The Cybersecurity Mess

Garfinkel, Simson L.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/44312
The Cybersecurity Mess

Simson L. Garfinkel
Associate Professor, Naval Postgraduate School
January 11, 2013

DISCLAIMER:

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

Monterey, CA — 1500 students
- US Military & Civilian (Scholarship for Service & SMART)
- Foreign Military (30 countries)

Graduate Schools of
Operational & Information Sciences (GSOIS)
- Computer Science
- Defense Analysis
- Information Sciences
- Operations Research
- Cyber Academic Group

National Capital Region (NCR) Office
- 900 N Glebe (Ballston)/Virginia Tech building
Inside Risks
The Cybersecurity Risk

Increased attention to cybersecurity has not resulted in improved cybersecurity.

T
rd of a notion that "cookies "—
"cookies" are typically used to track user activity on websites.

There are many reports of breaches and data thefts at some of the world's most sensitive institutions, and there's no guarantee that new systems are actually less secure than existing ones. A decade ago, computer systems were actually less secure than equivalent systems a decade ago. Numerous breakthroughs in cryptography, or even the use of encryption algorithms, have contributed to this.

Why the downward spiral? One reason is that cybersecurity's goal of reducing successful hacks is a large target to defend. Attackers have the luxury of choice: They can focus on the data that improves our services or the data that is essential to our operations. Even if the vulnerability were not in the data, the sensitive information stored in these systems can be used in other manners, such as social engineering, supply chain manipulation, or even kidnapping and extortion.

It may be that cybersecurity is one of the most effective ways to reduce the number of successful hacks. Even if the vulnerability were not in the data, the sensitive information stored in these systems can be used in other manners, such as social engineering, supply chain manipulation, or even kidnapping and extortion.

Views of Cybersecurity
The breadth of the problem means many different approaches are being proposed for solving the cybersecurity problem.

Cybersecurity can be viewed as

As an insider, what is needed is an objective position.
I have spent 25 years trying to secure computers...

...and I have given up!

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

Sept. 1987

1991

2000

2006

2006
Today’s systems are less secure than those of the 1970s.

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

- Computers are more complex — more places to attack them.
- There are multiple ways around each defense.
- It’s easier to attack systems than defend them.
- It’s easier to break things than to fix them.
A fatal exception 0E has occurred at 0028:C0011E36 in VXG VMM(01) + 00010E36. The current application will be terminated.

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

Press any key to continue _
We expect computers to crash...  

... expect them to be hacked.
I start every day with...

[ISN]
Internet Security News
[ISN] Former UNL student accused of hacking NeSIIS will face trial

By Lis Arneson
Daily Nebraskan
January 9, 2013

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

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

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

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

[...]

Visit the InfoSec News Security Bookstore
Best Selling Security Books and More!
http://www.shopinfosecnews.org
[ISN] Secret foot soldier targeting banks reveals meaner, leaner face of DDoS

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Subject</th>
<th>Date Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfoSec News</td>
<td><a href="mailto:isn@infosecnews.org">isn@infosecnews.org</a></td>
<td>[ISN] Former UNL student accused...</td>
<td>Today</td>
</tr>
<tr>
<td>InfoSec News</td>
<td><a href="mailto:isn@infosecnews.org">isn@infosecnews.org</a></td>
<td>[ISN] Hacker uses cat to deliver virus</td>
<td>Today</td>
</tr>
<tr>
<td>InfoSec News</td>
<td><a href="mailto:isn@infosecnews.org">isn@infosecnews.org</a></td>
<td>[ISN] Secret footsoldier targeting banks reveals meaner, leaner face of DDoS</td>
<td>Today</td>
</tr>
<tr>
<td>InfoSec News</td>
<td><a href="mailto:isn@infosecnews.org">isn@infosecnews.org</a></td>
<td>[ISN] Romanian Hacker Gets 21-Mo...</td>
<td>Today</td>
</tr>
<tr>
<td>InfoSec News</td>
<td><a href="mailto:isn@infosecnews.org">isn@infosecnews.org</a></td>
<td>[ISN] Ransom, implant attack highlights</td>
<td>Today</td>
</tr>
</tbody>
</table>


By Dan Goodin
Ars Technica
Jan 8 2013

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

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

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

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

[...]

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

http://infosecnews.org/
[ISN] Ransom, implant attack highlight need for healthcare security

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

By Taylor Armerding
CSO
January 08, 2013

All healthcare data breaches are not equal.

They’re all bad, and reaching epidemic levels. The Department of Health and Human Services, found that Protected Health Information (PHI) breaches nearly doubled from 2010 to 2011. The Department of Health and Human Services, has reported 525 breaches of 500 or more records, involving 21.4 individuals over the past three years, said Greg Kociolek, director of data security at Joint Commission, and Chief Information Officer of NewYork-Presbyterian Hospital.

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

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

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

[...]

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

http://infosecnews.org/
The cybersecurity mess: technical and social.

Most attention is focused on technical issues:

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

Non-technical issues are at the heart of the cybersecurity mess.

- Education & career paths
- Immigration
- Manufacturing policy

We will do better when we want to do better.
What do we think about cybersecurity today?
Cybersecurity is expensive.

Global cybersecurity spending: $60 billion in 2011
• *Cyber Security M&A*, pwc, 2011

172 Fortune 500 companies surveyed:
• Spending $5.3 billion per year on cybersecurity.
• Stopping 69% of attacks.

If they raise spending...
• $10.2 billion stops 84%
• $46.67 billion stops 95%
• “highest attainable level”

95% is not good enough.
Cybersecurity... is undefined.

There is no good definition for “cybersecurity”
- Preventing computers from being “hacked”
- Using “network security” to secure desktops & servers
- Something having to do with cybernetics

There is no way to measure cybersecurity
- Which OS is more secure?
- Which computer is more secure?
- Is “open source” more secure?
We do know one thing about cybersecurity...

Does spending more money make a computer more secure?
Cybersecurity research makes computers less secure!

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

The more we learn about securing computers, the better we get at attacking them
Cybersecurity is an “insider problem.”

bad actors
good people with bad instructions
remote access
malware

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

— ... but we can’t stop insiders.

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

Ames
Hanssen
Cybersecurity is a “network security” problem.

We can’t secure the hosts, so secure the network!
- Isolated networks for critical functions.
- Stand-alone hosts for most important functions.

But strong crypto limits visibility into network traffic, and…

http://www.flickr.com/photos/dungkal/2315647839/
... stuxnet shows that there are no isolated hosts.
“to a first approximation, every computer in the world is connected to every other computer.”


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.”
Secret Code in Color Printers Lets Government Track You

Tiny Dots Show Where and When You Made Your Print
San Francisco – A research team led by the Electronic Frontier Foundation (EFF) recently broke the code behind tiny tracking dots that some color laser printers secretly hide in every document.

Sample closeup of printer dots on a normal printed page

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

http://seeingyellow.com/
Cybersecurity is a process problem.

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

Microsoft Security Development Lifecycle

“Security is a process, not a product”

— Few organizations can afford SDL.
— Windows 7 Windows 8 is still hackable...

http://en.wikipedia.org/wiki/File:Bruce_Schneier_1.jpg
Windows RT "jailbroken", shows its Windows 8 roots

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

you@example.com

Hey Windows RT, your roots are showing!

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

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

2013 Security Threat Report
Straight from our labs to your brain
Cybersecurity is a money problem.

Security is a cost....

• ...Not an “enabler”
• No ROI

Chief Security Officers are in a no-win situation:

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

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

—Spaf’s first principle of security administration
Practical Unix Security, 1991
Cybersecurity is a “wicked problem”

There is no clear definition of the wicked problem

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

There is no “stopping rule”

— The problem can never be solved.

Solutions are not right or wrong

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

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

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

Every wicked problem is a symptom of another problem


  http://www.chathamhouse.org/publications/twt/archive/view/178579
Why is cybersecurity so hard?
Cybersecurity has an active, malicious adversary.

The adversary...

— *Turns your bugs into exploits*
— *Adapts to your defenses*
— *Waits until you make a mistake*
— *Attacks your employees when your systems are secure*
For example...
Compiler bugs are security vulnerabilities!

The adversary chooses:
- What to exploit
- When to exploit it
- How to exploit it

We have seen:
- Optimizations can become security vulnerabilities
- The same errors are repeatedly made by different programmers

What’s difference between a bug and an attack?
— The programmer’s intent.
The supply chain creates numerous security vulnerabilities
ACComplice: Location Inference using Accelerometers on Smartphones

Jun Han, Emmanuel Owusu, Le T. Nguyen, Adrian Perrig, Joy Zhang

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

I. INTRODUCTION

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

This research was supported by C-Lab at Carnegie Mellon under grant ENA1451.2.009 and NSF CNS-0847317, from the Army Research Office, and by support from NSF under TRUST STC CCF-0424422, BESIT DGE- 0450124, and CNS-092504, and by a Google research award. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies of the contractors, either express or implied, of ARO, CMU, Google, NSF or the U.S. Government or any of its agencies.

ACComplice: Location Inference using Accelerometers on Smartphones

Jun Han, Emmanuel Owusu, Le T. Nguyen, Adrian Perrig, Joy Zhang
[junhan, cowusu, lennguyen, perrig, sky]@cmu.edu
Carnegie Mellon University

Accelerometers are a particularly interesting threat as a large amount of accelerometer data is collected from devices including tablet PCs, MP3 players, and smartphones. This array of devices provides a large volume of data to exploit.

Furthermore, by correlating the accelerometers with mul-

Fig. 7. Verification of map matching algorithm with the known st

ter 2a and Experiment 2b, respectively. The green (star) cu-

This section explains an algorithm that can be used to predic-

We assume that the adversary can access, or exposes their cellular or Wi-Fi base

This is a very powerful side-channel that can be exploited even

This research was supported by C-Lab at Carnegie Mellon under grant

EN-1451.2.009 and NSF CNS-0847317, from the Army Research Office, and

by support from NSF under TRUST STC CCF-0424422, BESIT DGE- 0450124,

and CNS-092504, and by a Google research award. The views and conclusions con-

In the case of erroneous starting points, the map matching

DS

H

M

P

0

i

i

i

from 1 to s, where s is the number

This is aligned to every point on the map (each node represents

The adversary can extract a mobile user’s trajectory based on the leaked accelerometer

To verify the results, we perform the aforementioned map

We assume that the adversary can have access to a mobile phone’s accelerometer

Furthermore, by correlating the accelerometer data from multiple phones it is possible to

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 express 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 in corporate 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 herein demonstrates a clear violation of user control over sensitive private information.

This research was supported by C-Lab at Carnegie Mellon under grant ENA1451.2.009 and NSF CNS-0847317, from the Army Research Office, and by support from NSF under TRUST STC CCF-0424422, BESIT DGE- 0450124, and CNS-092504, and by a Google research award. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies of the contractors, either express or implied, of AR0, CMU, Google, NSF or the U.S. Government or any of its agencies.

ACComplice: Location Inference using Accelerometers on Smartphones

Jun Han, Emmanuel Owusu, Le T. Nguyen, Adrian Perrig, Joy Zhang

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

https://sparrow.ece.cmu.edu/group/pub/han_accomplice_comsnets12.pdf

Jun Han, Emmanuel Owusu, Thanh-Le Nguyen, Adrian Perrig, and Joy Zhang

”ACComplice: Location Inference using Accelerometers on Smartphones” In Proceedings of the 4th International Conference on Communication Systems and Networks (COMSNETS 2012), Bangalore, India, January 3-7, 2012.
Fortunately adversaries are not all powerful.

Adversaries are impacted by:

— Economic factors
— Attention span
— Other opportunities

You don’t have to run faster than the bear….
There are solutions to many cybersecurity problems... 
... but we don’t use them.

30% of the computers on the Internet run Windows XP
• Yes, Windows 7 has vulnerabilities, but it’s better.

Apple users don’t use anti-virus.
• Yes, Apple tries to fix bugs, but

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

DNSSEC

Smart Cards
Many people liken cybersecurity to the flu.

DHS calls for “cyber hygiene”

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

— “STOP, THINK, CONNECT”
A better disease model might be obesity…

Making people fat is good business:
- Farm subsidies
- Restaurants
- Healthcare and medical utilization
- Weight loss plans
  - Few make money when Americans stay trim and healthy.

Lax security is also good business:
- Cheaper cost of deploying software
- Private information for marketing
- Selling anti-virus & security products
- Cleaning up incidents
  - Few benefit from secure computers
Many people say that cyber war is like nuclear war.

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

http://www.acus.org/new_atlanticist/mind-cyber-gap-deterrence-cyberspace
Biowar is a better model for cyberwar.

— Cheap to produce
— Easy to attack
— Hard to control
— Hard to defend
— No clear end
Non-technical factors impact cybersecurity.

These factors reflect deep divisions within our society.

- **Shortened** development cycles

- **Education**: General failure in teaching science, engineering & math

- **HR**: Inability to attract and retain the best workers

- **Immigration Policy**: Foreign students; H1B Visa

- **Manufacturing Policy**: Building in your enemy’s factories is a bad idea

Solving the cybersecurity mess requires solving these issues
Short development cycles

Insufficient planning:
• Security not “baked in” to most products.
• Few or no security reviews
• Little Usable Security

Insufficient testing:
• Testing does not uncover security flaws
• No time to retest after fixing

Poor deployment:
• Little monitoring for security problems
• Difficult to fix current system when new system is under development
Education is not supplying enough security engineers

Students are not pursuing CS in high school & college

Those going into CS are not pursuing security

Many of those studying CS are not staying in the country
73% of states require computer “skills” for graduation. Only 37% require CS “concepts.”

And teachers are poorly paid!

— Salaries for beginning & average teachers lag CS engineers by 30%
— Adjusting for cost-of-living and shorter work week.

• Linda Darling-Hammond, Stanford University, 2004
http://www.srnleads.org/data/pdfs/ldh_achievement_gap_summit/inequality_TCR.pdf
High school students are not taking AP computer science!

http://www.acm.org/public-policy/AP%20Test%20Graph%202009.jpg
Computer Science undergraduate enrollment is low.

2010-2011 CRA Taulbee Survey:

Figure 2. BS Production (All Departments)

Source: Table 3: Bachelor’s Degrees Awarded by Department Type
7% of Bachelor’s degrees awarded to “nonresident alien” (12,800 to US citizens)

<table>
<thead>
<tr>
<th>Table 5. Bachelor’s Degrees Awarded by Ethnicity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonresident Alien</td>
</tr>
<tr>
<td>Nonresident Alien</td>
</tr>
<tr>
<td>Amer Indian or Alaska Native</td>
</tr>
<tr>
<td>Asian</td>
</tr>
<tr>
<td>Black or African-American</td>
</tr>
<tr>
<td>Native Hawaiian/Pac Islander</td>
</tr>
<tr>
<td>White</td>
</tr>
<tr>
<td>Multiracial, not Hispanic</td>
</tr>
<tr>
<td>Hispanic, any race</td>
</tr>
<tr>
<td>Total Residency &amp; Ethnicity Known</td>
</tr>
<tr>
<td>Resident, ethnicity unknown</td>
</tr>
<tr>
<td>Residency unknown</td>
</tr>
<tr>
<td>Grand Total</td>
</tr>
</tbody>
</table>

—Most do not go on to advanced degrees.
50% of Master’s degrees awarded to nonresident alien (4960 to US citizens)

### Table 9. Master’s Degrees Awarded by Ethnicity

<table>
<thead>
<tr>
<th>Ethnicity</th>
<th>CS</th>
<th>CE</th>
<th>I</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonresident Alien</td>
<td>3,332</td>
<td>776</td>
<td>389</td>
<td>4,497</td>
</tr>
<tr>
<td>Amer Indian or Alaska Native</td>
<td>12</td>
<td>0</td>
<td>12</td>
<td>24</td>
</tr>
<tr>
<td>Asian</td>
<td>753</td>
<td>108</td>
<td>245</td>
<td>1,106</td>
</tr>
<tr>
<td>Black or African-American</td>
<td>96</td>
<td>13</td>
<td>123</td>
<td>232</td>
</tr>
<tr>
<td>Native Hawaiian/Pac Island</td>
<td>19</td>
<td>0</td>
<td>6</td>
<td>25</td>
</tr>
<tr>
<td>White</td>
<td>1533</td>
<td>142</td>
<td>1113</td>
<td>2,788</td>
</tr>
<tr>
<td>Multiracial, not Hispanic</td>
<td>8</td>
<td>4</td>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>Hispanic, any race</td>
<td>119</td>
<td>26</td>
<td>92</td>
<td>237</td>
</tr>
<tr>
<td>Total Residency &amp; Ethnicity Known</td>
<td>5,872</td>
<td>1,069</td>
<td>1,984</td>
<td>8,925</td>
</tr>
<tr>
<td>Resident, ethnicity unknown</td>
<td>320</td>
<td>88</td>
<td>205</td>
<td>613</td>
</tr>
<tr>
<td>Residency unknown</td>
<td>419</td>
<td>26</td>
<td>17</td>
<td>462</td>
</tr>
<tr>
<td>Grand Total</td>
<td>6,611</td>
<td>1,183</td>
<td>2,206</td>
<td>10,000</td>
</tr>
</tbody>
</table>

— *We should let them stay in the country after they graduate*
50% of PhDs awarded in 2011 to nonresident aliens (642 to US citizens)

<table>
<thead>
<tr>
<th></th>
<th>CS</th>
<th>CE</th>
<th>I</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonresident Alien</td>
<td>634</td>
<td>130</td>
<td>44</td>
<td>808</td>
</tr>
<tr>
<td>Amer Indian or Alaska Native</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Asian</td>
<td>171</td>
<td>16</td>
<td>14</td>
<td>201</td>
</tr>
<tr>
<td>Black or African-American</td>
<td>16</td>
<td>1</td>
<td>6</td>
<td>23</td>
</tr>
<tr>
<td>Native Hawaiian/Pac Islander</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>White</td>
<td>465</td>
<td>42</td>
<td>52</td>
<td>559</td>
</tr>
<tr>
<td>Multiracial, not Hispanic</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Hispanic, any race</td>
<td>22</td>
<td>4</td>
<td>1</td>
<td>27</td>
</tr>
<tr>
<td>Total Residency &amp; Ethnicity Known</td>
<td>1,317</td>
<td>193</td>
<td>119</td>
<td>1,629</td>
</tr>
<tr>
<td>Resident, ethnicity unknown</td>
<td>43</td>
<td>4</td>
<td>2</td>
<td>49</td>
</tr>
<tr>
<td>Residency unknown</td>
<td>96</td>
<td>8</td>
<td>0</td>
<td>104</td>
</tr>
<tr>
<td>Grand Total</td>
<td>1,456</td>
<td>205</td>
<td>121</td>
<td>1,782</td>
</tr>
</tbody>
</table>

— *We did not train Russia’s weapons scientists at MIT during the Cold War.*
Just 67 / 1275 (5%) PhDs went into Information Assurance
15 professors & postdocs; 48 to industry & government

Table 14. Employment of New PhD Recipients By Specialty

<table>
<thead>
<tr>
<th>Specialty</th>
<th>Industry</th>
<th>Government</th>
<th>Self-Employed</th>
<th>Unemployed</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenure-track</td>
<td>14</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Researcher</td>
<td>6</td>
<td>1</td>
<td>4</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>Postdoc</td>
<td>38</td>
<td>1</td>
<td>12</td>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>Teaching Faculty</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

North American PhD Granting Depts.

<table>
<thead>
<tr>
<th>Specialty</th>
<th>Tenure-track</th>
<th>Researcher</th>
<th>Postdoc</th>
<th>Teaching Faculty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artifical Intelligence</td>
<td>14</td>
<td>6</td>
<td>38</td>
<td>2</td>
</tr>
<tr>
<td>Computer-Supported</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Cooperative Work</td>
<td>5</td>
<td>2</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Databases/Information Retrieval</td>
<td>6</td>
<td>1</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>Graphics/Visualization</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Hardware/Architecture</td>
<td>1</td>
<td>7</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Human-Computer Interaction</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>High-Performance Computing</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Informatics: Other Science</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Information Assurance/Security</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Information Science</td>
<td>9</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Networks</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>6</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Programming Languages/Compilers</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Robotic Vision</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Scientific/Computing</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Social Computing</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Social Informatics</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Software Engineering</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Theory and Algorithms</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>106</td>
<td>67</td>
<td>12</td>
<td>10</td>
</tr>
</tbody>
</table>

North American, Other Academic

<table>
<thead>
<tr>
<th>Specialty</th>
<th>Tenure-track</th>
<th>Researcher</th>
<th>Postdoc</th>
<th>Teaching Faculty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artifical Intelligence</td>
<td>3</td>
<td>0</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Computer-Supported</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Cooperative Work</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Databases/Information Retrieval</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Graphics/Visualization</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Hardware/Architecture</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Human-Computer Interaction</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>High-Performance Computing</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Informatics: Other Science</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Information Assurance/Security</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Information Science</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Networks</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Programming Languages/Compilers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Robotic Vision</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Scientific/Computing</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Social Computing</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Social Informatics</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Software Engineering</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Theory and Algorithms</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>18</td>
<td>3</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

North American, Non-Academic

<table>
<thead>
<tr>
<th>Specialty</th>
<th>Industry</th>
<th>Government</th>
<th>Self-Employed</th>
<th>Unemployed</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artificial Intelligence</td>
<td>64</td>
<td>2</td>
<td>49</td>
<td>46</td>
<td>41</td>
</tr>
<tr>
<td>Computer-Supported</td>
<td>24</td>
<td>2</td>
<td>24</td>
<td>20</td>
<td>17</td>
</tr>
<tr>
<td>Cooperative Work</td>
<td>20</td>
<td>5</td>
<td>20</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>Databases/Information Retrieval</td>
<td>50</td>
<td>1</td>
<td>50</td>
<td>49</td>
<td>46</td>
</tr>
<tr>
<td>Graphics/Visualization</td>
<td>38</td>
<td>2</td>
<td>38</td>
<td>38</td>
<td>38</td>
</tr>
<tr>
<td>Hardware/Architecture</td>
<td>8</td>
<td>1</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Human-Computer Interaction</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>High-Performance Computing</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Informatics: Other Science</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Information Assurance/Security</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Information Science</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Networks</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Programming Languages/Compilers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Robotic Vision</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Scientific/Computing</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Social Computing</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Social Informatics</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Software Engineering</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Theory and Algorithms</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>85</td>
<td>178</td>
<td>1,275</td>
<td>89.0%</td>
<td></td>
</tr>
</tbody>
</table>

Security should be taught to everyone, but we need specialists
Georgetown Prof: 50% of graduate students in sciences are foreigners because salaries aren’t high enough.

Highest paying occupations:

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

—Source: Bureau of Labor Stats

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

• US did not build WW2 aircraft in Germany
Security problems are bad for society as a whole... 

... because [wireless] computers are everywhere.

50 microprocessors per average car

http://www.autosec.org/

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

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

2008: demonstrated wireless attack on implantable pacemakers

2012: demonstrated wireless attack on insulin pump

DDoS the endocrine system!

From: InfoSec News <alerts@infosecnews.org>
Date: April 23, 2012 3:16:23 AM EDT
To: isn@infosecnews.org


By Dan Goodin
ars technica
April 22, 2012

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

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

"It wasn't even planned," Auriemma told Ars, referring to the most damaging of his two attacks, which rendered the device useless for three days...
By Tracy Kitten
Bank Info Security
April 19, 2012

Lax security makes non-banking sites prime targets for skimming attacks...
Cell phones cannot be secured.

Cell phones have:
- Wireless networks, microphone, camera, & batteries
- Downloaded apps
- Bad crypto

Cell phones can be used for:
- Tracking individuals
- Wiretapping rooms
- Personal data

Major security breakthroughs since 1980:

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

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

— “Why Cryptosystems Fail,” Ross Anderson, 
  http://www.cl.cam.ac.uk/~rja14/Papers/wcf.pdf
There is no obvious way to secure cyberspace.

We trust computers…

— *but we cannot make them trustworthy.*
(A “trusted” system is a computer that can violate your security policy.)

We know a lot about building secure computers…

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

We know about usable security…

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

We should design with the assumption that computers will fail…

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

Despite the newfound attention to cybersecurity, our systems seem to be growing more vulnerable every year.
To Make a Difference
Be a [polite] critic of USG Information Systems

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

Things you can do:

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

Use Section 508!

- Section 508 of the Rehabilitation Act (29 USC 794 d) requires that federal government information systems accommodate people with disabilities.

- Bad typography, poor choice of fonts, use of Flash *may be illegal*

- Speak with the Section 508 Coordinator — or volunteer to become one!
Be a helpful

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

Real live case:

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

• I was a hero!

Take the time to learn:

• Microsoft Word Styles; Acrobat Forms; Excel Macros
Push an INFOSEC AGENDA that is *realistic*.

Help your agencies deploy:
- IPv6
- DNSSEC
- Modern Web Browsers

Help your agencies eliminate:
- Windows XP
- Internet Explorer 6 / 7 / 8

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

Submit bug reports!
Don’t use pie charts

These two pie charts present exactly the same information.

This graph presents the same information better:

—And it’s Section 508 compliant!
Security problems reflect deep societal problems. You need to fix our society.

Follow the money.

IEEE Security & Privacy
Florêncio and Herley, Dec. 2012

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

Supporting slides:

Video
— https://www.usenix.org/conference/woot12/keynote-tba (1 hour, 25 minutes)
Backup Slides
Other things for SFS students to know...

Continuing education is really important!
- Go to conferences
- Read journals and magazines
- Keep reading the academic literature
- Concentrate on self-development.

Find a mentor.
Stay in touch with your faculty advisor!

Algorithms matter.
Data matters
- Learn how to present data