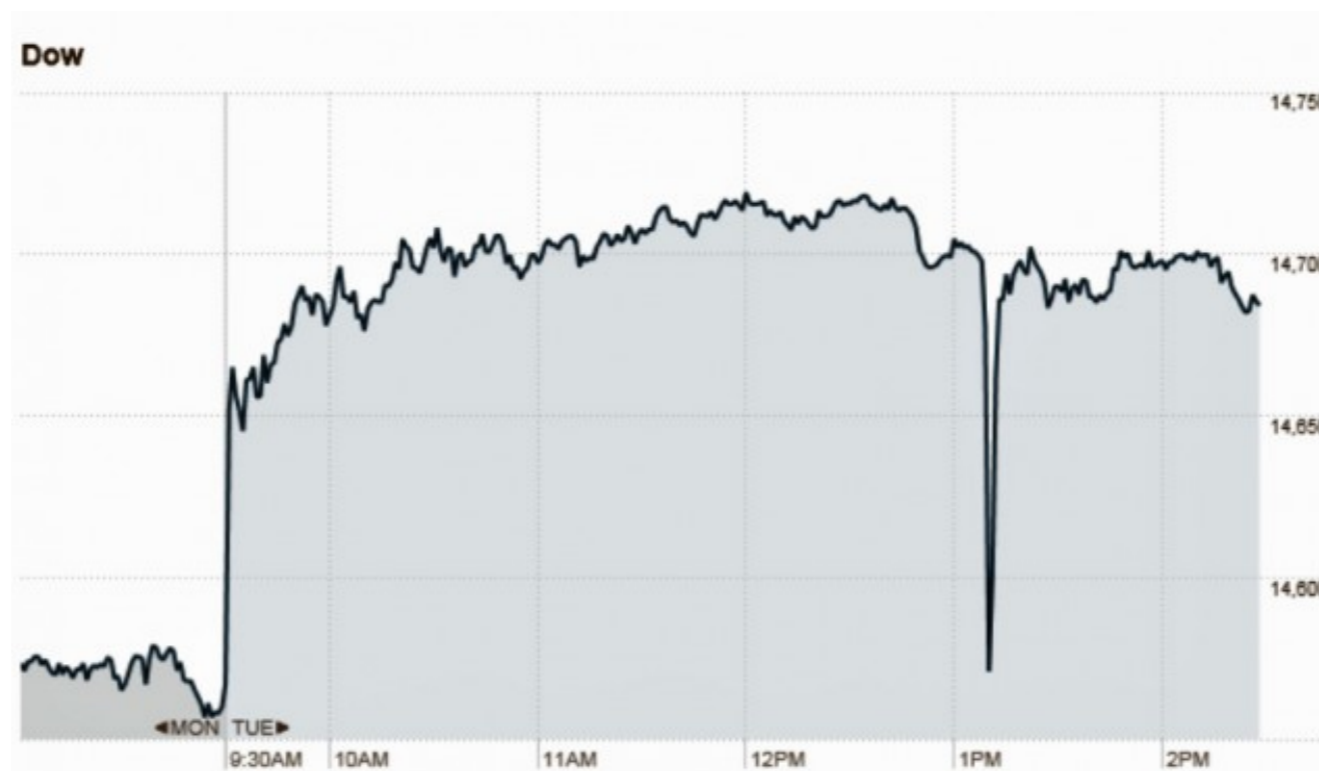
RISK ASSESSMENT / SECURITY & HACKTIVISM

Hacked AP Twitter feed reporting fake White House attack rocks markets

Account compromise comes after AP targeted by malware and phishing e-mails.

by Dan Goodin - Apr 23 2013, 3:44pm EDT

HACKING INTERNET CRIME 74



The seven-minute drop in the Dow Jones Industrial Average touched off by a single tweet falsely claiming the White House had been bombed. It temporarily wiped out about 1 percent of the average, which can translate into millions or billions of dollars in market capitalization.

Stock prices plunged and then quickly recovered after a Twitter account belonging to the Associated Press was hacked and used to send a bogus report falsely claiming that the White House had been bombed and President Obama was injured.



“Stolen laptop could contain important patient information” 14 May 2013

The screenshot shows a news article on the WFLI.com website. The article is titled "Stolen laptop could contain important patient information" and is dated Tuesday, May 14, 2013. The author is Kelly Roberts. The article reports that an employee's laptop computer was stolen from their car at IU Health Arnett in Lafayette, Indiana, on April 9. The laptop was password-protected but not encrypted. Hospital officials said the laptop contained patient information, including names, dates of birth, physicians' names, medical record numbers, diagnoses, and dates of service. The White County Sheriff's Office was immediately contacted, and IU Health Arnett began an internal investigation. The news made one patient, who wishes to remain anonymous, nervous.

The article includes a photo of IU Health Arnett and a "Larger Photo" button. There are also social media sharing options (Like, Tweet, Share, Email, Print) and a "Recommended Stories" section with links to other local news items.

How many “stolen laptop” cases have there been?

Possibly the only good news:
cyber-weapons may not be terribly effective, either.

The screenshot shows a web browser displaying the RUSI website. The URL is www.rusi.org/publications/journal/ref:A517E5BC42E13D/#.UZ0oqywwE9z. The page features a navigation menu with links for Home, Research, Analysis, Events, Publications, Membership, About us, Contact us, and Media. The main content area displays the article "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme" by Ivanka Barzashka, published in the RUSI Journal, April 2013, Vol. 158, No. 2. The article text states: "When news of Stuxnet first emerged, many thought that it had caused a major setback to Iran's uranium-enrichment programme. Ivanka Barzashka argues instead that while Stuxnet may have had the potential to seriously damage Iranian centrifuges, evidence of the worm's impact is circumstantial and inconclusive. Her analysis of the related data shows that the 2009 version of Stuxnet was neither very effective nor well-timed and, in hindsight, may have been of net benefit to Tehran." Below the text is a photograph of a person in a white lab coat and yellow hard hat standing in a large industrial facility, likely a centrifuge plant. The page also includes a sidebar with "Publications" and "Guidelines for Contributors" sections, and a right-hand column with "Related RUSI articles", "Events", and "Contacts" sections.

“The 2009 version of Stuxnet was neither very effective nor well-timed and, in hindsight, may have been of net benefit to Tehran.”



The cyber security mess: technical *and* social.

Most attention is focused on technical issues:

- Malware and anti-viruses
 - Default allow vs. default deny*
- Access Controls, Authentication, Encryption & Quantum Computing
- Supply chain issues
- Cyberspace as a globally connected “domain”

Non-technical issues are at the heart of the cyber security mess.

- Education & career paths
- Immigration
- Manufacturing policy

We will do better when we *want* to do better.



What do we ~~know~~
think about cyber
security today?



Cyber Security is expensive.

Global cyber security spending: \$60 billion in 2011

- *Cyber Security M&A*, pwc, 2011

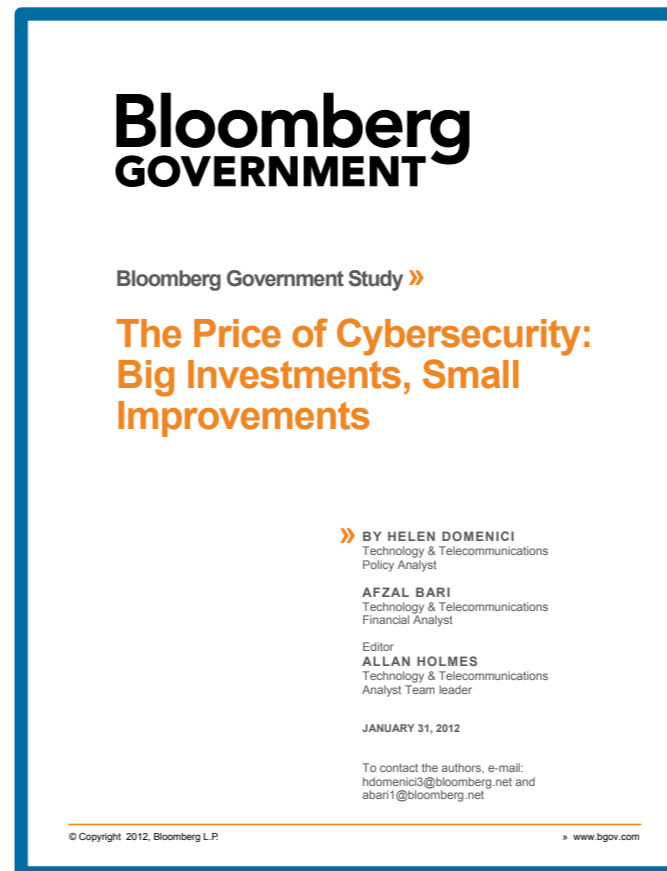
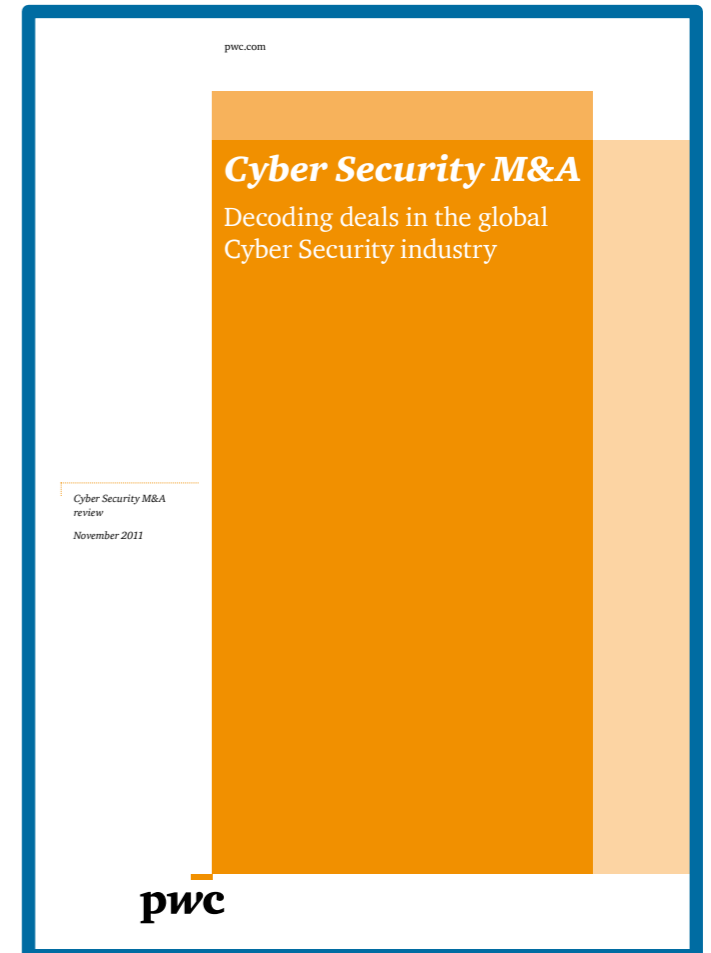
172 Fortune 500 companies surveyed:

- Spending \$5.3 billion per year on cyber security.
- Stopping 69% of attacks.

If they raise spending...

- \$10.2 billion stops 84%
- \$46.67 billion stops 95%
- “highest attainable level”

95% is not good enough.



Cyber Security... is undefined.

There is no good definition for “cyber”

- Computers?
- Computer networks?
- Hacking?
- Using “network security” to secure desktops & servers?
- ~~Something having to do with cybernetics~~



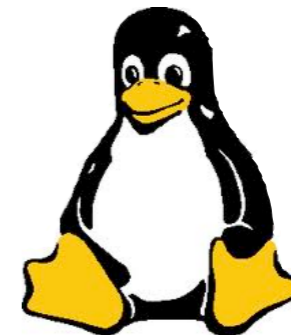
**Norbert
Weiner**



**William
Gibson**

There is no way to *measure* cyber security

- Which OS is more secure?
- Which computer is more secure?
- Is “open source” more secure?



—A system that seems “more secure” can suffer a total compromise from a single unknown attack.

We do know one thing about cyber security...

Does spending more money make a computer more secure?



Cyber Security research makes computers less secure!

- Data*
- Encoding*
- Apps*
- OS (programs & patches)*
- Network & VPNs*
- DNS, DNSSEC*
- IPv4 / IPv6*
- Embedded Systems*
- Human operators*
- Hiring process*
- Supply chain*
- Family members*



The more we learn about securing computers,
the better we get at attacking them

Cyber Security is an “insider problem.”

bad actors
good people with bad instructions
remote access
malware



<http://www.flickr.com/photos/shaneglobal/5115134303/>

If we can stop insiders, we might be able to secure cyberspace....

—... *but we can't stop insiders.*



Ames



Hanssen



Cyber Security is a “network security” problem.

We can't secure the hosts, so secure the network!

- Isolated networks for critical functions.
- Stand-alone hosts for most important functions.

OpenSSL
Cryptography and SSL/TLS Toolkit



<http://www.flickr.com/photos/dungkal/2315647839/>

But strong crypto limits visibility into network traffic, and...

... stuxnet shows that there are no isolated hosts.



“to a first approximation, every computer in the world is connected to every other computer.”



<http://www.nytimes.com/2011/06/30/technology/30morris.html>

—*Robert Morris (1932-2001), to the National Research Council’s Computer Science and Technology Board, Sept. 19, 1988*

“Computer Insecurity”, Peter G. Neumann *Issues In Science & Technology*, Fall 1994

“Action is needed on many fronts to protect computer systems and communications from unauthorized use and manipulation.”



ISSUES IN SCIENCE AND TECHNOLOGY

HOME BACK ISSUES

Summer 2003

INTRODUCTION

[Daniel Yankelovich](#) [SCIENCE AND THE PUBLIC PROCESS: Why the Gap Must Close \(Fall 1984\)](#)

RESEARCH & TECHNOLOGY

[D. Allan Bromley](#) [Science, Scientists, and the Science Budget \(Fall 1992\)](#)
[HTML](#) or [PDF](#)

[Lewis M. Branscomb](#) [Toward a U.S. Technology Policy \(Summer 1991\)](#)

[Ralph E. Gomory](#) [A Dialogue on Competitiveness \(Summer 1988\)](#)
[HTML](#) or [PDF](#)

[Harold T. Shapiro](#)

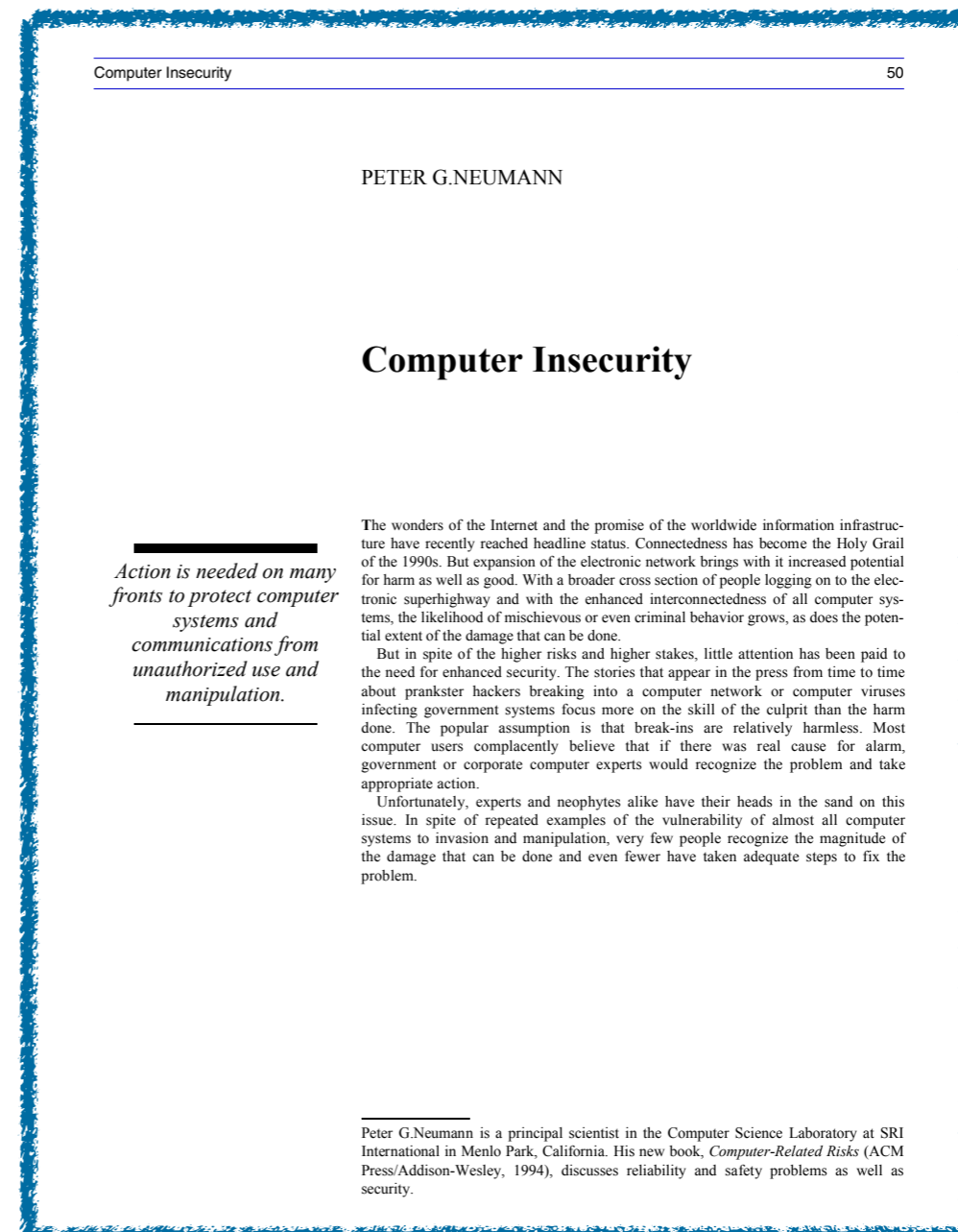
[Erich Bloch](#) [MANAGING FOR CHALLENGING TIMES: A National Research Strategy \(Winter 1986\)](#)
[HTML](#) or [PDF](#)

[John A. Armstrong](#) [University Research: New Goals, New Practices](#)
[HTML](#) or [PDF](#)

[Roland W. Schmitt](#) [Fulfilling the Promise of Academic Research \(Summer 1991\)](#)
[HTML](#) or [PDF](#)

[Larry R. Johnson](#) [Putting Maglev on Track \(Spring 1990\)](#)
[HTML](#) or [PDF](#)

<http://issues.org/19.4/updated/neumann.html>



Computer Insecurity 50

PETER G. NEUMANN

Computer Insecurity

Action is needed on many fronts to protect computer systems and communications from unauthorized use and manipulation.

The wonders of the Internet and the promise of the worldwide information infrastructure have recently reached headline status. Connectedness has become the Holy Grail of the 1990s. But expansion of the electronic network brings with it increased potential for harm as well as good. With a broader cross section of people logging on to the electronic superhighway and with the enhanced interconnectedness of all computer systems, the likelihood of mischievous or even criminal behavior grows, as does the potential extent of the damage that can be done.

But in spite of the higher risks and higher stakes, little attention has been paid to the need for enhanced security. The stories that appear in the press from time to time about prankster hackers breaking into a computer network or computer viruses infecting government systems focus more on the skill of the culprit than the harm done. The popular assumption is that break-ins are relatively harmless. Most computer users complacently believe that if there was real cause for alarm, government or corporate computer experts would recognize the problem and take appropriate action.

Unfortunately, experts and neophytes alike have their heads in the sand on this issue. In spite of repeated examples of the vulnerability of almost all computer systems to invasion and manipulation, very few people recognize the magnitude of the damage that can be done and even fewer have taken adequate steps to fix the problem.

Peter G. Neumann is a principal scientist in the Computer Science Laboratory at SRI International in Menlo Park, California. His new book, *Computer-Related Risks* (ACM Press/Addison-Wesley, 1994), discusses reliability and safety problems as well as security.

<http://issues.org/19.4/updated/neumann.pdf>



It is easy to hide & exfiltrate information...

October 16, 2005

Secret Code in Color Printers Lets Government Track You

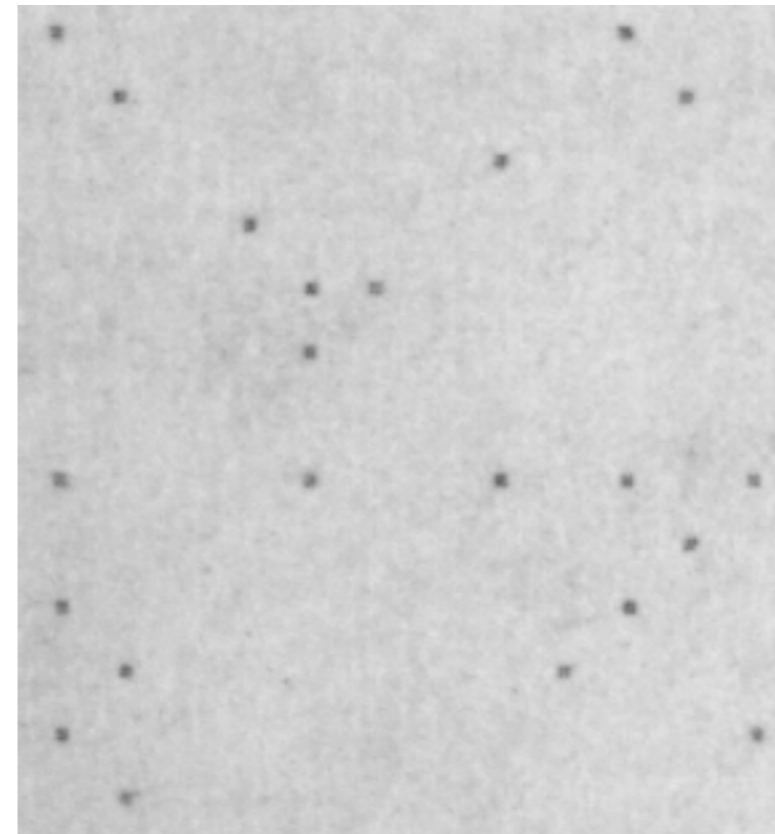
Tiny Dots Show Where and When You Made Your Print

San Francisco - A research team led by the Electronic Frontier Foundation (EFF) recently broke the code behind tiny tracking dots that some color laser printers secretly hide in every document.



**Sample closeup of
printer dots on a
normal printed page**

<http://seeingyellow.com/>



**Sample closeup of the
same dots showing only
the blue channels to
make the dots more
visible.**

Cyber Security is a process problem.

Security encompasses all aspects of an organization's IT and HR operations.

Microsoft Security Development Lifecycle

What is the Security Development Lifecycle ?

The Security Development Lifecycle (SDL) is a software development security assurance process consisting of security practices grouped by seven phases: training, requirements, design, implementation, verification, release, and response.



"Those practicing SDL specifically reported visibly better ROI results than the overall population."

Forrester Consulting

**"Security is a process,
not a product"**



http://en.wikipedia.org/wiki/File:Bruce_Schneier_1.jpg

- Few organizations can afford SDL.*
- ~~Windows 7~~ *Windows 8 is still hackable...*

Windows RT hack

Microsoft controlled the hardware and the software.

Windows RT — still hacked



nakedsecurity
Award-winning news, opinion, advice and research from **SOPHOS**

malware mac facebook android vulnerability data loss privacy more...

Smart octogenarian foils scammer w... The TURKTRUST SSL certificate fia...

Windows RT "jailbroken", shows its Windows 8 roots

Join thousands of others, and sign up for Naked Security's newsletter

Don't show me this again

by Chester Wisniewski on January 8, 2013 | 2 Comments
FILED UNDER: [Featured](#), [Microsoft](#), [Vulnerability](#), [Windows](#)

Hey Windows RT, your roots are showing!

Not that it is all that surprising to most people, but the first person to post about jailbreaking a Microsoft Windows RT device says it is a **direct port of Windows 8**.

Microsoft has gone to some lengths to disguise this fact: no desktop mode applications (except Office, Explorer and IE10), only runs software from the Windows Store and can't

Cyber Security is a money problem.

Security is a cost.....Not an “enabler”

- No ROI

Chief Security Officers are in a no-win situation:

- Security = passwords = frustration
- No reward for spending money to secure the infrastructure
- Money spent on security is “wasted” if there is no attack

“If you have responsibility for security but have no authority to set rules or punish violators, your own role in the organization is to take the blame when something big goes wrong.”

—*Spaf's first principle of security administration*
Practical Unix Security, 1991



Cyber Security is a “wicked problem”

No clear definition of the wicked problem

—*You don't understand the problem until you have a solution.*

No “stopping rule”

—*The problem can never be solved.*

Solutions not right or wrong

—*Benefits to one player hurt another — Information security vs. Free speech*

Solutions are “one-shot” — no learning by trial and error

—*No two systems are the same. The game keeps changing.*

Every wicked problem is a symptom of another problem

- Rittel and Webber, “Dilemmas in a General Theory of Planning,” 1973
- Dave Clement, “Cyber Security as a Wicked Problem,” Chatham House, October 2011
 - <http://www.chathamhouse.org/publications/twt/archive/view/178579>



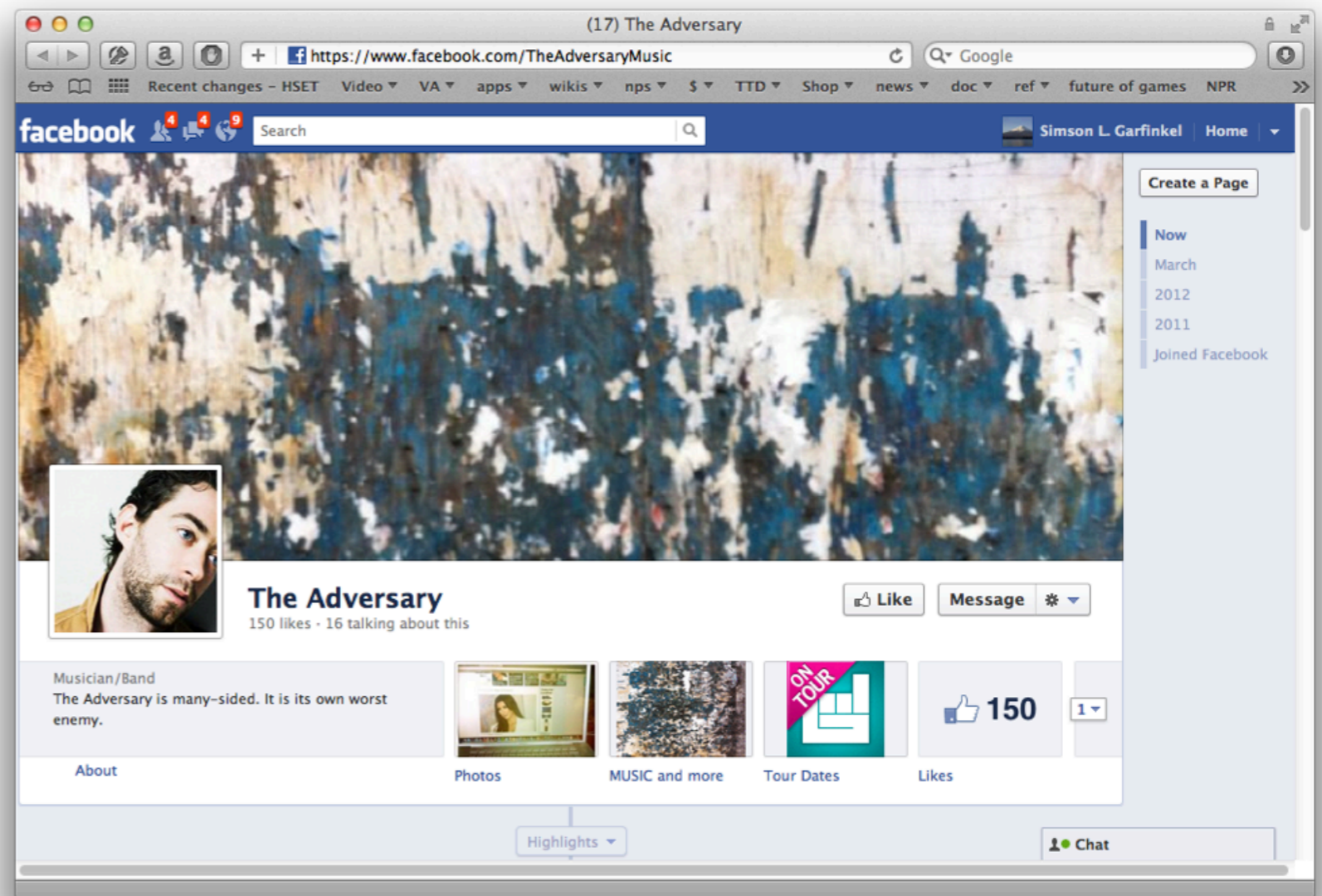
Why is cyber
security so
hard?



Cyber Security has an active, malicious adversary.

The adversary...

- Turns your bugs into exploits*
- Adapts to your defenses*
- Waits until you make a mistake*
- Attacks your employees when your systems are secure*



For example...

Compiler bugs are security vulnerabilities!

The adversary chooses:

- What to exploit
- When to exploit it
- How to exploit it

We have seen:

- Optimizations can become security vulnerabilities
- The same errors are repeatedly made by different programmers

What's difference between a bug and an attack?

—*The programmer's intent.*



The screenshot shows a web browser window displaying a US-CERT Vulnerability Note. The browser's address bar shows the URL <http://www.kb.cert.org/vuls/id/162289>. The page header features the US-CERT logo and the text "US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM". Below the header is a navigation bar with links for "DATABASE HOME", "SEARCH", "REPORT A VULNERABILITY", and "HELP". The main content area is titled "Vulnerability Note VU#162289" and "C compilers may silently discard some wraparound checks". It includes the original release date (04 Apr 2008) and the last revised date (08 Oct 2008). There are social media sharing buttons for Print, Tweet, Send, and Share. The "Overview" section states: "Some C compilers optimize away pointer arithmetic overflow tests that depend on undefined behavior without providing a diagnostic (a warning). Applications containing these tests may be vulnerable to buffer overflows if compiled with these compilers." The "Description" section begins with "In the C language, given the following types:" and shows a code snippet:

```
char *buf;
int len;
```

 It then explains that some C compilers will assume that `buf+len >= buf`. It provides a code snippet for a wrap check:

```
len = 1<<30;
[...]
if(buf+len < buf) /* wrap check */
    [...overflow occurred...]
```

 The final paragraph states: "are optimized out by these compilers; no object code to perform the check will appear in the resulting executable program. In the case where the wrap test expression is optimized out, a subsequent manipulation of len could cause an overflow. As a result, applications that perform such checks may be vulnerable to buffer overflows."

It's worse than that...

CPU bugs are remotely exploitable!

This means:

- Programs that are “secure” on one CPU may be vulnerable on another.
- Auditing the code & the compiler isn't enough.

Kaspersky:

- “Fact: malware that uses CPU bugs really does exist;”
- “not apocalypse, just a new threat;”
-

Remote Code Execution
through Intel CPU Bugs

CPU bugs are like a bullet from behind

Kris Kaspersky, Alice Chang
Endeavor Security, Inc.

HITB SEC CONF 2008 MALAYSIA
27th - 30th October 2008

5 Days of Hands-on Technical Security Training
200+ Experts Speaking and over 1000 International Experts
Nightclub, Security hardware, including over 10000 items!
Capture the Flag "RedHacking" Competition
Last Friday Party for 2000+ people
Water Village (Johor, Malaysia, 2008)
Non-stop live streaming

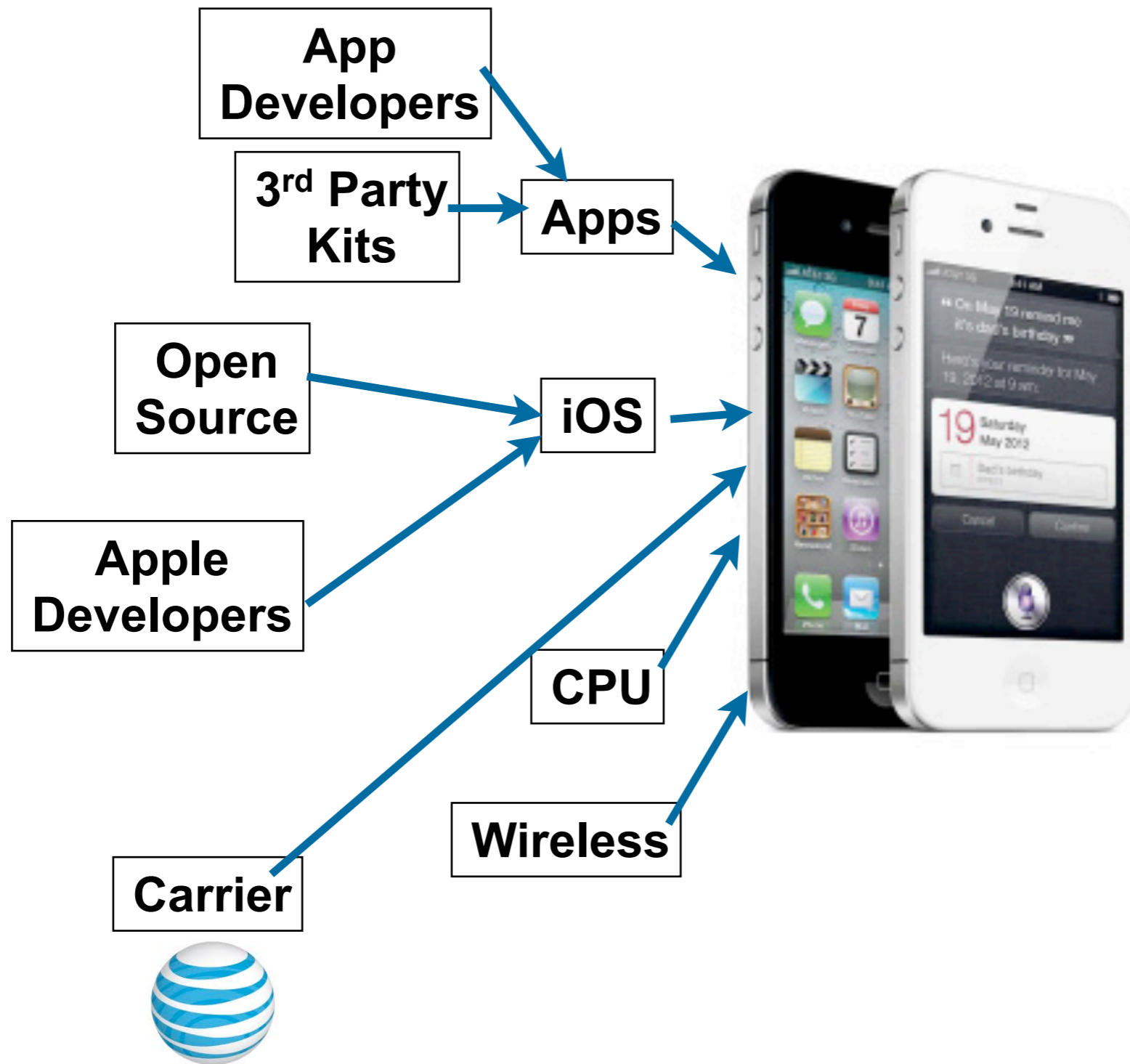
10Mbps INTERNET LINK
WIFI MESHWORK (STUDIONET)

endeavor
security, inc.

www.cs.dartmouth.edu/~sergey/cs258/2010/D2T1 - Kris Kaspersky - Remote Code Execution Through Intel CPU Bugs.pdf



The supply chain creates numerous security vulnerabilities



The attacker is smarter than you are... ... and has more time to find a good attack.



3 accelerometers
no privacy

ACComplce: Location Inference using Accelerometers on Smartphones

Jun Han, Emmanuel Owusu, Le T. Nguyen, Adrian Perrig, Joy Zhang
{junhan, eowusu, lenguyen, perrig, sky}@cmu.edu
Carnegie Mellon University

Abstract—The security and privacy risks posed by smartphone sensors such as microphones and cameras have been well documented. However, the importance of accelerometers has been largely ignored. We show that accelerometer readings can be used to infer the trajectory and starting point of an individual who is driving. This raises concerns for two main reasons. First, unauthorized access to an individual's location is a serious invasion of privacy and security. Second, current smartphone operating systems allow any application to observe accelerometer readings without requiring special privileges. We demonstrate that accelerometers can be used to locate a device owner to within a 200 meter radius of the true location. Our results are comparable to the typical accuracy for handheld global positioning systems.

I. INTRODUCTION

Location privacy has been a hot topic in recent news after it was reported that Apple, Google, and Microsoft collect records of the location of customers using their mobile operating systems [12]. In some cases, consumers are seeking compensation in civil suits against the companies [8]. Xu and Teo find that, in general, mobile phone users express lower levels of concern about privacy if they control access to their personal information. Additionally, users expect their smartphones to provide such a level of control [20].

There are situations in which people may want to broadcast their location. In fact, many social networking applications incorporate location-sharing services, such as geo-tagging photos and status updates, or checking in to a location with friends. However, in these instances, users can control when their location is shared and with whom. Furthermore, users express a need for an even richer set of location-privacy settings than those offered by current location-sharing applications [2]. User concerns over location-privacy are warranted. Websites like "Please Rob Me" underscore the potential dangers of exposing one's location to malicious parties [5]. The study presented here demonstrates a clear violation of user control over sensitive private information.

This research was supported by CyLab at Carnegie Mellon under grants DAAD19-02-1-0389 and W911NF-09-1-0273, from the Army Research Office, and by support from NSF under TRUST STC CCF-0424422, IGERT DGE-0903659, and CNS-1050224, and by a Google research award. The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either express or implied, of ARO, CMU, Google, NSF or the U.S. Government or any of its agencies.

978-1-4673-0298-2/12/\$31.00 © 2012 IEEE

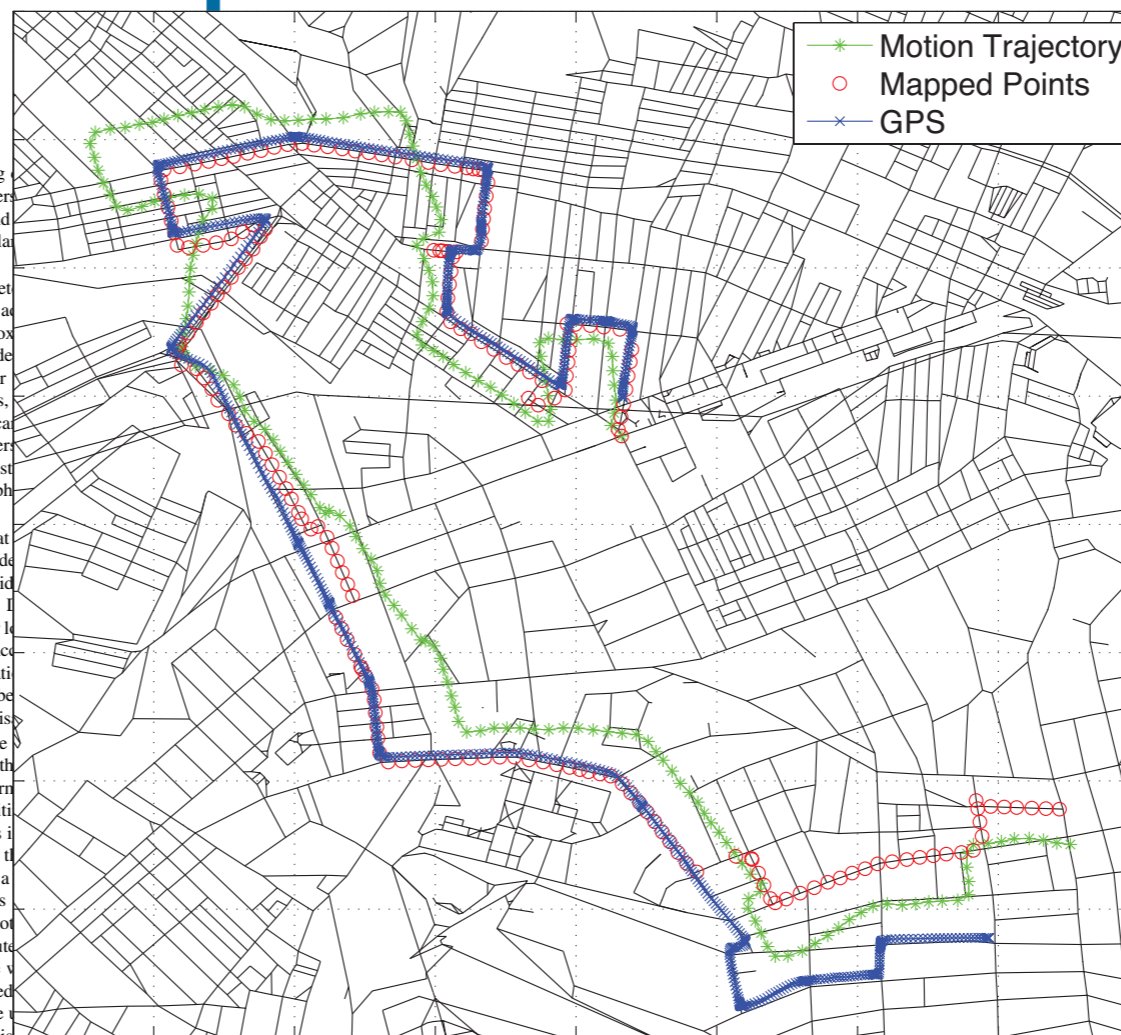
Accelerometers are a particularly interesting device due to their pervasiveness in a large assortment of personal devices including tablet PCs, MP3 players, and other mobile devices. This array of devices provides a large number of opportunities for spyware to exploit.

Furthermore, by correlating the accelerometer readings between multiple phones it is possible for an adversary to determine whether the phones are in close proximity. Phones undergoing similar motions can be identified by their accelerations, events such as earthquakes or activities like public transportation (e.g., bus, train, etc.) produce identifiable motion signatures that can be used to track a user's location long after they have been disabled [6]. But as we show, the accelerometer can be used to infer a location with no initial location. This is a very powerful side-channel that can be used to track location-based services on the device are disabled.

a) Contributions: Our key insight is that by analyzing the noisy trajectory output. This is because the idiosyncratic roadways create globally unique constraints. It can be used to track a user's location long after location services have been disabled [6]. But as we show, the accelerometer can be used to infer a location with no initial location. This is a very powerful side-channel that can be used to track location-based services on the device are disabled.

b) Threat Model: We assume that the adversary can execute applications on the mobile device, with privileges except the capability to send information over the network. The application will use some legitimate means to obtain access to network communication. This is accomplished by mimicking a popular application that requires a download; e.g., a video game. In the case of a game, access would be needed to upload high scores to a server. We assume that the OS is not patched so that the malicious application simply executes. The application can communicate with a server to leak acceleration information. Based on this information, the adversary can extract a mobile location from the compromised device via data analysis.

Our goal is to determine the location of an individual driving in a vehicle based solely on motion sensor measurements. The general approach that we take is to first derive an approximate motion trajectory given acceleration measurements—which we discuss in §II. We then correlate that trajectory with map



https://sparrow.ece.cmu.edu/group/pub/han_ACComplce_comsnets12.pdf

Jun Han, Emmanuel Owusu, Thanh-Le Nguyen, Adrian Perrig, and Joy Zhang
"ACComplce: Location Inference using Accelerometers on Smartphones" In Proceedings of the 4th International Conference on Communication Systems and Networks (COMSNETS 2012), Bangalore, India, January 3-7, 2012.



Fortunately adversaries are not all powerful.

Adversaries are impacted by:

- Economic factors*
- Attention span*
- Other opportunities*

You don't have to run faster than the bear....



There are solutions to many cyber security problems... ... but we don't use them.

30% of the computers on the Internet run Windows XP

- Windows 7 has vulnerabilities, but it's better.



Apple users don't use anti-virus.

- Yes, Apple tries to fix bugs, but

Most "SSL" websites only use it for logging in.

DNSSEC

Smart Cards



Country	Percentage
United Kingdom	12.8%
France	6.6%
Germany	4.4%
Spain	4.4%
Italy	3.3%
Netherlands	2.2%
Switzerland	1.1%
Ireland	1.1%
United States	56.6%
Mexico	0.3%
Canada	19.8%
Turkey	0.1%
Japan	0.1%
Philippines	0.1%

Many people liken cyber security to the flu.

DHS calls for “cyber hygiene”

- install anti-virus
- update your OS
- back up key files

—“STOP, THINK, CONNECT”

The screenshot shows a web browser window displaying a page from CIO.GOV. The page title is "National Cybersecurity Awareness Month Advocates Good “Cyber Hygiene”". The article text includes: "Surfing the web. Social networking. Shopping. Even the most innocuous online activities can pose a threat to our nation’s cybersecurity, and all Americans should play a part in protecting it." and "That’s the message behind the seventh annual National Cybersecurity Awareness Month this October. Sponsored by the Department of Homeland Security (DHS), National Cybersecurity Awareness Month encourages the practice of good “cyber hygiene”: taking simple precautions to reduce the cyber risks to our national and economic security." A quote box on the right side of the article reads: "Even the most innocuous online activities can pose a threat to our nation’s cybersecurity, and all Americans should play a part in protecting it." Below the main text, there is a section titled "Simple Steps to Staying Secure" which lists three bullet points: "Make sure to install anti-virus software and firewalls and that they are properly configured, and up-to-date.", "Update your operating system and critical program software.", and "Back up key files." The right sidebar contains "Related Blog Posts" with titles like "Cybersecurity Transformation and Information Sharing at the Department of Energy" and "The “Business” of Cybersecurity!".



Another model might be *obesity*....

Making people fat is good business:

- Farm subsidies
- Restaurants
- Healthcare and medical utilization
- Weight loss plans
 - Few make money when Americans stay trim and healthy.*

Lax security is also good business:

- Cheaper cost of deploying software
- Private information for marketing
- Selling anti-virus & security products
- Cleaning up incidents
 - Few benefit from secure computers*



Obesity Rates Increase

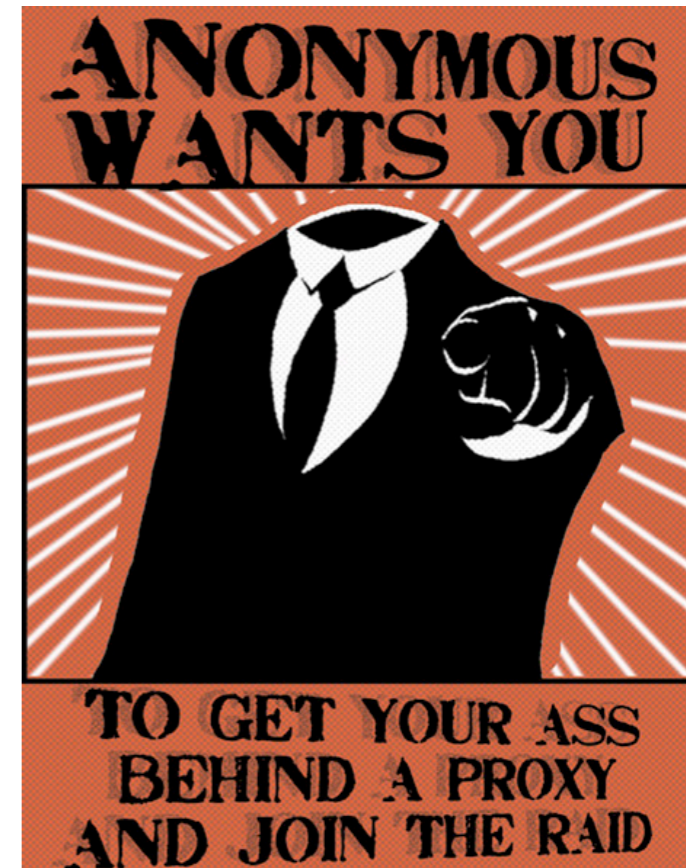
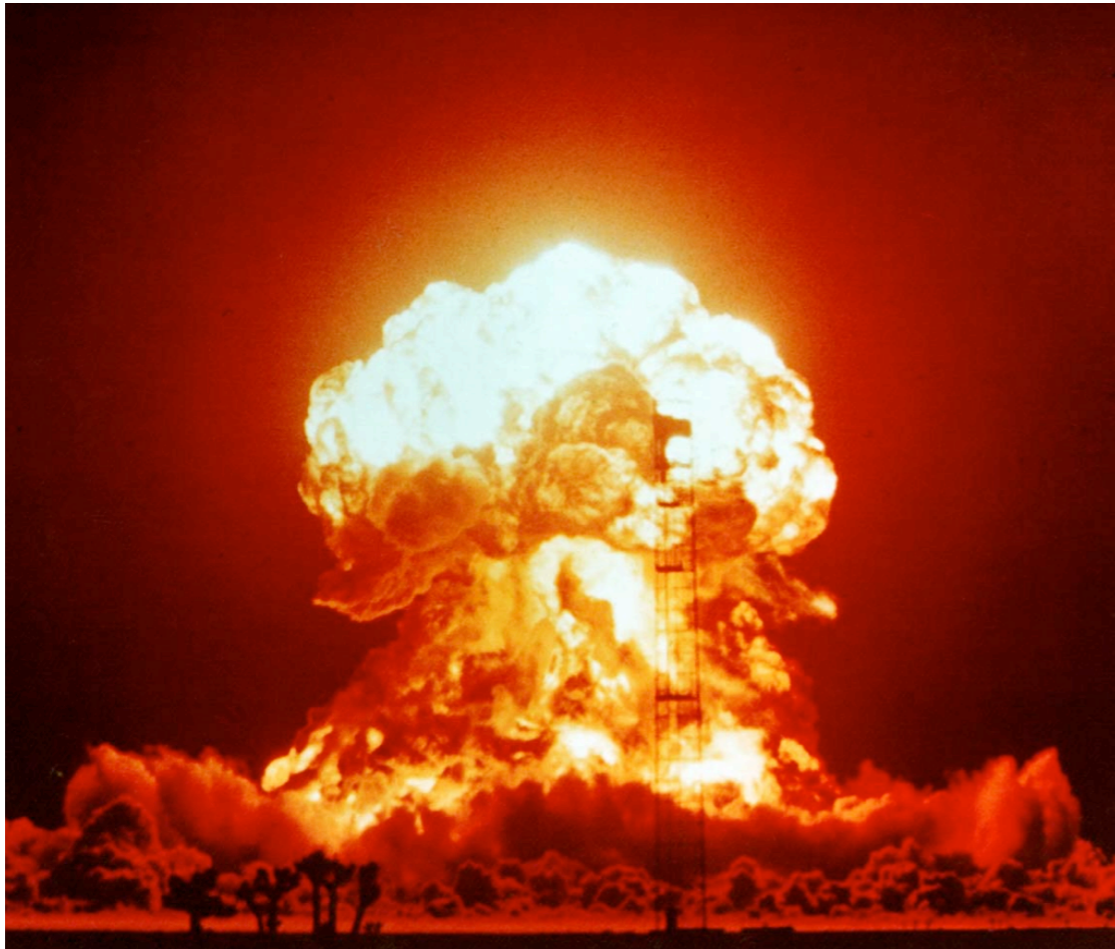
During the past 20 years, there has been a dramatic increase in obesity in the U.S.

OAC
Obesity Action Coalition

The Obesity Action Coalition (OAC) is the only non-profit organization whose sole focus is helping individuals affected by obesity through education, advocacy, and support.

www.obesityaction.org (800) 717-3117

Some people say that cyber war is like nuclear war.



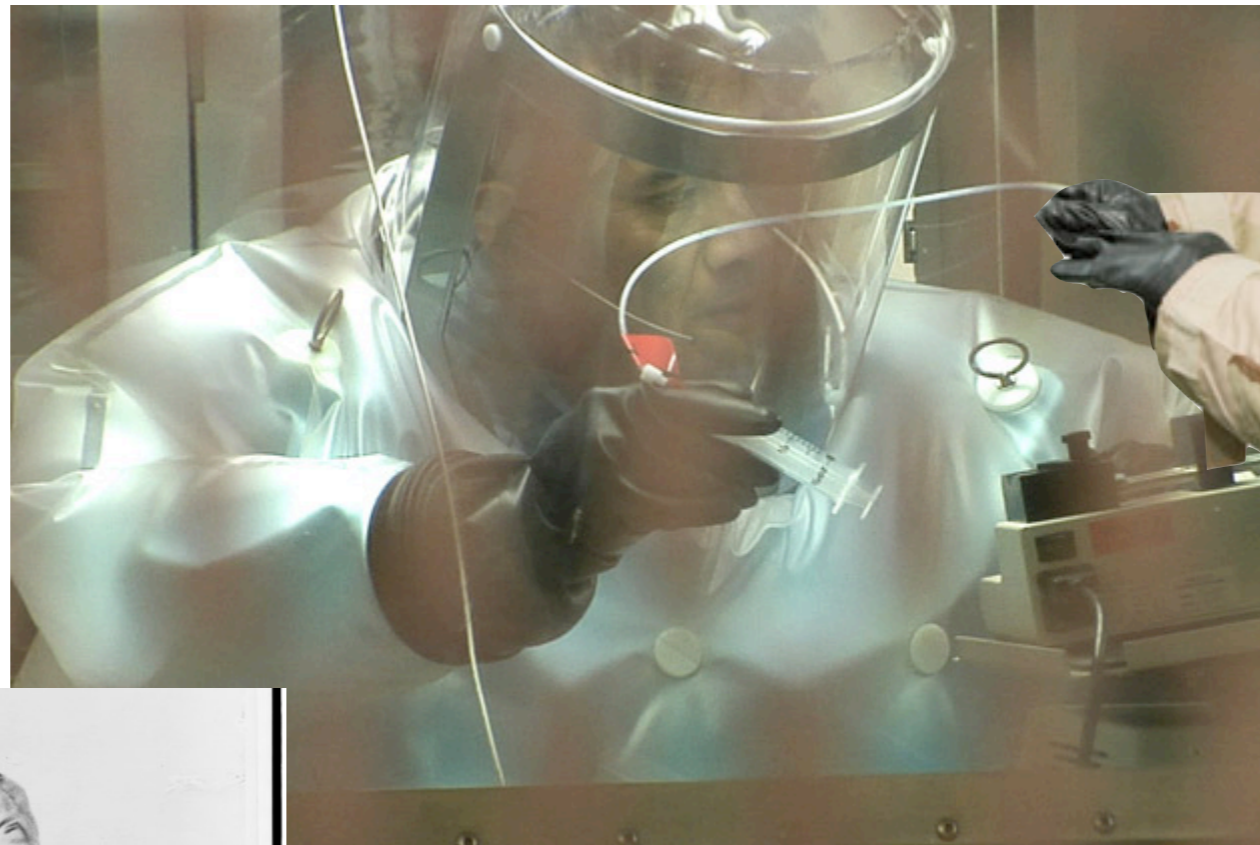
http://www.acus.org/new_atlanticist/mind-cyber-gap-deterrence-cyberspace



<http://www.beyondnuclear.org/security/>

Biowar may be a better model for cyberwar.

- Cheap to produce*
- Easy to attack*
- Hard to control*
- Hard to defend*
- No clear end*



Irving Lachow: Cyber Insecurity is Air Pollution

By-product of:

- eCommerce
- Web browsing
- email
- social media

Inherent with [today's] technology

Impacts society as a whole

“Negative externality”

Good news: we can reduce insecurity to an acceptable level.



TECHNOLOGY

Cyber Insecurity: The 21st Century's Version of Air Pollution

By Irving Lachow | May 10, 2013 | 1 Comment

Like 47 Tweet 77 Share 18 Send to Kindle

GETTY IMAGES

– Then-defense secretary Leon Panetta referred to the threat of cyber attacks as a “**cyber Pearl Harbor**.”

– A senior Cyber Command official has declared that we are in the middle of a “**cyber arms race**.”

– Other experts have used **public health** as a metaphor for the cyber security challenge facing our nation.

Email Print

Share Comment

Follow @TIME

Non-technical factors impact cyber security.

These factors reflect deep divisions within our society.

- **Shortened** development cycles
- **Education:** General failure in teaching science, engineering & math
- **HR:** Inability to attract and retain the best workers
- **Immigration Policy:** Foreign students; H1B Visa
- **Manufacturing Policy:** Building in your enemy's factories is a bad idea

Solving the cyber security mess requires solving these issues



Short development cycles

Insufficient planning:

- Security not “baked in” to most products.
- Few or no security reviews
- Little Usable Security

Insufficient testing:

- Testing does not uncover security flaws
- No time to retest after fixing

Poor deployment:

- Little monitoring for security problems
- Difficult to fix current system when new system is under development



The screenshot shows a web browser window with the URL <http://www.examiner.com/vi>. The page is from Examiner.com, dated September 7, 2009. The article title is "Final Fantasy producers: expect shorter development cycle in the future" by Eric Keihl, Pittsburgh Video Game Examiner. The article text discusses Square Enix producers Yoshi Kitase and Motomu Toriyama's comments on shortening development cycles for future projects. A photo of a woman with a large gun is shown on the right side of the article.

Final Fantasy producers: expect shorter de...re - Pittsburgh Video Game | Examiner.com

<http://www.examiner.com/vi> Reader

Google

Recent changes - HSET Video VA apps wikis nps \$ TTD

We think you're near Pitts

examiner.com

Google

INTERESTS Creative Games Automotive Gadgets & Tech Travel More

GAMES | September 7, 2009 | ADD A COMMENT

Final Fantasy producers: expect shorter development cycle in the future

 **Eric Keihl**
Pittsburgh Video Game Examiner
[+ Subscribe](#)

[Like](#) [Tweet](#) [+1](#) [StumbleUpon](#) [Email](#) [Report](#) [Print](#)

Good news for *Final Fantasy* fans (and cosplayers:) in an interview at [Gamescom](#), Square Enix producers Yoshi Kitase and Motomu Toriyama explained that since their development team is now used to the current-generation hardware, "development time for future projects should be shortened." Welcome words for those who have a patiently endured the 4 years of waiting between *Final Fantasy XII* and *Final Fantasy XIII* (set for a US release in 2010,) though just how much the development cycle will be contracted remains to be seen.

If history is any indication, the franchise could well return to the routine of the early 90's (*III* - *V*) and early 00's (*VIII* - *XI*) when new games were being released


A woman, save the world? How delightfully absurd!

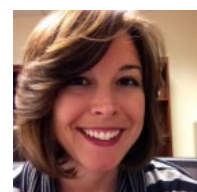
Education is not supplying enough security engineers

Security HR Pipeline

- High School → College → Graduate School → Career

Mastery Issue:

- Many professional programmers learn their craft in college.
- College English graduates: 16 years' instruction in writing
- College CS graduates: 4 years' instruction in programming
—*Is it any wonder their code has security vulnerabilities?*

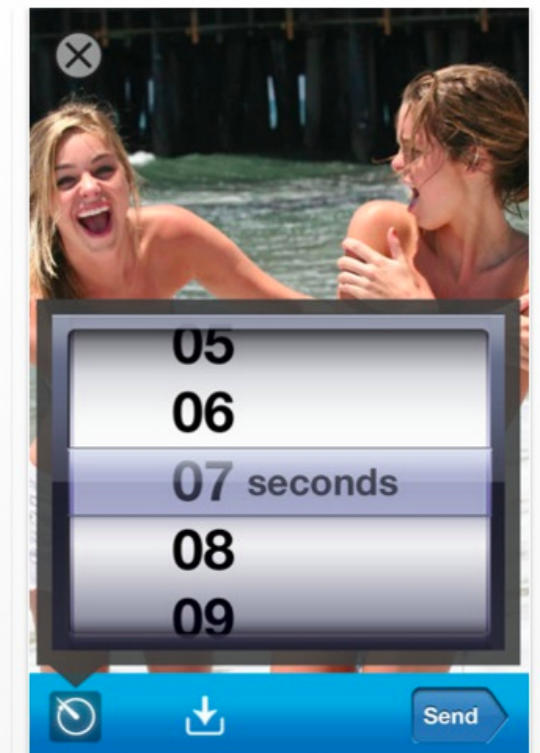


Kashmir Hill, Forbes Staff
Welcome to The Not-So Private
[Follow](#) (1,349) [Follow](#)

TECH | 5/09/2013 @ 4:51PM | 261,967 views

Snapchats Don't Disappear: Forensics Firm Has Pulled Dozens of Supposedly-Deleted Photos From Android Phones

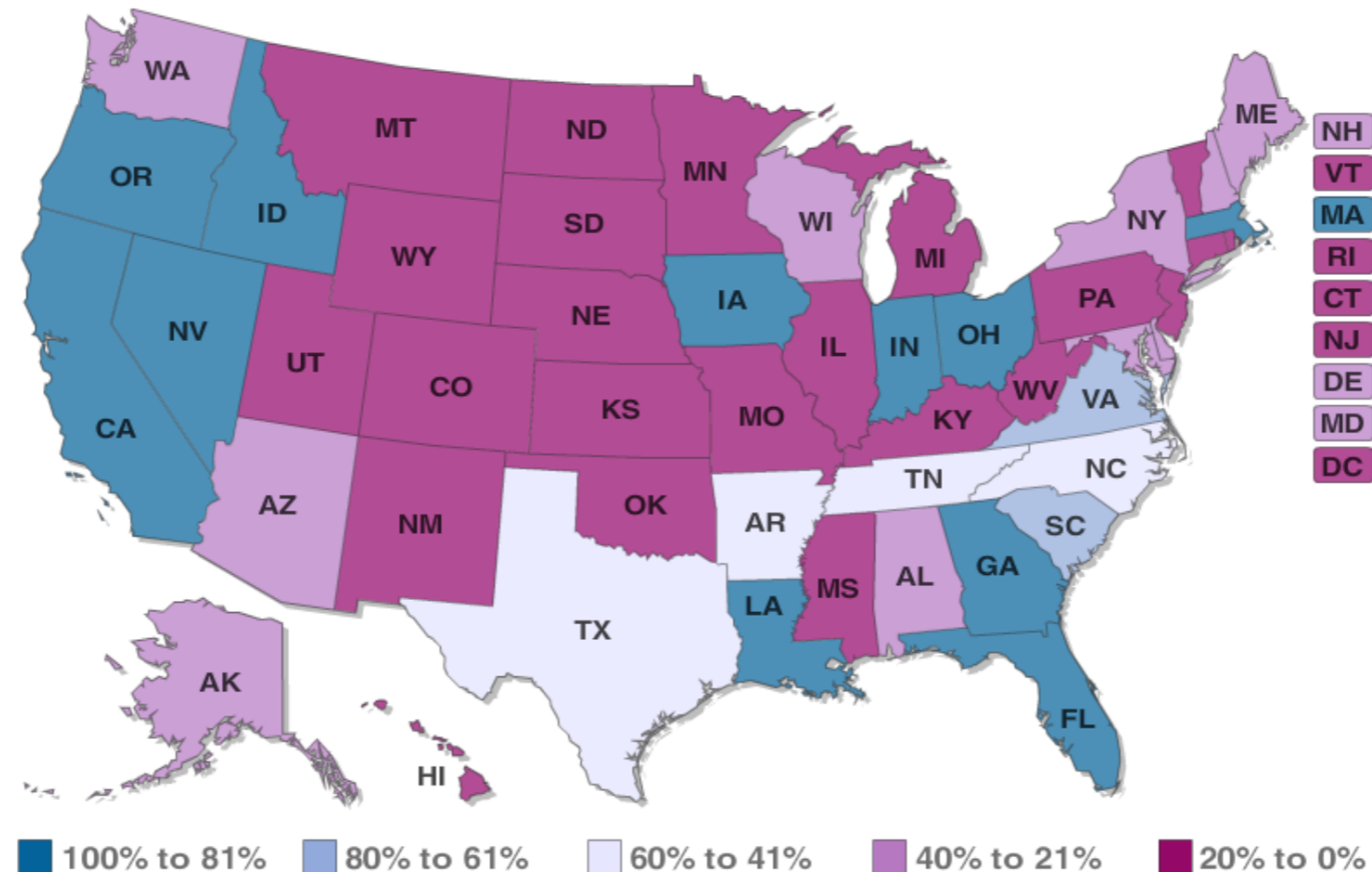
iPhone Screenshots



<http://www.forbes.com/sites/kashmirhill/2013/05/09/snapchats-dont-disappear/>

73% of states require computer “skills” for graduation.
Only 37% require CS “concepts”

Concepts Adoption Rates



And teachers are poorly paid!

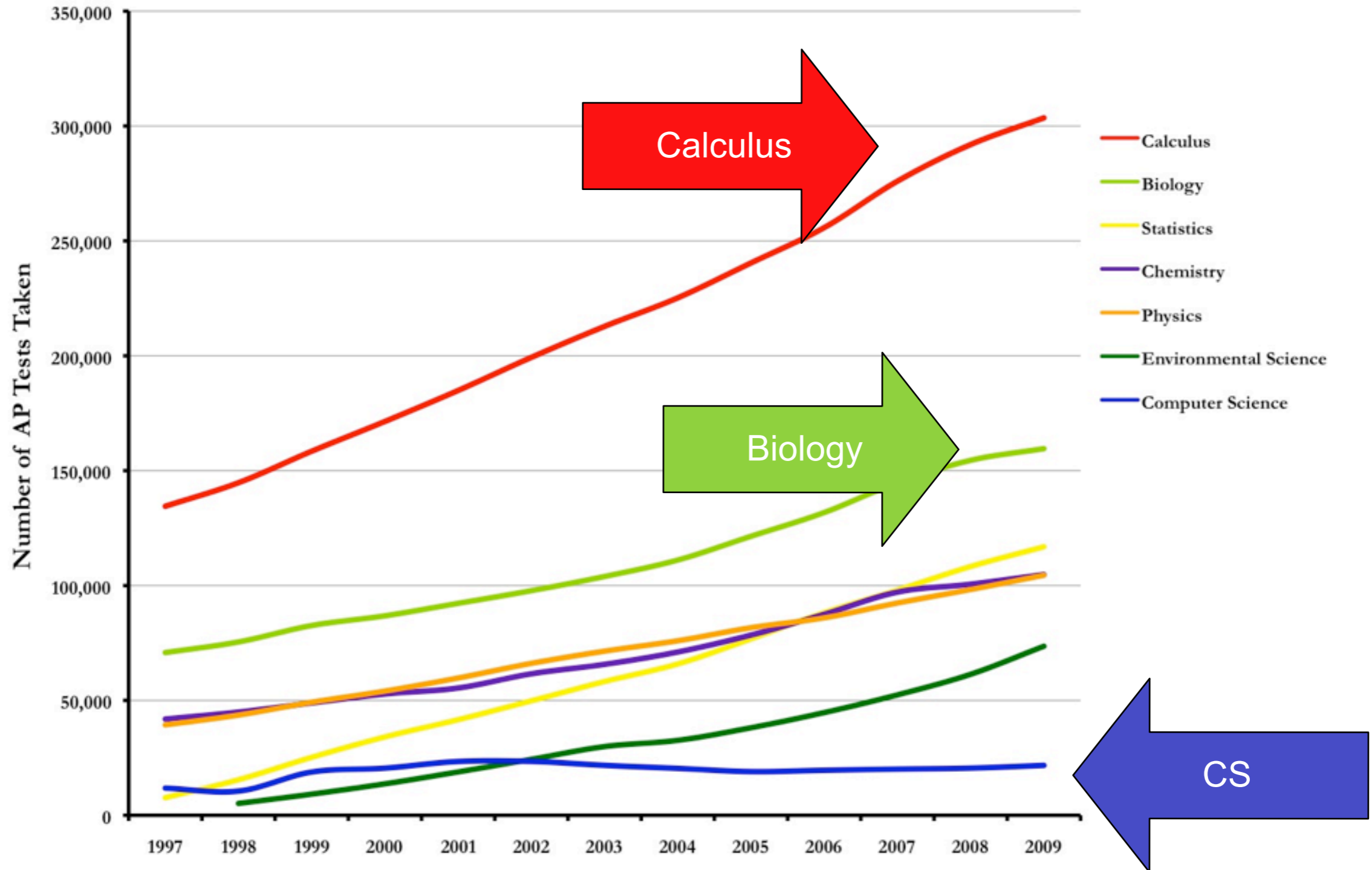
—Salaries for beginning & average teachers lag CS engineers by 30%

—Adjusting for cost-of-living and shorter work week.

- Linda Darling-Hammond, Stanford University, 2004
http://www.srnleads.org/data/pdfs/ldh_achievemen_gap_summit/inequality_TCR.pdf



High school students are not taking AP computer science!

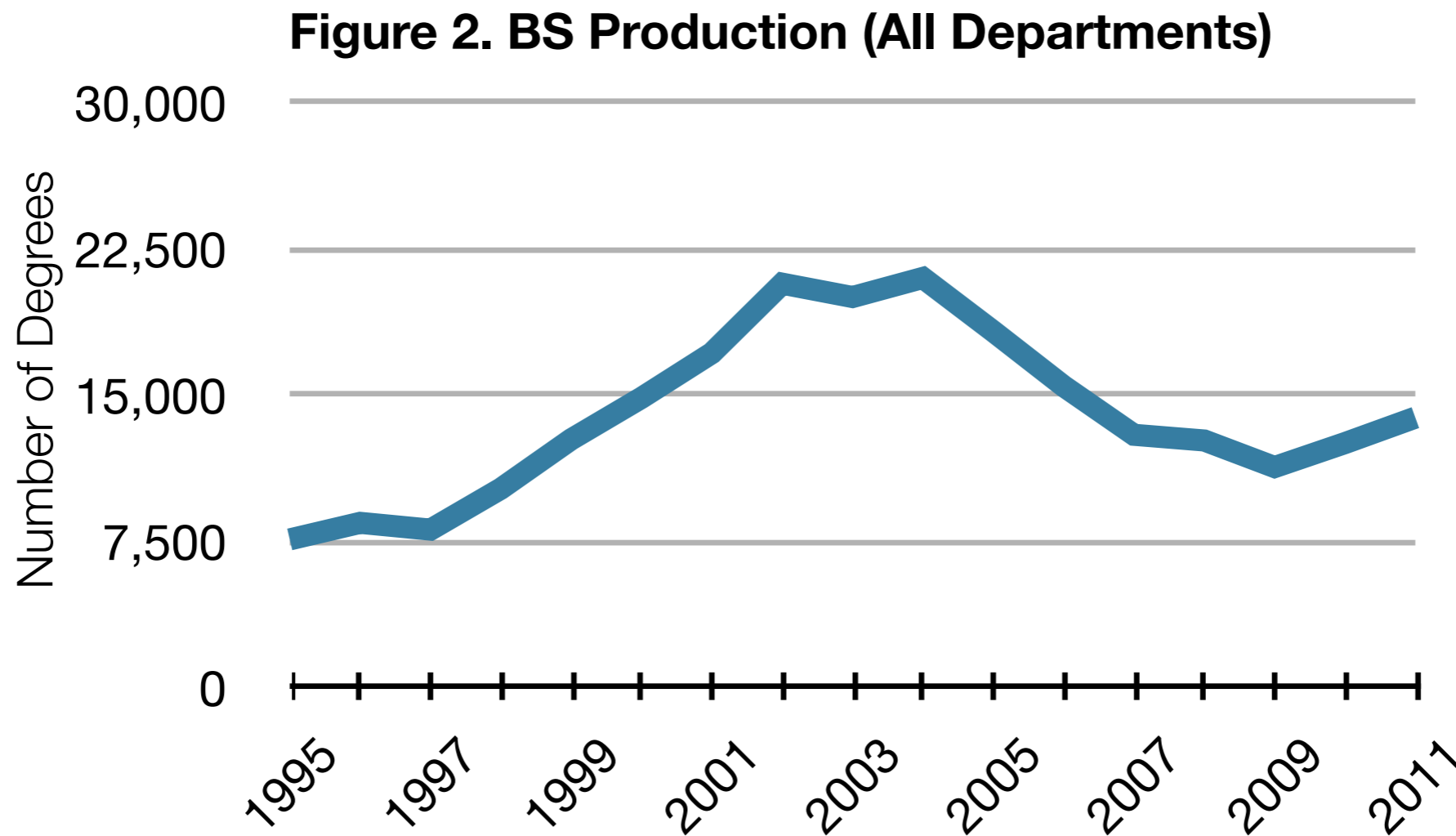


<http://www.acm.org/public-policy/AP%20Test%20Graph%202009.jpg>



Computer Science undergraduate enrollment is low.

2010-2011 CRA Taulbee Survey:



Source: Table 3: Bachelor's Degrees Awarded by Department Type



7% of Bachelor's degrees awarded to "nonresident alien" (12,800 to US citizens)

	CS		CE		I		Total	
Nonresident Alien	524	7.0%	179	10.0%	78	3.6%	781	6.8%
Amer Indian or Alaska Native	39	0.5%	8	0.4%	16	0.7%	63	0.5%
Asian	1,115	14.8%	337	18.8%	302	13.9%	1,754	15.3%
Black or African-American	274	3.6%	106	5.9%	151	6.9%	531	4.6%
Native Hawaiian/Pac Islander	22	0.3%	7	0.4%	8	0.4%	37	0.3%
White	5026	66.9%	981	54.7%	1432	65.8%	7,439	64.8%
Multiracial, not Hispanic	104	1.4%	28	1.6%	3	0.1%	135	1.2%
Hispanic, any race	409	5.4%	146	8.1%	187	8.6%	742	6.5%
Total Residency & Ethnicity Known	7,513		1,792		2,177		11,482	
Resident, ethnicity unknown	741		200		99		1,040	
Residency unknown	1032		112		140		1,284	
Grand Total	9,286		2,104		2,416		13,806	

—Most do not go on to advanced degrees.



50% of Master's degrees awarded to nonresident alien (4960 to US citizens)

Table 9. Master's Degrees Awarded by Ethnicity

	CS		CE		I		Total	
	Count	Percentage	Count	Percentage	Count	Percentage	Count	Percentage
Nonresident Alien	3,332	56.7%	776	72.6%	389	19.6%	4,497	50.4%
Amer Indian or Alaska Native	12	0.2%	0	0.0%	12	0.6%	24	0.3%
Asian	753	12.8%	108	10.1%	245	12.3%	1,106	12.4%
Black or African-American	96	1.6%	13	1.2%	123	6.2%	232	2.6%
Native Hawaiian/Pac Island	19	0.3%	0	0.0%	6	0.3%	25	0.3%
White	1533	26.1%	142	13.3%	1113	56.1%	2,788	31.2%
Multiracial, not Hispanic	8	0.1%	4	0.4%	4	0.2%	16	0.2%
Hispanic, any race	119	2.0%	26	2.4%	92	4.6%	237	2.7%
Total Residency & Ethnicity Known	5,872		1,069		1,984		8,925	
Resident, ethnicity unknown	320		88		205		613	
Residency unknown	419		26		17		462	
Grand Total	6,611		1,183		2,206		10,000	



50% of PhDs awarded in 2011 to nonresident aliens (642 to US citizens)

Table 13. PhDs Awarded by Ethnicity

	CS		CE		I		Total	
Nonresident Alien	634	48.1%	130	67.4%	44	37.0%	808	49.6%
Amer Indian or Alaska Native	2	0.2%	0	0.0%	2	1.7%	4	0.2%
Asian	171	13.0%	16	8.3%	14	11.8%	201	12.3%
Black or African-American	16	1.2%	1	0.5%	6	5.0%	23	1.4%
Native Hawaiian/Pac Islander	4	0.3%	0	0.0%	0	0.0%	4	0.2%
White	465	35.3%	42	21.8%	52	43.7%	559	34.3%
Multiracial, not Hispanic	3	0.2%	0	0.0%	0	0.0%	3	0.2%
Hispanic, any race	22	1.7%	4	2.1%	1	0.8%	27	1.7%
Total Residency & Ethnicity Known	1,317		193		119		1,629	
Resident, ethnicity unknown	43		4		2		49	
Residency unknown	96		8		0		104	
Grand Total	1,456		205		121		1,782	

—We did not train Russia's weapons scientists at MIT during the Cold War.



Just 67 / 1275 (5%) PhDs went into Information Assurance 15 professors & postdocs; 48 to industry & government

Table 14. Employment of New PhD Recipients By Specialty

	Artificial Intelligence	Computer-Supported Cooperative Work	Databases / Information Retrieval	Graphics/Visualization	Hardware/Architecture	Human-Computer Interaction	High-Performance Computing	Informatics: Biomedical/ Other Science	Information Assurance/Security	Information Science	Information Systems	Networks	Operating Systems	Programming Languages/ Compilers	Robotics/Vision	Scientific/ Numerical Computing	Social Computing/ Social Informatics	Software Engineering	Theory and Algorithms	Other	Total	
North American PhD Granting Depts.																						
Tenure-track	14	1	5	6	2	10	1	2	5	9	2	6	2	3	3	1	4	7	6	13	102	7.1%
Researcher	6	1	4	6	1	1	0	6	2	0	2	7	2	2	2	3	1	3	7	17	73	5.1%
Postdoc	38	1	12	17	4	12	0	20	7	5	2	12	7	7	14	6	3	10	30	34	241	16.8%
Teaching Faculty	2	1	1	0	0	1	0	1	1	2	1	1	1	1	0	0	3	4	4	4	28	2.0%
North American, Other Academic																						
Other CS/CE/I Dept.	3	0	4	1	1	1	4	2	2	0	5	6	1	0	0	0	0	3	1	18	52	3.6%
Non-CS/CE/I Dept.																						
North American, Non-Academic																						
Industry	64	2	49	46	41	24	20	17	40	5	6	67	29	22	25	6	12	86	32	83	676	47.2%
Government	7	0	5	2	6	2	5	3	8	1	2	1	0	0	2	4	1	4	2	5	60	4.2%
Self-Employed	0	0	0	1	0	1	0	1	0	0	2	2	2	0	1	0	0	1	1	1	13	0.9%
Unemployed	2	0	2	1	2	2	1	0	2	0	1	3	0	0	1	0	2	0	1	3	23	1.6%
Other	2	0	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	1	0	7	0.5%
Total Inside North America																						
	138	6	83	80	57	54	32	53	67	22	23	106	44	35	48	20	26	118	85	178	1,275	89.0%

Security should be taught to everyone, but we need specialists



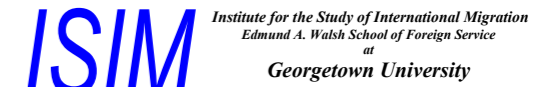
Georgetown Prof: 50% of graduate students in sciences are foreigners because salaries aren't high enough.

“...the problem may not be that there are too few STEM qualified college graduates, but rather that STEM firms are unable to attract them.

Highly qualified students may be choosing a non-STEM job because it pays better, offers a more stable professional career, and/or perceived as less exposed to competition from low-wage economies.”



John J. Heldrich Center for Workforce Development



Steady as She Goes? Three Generations of Students through the Science and Engineering Pipeline *

October 2009

B. Lindsay Lowell^a
Hal Salzman^{b,c}
Hamutal Bernstein^a
with
Everett Henderson^c

Paper presented at:
Annual Meetings of the
Association for Public Policy
Analysis and Management
Washington, D.C.

November 7, 2009

^a Institute for the Study of International Migration, Georgetown University
B. Lindsay Lowell: lowellbl@georgetown.edu

^b Heldrich Center for Workforce Development
Bloustein School of Public Policy
Rutgers University &
^c The Urban Institute
Hal Salzman: HSalzman@Rutgers.edu

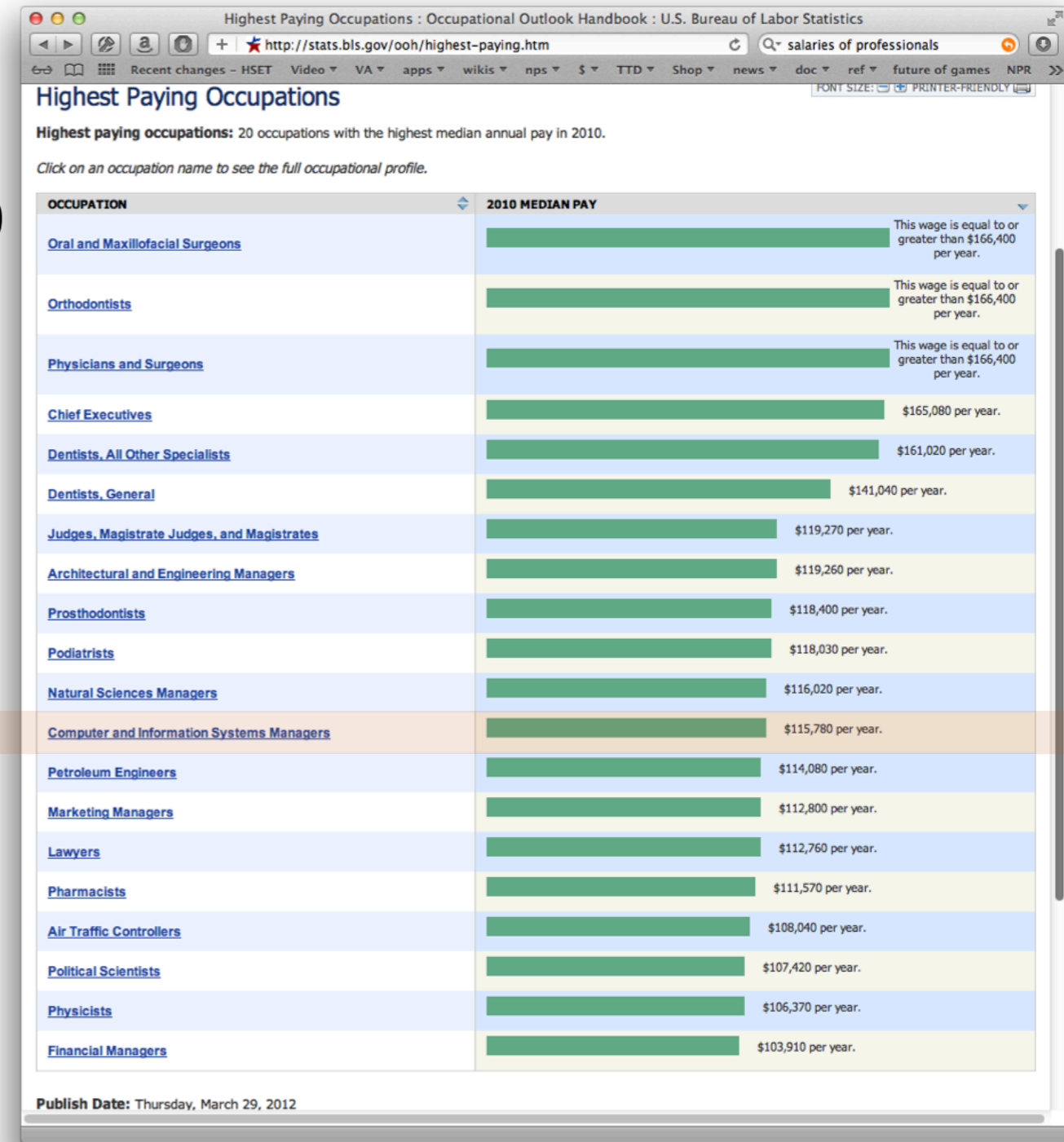
* Michael Teitelbaum provided insightful comments on an earlier draft of this paper and on the research throughout the project. We appreciatively acknowledge the contributions to this paper by Katie Vinopal of the Urban Institute. Research for this paper was funded by the Alfred P. Sloan Foundation.



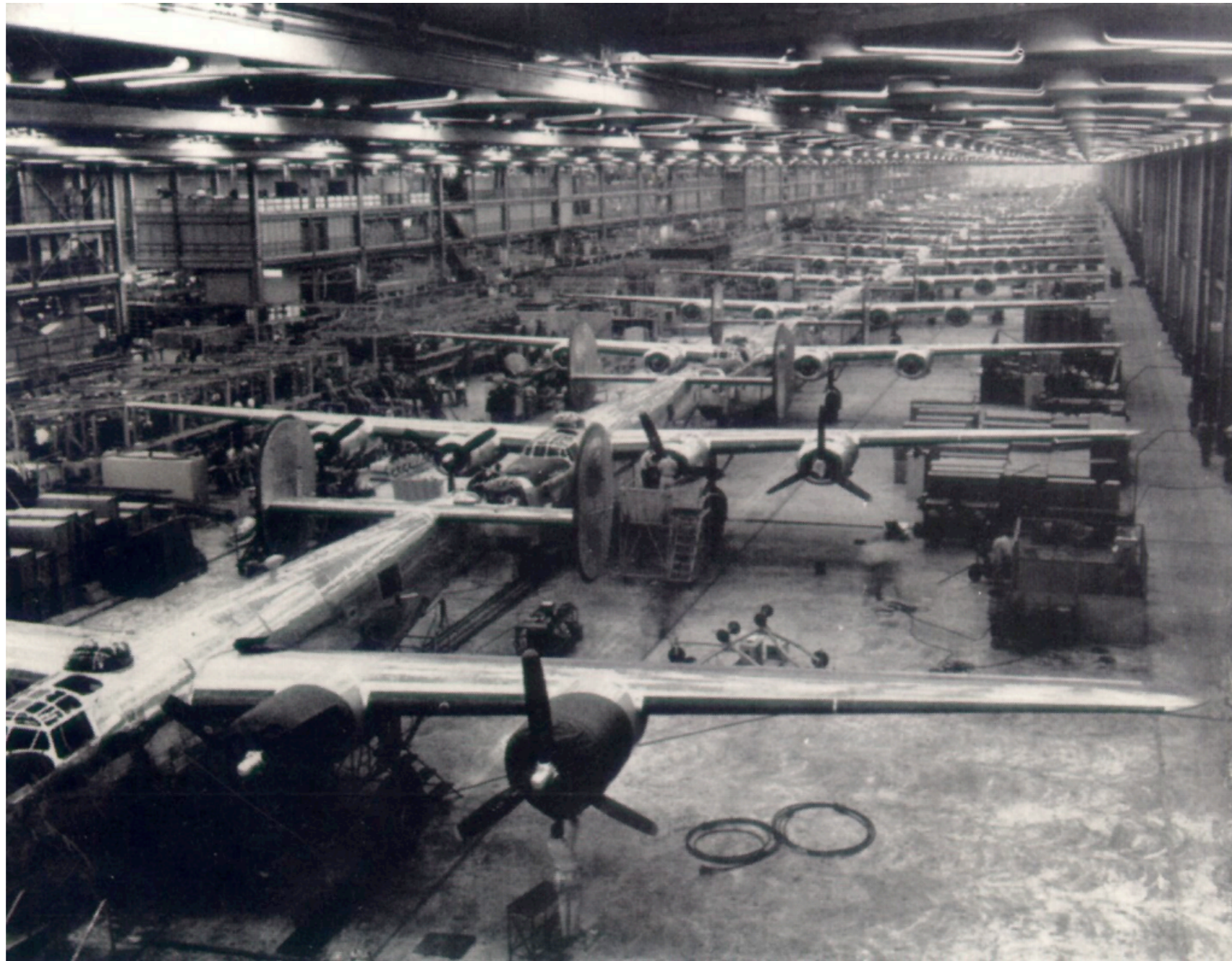
Bureau of Labor Statistics puts CS as 12th highest paying profession, after...

Highest paying occupations:

- Oral Surgeons > \$166,400
- Orthodontists > \$166,400
- Physicians and Surgeons >\$166,400
- CEOs: \$165,080
- Dentists: \$161,020
- Judges: \$119,260
- Architectural & Eng. Mgrs \$119,260
- Prosthodontists \$118,400
- Podiatrists \$118,030
- Natural Sci. Mgrs. \$116,020
- Computer Scientists: \$115,070
- Petroleum Engineers \$114,080
- Marketing Managers \$112,800
- Lawyers: \$112,760



Manufacturing policy



- US did not buy WW2 aircraft in Germany

Security problems are bad for society as a whole...

... because [wireless] computers are everywhere.

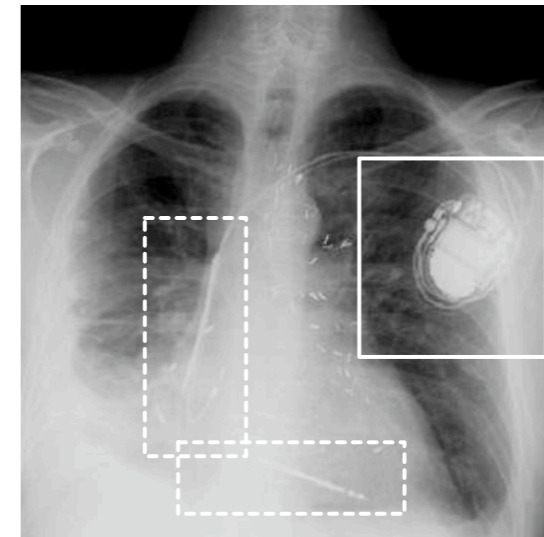


**50 microprocessors
per average car**

<http://www.autosec.org/>

- *Comprehensive Experimental Analysis of Automotive Attack Surfaces (2011)*
- *Experimental Security Analysis of a Modern Automobile (2010)*

Remote take-over of EVERY safety-critical system from ANY wired or wireless interface



2008: demonstrated wireless attack on implantable pacemakers

2012: demonstrated wireless attack on insulin pump

DDoS the endocrine system!

[ISN] TV-based botnets? DoS attacks on your fridge? More plausible than you think

From: InfoSec News <alerts@infosecnews.org>

Subject: [ISN] TV-based botnets? DoS attacks on your fridge? More plausible than you think

Date: April 23, 2012 3:16:23 AM EDT

To: isn@infosecnews.org

<http://arstechnica.com/business/news/2012/04/tv-based-botnets-ddos-attacks-on-your-fridge-more-plausible-than-you-think.ars>

By Dan Goodin
ars technica
April 22, 2012



It's still premature to say you need firewall or antivirus protection for your television set, but a duo of recently diagnosed firmware vulnerabilities in widely used TV models made by two leading manufacturers suggests the notion isn't as far-fetched as many may think.

... While poking around a Samsung D6000 model belonging to his brother, he inadvertently discovered a way to remotely send the TV into an endless restart mode that persists even after unplugging the device and turning it back on.

"It wasn't even planned," Auriemma told Ars, referring to the most damaging of his two attacks, which rendered the device useless for three days...



[ISN] ATM Attacks Exploit Lax Security

From: InfoSec News <alerts@infosecnews.org>
Subject: [ISN] ATM Attacks Exploit Lax Security
Date: April 23, 2012 3:15:54 AM EDT
To: isn@infosecnews.org

<http://www.bankinfosecurity.com/atm-attacks-exploit-lax-security-a-4689>

By Tracy Kitten
Bank Info Security
April 19, 2012

Lax security makes non-banking sites prime targets for skimming attacks...



<http://krebsonsecurity.com/2011/12/pro-grade-3d-printer-made-atm-skimmer/>



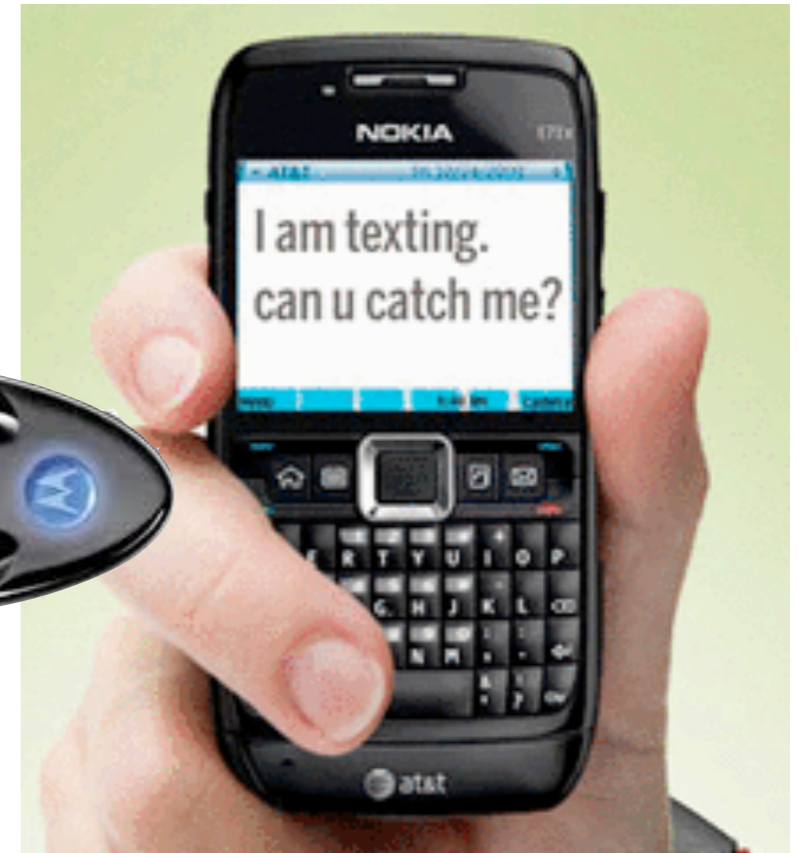
Cell phones cannot be secured.

Cell phones have:

- Wireless networks, microphone, camera, & batteries
- Downloaded apps
- Bad crypto

Cell phones can be used for:

- Tracking individuals
- Wiretapping rooms
- Personal data



<http://connectedvehicle.challenge.gov/submissions/2706-no-driving-while-texting-dwt-by-tomahawk-systems-llc>

Five DARPA & NSF cyber security PMs walk into a bar...

Major security breakthroughs since 1980:

- Public key cryptography (RSA with certificates to distribute public keys)
- Fast symmetric cryptography (AES)
- Fast public key cryptography (elliptic curves)
- Easy-to-use cryptography (SSL/TLS)
- Sandboxing (Java, C# and virtualization)
- Firewalls
- BAN logic
- Fuzzing.

But none of these breakthroughs has been a “silver bullet”

—“*Why Cryptosystems Fail*,” Ross Anderson,
1st Conference on Computer and Communications Security, 1993.
<http://www.cl.cam.ac.uk/~rja14/Papers/wcf.pdf>



There is no obvious way to secure cyberspace.

We *trust* computers...

—*but we cannot make them trustworthy.*

(A “*trusted*” system is a computer that can violate your security policy.)

We know a lot about building secure computers...

—*but we do not use this information when building and deploying them.*

We know about usable security...

—*but we can’t make any progress on usernames and passwords*

We should design with the assumption that computers will fail...

—*but it is cheaper to design without redundancy or resiliency.*

Despite the newfound attention to cyber security, our systems seem to be growing more vulnerable every year.



Be a [polite] critic of USG Information Systems

Our computers are *terrible*, but we can make them better.

Things you can do:

- Participate in contracting efforts and reviews.
- Read user agreements.
- Report bugs

Use Section 508!

- Section 508 of the Rehabilitation Act (29 USC 794 d) requires that federal government information systems accommodate people with disabilities.
- Bad typography, poor choice of fonts, use of Flash *may be illegal!*
- Speak with the Section 508 Coordinator — or volunteer to become one!

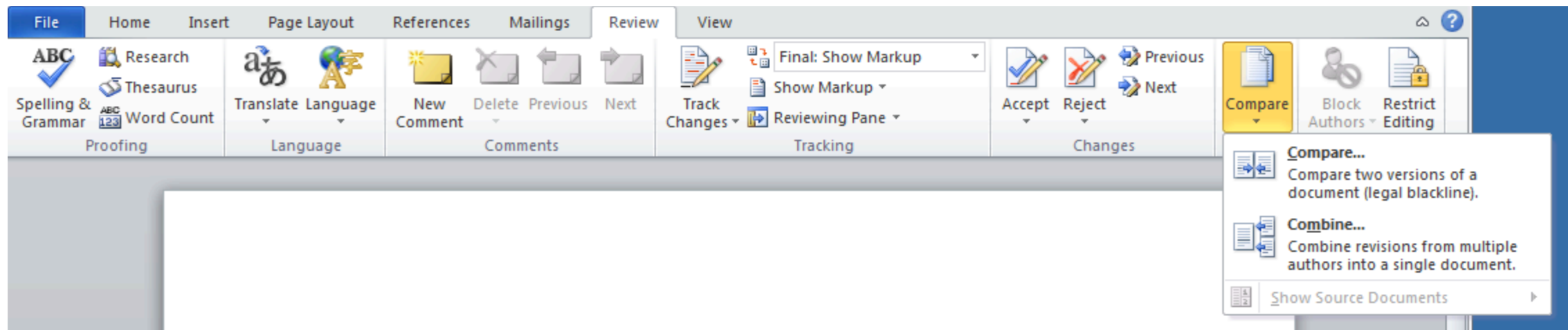


Be a helpful

We don't teach people to use Windows / Word / Excel productively.

Real live case:

- A Microsoft Word document was passed to multiple people for edits.
- I showed the admin how to “compare” and “merge” documents.



- I was a hero!

Take the time to learn:

- Microsoft Word Styles; Acrobat Forms; Excel Macros



Push an INFOSEC AGENDA that is *realistic*.

Help your agencies deploy:

- IPv6
- DNSSEC
- Modern Web Browsers

Help your agencies eliminate:

- Windows XP
- Internet Explorer 6 / 7 / 8

Ask about backups!

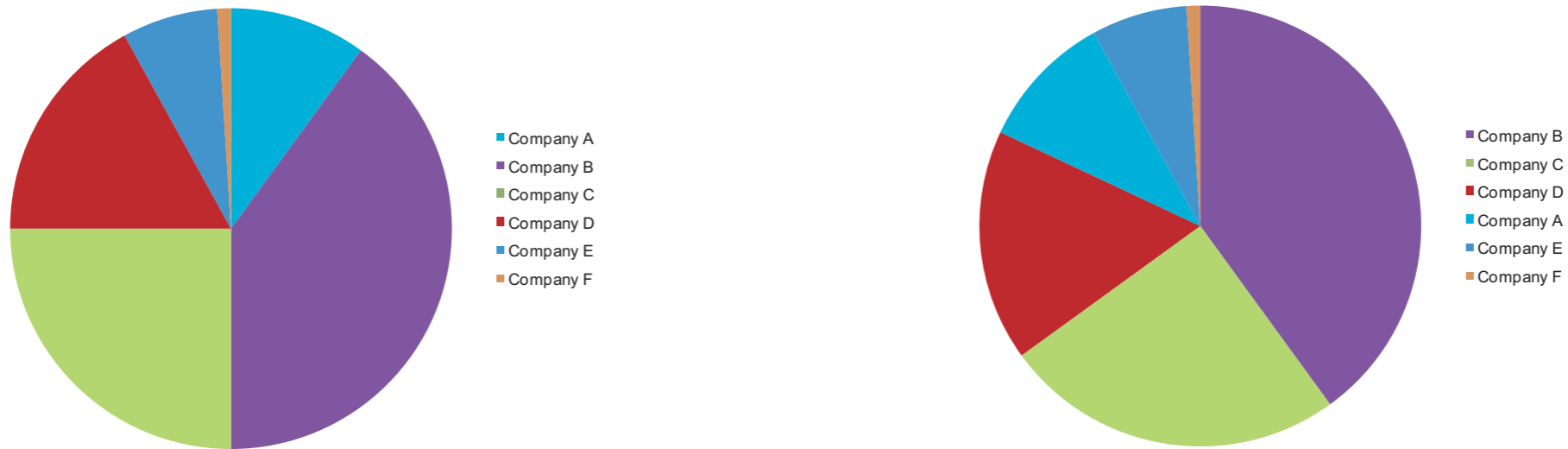
- “Delete” an important file “by accident.”
- Can your IT group get it back? ***IF NOT, REPORT IT!***

Submit bug reports!

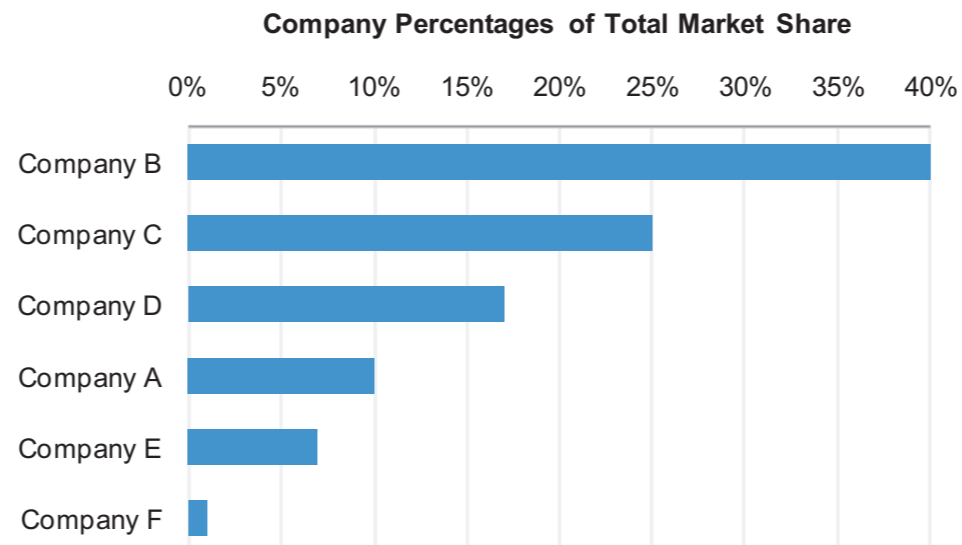


Don't use pie charts

These two pie charts present exactly the same information.



This graph presents the same information better:



—And it's Section 508 compliant!

Save the Pies for Dessert

Stephen Few, Perceptual Edge
Visual Business Intelligence Newsletter
August 2007



Other things for SFS students to know...

Continuing education is really important!

- Go to conferences
- Read journals and magazines
- Keep reading the academic literature
- Concentrate on self-development.

Find a mentor.

Stay in touch with your faculty advisor!

Algorithms matter.

Data matters

- Learn how to present data



Security problems reflect deep societal problems. We need to fix our society.

Follow the money.

IEEE Security & Privacy

Florêncio and Herley, Dec. 2012

- Emptying accounts is hard
- Mules, not victims, lose money
- Passwords are not the bottleneck
- Underground markets are not thriving
- Credential Stealing is a terrible business

Supporting slides:

— https://www.usenix.org/sites/default/files/conference/protected-files/woot_herley.pdf

Video

— <https://www.usenix.org/conference/woot12/keynote-tba> (1 hour, 25 minutes)



PASSWORDS

Is Everything We Know about Password Stealing Wrong?

Dinei Florêncio and Cormac Herley | Microsoft Research

Passwords are but one link in the cybercrime value chain. Contrary to popular belief, compromised users are made whole and thieves have a hard time monetizing stolen credentials.

It's not what you don't know that kills you, it's what you know for sure that ain't true. —Mark Twain

It is worth, at the outset, dispelling a widely held misapprehension about password stealing. Thieves certainly steal passwords, and money is certainly a large part of their motivation. However, when they successfully extract money from financial accounts, individual consumers do not pay. In the US, Federal Reserve Regulation E limits consumer liability to US\$50 in the event of fraud (this is separate from Regulation CC's \$50 limit for credit card fraud) and covers "any electronic transfer that is initiated through an electronic terminal, telephone, computer or magnetic tape."¹ This regulation governs banks, brokerages, and credit unions, and many organizations go beyond it and offer consumers a zero-liability policy.

Bank of America, for example, "guarantees zero liability for any unauthorized activity originating from Online Banking or Bill Pay."² Wells Fargo says, "We guarantee that you will be covered for 100 percent of funds removed from your Wells Fargo accounts in the unlikely event that someone you haven't authorized removes those funds through our Online Services."³ Fidelity "will reimburse your Fidelity account for any losses due to unauthorized activity,"⁴ and "under HSBC's \$0 Liability, Online Guarantee, you're covered 100% and liable for \$0."⁵ Even nontraditional financial institutions offer this guarantee. For example, in eBay's December 2009 10-K filing, the company states, "PayPal currently voluntarily reimburses consumers for all financial losses from transactions not authorized by the consumer, not just losses above \$50."⁶

Thus, in the US, individual consumers are largely insulated from the direct financial consequences of credential theft (we later briefly mention losses of small businesses and indirect losses). (Although consumer protections in the US are good, they are by no means unique. EU Directive 2007/64/EC of the European Parliament limits consumer liability to €150, and many banks go beyond this. Mannan and van Oorschot found that most major Canadian banks offer a "100% reimbursement guarantee for online banking fraud losses," but they also suggest that most consumers are unlikely to meet the standard of care required to be eligible.⁷) Consumers who have their accounts emptied through stolen credentials are made whole. Of course, the cost of the fraud does not just go away: covering fraud is a cost that gets passed back to consumers in the form of increased fees. However, the idea that consumers are "just a few clicks away" from having their accounts irretrievably emptied is simply incorrect. There is a world of difference between being personally liable for losses and sharing losses that are diluted across the whole population. Although "we all pay for cybercrime" is true in a general sense, individual users do not face grave financial risk.

We begin with this misconception because it is widely held and generates enormous confusion. Regulation

1540-7993/12/S31.00 © 2012 IEEE Copublished by the IEEE Computer and Reliability Societies November/December 2012 63

We need to build a society that values computing.

K-12 Education that:

- Integrates data, communications & computation across the curricula
- Graduating programmers should have 10 years' experience before writing code that can steal you credit card numbers!

Recovery Oriented Computing — backups that are:

- Trustworthy — (digital signatures)
- Multiple tiers — Online / Offline / Disconnected / Geographically Remote
- Durable — years / decades
- Organized — so information can be found

Policies that accomplish their stated goals.

- 16 character passwords are no more secure than 12 character passwords

S





Backup Slides