The Cybersecurity Mess

Simson L. Garfinkel
Associate Professor, Naval Postgraduate School

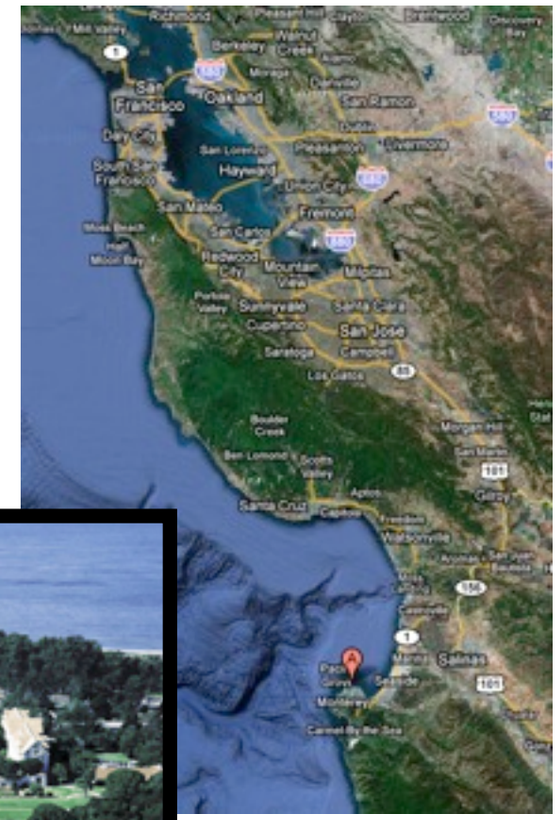
April 25, 2013

“The views expression in this presentation are those of the author and do not reflect the official policy of the Department of Defense or the US Government.”

NPS is the Navy's Research University.

Monterey, CA — 1500 students

- US Military (All 5 services)
- US Civilian (Scholarship for Service & SMART)
- Foreign Military (30 countries)
- *All students are fully funded*



Schools:

- Business & Public Policy
- Engineering & Applied Sciences
- Operational & Information Sciences
- International Graduate Studies

NCR Initiative — Arlington, VA

- 8 offices on 5th floor, Virginia Tech building
- Current staffing: 4 professors, 2 lab managers, 2 programmers, 4 contractors
- **OPEN SLOTS FOR .GOV PHDs!**

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

viewpoints

DOI:10.1145/2184319.2184330

Simson 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 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 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 unlowered. 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.

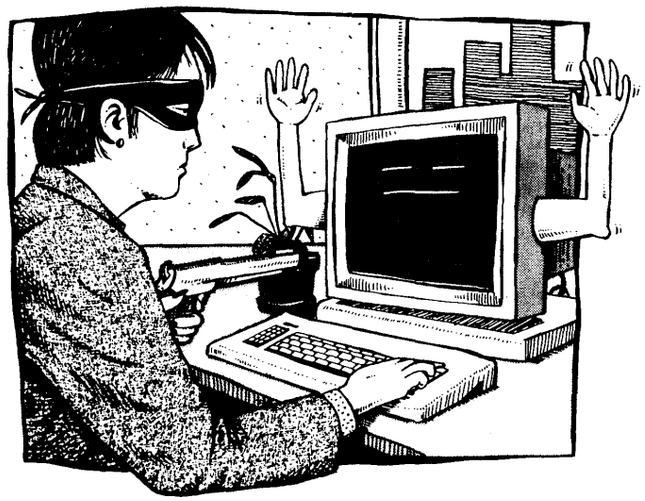
It may be that cybersecurity appears to be getting worse simply because society as a whole is becoming much more dependent upon computers. Even if the vulnerability were not increasing, the successful hacks can have significantly more reach today than a decade ago.

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]

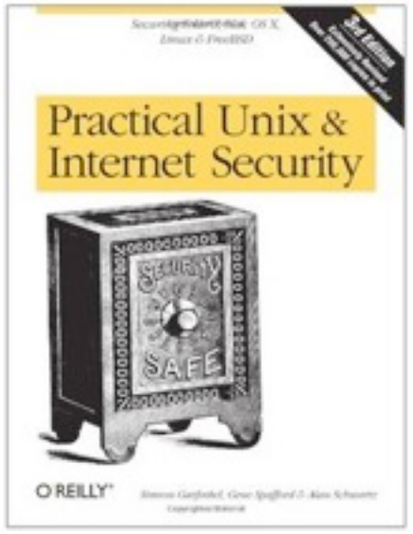
Simson L. Garfinkel

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

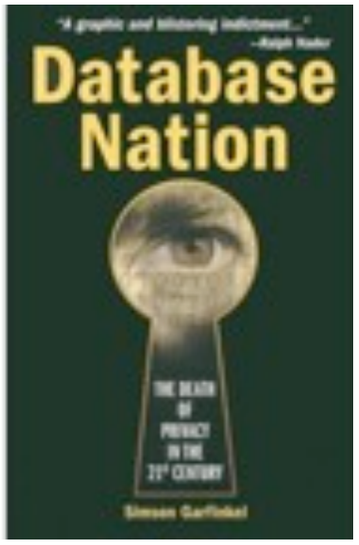
LAWYERS MUST UNDERSTAND issues of computer security, both for the protection of their own interests and the interests of their clients. Lawyers today must automatically recognize insecure computer systems and lax operating procedures in the same way as lawyers now recognize

39

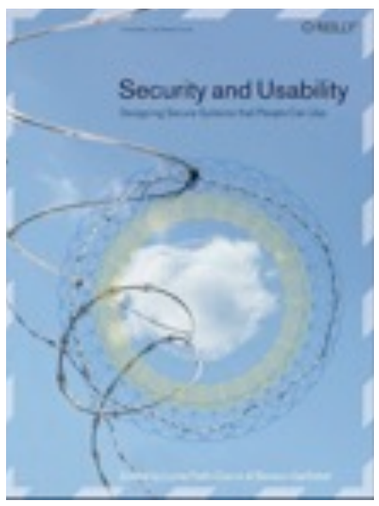
Sept. 1987



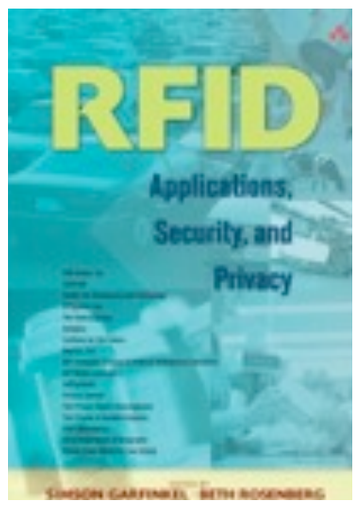
1991



2000



2006



2006

...and I have given up!

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

Reasons:

- 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.

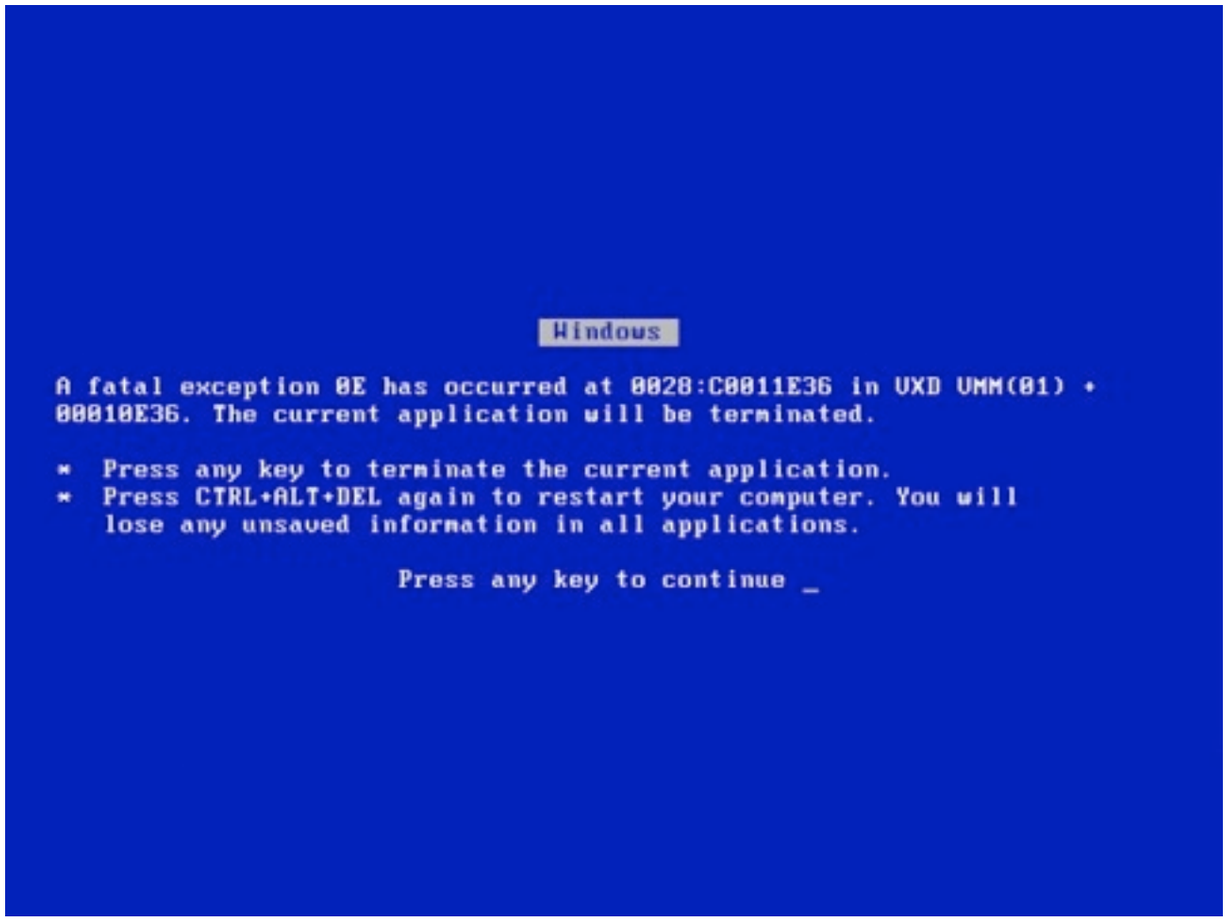
Windows

A fatal exception 0E has occurred at 0028:C0011E36 in VXD VMM(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

All Mailboxes (Found 5315 matches for search)

Junk | Reply | Reply All | Forward | Get Mail | Delete | Archive | New Message | Note | Show Related Messages | Flag | SUBJECT isn | 5315 Found

Hide | Search: All | Archive | Inbox (27) | Drafts (5) | Sent (2) | Flagged | Notes | Save

MAILBOXES
- Inbox 27
- Drafts 5
- Sent 2
- Trash 27

REMINDERS
- Flagged 7

RSS
- Apple Hot News 38

ON MY MAC
- 2007 Archive 36600
- 2007 Outgoing 1
- 2008 Archive 29235
- 2008 Outgoing 7
- 2008 Professional 2
- 2008 Sys 17
- 2009 Outgoing 35
- NPS Archive 2010 3304
- NPS Archive 2011
- NPS Outgoing 2010 139
- NPS Outgoing 2011
- SLG Archive 2010 7443

MAIL ACTIVITY

From	To	Subject	Date R...	Mailbox
InfoSec News	isn@infos...	[ISN] Google Working on Password Generator f...	2/17/12	All Mail
InfoSec News	isn@infos...	[ISN] Secunia Weekly Summary - Issue: 2012-07	2/17/12	All Mail
InfoSec News	isn@infos...	[ISN] Blue Coat Systems taken private for $1.3...	2/17/12	All Mail
InfoSec News	isn@infos...	[ISN] RSA brushes off crypto research findings...	2/17/12	All Mail
InfoSec News	isn@infos...	[ISN] Anonymous-Backed Attacks Took Nasda...	2/17/12	All Mail
InfoSec News	isn@infos...	[ISN] Most Small Healthcare Practices Hacked I...	2/17/12	All Mail
InfoSec News	isn@infos...	[ISN] Attempted Cyber-Attack on Bank Hapoalim	2/17/12	All Mail
InfoSec News	isn@infos...	[ISN] Air Force Special Operations Command e...	2/20/12	All Mail
InfoSec News	isn@infos...	[ISN] 8 Lessons From Nortel's 10-Year Security...	2/20/12	All Mail

From: **InfoSec News** Hide
Subject: [ISN] Anonymous-Backed Attacks Took Nasdaq Website Offline
Date: February 17, 2012 5:34:14 AM EST All Mail
To: isn@infosecnews.org

http://www.informationweek.com/news/security/attacks/232600975

By Mathew J. Schwartz
InformationWeek
February 16, 2012

The websites of the Nasdaq and BATS stock exchanges, together with the Chicago Board Options Exchange (CBOE), were offline earlier this week after a hacktivist group with apparent Anonymous ties targeted them with distributed denial of service (DDoS) attacks. But while customers were intermittently unable to use some of the exchanges' websites, all said that their trading systems weren't affected.

The attacks had been previewed the day before they were launched. In a post to Pastebin, a group calling itself "the 'L0NGwave99' cyber group" said Sunday it was going to launch "Operation Digital Tornado" in support of the "99% movement" Monday at 9 a.m. New York time. A later message promised the same for Tuesday.

"The NASDAQ stock exchange besides a number of U.S. stock markets are going to face some problems and may need maintenance," said the L0NGwave99 statement, which promised to launch DDoS-driven takedowns against www.nasdaq.com, www.batstrading.com (BATS), www.cboe.com (CBOE), and www.ms4x.com (the Miami Stock Exchange).

"Will anybody be able to stop the people?s (sic) storm of seeking justice against the liar and deceptive Capitalism-Liberalism? Soon we will see..." read the group's statement.

[...]

Certified Ethical Hacker and CISSP training with Expanding Security gives

[ISN] Anonymous-Backed Attacks Took Nasdaq Website Offline

From: **InfoSec News <alerts@infosecnews.org>**
Subject: [ISN] Anonymous-Backed Attacks Took Nasdaq Website Offline
Date: February 17, 2012 5:34:14 AM EST
To: isn@infosecnews.org

http://www.informationweek.com/news/security/attacks/232600975

By Mathew J. Schwartz
InformationWeek
February 16, 2012

The websites of the Nasdaq and BATS stock exchanges, together with the Chicago Board Options Exchange (CBOE), were offline earlier this week after a hacktivist group with apparent Anonymous ties targeted them with distributed denial of service (DDoS) attacks. But while customers were intermittently unable to use some of the exchanges' websites, all said that their trading systems weren't affected.

The attacks had been previewed the day before they were launched. In a post to Pastebin, a group calling itself "the 'L0NGwave99' cyber group" said Sunday it was going to launch "Operation Digital Tornado" in support of the "99% movement" Monday at 9 a.m. New York time. A later message promised the same for Tuesday.

"The NASDAQ stock exchange besides a number of U.S. stock markets are going to face

[ISN] Most Small Healthcare Practices Hacked In The Past 12 Months

From: **InfoSec News <alerts@infosecnews.org>**
Subject: [ISN] Most Small Healthcare Practices Hacked In The Past 12 Months
Date: February 17, 2012 5:34:29 AM EST
To: isn@infosecnews.org

http://www.darkreading.com/database-security/167901020/security/news/232601045/most-small-healthcare-practices-hacked-in-the-past-12-months.html

By Kelly Jackson Higgins
Dark Reading
Feb 16, 2012

If you were wondering how safe your medical records are at your doctor's office, then this might make you sick: Ninety-one percent of small healthcare practices in North America say they have suffered a data breach in the past 12 months.

The survey, conducted by the Ponemon Institute and commissioned by MegaPath, queried more than 700 IT and administrative personnel in healthcare organizations of no more than 250 employees.

Among the findings: Only 31 percent say their management considers data security and privacy a top priority, and 29 percent say their breaches resulted in medical identity theft. "Cybercriminals are hunting for medical records," said Larry Ponemon, chairman and founder

[ISN] Air Force Special Operations Command eyes Russian security software for iPads

From: **InfoSec News <alerts@infosecnews.org>**
Subject: [ISN] Air Force Special Operations Command eyes Russian security software for iPads
Date: February 20, 2012 3:16:00 AM EST
To: isn@infosecnews.org

http://www.nextgov.com/nextgov/ng_20120217_4350.php

By Bob Brewin
Nextgov
02/17/2012

When the Air Force Special Operations Command decided to buy 2,861 made-in-China Apple iPad tablet computers in January to provide flight crews with electronic navigation charts and technical manuals, it specified mission security software developed, maintained and updated in Russia.

The command followed in the path of Alaska Airlines, which in May 2011 became the first domestic carrier to drop paper charts and manuals in exchange for electronic flight bags. Alaska chose the same software, GoodReader, developed by Moscow-based Good.iware, to display charts in a PDF format on iPads. Delta Air Lines kicked off a test in August for electronic flight bags and the carrier said it planned to use GoodReader software.

[ISN] 8 Lessons From Nortel's 10-Year Security Breach

From: **InfoSec News <alerts@infosecnews.org>**
Subject: [ISN] 8 Lessons From Nortel's 10-Year Security Breach
Date: February 20, 2012 3:16:51 AM EST
To: isn@infosecnews.org

http://www.informationweek.com/news/security/attacks/232601092

By Mathew J. Schwartz
InformationWeek
February 17, 2012

It is every corporate security manager's worst nightmare.

News surfaced this week that Nortel's network was hacked in 2000, after which attackers enjoyed access to the telecommunications and networking company's secrets for 10 years.

The intrusions reportedly began after attackers used passwords stolen from the company's CEO, as well as six other senior executives, together with spyware. By 2004, a Nortel employee did detect unusual download patterns associated with senior executives' accounts, and changed related passwords. The security team also began watching for signs of suspicious activity, but apparently stopped doing so after a few months. The full extent of the breach wasn't discovered until 2010, by which time hackers had been accessing Nortel secrets--from technical papers and business plans, to research reports and employees'

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

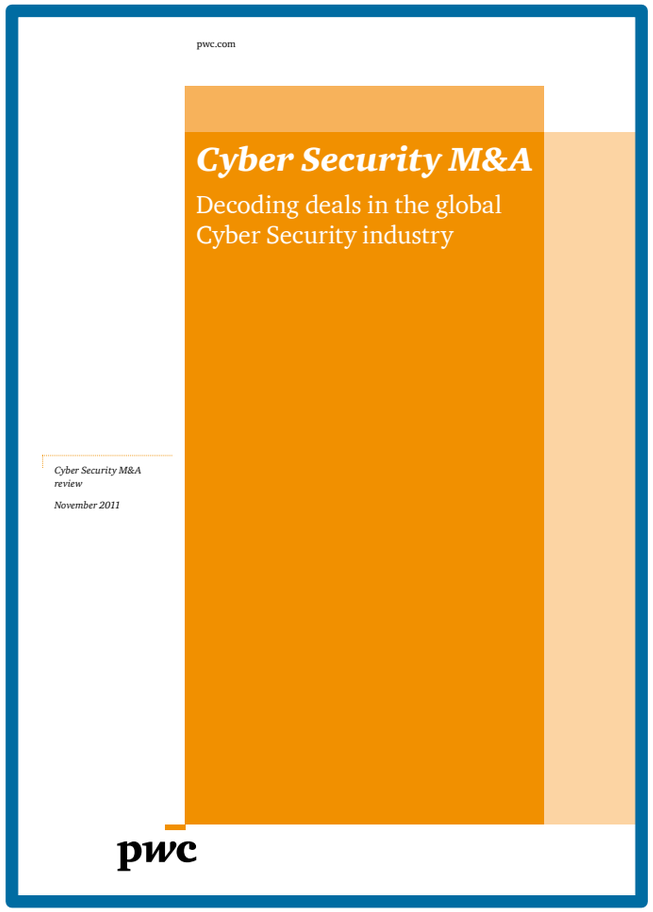
We will do better when we *want* to do better.

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

Cybersecurity is expensive.

Global cybersecurity spending: $60 billion in 2011

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


pwc.com

Cyber Security M&A

Decoding deals in the global Cyber Security industry

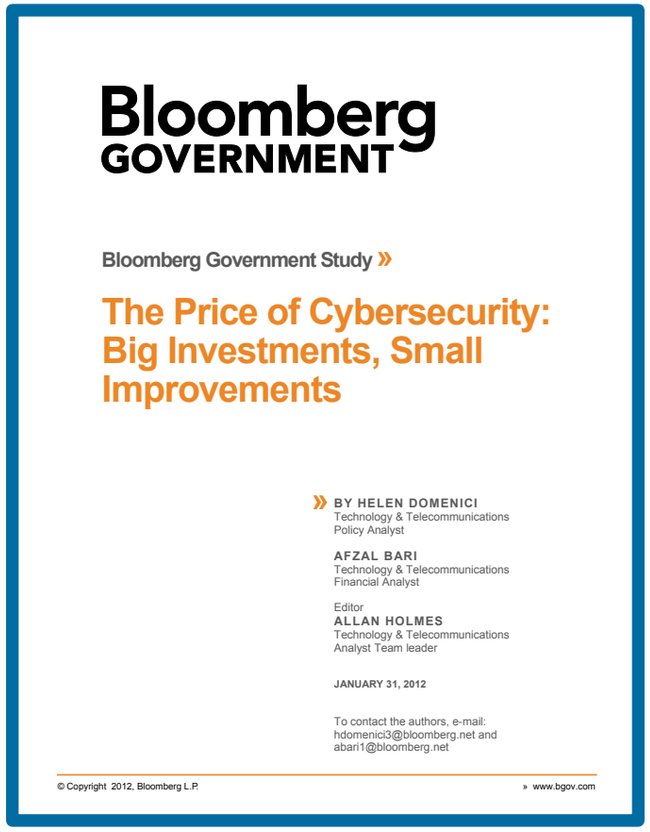
Cyber Security M&A review

November 2011

pwc

172 Fortune 500 companies surveyed:

- Spending $5.3 billion per year on cybersecurity.
- Stopping 69% of attacks.


Bloomberg GOVERNMENT

Bloomberg Government Study »

The Price of Cybersecurity: Big Investments, Small Improvements

» BY HELEN DOMENICI
Technology & Telecommunications Policy Analyst

AFZAL BARI
Technology & Telecommunications Financial Analyst

Editor
ALLAN HOLMES
Technology & Telecommunications Analyst Team leader

JANUARY 31, 2012

To contact the authors, e-mail: hdomenici3@bloomberg.net and abari1@bloomberg.net

» www.bgov.com

If they raise spending...

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

95% is not good enough.

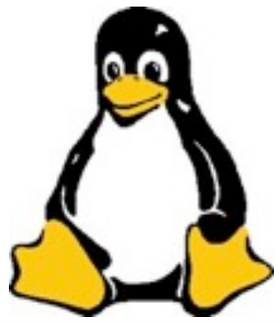
Cybersecurity... is undefined.

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~~

There is no way to *measure* cybersecurity

- Which OS is more secure?
- Which computer is more secure?
- Is “open source” more secure?
- Does spending more money make a computer more secure? ***NO***



Why the downward spiral?

Cybersecurity research does not make computers more secure

- "Reducing successful hacks" creates too big a target.
  - *Targets include data, apps, OS, network, human operators, hiring process, supply chain, family members, ...*
- Security research creates better attacks.

The environment is less secure:

- Increased interconnectedness
- Computers in more positions of trust
  - *Attacks today do more damage than attacks in the 1990s.*
-

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 can secure cyberspace….

—*But we can’t stop insiders.*

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.

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

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

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

Every computer is connected to every other computer on the planet.

- USB sticks, DVDs, printers (“yellow dots”), scanners.
- Downloaded software (OS, applications), firmware, microcode

Every system is part of a computational ecology.

“Yellow Dots”

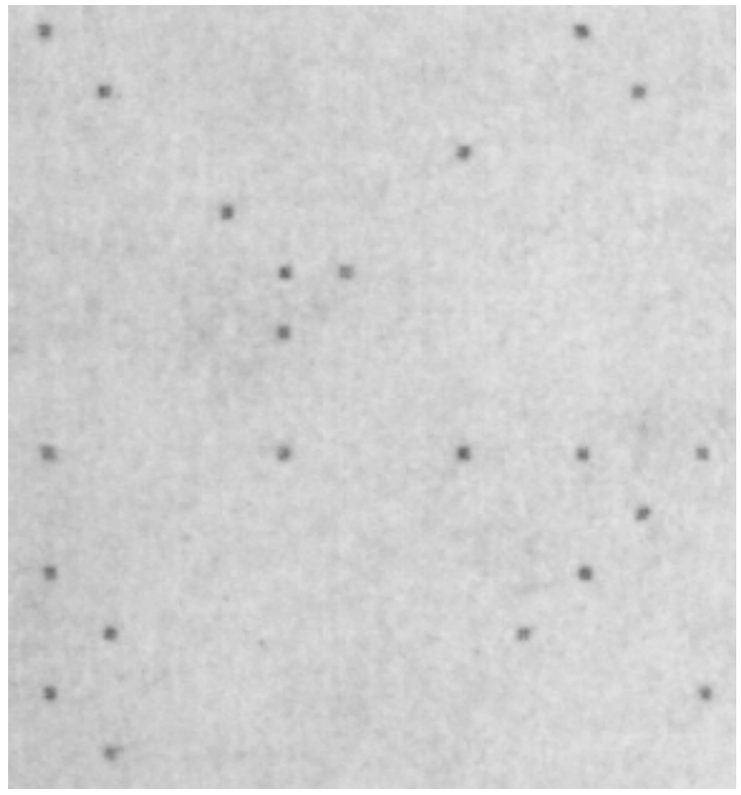
October 16, 2005

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



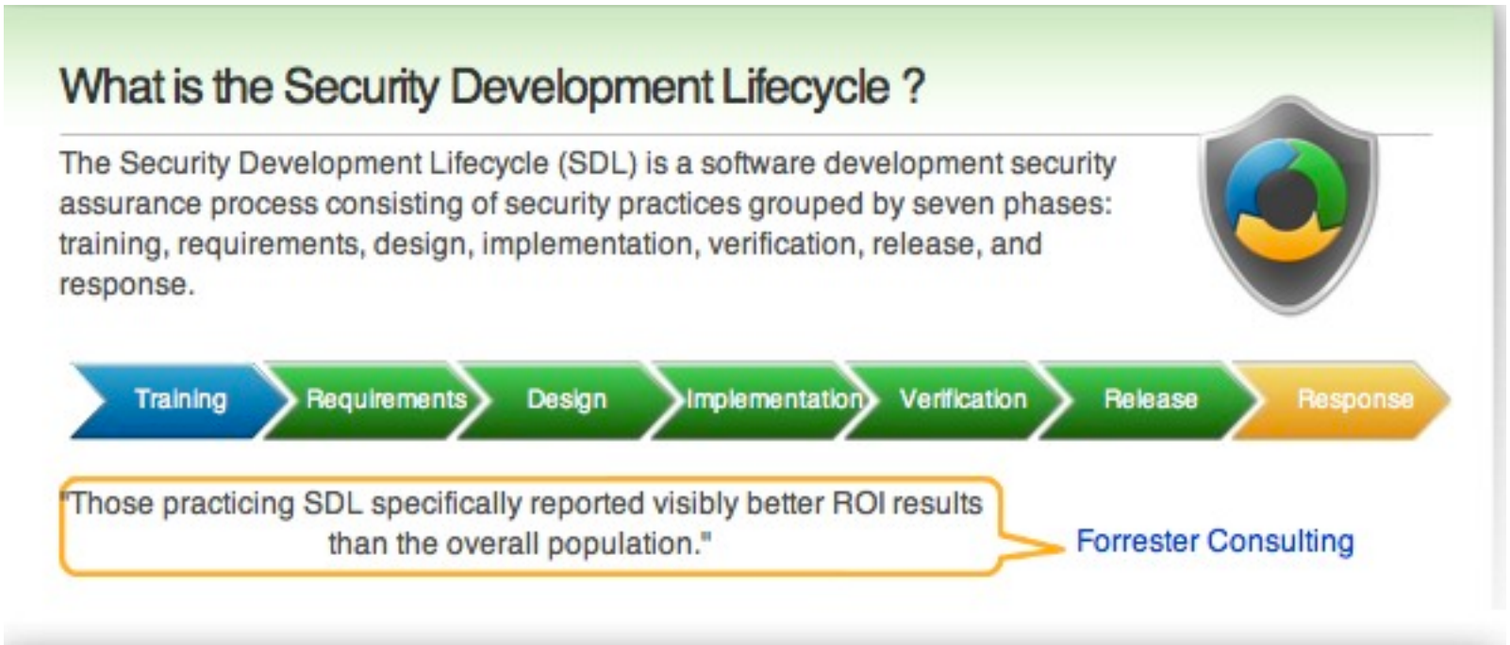
Sample closeup of the same dots showing only the blue channels to make the dots more visible.

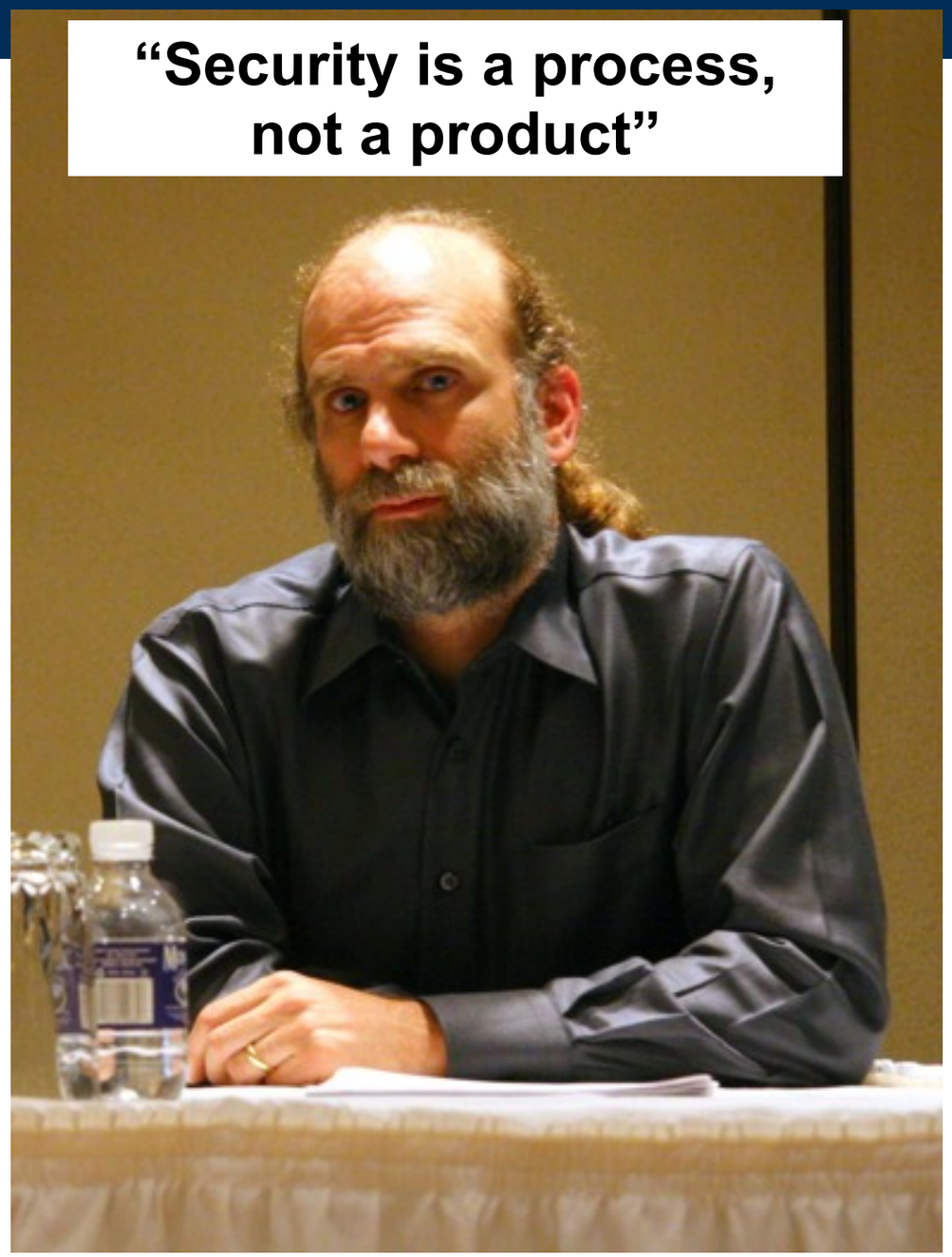
http://seeingyellow.com/

Cybersecurity is a process problem.

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

Microsoft Security Development Lifecycle





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

— *Few organizations can afford SDL.*

— *Windows 7 is still hackable...*

Cybersecurity is a money problem.

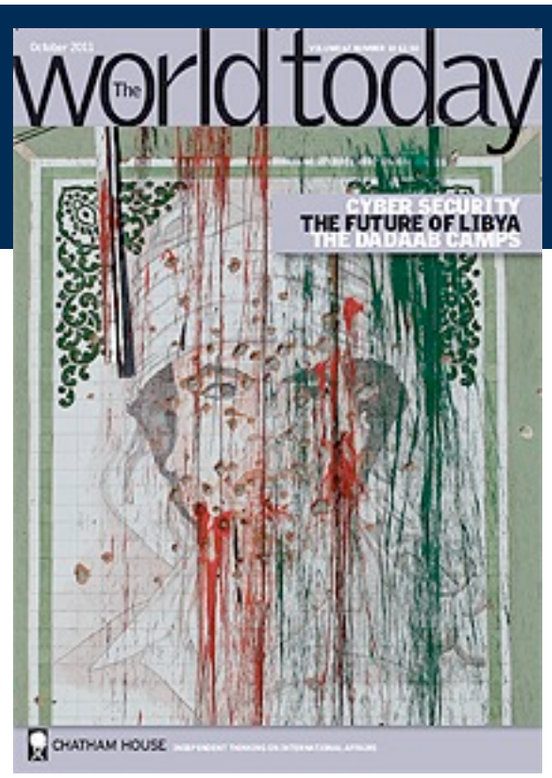
Security is a cost....

- ...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

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 an 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*

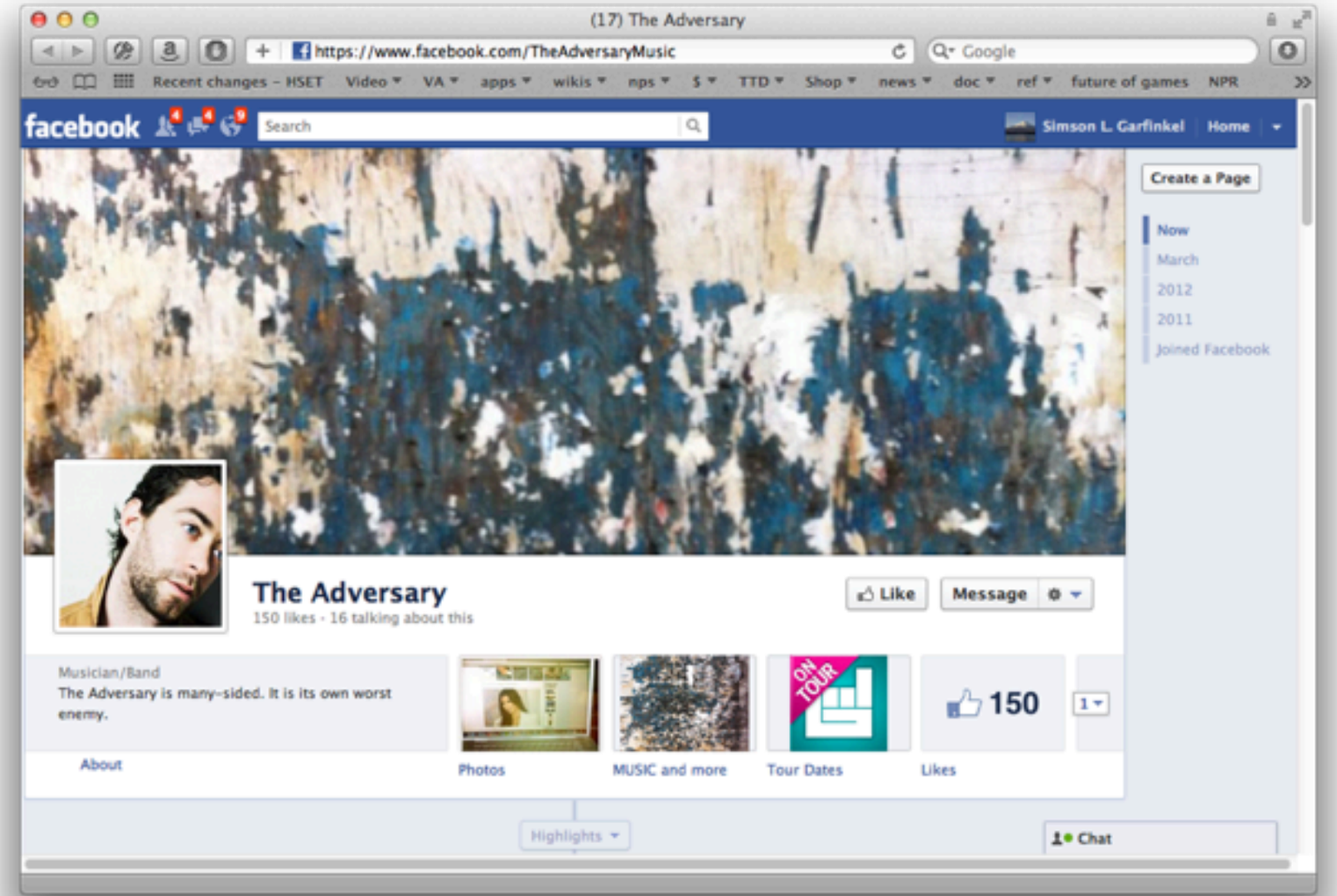
— *Dave Clement, “Cyber Security as a Wicked Problem,” Chatham House, October 2011 http://www.chathamhouse.org/publications/twt/archive/view/178579*

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*



Compiler bugs are security vulnerabilities!

The adversary chooses:

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

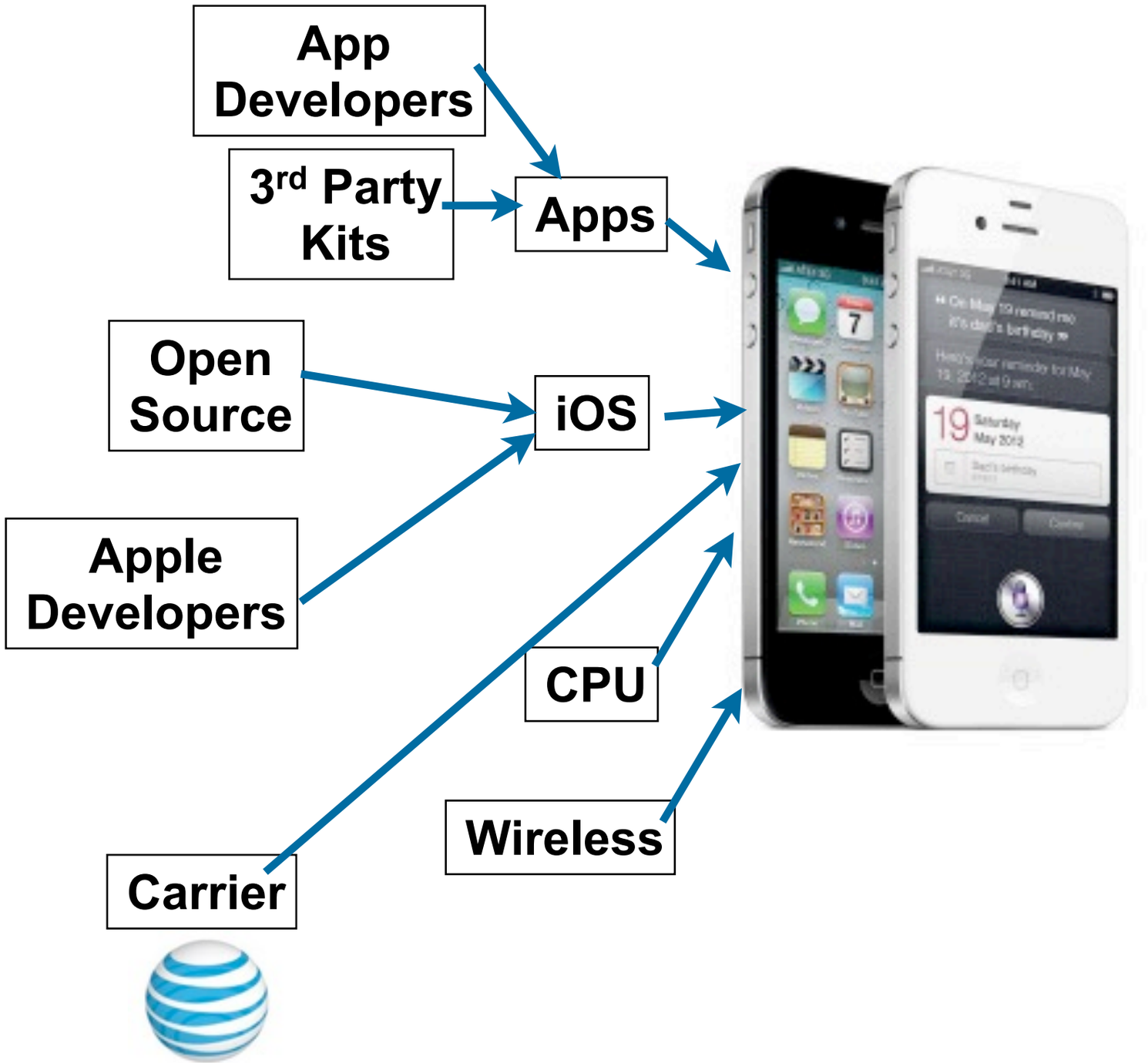
We have seen:

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

What's difference between a bug an an attack?

— *The programmer's intent.*

The supply chain creates numerous security vulnerabilities



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

ACComplice: 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 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.

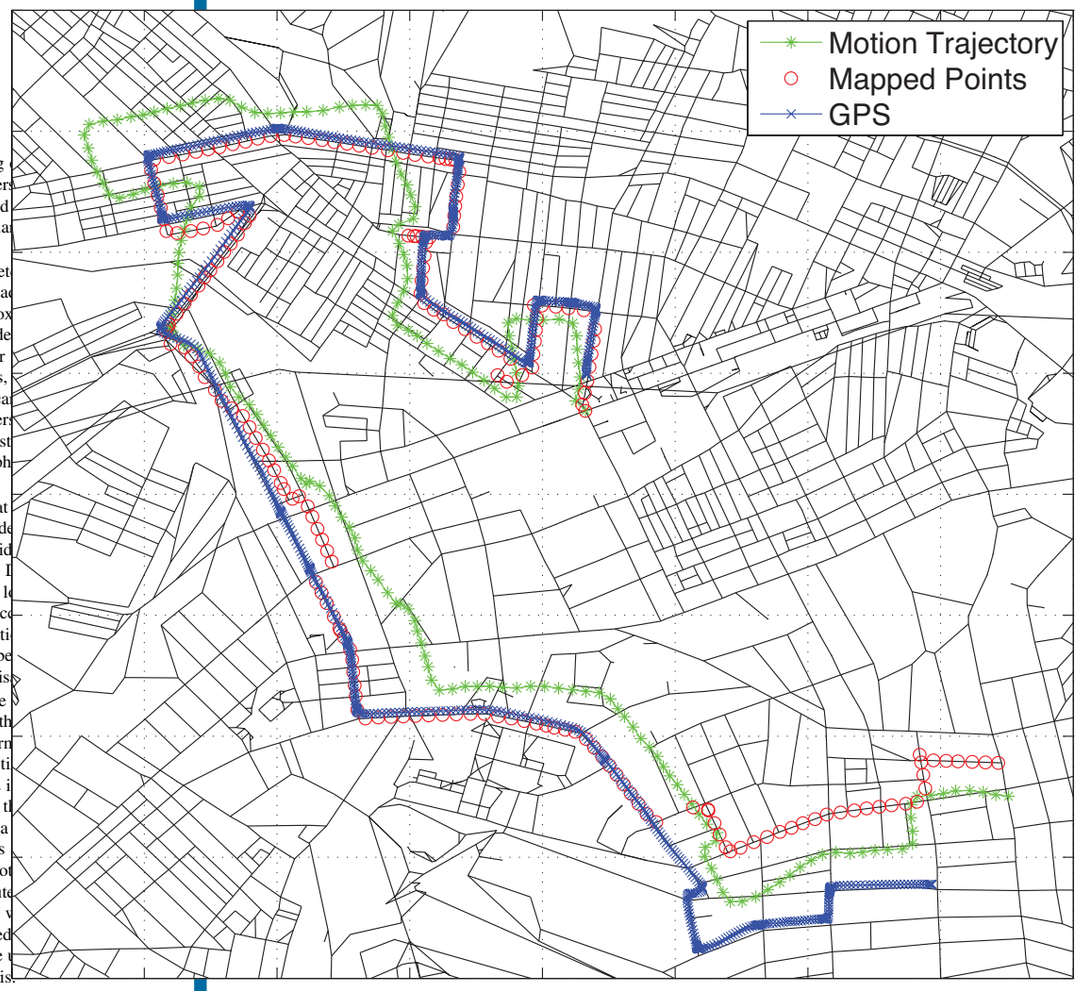
Accelerometers are a particularly interesting
their pervasiveness in a large assortment of pers
devices including tablet PCs, MP3 players, and
ing devices. This array of devices provides a la
spyware to exploit.

Furthermore, by correlating the acceleromet
tween multiple phones it is possible for an a
termine whether the phones are in close prox
phones undergoing similar motions can be ide
accelerations, events such as earthquakes or
activities like public transportation (e.g., bus,
produce identifiable motion signatures that ca
with other users. As a consequence, if one per
access, or exposes their cellular or Wi-Fi base st
essentially expose the location of all nearby ph
the adversary has access to these devices.

a) Contributions: Our key insight is that
enable the identification of one's location de
noisy trajectory output. This is because the id
roadways create globally unique constraints. I
can be used to track a user's location long after l
have been disabled [6]. But as we show, the acc
be used to infer a location with no initial locati
This is a very powerful side-channel that can be
if location-based services on the device are dis

b) Threat Model: We assume that the
execute applications on the mobile device, with
privileges except the capability to send inform
network. The application will use some legiti
obtain access to network communication. This i
plished by mimicking a popular application t
download; e.g., a video game. In the case of a
access would be needed to upload high scores
advertisements. We assume that the OS is not
so that the malicious application simply execute
application. The application can communicate v
server to leak acceleration information. Based
information, the adversary can extract a mobile
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_ACComplice_comsnets12.pdf
Jun Han, Emmanuel Owusu, Thanh-Le Nguyen, Adrian Perrig, and Joy Zhang "ACComplice: 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….

http://forums.corvetteforum.com/off-topic/2824193-i-only-have-to-outrun-you-polar-bear-tag.html

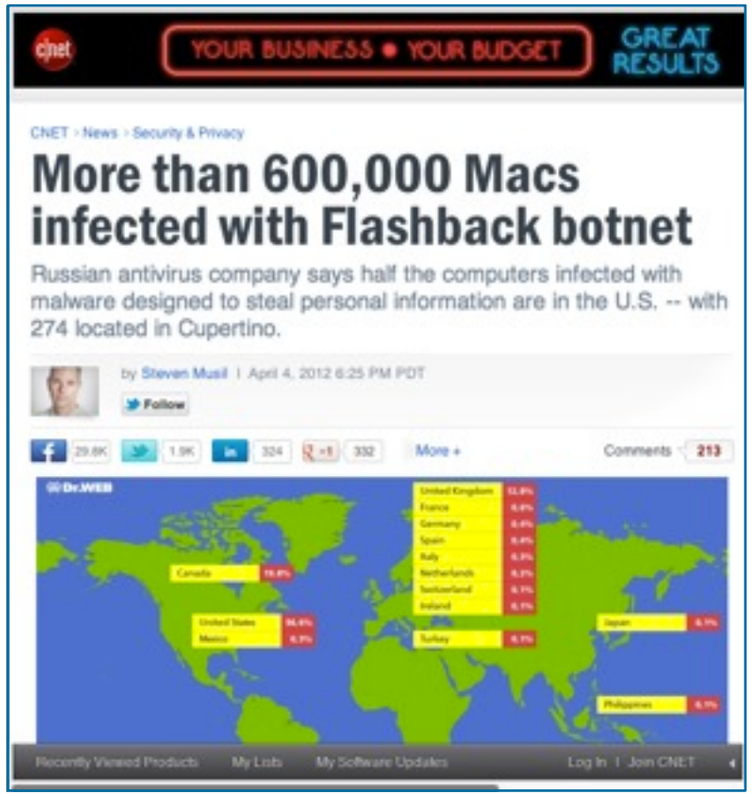
There are solutions to many cybersecurity problems...
... but we don't use them.

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 is *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*

Nontechnical factors impacting cybersecurity.

Non-technical factors reflect deep divisions within our society.

- ***Shortened*** development cycles
- ***Education:*** General failure of our schools at 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

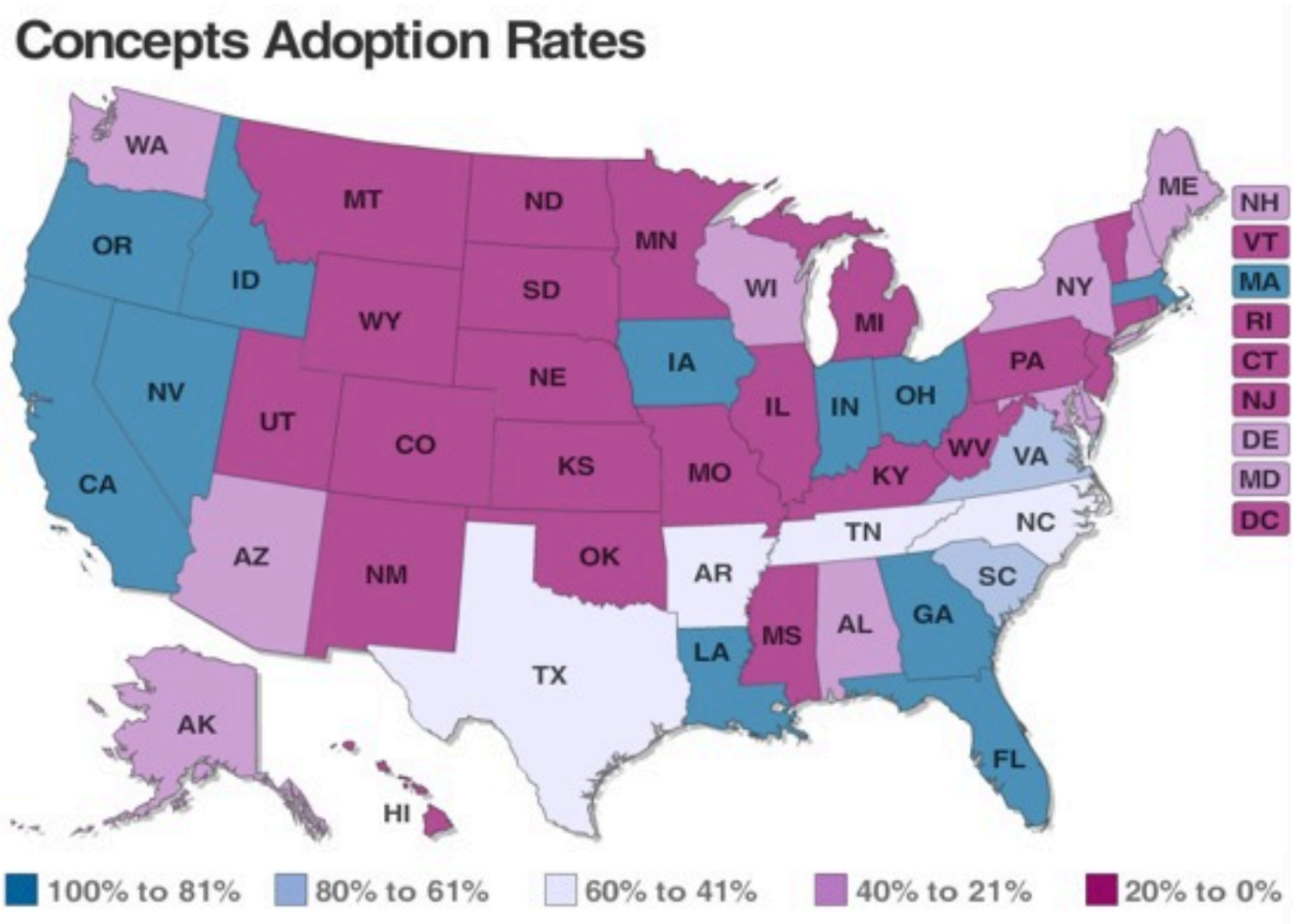
Education is not supplying enough security engineers

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

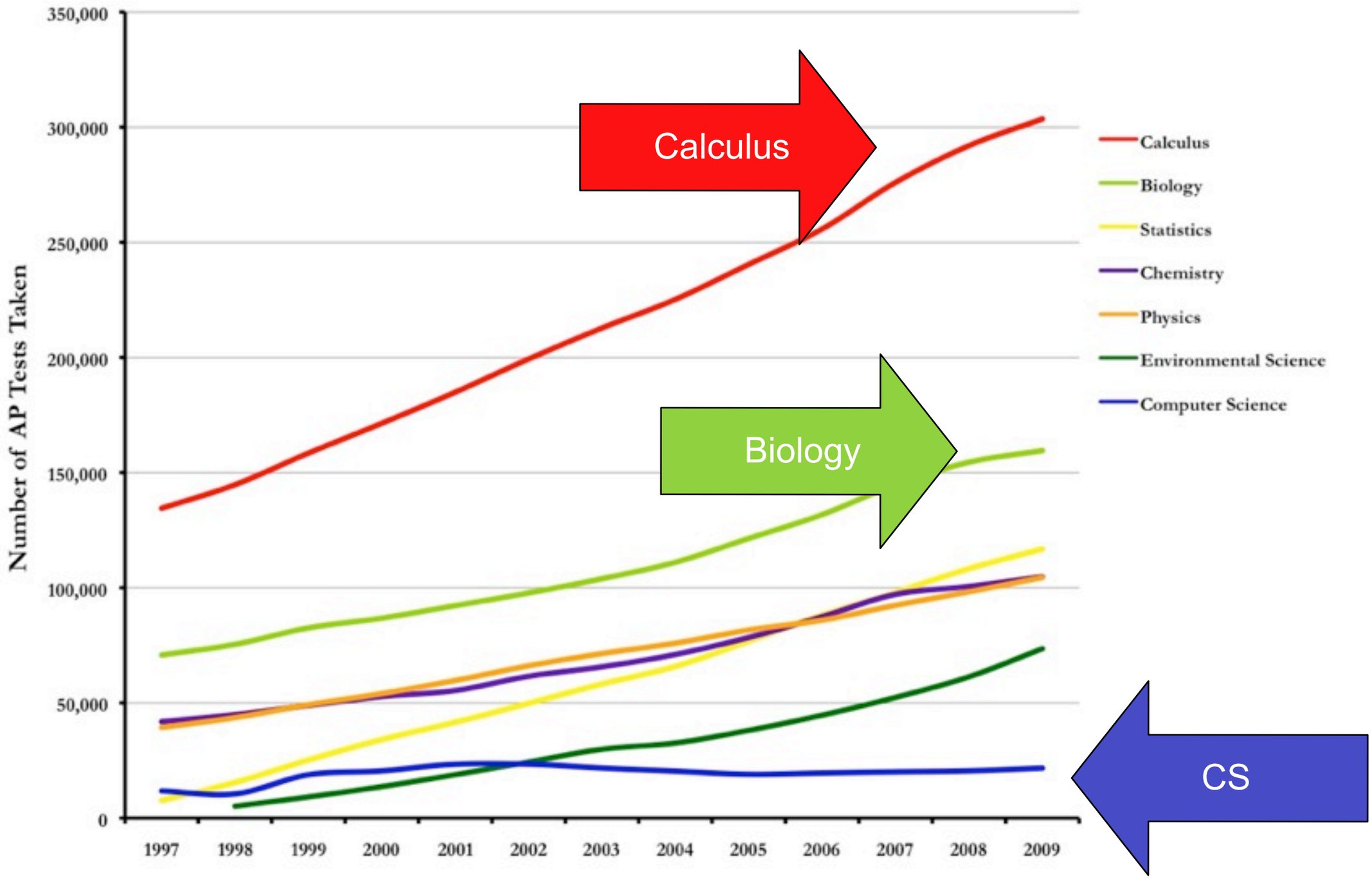
73% of states require computer “skills” for graduation. Only 37% require CS “concepts”



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!

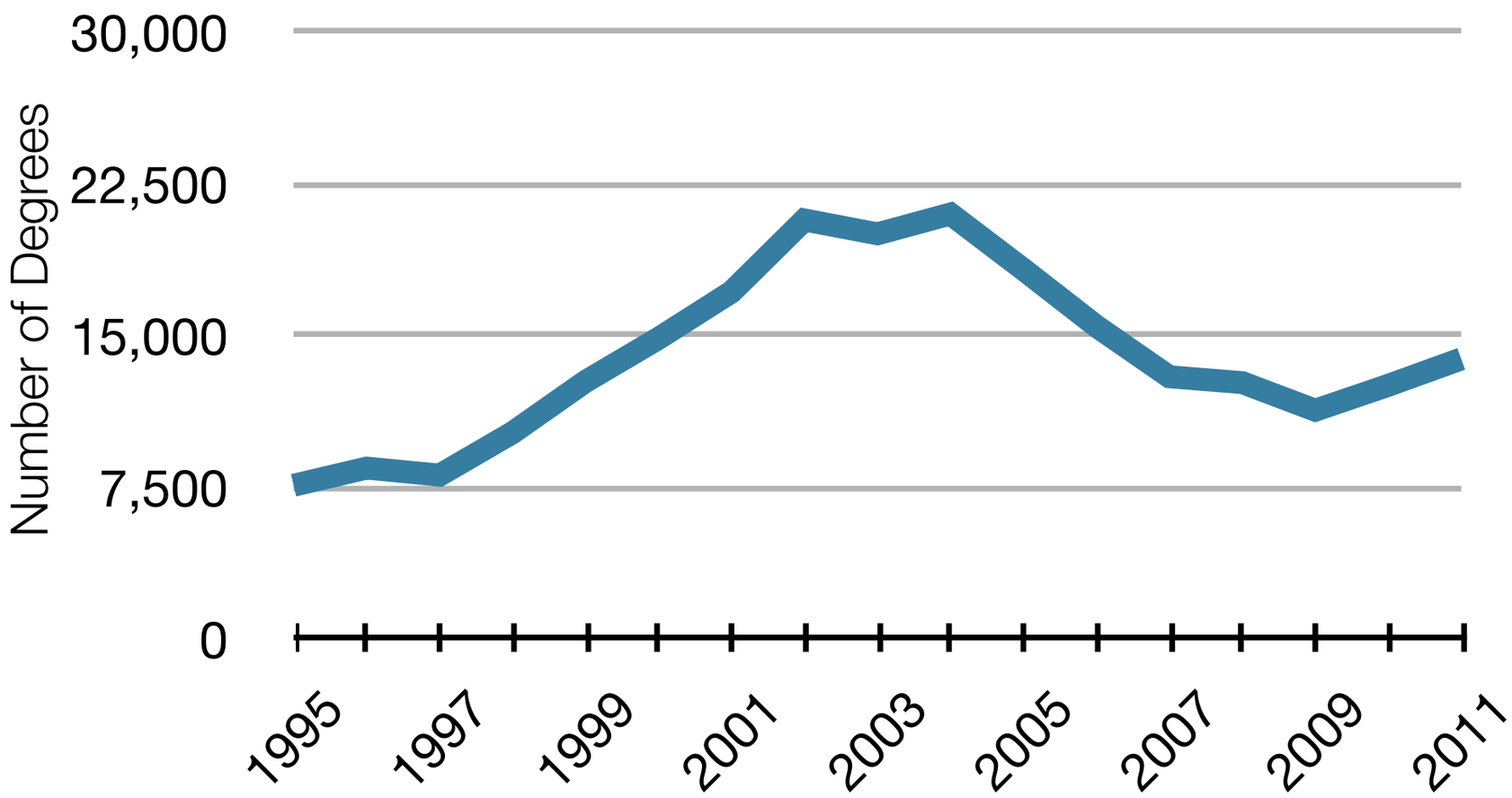


http://www.acm.org/public-policy/AP%20Test%20Graph%202009.jpg

Computer Science undergraduate enrollment is low...

2010-2011 CRA Taulbee Survey:

Figure 2. BS Production (All Departments)



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	
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 aliens (4960 to US citizens)

Table 9. Master's Degrees Awarded by Ethnicity								
	CS		CE		I		Total	
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	

— *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 weapon's scientists at MIT during the Cold War.

Just 67/1275 (5%) PhDs went into Information Assurance

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: Biomedica/ 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%

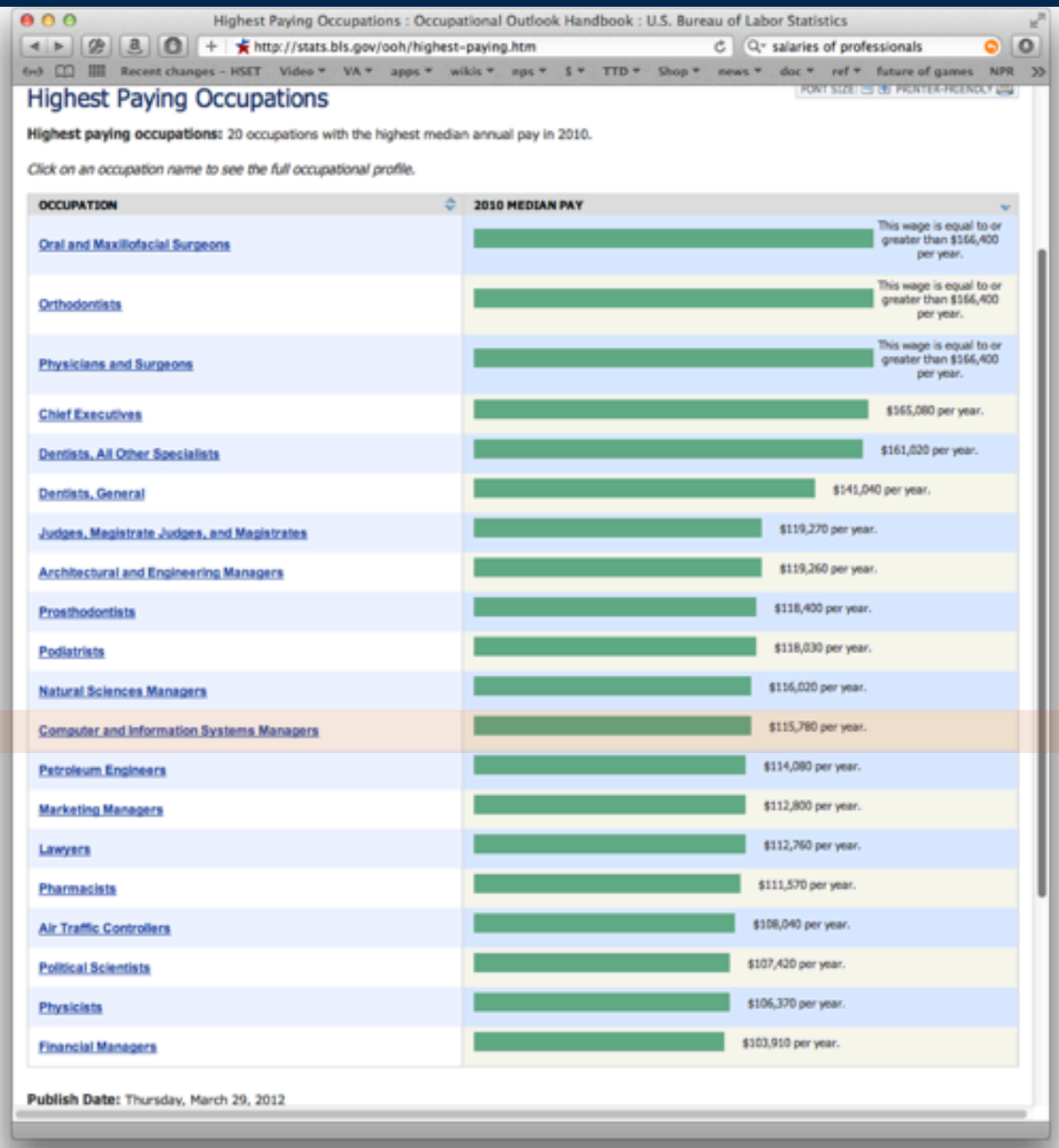
Security should be taught to everyone, but we need specialists

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

Highest paying occupations:

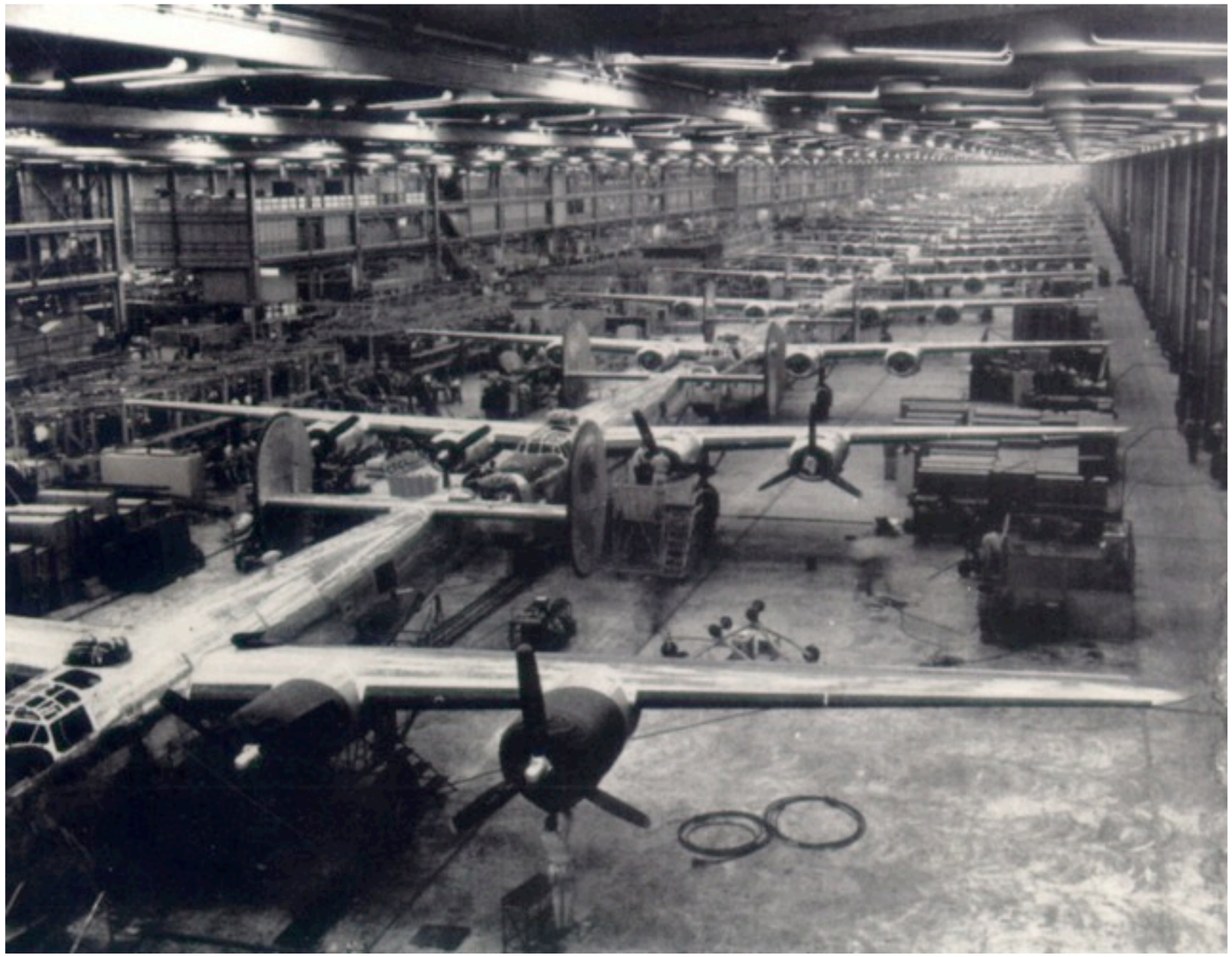
- Medical: >$166,400
- CEOs: $165,080
- Dentists: $161,020
- Judges: $119,260
- …
- Computer Scientists: $115,070
- …
- Lawyers: $112,760

—*Source: Bureau of Labor Stats*



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

Manufacturing policy

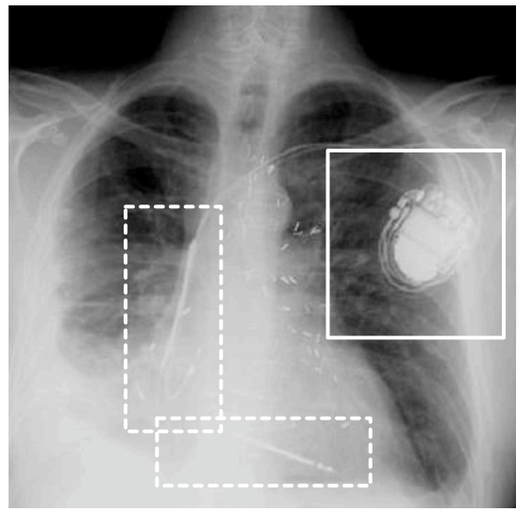


The USA did not build WW2 bombers in German aircraft factories.

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

… because computers are everywhere.

50 microprocessors per average car



2008: demonstrated wireless attack on implantable pacemakers

- April 2012: McAfee announces successful wireless attack on insulin pump.
  - —*DDOS for 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.

The most recent bug, found in a wide range of high-definition TVs from Samsung, was disclosed on Thursday by Luigi Auriemma, an Italy-based researcher who regularly finds security flaws in Microsoft Windows, video games, and even the industrial-strength systems used to control dams, gas refineries, and other critical infrastructure. 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

[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

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, like the ones that hit eight hospitals in Toronto.

Earlier this week, Toronto police announced that eight area hospitals had been recent targets for ATM skimming attacks. Over the past six months, authorities believe fraudsters targeted these hospitals because of traffic and the high-volume cash dispensers in these locations. But security experts say the ATMs were more likely hit because they're easy targets.

"ATM placement in establishments like hospitals and 'cash only' enterprises seems to be an afterthought to security, with the installation of ATMs in really remote areas of the building, where fraudsters can easily tinker with skimming-device placement and retrieval without the threat of immediate capture," says John Buzzard, who monitors card fraud for FICO's Card

Cell phones (&c) 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 program managers 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 cybersecurity, our systems seem to be growing more vulnerable every year.