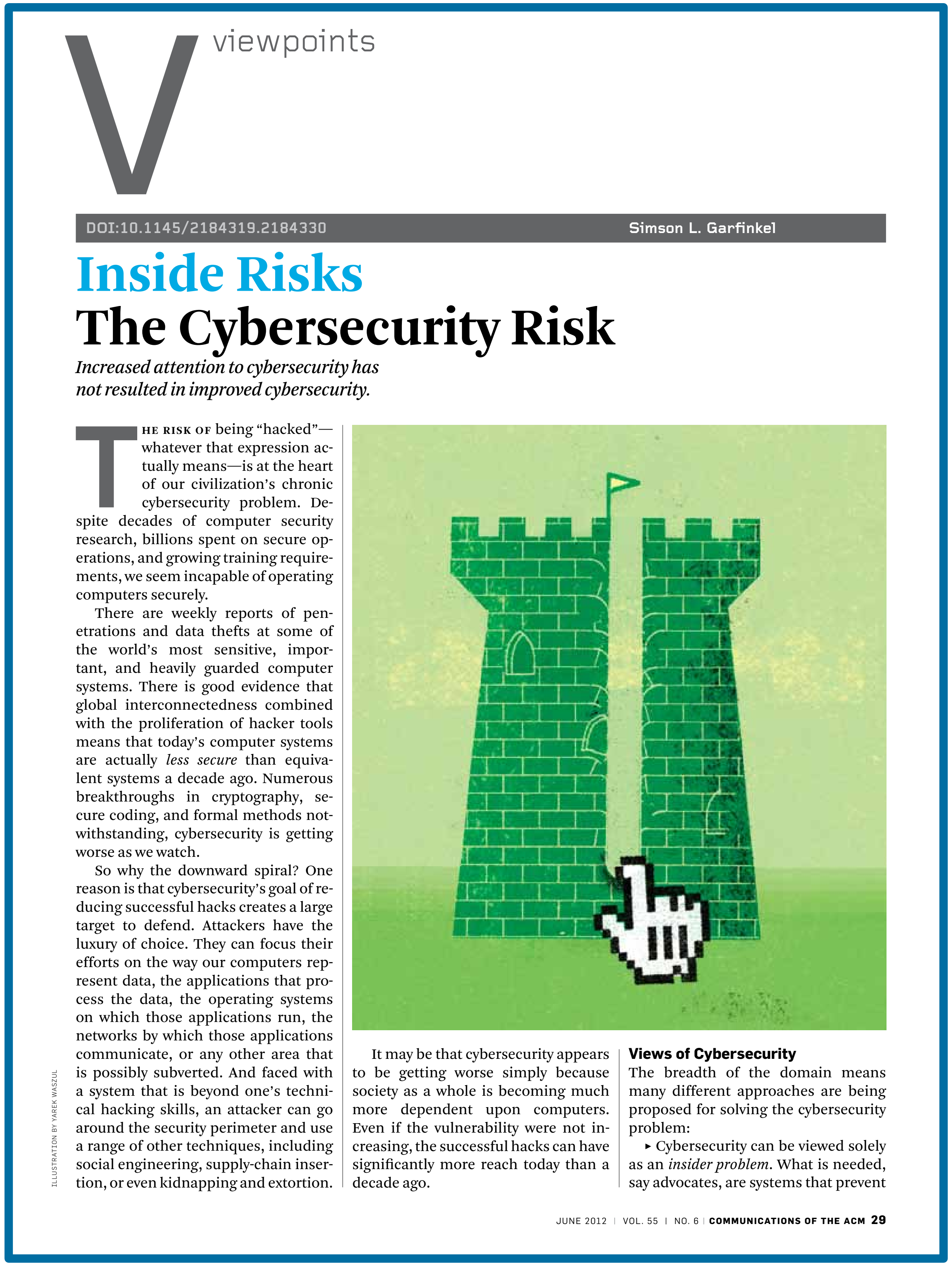
The Cyber Security Mess

Simson L. Garfinkel

December 14, 2016

Photos from https://pixabay.com

“The Cyber Security 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 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.

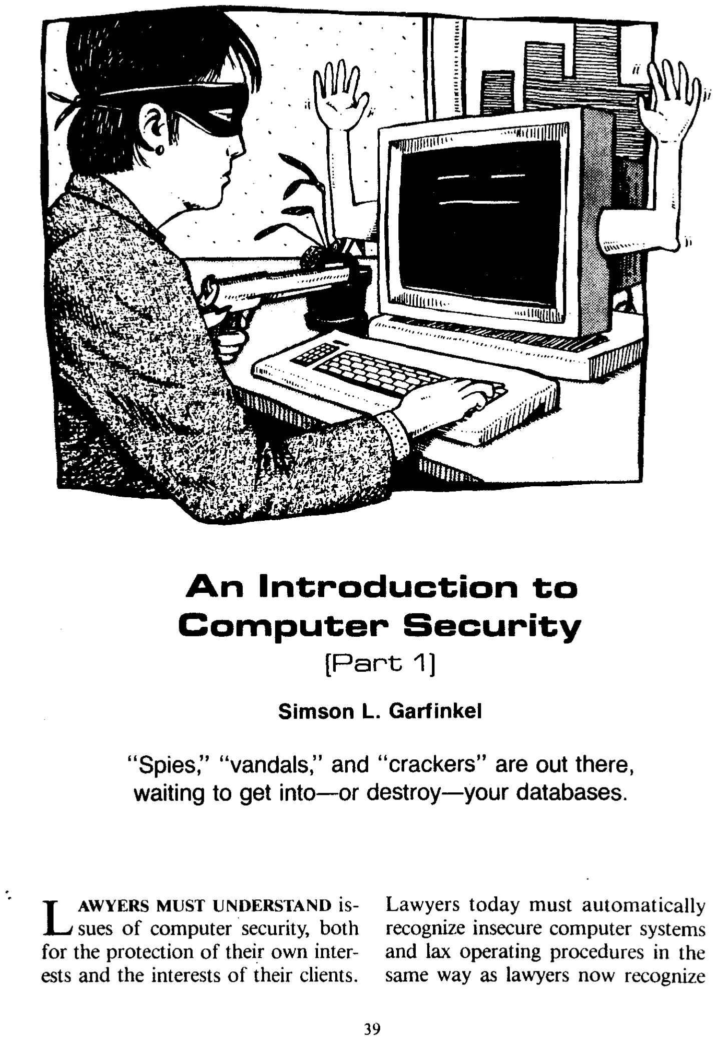
Views of Cybersecurity

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

http://simson.net/clips/academic/2012.CACM.Cybersecurity.pdf

I have spent 29 years trying to secure computers...



An Introduction to Computer Security

[Part 1]

Simson L. Garfinkel

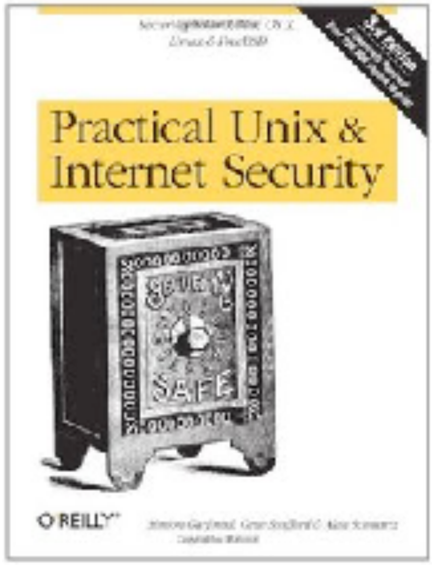
"Spies," "vandals," and "crackers" are out there, waiting to get into—or destroy—your databases.

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

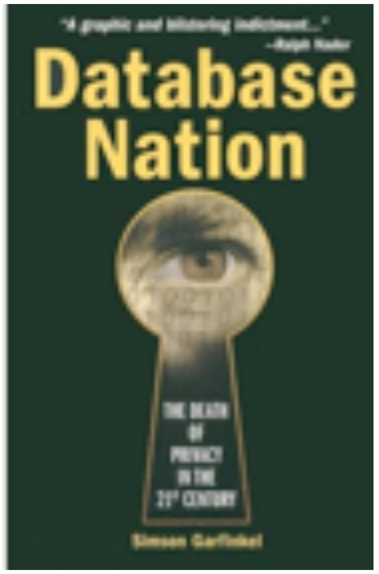
The Practical Lawyer
Sept. 1987

System Security



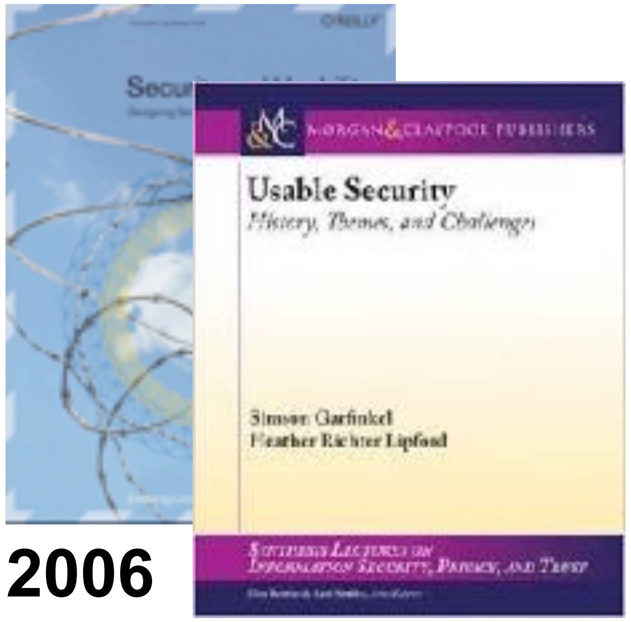
1991

Privacy Policy



2000

Usable Security


O'REILLY
Secu
MORGAN & CLAYPOOL PUBLISHERS
Usable Security
History, Themes, and Challenges
Simson Garfinkel
Heather Richter Lipford
Synthesis Lectures on Information Security, Privacy, and Trust

2006

2014

Internet of Things

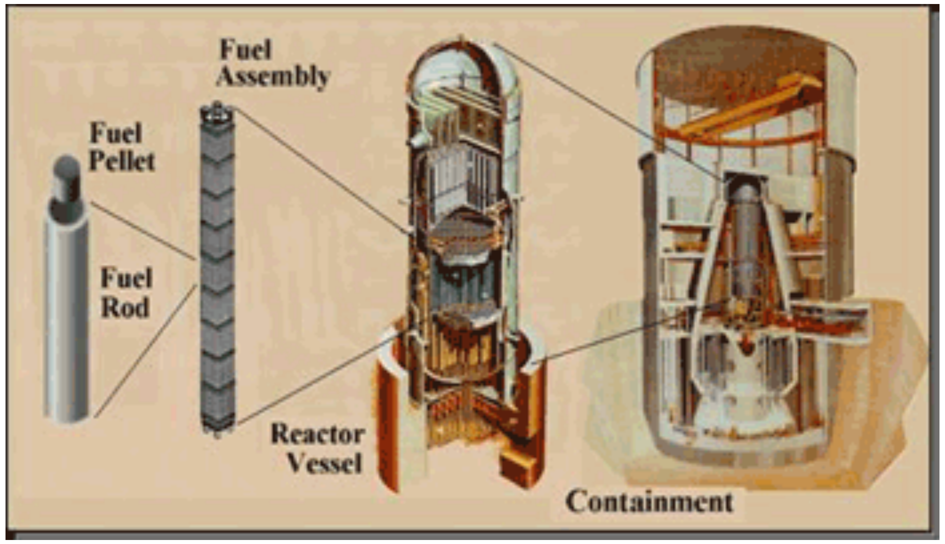
RFID
Applications, Security, and Privacy
SIMSON GARFINKEL BETH ROSENBERG

2006

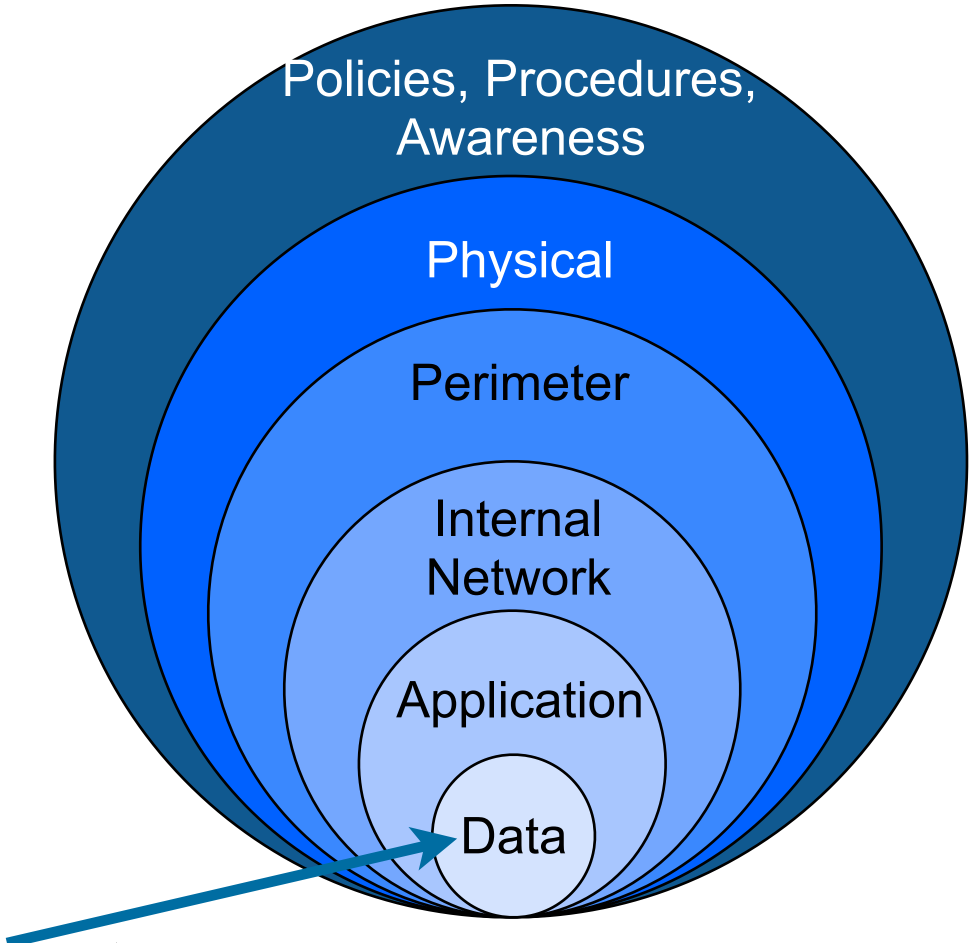
Today’s systems are less secure than those of the 1970s.

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

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

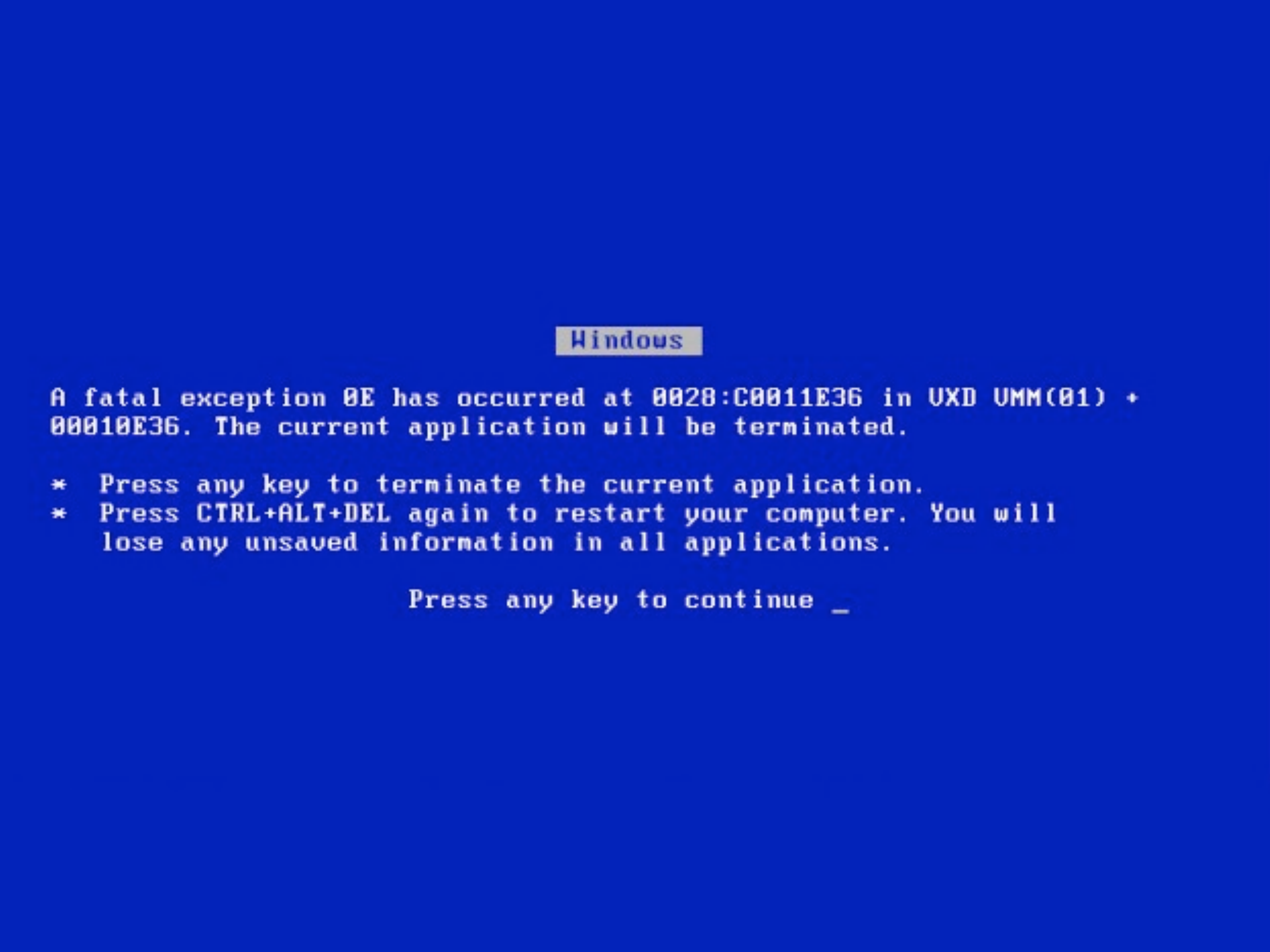


Defense in depth of nuclear reactors
http://www.nrc.gov/about-nrc/regulatory/research/soar/soarca-accident-progression.html



Cyber can directly target inner defenses

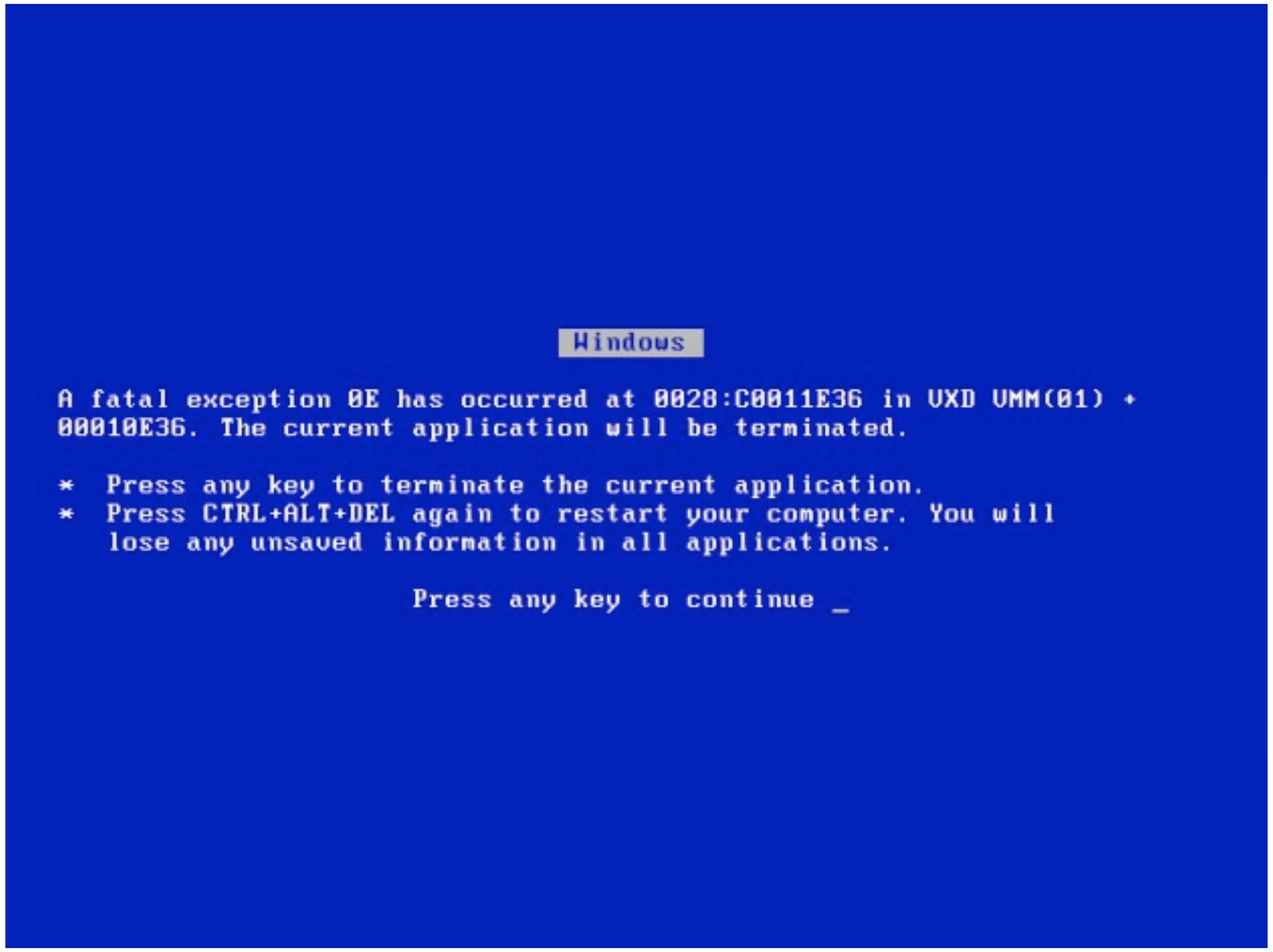
It’s easier to break things than to fix them.



```
                              Windows

A fatal exception 0E has occurred at 0028:C0011E36 in 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 _
```

Today we expect computers to crash

We also expect them to be hacked.

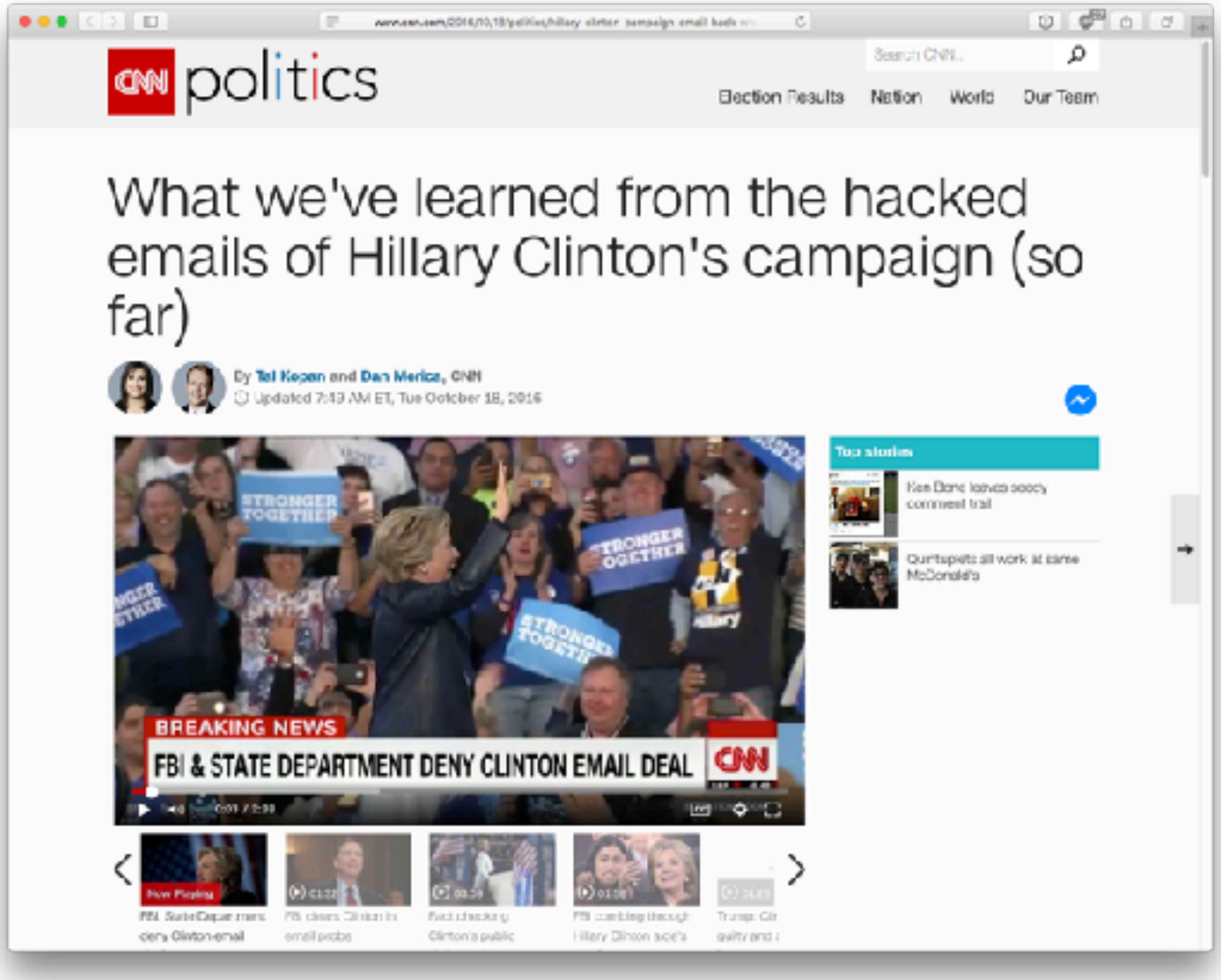


```
                              Windows

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 _
```

The solution is not better security

Today we expect computers to crash

We also expect them to be hacked.


CNN politics
Search CNN...
Election Results
Nation
World
Our Team

What we've learned from the hacked emails of Hillary Clinton's campaign (so far)

By Tal Kopan and Dan Merica, CNN
Updated 7:43 AM ET, Tue October 18, 2016

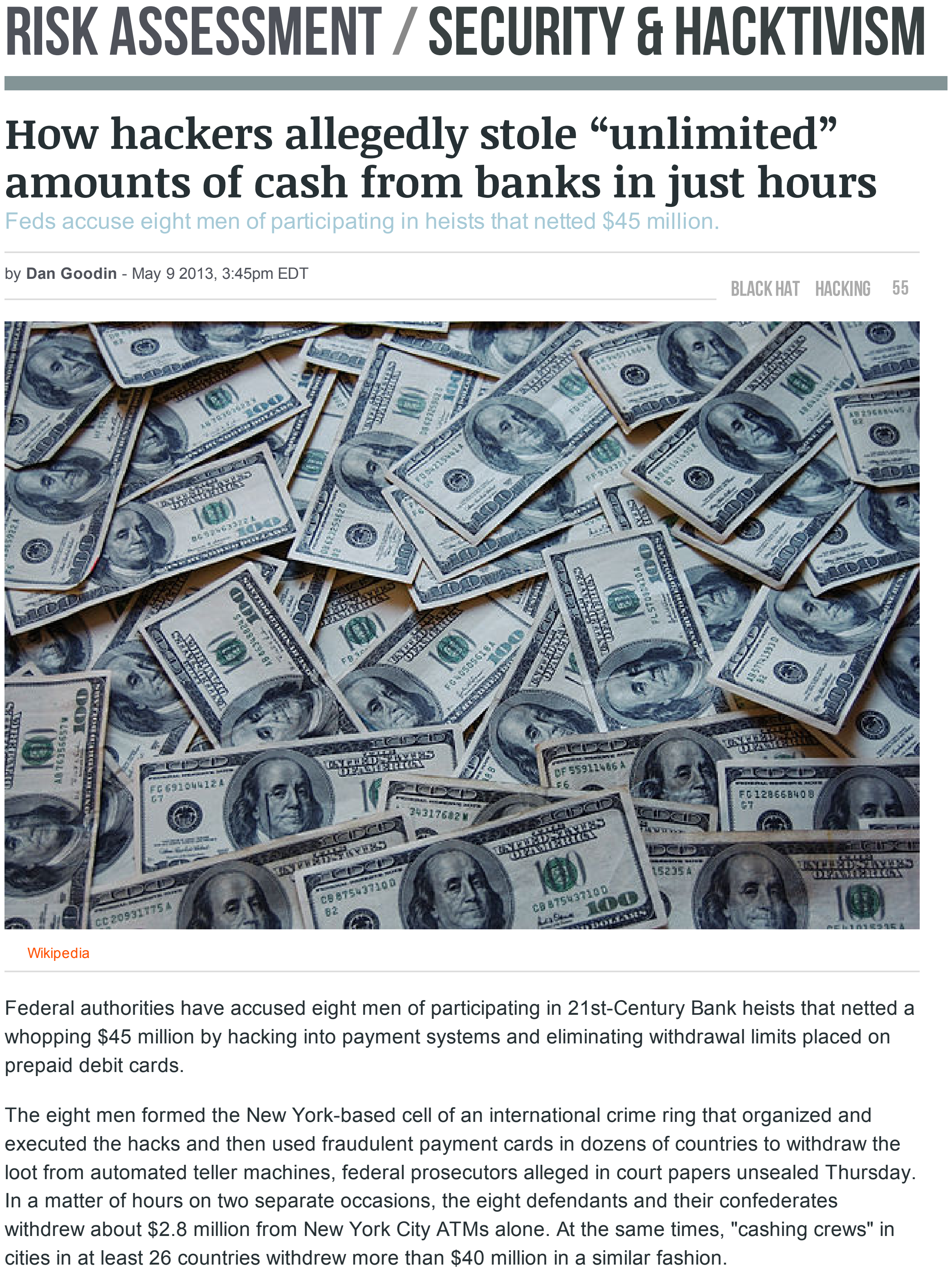
STRONGER TOGETHER
BREAKING NEWS
FBI & STATE DEPARTMENT DENY CLINTON EMAIL DEAL
CNN
Top stories
Ken Bone leaves seedy comment trail
Quintuplets all work at same McDonald's
Now Playing
FBI, State Department deny Clinton email
FBI clears Clinton in email probe
Fact checking Clinton's public
FBI combing through Hillary Clinton aide's
Trump: Clinton guilty and

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

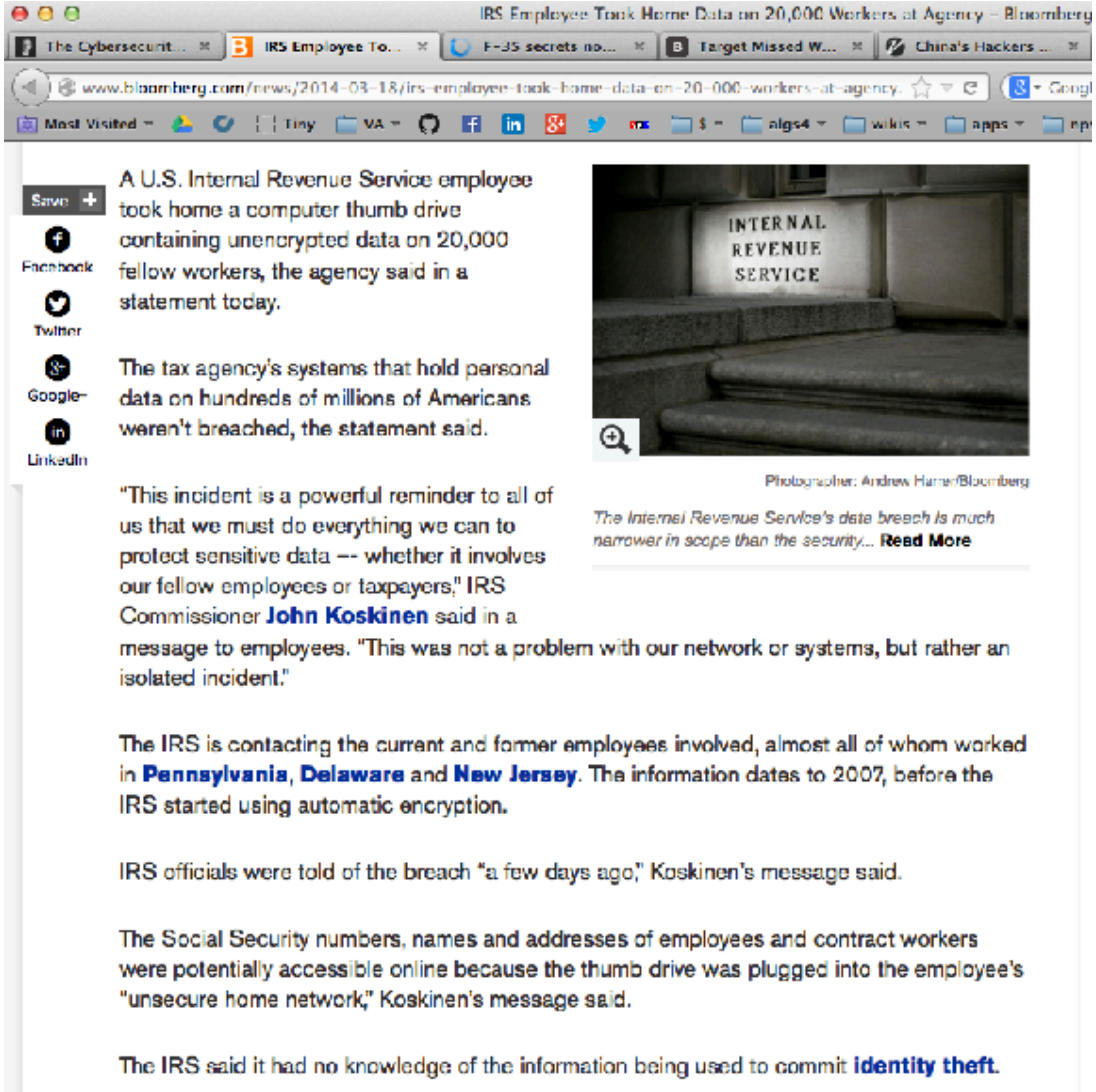
Federal authorities have accused eight men of participating in 21st-Century Bank heists that netted a whopping $45 million by hacking into payment systems and eliminating withdrawal limits placed on prepaid debit cards.

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.

http://arstechnica.com/security/2013/05/how-hackers-allegedly-stole-unlimited-amounts-of-cash-from-banks-in-just-hours/

May 2013

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



A U.S. Internal Revenue Service employee took home a computer thumb drive containing unencrypted data on 20,000 fellow workers, the agency said in a statement today.

The tax agency's systems that hold personal data on hundreds of millions of Americans weren't breached, the statement said.

"This incident is a powerful reminder to all of us that we must do everything we can to protect sensitive data -- whether it involves our fellow employees or taxpayers," IRS Commissioner **John Koskinen** said in a message to employees. "This was not a problem with our network or systems, but rather an isolated incident."

Photographer: Andrew Harrer/Bloomberg

The Internal Revenue Service's data breach is much narrower in scope than the security... **Read More**

The IRS is contacting the current and former employees involved, almost all of whom worked in **Pennsylvania**, **Delaware** and **New Jersey**. The information dates to 2007, before the IRS started using automatic encryption.

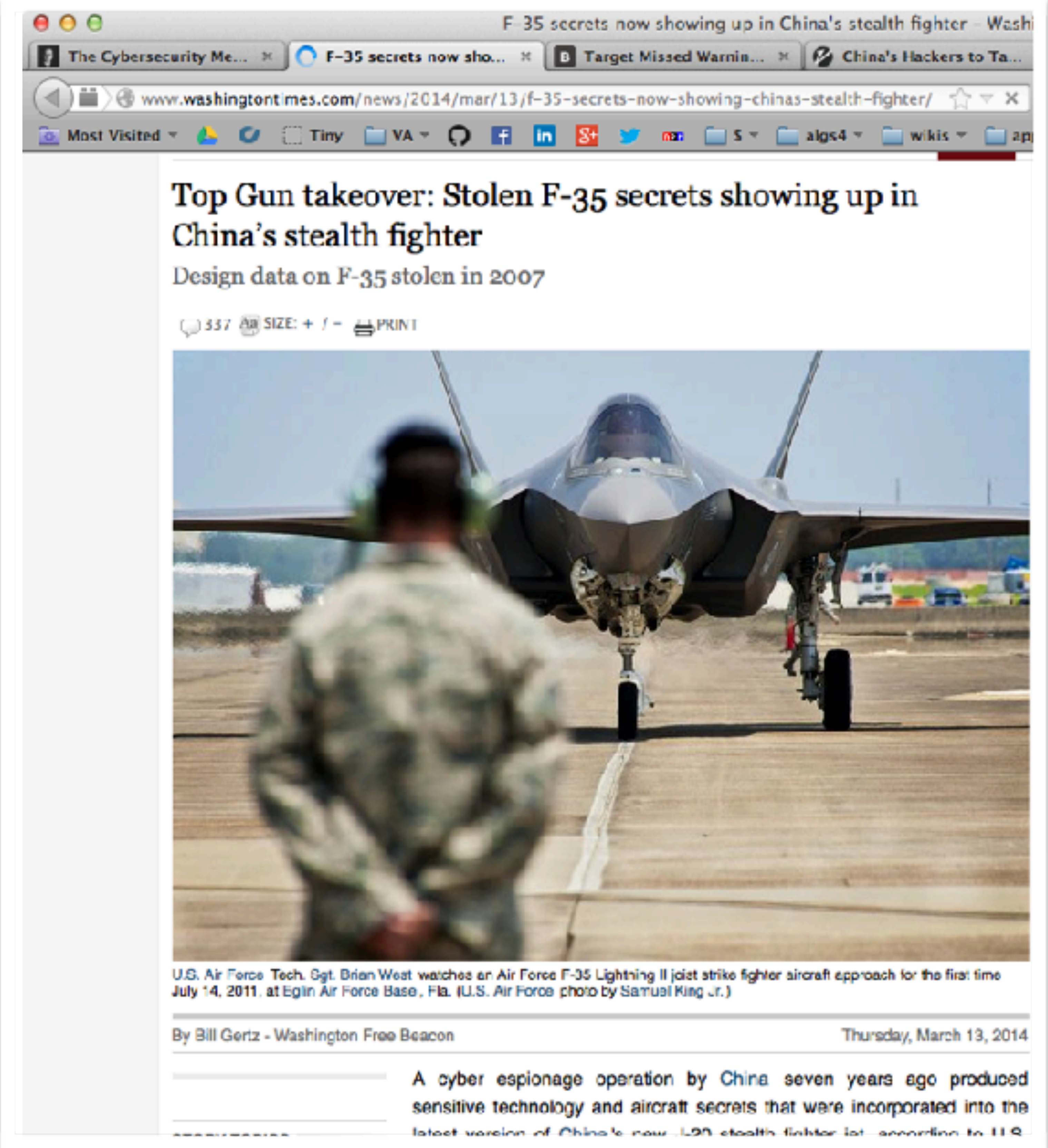
IRS officials were told of the breach "a few days ago," Koskinen's message said.

The Social Security numbers, names and addresses of employees and contract workers were potentially accessible online because the thumb drive was plugged into the employee's "unsecure home network," Koskinen's message said.

The IRS said it had no knowledge of the information being used to commit **identity theft**.

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


F-35 secrets now showing up in China's stealth fighter - Washi
The Cybersecurity Me...
F-35 secrets now sho...
Target Missed Warnin...
China's Hackers to Ta...
www.washingtontimes.com/news/2014/mar/13/f-35-secrets-now-showing-chinas-stealth-fighter/
Most Visited
Tiny
VA
S
algs4
wikis
ap
337
SIZE: + / −
PRINT

Top Gun takeover: Stolen F-35 secrets showing up in China’s stealth fighter

Design data on F-35 stolen in 2007

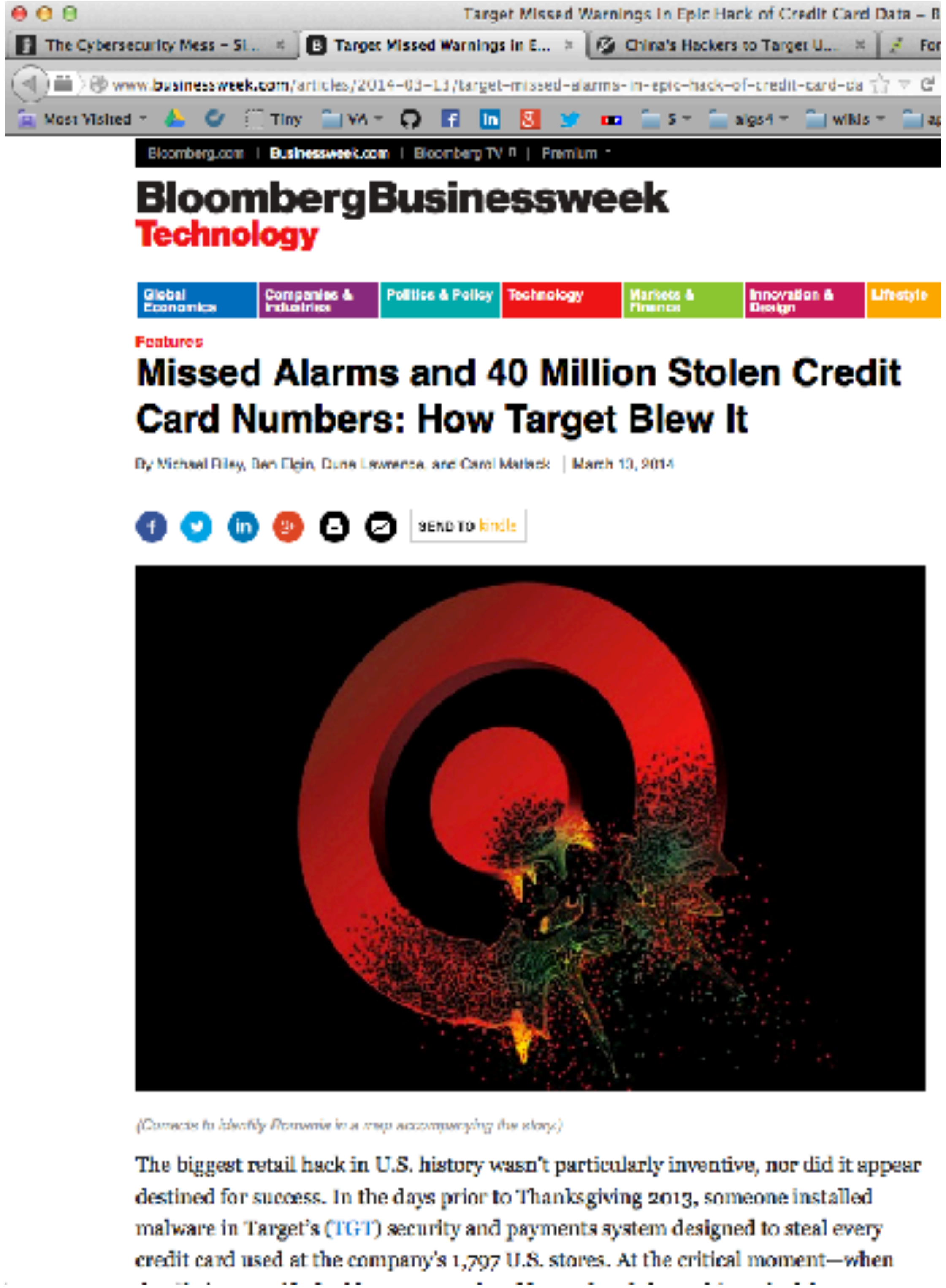
U.S. Air Force Tech. Sgt. Brian West watches an Air Force F-35 Lightning II joist strike fighter aircraft approach for the first time July 14, 2011, at Eglin Air Force Base, Fla. (U.S. Air Force photo by Samuel King Jr.)

By Bill Gertz - Washington Free Beacon

Thursday, March 13, 2014

A cyber espionage operation by China seven years ago produced sensitive technology and aircraft secrets that were incorporated into the latest version of China's new J-20 stealth fighter jet, according to U.S.

March 2014: Target ignored alarms before hack.


Target Missed Warnings in Epic Hack of Credit Card Data – B
The Cybersecurity Mess – Sl...
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
5
algs4
wikis
Bloomberg.com | Businessweek.com | Bloomberg TV | Premium
Global Economics
Companies & Industries
Politics & Policy
Technology
Markets & Finance
Innovation & Design
Lifestyle
SEND TO kindle

BloombergBusinessweek
Technology

Features

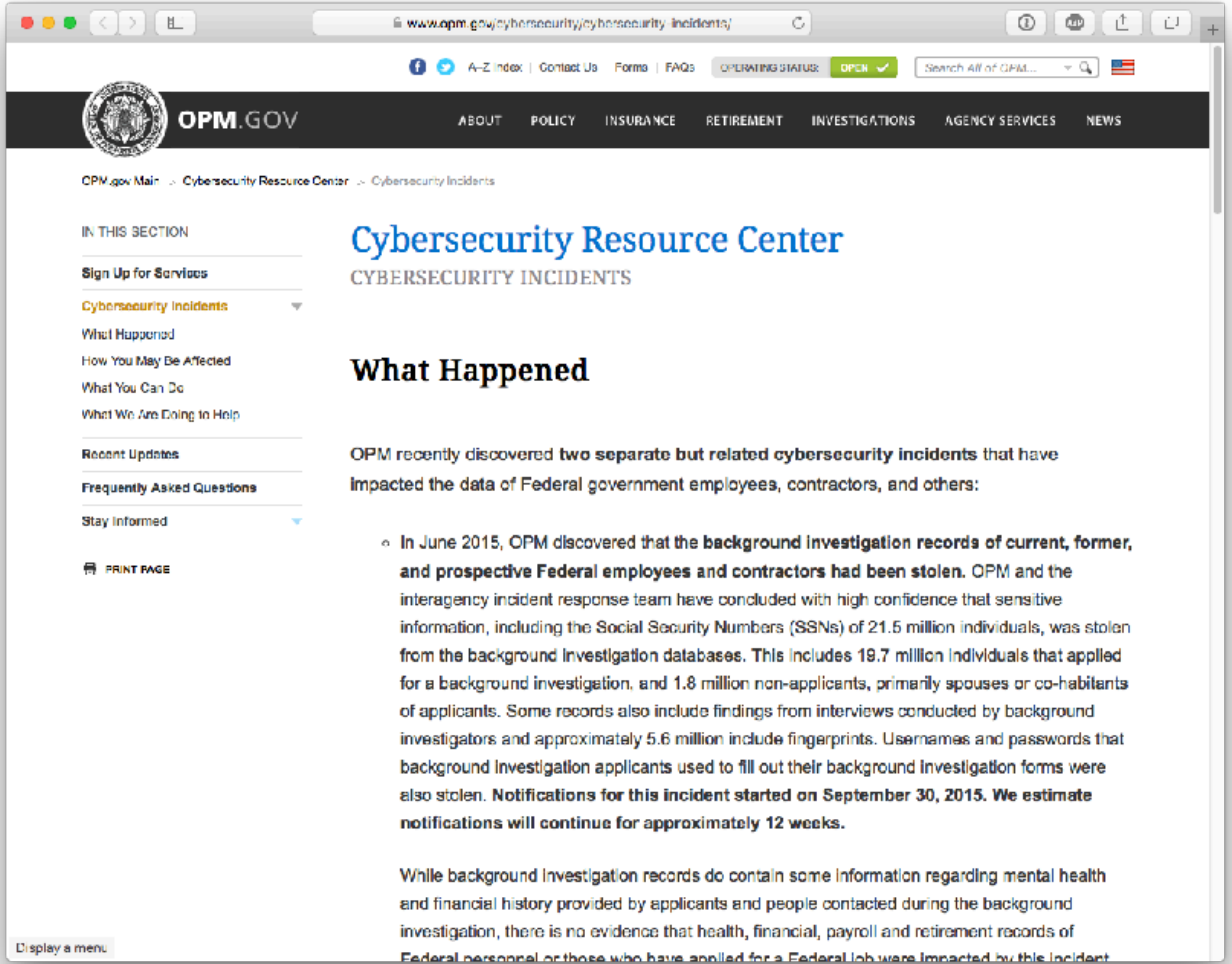
Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

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



Cybersecurity Resource Center

CYBERSECURITY INCIDENTS

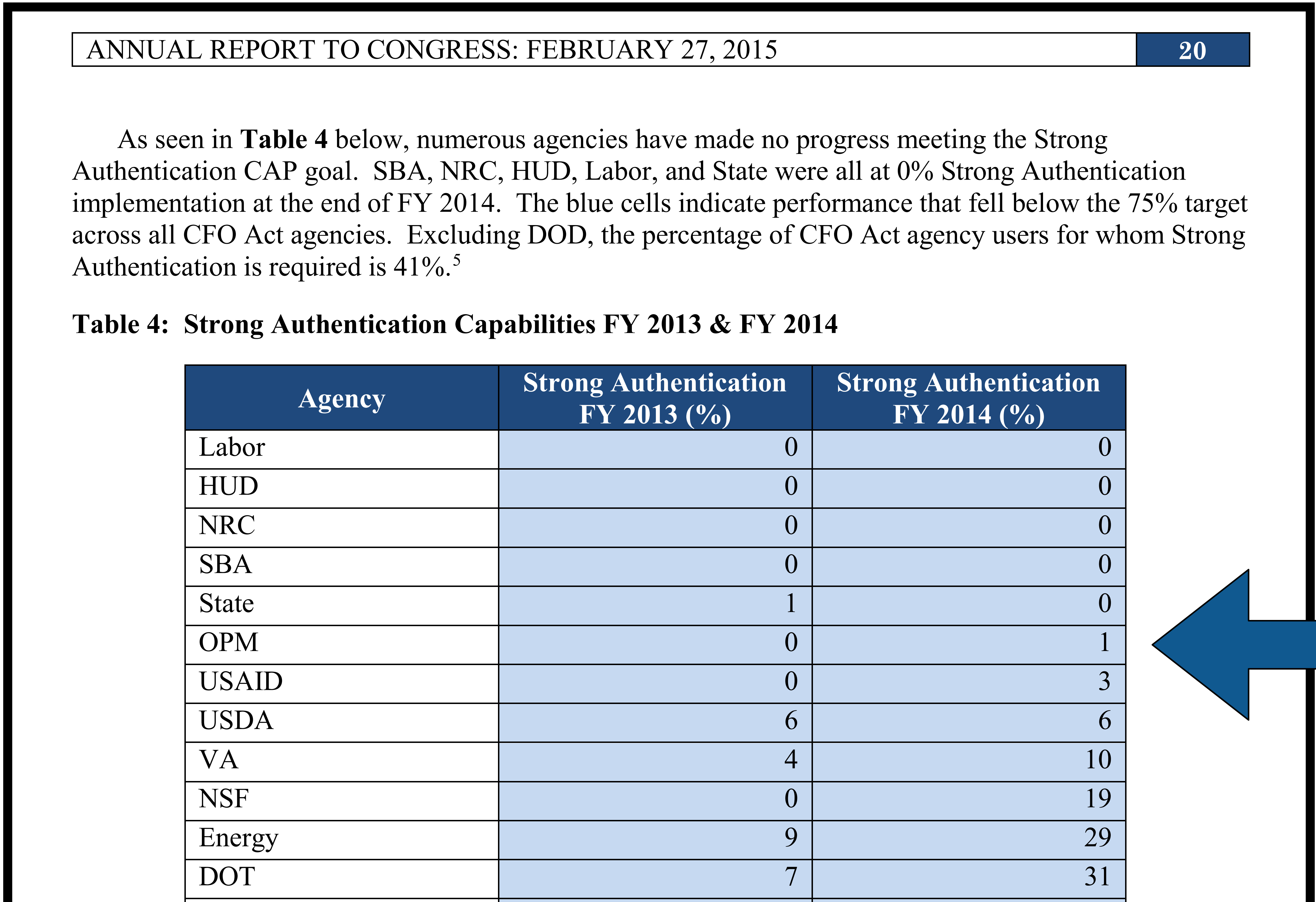
What Happened

OPM recently discovered **two separate but related cybersecurity incidents** that have impacted the data of Federal government employees, contractors, and others:

- In June 2015, OPM discovered that the **background investigation records of current, former, and prospective Federal employees and contractors had been stolen.** OPM and the interagency incident response team have concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, primarily spouses or co-habitants of applicants. Some records also include findings from interviews conducted by background investigators and approximately 5.6 million include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen. **Notifications for this incident started on September 30, 2015. We estimate notifications will continue for approximately 12 weeks.**

  While background investigation records do contain some information regarding mental health and financial history provided by applicants and people contacted during the background investigation, there is no evidence that health, financial, payroll and retirement records of Federal personnel or those who have applied for a Federal job were impacted by this incident

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

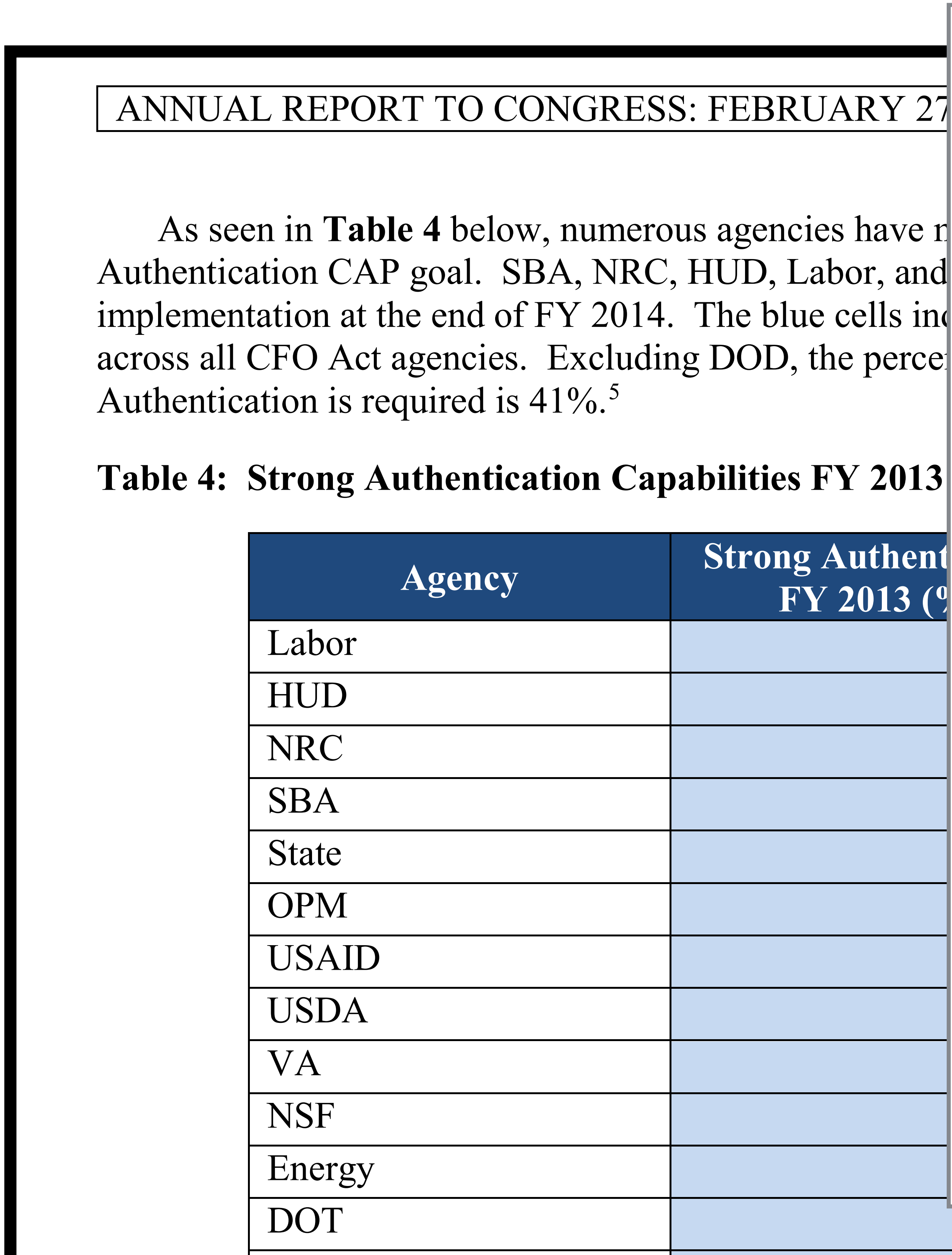


As seen in **Table 4** below, numerous agencies have made no progress meeting the Strong Authentication CAP goal. SBA, NRC, HUD, Labor, and State were all at 0% Strong Authentication implementation at the end of FY 2014. The blue cells indicate performance that fell below the 75% target across all CFO 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

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

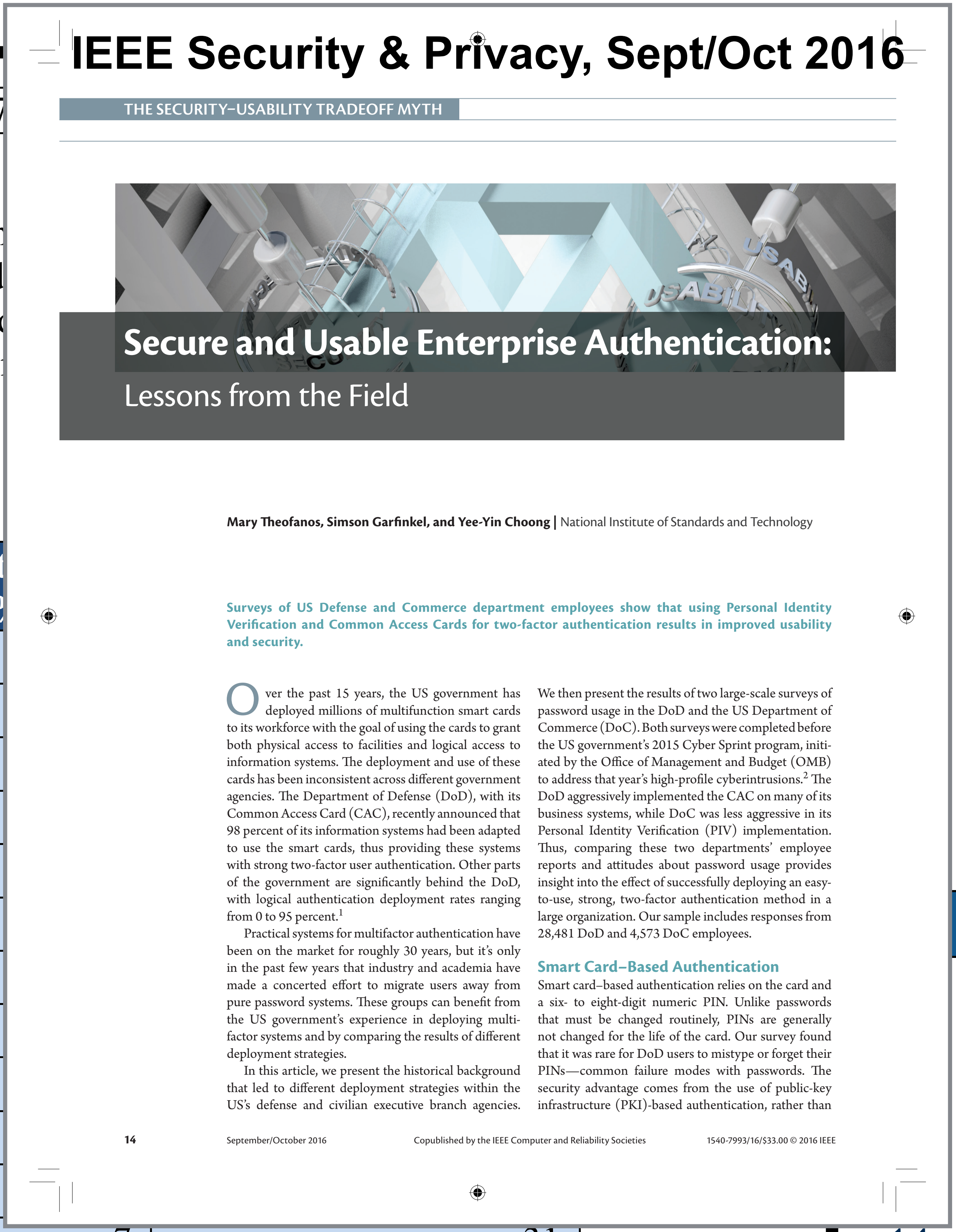


ANNUAL REPORT TO CONGRESS: FEBRUARY 27

As seen in **Table 4** below, numerous agencies have n
Authentication CAP goal. SBA, NRC, HUD, Labor, and
implementation at the end of FY 2014. The blue cells ind
across all CFO Act agencies. Excluding DOD, the percen
Authentication is required is 41%.[5]

Table 4: Strong Authentication Capabilities FY 2013

Agency	Strong Authent FY 2013 (%	
Labor		
HUD		
NRC		
SBA		
State		
OPM		
USAID		
USDA		
VA		
NSF		
Energy		
DOT	7	31



IEEE Security & Privacy, Sept/Oct 2016

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.

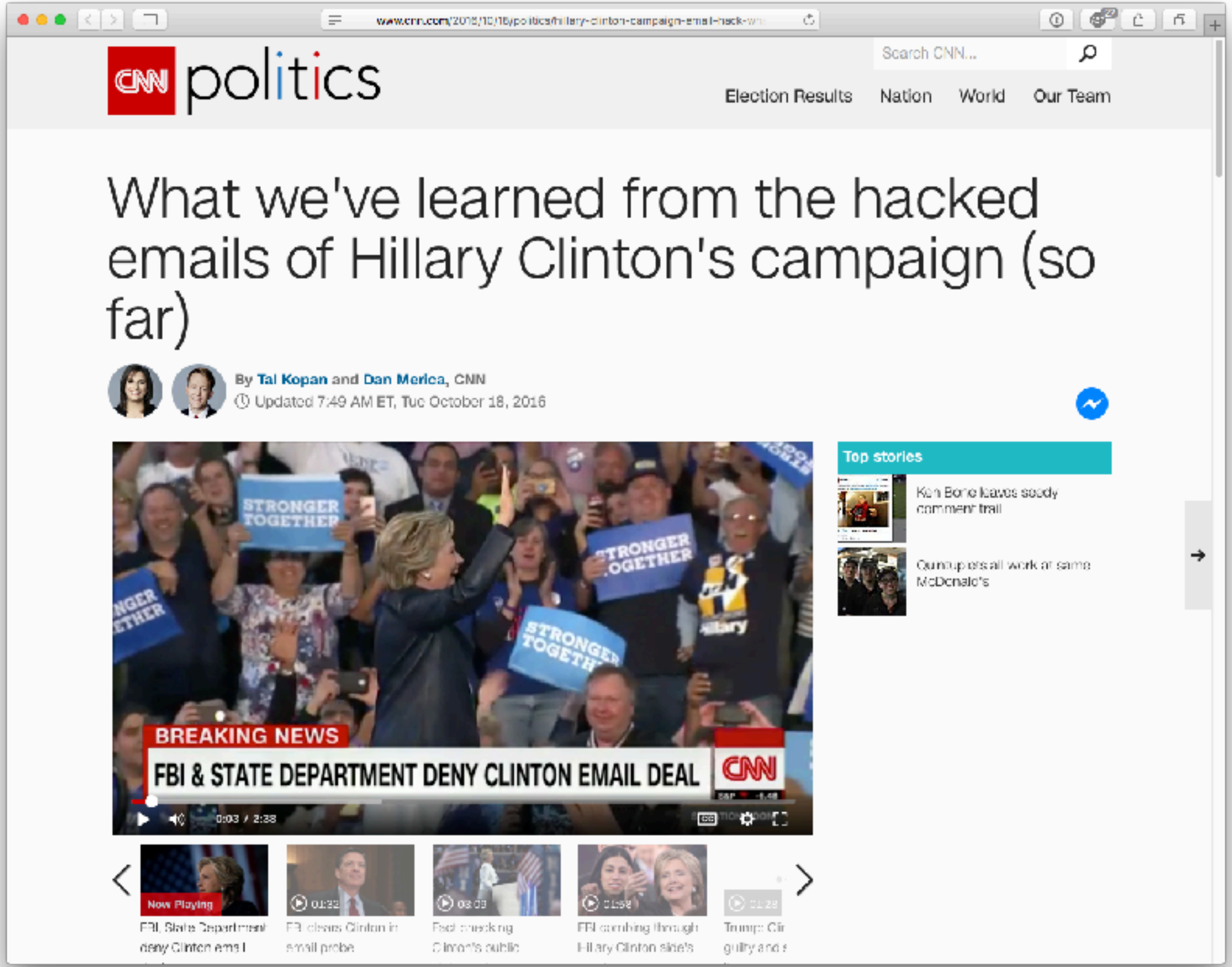
In this article, we present the historical background that led to different deployment strategies within the US's defense and civilian executive branch agencies. We then present the results of two large-scale surveys of password usage in the DoD and the US Department of Commerce (DoC). Both surveys were 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

1540-7993/16/$33.00 © 2016 IEEE

Summer 2016...



www.cnn.com/2016/10/16/politics/hillary-clinton-campaign-email-hack-wi
CNN politics
Search CNN...
Election Results
Nation
World
Our Team

What we've learned from the hacked emails of Hillary Clinton's campaign (so far)

By Tal Kopan and Dan Merica, CNN

Updated 7:49 AM ET, Tue October 18, 2016

Top stories

Ken Bone leaves seedy comment trail

Quintuplets all work at same McDonald's

FBI, State Department deny Clinton emai

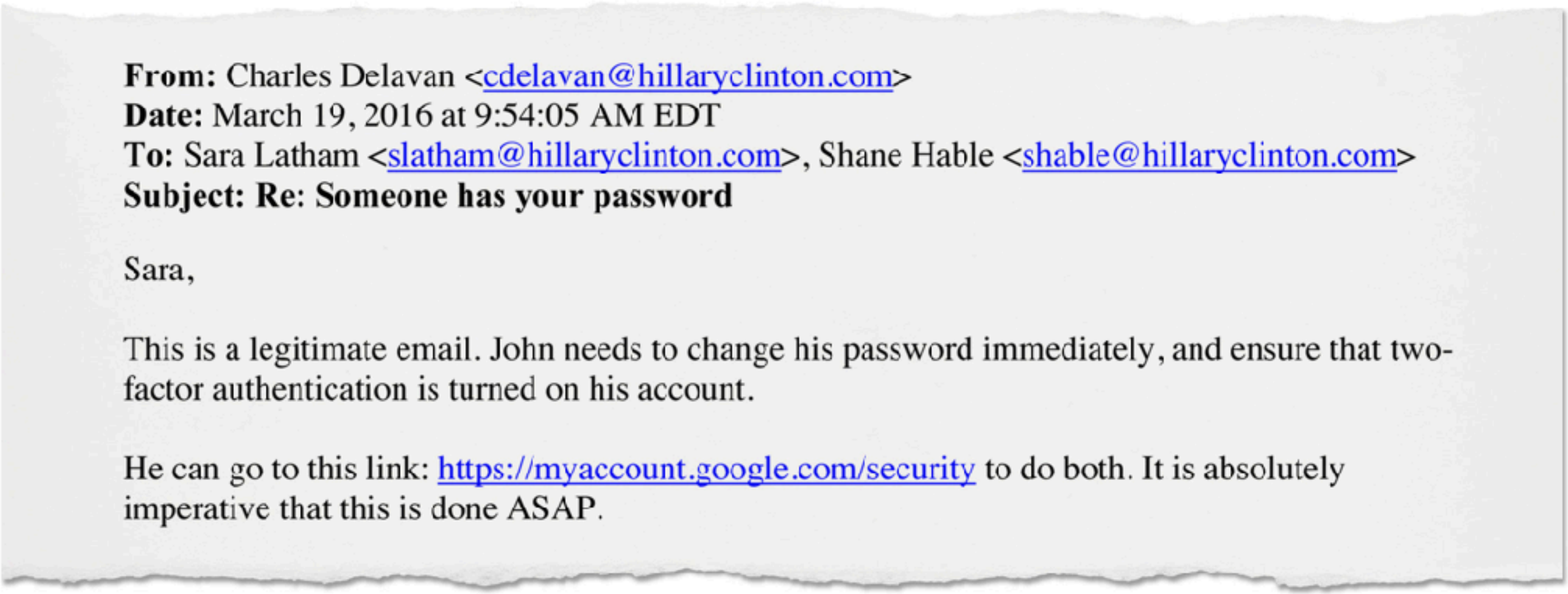
FBI clears Clinton in email probe

Fact-checking Clinton's public

FBI combing through Hillary Clinton aide's

Trump: Cli guilty and s

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... is undefined.

“Cybernetics”

Norbert Weiner
1948

“Cyberspace”

William Gibson
1982

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.

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:

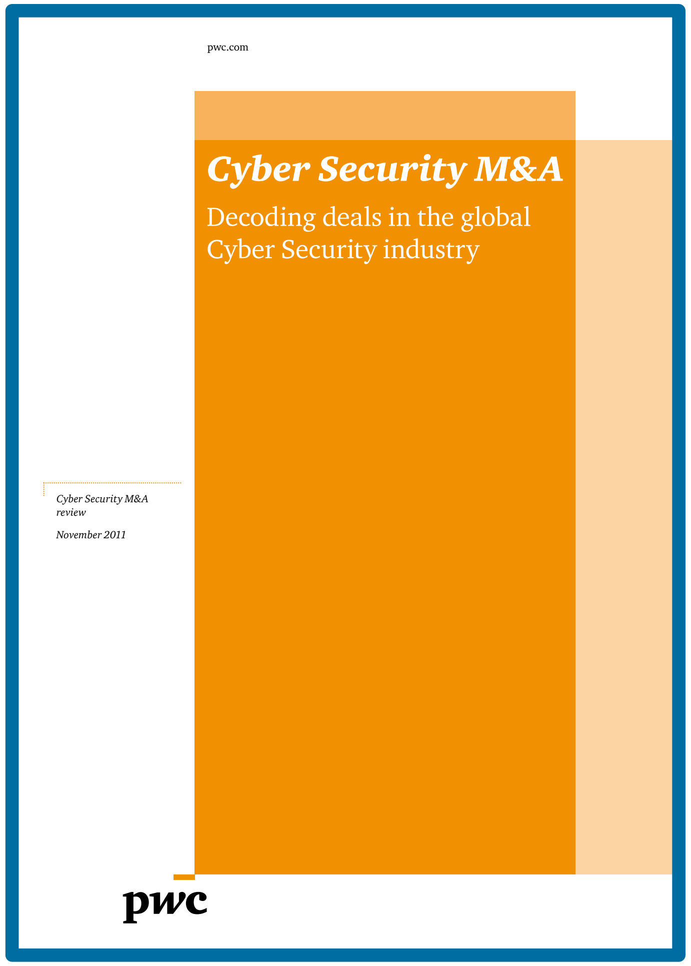
- Spending $5.3 billion per year on cyber security.
- Stopping 69% of attacks.

If they raise spending...

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

95% is not good enough.

Spending more money does not make a computer more secure.



pwc.com

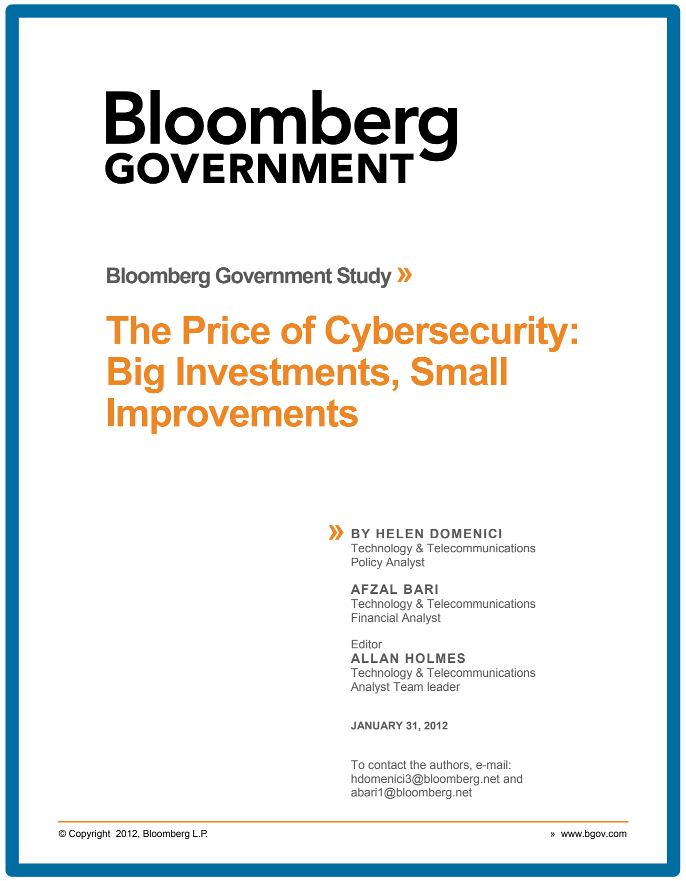
Cyber Security M&A

Decoding deals in the global Cyber Security industry

Cyber Security M&A review

November 2011

pwc



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

© Copyright 2012, Bloomberg L.P. » www.bgov.com

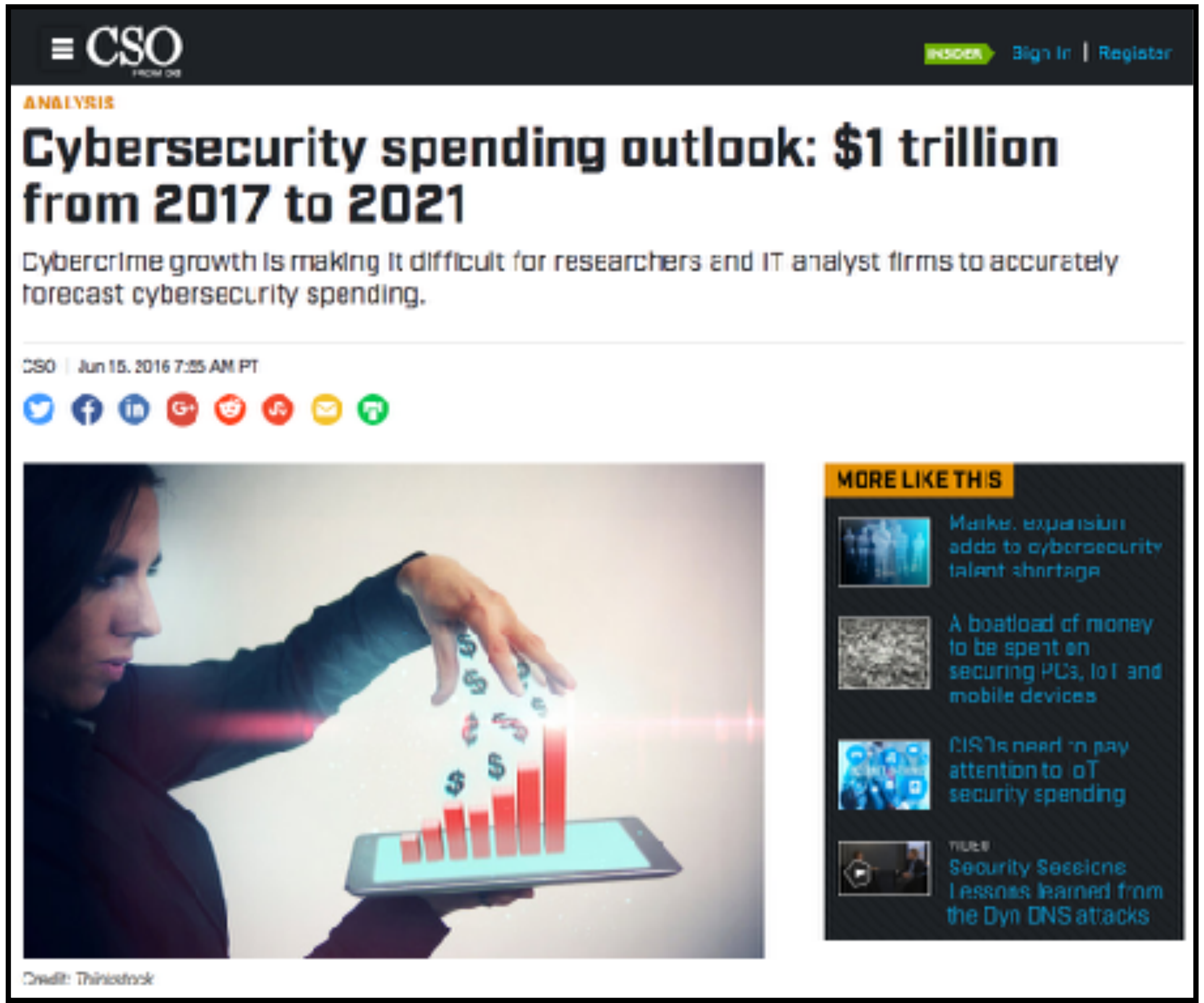
Expenditures are increasing...

$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/*



ANALYSIS

Cybersecurity spending outlook: $1 trillion from 2017 to 2021

Cybercrime growth is making it difficult for researchers and IT analyst firms to accurately forecast cybersecurity spending.

CSO | Jun 15, 2016 7:55 AM PT

Credit: Thinkstock

Market expansion adds to cybersecurity talent shortage

A boatload of money to be spent on securing PCs, IoT and mobile devices

CISOs need to pay attention to IoT security spending

VIDEO

Security Sessions Lessons learned from the Dyn DNS attacks

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.

OpenSSL™
Cryptography and SSL/TLS Toolkit

SSH...
OpenSSH
KEEPING YOUR COMMUNIQUÉS SECRET
TOP SECRET

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.”

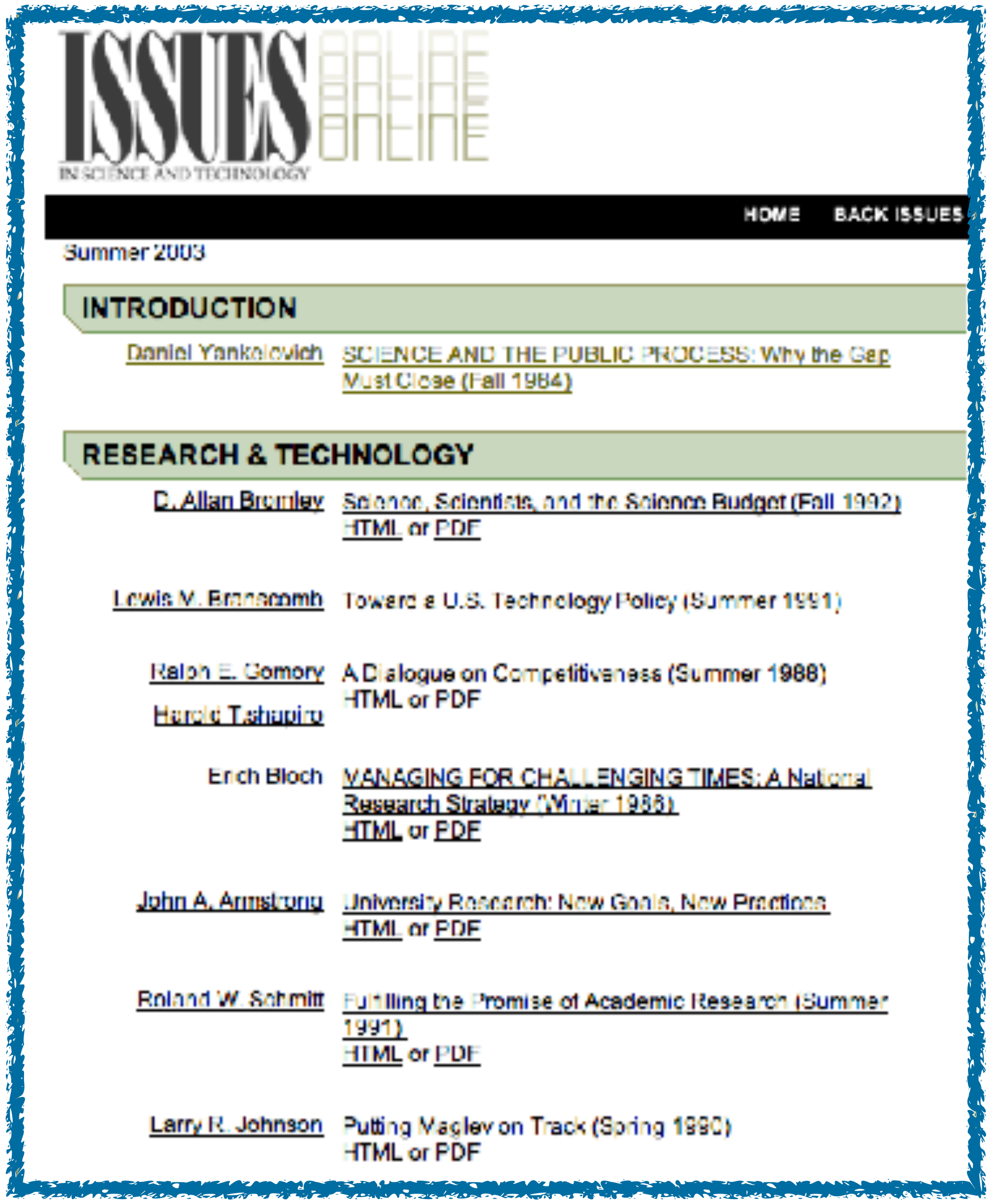
http://www.nytimes.com/2011/06/30/technology/30morris.html

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

"Computer Insecurity", Peter G. Neumann

Issues In Science & Technology, Fall 1994

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



Summer 2003

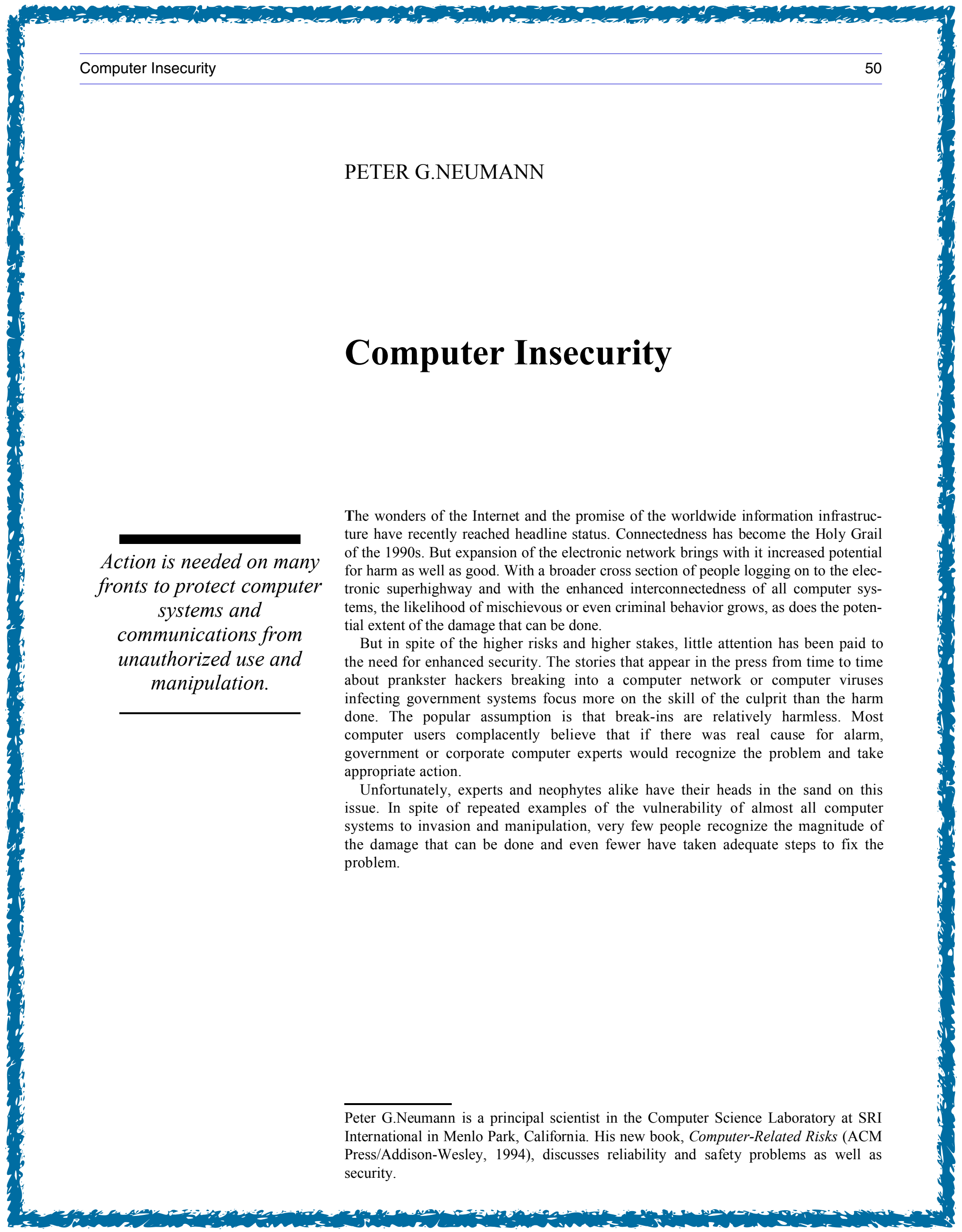
INTRODUCTION

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.

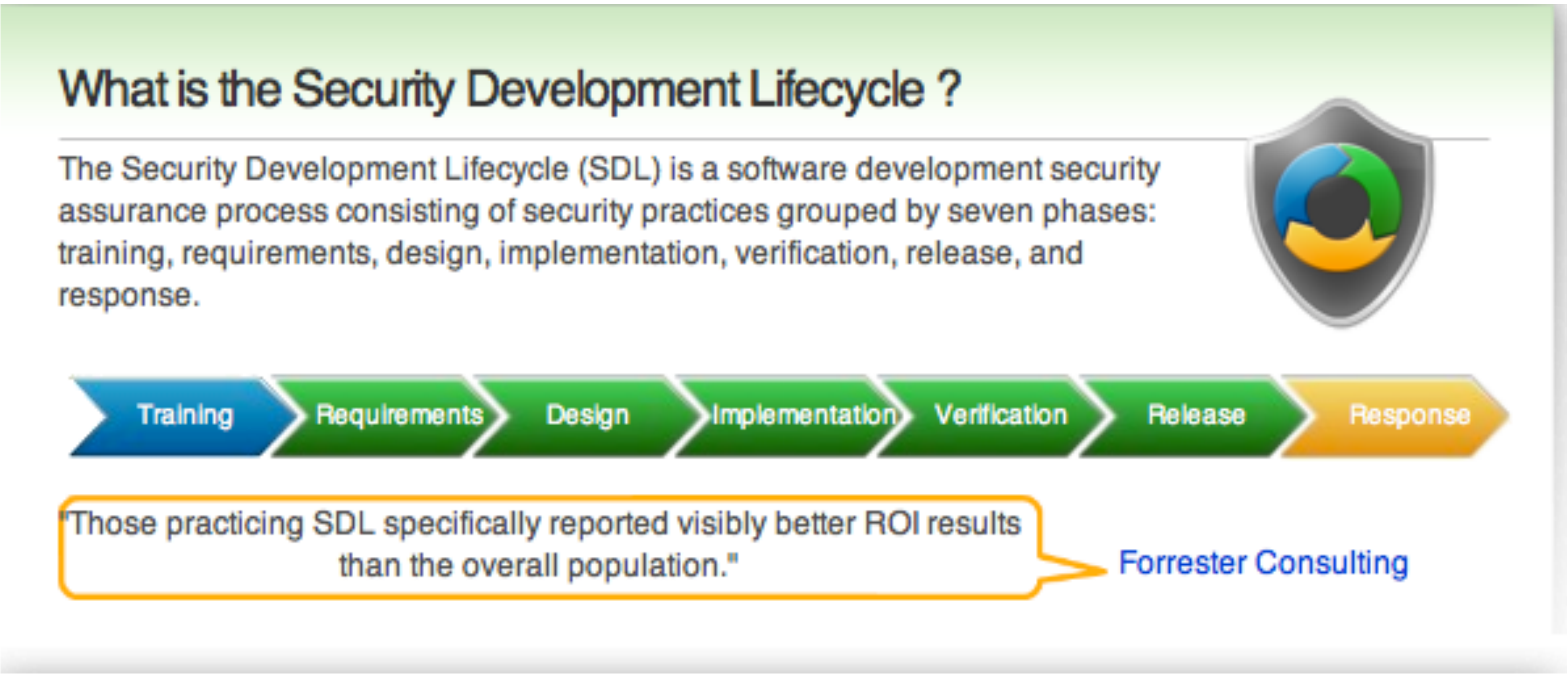
Peter G.Neumann is a principal scientist in the Computer Science Laboratory at SRI International in Menlo Park, California. His new book, *Computer-Related Risks* (ACM Press/Addison-Wesley, 1994), discusses reliability and safety problems as well as security.

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



What is the Security Development Lifecycle ?

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

Training → Requirements → Design → Implementation → Verification → Release → Response

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

Forrester Consulting

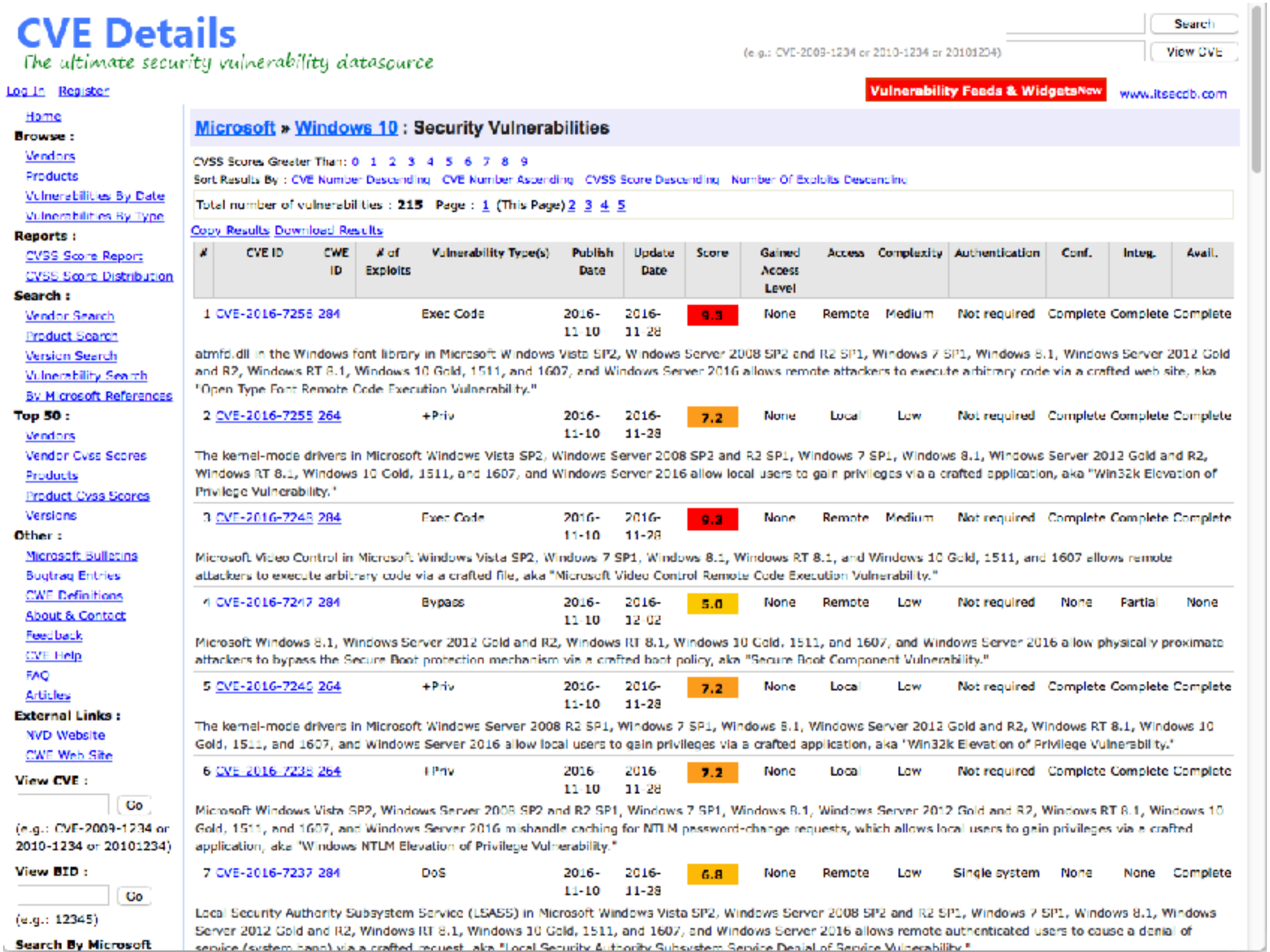
“Security is a process, not a product”

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

—*Few organizations can afford SDL.*

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

Windows 10: 215 vulnerabilities...



CVE Details

The ultimate security vulnerability datasource

Search

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

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

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2016-7256</td><td>284</td><td></td><td>Exec Code</td><td>2016-11-10</td><td>2016-11-28</td><td>9.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">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."</td></tr>
<tr><td>2</td><td>CVE-2016-7255</td><td>264</td><td></td><td>+Priv</td><td>2016-11-10</td><td>2016-11-28</td><td>7.2</td><td>None</td><td>Local</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">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."</td></tr>
<tr><td>3</td><td>CVE-2016-7248</td><td>284</td><td></td><td>Exec Code</td><td>2016-11-10</td><td>2016-11-28</td><td>9.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">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."</td></tr>
<tr><td>4</td><td>CVE-2016-7247</td><td>284</td><td></td><td>Bypass</td><td>2016-11-10</td><td>2016-12-02</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">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."</td></tr>
<tr><td>5</td><td>CVE-2016-7246</td><td>264</td><td></td><td>+Priv</td><td>2016-11-10</td><td>2016-11-28</td><td>7.2</td><td>None</td><td>Local</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">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."</td></tr>
<tr><td>6</td><td>CVE-2016-7238</td><td>264</td><td></td><td>+Priv</td><td>2016-11-10</td><td>2016-11-28</td><td>7.2</td><td>None</td><td>Local</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">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."</td></tr>
<tr><td>7</td><td>CVE-2016-7237</td><td>284</td><td></td><td>DoS</td><td>2016-11-10</td><td>2016-11-28</td><td>6.8</td><td>None</td><td>Remote</td><td>Low</td><td>Single system</td><td>None</td><td>None</td><td>Complete</td></tr>
<tr><td colspan="15">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."</td></tr>
</table>

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”

Chatham House • Oct. 2011
Cyber Security
As 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*

Is it the technology?

Why is the cyber *so* hard?

Cyber Security has an active, malicious adversary.

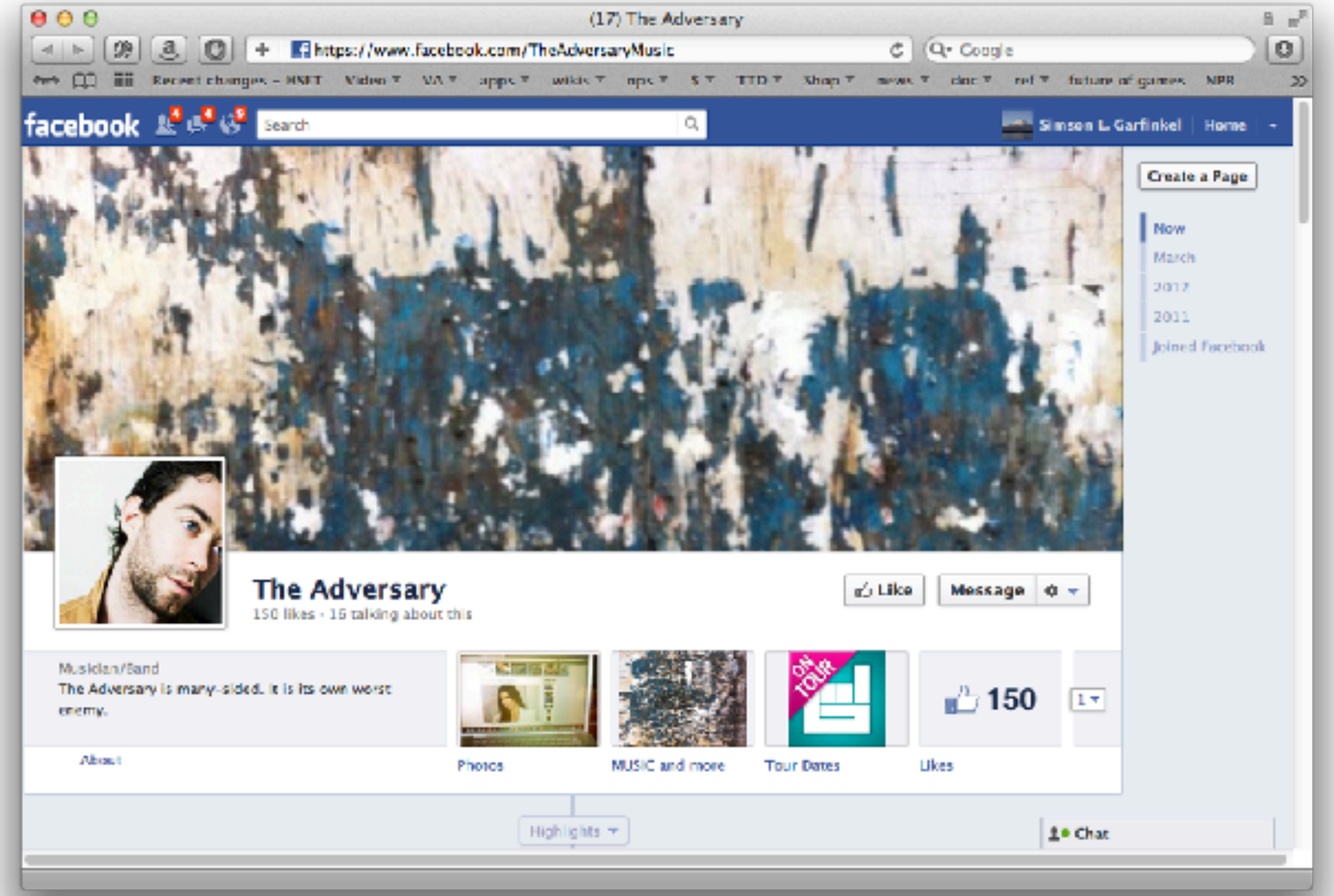
The adversary...

Turns your bugs into exploits

Adapts to your defenses

Waits until you make a mistake

Attacks your employees when your systems are secure



(17) The Adversary

https://www.facebook.com/TheAdversaryMusic

The Adversary

150 likes · 16 talking about this

Musician/Band

The Adversary is many-sided. It is its own worst enemy.

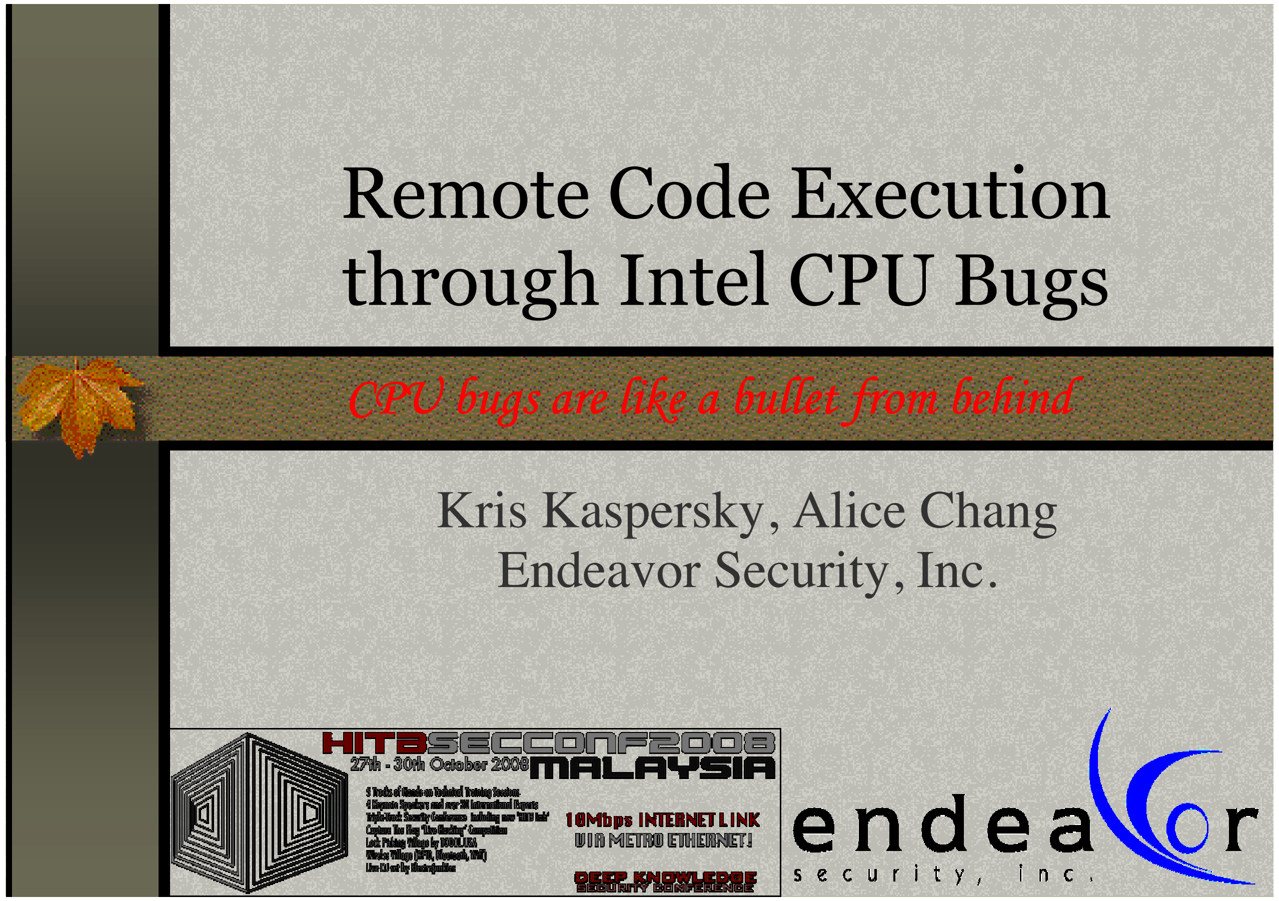
Bugs in CPU silicon are remotely exploitable!

This means:

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

Kaspersky:

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



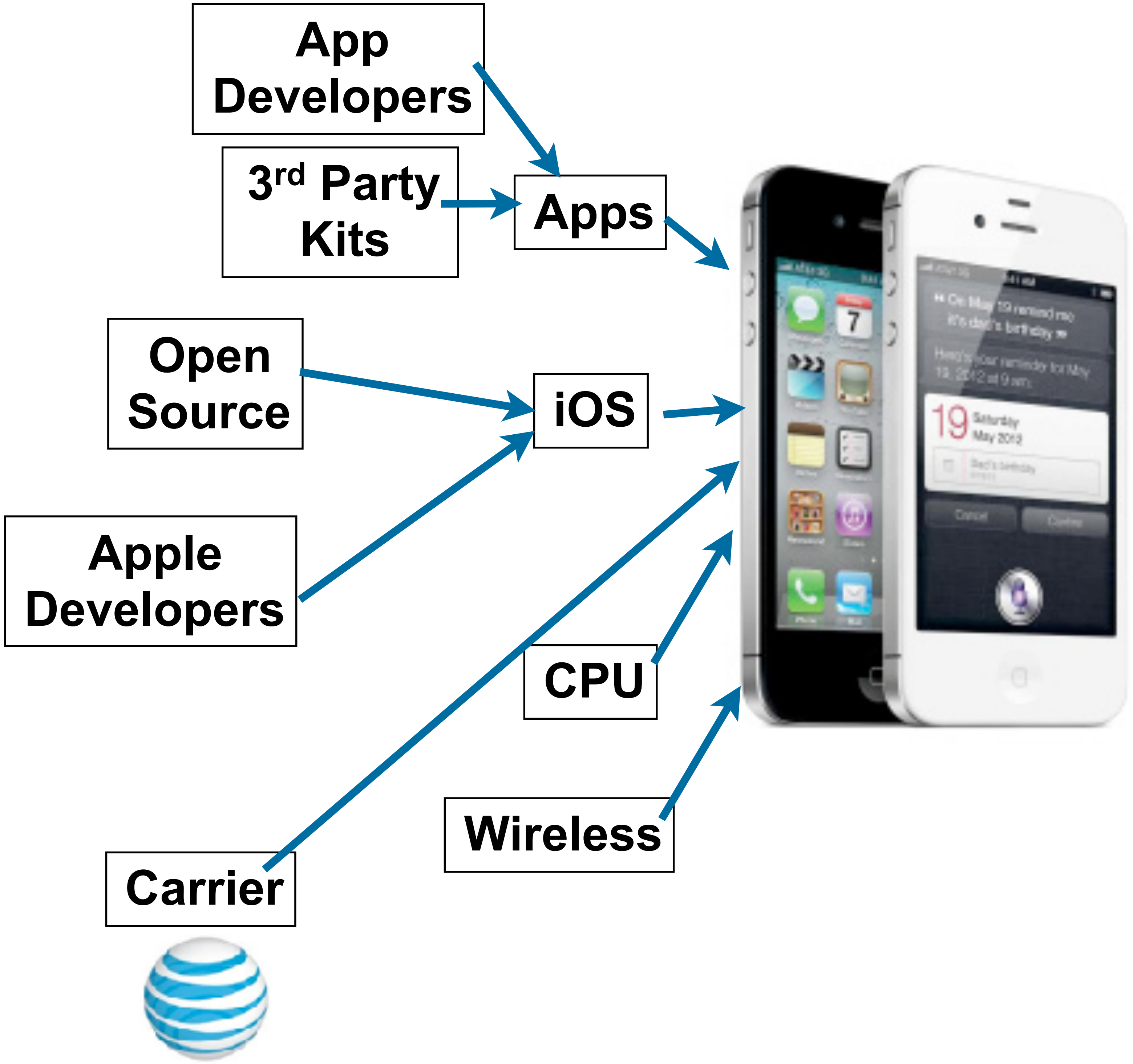
Remote Code Execution through Intel CPU Bugs

CPU bugs are like a bullet from behind

Kris Kaspersky, Alice Chang
Endeavor Security, Inc.

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



App Developers

3rd Party Kits

Apps

Open Source

iOS

Apple Developers

CPU

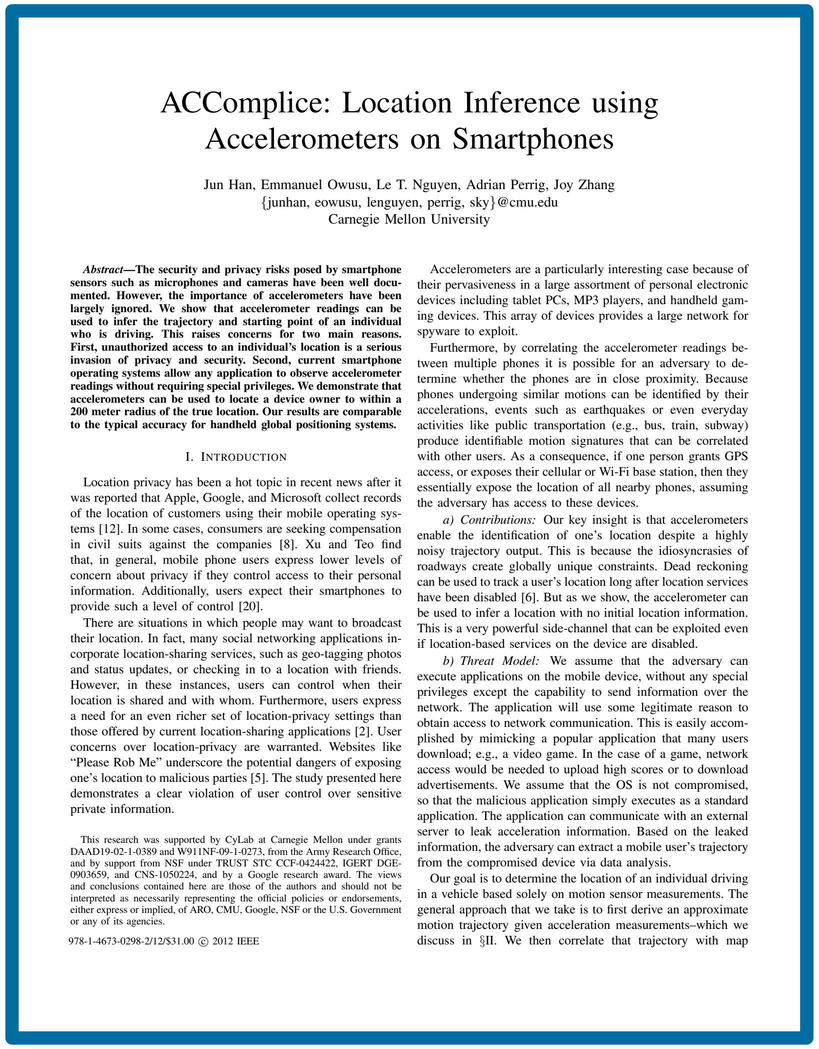
Wireless

Carrier

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.

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.

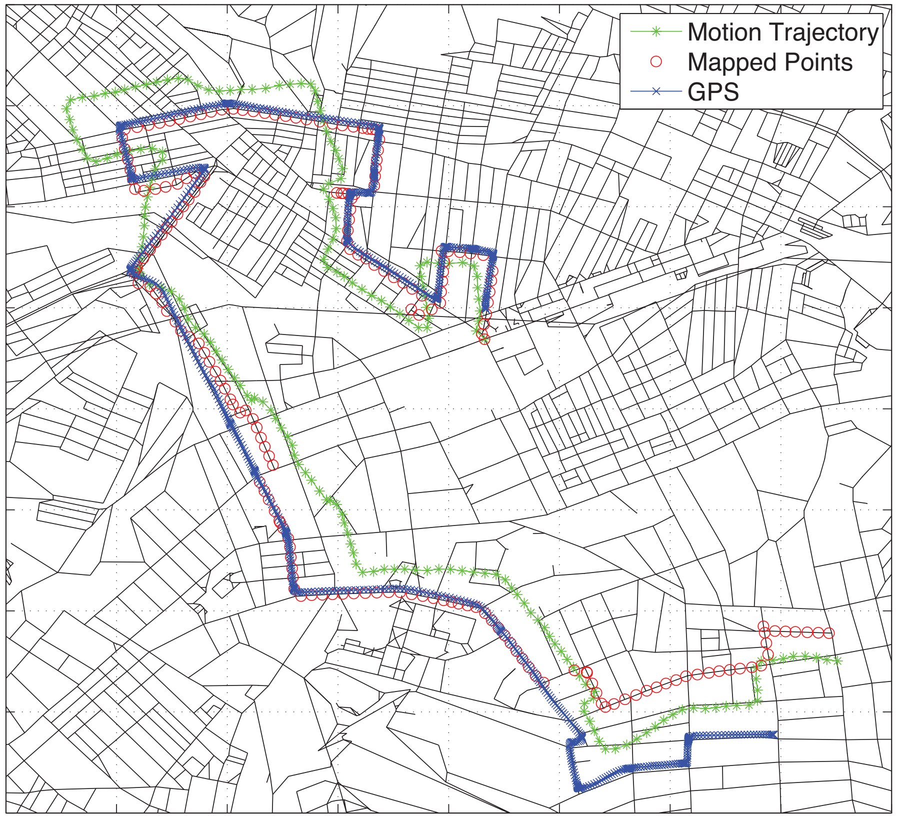
a) Contributions: Our key insight is that accelerometers enable the identification of one's location despite a highly noisy trajectory output. This is because the idiosyncrasies of roadways create globally unique constraints. Dead reckoning can be used to track a user's location long after location services 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

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



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.

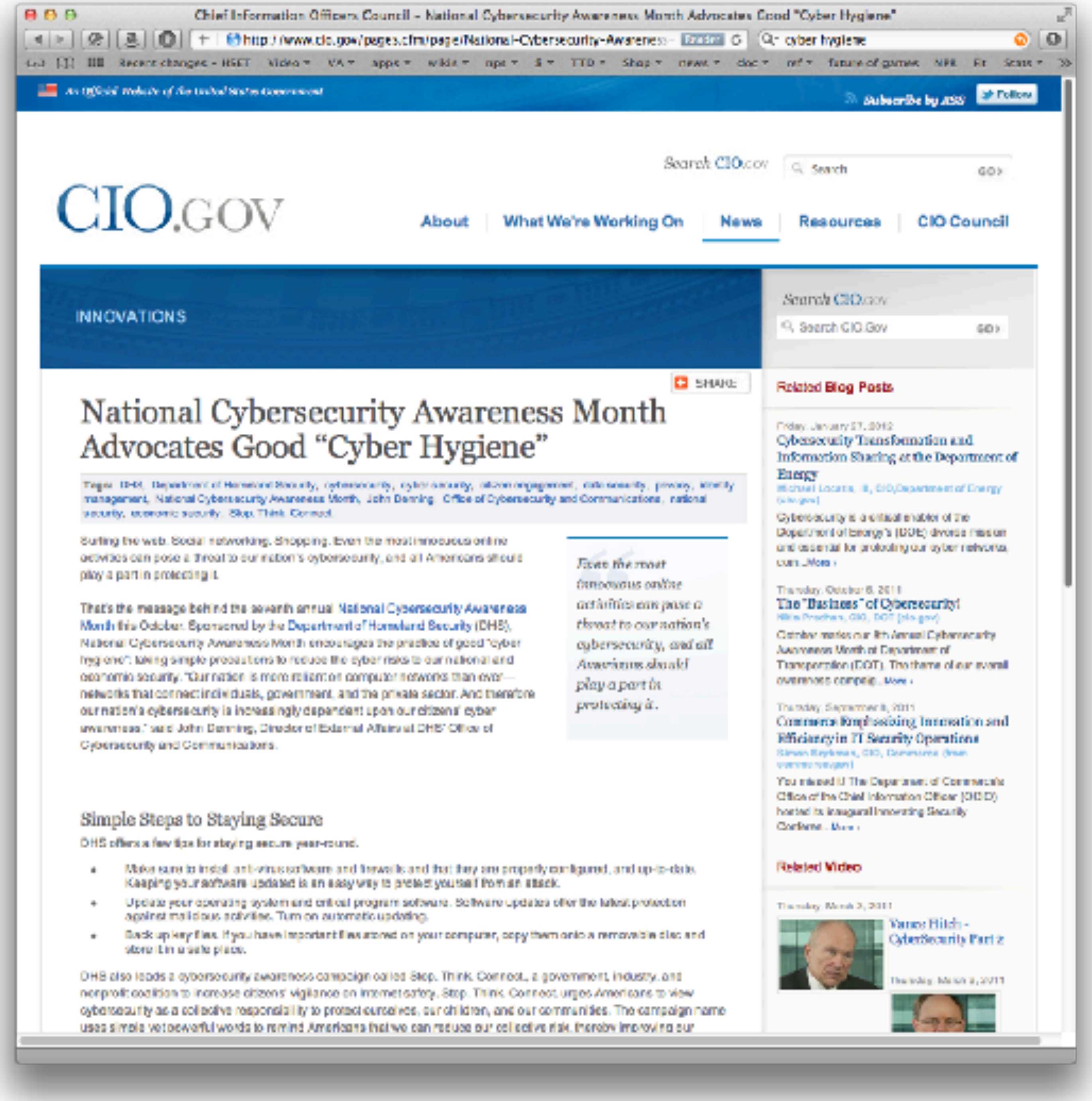
**6 accelerometers
no privacy**

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”



National Cybersecurity Awareness Month Advocates Good “Cyber Hygiene”

Tags: DHS, Department of Homeland Security, cybersecurity, cyber security, citizen engagement, data security, privacy, identity management, National Cybersecurity Awareness Month, John Denning, Office of Cybersecurity and Communications, national security, economic security, Stop. Think. Connect.

Surfing the web. Social networking. Shopping. Even the most innocuous online activities can pose a threat to our nation's cybersecurity, and all Americans should play a part in protecting it.

That's the message behind the seventh annual National Cybersecurity Awareness Month this October. Sponsored by the Department of Homeland Security (DHS), National Cybersecurity Awareness Month encourages the practice of good "cyber hygiene": taking simple precautions to reduce the cyber risks to our national and economic security. "Our nation is more reliant on computer networks than ever—networks that connect individuals, government, and the private sector. And therefore our nation's cybersecurity is increasingly dependent upon our citizens' cyber awareness," said John Denning, Director of External Affairs at DHS' Office of Cybersecurity and Communications.

Even the most innocuous online activities can pose a threat to our nation's cybersecurity, and all Americans should play a part in protecting it.

Simple Steps to Staying Secure

DHS offers a few tips for staying secure year-round.

- Make sure to install anti-virus software and firewalls and that they are properly configured, and up-to-date. Keeping your software updated is an easy way to protect yourself from an attack.
- Update your operating system and critical program software. Software updates offer the latest protection against malicious activities. Turn on automatic updating.
- Back up key files. If you have important files stored on your computer, copy them onto a removable disc and store it in a safe place.

DHS also leads a cybersecurity awareness campaign called Stop. Think. Connect., a government, industry, and nonprofit coalition to increase citizens' vigilance on Internet safety. Stop. Think. Connect. urges Americans to view cybersecurity as a collective responsibility to protect ourselves, our children, and our communities. The campaign name uses simple yet powerful words to remind Americans that we can reduce our collective risk, thereby improving our

Related Blog Posts

Friday, January 27, 2012
Cybersecurity Transformation and Information Sharing at the Department of Energy
Michael Locatis, III, CIO, Department of Energy [cio.gov]
Cybersecurity is a critical enabler of the Department of Energy's (DOE) diverse mission and essential for protecting our cyber networks, com... More ›

Thursday, October 6, 2011
The "Business" of Cybersecurity!
Nitin Pradhan, CIO, DOT [cio.gov]
October marks our 8th Annual Cybersecurity Awareness Month at Department of Transportation (DOT). The theme of our overall awareness campaig... More ›

Thursday, September 8, 2011
Commerce Emphasizing Innovation and Efficiency in IT Security Operations
Simon Szykman, CIO, Commerce [from commerce.gov]
You missed it! The Department of Commerce's Office of the Chief Information Officer (OCIO) hosted its inaugural Innovating Security Conference... More ›

Related Video

Thursday, March 3, 2011
Vance Hitch - CyberSecurity Part 2

Thursday, March 3, 2011

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.

Obesity Rates Increase

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

The Obesity Action Coalition (OAC) is the only [illegible] advocacy and support

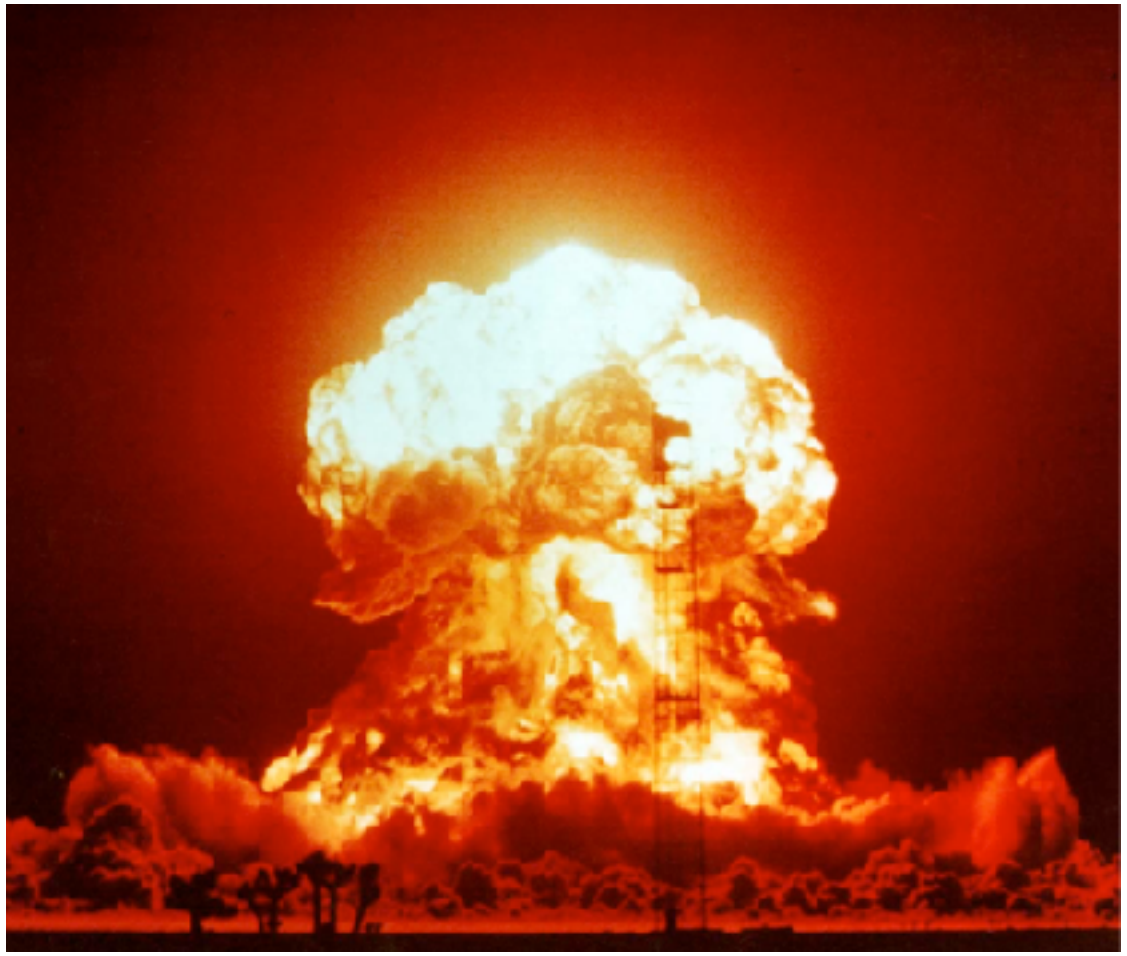
www.obesityaction.org (800) 717-3117

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.

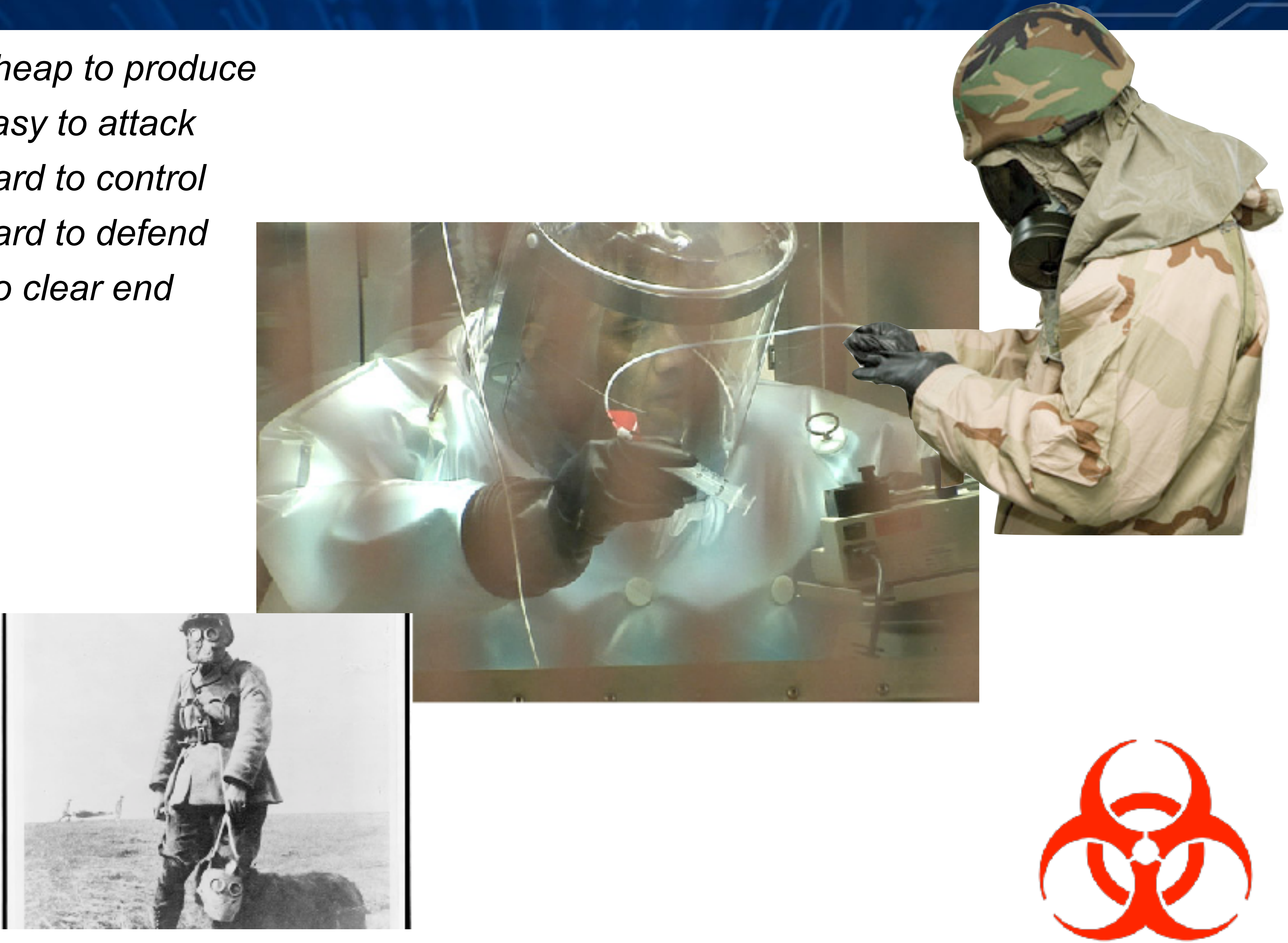
Cheap to produce

Easy to attack

Hard to control

Hard to defend

No clear end



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

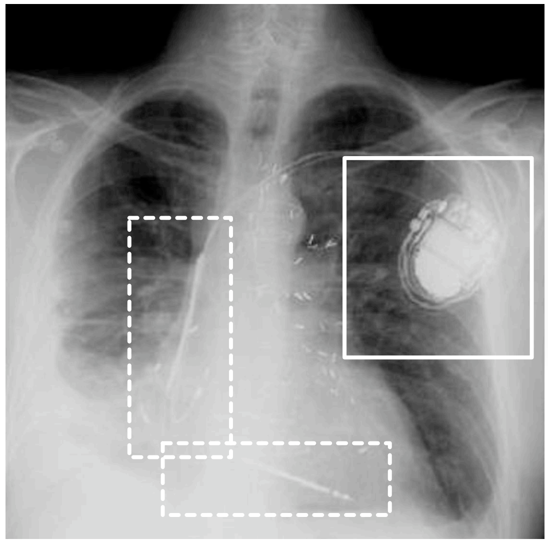
… because [wireless] computers are everywhere.

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!

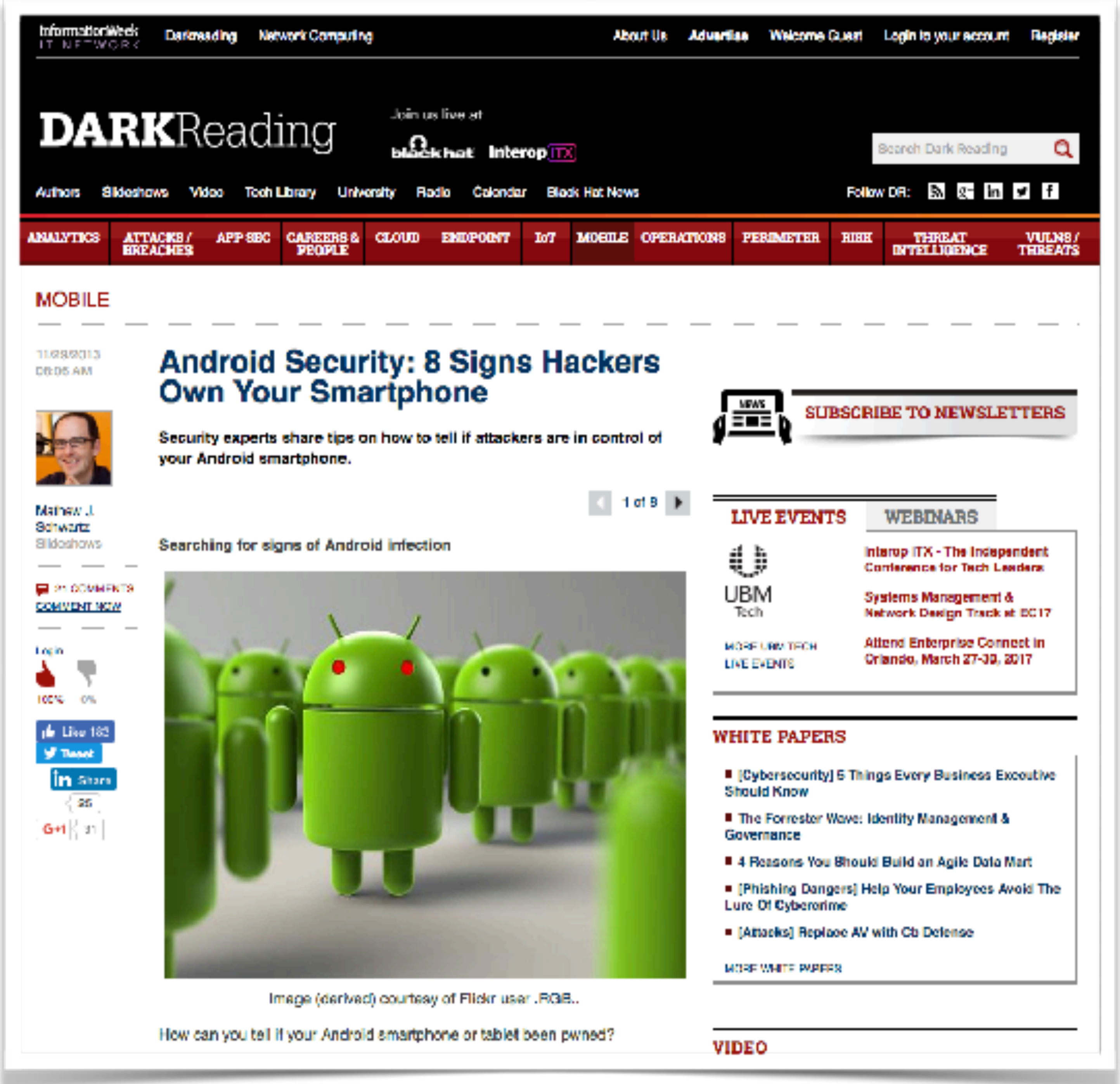
[Android] Cell phones ~~cannot~~ have not be secured.

Cell phones have:

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

Cell phones can be used for:

- Tracking individuals
- Wiretapping rooms
- Personal data



11/28/2013 08:05 AM

Mathew J. Schwartz
Slideshows

21 COMMENTS

Android Security: 8 Signs Hackers Own Your Smartphone

Security experts share tips on how to tell if attackers are in control of your Android smartphone.

Searching for signs of Android infection

Image (derived) courtesy of Flickr user .RGB..

How can you tell if your Android smartphone or tablet been pwned?

Interop ITX - The Independent Conference for Tech Leaders

Systems Management & Network Design Track at EC17

Attend Enterprise Connect in Orlando, March 27-30, 2017

WHITE PAPERS

- [Cybersecurity] 5 Things Every Business Executive Should Know
- The Forrester Wave: Identity Management & Governance
- 4 Reasons You Should Build an Agile Data Mart
- [Phishing Dangers] Help Your Employees Avoid The Lure Of Cybercrime
- [Attacks] Replace AV with Cb Defense

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….

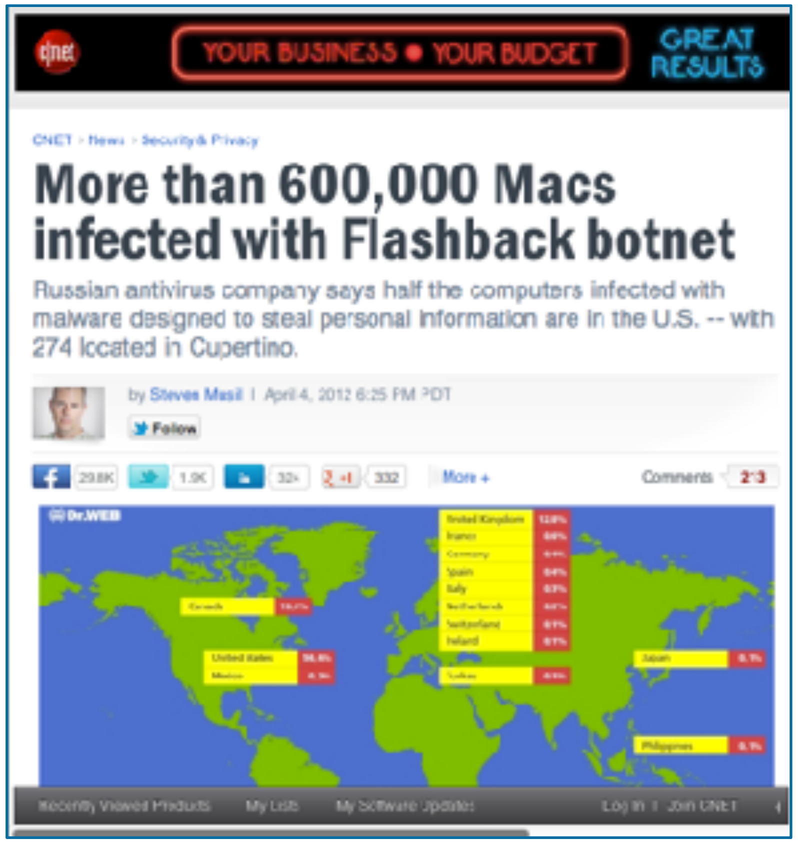
http://forums.corvetteforum.com/off-topic/2824193-i-only-have-to-outrun-you-polar-bear-tag.html

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!



CNET › News › Security & Privacy

More than 600,000 Macs infected with Flashback botnet

Russian antivirus company says half the computers infected with malware designed to steal personal information are in the U.S. -- with 274 located in Cupertino.

by Steven Musil | April 4, 2012 6:25 PM PDT

Apple users don't run anti-virus.

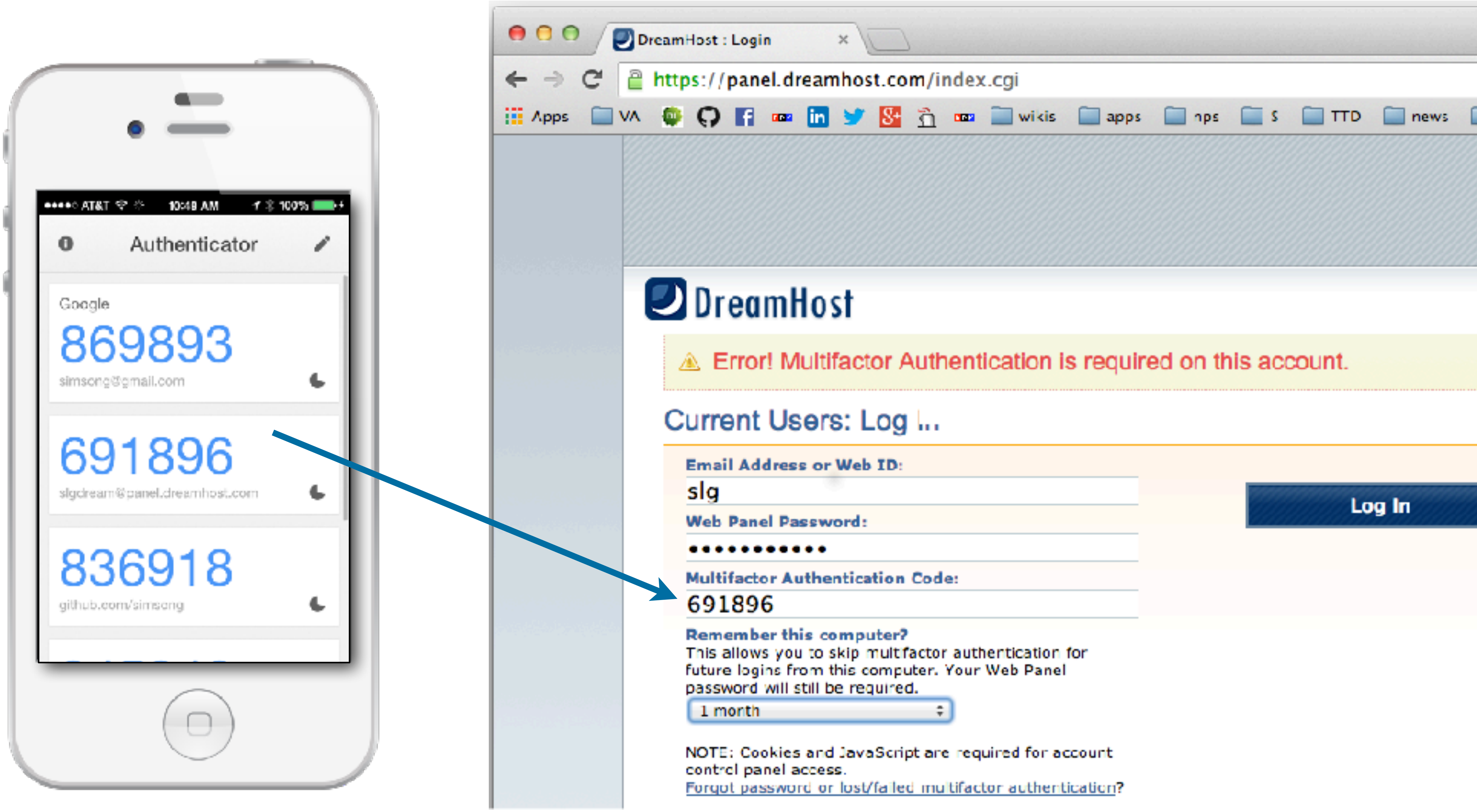
- Yes, Apple tries to fix bugs, but

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.



Google
869893
simsong@gmail.com

691896
slgdream@panel.dreamhost.com

836918
github.com/simsong

DreamHost

Error! Multifactor Authentication is required on this account.

Current Users: Log In...

Email Address or Web ID: slg

Web Panel Password: ●●●●●●●●●●●●

Multifactor Authentication Code: 691896

Remember this computer?
This allows you to skip multifactor authentication for future logins from this computer. Your Web Panel password will still be required.
1 month

NOTE: Cookies and JavaScript are required for account control panel access.
Forgot password or lost/failed multifactor authentication?

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:

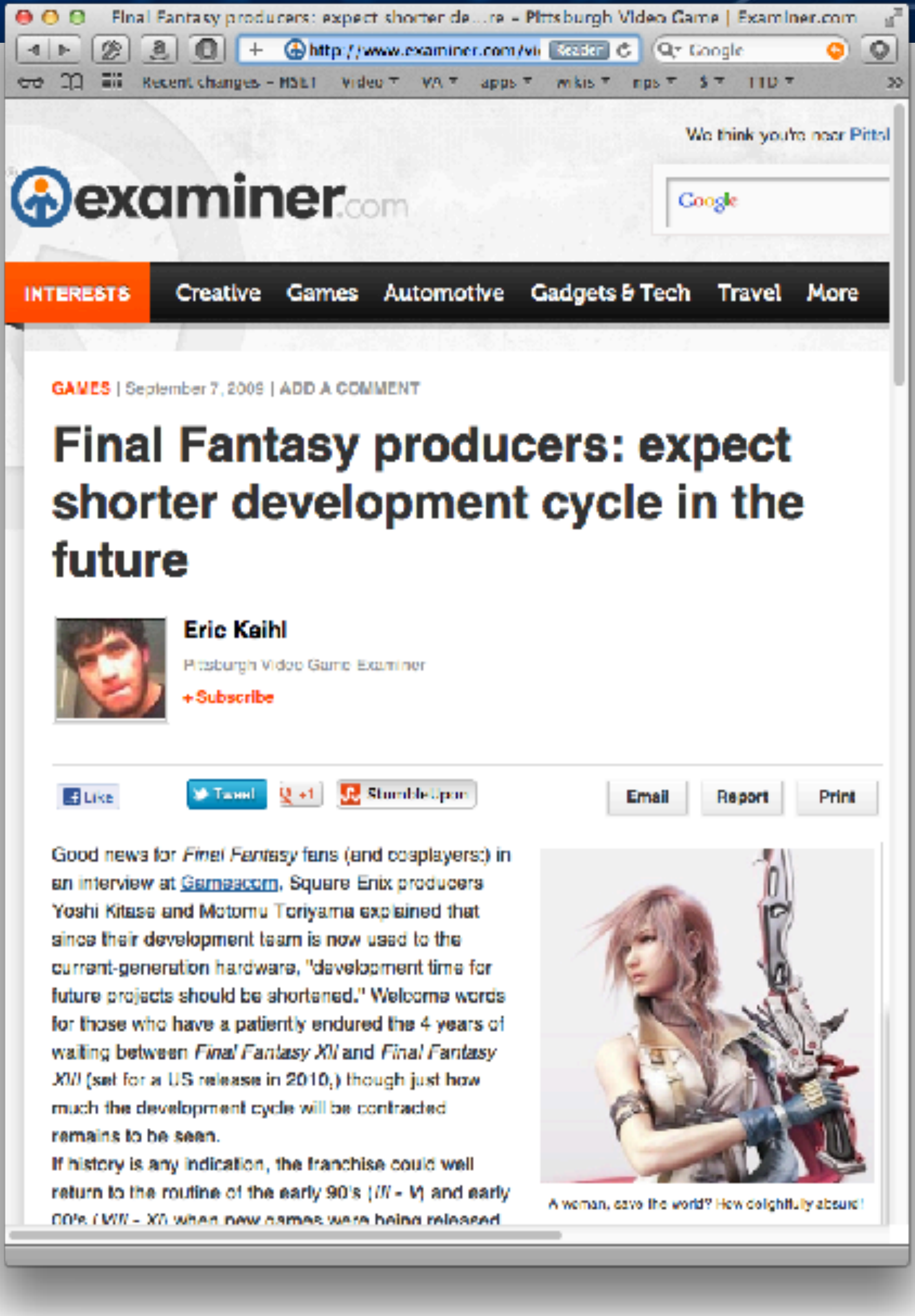
- Security not “baked in” to most products
- Few or no security reviews
- Little Usable Security

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


Final Fantasy producers: expect shorter de...re - Pittsburgh Video Game | Examiner.com
http://www.examiner.com/vi
Reader
Google
Recent changes - MSE1
Video
VA
apps
wikis
mps
$
11D
We think you're near Pitts
examiner.com
Google
INTERESTS
Creative
Games
Automotive
Gadgets & Tech
Travel
More

GAMES | September 7, 2009 | ADD A COMMENT

Final Fantasy producers: expect shorter development cycle in the future

Eric Kaihl
Pittsburgh Video Game Examiner
+Subscribe

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

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

A woman, save the world? How delightfully absurd!

Short development cycles

Insufficient planning:

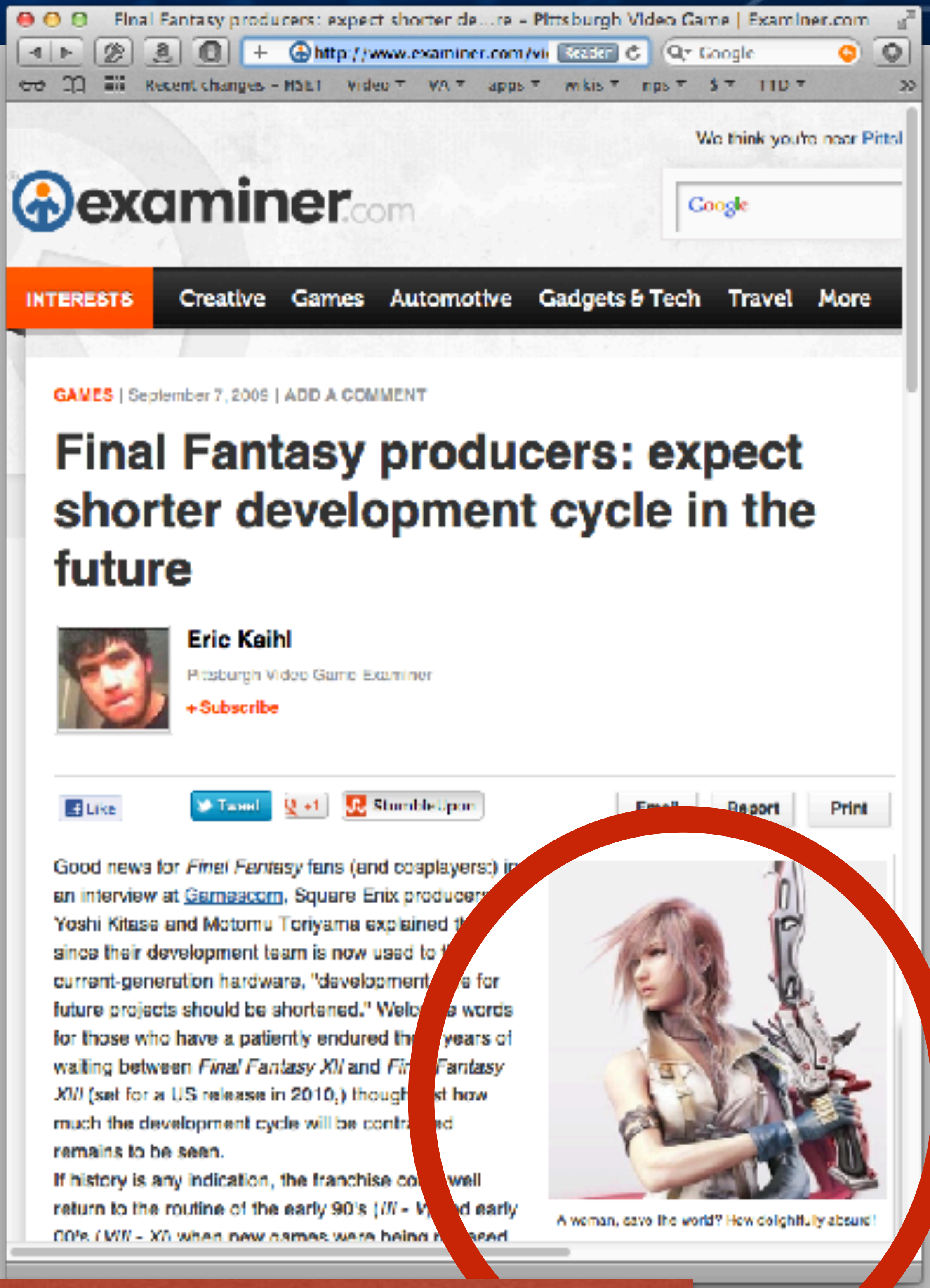
- Security not “baked in” to most products
- Few or no security reviews
- Little Usable Security

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



Final Fantasy producers: expect shorter de...re – Pittsburgh Video Game | Examiner.com
http://www.examiner.com/vi
Reader
Google
Recent changes – MSE1
video
VA
apps
wikis
mps
$
11D
We think you're near Pitts
examiner.com
Google
INTERESTS
Creative
Games
Automotive
Gadgets & Tech
Travel
More

GAMES | September 7, 2009 | ADD A COMMENT

Final Fantasy producers: expect shorter development cycle in the future

Eric Kaihl
Pittsburgh Video Game Examiner
+Subscribe

Good news for *Final Fantasy* fans (and cosplayers:) in
an interview at Gamescom, Square Enix producers
Yoshi Kitase and Motomu Toriyama explained th
since their development team is now used to t
current-generation hardware, "development s for
future projects should be shortened." Welc e words
for those who have a patiently endured th years of
waiting between *Final Fantasy XII* and *Fi Fantasy
XIII* (set for a US release in 2010,) though st how
much the development cycle will be contr ed
remains to be seen.
If history is any indication, the franchise co well
return to the routine of the early 90's (*III* - V d early
00's (*VII* - *X*) when new games were being r ased

A woman, save the world? How delightfully absurd!

Address institutionalized harassment of women

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

Security HR Pipeline

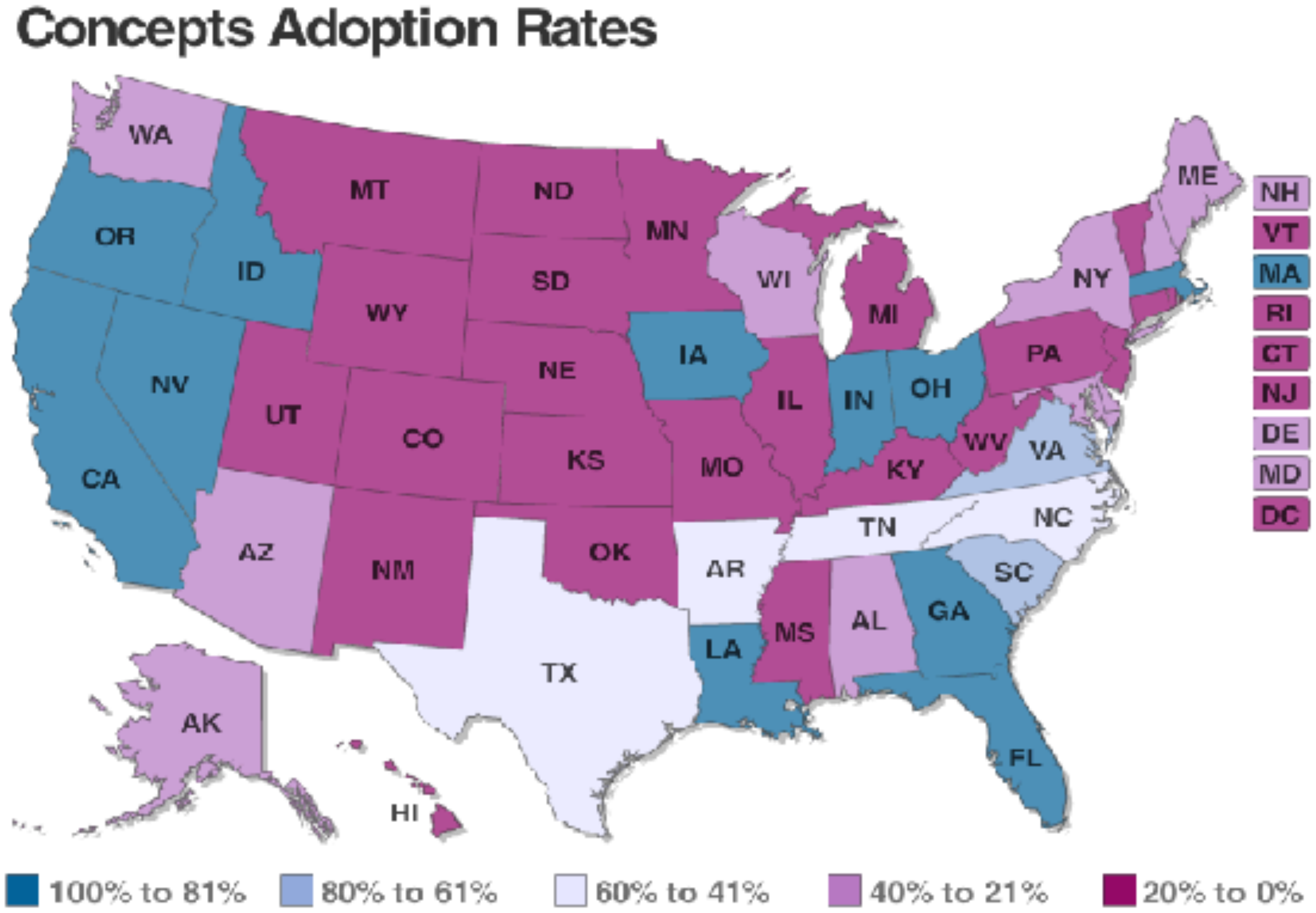
- High School → College → Graduate School → Career

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?*

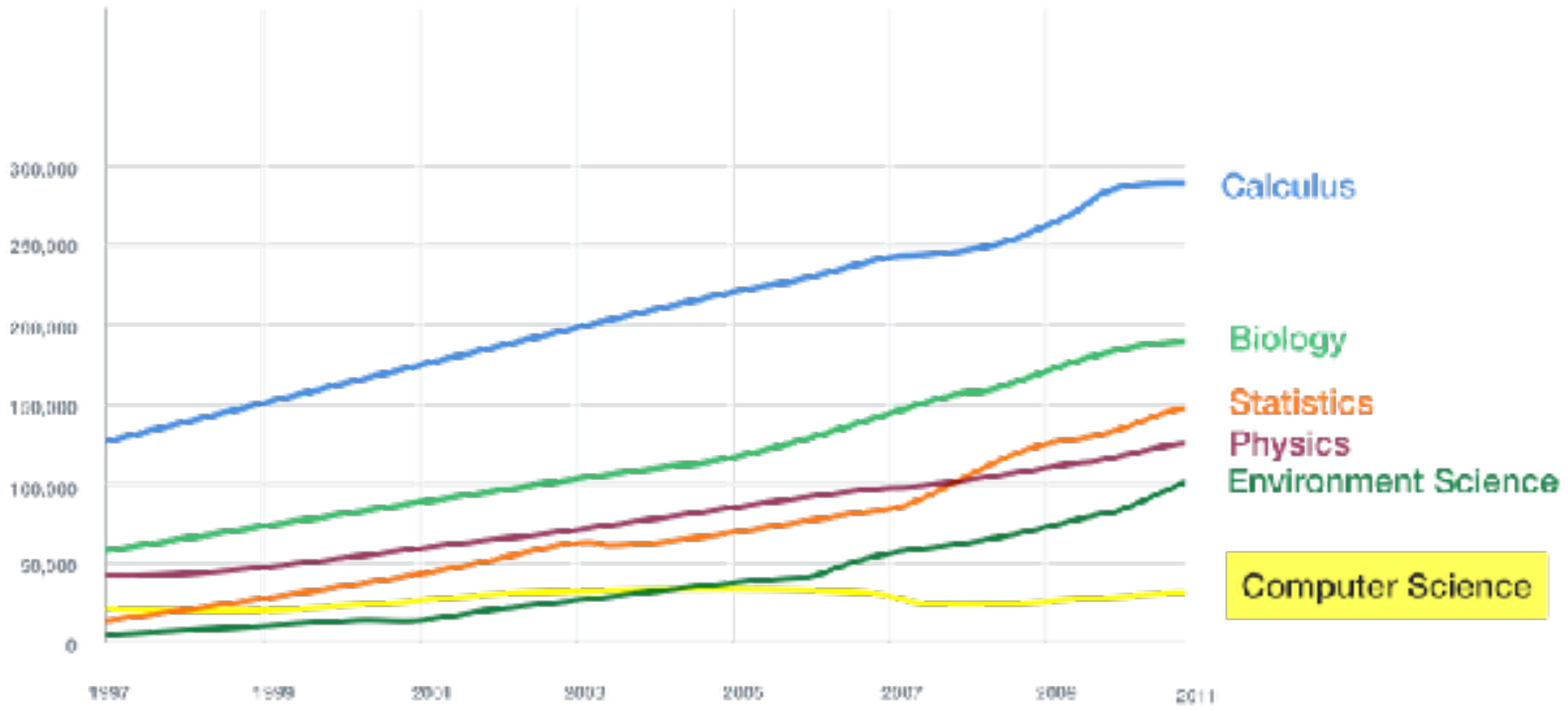
73% of states require computer “skills” for graduation. Only 37% require CS “concepts”

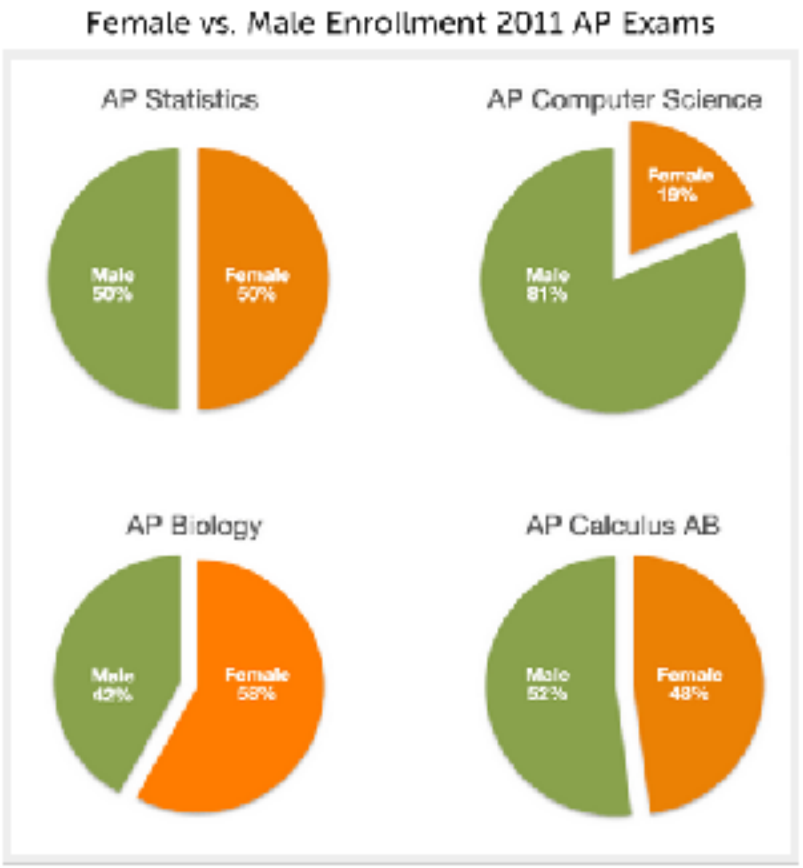


CS teachers are paid far less than CS engineers.

High school students are not taking AP computer science!

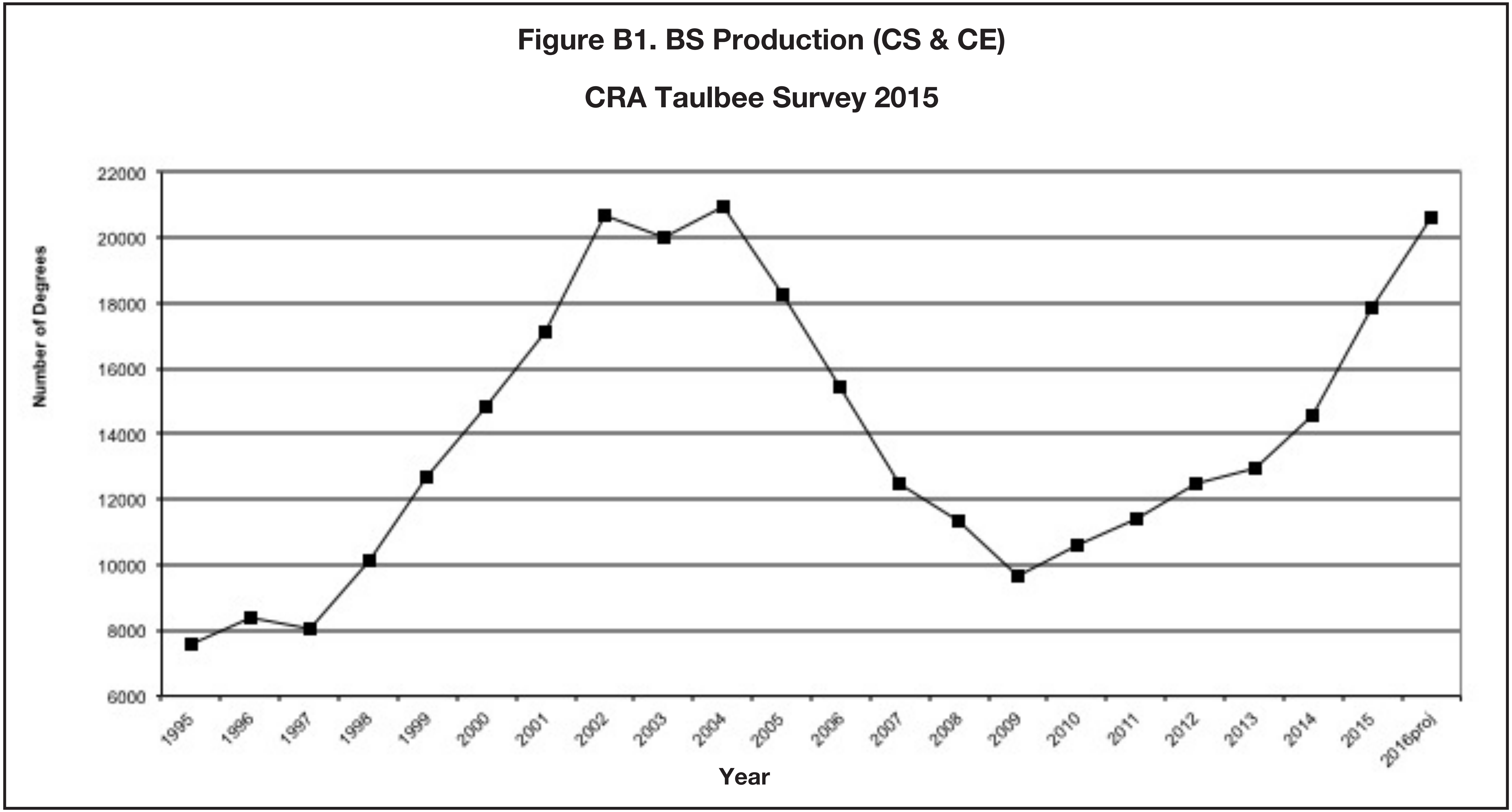
AP Exams 1997 -2011





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	1,405	79	61	64	604	111	0	66	64	435	214	0	55	46	8,431	60.5%
Amer Indian or Alaska Native	29	10	0	0	1	4	2	0	0	1	0	2	0	0	0	47	0.3%
Asian	706	194	16	8	9	64	12	0	7	7	56	40	0	7	9	1,088	7.8%
Black or African-American	95	50	5	1	2	9	9	0	1	5	22	26	0	3	6	216	1.5%
Native Hawaiian/ Pac Islander	5	2	0	0	0	1	0	0	0	0	6	1	0	1	0	15	0.1%
White	2,585	482	75	28	22	203	34	0	22	20	258	155	0	33	34	3,792	27.2%
Multiracial, not Hispanic	55	11	3	1	1	10	1	0	1	1	5	8	0	1	2	93	0.7%
Hispanic, any race	162	32	10	2	2	22	4	0	2	2	13	15	0	2	3	258	1.9%
Total Res & Ethnicity Known	9,220	2,186	188			917	173	-			795	461	0			13,940	
Resident, ethnicity unknown	469	103	16			9	1	-			208	43	0			849	
Not Reported (N/R)	373	72	165			17	0	-			41	13	0			608	
Gender Totals	10,062	2,361	296			943	174	-			1,044	517	0			15,397	
%	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

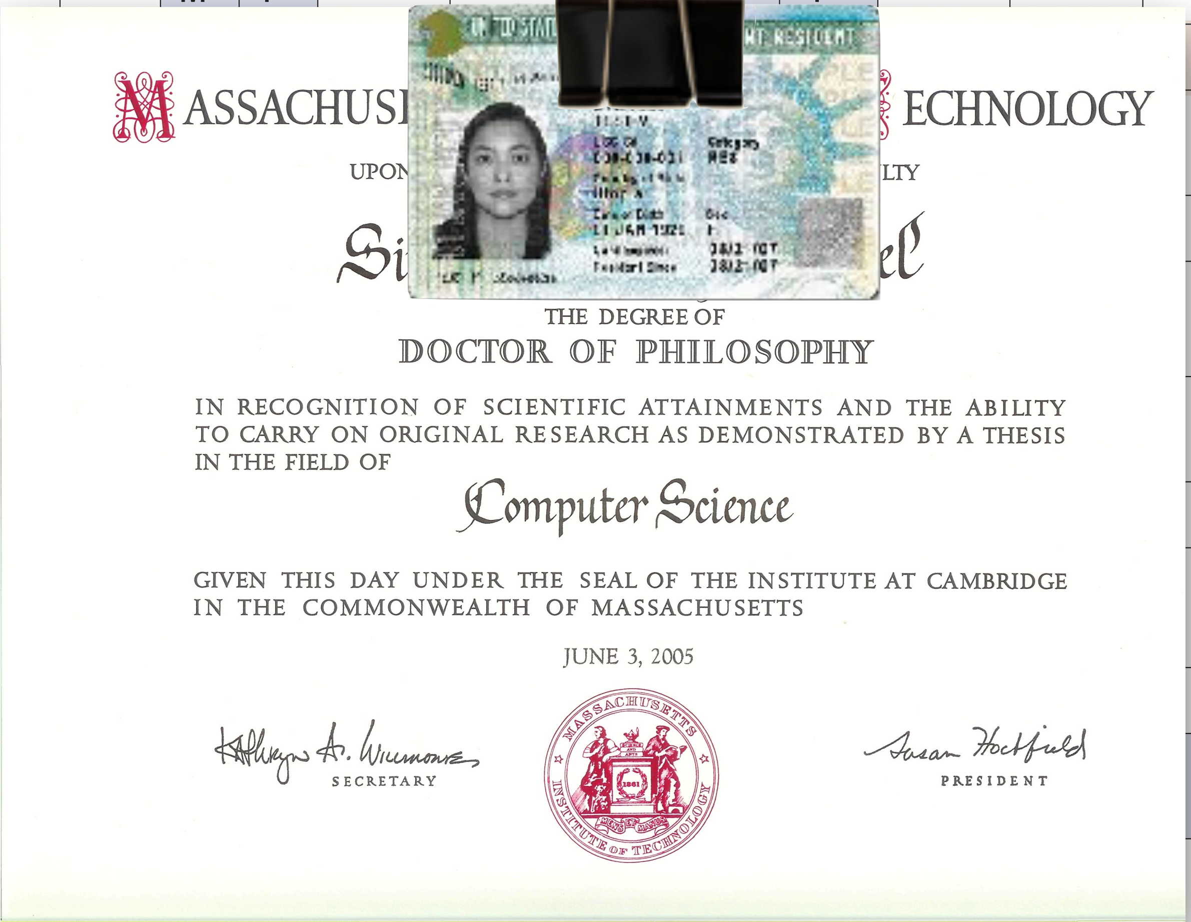
—We did not train Russia’s weapons scientists in Boston during the Cold War.

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											0			849	
Not Reported (N/R)	373	72	165			17	0	-			41	13	0			608	
Gender Totals	10,062	2,361	296			943	174	-			1,044	517	0			15,397	
%	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



MASSACHUS ECHNOLOGY

UPON LTY

Si el

THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN RECOGNITION OF SCIENTIFIC ATTAINMENTS AND THE ABILITY TO CARRY ON ORIGINAL RESEARCH AS DEMONSTRATED BY A THESIS IN THE FIELD OF

Computer Science

GIVEN THIS DAY UNDER THE SEAL OF THE INSTITUTE AT CAMBRIDGE IN THE COMMONWEALTH OF MASSACHUSETTS

JUNE 3, 2005

SECRETARY

PRESIDENT

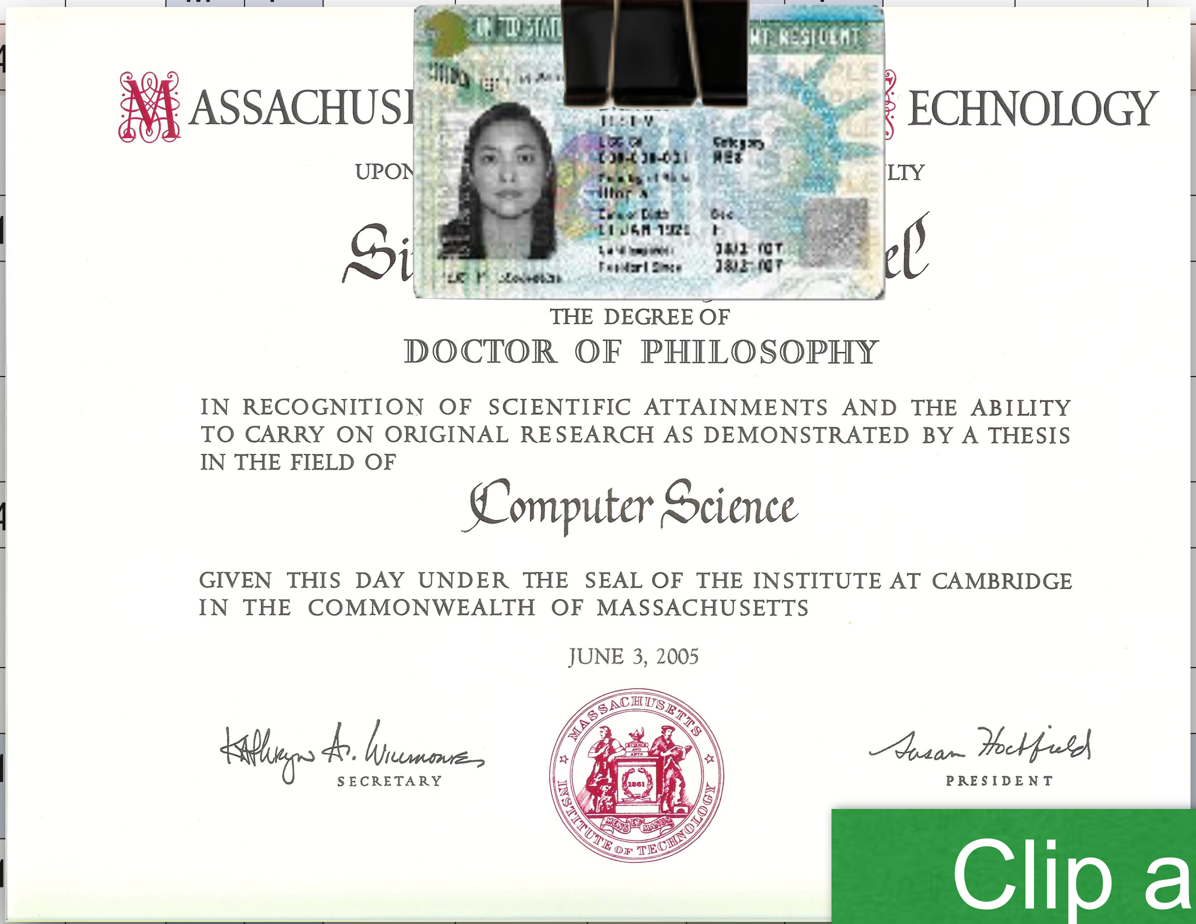
—We did not train Russia's weapons scientists in Boston during the Cold War.

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



MASSACHUS ... ECHNOLOGY

UPON ... LTY

Si ... el

THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN RECOGNITION OF SCIENTIFIC ATTAINMENTS AND THE ABILITY TO CARRY ON ORIGINAL RESEARCH AS DEMONSTRATED BY A THESIS IN THE FIELD OF

Computer Science

GIVEN THIS DAY UNDER THE SEAL OF THE INSTITUTE AT CAMBRIDGE IN THE COMMONWEALTH OF MASSACHUSETTS

JUNE 3, 2005

Kathryn A. Willmore
SECRETARY

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Susan Hockfield
PRESIDENT

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

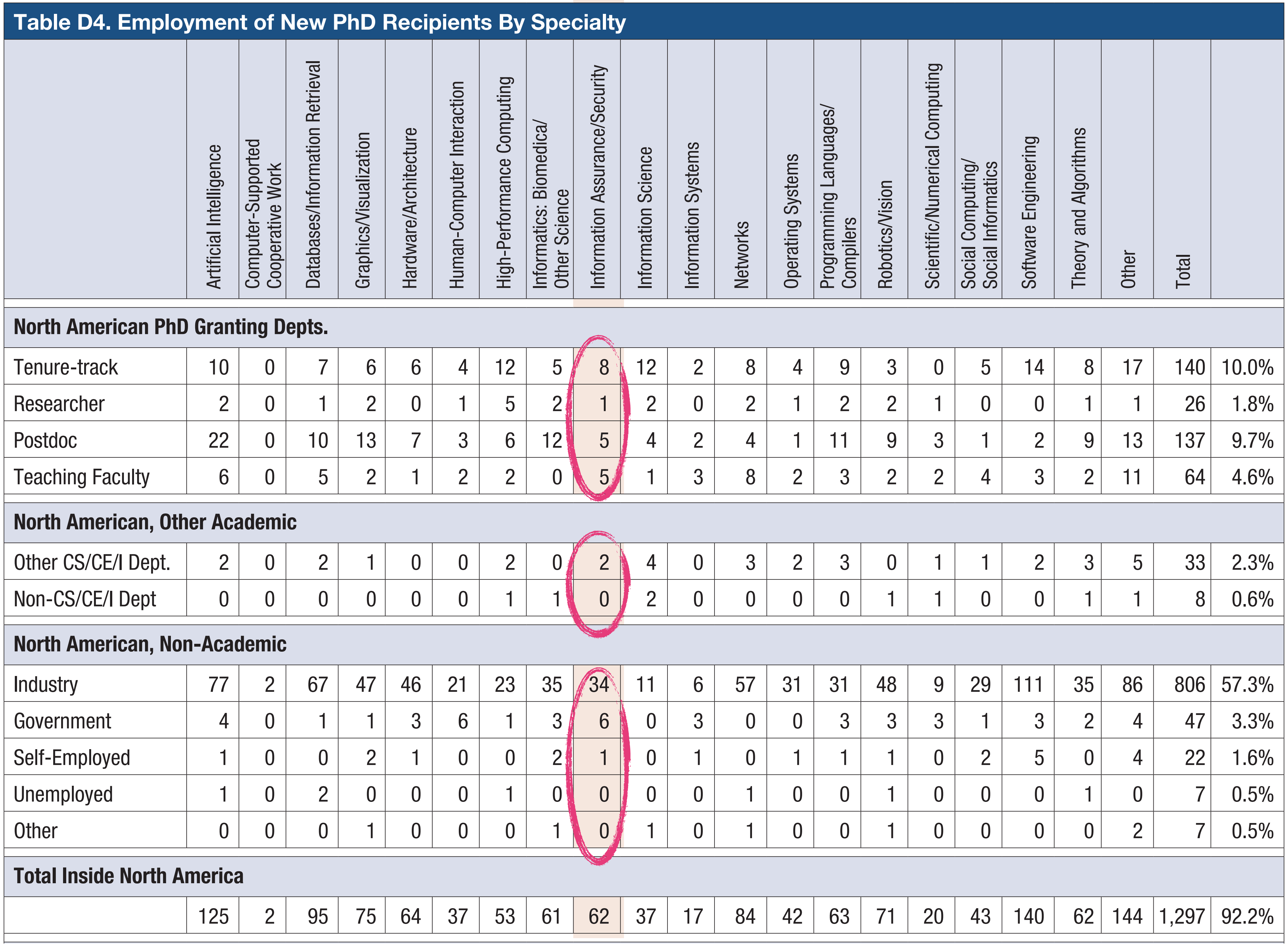


Table D4. Employment of New PhD Recipients By Specialty

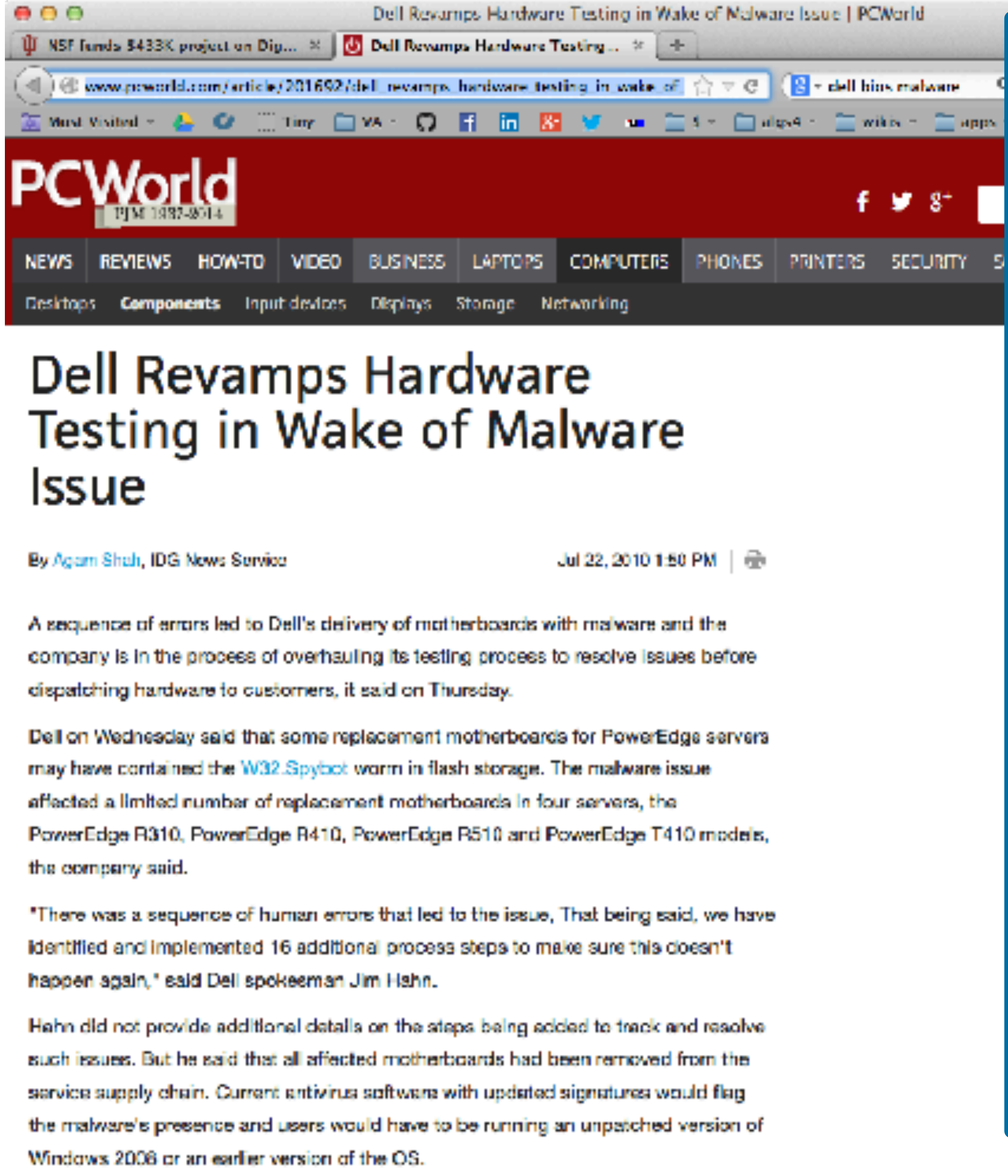
	Artificial Intelligence	Computer-Supported Cooperative Work	Databases/Information Retrieval	Graphics/Visualization	Hardware/Architecture	Human-Computer Interaction	High-Performance Computing	Informatics: Biomedical/ Other Science	Information Assurance/Security	Information Science	Information Systems	Networks	Operating Systems	Programming Languages/ Compilers	Robotics/Vision	Scientific/Numerical Computing	Social Computing/ Social Informatics	Software Engineering	Theory and Algorithms	Other	Total	
North American PhD Granting Depts.																						
Tenure-track	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

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
dell bios malware
Most Visited
Tiny
VA
algs4
wikis
apps
PCWorld
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

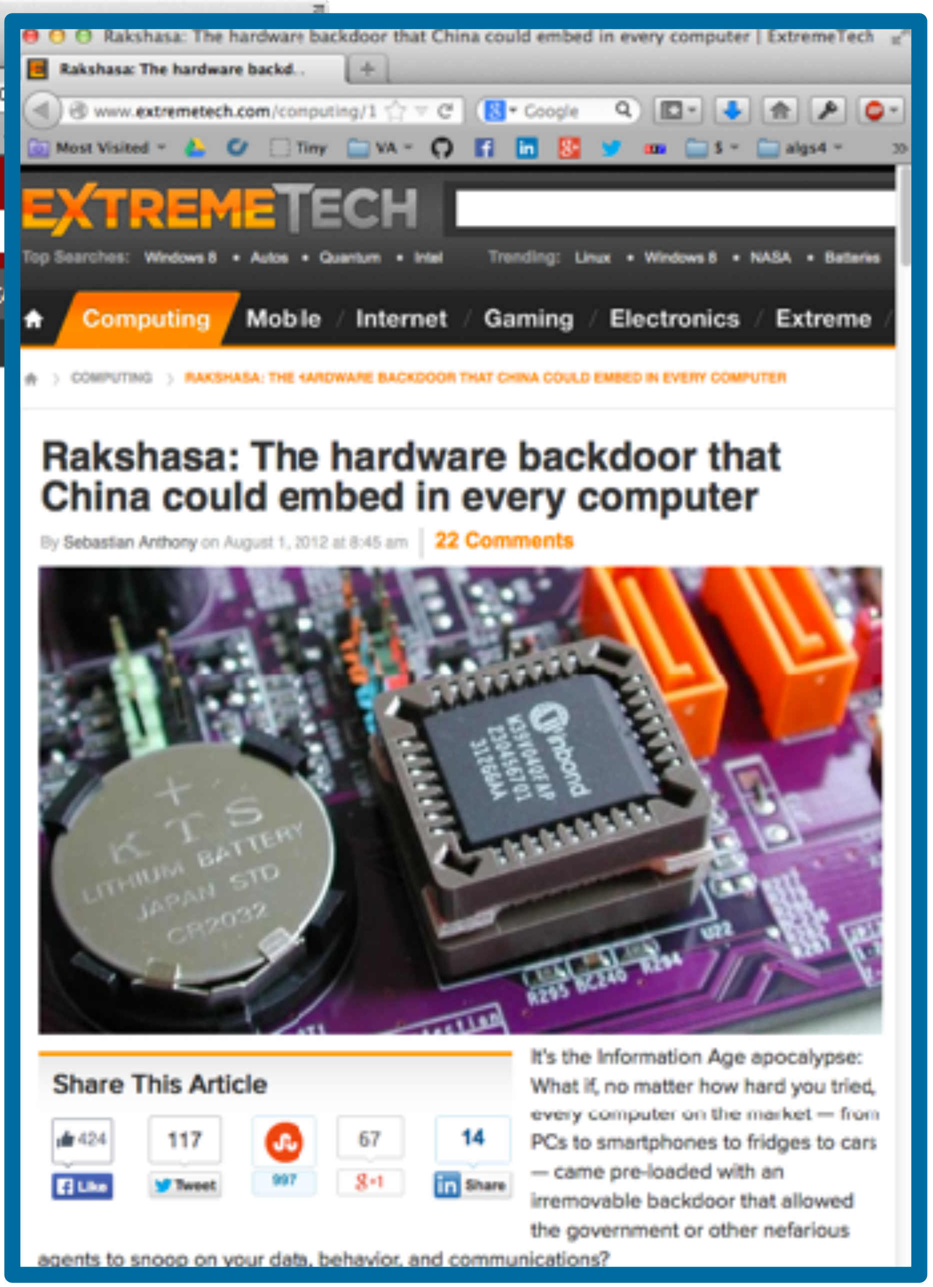
By Agam Shah, IDG News Service   Jul 22, 2010 1:50 PM

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 2000 or an earlier version of the OS.


Rakshasa: The hardware backdoor that China could embed in every computer | ExtremeTech
Rakshasa: The hardware backd...
www.extremetech.com/computing/1
Google
Most Visited
Tiny
VA
$
algs4
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
KTS LITHIUM BATTERY JAPAN STD CR2032
Winbond
Share This Article
424
Like
117
Tweet
997
67
+1
14
Share

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

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

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.

Thank you!

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

2013 IEEE International Conference on

Technologies for Homeland Security

12-14 November 2013, Westin Hotel, Waltham, MA

IEEE Advancing Technology for Humanity

DETECTING THREATENING INSIDERS WITH LIGHTWEIGHT MEDIA FORENSICS

Naval Postgraduate School &
The University of Texas at San Antonio

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

8am, Wednesday November 13th, 2013

NPS PRAESTANTIA PER SCIENTIAM 1909

UTSA

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***

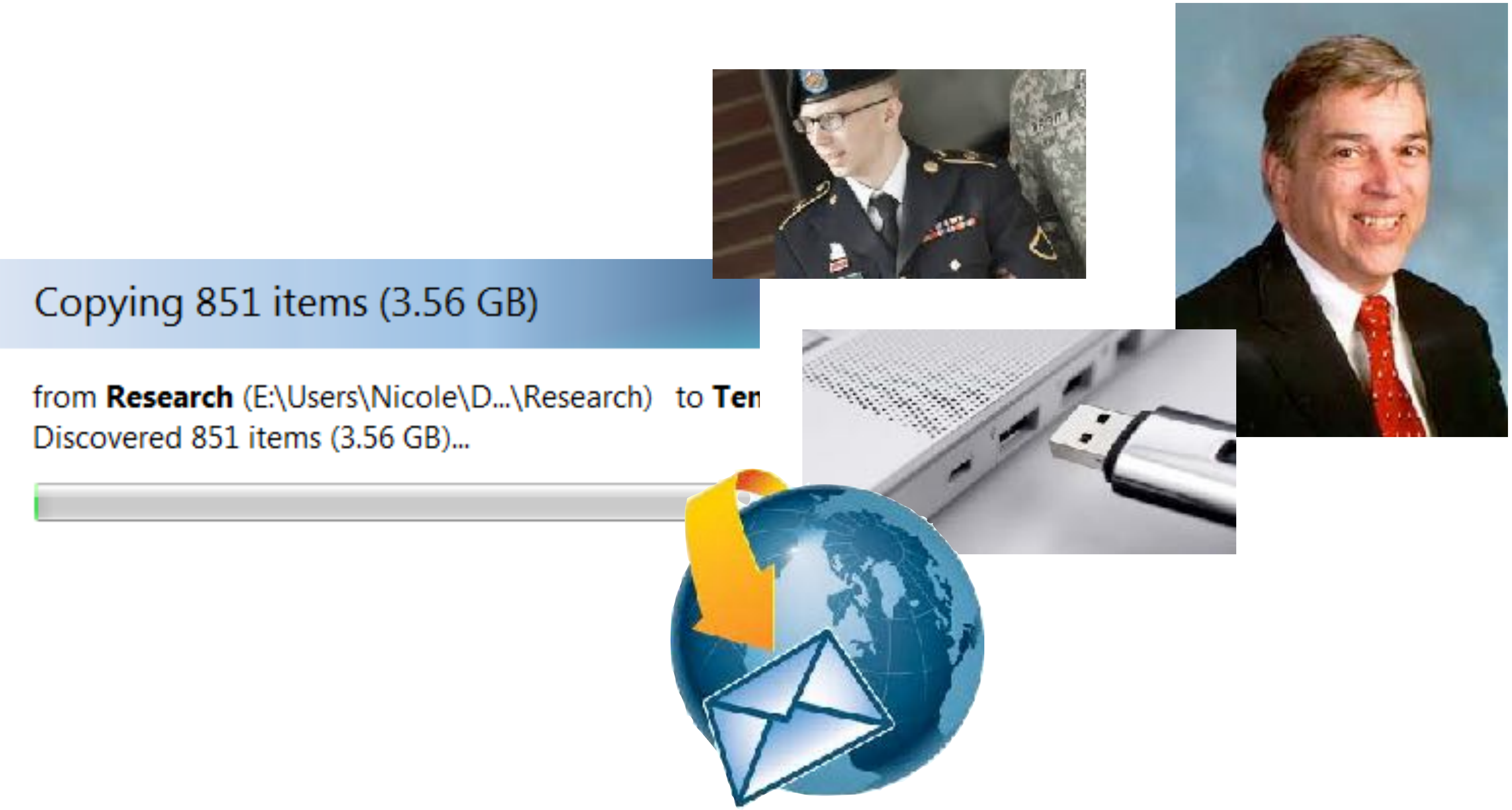
These signatures are typically hand written.

- *—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



Copying 851 items (3.56 GB)

from **Research** (E:\Users\Nicole\D...\Research) to **Ten**
Discovered 851 items (3.56 GB)...

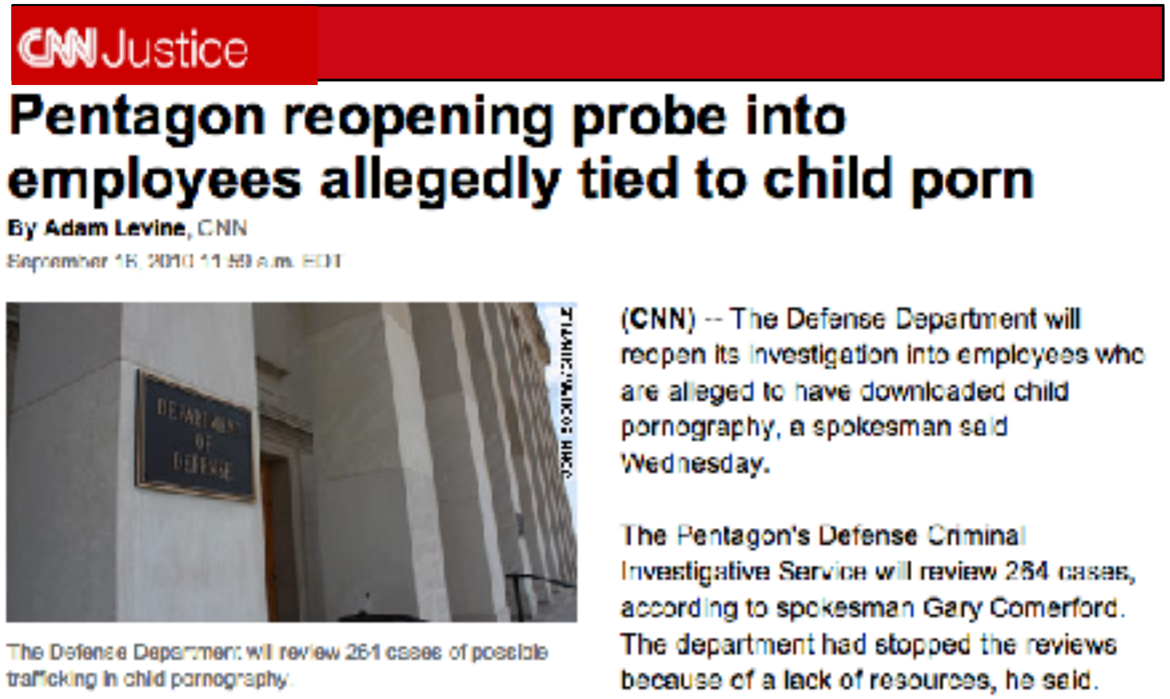
We also want to detect other kinds of illegal employee activity.

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 15, 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.

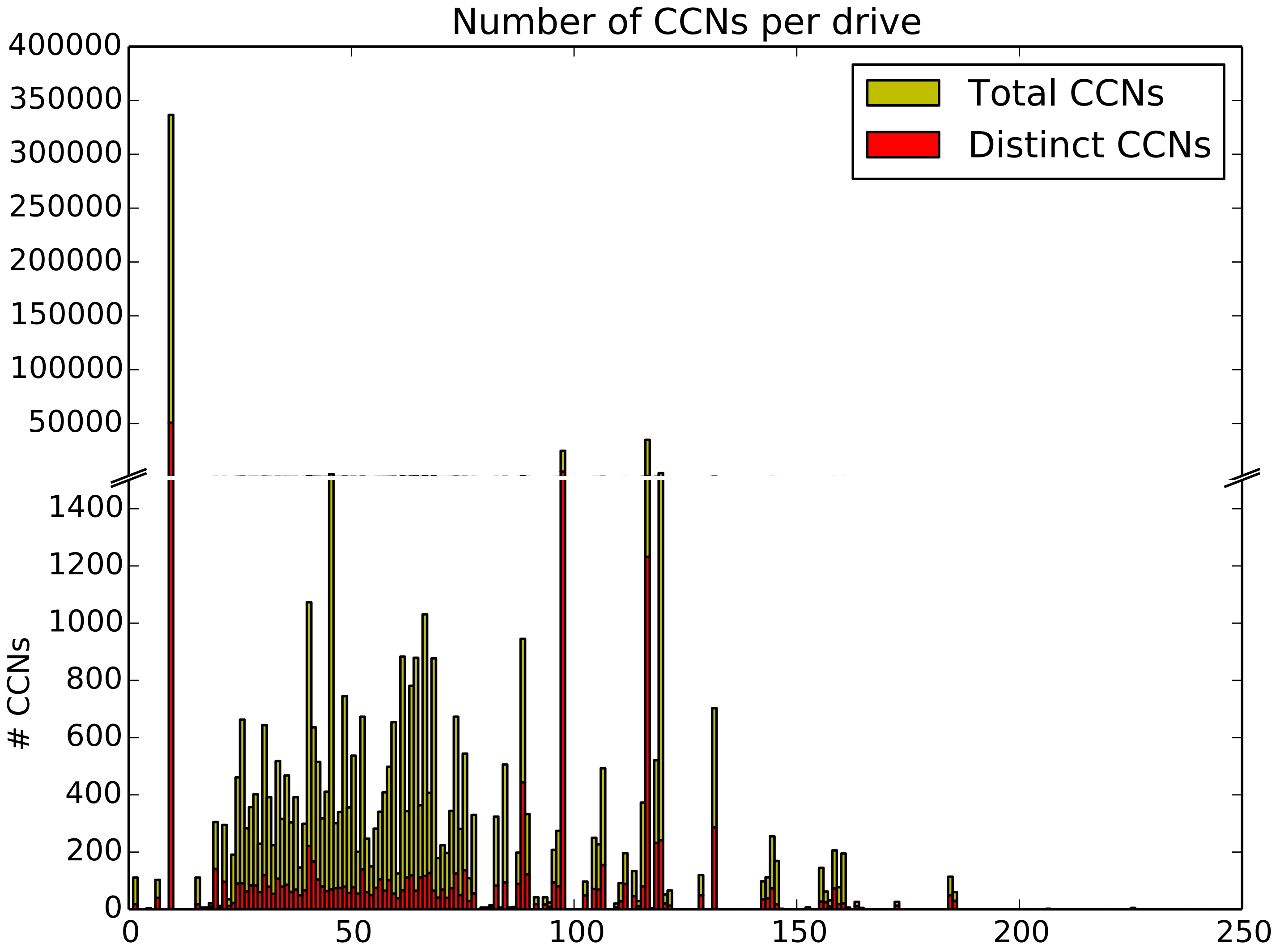
Our plan: look for storage devices that are different than their peers.

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.

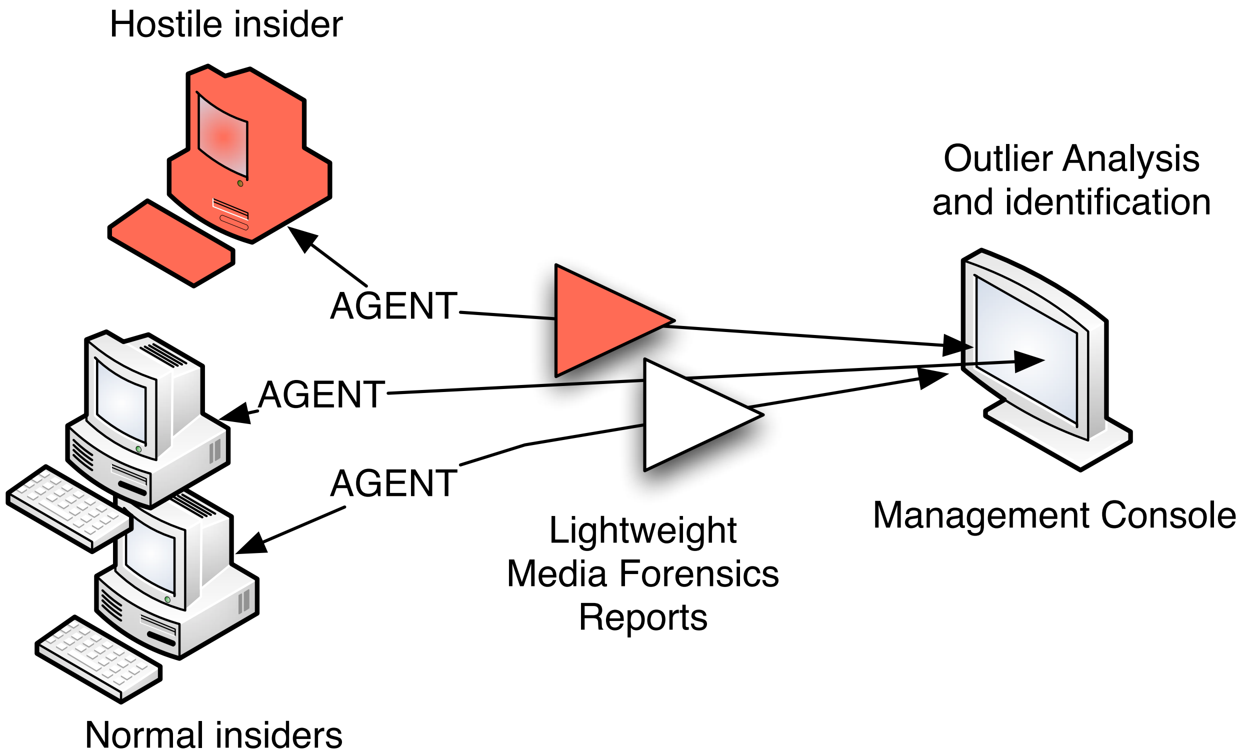


Garfinkel, S. and Shelat, A., "Remembrance of Data Passed: A Study of Disk Sanitization Practices," IEEE Security & Privacy, January/February 2003.

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)


Hostile insider
Outlier Analysis and identification
AGENT
AGENT
AGENT
Lightweight Media Forensics Reports
Management Console
Normal insiders

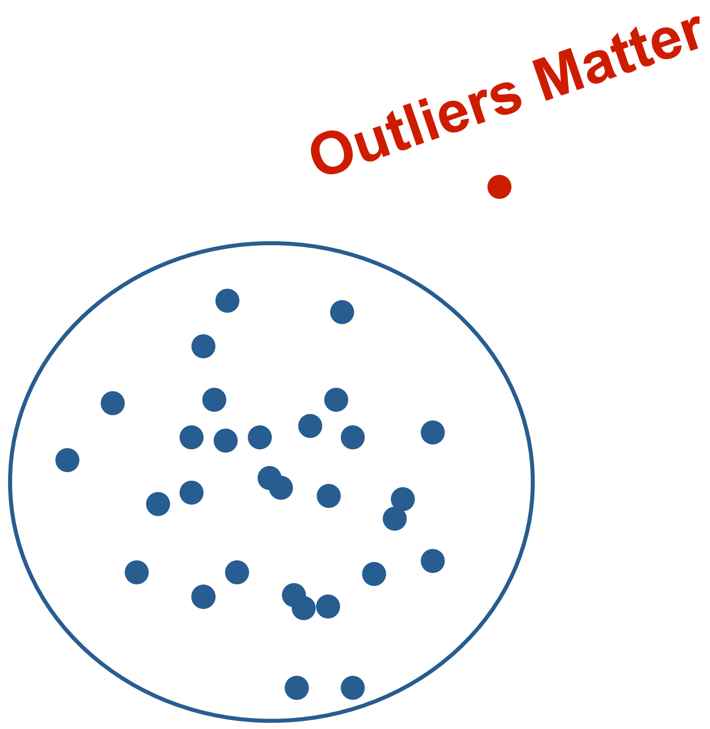
Statistical profile

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

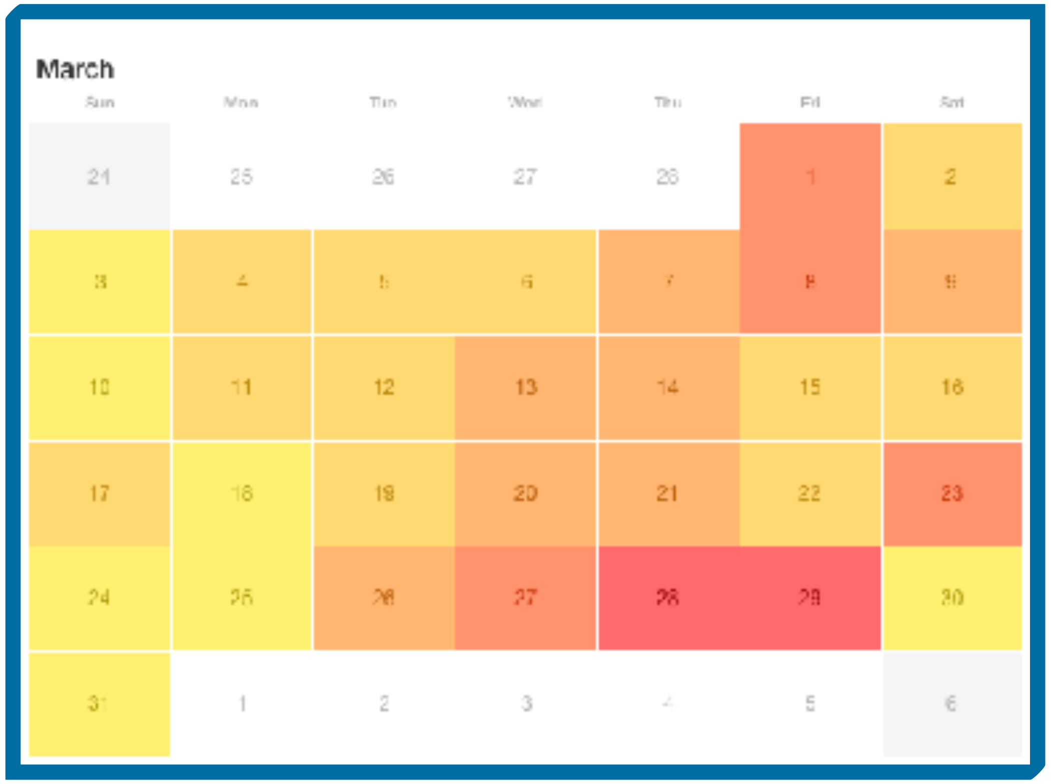
We cluster the storage profiles to find “outliers.”

What’s an outlier?

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



“Normal” Storage Profile



March

Sun	Mon	Tue	Wed	Thu	Fri	Sat
24	25	26	27	28	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

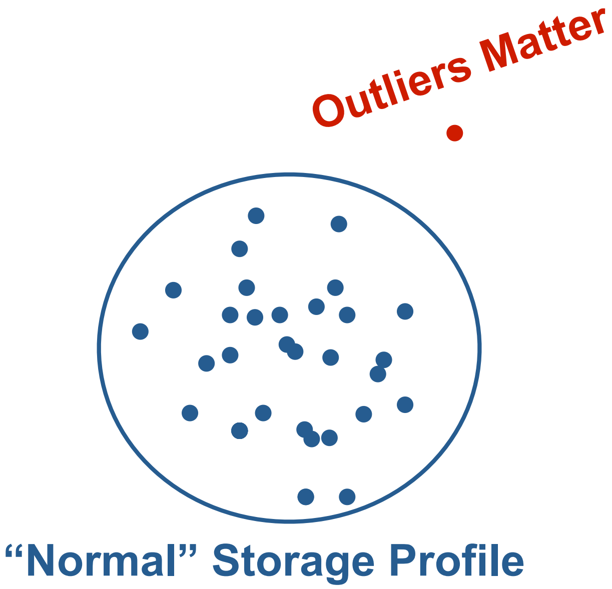
Outlier detection should have significant benefits:

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

Design constraints:

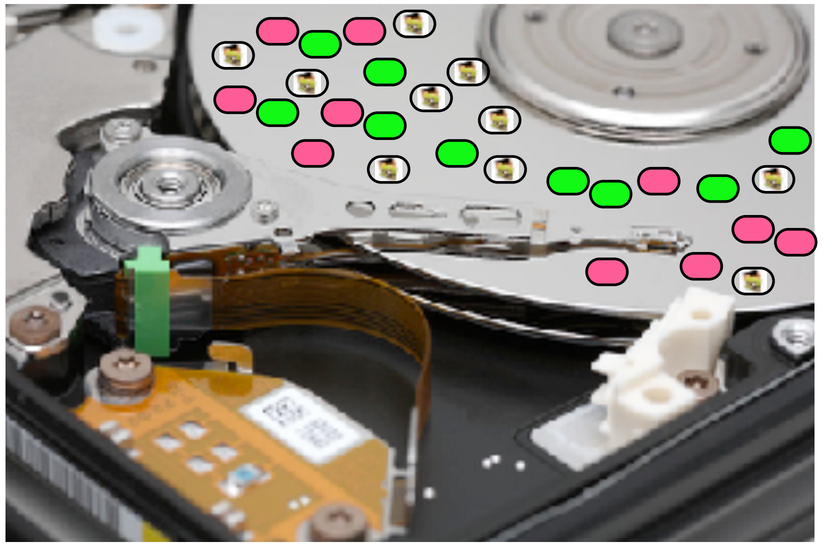
- Agent must be scalable and cannot interfer with operations
  - —*Desktop: background process, samples disk data*
  - —*Network load: small, aggregated data transfer*
  - —*Management console: scalable algorithms used*

- 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*



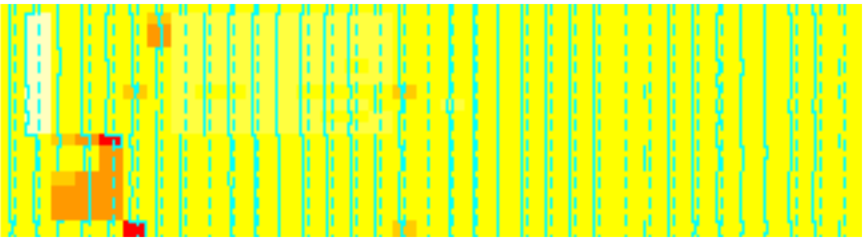
Garfinkel, Simson, Digital media triage with bulk data analysis and bulk_extractor. Computers and Security 32: 56-72 (2013)

2. Client-server, enterprise response framework
   - Google Rapid Response (GRR)

grr

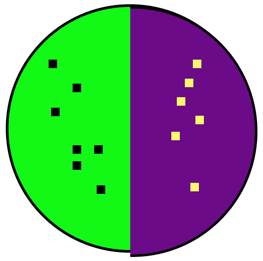
GRR Rapid Response is an Incident Response Framework

3. Anomaly detection agent
   - Univariate and multivariate outlier detection



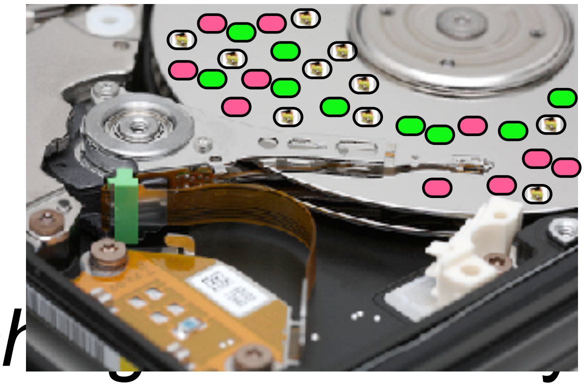
Random sampling is a great way to analyze data.

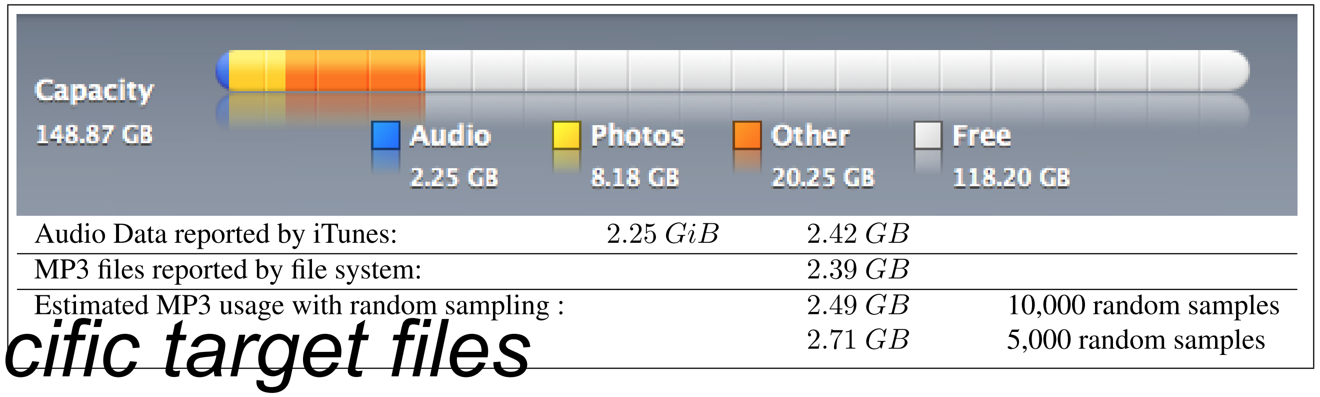
Simple random sampling can determine % free space



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





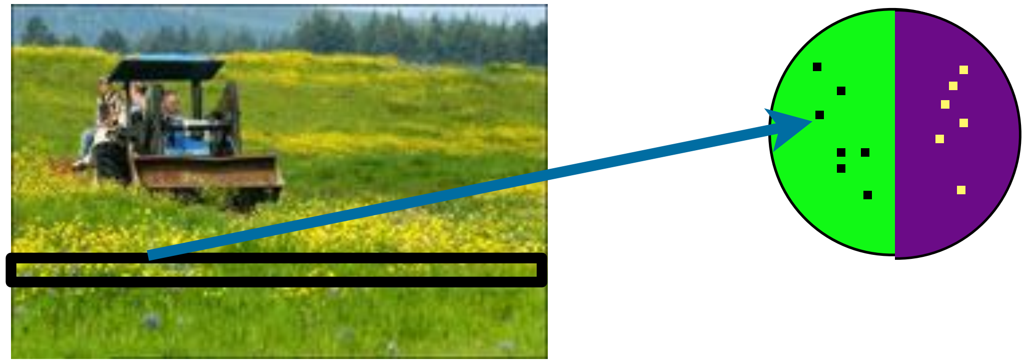
Capacity
148.87 GB

Audio	Photos	Other	Free
2.25 GB	8.18 GB	20.25 GB	118.20 GB

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 hash … *specific target 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:

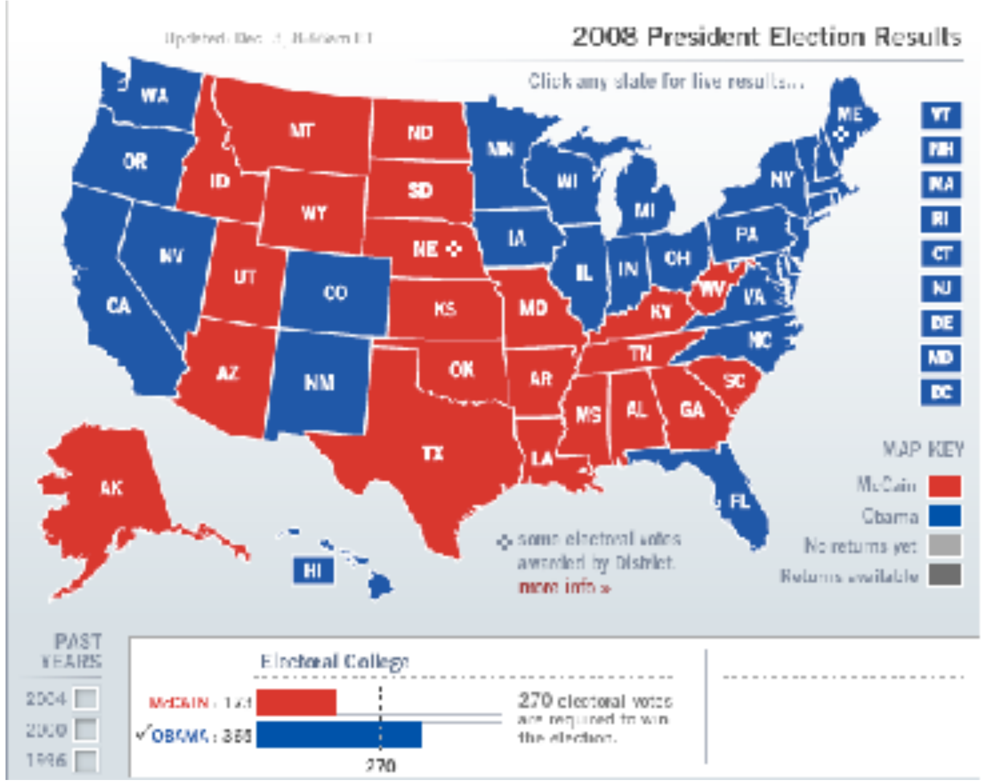
- 36 GB in one strip
- 100,000 randomly chosen 64KiB strips (assuming 3 msec/seek)

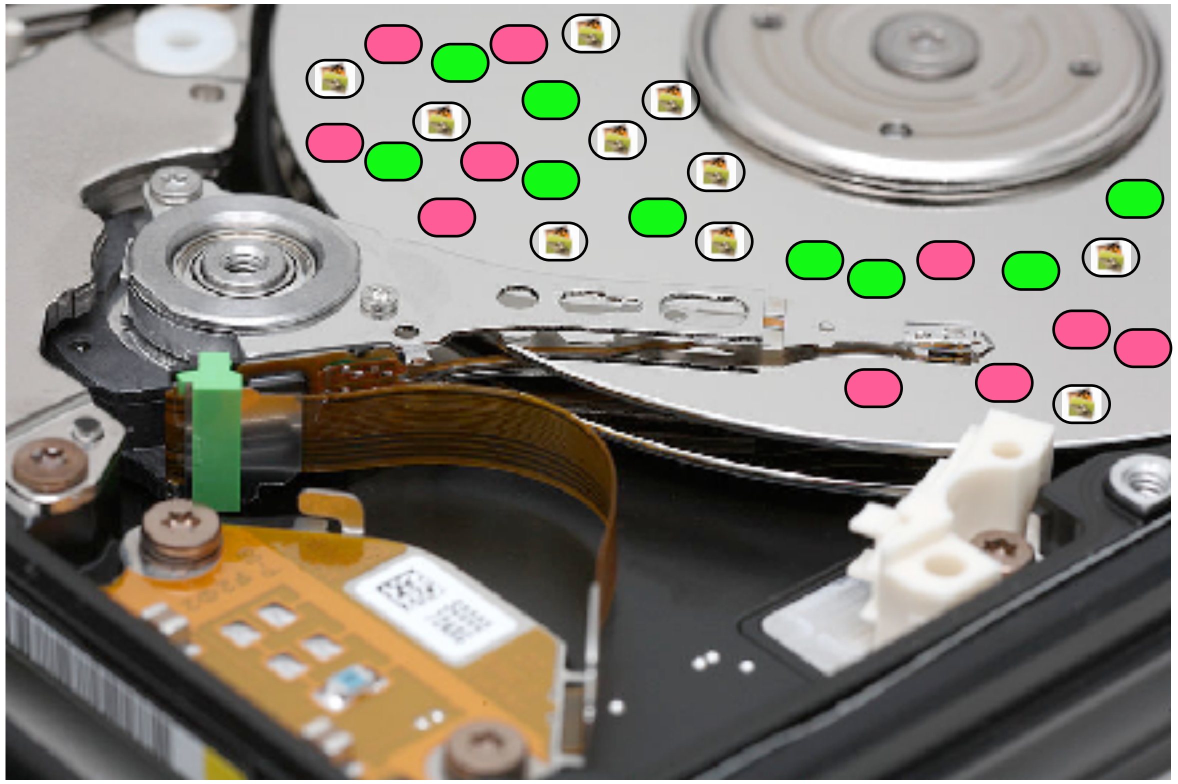
Minutes	208	5	5
Data	1 TB	36 GB	6.5 GB
# Seeks	1	1	100,000
% of data	100%	3.6%	0.65%

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

US elections can be predicted by sampling thousands of households:

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

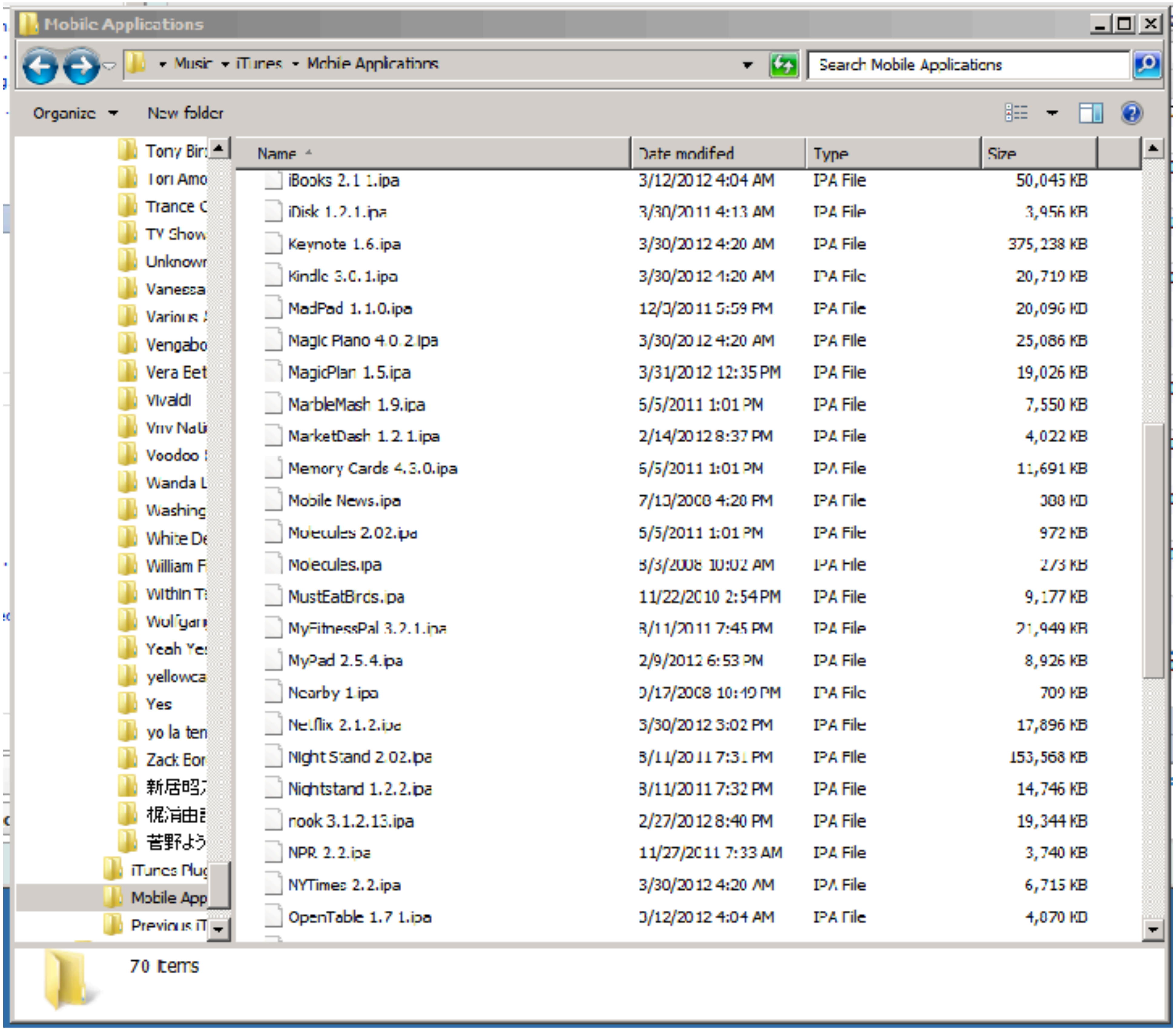




The challenge is identifying *likely voters.*

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

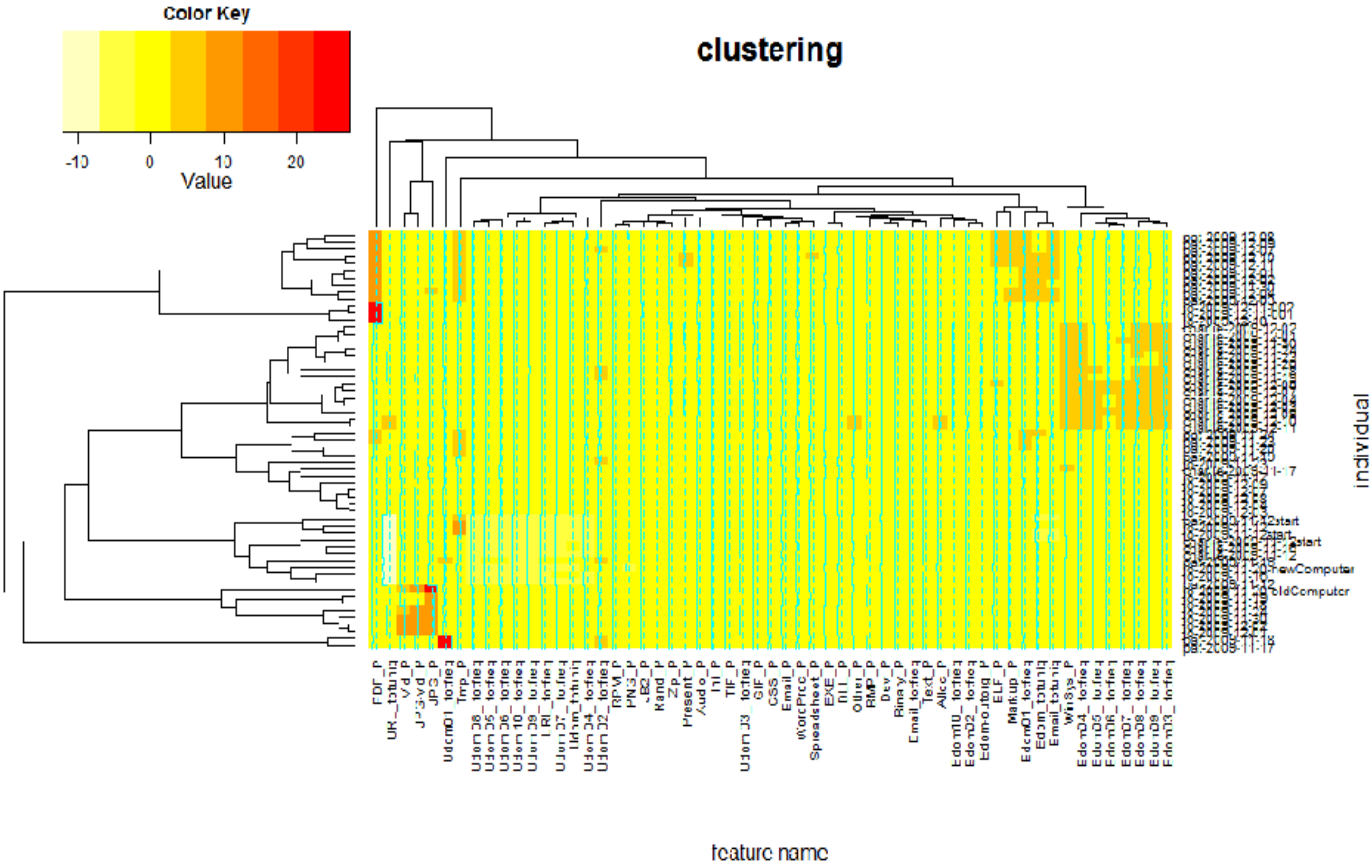
We think of computers as devices with *files*.



Name	Date modified	Type	Size
iBooks 2.1.1.ipa	3/12/2012 4:04 AM	IPA File	50,045 KB
iDisk 1.2.1.ipa	3/30/2011 4:13 AM	IPA File	3,956 KB
Keynote 1.6.ipa	3/30/2012 4:20 AM	IPA File	375,238 KB
Kindle 3.0.1.ipa	3/30/2012 4:20 AM	IPA File	20,719 KB
MadPad 1.1.0.ipa	12/3/2011 5:59 PM	IPA File	20,096 KB
Magic Piano 4.0.2.ipa	3/30/2012 4:20 AM	IPA File	25,086 KB
MagicPlan 1.5.ipa	3/31/2012 12:35 PM	IPA File	19,026 KB
MarbleMash 1.9.ipa	5/5/2011 1:01 PM	IPA File	7,550 KB
MarketDash 1.2.1.ipa	2/14/2012 8:37 PM	IPA File	4,022 KB
Memory Cards 4.3.0.ipa	5/5/2011 1:01 PM	IPA File	11,691 KB
Mobile News.ipa	7/13/2008 4:20 PM	IPA File	388 KB
Molecules 2.02.ipa	5/5/2011 1:01 PM	IPA File	972 KB
Molecules.ipa	8/3/2008 10:02 AM	IPA File	273 KB
MustEatBrds.ipa	11/22/2010 2:54 PM	IPA File	9,177 KB
MyFitnessPal 3.2.1.ipa	8/11/2011 7:45 PM	IPA File	21,949 KB
MyPad 2.5.4.ipa	2/9/2012 6:53 PM	IPA File	8,926 KB
Nearby 1.ipa	9/17/2008 10:49 PM	IPA File	709 KB
Netflix 2.1.2.ipa	3/30/2012 3:02 PM	IPA File	17,896 KB
Night Stand 2.02.ipa	8/11/2011 7:31 PM	IPA File	153,568 KB
Nightstand 1.2.2.ipa	8/11/2011 7:32 PM	IPA File	14,746 KB
Nook 3.1.2.13.ipa	2/27/2012 8:40 PM	IPA File	19,344 KB
NPR 2.2.ipa	11/27/2011 7:33 AM	IPA File	3,740 KB
NYTimes 2.2.ipa	3/30/2012 4:20 AM	IPA File	6,715 KB
OpenTable 1.7.1.ipa	3/12/2012 4:04 AM	IPA File	4,070 KB

70 items

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 Synthetic data experimentation Real Data Corpus experimentation
Year 2	Integrate GRR Develop/test management console	Develop/test data outlier detection Develop/test visualization component
Year 3	Large-scale testing on partner net	Final dev. of outlier detection algorithm Final dev. of visualization agent

Many challenges remain.

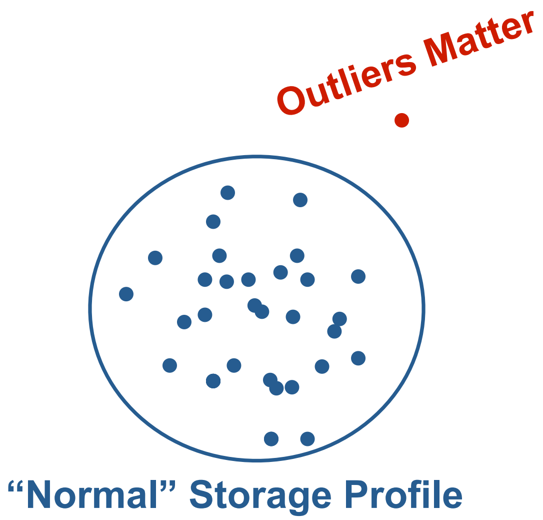
“Anomalous” suggests “normal” exists

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

Clustering algorithm selection/development

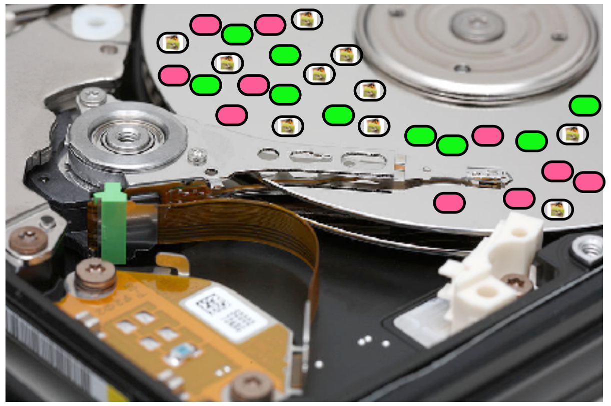
- Accuracy and speed trade-off of extant algorithms
- Develop combinatorial algorithm to improve accuracy
- Need for automated parameter selection amidst noise
- Feature selection

Engineering of visualization component



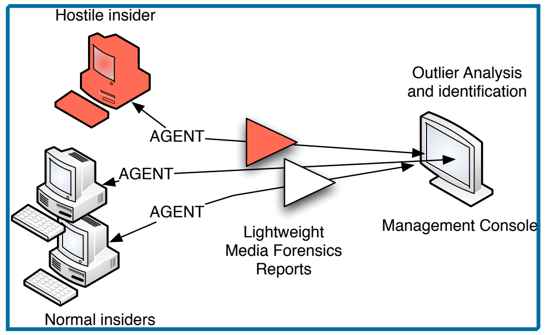
In conclusion, we are developing a system that uses "lightweight media forensics" to find hostile insiders.

We use random sampling to build a storage profile of media



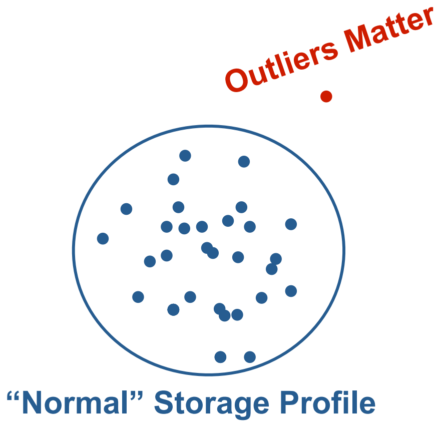
We collect these profiles on a central server

We cluster & data mine to find outliers.


Hostile insider
Outlier Analysis and identification
AGENT
AGENT
AGENT
Lightweight Media Forensics Reports
Management Console
Normal insiders

Contact:

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


Outliers Matter
"Normal" Storage Profile