# The Cyber Security Mess

Simson L. Garfinkel

April 4, 2018

Spamhause

Photos from https://pixabay.com

# The Cybersecurity Mess

**Abstract:**

Why is it so hard to secure computers? After more than 40 years of concerted effort in network security, why can't we keep the hackers out?

The problem, I argue, is not the practice of computer security, but its definition, it's very conception. As we are accepted it, computer security is what social scientists call a "wicked problem" — a poorly defined, high-impact problem for which the solution depends upon satisfying many competing stakeholders and conflicting goals. Solving the cybersecurity mess means addressing both *technical factors*—factors that dominate the discussion—and *nontechnical factors*, which reflect deep, divisive political, social, and economic problems without our society as a whole. This problems, which include the decline of the US manufacturing base, the failure of our schools at science, technology, engineering and math (STEM), an inherent power struggle between the makers of information systems and their users, and our inability to frame a coherent immigration policy, are core reasons why we are unable to make technical progress. While it is certainly possible that the need to secure our computers may force us to find a general solution to these problems, such Pollyannish hopes seem unlikely.

This talk follows the history of cybersecurity efforts, showing that while there's nothing new under the sun, things really are getting worse. And while there are little-used technologies that really can make computers dramatically more secure (such as typesafe languages, formal methods, and provably correct computer systems), these approaches are so expensive that they may never see widespread adoption.

So what's the solution? I propose that it's resilience, redundancy, heterogeneity, and regulation. Yes, this talk is designed to leave everyone in the audience both agreeing with the speaker, and angry at the speaker.

**Bio:** Simson Garfinkel is an adjunct lecturer at Georgetown University's Graduate School of Data Analytics and the Chief of the Center for Disclosure Avoidance at the US Census Bureau. He was previously a computer scientist at the National Institute of Standards and Technology (2015-2017) and, before that, an Associate Professor of Computer Science at the Naval Postgraduate School (2006-2015). Before earning his PhD in Computer Science from at MIT (2002-2005), he was an award-winning journalist and a serial entrepreneur. In 2012 he was elected a Fellow of the Association for Computing Machinery for his contributions to digital forensics and to computer security eduction.

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



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 subverted. And faced with a system that is beyond one’s technical hacking skills, an attacker can go around the security perimeter and use a range of other techniques, including social engineering, supply-chain insertion, or even kidnapping and extortion.

ILLUSTRATION BY YAREK WASZUL

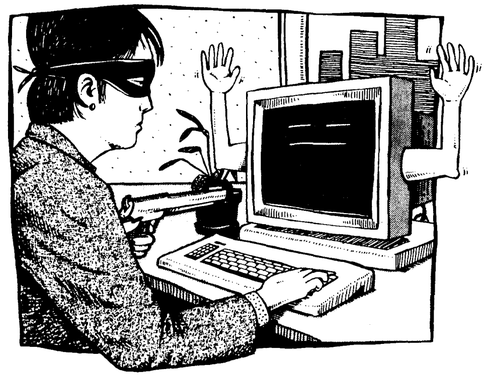
It may be that cybersecurity appears to be getting worse simply because society as a whole is becoming much more dependent upon computers. Even if the vulnerability were not increasing, the successful hacks can have significantly more reach today than a decade ago.

### 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 29 years trying to secure computers...



**An Introduction to Computer Security**
[Part 1]

**Simson L. Garfinkel**

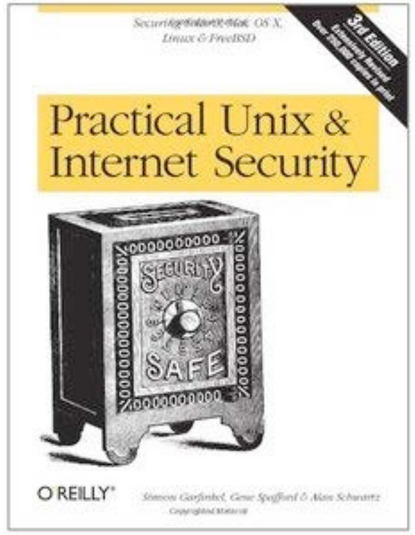
"Spies," "vandals," and "crackers" are out there, waiting to get into—or destroy—your databases.

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

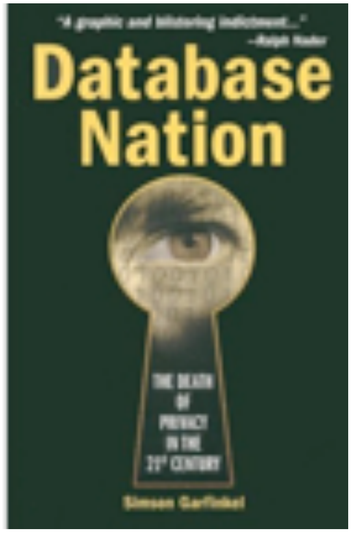
***The Practical Lawyer***
**Sept. 1987**

**System Security**



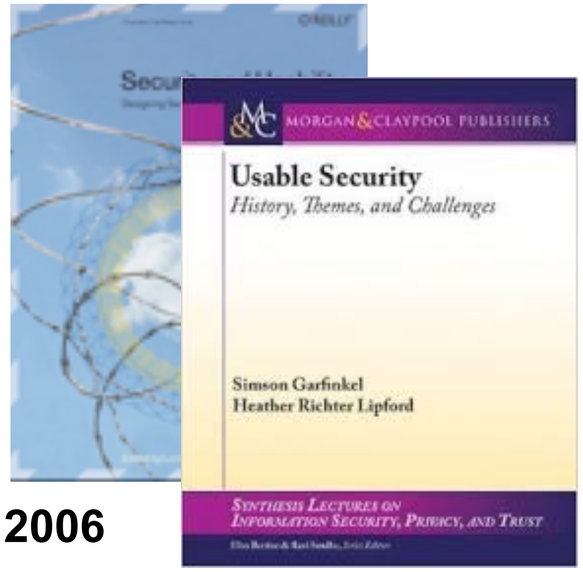

**1991**

**Privacy Policy**




**2000**

**Usable Security**




**2006**

**2014**

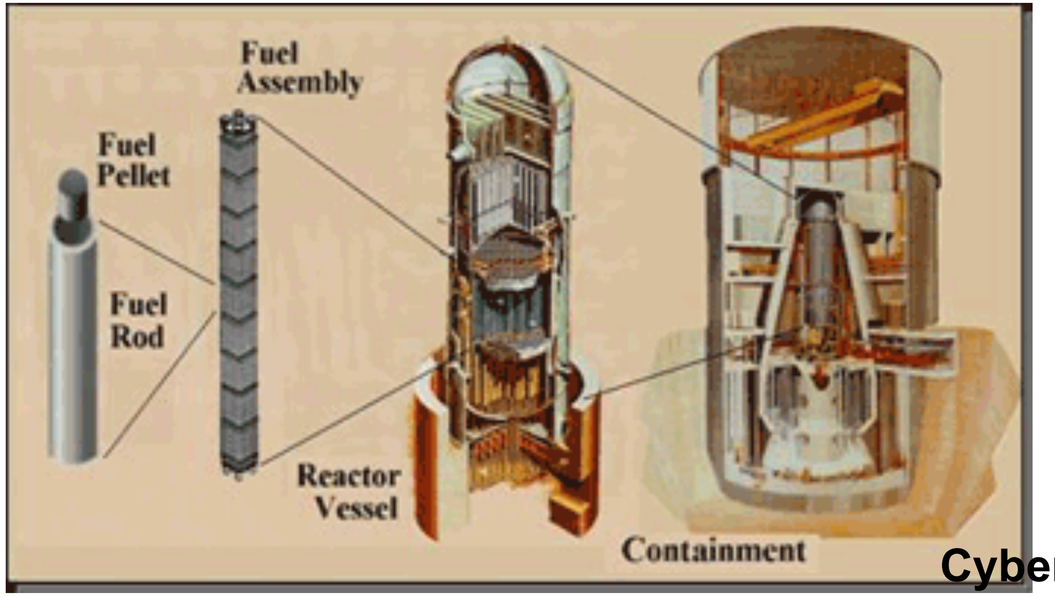
**Internet of Things**


**2006**

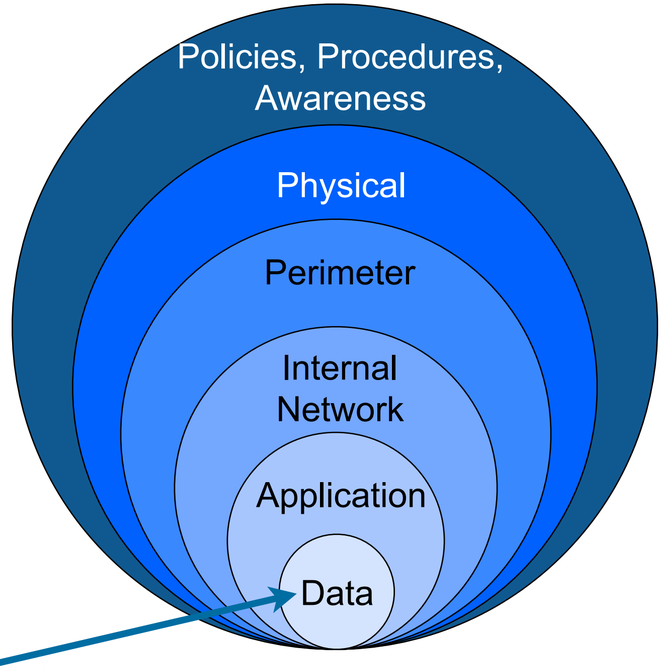
# Today's systems are less secure than those of the 1970s.

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

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




**Defense in depth of nuclear reactors**
http://www.nrc.gov/about-nrc/regulatory/research/soar/soarca-accident-progression.html




**Cyber can directly target inner defenses**

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

B&N Nook Color, An Energy Star Ally.


# Today we expect computers to crash

**We also expect them to be hacked.**


The solution is not better security

# Cybersecurity impacts the real world.


**(Cyber is In Real Life.)**

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

RISK ASSESSMENT / SECURITY & HACKTIVISM

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

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

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

BLACK HAT HACKING 55

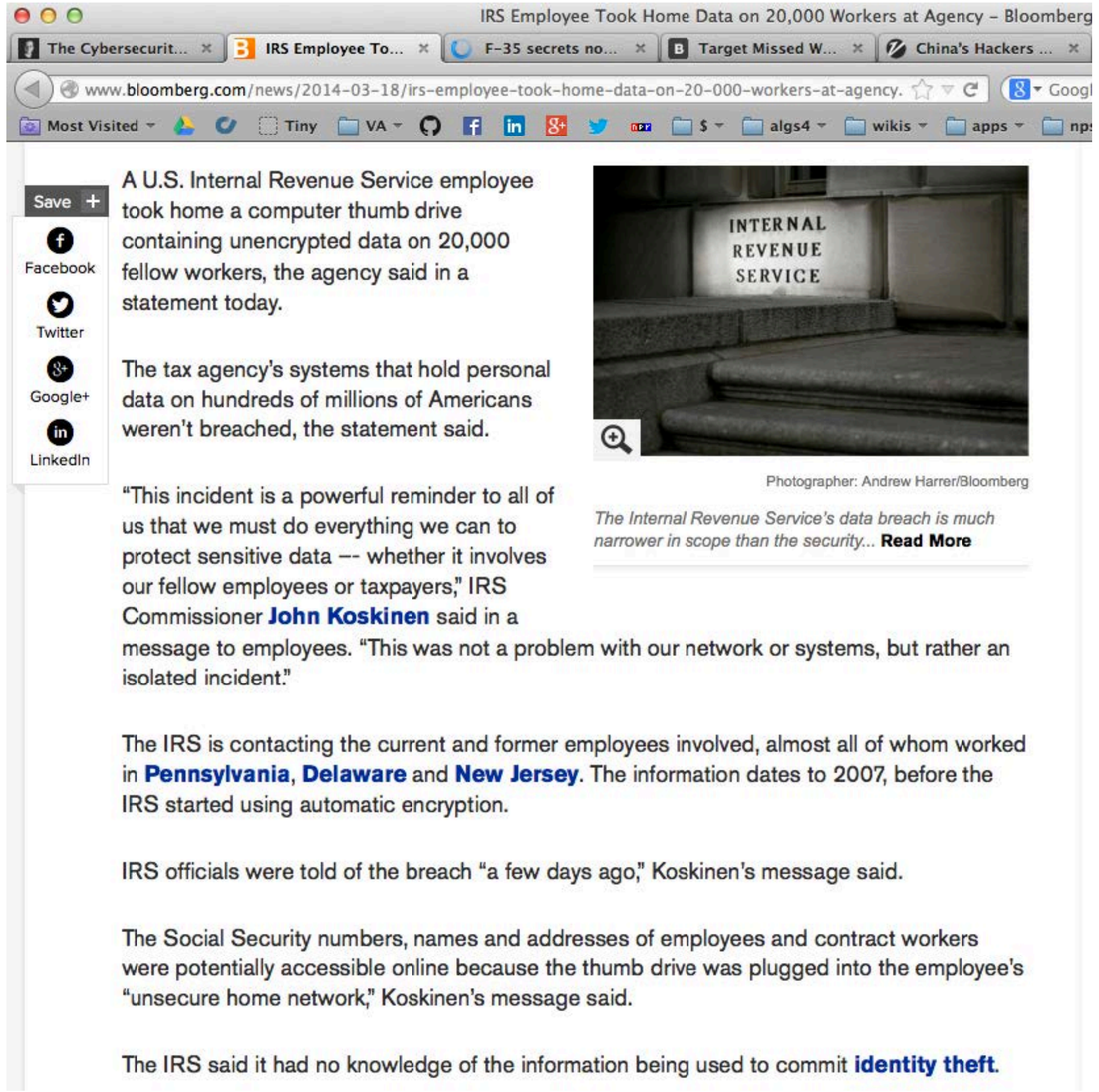
Wikipedia

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

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

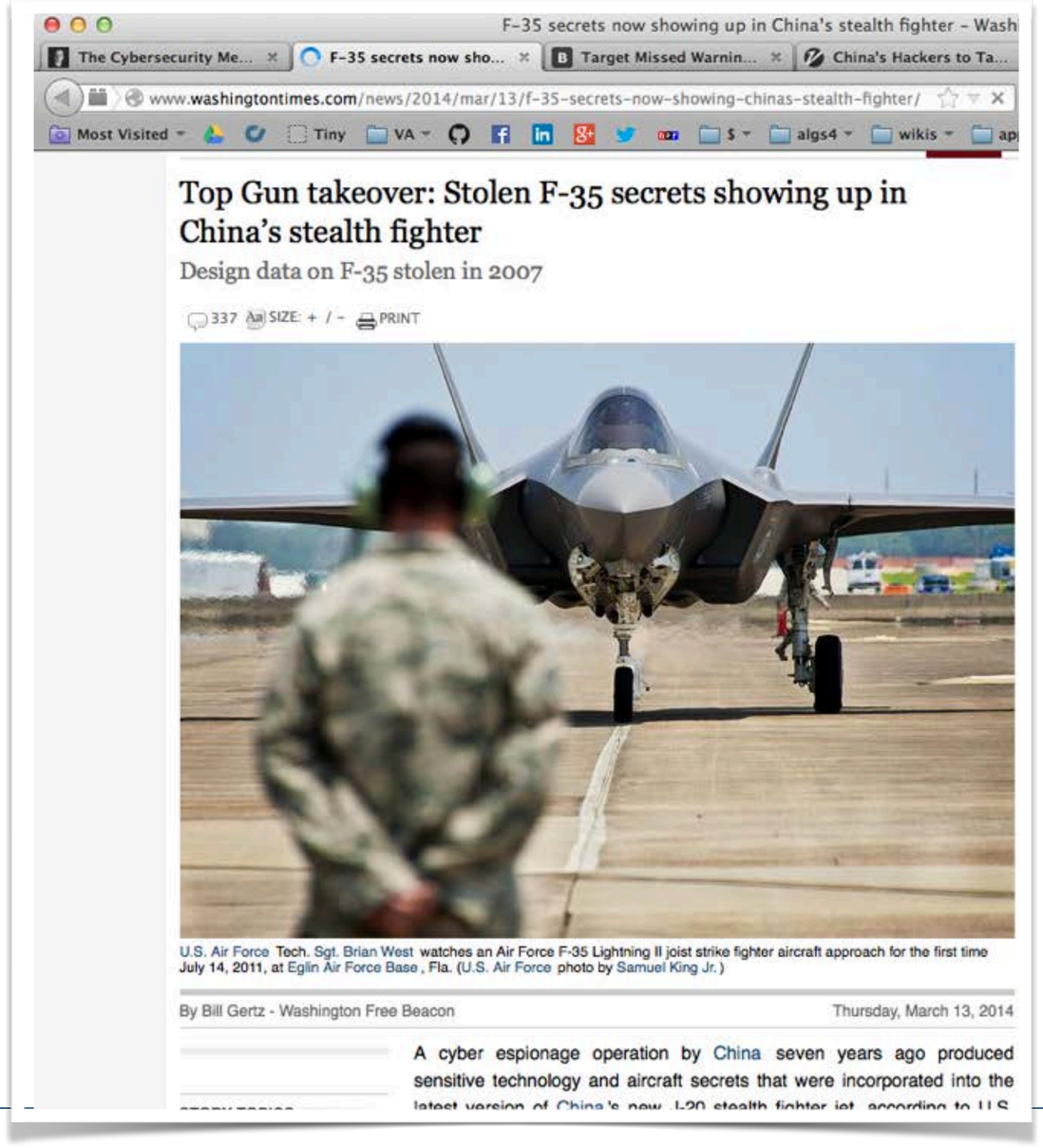
# May 2013

# March 2014:
# IRS Employee Took Home Data on 20,000 Workers




http://www.bloomberg.com/news/2014-03-18/irs-employee-took-home-data-on-20-000-workers-at-agency.html

# March 2014:
# Stolen F-35 secrets show up in China's stealth Fighter



# March 2014: Target ignored alarms before hack.

Target Missed Warnings in Epic Hack of Credit Card Data – B

The Cybersecurity Mess – Si... | Target Missed Warnings in E... | China's Hackers to Target U.... | For

www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-da

Most Visited | Tiny | VA | $ | algs4 | wikis

Bloomberg.com | Businessweek.com | Bloomberg TV | Premium

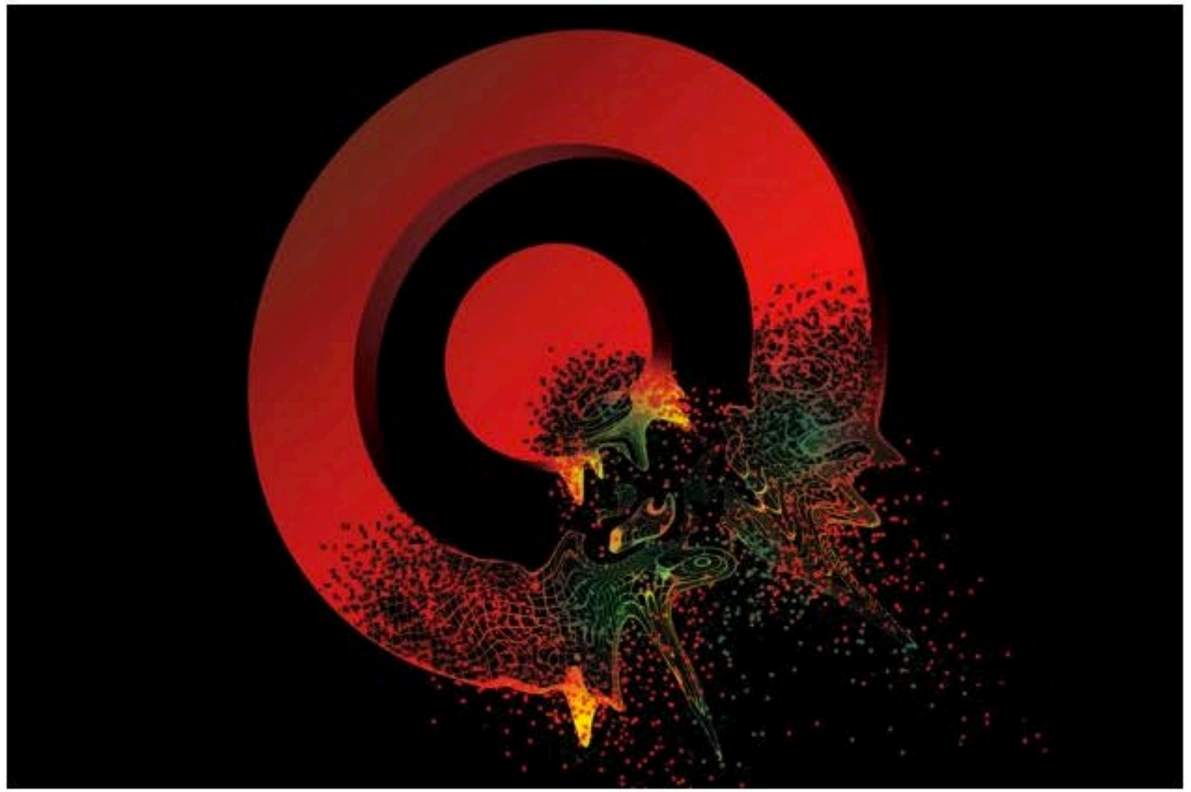
**BloombergBusinessweek**
**Technology**

Global Economics | Companies & Industries | Politics & Policy | Technology | Markets & Finance | Innovation & Design | Lifestyle

Features

## Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

By Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack | March 13, 2014



*(Corrects to identify Romania in a map accompanying the story.)*

The biggest retail hack in U.S. history wasn't particularly inventive, nor did it appear destined for success. In the days prior to Thanksgiving 2013, someone installed malware in Target's (TGT) security and payments system designed to steal every credit card used at the company's 1,797 U.S. stores. At the critical moment—when

# June 2015: OPM Data Breach
# 19.7 million individuals applying for security clearances

# OPM's Strong Authentication Capabilities before hack: 1% — OMB FISMA Report, Feb. 27, 2015



As seen in **Table 4** below, numerous agencies have made no progress meeting the Strong Authentication CAP goal. SBA, NRC, HUD, Labor, and State were all at 0% Strong Authentication implementation at the end of FY 2014. The blue cells indicate performance that fell below the 75% target across all CFO Act agencies. Excluding DOD, the percentage of CFO Act agency users for whom Strong Authentication is required is 41%.[5]

**Table 4: Strong Authentication Capabilities FY 2013 & FY 2014**

| Agency | Strong Authentication FY 2013 (%) | Strong Authentication FY 2014 (%) |
|---|---|---|
| Labor | 0 | 0 |
| HUD | 0 | 0 |
| NRC | 0 | 0 |
| SBA | 0 | 0 |
| State | 1 | 0 |
| OPM | 0 | 1 |
| USAID | 0 | 3 |
| USDA | 6 | 6 |
| VA | 4 | 10 |
| NSF | 0 | 19 |
| Energy | 9 | 29 |
| DOT | 7 | 31 |
| Interior | 0 | 36 |

IEEE Security & Privacy, Sept/Oct 2016

THE SECURITY–USABILITY TRADEOFF MYTH

Secure and Usable Enterprise Authentication:
Lessons from the Field

Mary Theofanos, Simson Garfinkel, and Yee-Yin Choong | National Institute of Standards and Technology

Surveys of US Defense and Commerce department employees show that using Personal Identity Verification and Common Access Cards for two-factor authentication results in improved usability and security.

Over the past 15 years, the US government has deployed millions of multifunction smart cards to its workforce with the goal of using the cards to grant both physical access to facilities and logical access to information systems. The deployment and use of these cards has been inconsistent across different government agencies. The Department of Defense (DoD), with its Common Access Card (CAC), recently announced that 98 percent of its information systems had been adapted to use the smart cards, thus providing these systems with strong two-factor user authentication. Other parts of the government are significantly behind the DoD, with logical authentication deployment rates ranging from 0 to 95 percent.[1]

Practical systems for multifactor authentication have been on the market for roughly 30 years, but it's only in the past few years that industry and academia have made a concerted effort to migrate users away from pure password systems. These groups can benefit from the US government's experience in deploying multifactor systems and by comparing the results of different deployment strategies.

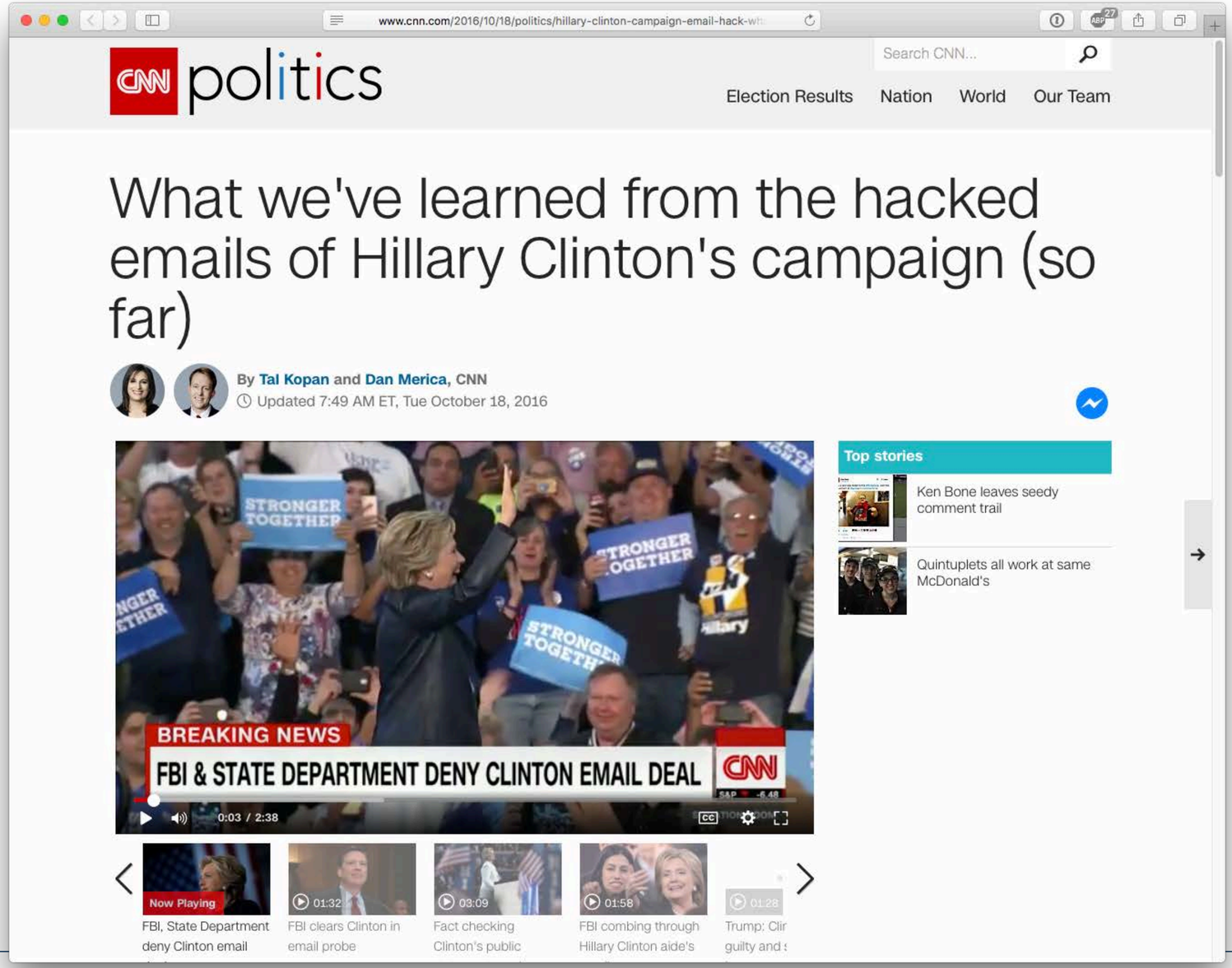
In this article, we present the historical background that led to different deployment strategies within the US's defense and civilian executive branch agencies. We then present the results of two large-scale surveys of password usage in the DoD and the US Department of Commerce (DoC). Both surveys were completed before the US government's 2015 Cyber Sprint program, initiated by the Office of Management and Budget (OMB) to address that year's high-profile cyberintrusions.[2] The DoD aggressively implemented the CAC on many of its business systems, while DoC was less aggressive in its Personal Identity Verification (PIV) implementation. Thus, comparing these two departments' employee reports and attitudes about password usage provides insight into the effect of successfully deploying an easy-to-use, strong, two-factor authentication method in a large organization. Our sample includes responses from 28,481 DoD and 4,573 DoC employees.

## Smart Card–Based Authentication

Smart card–based authentication relies on the card and a six- to eight-digit numeric PIN. Unlike passwords that must be changed routinely, PINs are generally not changed for the life of the card. Our survey found that it was rare for DoD users to mistype or forget their PINs—common failure modes with passwords. The security advantage comes from the use of public-key infrastructure (PKI)-based authentication, rather than

14 September/October 2016 Copublished by the IEEE Computer and Reliability Societies 1540-7993/16/$33.00 © 2016 IEEE

# Summer 2016...
# “Russia, if you can hear me, I hope you can find the 30,000 missing e-mails,”



# John [Podesta] needs to change his password immediately, and ensure that two-factor authentication is turned on...

**From:** Charles Delavan <cdelavan@hillaryclinton.com>
**Date:** March 19, 2016 at 9:54:05 AM EDT
**To:** Sara Latham <slatham@hillaryclinton.com>, Shane Hable <shable@hillaryclinton.com>
**Subject: Re: Someone has your password**

Sara,

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this is done ASAP.

***The New York Times*, December 13, 2016**

# “The cyber” is mess: it’s technical and social.

**Most attention is focused on technical issues:**

- Malware and anti-viruses
- Access controls, authentication & cryptography
- Supply chain issues
- Cyberspace as a globally connected “domain”

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

- Education & career paths
- Immigration
- Manufacturing policy

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

# What do we know about cyber security today?

# Cyber Security: the term is undefined.

**There is no good definition for “cyber”**

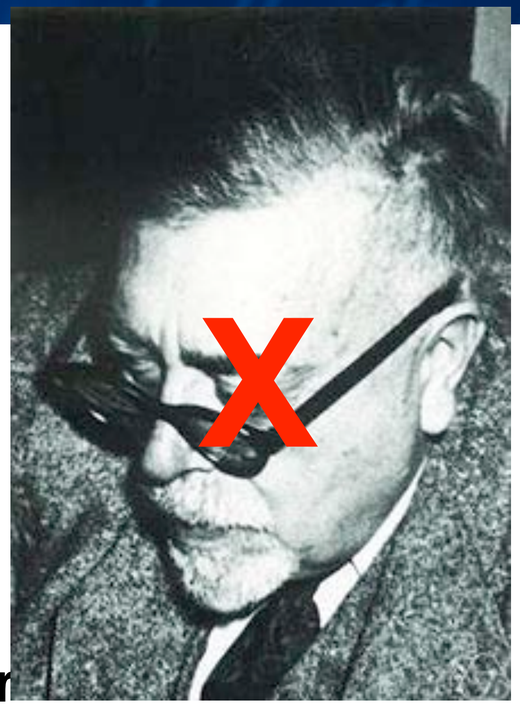
- ~~Something having to do with cybernetics~~
- Computers?
- Computer networks?
- Hacking?
- Using “network security” to secure desktops & servers?

**There is no way to *measure* the security of the “cyber**

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

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

**“Cybernetics”**



**Norbert Weiner**
**1948**

**“Cyberspace”**

**William Gibson**
**1982**

# We *can* measure expenditures.
# Cyber Security is expensive.

**Global cyber security spending: $60 billion in 2011**

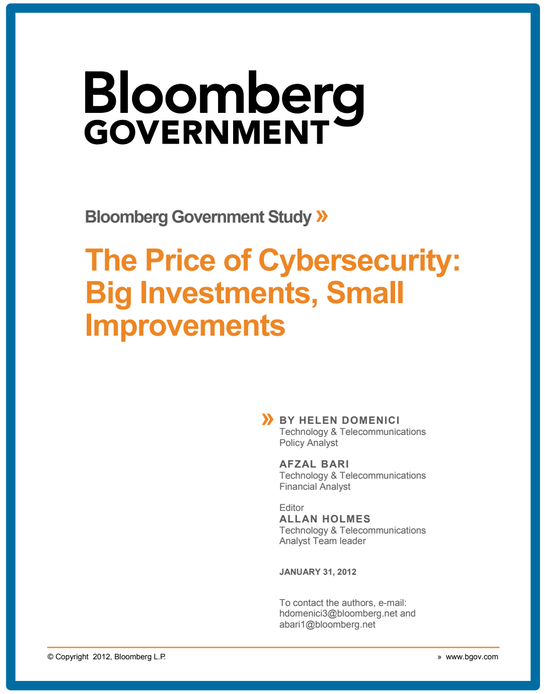
- *Cyber Security M&A,* pwc, 2011

**172 Fortune 500 companies surveyed:**

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

**If they raise spending...**

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


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

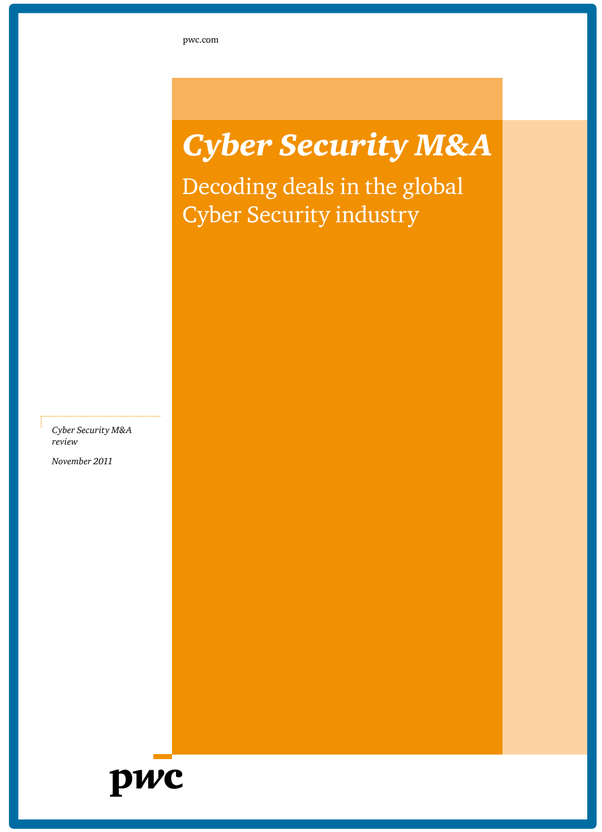
Editor
ALLAN HOLMES
Technology & Telecommunications
Analyst Team leader

JANUARY 31, 2012

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



» www.bgov.com


pwc.com

Cyber Security M&A

Decoding deals in the global Cyber Security industry

*Cyber Security M&A review*

*November 2011*

pwc

**95% is not good enough.**

**Spending more money does not make a computer more secure.**

# Expenditures are increasing...

**$73.7 billion in 2016**

—*International Data Corporation*
*http://fortune.com/2016/10/12/cybersecurity-global-spending/*

**$1 trillion spent globally from 2015 to 2021 = $200B/year**

—*Cybersecurity Ventures,*
*http://cybersecurityventures.com/*

# Paradox:
# Cyber security research makes computers less secure!

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

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

# Cyber Security is an “insider problem.”

**bad actors**

**good people with bad instructions**

**remote access**

**malware**

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

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

*—but we can’t stop insiders.*

**Ames**

**Hanssen**

**Manning**

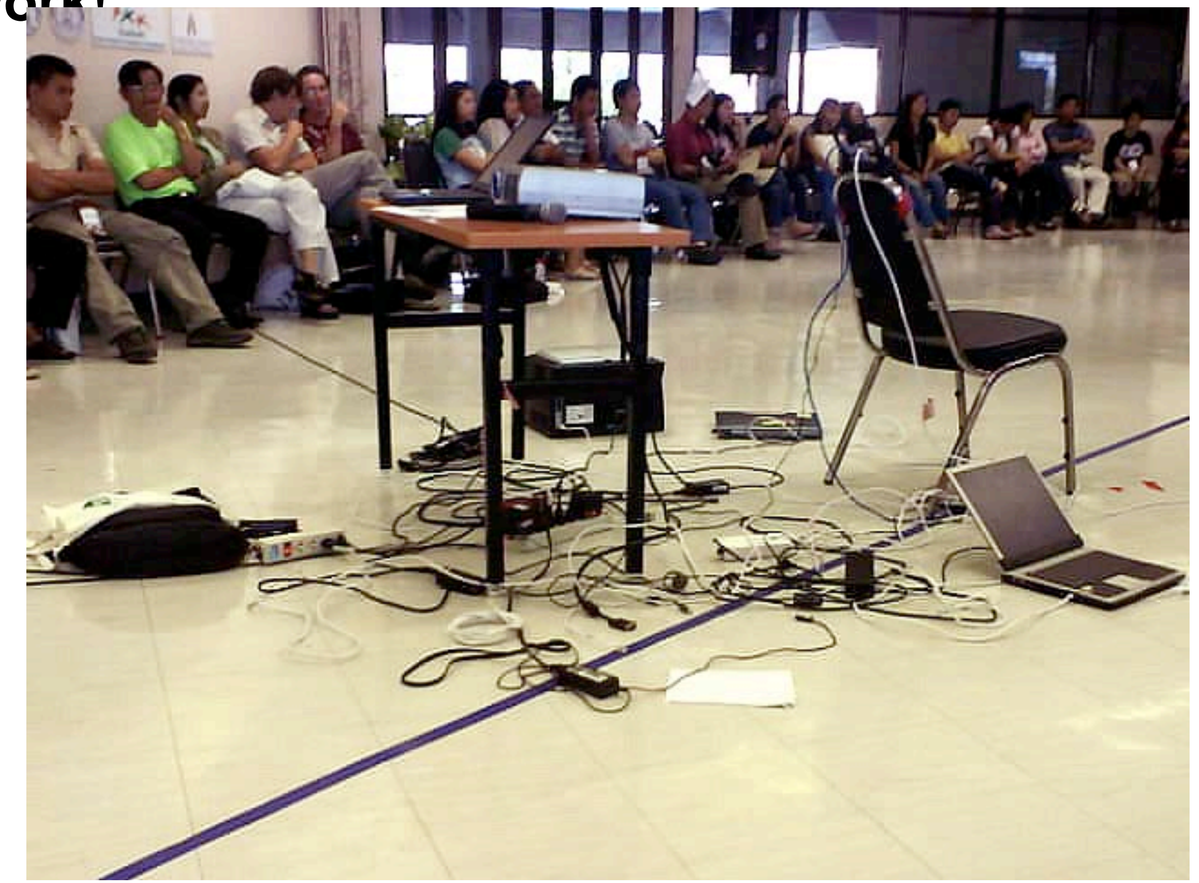
**Snowden**

# Cyber Security is a “network security” problem.

**We can’t secure the hosts, so secure the network!**

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





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

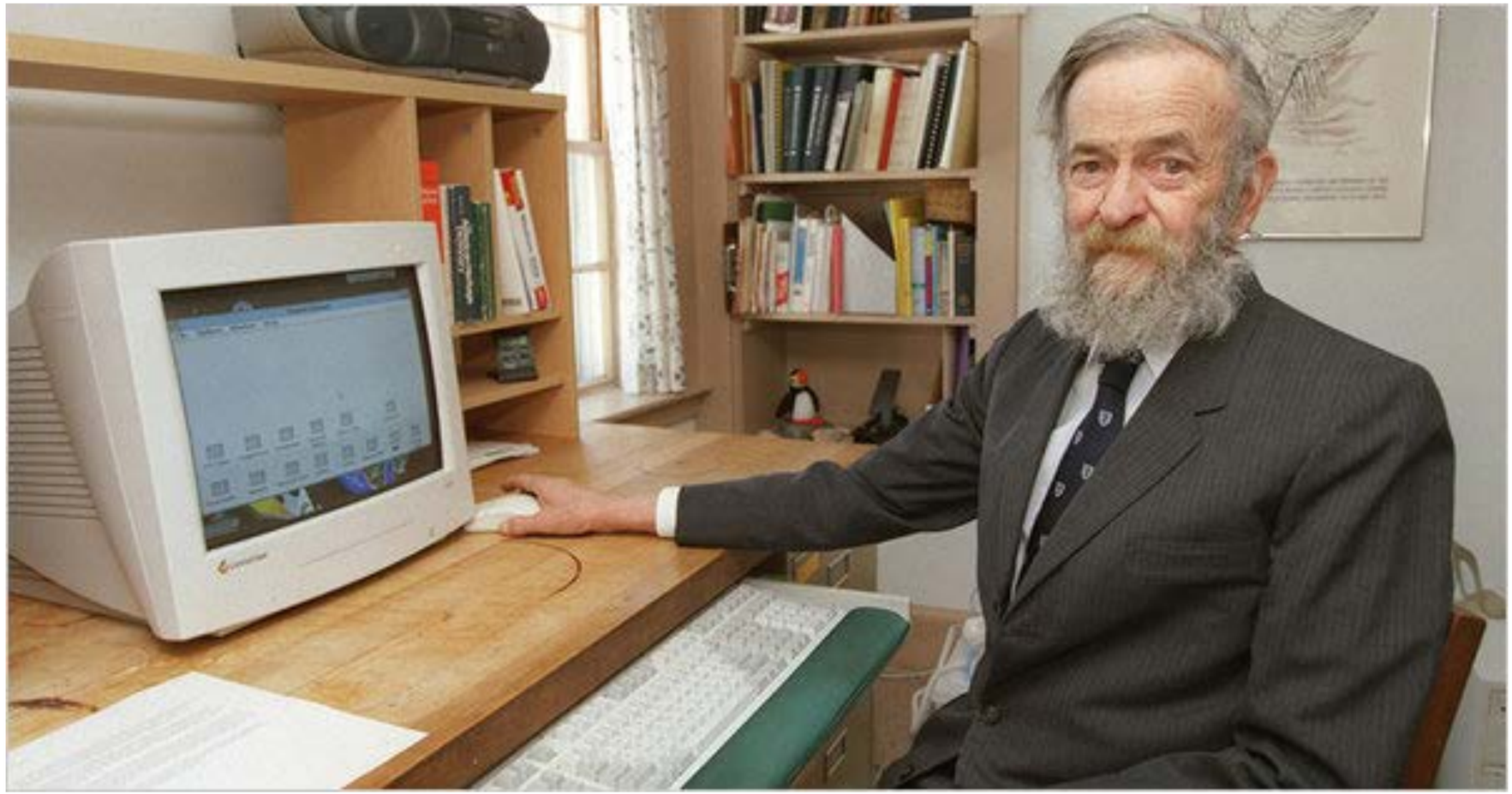
**But strong crypto limits visibility into network traffic, and...**

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

http://www.npr.org/2013/10/14/232048549/are-irans-centrifuges-just-few-turns-from-a-nuclear-bomb

**Iranian President Mahmoud Ahmadinejad inspects nuclear centrifuges • March 8, 2007**

# “to a first approximation, every computer in the world is connected to every other computer.” — Dr. Robert Morris



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*

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

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

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, Harold T.shapiro — A Dialogue on Competitiveness (Summer 1988) HTML or PDF

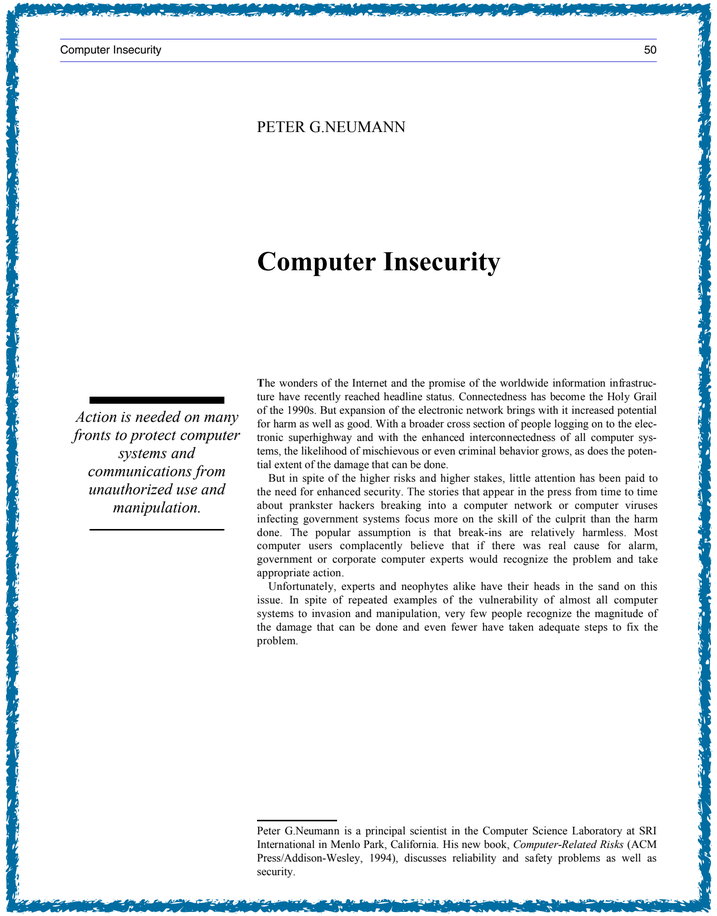
Erich Bloch — MANAGING FOR CHALLENGING TIMES: A National Research Strategy (Winter 1986) HTML or PDF

John A. Armstrong — University Research: New Goals, New Practices HTML or PDF

Roland W. Schmitt — Fulfilling the Promise of Academic Research (Summer 1991) HTML or PDF

Larry R. Johnson — Putting Maglev on Track (Spring 1990) HTML or PDF

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



Computer Insecurity 50

PETER G.NEUMANN

**Computer Insecurity**

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

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

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

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

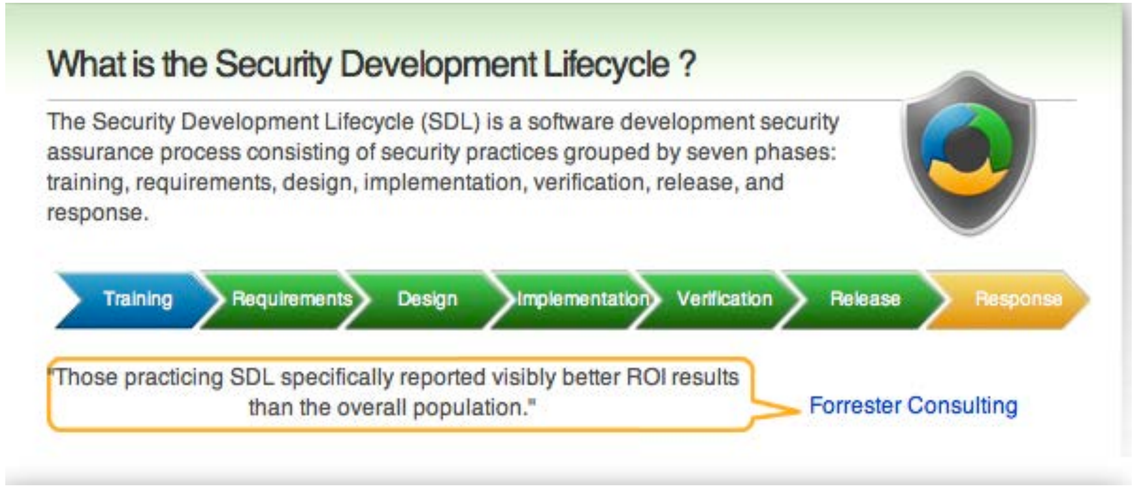
Peter G.Neumann is a principal scientist in the Computer Science Laboratory at SRI International in Menlo Park, California. His new book, *Computer-Related Risks* (ACM Press/Addison-Wesley, 1994), discusses reliability and safety problems as well as security.

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

# Cyber Security is a “process” problem.

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

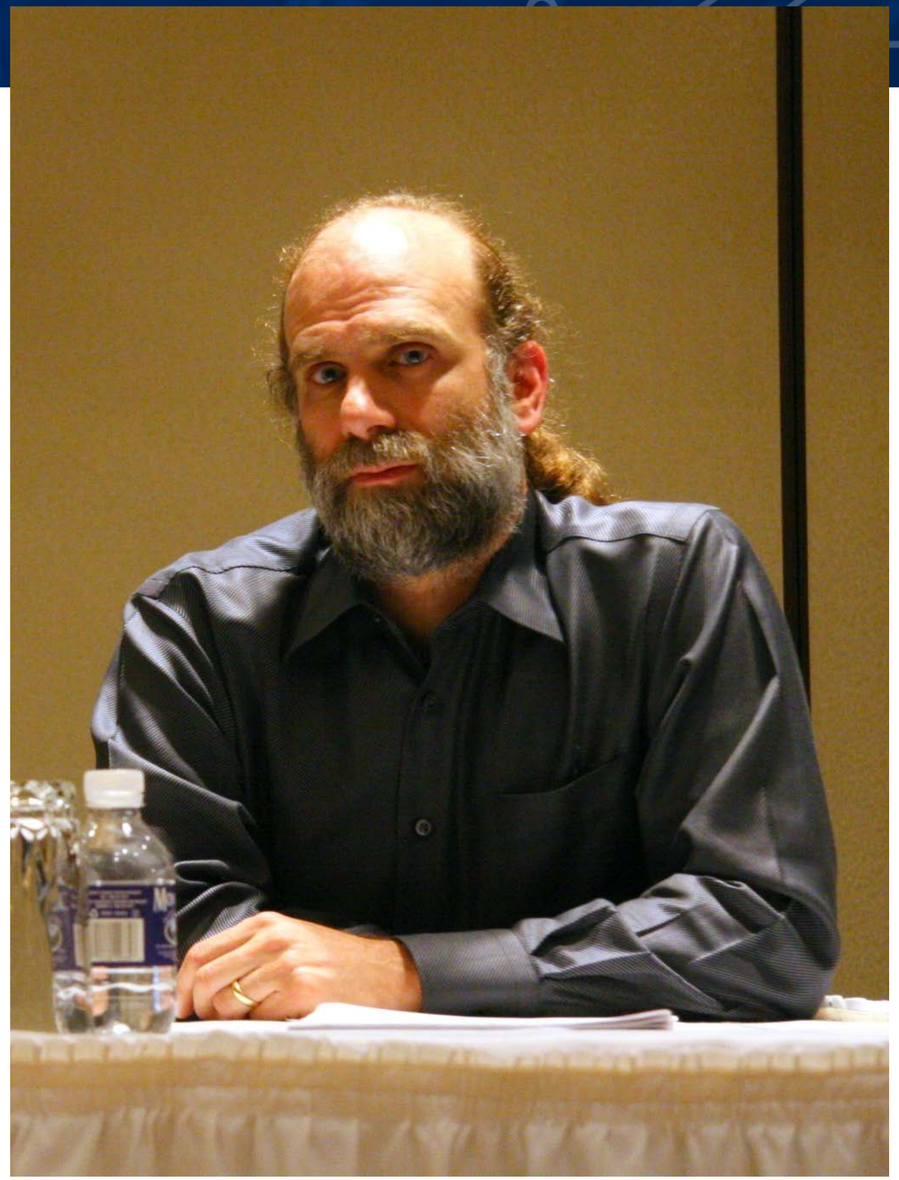
**Microsoft Security Development Lifecycle**




—*Few organizations can afford SDL.*

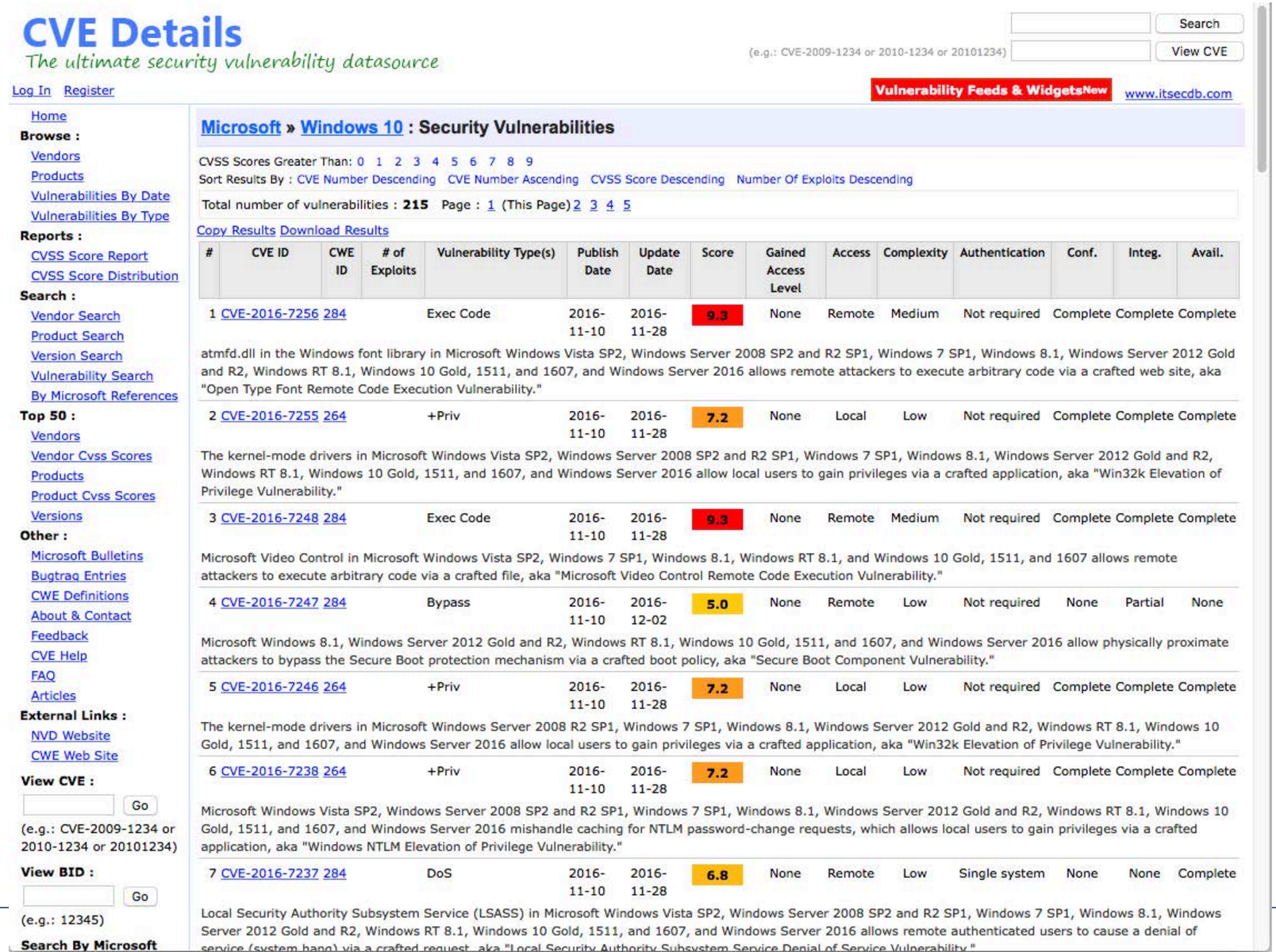
—*~~Windows 7 Windows 8~~ Windows 10 is still hackable...*

**“Security is a process, not a product”**



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

# Windows 10: 215 vulnerabilities...



CVE Details

*The ultimate security vulnerability datasource*

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) Search | View CVE

Log In Register

Vulnerability Feeds & Widgets New www.itsecdb.com

Home

**Browse :**
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type

**Reports :**
CVSS Score Report
CVSS Score Distribution

**Search :**
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References

**Top 50 :**
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions

**Other :**
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles

**External Links :**
NVD Website
CWE Web Site

**View CVE :**
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

**View BID :**
Go
(e.g.: 12345)

**Search By Microsoft**

## Microsoft » Windows 10 : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **215** Page : 1 (This Page) 2 3 4 5

Copy Results Download Results

| # | CVE ID | CWE ID | # of Exploits | Vulnerability Type(s) | Publish Date | Update Date | Score | Gained Access Level | Access | Complexity | Authentication | Conf. | Integ. | Avail. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | CVE-2016-7256 | 284 | | Exec Code | 2016-11-10 | 2016-11-28 | 9.3 | None | Remote | Medium | Not required | Complete | Complete | Complete |
| atmfd.dll in the Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka "Open Type Font Remote Code Execution Vulnerability." | | | | | | | | | | | | | | |
| 2 | CVE-2016-7255 | 264 | | +Priv | 2016-11-10 | 2016-11-28 | 7.2 | None | Local | Low | Not required | Complete | Complete | Complete |
| The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability." | | | | | | | | | | | | | | |
| 3 | CVE-2016-7248 | 284 | | Exec Code | 2016-11-10 | 2016-11-28 | 9.3 | None | Remote | Medium | Not required | Complete | Complete | Complete |
| Microsoft Video Control in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to execute arbitrary code via a crafted file, aka "Microsoft Video Control Remote Code Execution Vulnerability." | | | | | | | | | | | | | | |
| 4 | CVE-2016-7247 | 284 | | Bypass | 2016-11-10 | 2016-12-02 | 5.0 | None | Remote | Low | Not required | None | Partial | None |
| Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow physically proximate attackers to bypass the Secure Boot protection mechanism via a crafted boot policy, aka "Secure Boot Component Vulnerability." | | | | | | | | | | | | | | |
| 5 | CVE-2016-7246 | 264 | | +Priv | 2016-11-10 | 2016-11-28 | 7.2 | None | Local | Low | Not required | Complete | Complete | Complete |
| The kernel-mode drivers in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability." | | | | | | | | | | | | | | |
| 6 | CVE-2016-7238 | 264 | | +Priv | 2016-11-10 | 2016-11-28 | 7.2 | None | Local | Low | Not required | Complete | Complete | Complete |
| Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 mishandle caching for NTLM password-change requests, which allows local users to gain privileges via a crafted application, aka "Windows NTLM Elevation of Privilege Vulnerability." | | | | | | | | | | | | | | |
| 7 | CVE-2016-7237 | 284 | | DoS | 2016-11-10 | 2016-11-28 | 6.8 | None | Remote | Low | Single system | None | None | Complete |
| Local Security Authority Subsystem Service (LSASS) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote authenticated users to cause a denial of service (system hang) via a crafted request, aka "Local Security Authority Subsystem Service Denial of Service Vulnerability." | | | | | | | | | | | | | | |

# Cyber Security is a money problem.

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

- No ROI

**Chief Security Officers are in a no-win situation:**

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

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

- Spaf’s first principle of security administration
  *Practical Unix Security*, 1991

# Cyber Security is a “wicked problem”

**No clear definition**

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

**No “stopping rule”**

—*The problem can never be solved.*

**Solutions not right or wrong**

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

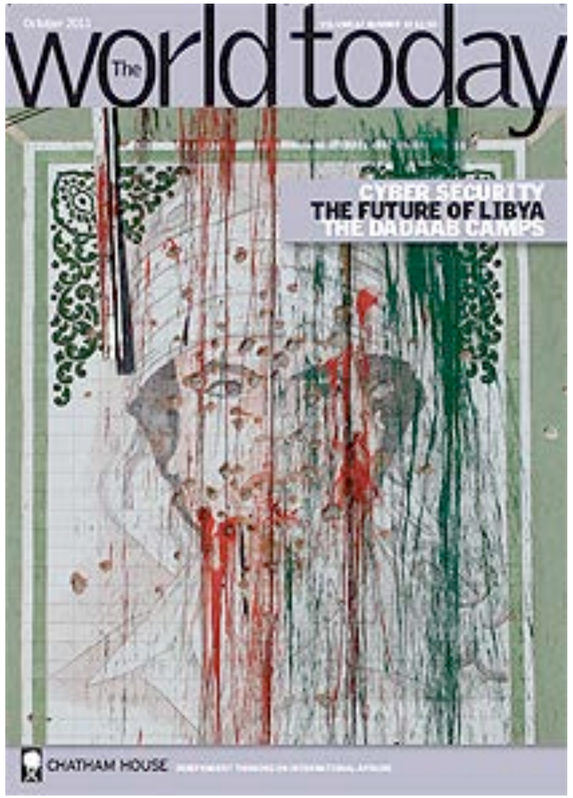
**Solutions are “one-shot” — no learning by trial and error**

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

**Every wicked problem is a symptom of another problem**

—*Rittel and Webber, “Dilemmas in a General Theory of Planning,” 1973*

—*Dave Clement, “Cyber Security as a Wicked Problem,” Chatham House, 2011*




**Chatham House**
**Oct. 2011**
**Cyber Security**
**As a Wicked Problem**

# Why is the cyber *so* hard?

# Cyber Security has an active, malicious adversary.

## The adversary...

Turns your bugs into exploits

Adapts to your defenses

Waits until you make a mistake

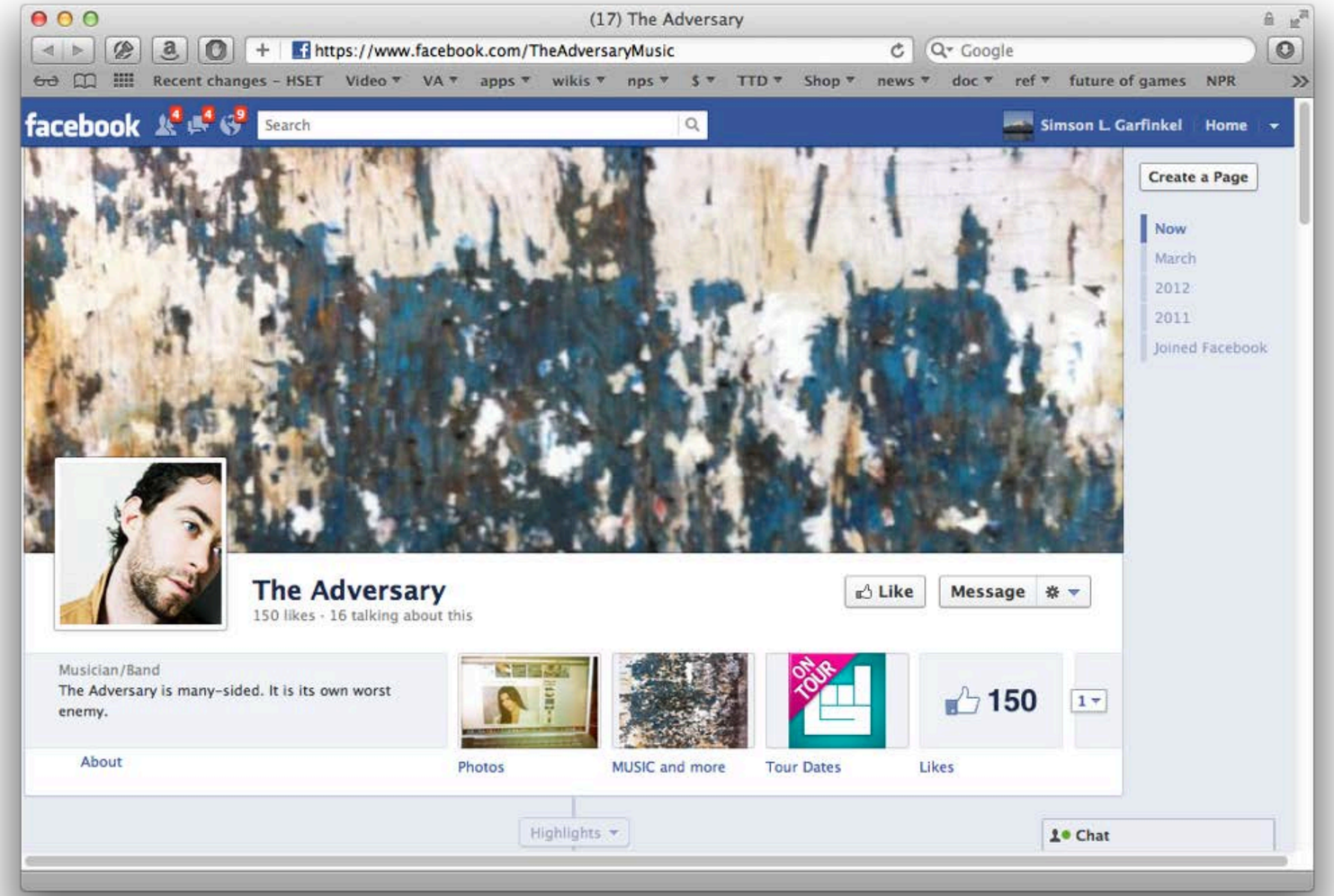
Attacks your employees when your systems are secure

*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!*

*—Elk Cloner, 1982*
*(Rich Skrenta, age 15)*



# For example...
# Compiler bugs are security vulnerabilities!

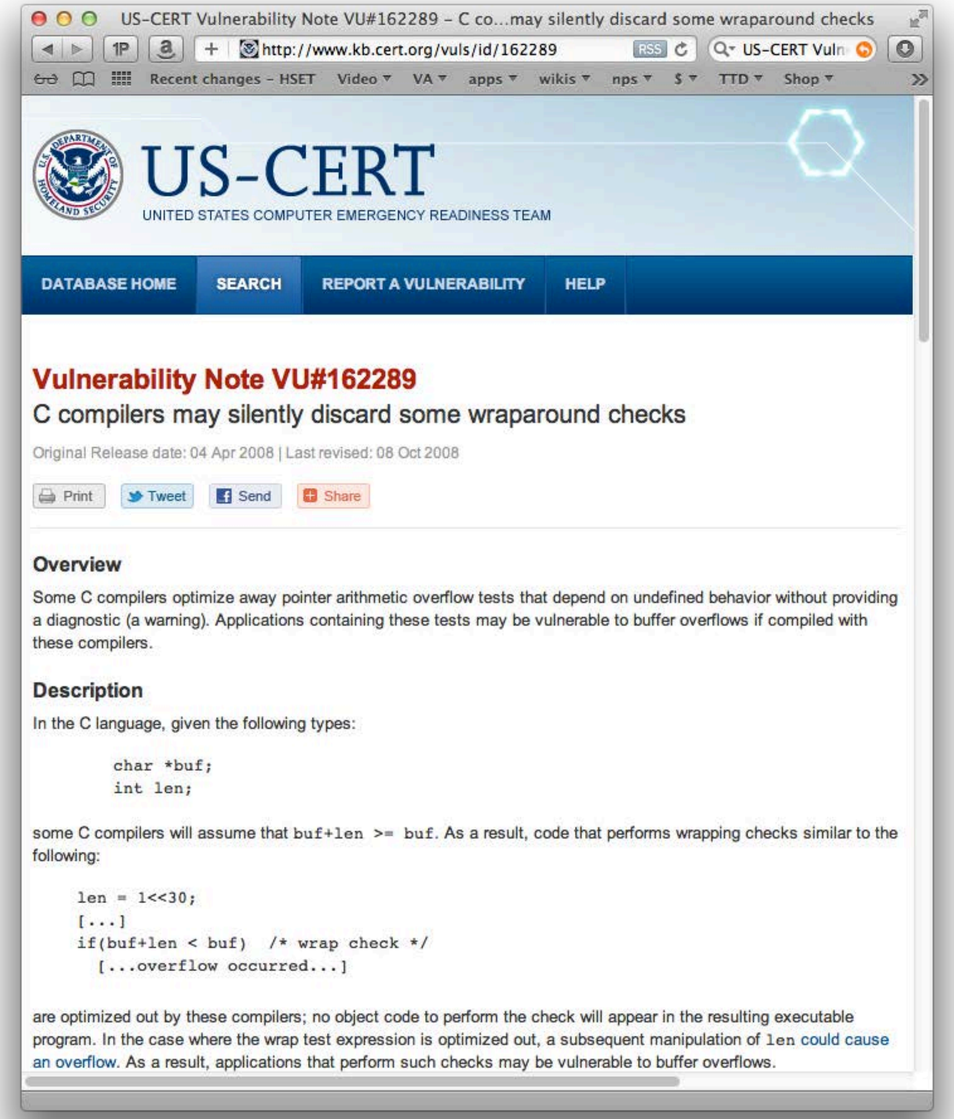
**Compilers are core technology used in software development.**

## We have seen:

- Optimizations to make programs run faster 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.*



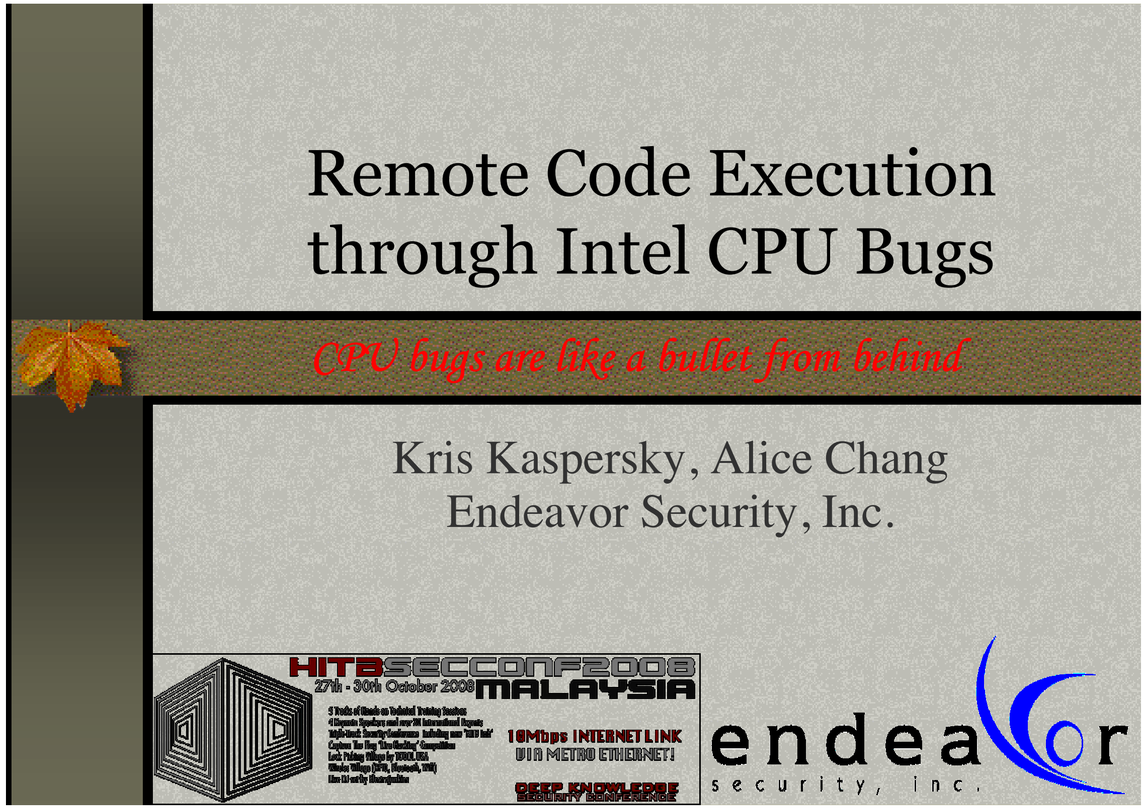
# Bugs in CPU silicon are remotely exploitable! Kaspersky (2010)

**This means:**

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

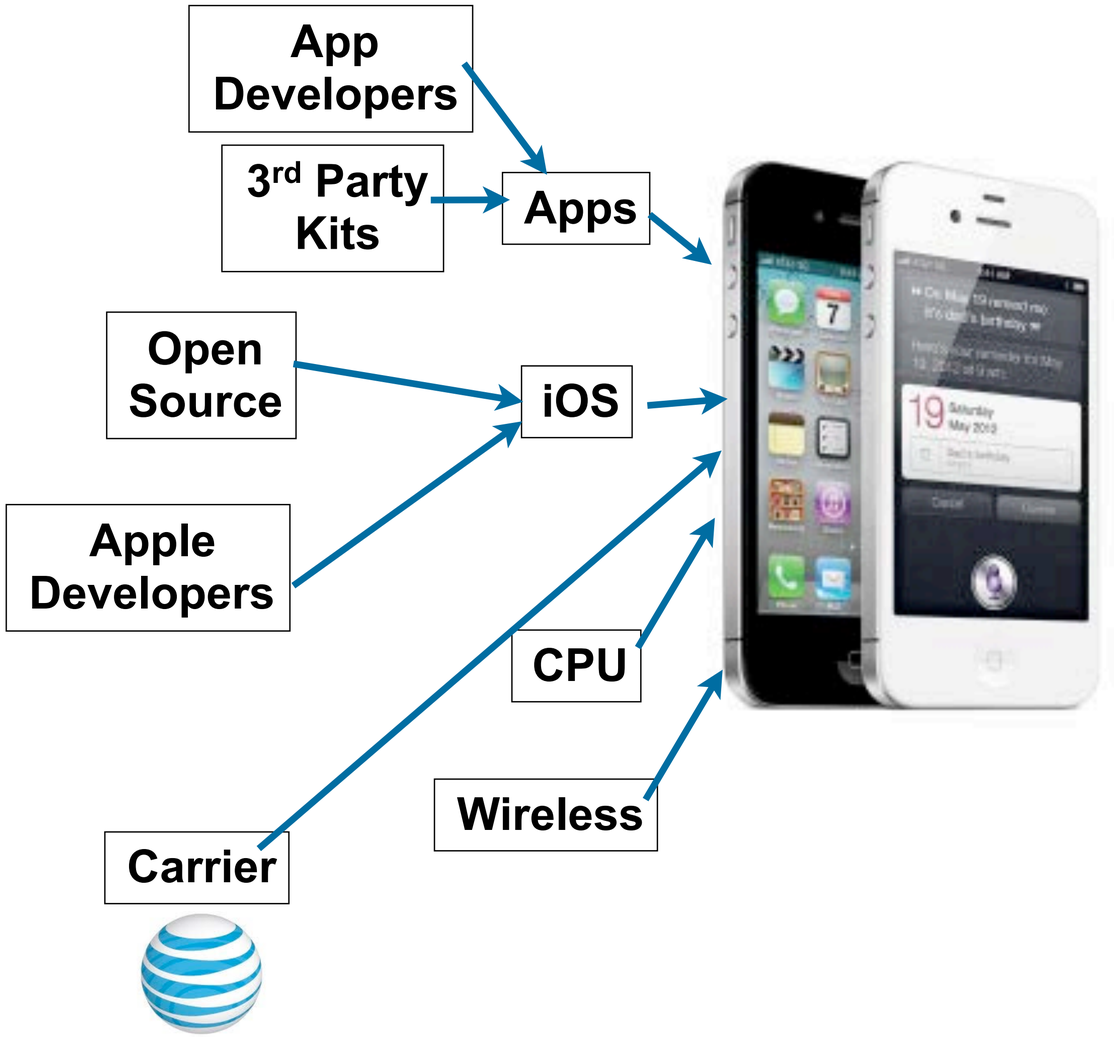
**Kaspersky:**

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




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

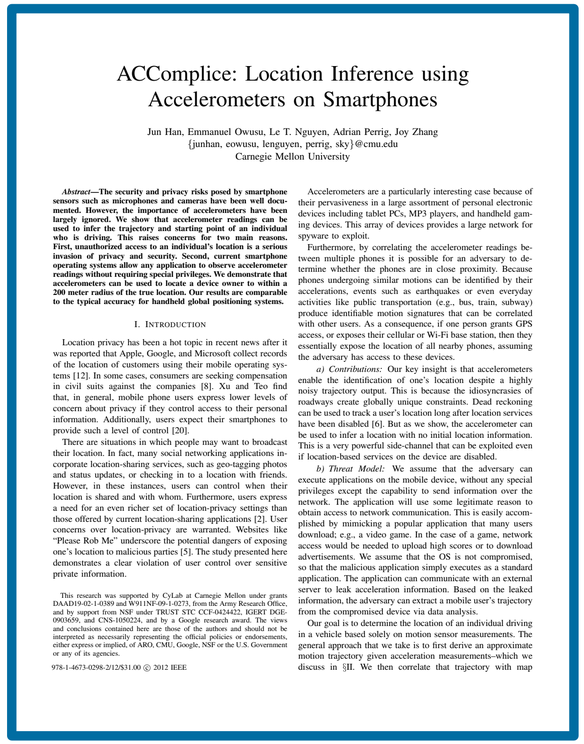
# The supply chain creates numerous security vulnerabilities



# There are more attackers than defenders, they are smarter, and they have the time to find really good attacks.

**Smartphone designers were sure that there was no privacy leakage in accelerometers. We now know they can:**

- Reveal your position
- Reveal your PIN



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.

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

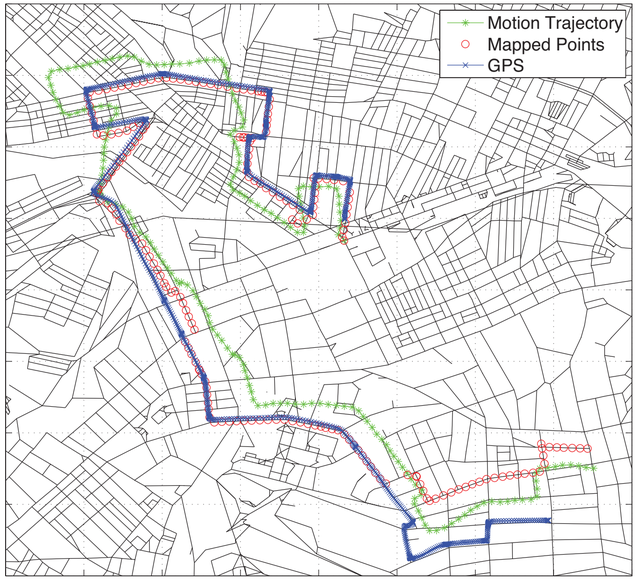
Accelerometers are a particularly interesting case because of their pervasiveness in a large assortment of personal electronic devices including tablet PCs, MP3 players, and handheld gaming devices. This array of devices provides a large network for spyware to exploit.

Furthermore, by correlating the accelerometer readings between multiple phones it is possible for an adversary to determine whether the phones are in close proximity. Because phones undergoing similar motions can be identified by their accelerations, events such as earthquakes or even everyday activities like public transportation (e.g., bus, train, subway) produce identifiable motion signatures that can be correlated with other users. As a consequence, if one person grants GPS access, or exposes their cellular or Wi-Fi base station, then they essentially expose the location of all nearby phones, assuming the adversary has access to these devices.

*a) Contributions:* Our key insight is that accelerometers enable the identification of one's location despite a highly noisy trajectory output. This is because the idiosyncrasies of roadways create globally unique constraints. Dead reckoning 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 information. This is a very powerful side-channel that can be exploited even if location-based services on the device are disabled.

*b) Threat Model:* We assume that the adversary can execute applications on the mobile device, without any special privileges except the capability to send information over the network. The application will use some legitimate reason to obtain access to network communication. This is easily accomplished by mimicking a popular application that many users download; e.g., a video game. In the case of a game, network access would be needed to upload high scores or to download advertisements. We assume that the OS is not compromised, so that the malicious application simply executes as a standard application. The application can communicate with an external server to leak acceleration information. Based on the leaked information, the adversary can extract a mobile user's trajectory 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




**6 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.

# Many people liken cyber security to the flu.

## DHS calls for “cyber hygiene”

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

—*“STOP, THINK, CONNECT”*

# Another model is *obesity*....

**Making people fat is good business:**

- Farm subsidies
- Restaurants
- Healthcare and medical utilization
- Weight loss plans

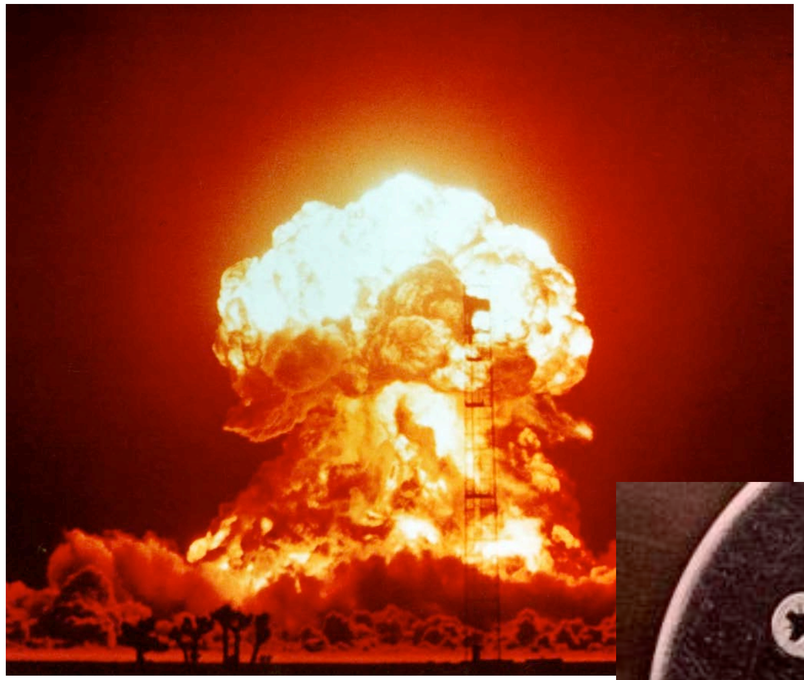
  *Few make money when Americans stay trim and healthy.*

**Lax security is also good business:**

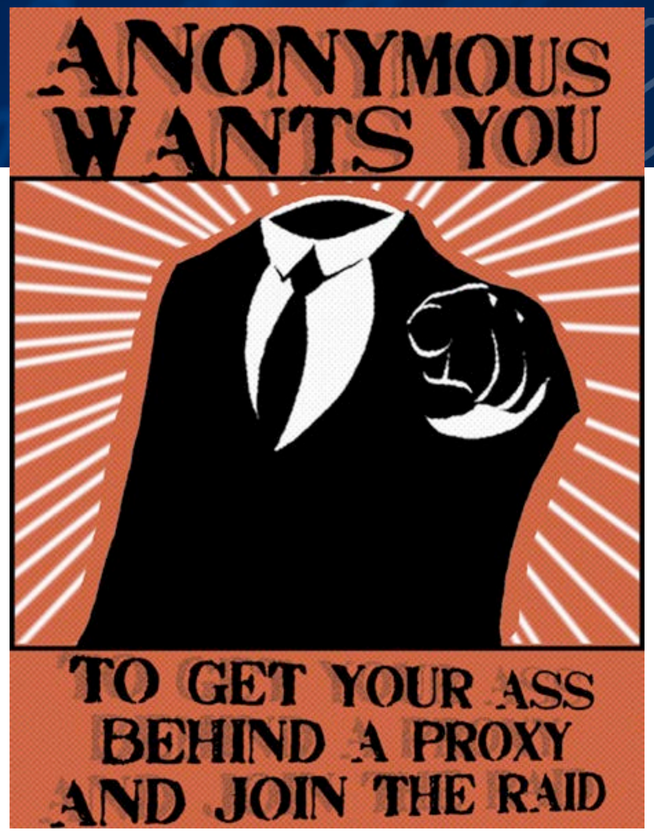
- Cheaper cost of deploying software
- Private information for marketing
- Selling anti-virus & security products
- Cleaning up incidents

  *Few benefit from secure computers*

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




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




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

# Biowar may be a better model for cyberwar.

*Cheap to produce*

*Easy to attack*

*Hard to control*

*Hard to defend*

*No clear end*

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

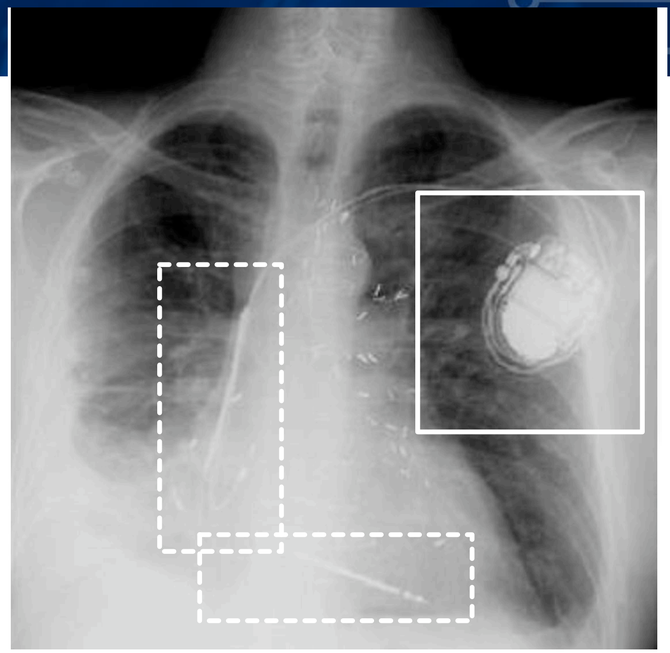
**… because [wireless] computers are everywhere.**

**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!**

# [Android] Cell phones ~~cannot~~ have not be[en] 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

# How do we address the cybersecurity challenge?

**1. Deploy technology that works**

**2. Address the non-technical issues**

# We have made major advances in cyber security.

**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.

**None of these breakthroughs has been a "silver bullet," but they have all helped.**

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

# We must continue to deploy technology that works, because 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 cyber security problems... We should use them!

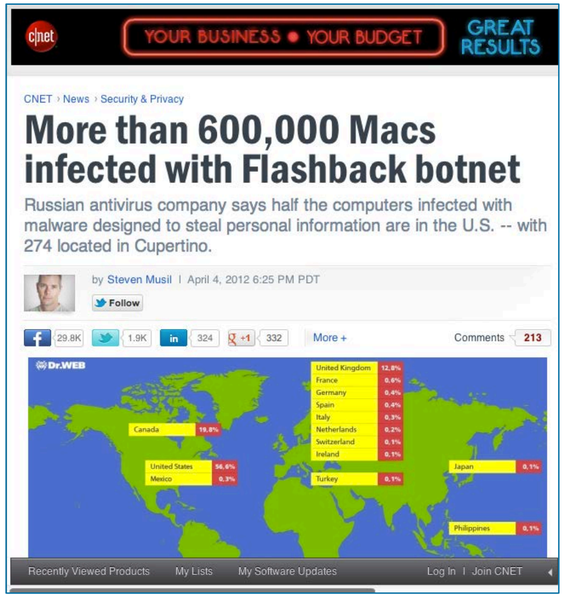
**8.63% of the desktop computers still run Windows XP**

*—http://netmarketshare.com/*

- Support was ended in 2014!


**Apple users don't run anti-virus.**

- Yes, Apple tries to fix bugs, but

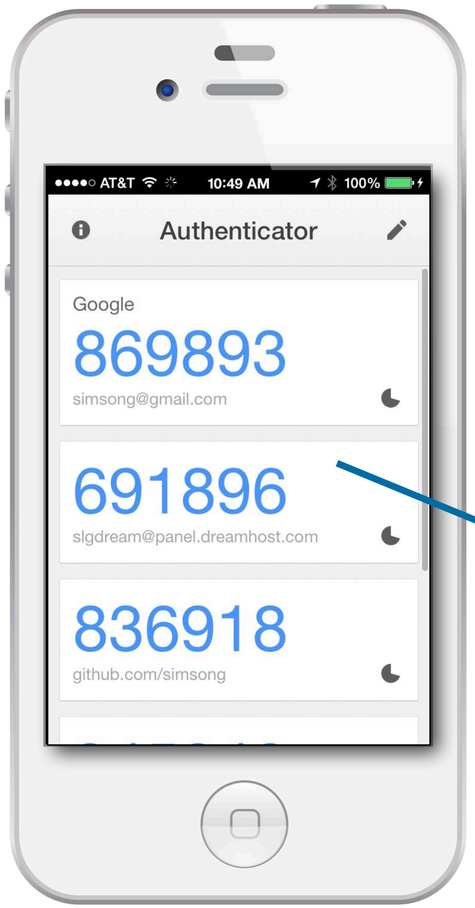


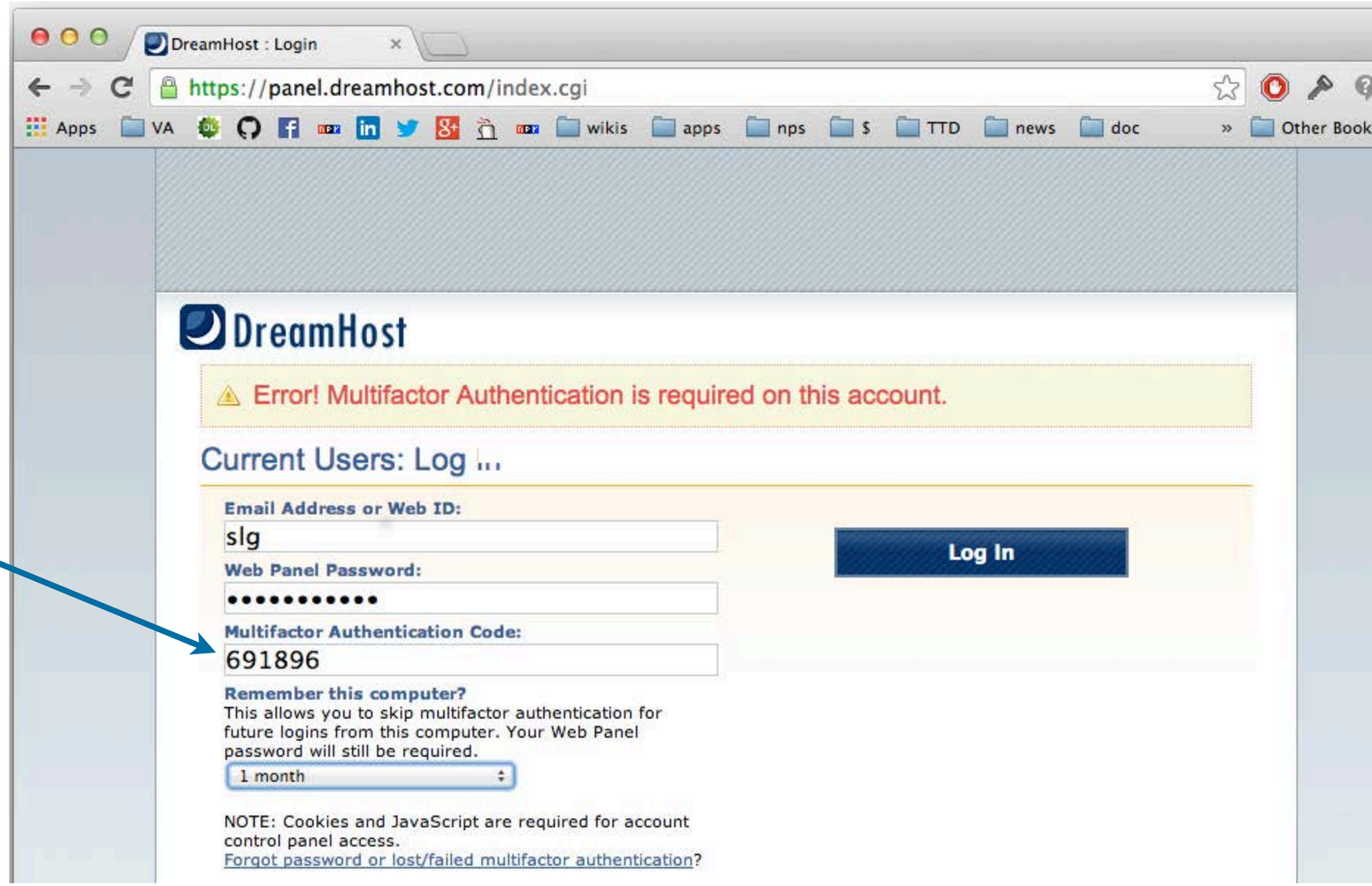

**Most "SSL" websites only use it for logging in.**

**DNSSEC lags**

**Smart Cards aren't**

# Example: Google Authenticator's 2-factor authentication protections against password stealing.



# Universal Second Factor (2UF)


# We must address non-technical factors that impact cyber.

**These factors reflect deep divisions within our society.**

- ***Shortened*** development cycles

- ***Education:*** Not enough CS graduates; not enough security in CS.

- ***Labor:***
  - —***Immigration Policy:*** *Foreign students; H1B Visa*
  - —***HR:*** *Inability to attract and retain the best workers*

- ***Manufacturing Policy:*** Where we are building our computers.

**Solving the cyber security mess requires addressing these issues.**

# Short development cycles

**Insufficient planning:**

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

**I**

**F**

"A woman, save the world? How delightfully absurd."

We must address institutionalized harassment of women

# Education is not supplying enough security engineers. Software engineers don't learn enough about security.

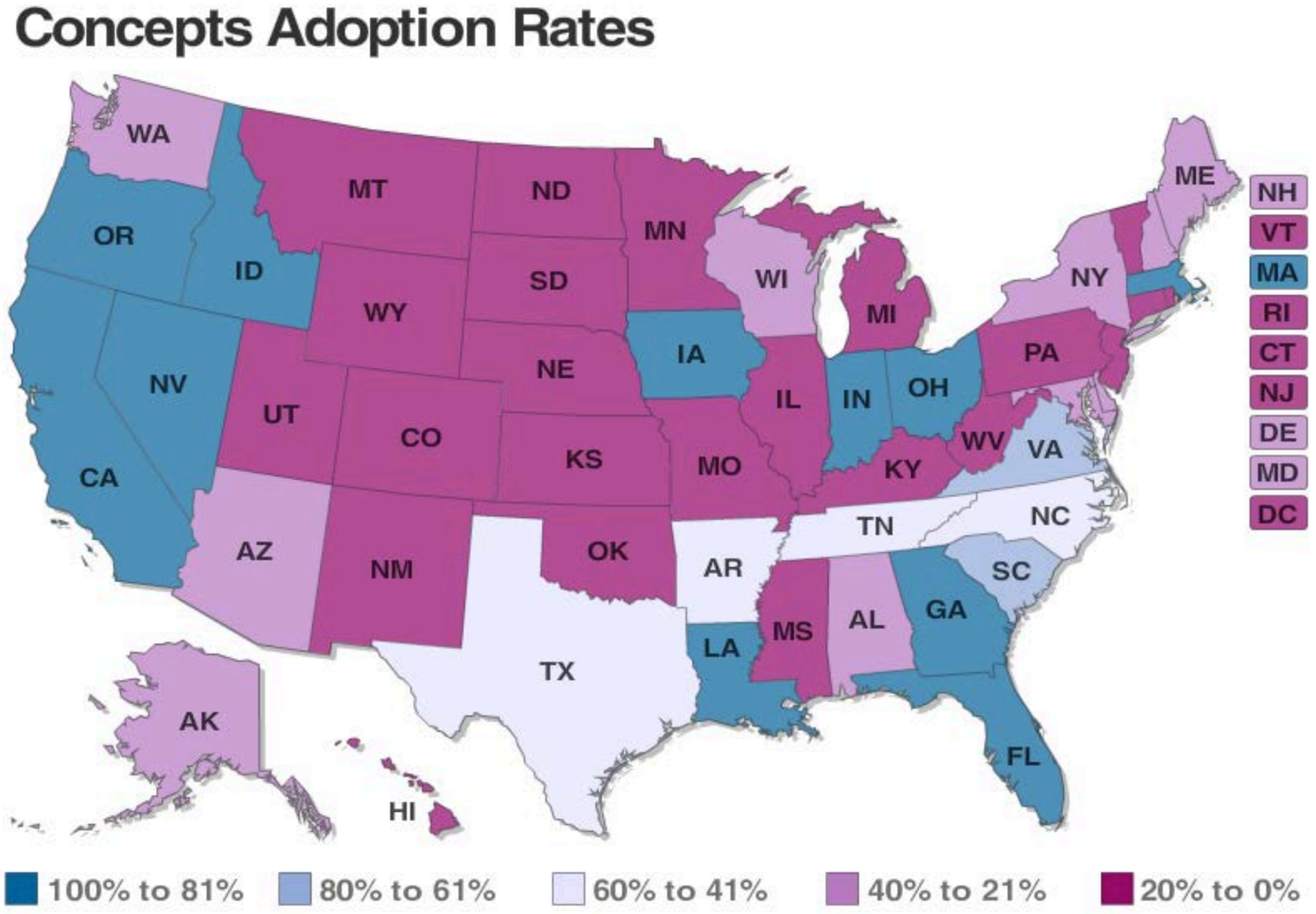
**Security HR Pipeline**

- High School → College → Graduate School → Career

**It takes *years* to master security...**

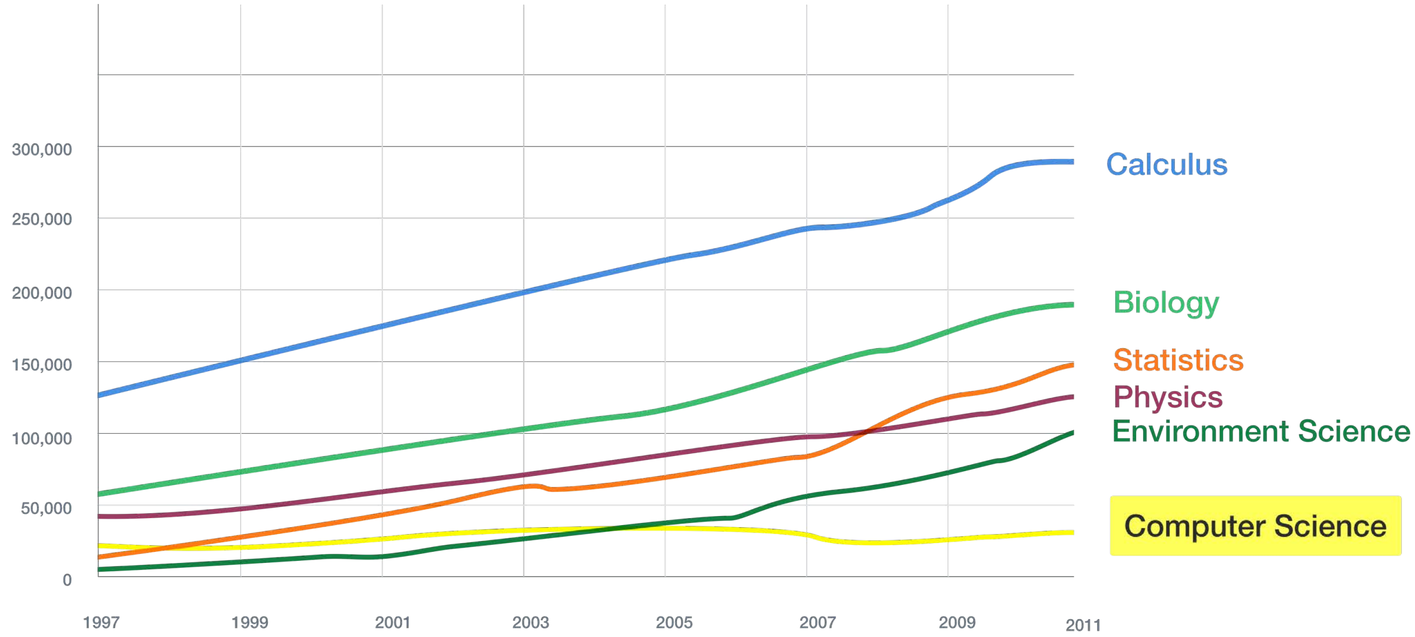
- Many professional programmers learn their craft in college
- College English graduates: 16 years' instruction in writing
- College CS graduates: 4 years' instruction in programming
  —*Is it any wonder their code has security vulnerabilities?*

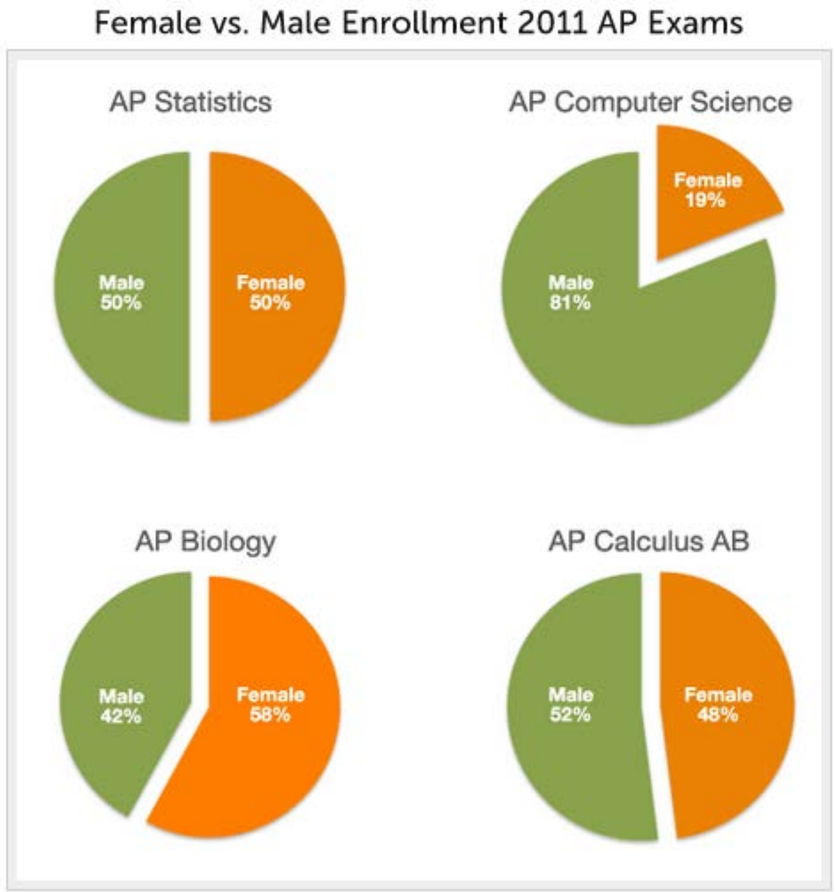
# 73% of states require computer “skills” for graduation.
# Only 37% require CS “concepts”




**CS teachers are paid far less than CS engineers.**

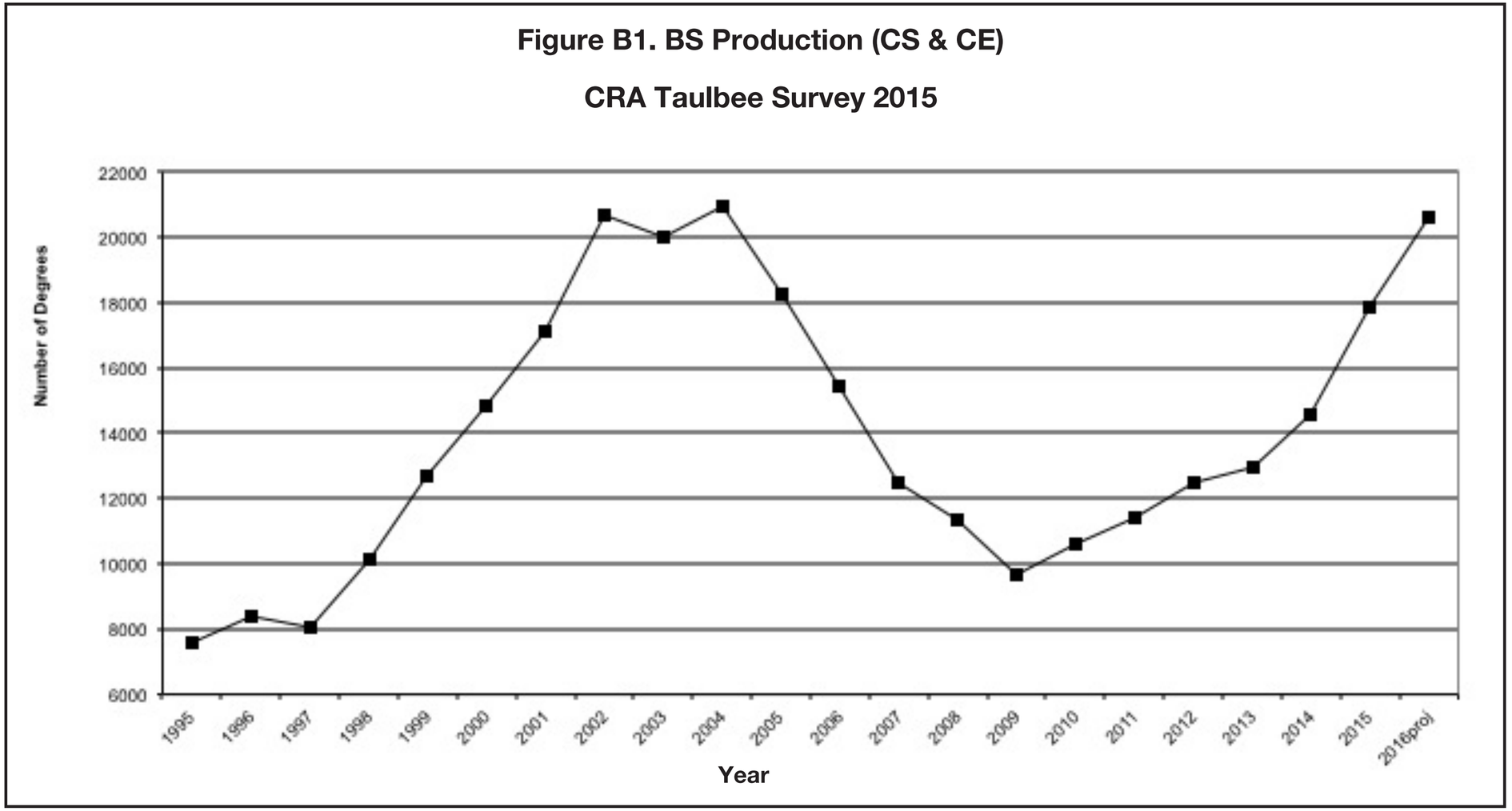
# High school students are not taking AP computer science!




Source: College Board, Advanced Placement (AP) Exam Data 2011, available at http://professionals.collegeboard.com/data-reports-research/ap/data

# Good news:
# Computer Science BS production is once again at its peak!

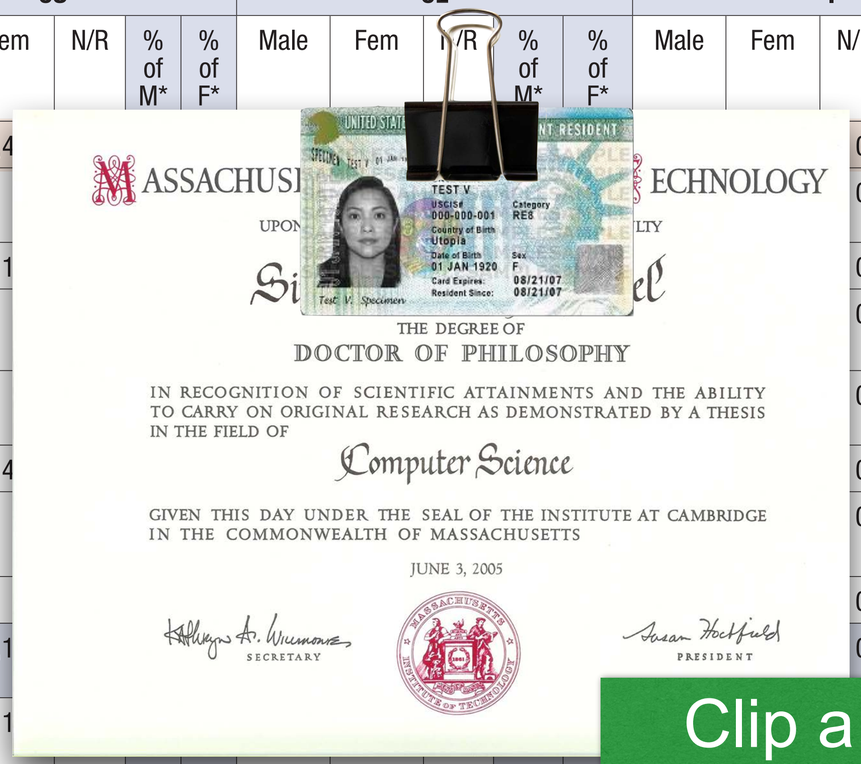


# 60.5% of PhDs awarded in 2015 to nonresident aliens

**Table D10. PhD Enrollment by Gender and Ethnicity, From 153 Departments Providing Breakdown Data**

| | CS | | | | | CE | | | | | I | | | | | Ethnicity Totals | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Male | Fem | N/R | % of M* | % of F* | Male | Fem | N/R | % of M* | % of F* | Male | Fem | N/R | % of M* | % of F* | Total | % |
| Nonresident Alien | 5,583 | 1,4 | | | | | | | | | | | 0 | 55 | 46 | 8,431 | 60.5% |
| Amer Indian or Alaska Native | 29 | | | | | | | | | | | | 0 | 0 | 0 | 47 | 0.3% |
| Asian | 706 | 1 | | | | | | | | | | | 0 | 7 | 9 | 1,088 | 7.8% |
| Black or African-American | 95 | | | | | | | | | | | | 0 | 3 | 6 | 216 | 1.5% |
| Native Hawaiian/ Pac Islander | 5 | | | | | | | | | | | | 0 | 1 | 0 | 15 | 0.1% |
| White | 2,585 | 4 | | | | | | | | | | | 0 | 33 | 34 | 3,792 | 27.2% |
| Multiracial, not Hispanic | 55 | | | | | | | | | | | | 0 | 1 | 2 | 93 | 0.7% |
| Hispanic, any race | 162 | | | | | | | | | | | | 0 | 2 | 3 | 258 | 1.9% |
| Total Res & Ethnicity Known | 9,220 | 2,1 | | | | | | | | | | | 0 | | | 13,940 | |
| Resident, ethnicity unknown | 469 | 1 | | | | | | | | | | | | | | | |
| Not Reported (N/R) | 373 | 72 | 165 | | | 17 | 0 | | | | | | | | | | |
| Gender Totals | 10,062 | 2,361 | 296 | | | 943 | 174 | | | | | | | | | | |
| % | 81.0% | 19.0% | | | | 84.4% | 15.6% | | | | 66.9% | 33.1% | | | | | |

* % of M and % of F columns are the percent of that gender who are of the specified ethnicity, of those whose ethnicity is known




Clip a green card to every PhD diploma

*—We did not train Russia's weapons scientists in Boston during the Cold War.*

# Just 67 / 1275 (5%) PhDs went into Information Assurance
# 21 professors & postdocs; 41 to industry & government

**Table D4. 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 | 10 | 0 | 7 | 6 | 6 | 4 | 12 | 5 | 8 | 12 | 2 | 8 | 4 | 9 | 3 | 0 | 5 | 14 | 8 | 17 | 140 | 10.0% |
| Researcher | 2 | 0 | 1 | 2 | 0 | 1 | 5 | 2 | 1 | 2 | 0 | 2 | 1 | 2 | 2 | 1 | 0 | 0 | 1 | 1 | 26 | 1.8% |
| Postdoc | 22 | 0 | 10 | 13 | 7 | 3 | 6 | 12 | 5 | 4 | 2 | 4 | 1 | 11 | 9 | 3 | 1 | 2 | 9 | 13 | 137 | 9.7% |
| Teaching Faculty | 6 | 0 | 5 | 2 | 1 | 2 | 2 | 0 | 5 | 1 | 3 | 8 | 2 | 3 | 2 | 2 | 4 | 3 | 2 | 11 | 64 | 4.6% |
| **North American, Other Academic** | | | | | | | | | | | | | | | | | | | | | | |
| Other CS/CE/I Dept. | 2 | 0 | 2 | 1 | 0 | 0 | 2 | 0 | 2 | 4 | 0 | 3 | 2 | 3 | 0 | 1 | 1 | 2 | 3 | 5 | 33 | 2.3% |
| Non-CS/CE/I Dept | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 2 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 8 | 0.6% |
| **North American, Non-Academic** | | | | | | | | | | | | | | | | | | | | | | |
| Industry | 77 | 2 | 67 | 47 | 46 | 21 | 23 | 35 | 34 | 11 | 6 | 57 | 31 | 31 | 48 | 9 | 29 | 111 | 35 | 86 | 806 | 57.3% |
| Government | 4 | 0 | 1 | 1 | 3 | 6 | 1 | 3 | 6 | 0 | 3 | 0 | 0 | 3 | 3 | 3 | 1 | 3 | 2 | 4 | 47 | 3.3% |
| Self-Employed | 1 | 0 | 0 | 2 | 1 | 0 | 0 | 2 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 2 | 5 | 0 | 4 | 22 | 1.6% |
| Unemployed | 1 | 0 | 2 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 7 | 0.5% |
| Other | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 2 | 7 | 0.5% |
| **Total Inside North America** | | | | | | | | | | | | | | | | | | | | | | |
| | 125 | 2 | 95 | 75 | 64 | 37 | 53 | 61 | 62 | 37 | 17 | 84 | 42 | 63 | 71 | 20 | 43 | 140 | 62 | 144 | 1,297 | 92.2% |

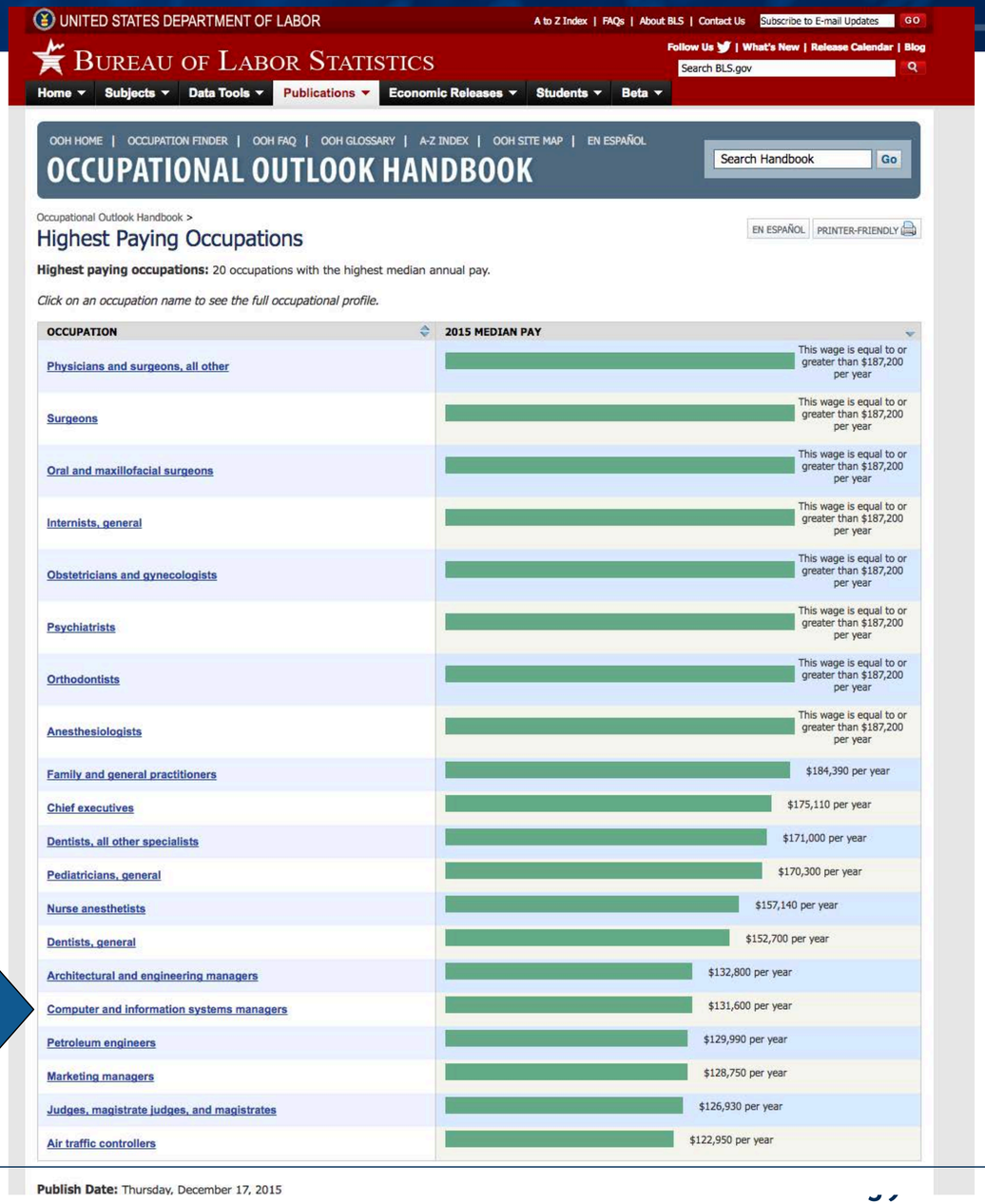
**Security should be taught to everyone, but we need specialists**

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

**Highest paying occupations:**

- Physicians and surgeons > $187K
- Family practitioners: $184K
- CEOs: $175K
- Nurse anesthetists: $157K
- Dentists: $153K
- Architectural and engineering managers: $133K
- Computer and information systems managers: $131K

**(2015 data)**



# Computer scientists make less than MIS managers...

BUREAU OF LABOR STATISTICS

Follow Us | What's New | Release Calendar | Blog

Search BLS.gov

Home | Subjects | Data Tools | Publications | Economic Releases | Students | Beta

OOH HOME | OCCUPATION FINDER | OOH FAQ | OOH GLOSSARY | A-Z INDEX | OOH SITE MAP | EN ESPAÑOL

## OCCUPATIONAL OUTLOOK HANDBOOK

Search Handbook Go

Computer and Information Technology >

## Computer and Information Research Scientists

EN ESPAÑOL | PRINTER-FRIENDLY

Summary | What They Do | Work Environment | How to Become One | Pay | Job Outlook | State & Area Data | Similar Occupations | More Info

### Summary

| Quick Facts: Computer and Information Research Scientists | |
|---|---|
| 2015 Median Pay | $110,620 per year<br>$53.18 per hour |
| Typical Entry-Level Education | Doctoral or professional degree |
| Work Experience in a Related Occupation | None |
| On-the-job Training | None |
| Number of Jobs, 2014 | 25,600 |
| Job Outlook, 2014-24 | 11% (Faster than average) |
| Employment Change, 2014-24 | 2,700 |

Computer and information research scientists study and solve complex problems in computing.

**What Computer and Information Research Scientists Do**

Computer and information research scientists invent and design new approaches to computing technology and find innovative uses for existing technology. They study and solve complex problems in computing for business, medicine, science, and other fields.

**Work Environment**

Most computer and information research scientists work full time. About 1 in 10 worked more than 40 hours per week in 2014.

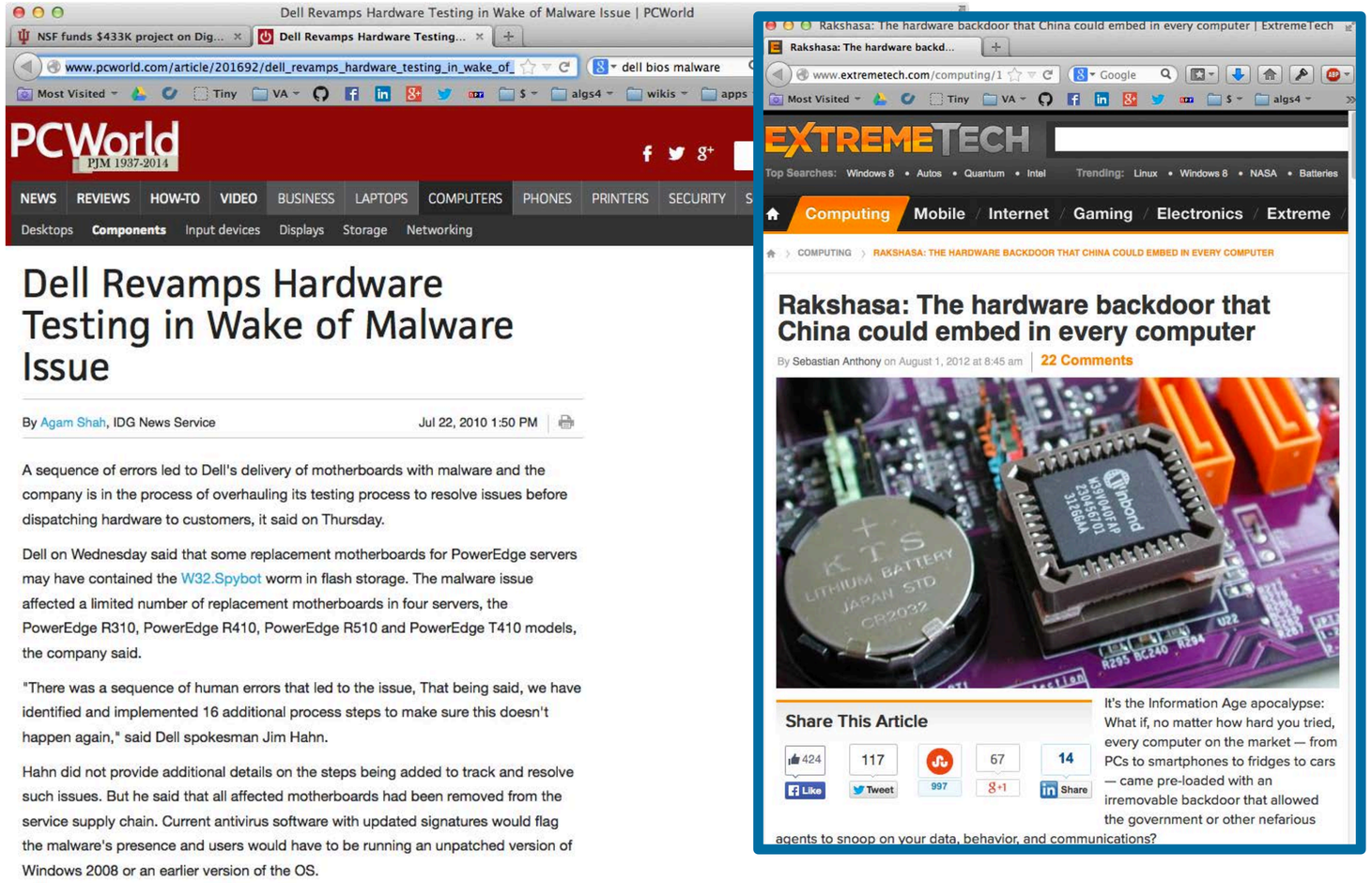
**How to Become a Computer and Information Research Scientist**

Most jobs for computer and information research scientists require a Ph.D. in computer science or a related field. In the federal government, a bachelor's degree may be sufficient for some jobs.

# Manufacturing policy —
# The US did not buy WW2 aircraft from Germany

Boeing Whichata B-29 Assembly Line, 1944
http://en.wikipedia.org/wiki/File:Boeing-Whichata_B-29_Assembly_Line_-_1944.jpg

# But we buy *nearly all* of our computers from China.



Dell Revamps Hardware Testing in Wake of Malware Issue | PCWorld

NSF funds $433K project on Dig... | Dell Revamps Hardware Testing...

www.pcworld.com/article/201692/dell_revamps_hardware_testing_in_wake_of_

PCWorld PJM 1937-2014

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS COMPUTERS PHONES PRINTERS SECURITY

Desktops Components Input devices Displays Storage Networking

## Dell Revamps Hardware Testing in Wake of Malware Issue

By Agam Shah, IDG News Service Jul 22, 2010 1:50 PM

A sequence of errors led to Dell's delivery of motherboards with malware and the company is in the process of overhauling its testing process to resolve issues before dispatching hardware to customers, it said on Thursday.

Dell on Wednesday said that some replacement motherboards for PowerEdge servers may have contained the W32.Spybot worm in flash storage. The malware issue affected a limited number of replacement motherboards in four servers, the PowerEdge R310, PowerEdge R410, PowerEdge R510 and PowerEdge T410 models, the company said.

"There was a sequence of human errors that led to the issue, That being said, we have identified and implemented 16 additional process steps to make sure this doesn't happen again," said Dell spokesman Jim Hahn.

Hahn did not provide additional details on the steps being added to track and resolve such issues. But he said that all affected motherboards had been removed from the service supply chain. Current antivirus software with updated signatures would flag the malware's presence and users would have to be running an unpatched version of Windows 2008 or an earlier version of the OS.

Rakshasa: The hardware backdoor that China could embed in every computer | ExtremeTech

www.extremetech.com/computing/1

EXTREMETECH

Top Searches: Windows 8 • Autos • Quantum • Intel Trending: Linux • Windows 8 • NASA • Batteries

Computing Mobile Internet Gaming Electronics Extreme

COMPUTING › RAKSHASA: THE HARDWARE BACKDOOR THAT CHINA COULD EMBED IN EVERY COMPUTER

## Rakshasa: The hardware backdoor that China could embed in every computer

By Sebastian Anthony on August 1, 2012 at 8:45 am | 22 Comments

Share This Article

424 Like 117 Tweet 997 67 +1 14 Share

It's the Information Age apocalypse: What if, no matter how hard you tried, every computer on the market — from PCs to smartphones to fridges to cars — came pre-loaded with an irremovable backdoor that allowed the government or other nefarious agents to snoop on your data, behavior, and communications?

**It's *easy* to put backdoors in hardware and software.**

# 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 new found attention to cyber security,**
**our systems seem to be growing more vulnerable every year.**

**Questions?**

# Backup Slides:
# HCI-SEC

# Major Themes in HCI-SEC Academic Research

**UserAuthentication**

- Text Passwords
- Graphical Authentication
- Biometrics
- Token-based Authentication
- CAPTCHAs

**Email Security and PKI**

- Automatic,Transparent Encryption

**Anti-PhishingTechnology**

**Password Managers**

**Device Pairing**

**Web Privacy**

**Policy Specification and Interaction**

**Security Experts**

**Mobile Security and Privacy**

- Location Privacy
- Application platforms
- Mobile authentication

**Social Media Privacy**

# HCI-SEC Lessons and Challenges

## Lessons Learned:

- Users need better information, not more information
- To make good decisions, users require clear context
- Plain Language Works,Even if it is less precise
- Where Possible, Reduce Decisions and Configuration Options
- Education Works, but cannot overcome economics

## Research Challenges

- Authentication Challenges
- Administration Challenges
- Privacy Challenges
- Challenge of Modelling the Adversary
- The Challenge of Social Media and Social Computing
- Teaching Challenges

# HCI-SEC Conclusion: The Next 10 years

**More HCI-SEC Research Centers**

**More HCI-SEC ResearchTargets**

**Increased Researching on Nudges and Pusuasion**

**Increased Emphasis on Offensive Work**

**Increased demand for HCI-SEC from non-technical sectors**

# Backup Slides: Insider Threat


# CT
# TWEIGHT MEDIA FORENSICS

stgraduate School &
ersity of Texas at San Antonio

on Garfinkel (NPS) & Dr. Nicole Beebe (UTSA)

*nesday November 13th, 2013*

# Team Profile

## Naval Postgraduate School


- Simson L. Garfinkel
  Assoc. Prof
  Computer Science
  —*simsong@acm.org*
  —*+1.202.649.0029*


## The University of Texas at San Antonio


- N. Beebe, Asst. Prof.
  Info Systems/Cyber Security
  —*Nicole.Beebe@utsa.edu*
  —*+1.210.269.5647*


# The current approaches for finding hostile insiders are based on “signatures.”

**Sample signature to find a problem employee:**

**(CERT 2011)**

- ***if the mail is from a departing insider***
- ***and the message was sent in last 30 days***
- ***and the recipient is not in organization’s domain***
- ***and the total bytes summed by day is more than X,***

➜ ***send an alert to security operator***

**These signatures are typically hand written.**

—*Brittle*

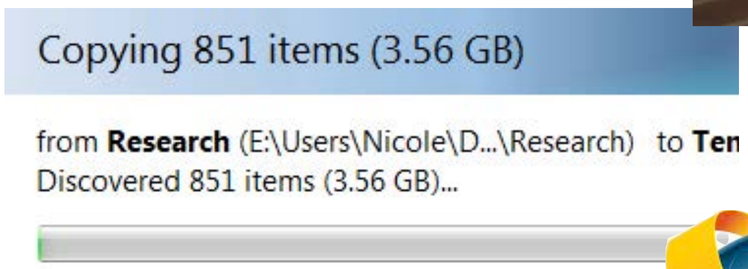
—*Don’t scale*

—*Miss new patterns*

# We propose a new approach for finding threatening insiders—storage profile anomalies.

**Hypothesis 1:**
**Some insiders hoard before exfiltration**

- Manning
- Snowden




# We also want to detect other kinds of illegal employee activity.

**Hypothesis 2:**
**Some illegal activity has storage indicators:**

- Contraband software (hacking tools) and data
- Large amount of:
  - —*graphics*
  - —*PII; PHI; account numbers*
  - —*Encrypted data*
- Stolen documents

**Illegal employee activity is:**

- Bad for business
- Exploitation threat
- Fraud risk

CNN Justice

**Pentagon reopening probe into employees allegedly tied to child porn**

**By Adam Levine**, CNN
September 16, 2010 11:59 a.m. EDT

The Defense Department will review 264 cases of possible trafficking in child pornography.

**(CNN)** -- The Defense Department will reopen its investigation into employees who are alleged to have downloaded child pornography, a spokesman said Wednesday.

The Pentagon's Defense Criminal Investigative Service will review 264 cases, according to spokesman Gary Comerford. The department had stopped the reviews because of a lack of resources, he said.

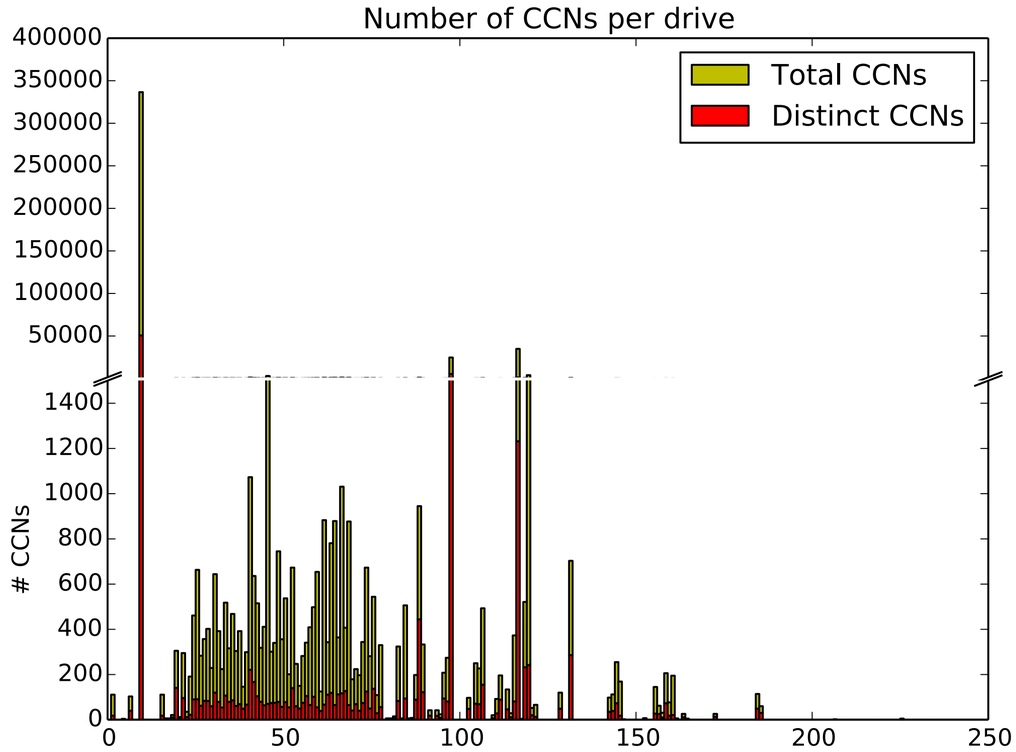
# Our plan: look for storage devices that are different than their peers.

## We build a “storage profile” from features:

- # of credit card numbers, phone #s; SSNs, DOBs, etc.
- % pictures; %video
- % Doc files; %PDFs;

## “Different” relative to:

- User’s history
- User’s organization
- Others in role.

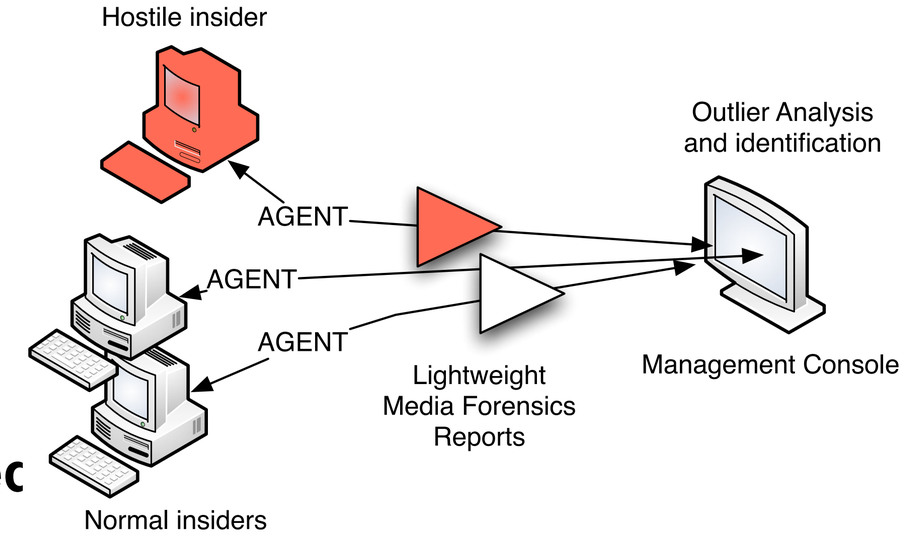



Garfinkel, S. and Shelat, A., "Remembrance of Data Passed: A Study of Disk Sanitization Practices," IEEE Security & Privacy, January/February 2003.

# Our approach:
# Collect “storage profiles” and look for outliers.

**We profile storage on the hard drive/storage device:**

- Allocated & “deleted” files; Unallocated space (file fragments)



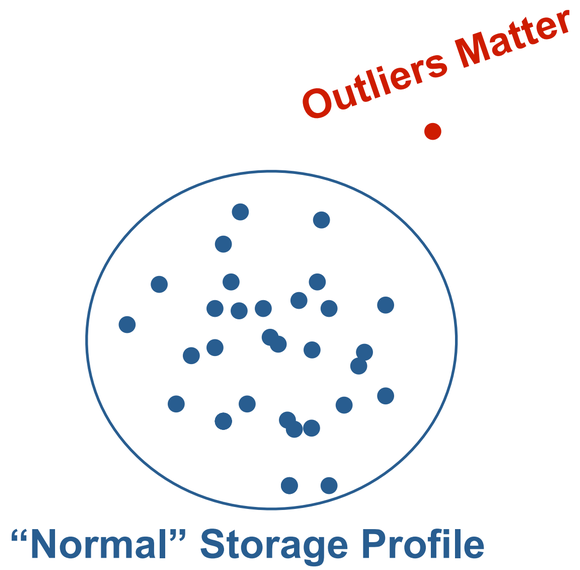

**Statistical profile is collected**

- Frequently, at “random” times
- Securely — by going to raw media
- Centrally — at management console

# We cluster the storage profiles to find “outliers.”

## What’s an outlier?

- Something that’s different from its peers
- Something different from its own history



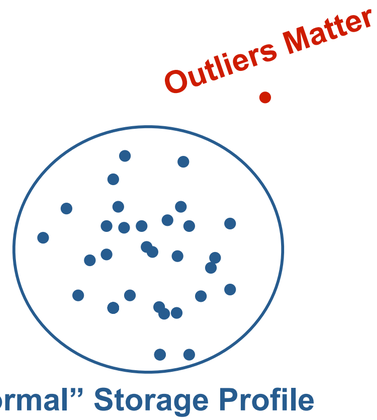

# Outlier detection should have significant benefits:

- Not signature based
- Not reliant on access patterns
- Not reliant on policy definition, discovery, auditing

**Design constraints:**

- Agent must be scalable and cannot interfer with operations
  - —*Desktop: background process, samples disk data*
  - —*Network load: small, aggregated data transfer*
  - —*Management console: scalable algorithms used*

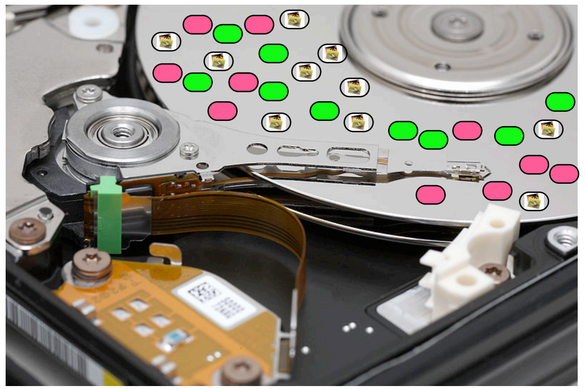
- Must work with isolated systems
- Must be OS agnostic
- Must includes deleted data in collection/analysis



# Our system has three parts:

## 1. Sample disk to collect desired data

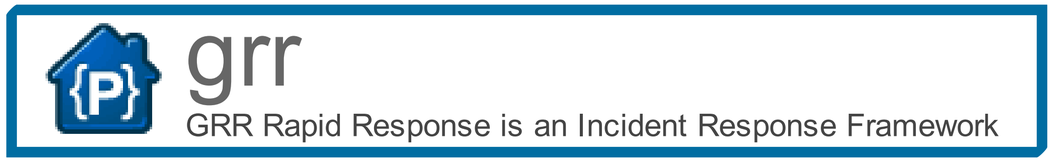
- bulk_extractor
  - *a lightweight media forensics tool*



Garfinkel, Simson, Digital media triage with bulk data analysis and bulk_extractor. Computers and Security 32: 56-72 (2013)

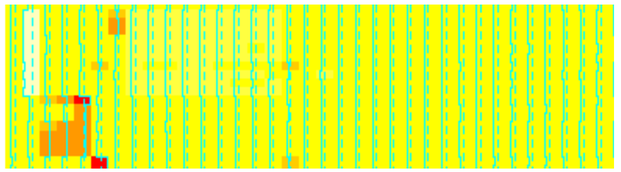
## 2. Client-server, enterprise response framework

- Google Rapid Response (GRR)



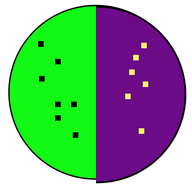

## 3. Anomaly detection agent

- Univariate and multivariate outlier detection



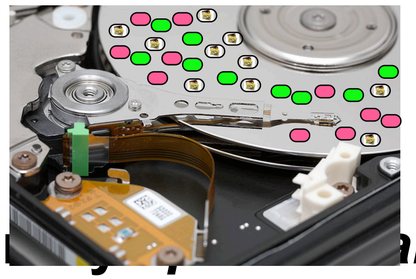
# Random sampling is a great way to analyze data.

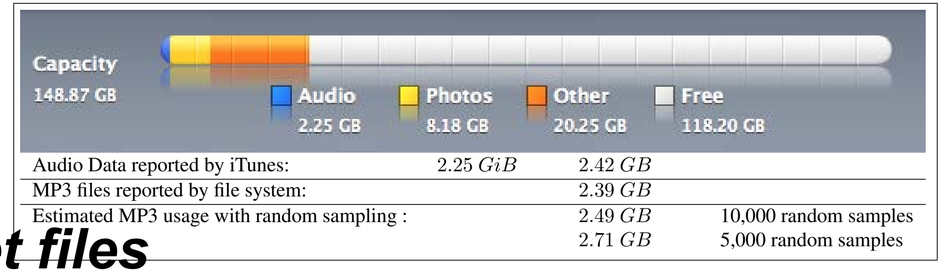
## Simple random sampling can determine % free space



Garfinkel, Simson, Vassil Roussev, Alex Nelson and Douglas White, Using purpose-built functions and block hashes to enable small block and sub-file forensics, DFRWS 2010, Portland, OR

## Data characterization can determine the *kind* of stored data

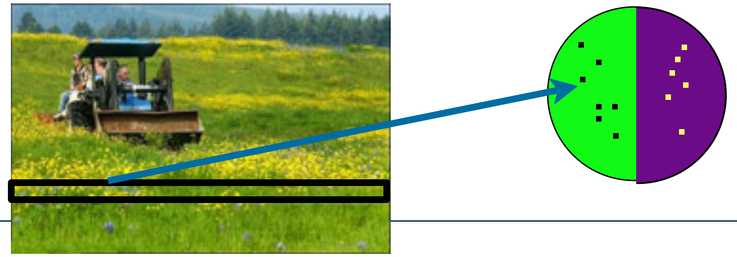





| | | | |
|---|---|---|---|
| Audio Data reported by iTunes: | 2.25 $GiB$ | 2.42 $GB$ | |
| MP3 files reported by file system: | | 2.39 $GB$ | |
| Estimated MP3 usage with random sampling : | | 2.49 $GB$ | 10,000 random samples |
| | | 2.71 $GB$ | 5,000 random samples |

## *Sector hashing* can ide[illegible]*arget files*

Young J., Foster, K., Garfinkel, S., and Fairbanks, K., Distinct sector hashes for target file detection, IEEE Computer, December 2012



# It takes 3.5 hours to read a 1TB hard drive.

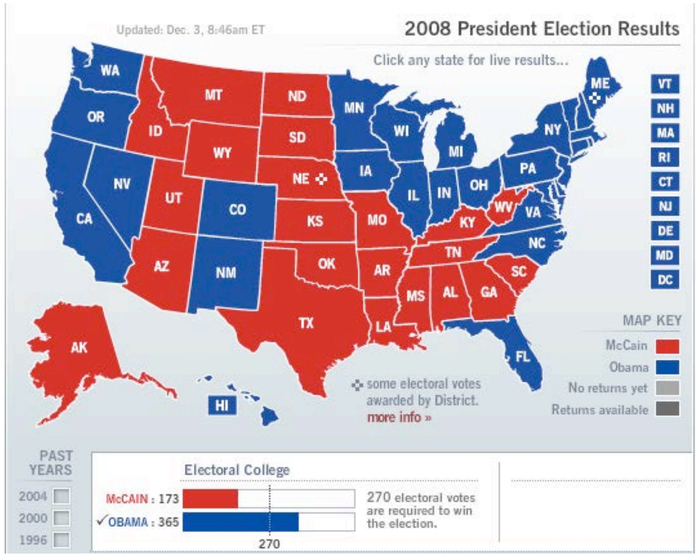
**In 5 minutes you can read:**

- 36 GB in one strip
- 100,000 randomly chosen 64KiB strips (assuming 3 msec/seek)

| |  |  |  |
|---|---|---|---|
| Minutes | 208 | 5 | 5 |
| Data | 1 TB | 36 GB | 6.5 GB |
| # Seeks | 1 | 1 | 100,000 |
| % of data | 100% | 3.6% | 0.65% |

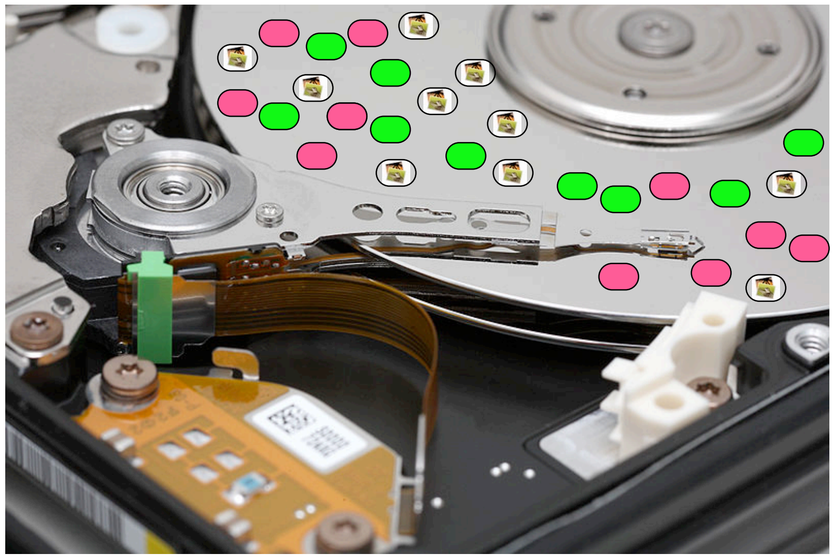
# The statistics of a *randomly chosen sample* predict the *statistics of a population.*

**US elections can be predicted by sampling thousands of households:**



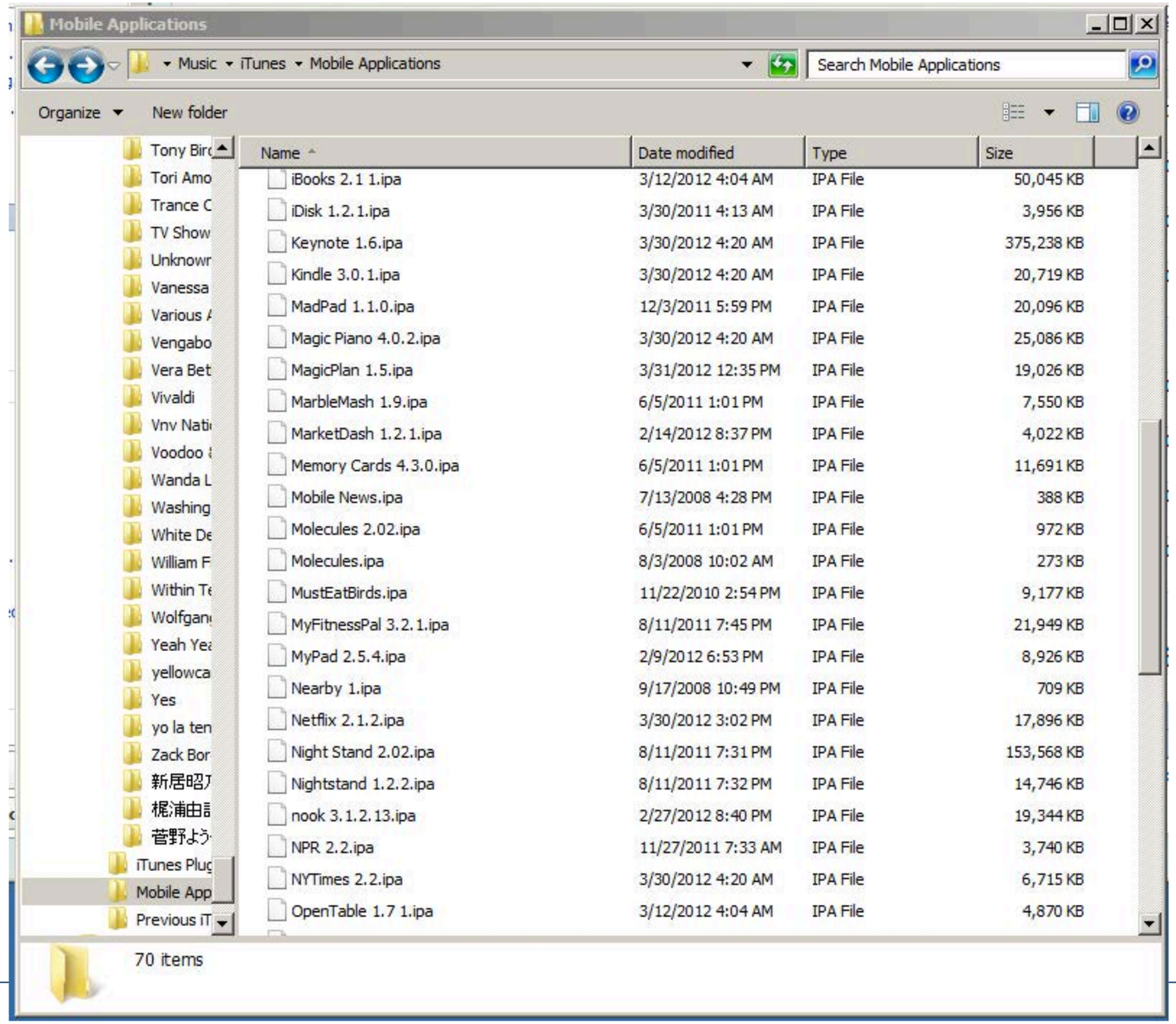

The challenge is identifying *likely voters.*

Hard drive contents can be predicted by sampling thousands of sectors:

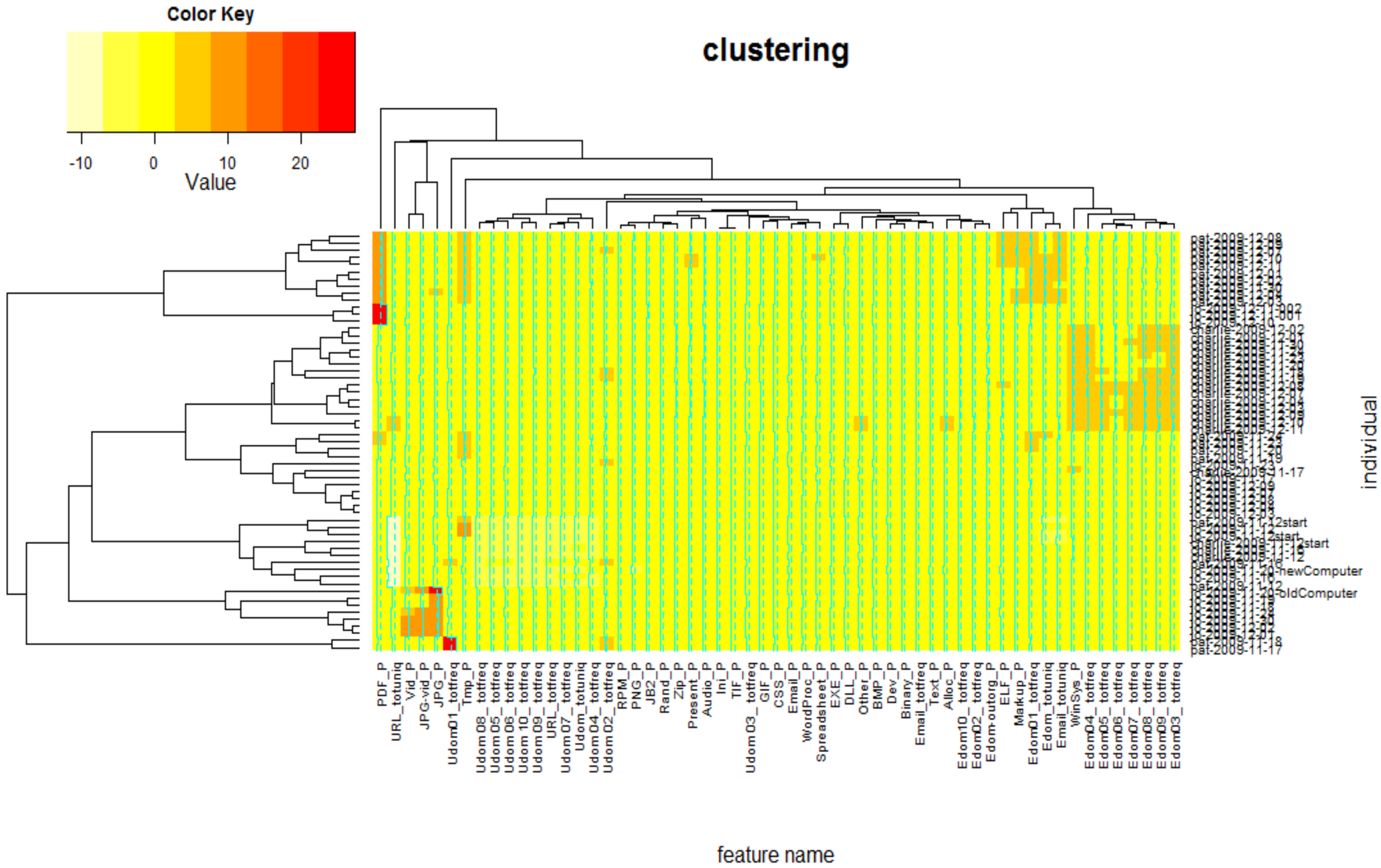


The challenge is *identifying the sector* content that is sampled.

# We think of computers as devices with *files*.



# This heatmap of anomalies let an analyst easily identify clusters and outliers.



# Current status —

## bulk_extractor updated v1.4 just released

- Added features & GRR integration preparation

## Sceadan data type classifier updated v1.2 released

## Extraction, transformation, loading of datesets

- M57 Patents (digitalcorpora.org) case

## Progress on anomaly detection algorithm

- Real Data Corpus extraction, translation and loading near complete
- Theoretical development
- Empirical data descriptive analyses (test assumptions)
- Univariate anomaly detection performing well on synthetic data set

# We are in year 1 of a 3-year effort.

| | NPS Lead | UTSA Lead |
|---|---|---|
| Year 1 | bulk_extractor upgrades | Outlier detection algorithm<br>Synthetic data experimentation<br>Real Data Corpus experimentation |
| Year 2 | Integrate GRR<br>Develop/test management console | Develop/test data outlier detection<br>Develop/test visualization component |
| Year 3 | Large-scale testing on partner net | Final dev. of outlier detection algorithm<br>Final dev. of visualization agent |

# Many challenges remain.

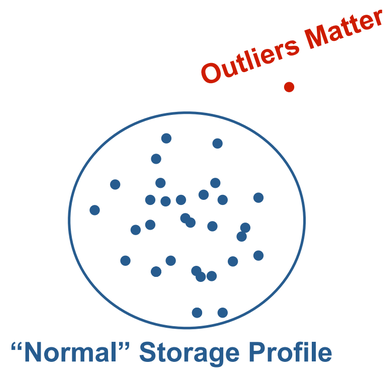
## “Anomalous” suggests “normal” exists

- Large, diverse, dislocated organizations
- High fluidity and variety in workforce
- Remote, mobile, multi-device access requirements
- Uninterruptible, critical computational operations

## Clustering algorithm selection/development

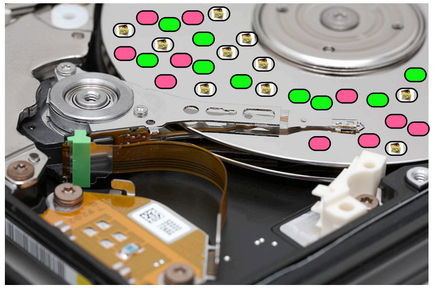
- Accuracy and speed trade-off of extant algorithms
- Develop combinatorial algorithm to improve accuracy
- Need for automated parameter selection amidst noise
- Feature selection

## Engineering of visualization component



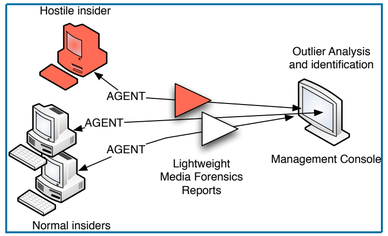
# In conclusion, we are developing a system that uses “lightweight media forensics” to find hostile insiders.

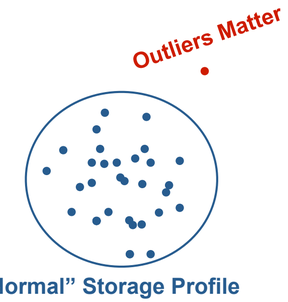
**We use random sampling to build a storage profile of media**



**We collect these profiles on a central server**

**We cluster & data mine to find outliers.**




## Contact:


- Simson L. Garfinkel simsong@acm.org
- Nicole Beebe *Nicole.Beebe@utsa.edu*