



# The Cybersecurity Mess

Simson L. Garfinkel

Associate Professor, Naval Postgraduate School

January 11, 2013

## DISCLAIMER:

"It will get on all your disks. It will infiltrate your chips.  
Yes it's Cloner! It will stick to you like glue.  
It will modify RAM too. Send in the Cloner!"

# NPS is the Navy's Research University.

Monterey, CA — 1500 students

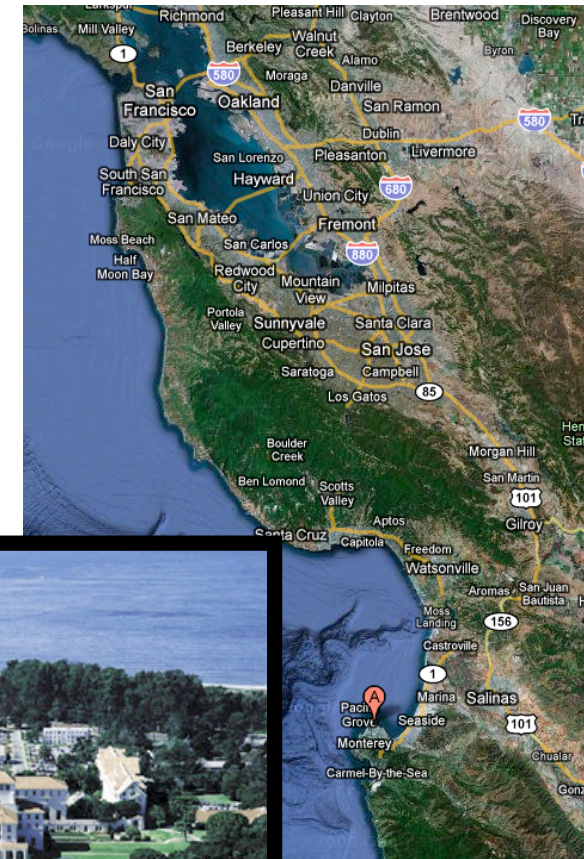
- US Military & Civilian (Scholarship for Service & SMART)
- Foreign Military (30 countries)

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 Cybersecurity Risk”, *Communications of the ACM*, June 2012, 55(6)

V

viewpoints

DOI:10.1145/2184318.2184318

Simon L. Garfinkel

Inside Risks

The Cybersecurity Risk

Increased attention to cybersecurity has not resulted in improved cybersecurity.

**T**he 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 secure 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 all the while.

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 vulnerable. 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.

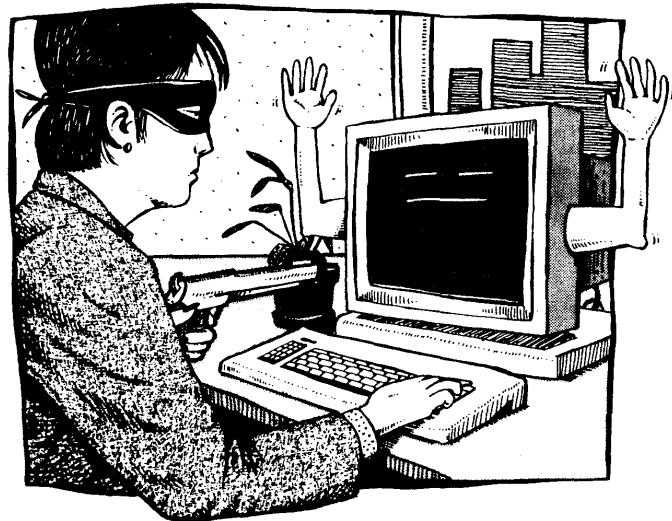
**Views of Cybersecurity**

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

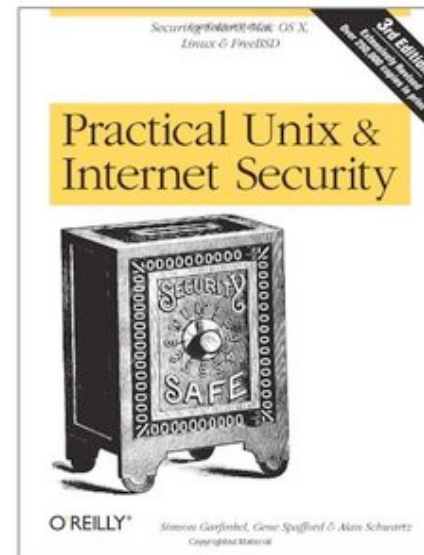
"Spies," "vandals," and "crackers" are out there,  
waiting to get into—or destroy—your databases.

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

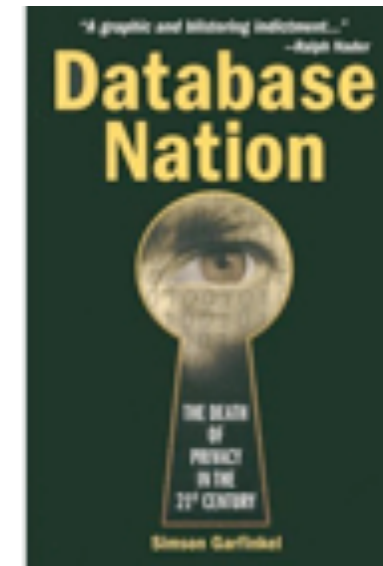
Lawyers today must automatically recognize insecure computer systems and lax operating procedures in the same way as lawyers now recognize

39

Sept. 1987



1991



2000



2006



2006

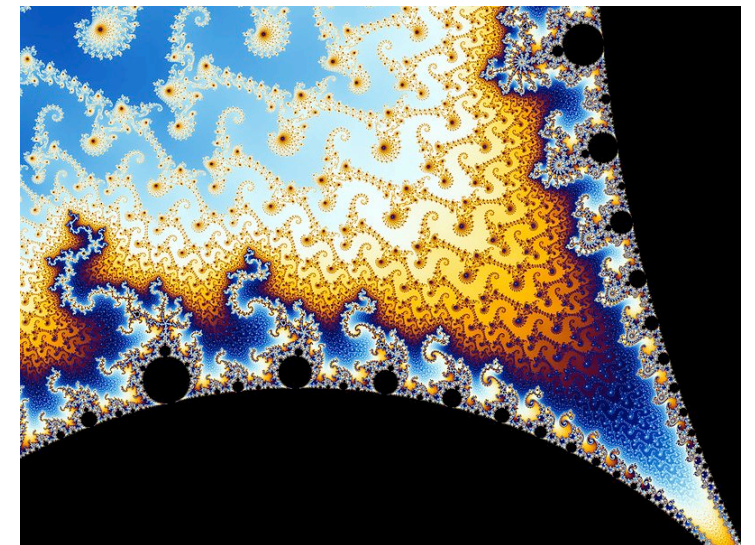
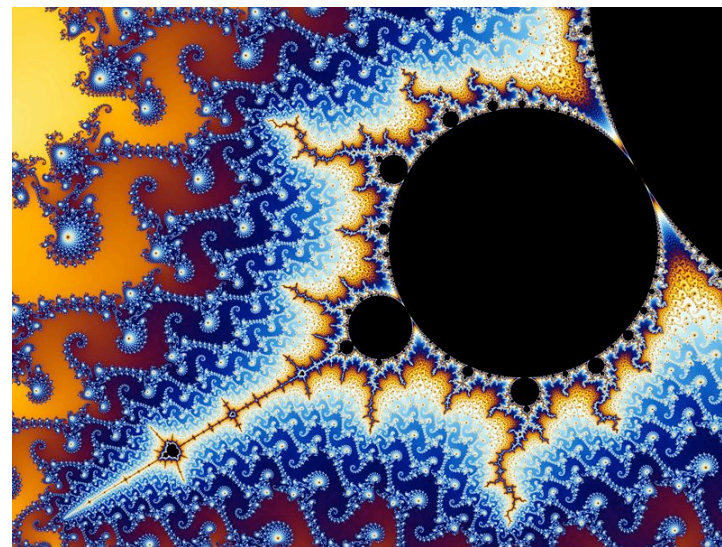
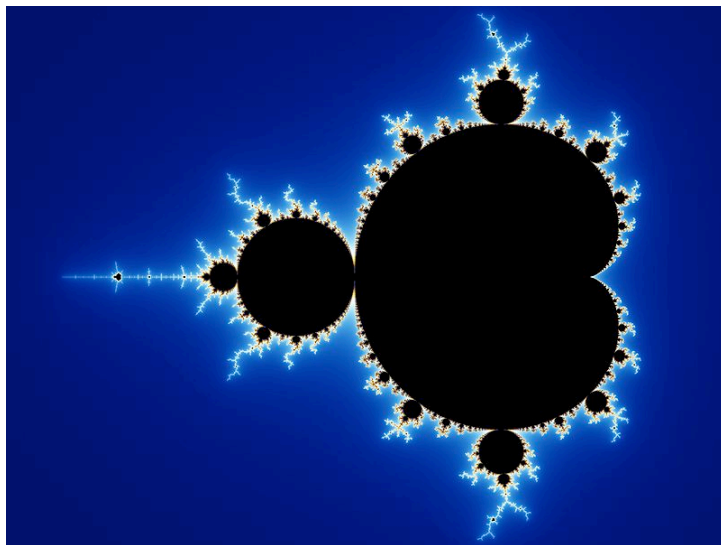
...and I have given up!



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

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

- Computers are more complex — more places to attack them.
- There are multiple ways around each defense.
- It's easier to attack systems than defend them.
- It's easier to break things than to fix them.



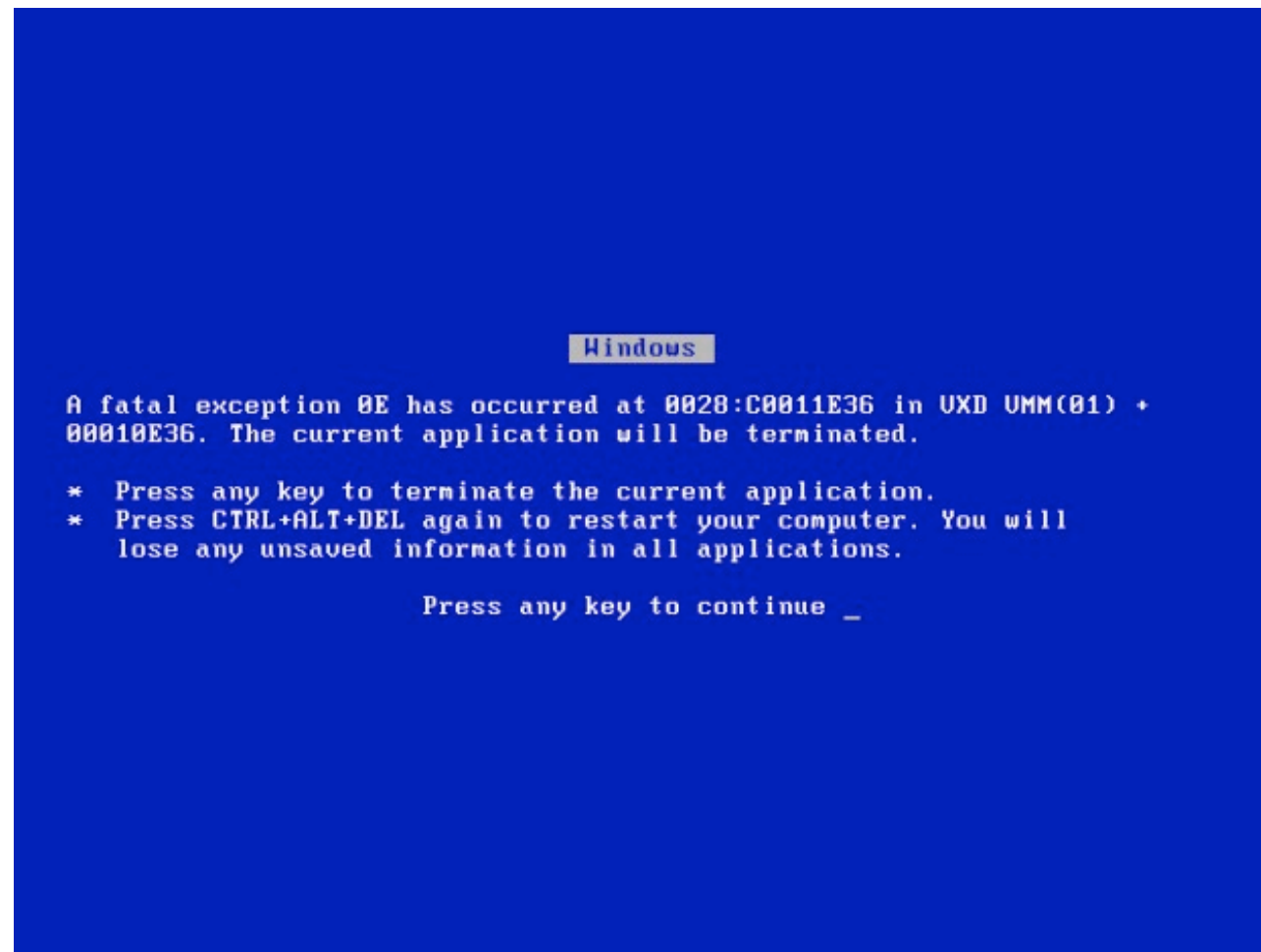
### Windows

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 \_

# We expect computers to crash...



... expect them to be hacked.



I start every day with...

# [ISN] Internet Security News

# [ISN] — infosecnews.org

Inbox — Gmail (32 messages, 7 unread)

Delete Junk Reply Reply All Forward Get Mail Reply Forward Archive Flag Search

Flagged

From	To	Subject	Date Received
InfoSec News	isn@infosecnews.org	[ISN] Former UNL student accused...	Today 3:19 AM
InfoSec News	isn@infosecnews.org	[ISN] Hacker uses cat to deliver viru...	Today 3:20 AM
InfoSec News	isn@infosecnews.org	[ISN] Secret footsoldier targeting ba...	Today 3:21 AM
InfoSec News	isn@infosecnews.org	[ISN] Romanian Hacker Gets 21-Mo...	Today 3:23 AM
InfoSec News	isn@infosecnews.org	[ISN] Ransom, implant attack highli...	Today 3:24 AM

---

**InfoSec News** January 9, 2013 3:19 AM  
To: isn@infosecnews.org  
[ISN] Former UNL student accused of hacking NeSIS will face trial

---

[http://www.dailynebraskan.com/news/article\\_6d15f3d6-5a1a-11e2-a4d4-0019bb30f31a.html](http://www.dailynebraskan.com/news/article_6d15f3d6-5a1a-11e2-a4d4-0019bb30f31a.html)

By Lis Arneson  
Daily Nebraskan  
January 9, 2013

The case against a former University of Nebraska-Lincoln student accused of hacking into the University of Nebraska's Nebraska Student Information System on May 23 will head to trial.

Daniel Stratman, 22, refused to enter a plea during his arraignment Tuesday afternoon before U.S. Magistrate Judge Cheryl Zwart. As a result, the district court entered a plea of not guilty.

The U.S. Attorneys' Office filed charges against Stratman on Dec. 6.

In court documents, Assistant U.S. Attorney Steven Russell said that between April 24 and May 24, Stratman intentionally accessed a protected computer without authorization, which resulted in reckless damage. The charge claims that Stratman's conduct caused a loss of at least \$5,000.

[...]

---

Visit the InfoSec News Security Bookstore  
Best Selling Security Books and More!  
<http://www.shopinfosecnews.org>

# [ISN] Secret foot soldier targeting banks reveals meaner, leaner face of DDos

From	To	Subject	Date Received
InfoSec News	isn@infosecnews.org	[ISN] Former UNL student accused...	Today 3:19 AM
InfoSec News	isn@infosecnews.org	[ISN] Hacker uses cat to deliver viru...	Today 3:20 AM
InfoSec News	isn@infosecnews.org	[ISN] Secret footsoldier targeting ba...	Today 3:21 AM
InfoSec News	isn@infosecnews.org	[ISN] Romanian Hacker Gets 21-Mo...	Today 3:23 AM
InfoSec News	isn@infosecnews.org	[ISN] Ransom, implant attack highli...	Today 3:24 AM

## InfoSec News

January 9, 2013 3:21 AM

To: isn@infosecnews.org

[ISN] Secret footsoldier targeting banks reveals meaner, leaner face of DDos

<http://arstechnica.com/security/2013/01/secret-footsoldier-targeting-banks-reveals-meaner-leaner-face-of-ddos/>

By Dan Goodin  
Ars Technica  
Jan 8 2013

Over the past two weeks, a new wave of Web attacks has battered major US banks, causing disruptions for many of their online services. Now, an Israel-based security firm has uncovered one of the secret footsoldiers behind the mass assault: a compromised website that was rigged to unleash a torrent of junk traffic on three of the world's biggest financial institutions.

The discovery by Web application security firm Incapsula helps explain the strategy behind the four-month-old campaign, which has been carried out under the flag of a group calling itself Izz ad-Din al-Qassam—rather than compromise and recruit thousands or tens of thousands of end-user PCs to carry out the distributed denial-of-service attacks, why not target a handful of Web servers that have orders of magnitude more bandwidth and processing power?

Over the weekend, Incapsula researchers noticed a general-interest website located in the UK that was exhibiting suspicious behavior. They quickly discovered a backdoor that had been planted on it that was programmed to receive instructions from remote attackers. An analysis showed the website, which had just recently contracted with Incapsula, was being directed to send a flood of HTTP and UDP packets to major banks including PNC Financial Services, HSBC, and Fifth Third Bank.

"Since the commands were blocked by our service the attack was mitigated even before it started, so we can't be absolutely sure about the scope of damage this attack would cause," Incapsula Security Analyst Ronen Atias wrote in a blog post published Tuesday. "Still, it is safe to assume that it would be enough to seriously harm an average medium-sized website."

[...]

Visit the InfoSec News Security Bookstore  
Best Selling Security Books and More!  
<http://www.shopinfosecnews.org>





# [ISN] Ransom, implant attack highlight need for healthcare security

From	To	Subject	Date Received
InfoSec News	isn@infosecnews.org	[ISN] Former UNL student accused...	Today 3:19 AM
InfoSec News	isn@infosecnews.org	[ISN] Hacker uses cat to deliver viru...	Today 3:20 AM
InfoSec News	isn@infosecnews.org	[ISN] Secret footsoldier targeting ba...	Today 3:21 AM
InfoSec News	isn@infosecnews.org	[ISN] Romanian Hacker Gets 21-Mo...	Today 3:23 AM
InfoSec News	isn@infosecnews.org	[ISN] Ransom, implant attack highli...	Today 3:24 AM

## InfoSec News

January 9, 2013 3:24 AM

To: isn@infosecnews.org

[ISN] Ransom, implant attack highlight need for healthcare security

<http://www.csoonline.com/article/725880/ransom-implant-attack-highlight-need-for-healthcare-security>

By Taylor Armerding

CSO

January 08, 2013

All healthcare data breaches are not equal.

They're all bad, and reaching epidemic levels. The Department of Health and Human Services, found that Protected Health Information (PHI) breaches nearly doubled from 2010 to 2011. The DHS has reported 525 breaches of 500 or more records, involving 21.4 individuals over the past three years, according to a report by Daniel Berger.

But the raw numbers are only a piece of the story. Gienna Shaw, editor of FierceHealthIT, wrote in a post this week: "It's not the numbers that interest me most. It's the stories behind them," she wrote. "And there are so many stories ..."

One involved the Surgeons of Lake County, a small medical practice in Libertyville, Ill. Hackers broke into the system last summer, gained access to the names, addresses, Social Security numbers, credit card numbers and some medical information on more than 7,000 patients, then encrypted all the information and demanded a ransom.

Another involved medical students creating fake identities so they could post patient information on Facebook and other social media sites. A third involved malware infecting hospital equipment.

[...]

Visit the InfoSec News Security Bookstore

Best Selling Security Books and More!

<http://www.shopinfosecnews.org>



# The cybersecurity 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 cybersecurity mess.

- Education & career paths
- Immigration
- Manufacturing policy

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



What do we ~~know~~  
think about  
cybersecurity today?



# Cybersecurity is expensive.

Global cybersecurity spending: \$60 billion in 2011

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

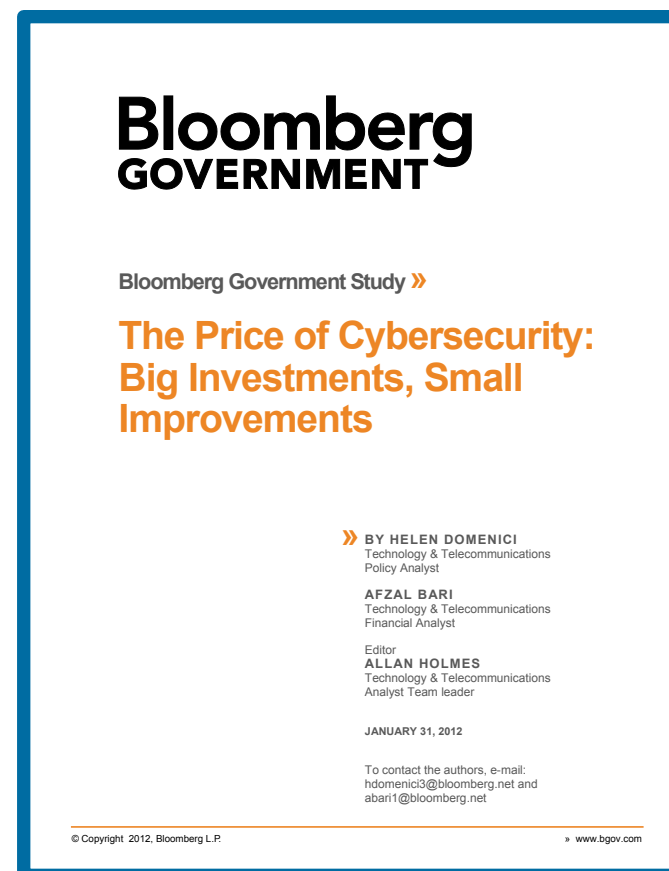
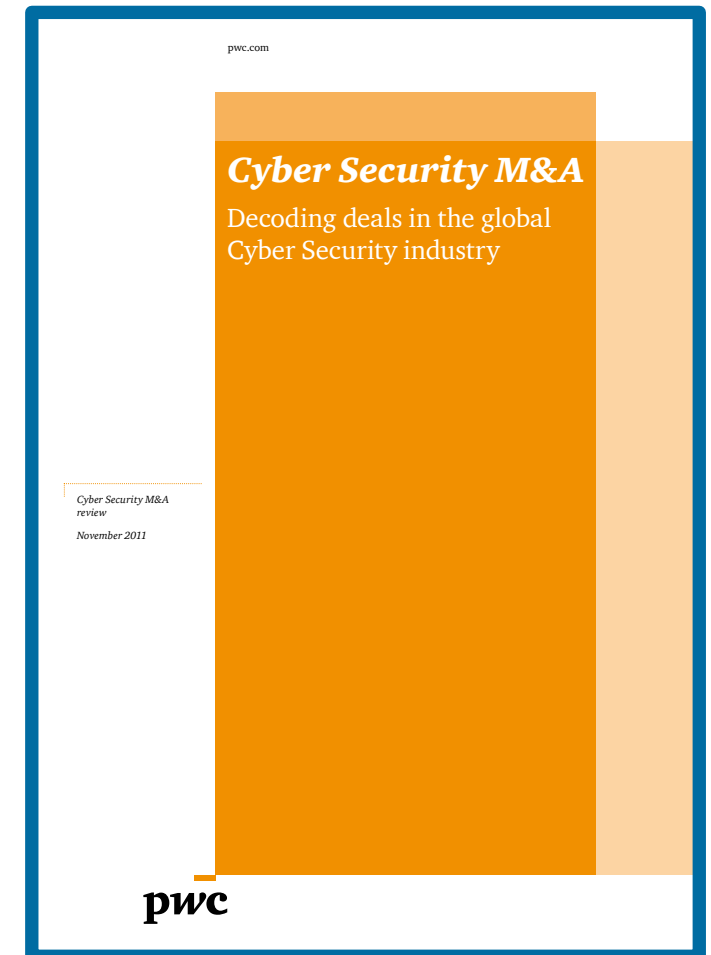
172 Fortune 500 companies surveyed:

- Spending \$5.3 billion per year on cybersecurity.
- 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.



# Cybersecurity... is undefined.

There is no good definition for “cybersecurity”

- Preventing computers from being “hacked”
- Using “network security” to secure desktops & servers
- ~~Something having to do with cybernetics~~



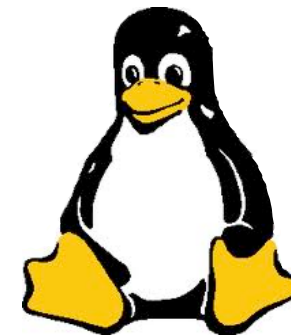
**Norbert  
Weiner**



**William  
Gibson**

There is no way to *measure* cybersecurity

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



# We do know one thing about cybersecurity...

Does spending more money make a computer more secure?



# Cybersecurity 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



# Cybersecurity 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**

# Cybersecurity 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.”

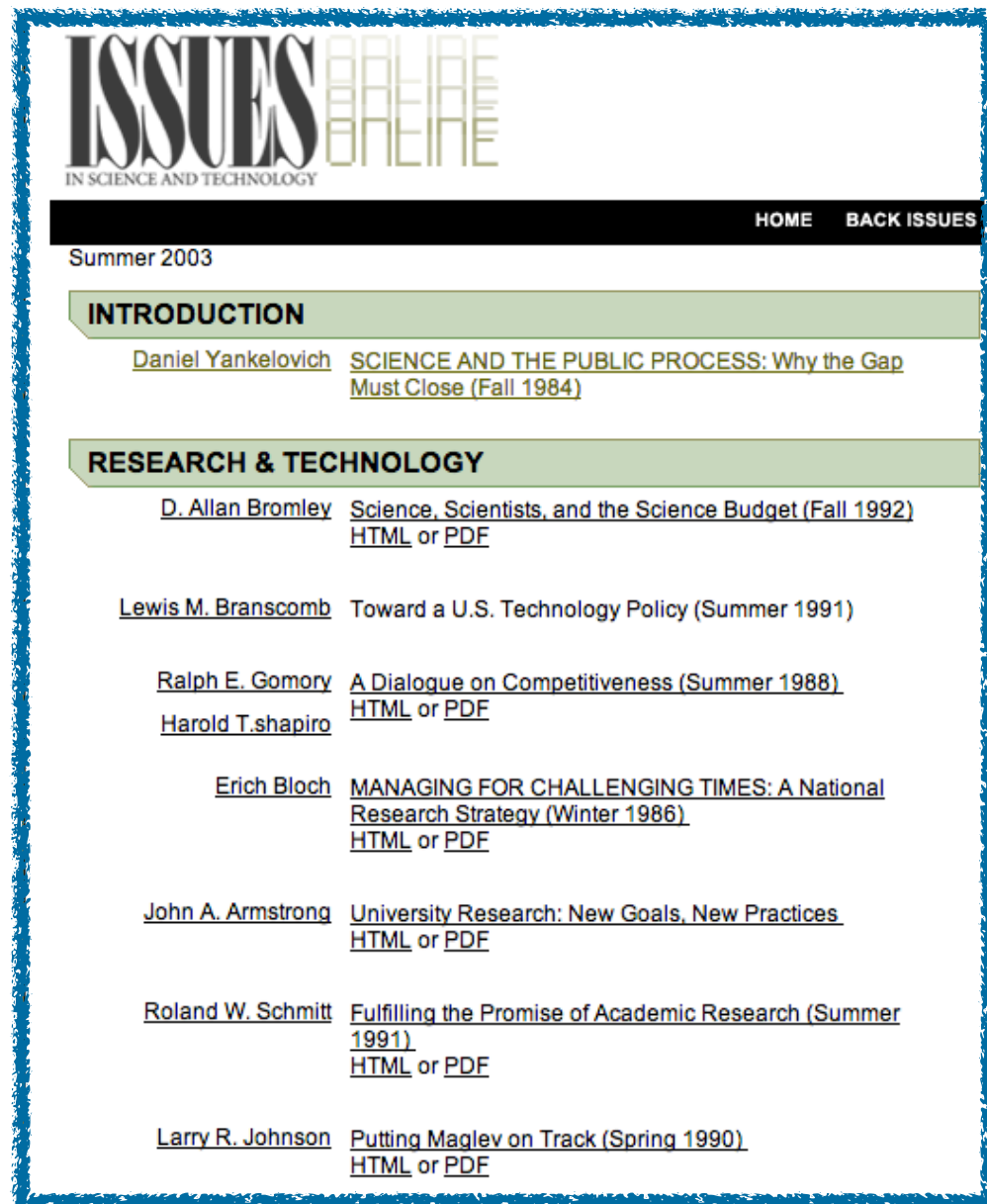


<http://www.nytimes.com/2011/06/30/technology/30morris.html>

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 ONLINE  
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](#)

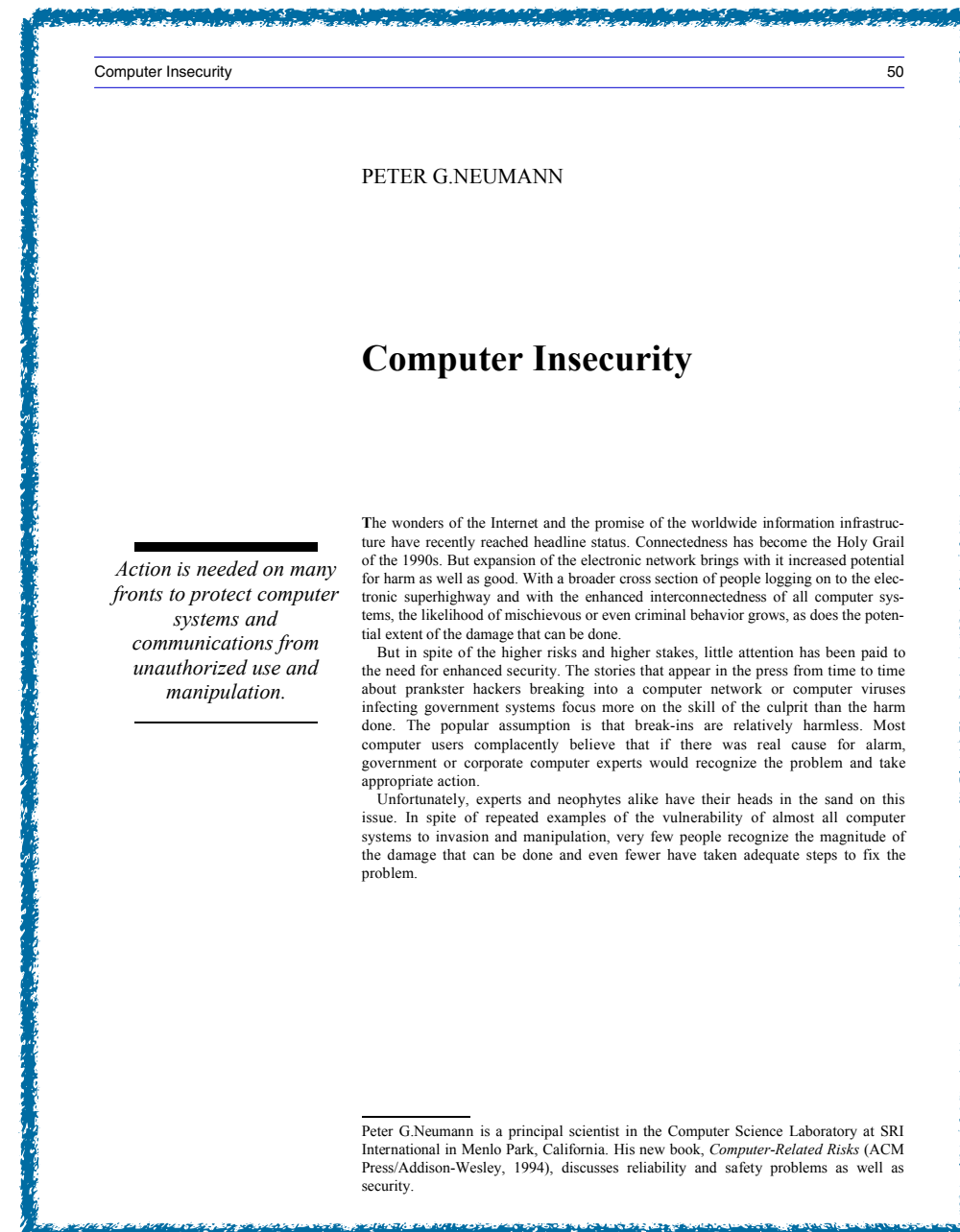
[Harold T. Shapiro](#)

[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](#)



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.html>

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

# “Yellow Dots”

October 16, 2005

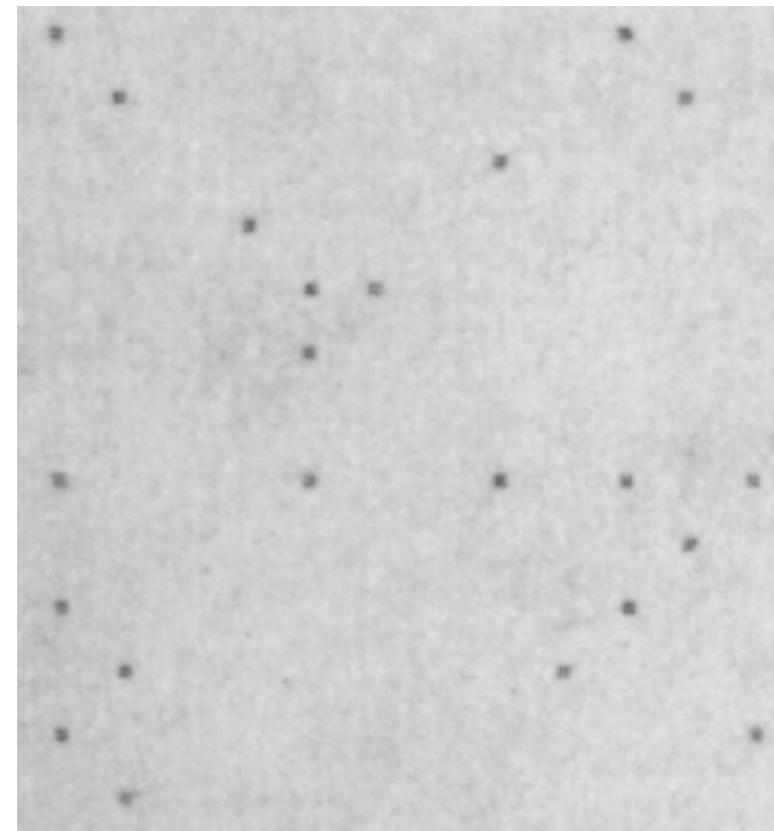
## Secret Code in Color Printers Lets Government Track You

### 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**



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

<http://seeingyellow.com/>



# Cybersecurity 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 ?

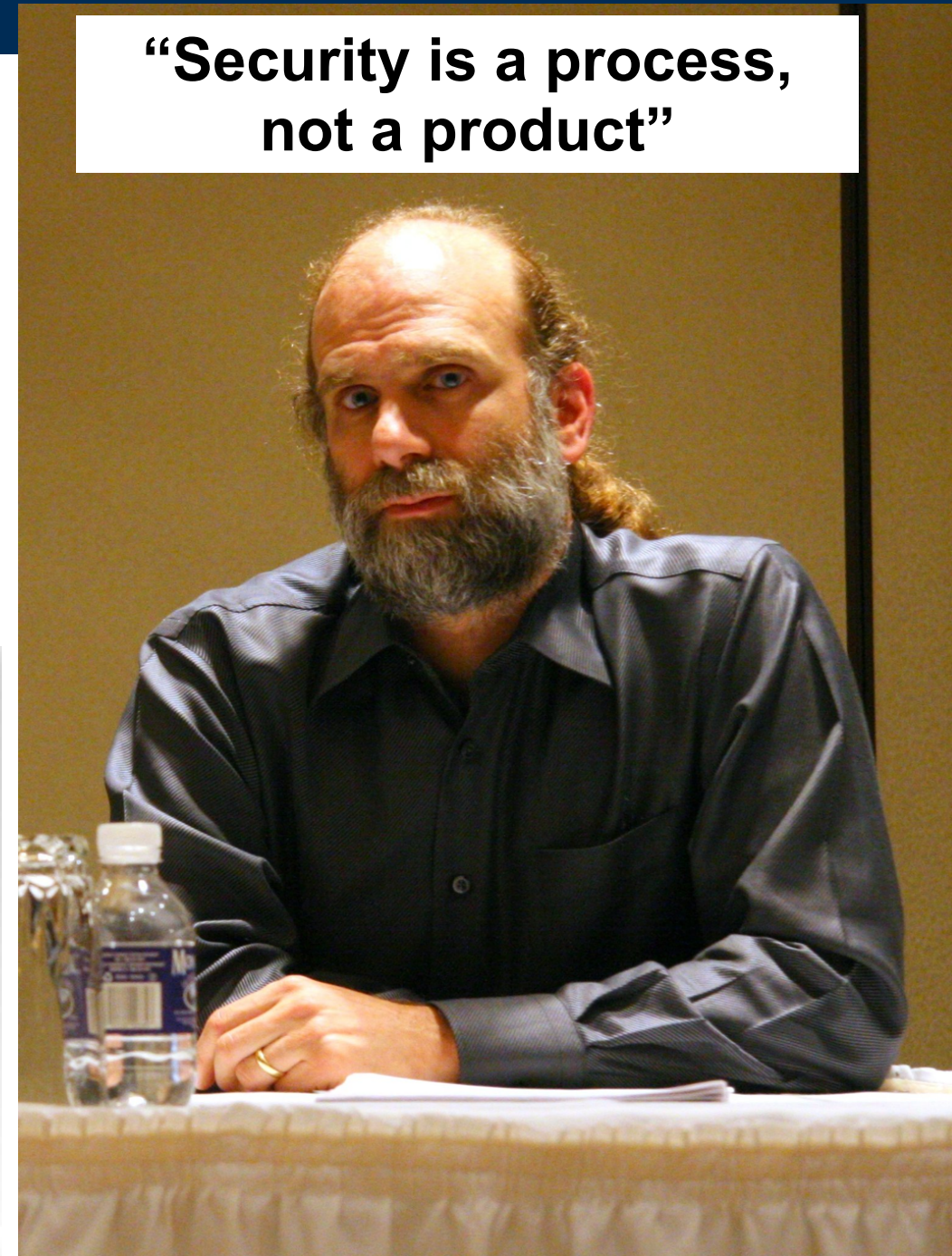
The Security Development Lifecycle (SDL) is a software development security assurance process consisting of security practices grouped by seven phases: training, requirements, design, implementation, verification, release, and response.



"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](http://en.wikipedia.org/wiki/File:Bruce_Schneier_1.jpg)

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



# nakedsecurity

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

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



search articles

142

Like

4

+1

120

Tweet

14

Share

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

you@example.com

Do it!

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



Naked Security  
from Sophos on  
Facebook

Like

204,458

## 2013 Security Threat Report

Straight from our labs to your brain



Popular

Recent

Related



Microsoft wants to hear about your Android malware problems.. so it can promote Windows Phones

Microsoft warns of

# Cybersecurity 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*



# Cybersecurity is a “wicked problem”

There is no clear definition of the wicked problem

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

There is no “stopping rule”

- *The problem can never be solved.*

Solutions are 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>*



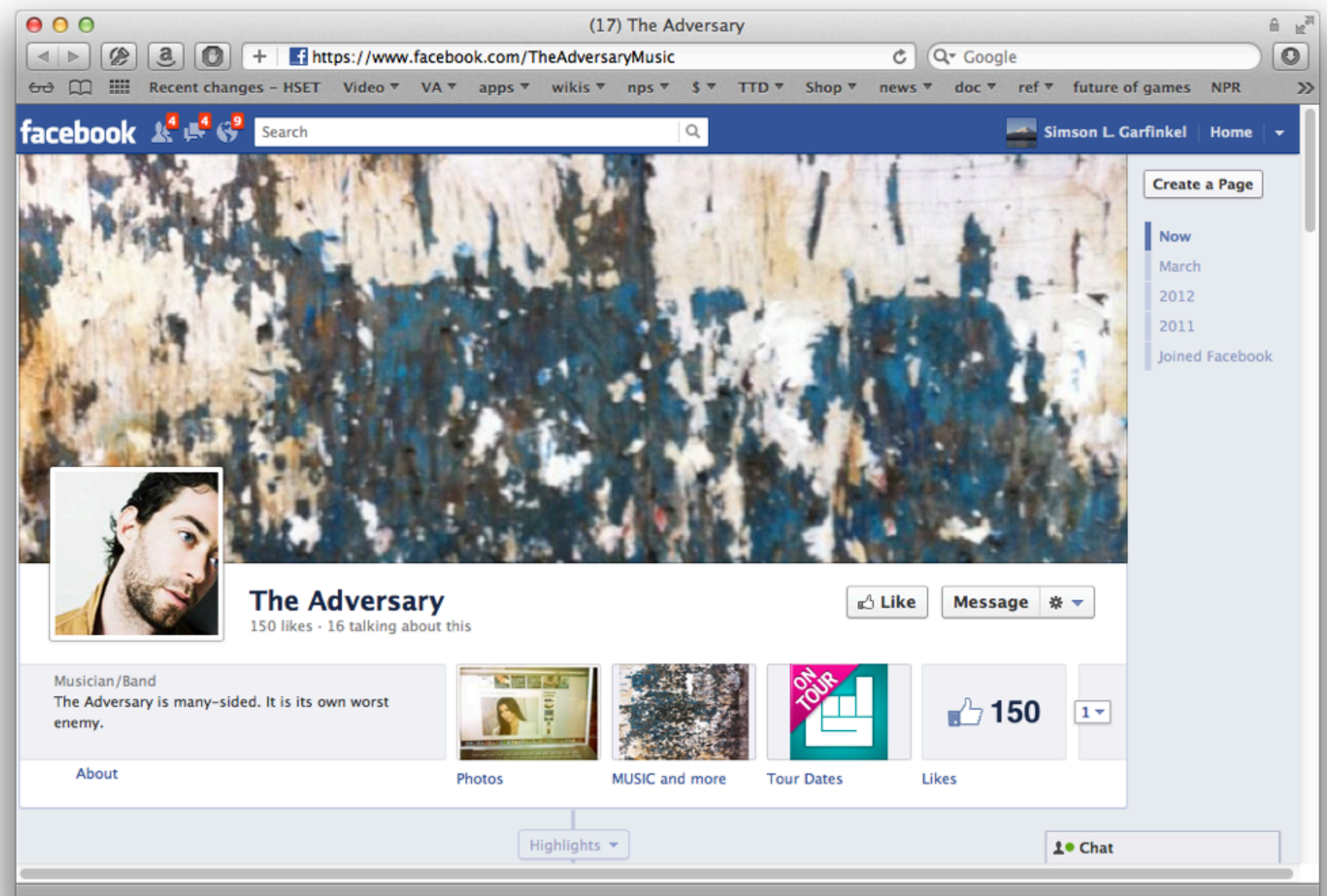
Why is  
cybersecurity  
so hard?



# Cybersecurity 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.*



US-CERT Vulnerability Note VU#162289 – C compilers may silently discard some wraparound checks

http://www.kb.cert.org/vuls/id/162289

US-CERT  
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

DATABASE HOME SEARCH REPORT A VULNERABILITY HELP

### Vulnerability Note VU#162289

#### C compilers may silently discard some wraparound checks

Original Release date: 04 Apr 2008 | Last revised: 08 Oct 2008

Print Tweet Send Share

#### Overview

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.

#### Description

In the C language, given the following types:

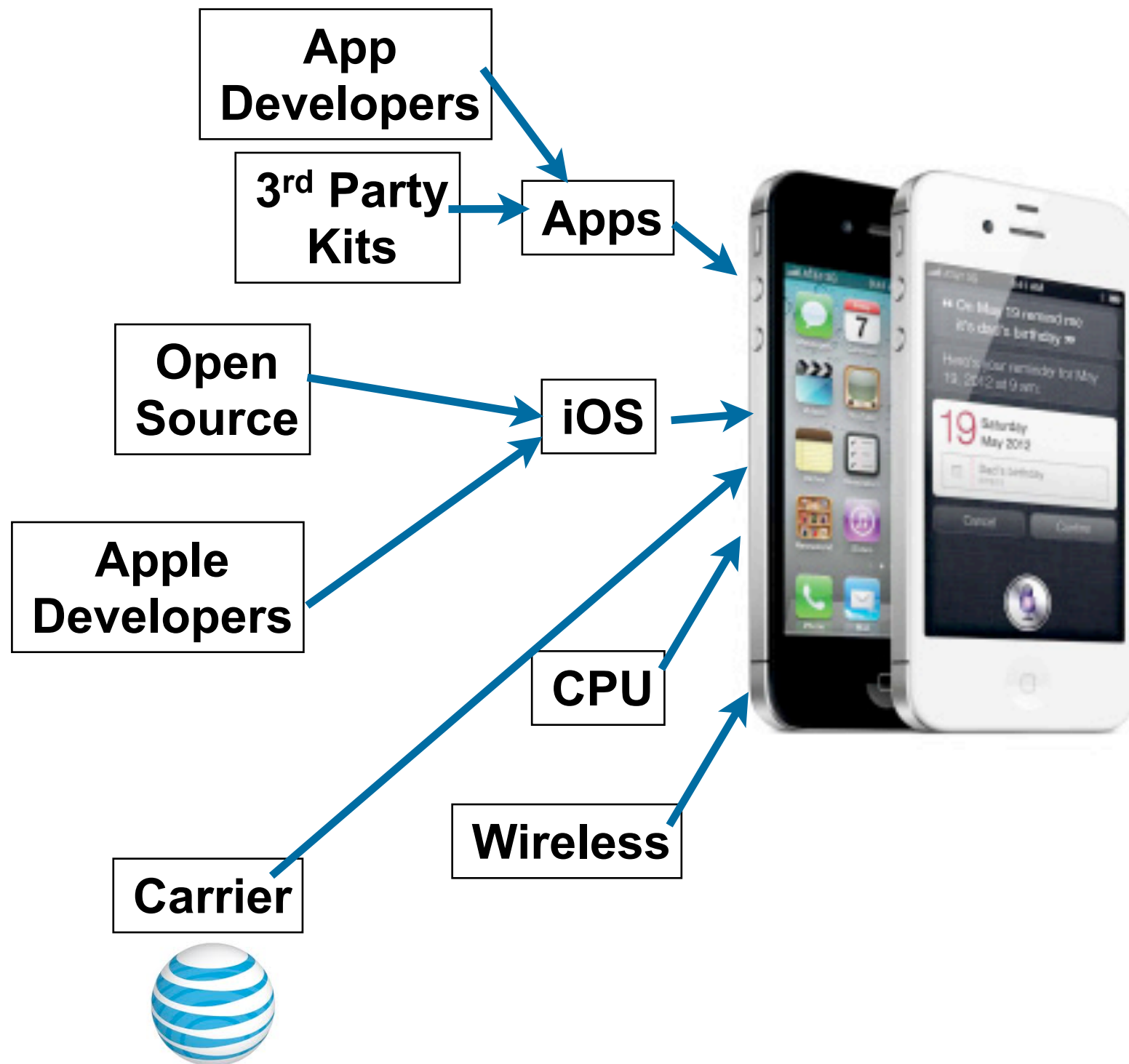
```
char *buf;  
int len;
```

some C compilers will assume that `buf+len >= buf`. As a result, code that performs wrapping checks similar to the following:

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

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.

# The supply chain creates numerous security vulnerabilities





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

## ACComplix: Location Inference using Accelerometers on Smartphones

Jun Han, Emmanuel Owusu, Le T. Nguyen, Adrian Perrig, Joy Zhang  
{junhan, owusu, 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 have 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

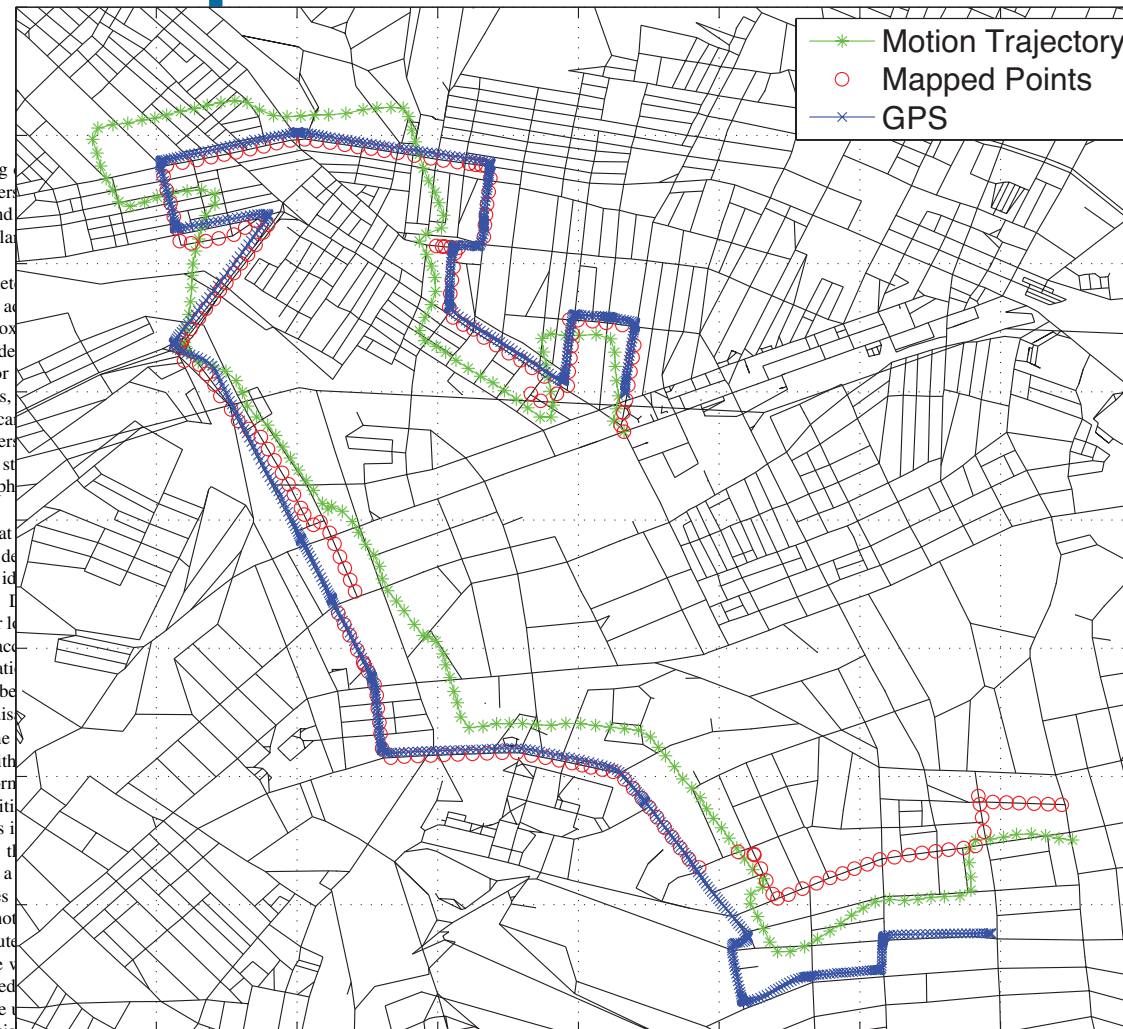
Accelerometers are a particularly interesting device in a large assortment of personal devices including tablet PCs, MP3 players, and other devices. This array of devices provides a large spyware to exploit.

Furthermore, by correlating the accelerometer between multiple phones it is possible for an attacker to determine whether the phones are in close proximity. Phones undergoing similar motions can be identified, events such as earthquakes or activities like public transportation (e.g., bus, train) produce identifiable motion signatures that can be used with other users. As a consequence, if one person's location is exposed, or exposes their cellular or Wi-Fi base station, the adversary has access to these devices.

*a) Contributions:* Our key insight is that by correlating the accelerometer between multiple phones it is possible for an attacker to enable the identification of one's location despite 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 for location-based services on the device are disabled.

*b) Threat Model:* We assume that the attacker 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 to download; e.g., a video game. In the case of a successful download, the application would be needed to upload high scores or advertisements. We assume that the OS is not compromised so that the malicious application simply executes as a legitimate application. 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



**3 accelerometers  
no privacy**

[https://sparrow.ece.cmu.edu/group/pub/han\\_ACComplix\\_comsnets12.pdf](https://sparrow.ece.cmu.edu/group/pub/han_ACComplix_comsnets12.pdf)

Jun Han, Emmanuel Owusu, Thanh-Le Nguyen, Adrian Perrig, and Joy Zhang  
"ACComplix: 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 cybersecurity problems... ... but we don't use them.

30% of the computers on the Internet run Windows XP

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



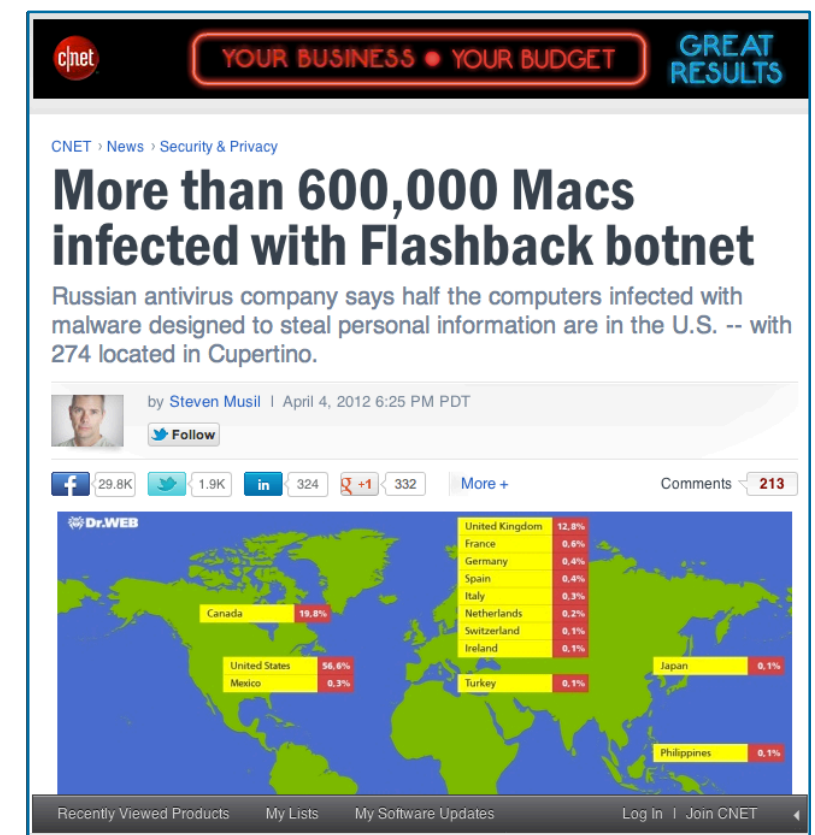
Apple users don't use anti-virus.

- Yes, Apple tries to fix bugs, but

Most “SSL” websites only use it for logging in.

DNSSEC

Smart Cards



# Many people liken cybersecurity to the flu.

## DHS calls for “cyber hygiene”

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

— “STOP, THINK, CONNECT”





# A better disease 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.*

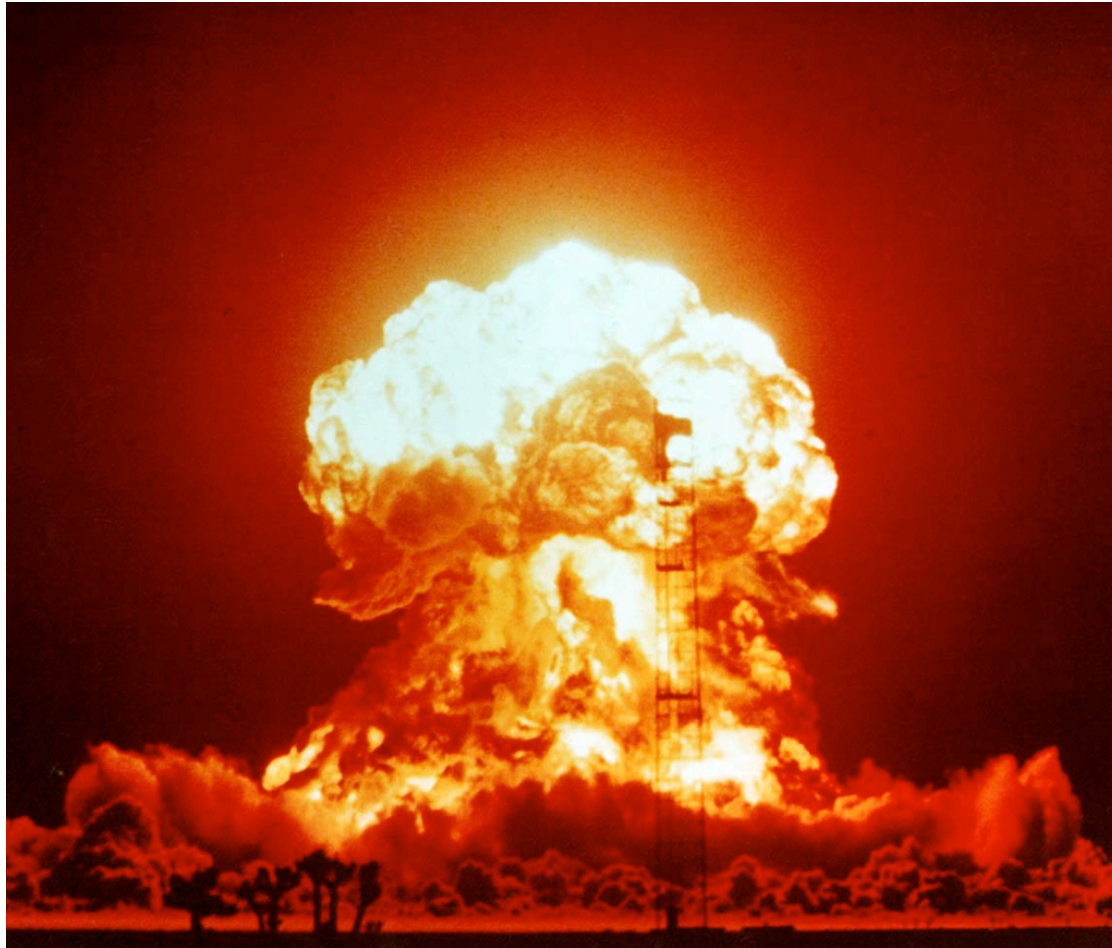
## Lax security is also good business:

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





# Many people say that cyber war is like nuclear war.



[http://www.acus.org/new\\_atlanticist/mind-cyber-gap-deterrence-cyberspace](http://www.acus.org/new_atlanticist/mind-cyber-gap-deterrence-cyberspace)

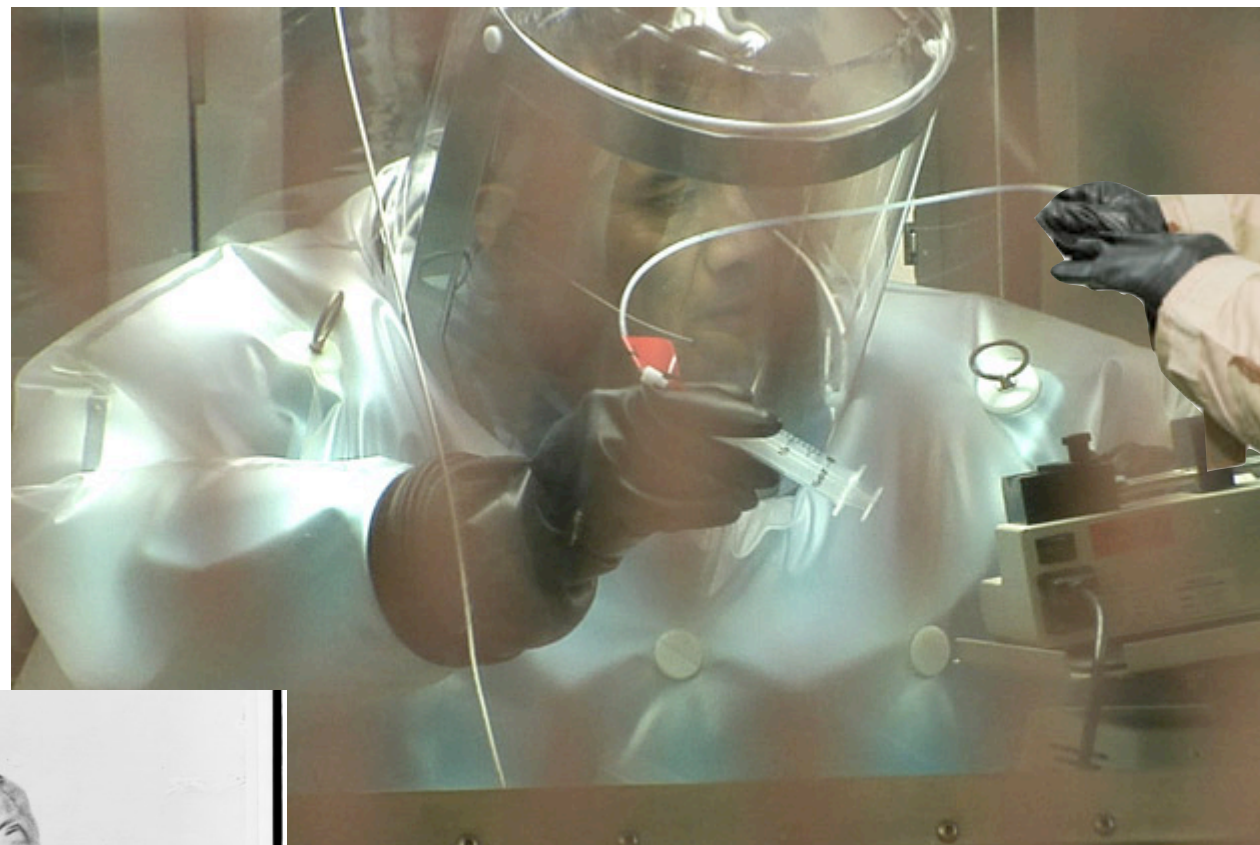


<http://www.beyondnuclear.org/security/>



# Biowar is a better model for cyberwar.

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





# Non-technical factors impact cybersecurity.

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 cybersecurity mess requires solving these issues

# Short development cycles

## Insufficient planning:

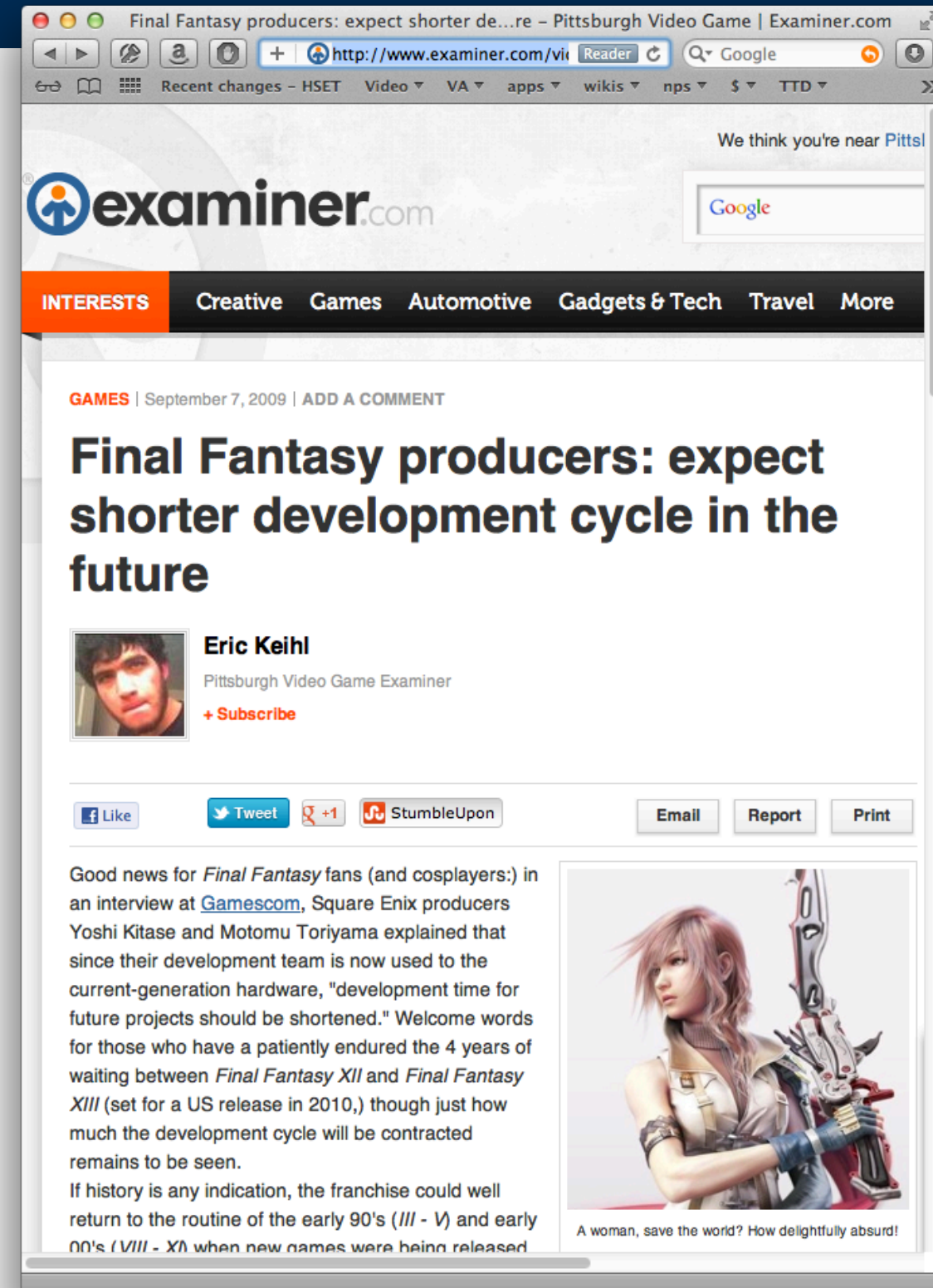
- Security not “baked in” to most products.
- Few or no security reviews
- Little Usable Security

## 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



# Education is not supplying enough security engineers

Students are not pursuing CS in high school & college

Those going into CS are not pursuing security

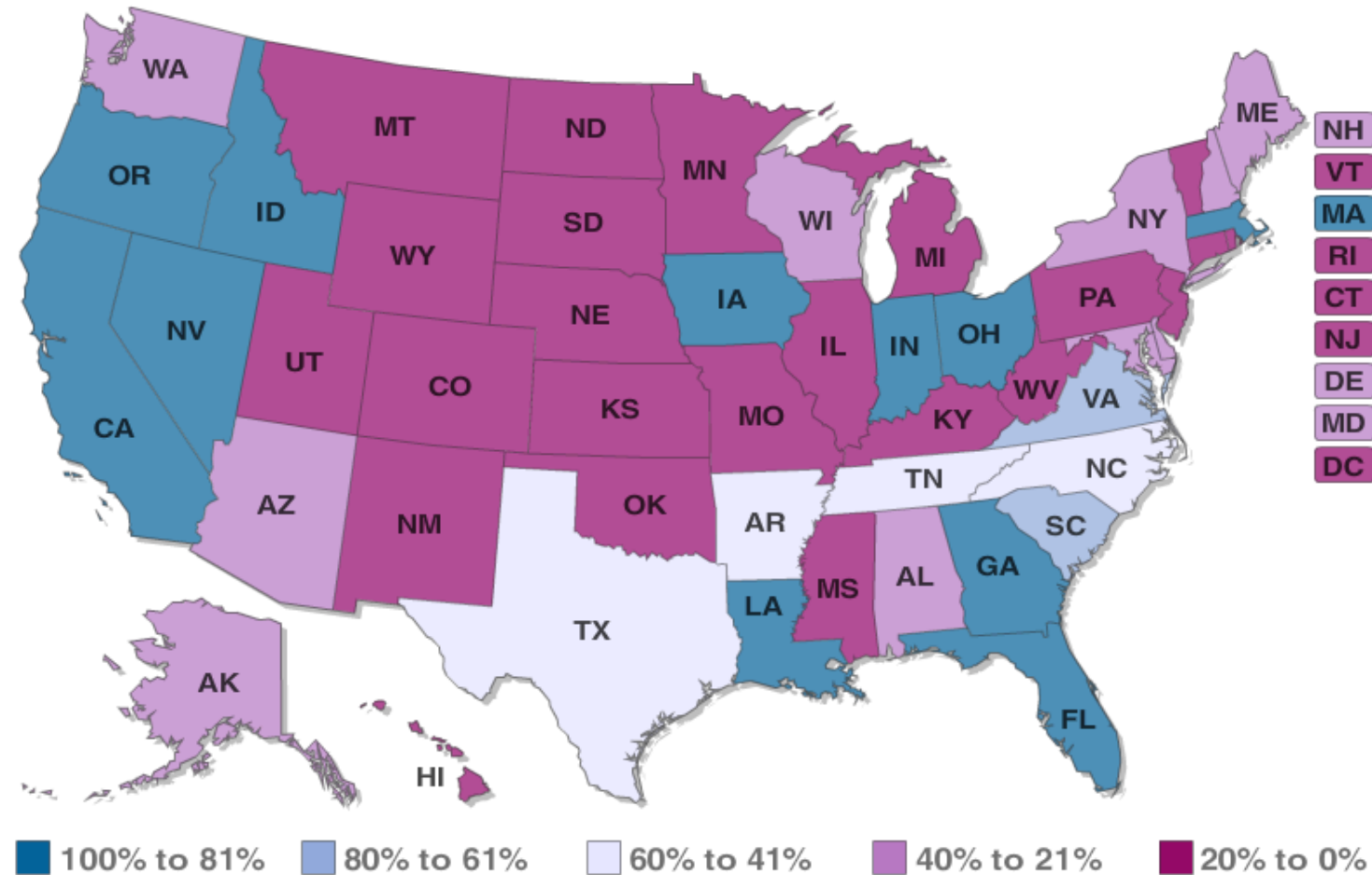
Many of those studying CS are not staying in the country





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

Concepts Adoption Rates

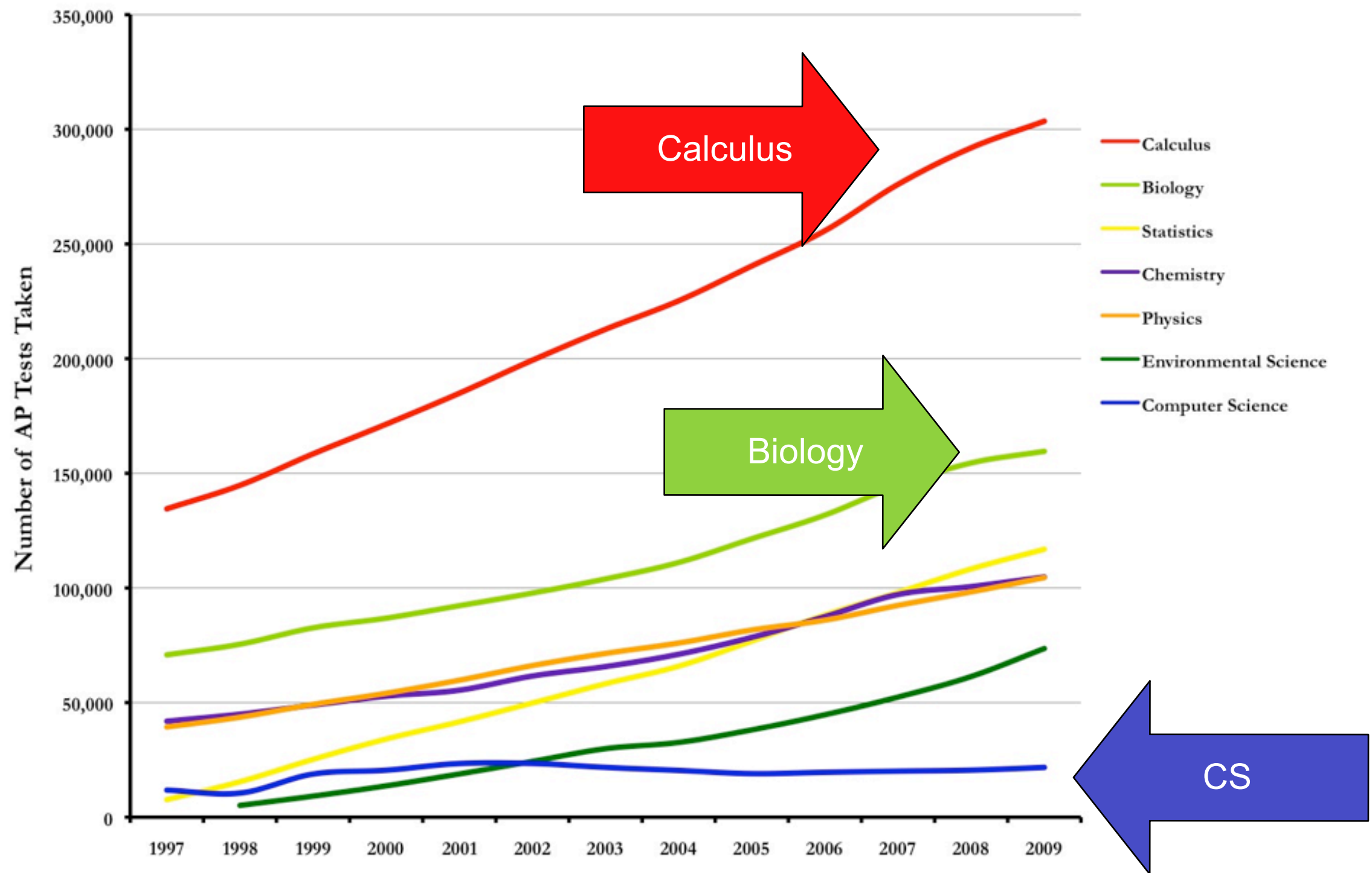


## And teachers are poorly paid!

- *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](http://www.srnleads.org/data/pdfs/ldh_achievemen_gap_summit/inequality_TCR.pdf)

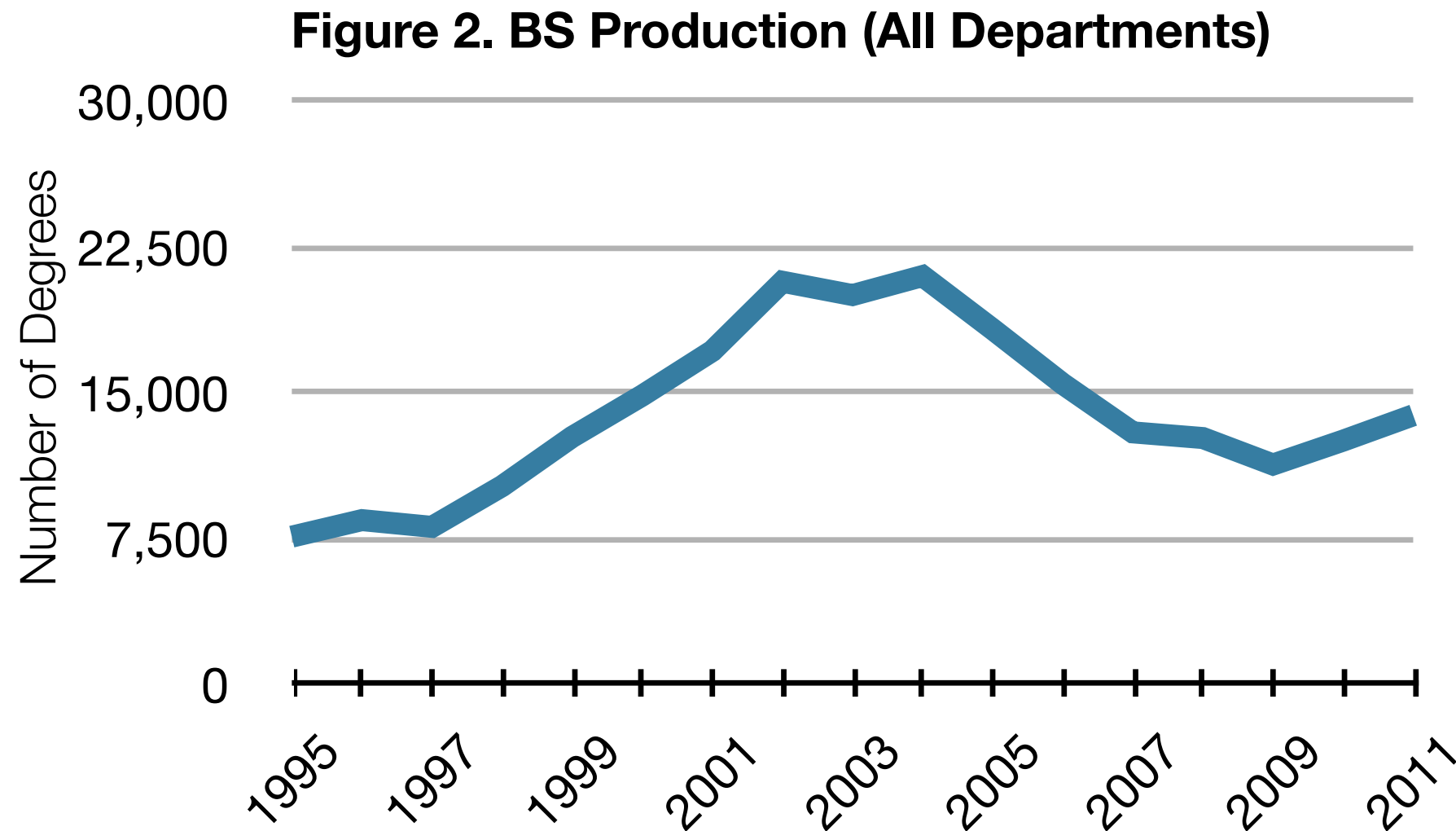
# High school students are not taking AP computer science!



<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)

**Table 5. Bachelor's Degrees Awarded by Ethnicity**

	CS		CE		I		Total	
<b>Nonresident Alien</b>	524	7.0%	179	10.0%	78	3.6%	781	6.8%
<b>Amer Indian or Alaska Native</b>	39	0.5%	8	0.4%	16	0.7%	63	0.5%
<b>Asian</b>	1,115	14.8%	337	18.8%	302	13.9%	1,754	15.3%
<b>Black or African-American</b>	274	3.6%	106	5.9%	151	6.9%	531	4.6%
<b>Native Hawaiian/Pac Islander</b>	22	0.3%	7	0.4%	8	0.4%	37	0.3%
<b>White</b>	5026	66.9%	981	54.7%	1432	65.8%	7,439	64.8%
<b>Multiracial, not Hispanic</b>	104	1.4%	28	1.6%	3	0.1%	135	1.2%
<b>Hispanic, any race</b>	409	5.4%	146	8.1%	187	8.6%	742	6.5%
<b>Total Residency &amp; Ethnicity Known</b>	7,513		1,792		2,177		11,482	
<b>Resident, ethnicity unknown</b>	741		200		99		1,040	
<b>Residency unknown</b>	1032		112		140		1,284	
<b>Grand Total</b>	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		
<b>Nonresident Alien</b>	3,332	56.7%	776	72.6%	389	19.6%	4,497	50.4%	
<b>Amer Indian or Alaska Native</b>	12	0.2%	0	0.0%	12	0.6%	24	0.3%	
<b>Asian</b>	753	12.8%	108	10.1%	245	12.3%	1,106	12.4%	
<b>Black or African-American</b>	96	1.6%	13	1.2%	123	6.2%	232	2.6%	
<b>Native Hawaiian/Pac Island</b>	19	0.3%	0	0.0%	6	0.3%	25	0.3%	
<b>White</b>	1533	26.1%	142	13.3%	1113	56.1%	2,788	31.2%	
<b>Multiracial, not Hispanic</b>	8	0.1%	4	0.4%	4	0.2%	16	0.2%	
<b>Hispanic, any race</b>	119	2.0%	26	2.4%	92	4.6%	237	2.7%	
<b>Total Residency &amp; Ethnicity Known</b>	5,872		1,069		1,984		8,925		
<b>Resident, ethnicity unknown</b>	320		88		205		613		
<b>Residency unknown</b>	419		26		17		462		
<b>Grand Total</b>	6,611		1,183		2,206		10,000		

— *We should let them stay in the country after they graduate*

# 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	
<b>North American PhD Granting Depts.</b>																						
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%
<b>North American, Other Academic</b>																						
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.																						
<b>North American, Non-Academic</b>																						
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%
<b>Total Inside North America</b>																						
	138	6	83	80	57	54	32	53	67	22	23	106	44	35	48	20	26	118	85	178	1,275	89.0%

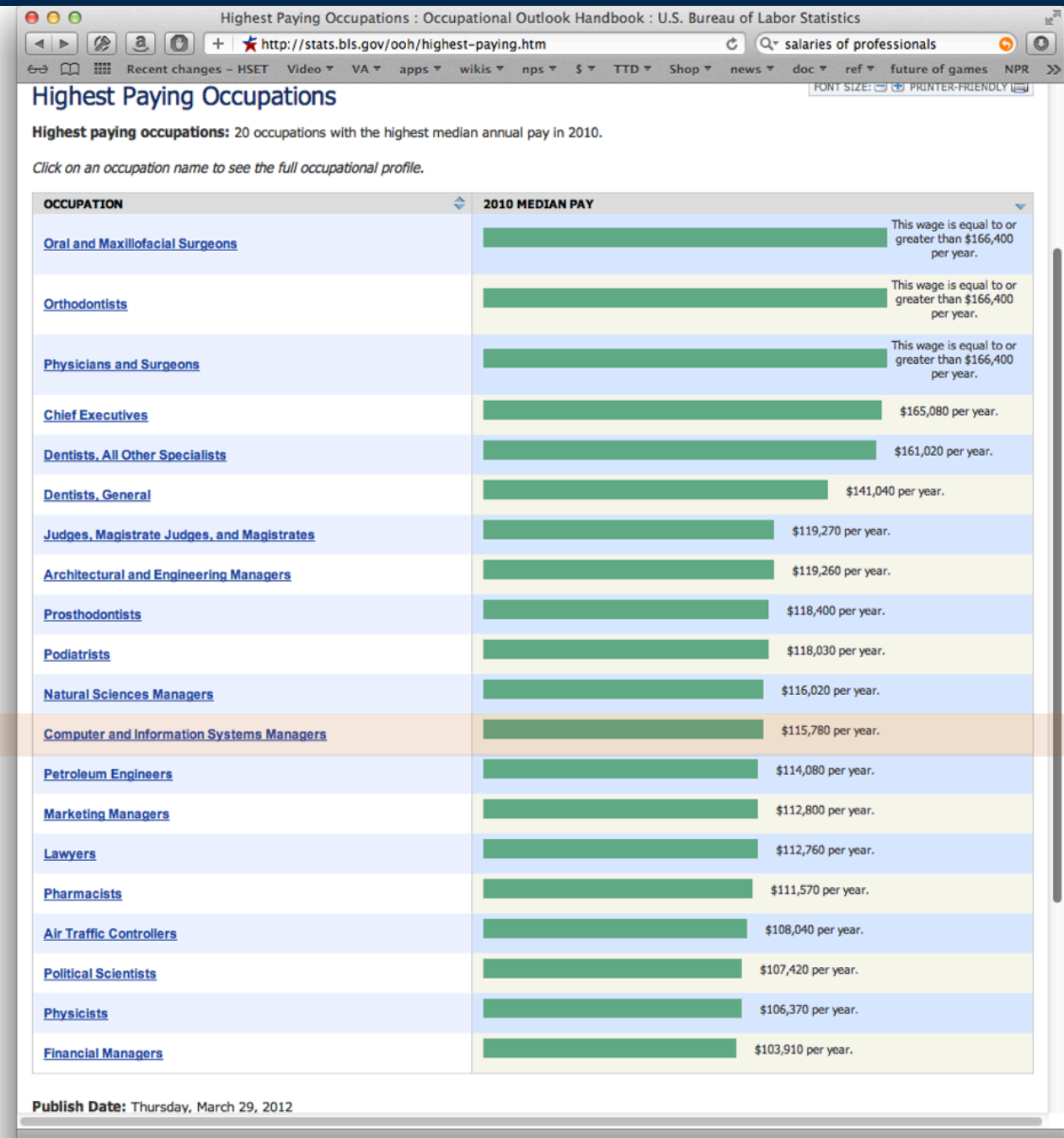
Security should be taught to everyone, but we need specialists

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

## Highest paying occupations:

- Medical: >\$166,400
- CEOs: \$165,080
- Dentists: \$161,020
- Judges: \$119,260
- ...
- Computer Scientists: \$115,070
- ...
- Lawyers: \$112,760

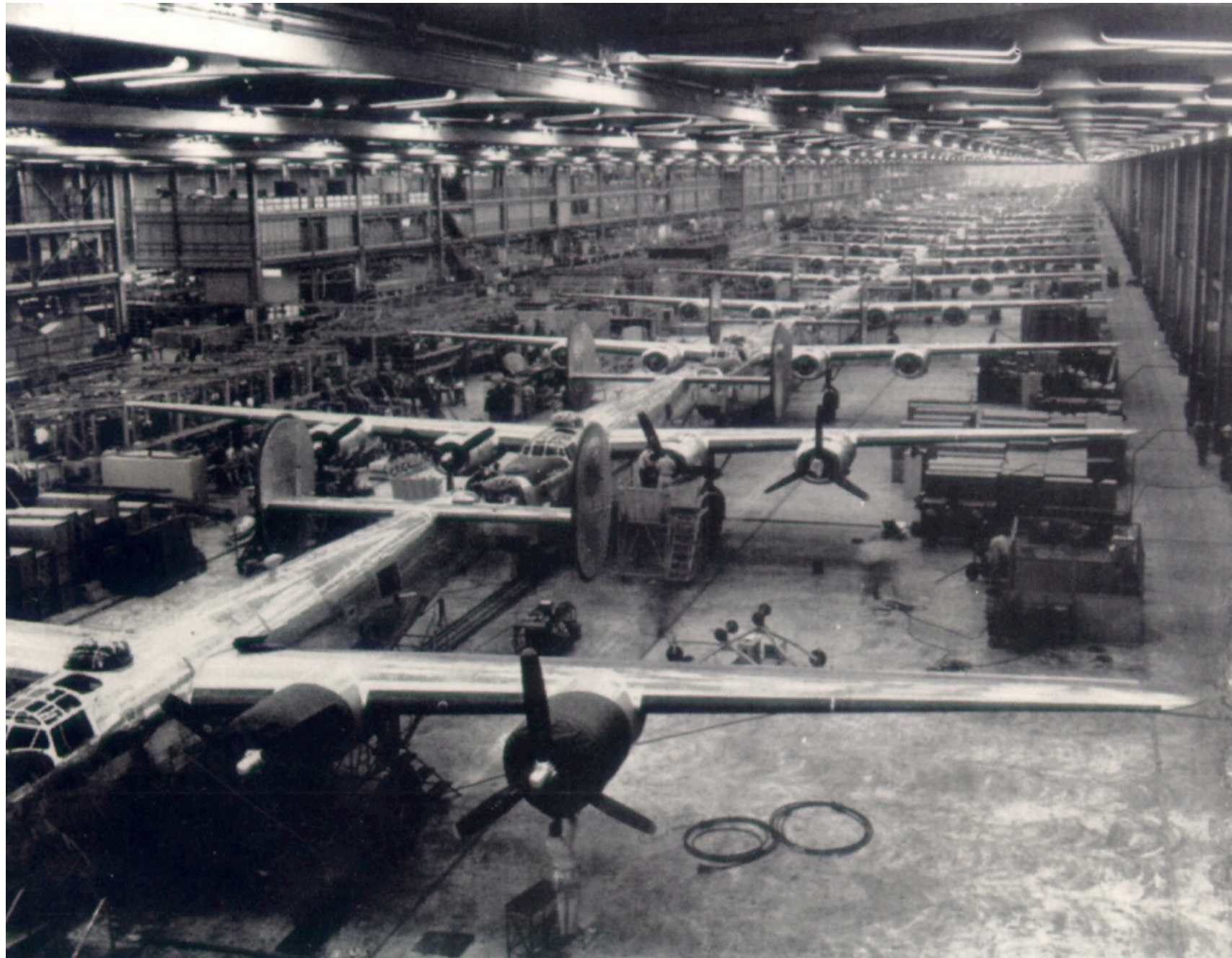
— *Source: Bureau of Labor Stats*



— *Lindsay Lowell, Georgetown Institute for Study of International Migration.*



# Manufacturing policy



- US did not build WW2 aircraft in Germany



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

... because [wireless] computers are everywhere.

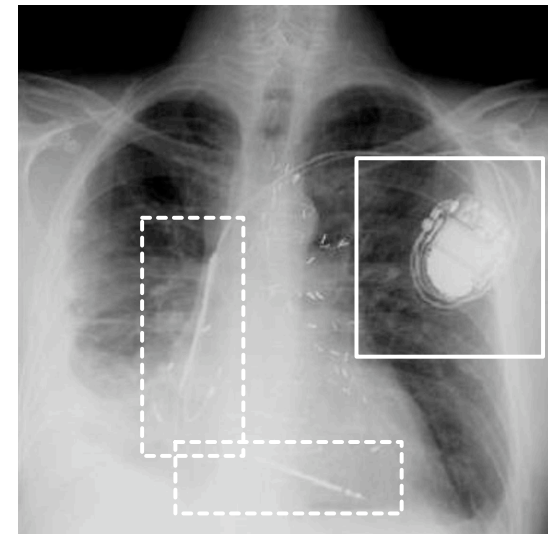


**50 microprocessors  
per average car**

<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](mailto: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](mailto: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](mailto:alerts@infosecnews.org)>

**Subject:** [ISN] ATM Attacks Exploit Lax Security

**Date:** April 23, 2012 3:15:54 AM EDT

**To:** [isn@infosecnews.org](mailto:isn@infosecnews.org)

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



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

By Tracy Kitten  
Bank Info Security  
April 19, 2012

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





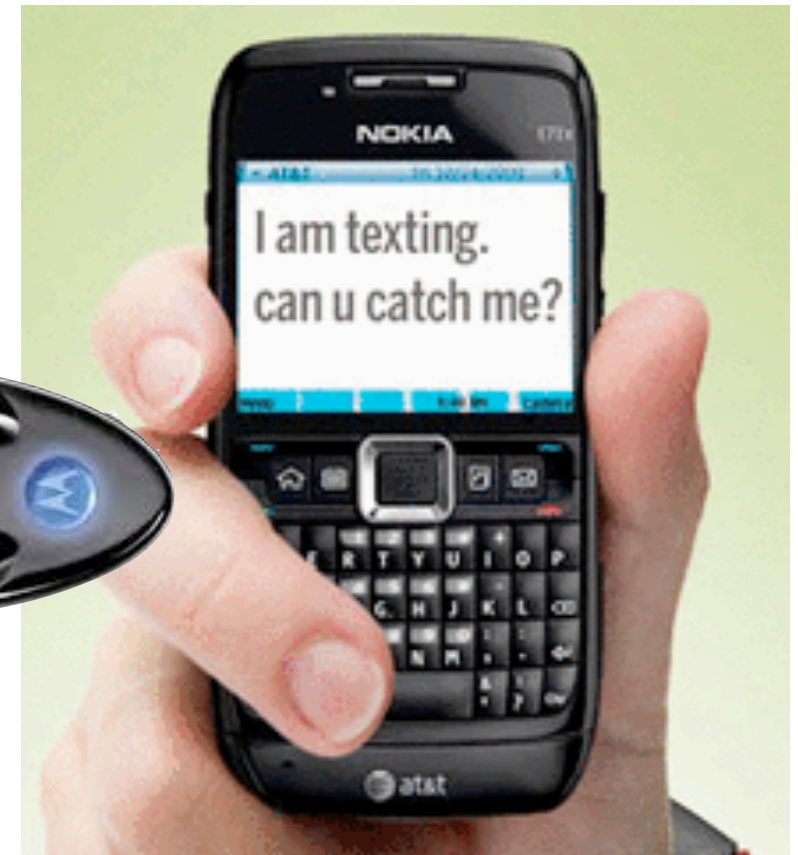
# Cell phones cannot be secured.

## 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 cybersecurity 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,  
1<sup>st</sup> 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 cybersecurity, our systems seem to be growing more vulnerable every year.





**To Make a Difference**

# 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!

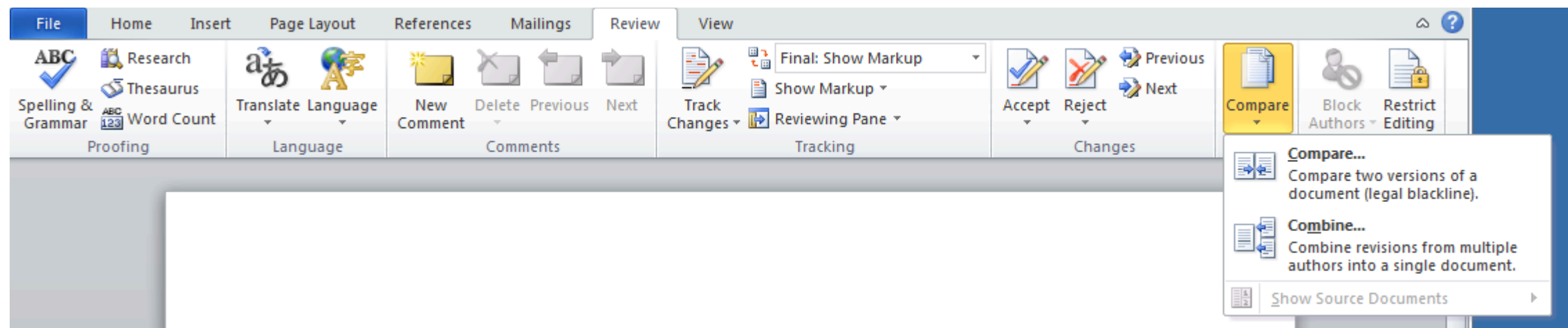
- Section 508 of the Rehabilitation Act (29 USC 794 d) requires that federal government information systems accommodate people with disabilities.
- Bad typography, poor choice of fonts, use of Flash *may be illegal!*
- Speak with the Section 508 Coordinator — or volunteer to become one!

# 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!

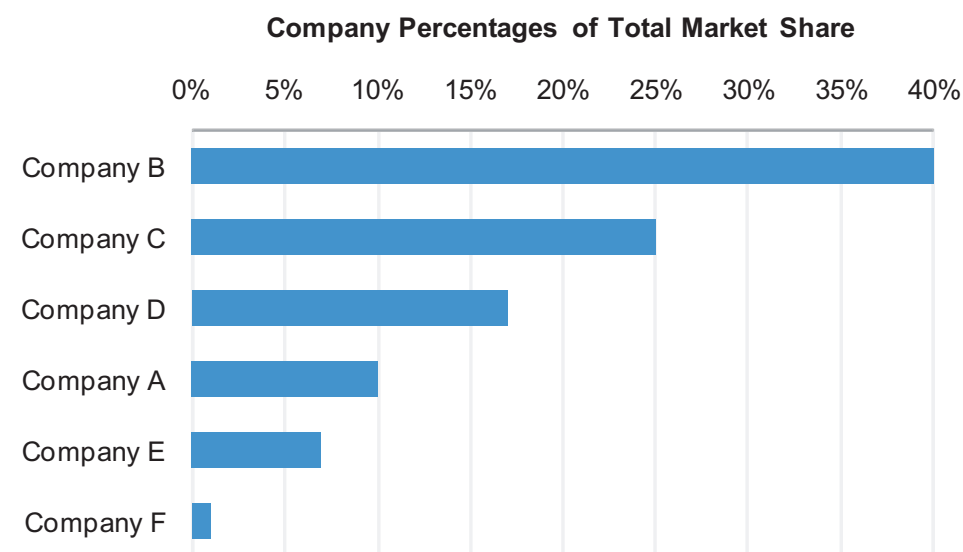


# Don't use pie charts

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

# Security problems reflect deep societal problems. You 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](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."<sup>1</sup> 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."<sup>2</sup> 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."<sup>3</sup> Fidelity "will reimburse your Fidelity account for any losses due to unauthorized activity,"<sup>4</sup> and "under HSBC's \$0 Liability, Online Guarantee, you're covered 100% and liable for \$0."<sup>5</sup> 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."<sup>6</sup>

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.<sup>7</sup>) 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





# Backup Slides

# 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