Note: This presentation is to inform interested parties of research and to encourage discussion of work in progress. Any views expressed on the issues are those of the author and not those of the U.S. Census Bureau.

Cybersecurity research is not making us more secure

Simson L. Garfinkel

*Senior Computer Scientist for Confidentiality and Data Access, US Census Bureau**

October 30, 2018

University of Pennsylvania

**Affiliation presented only for purpose of identification.*

Photos from https://pixabay.com

"Cybersecurity research is not making us more secure."
Interpreting this inflammatory title...

1. Cybersecurity research is making us **less secure**?

2. **Other things** are making us secure, but it's not cybersecurity research?

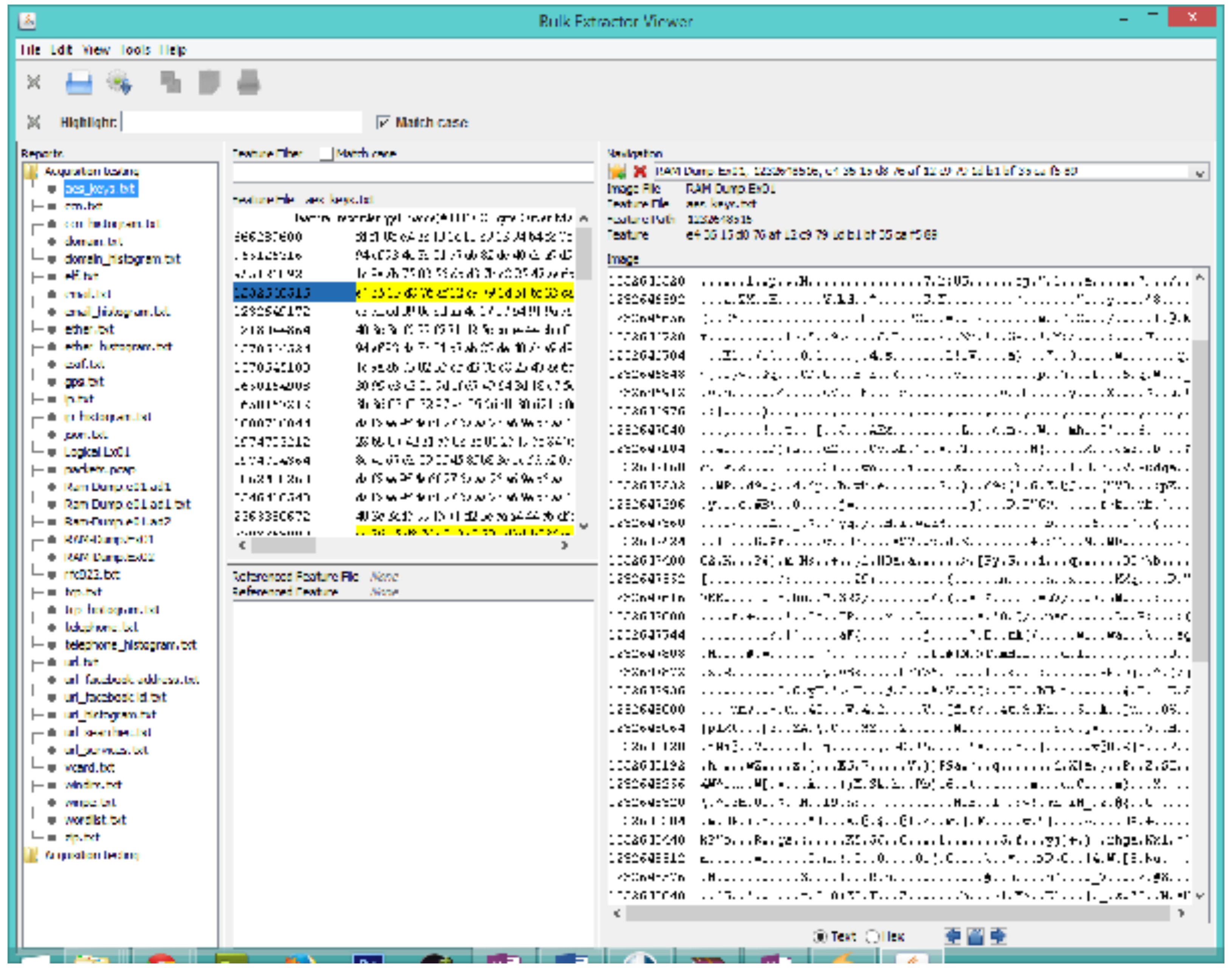
   Are computers more secure than 10 years ago?

   Are **we [society?]** more secure than 10 years ago?

3. **Other things are needed**, so that cybersecurity research could realize its promise of making us more secure?

4. **What's the purpose of cybersecurity research**, if not to make us more secure?

This talk is influenced by three projects.



Bulk_Extractor Digital Forensics Tool
2006-2014

Based on cybersecurity research at:
MIT 1989-1990
MIT 2002-2005
Harvard SEAS 2005-2006
Naval Postgraduate School 2006-2014

V 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.

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

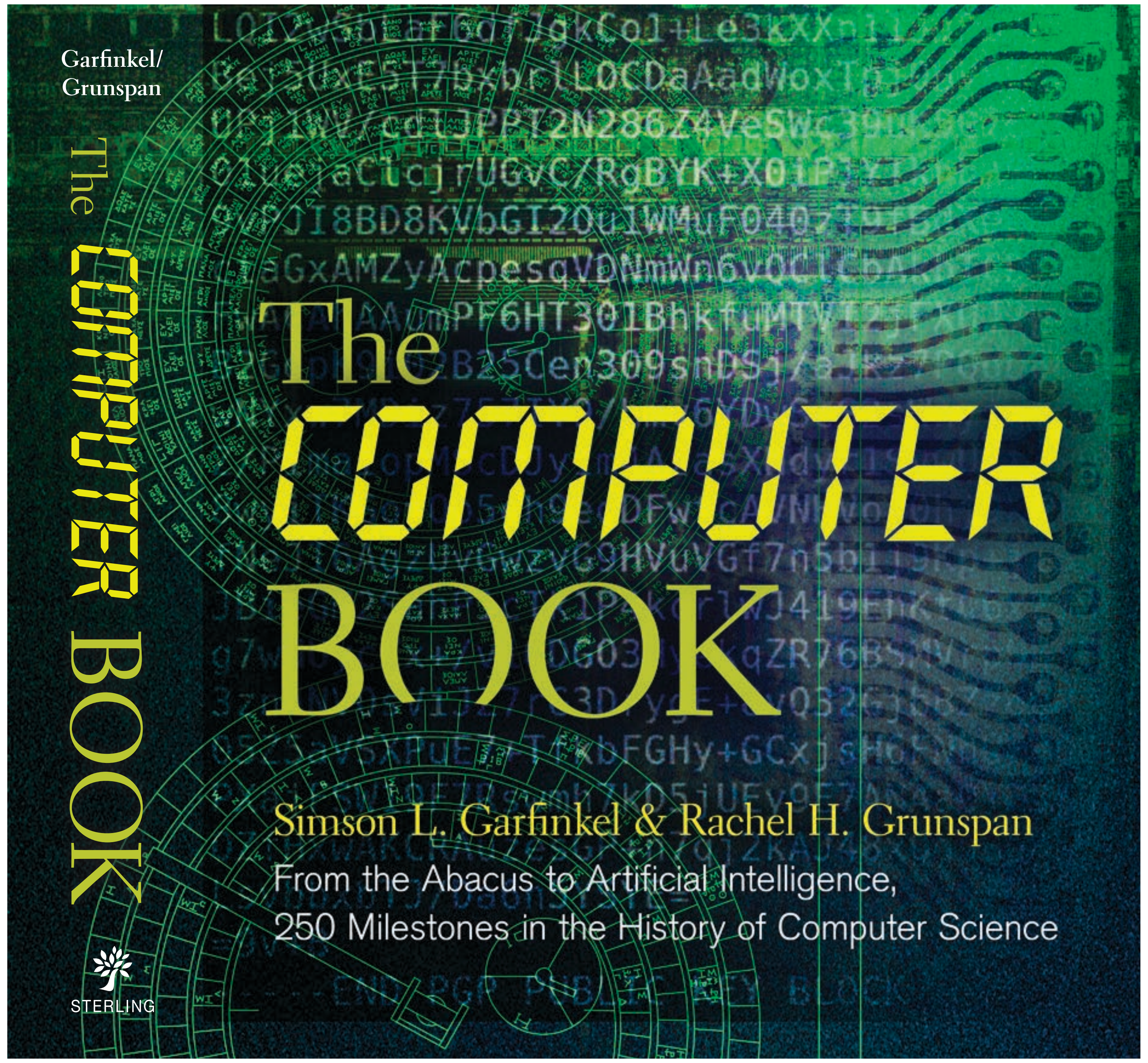
ILLUSTRATION BY YAREK WASZUL

JUNE 2012 | VOL. 55 | NO. 6 | COMMUNICATIONS OF THE ACM 29

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

"The Cyber Security Risk",
Communications of the ACM,
June 2012, 55(6)

Based on experiences as:
Founder of thee Internet startups
Computer journalist, 1988-2003



The Computer Book
Garfinkel and Grunspan,
Sterling Milestones, 2018

Based on:
Thousands of Google searches,
April to December, 2017

The Computer Book: From the Abacus to Artificial Intelligence, 250 Milestones in the History of Computer Science
Garfinkel and Grunspan, 2018

1945

EDVAC First Draft Report

John Mauchly, J. Persper Eckert,
John von Neumann, Herman Goldstine

"Inventors"

Year of Milestone

Title of Milestone

Photo, possibly historic

NOTE: These pages are only *similar to* the actual pages from *The Computer Book*

http://www.computerhistory.org/collections/catalog/102689071

1943

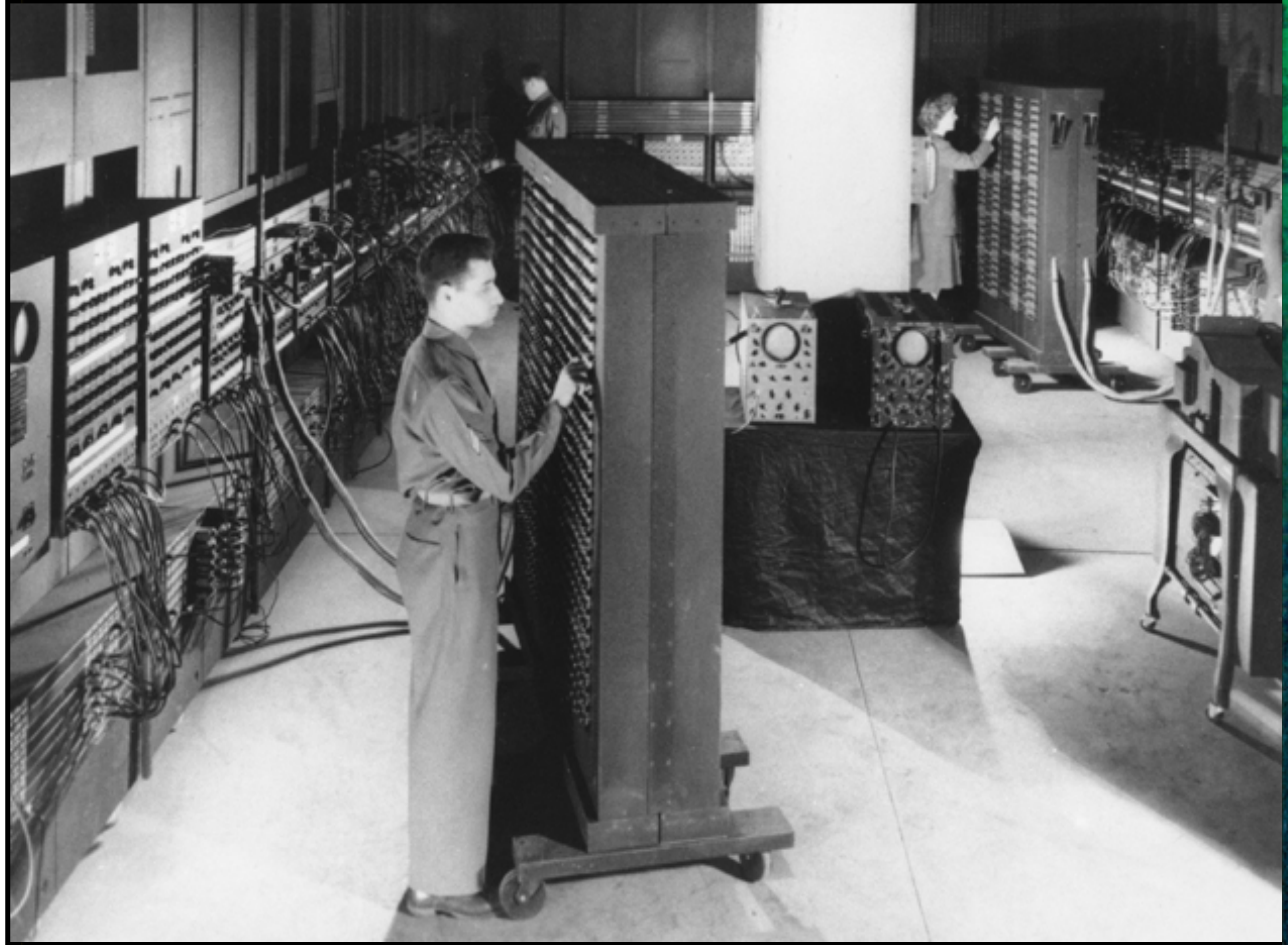
ENIAC

John Mauchly, J. Preper Eckert

Program stored on 1,200 10-position switches.

The hardware design team did not consider the possibility that software might be hard to write or to debug.

NOTE: Not actually the text from our book



https://www.engadget.com/2014/11/25/eniac-on-public-display/

This talk has four parts.

1. Cybersecurity is too hard for users to get right.

We expect too much from users

Most cybersecurity decisions should be made by cybersecurity experts

There are many things that should be left to **experts**

Examples include:

- Aviation, Construction, Medicines, Teaching, ...

"An expert is someone who has a prolonged or intense experience through practice and education in a particular field." —Wikipedia

Larry Walters lawn chair flight
July 2, 1982

Part 2: Experts

1. Cybersecurity is too hard for users to get right

2. Cybersecurity experts can't get it right, either

At least, not all the time

All experts make mistakes due to limitations of expert knowledge

This happens in cybersecurity, just like in other fields

Tacoma Narrows Bridge Collapse (1940)

Part 3: Leadership

1. Cybersecurity is too hard for users to get right

2. Cybersecurity experts can't get it right, either

3. **Despite talk, leadership does not value cybersecurity**

Leadership does not [properly] value many things:

Safety — e.g. the Challenger Disaster (STS-51-L)

Systemic risk — e.g. the Financial Crisis

STS-51-L Disaster, January 28, 1986

THE TI

Max 13C, min 5C

Tuesday September 16 2008 timesonline.co.uk No 69430

Lehman collapse sends shockwave round world

ares and oil prices plunge, thousands lose jobs

Lehman Brothers bankruptcy, September 15, 2008

1. Cybersecurity is too hard for users to get right

2. Cybersecurity experts can't get it right, either

3. Despite talk, leadership does not value cybersecurity

4. Research is needed on how to transition research

Technology transition is a major problem!

There is no financial incentive for vendors to make products secure

Xerox Star Personal Computer, 1981
$16,500 ($45,822 in 2018)
384 KiB RAM
10-40 MB hard drive
17 inch 1024x800 graphical display

Technology transitioning is a longstanding problem.

1973

Xerox Alto

Butler Lampson, Charles P. Thacker

GUI Display

Word Processing • Email

Local Area Network

Laser Printer

2000 machines produced

0 sold—it wasn't a product

https://www.geekwire.com/2016/1973-xerox-computer-inspired-paul-allen-others-restored-running-seattle-museum/

Part 4: Technology Transition

IBM Personal Computer, 1981
16 KiB RAM
$1,565 ($4,346 in 2018)
360K floppy drives (1 or 2)
80x25 monochrome display or
640x480 CGA graphics display

Xerox Star Personal Computer, 1981
$16,500 ($45,822 in 2018)
384 KiB RAM
10-40 MB hard drive
17 inch 1024x800 graphical display

1

Cybersecurity is too hard [for average users]

Cybersecurity is hard because there is an active, malicious adversary.

The Adversary

Turns bugs into exploits

Adapts to our defenses

Has more time than we do

Attacks employees when systems are secure

https://www.deviantart.com/pptsy/art/The-Adversary-504369005

With this powerful adversary, we expect a lot from users.

1. Use a **strong password** on **all devices**
2. Passwords must be **encrypted in transit and in storage**
3. Apply security patches on a **timely basis** (e.g. **immediately**)
4. **Active firewall** on all networked devices
5. Keep **anti-virus** current; enable **real-time scanning**
6. Employ **centralized endpoint management**
7. **Encrypt all data** on portable devices
8. Put servers in a **locked, physically secure area**
9. Backup data, and **test backups regularly**
10. **Wipe or destroy** devices when they are retired

Sound familiar?

The University of Pennsylvania expects all that and much more of its users *and* system administrators.

I. Title

A. Name: Computer Security Policy

B. Number: 20100308-computersecurity

C. Author: D. Millar, J. Choate, E. Katz, M. Muth, J. Beeman (ISC), L. Steinfeld (OACP)

D. Status:

[ ] proposed [ ] under review [X] approved [ ] rejected [ ] obsolete

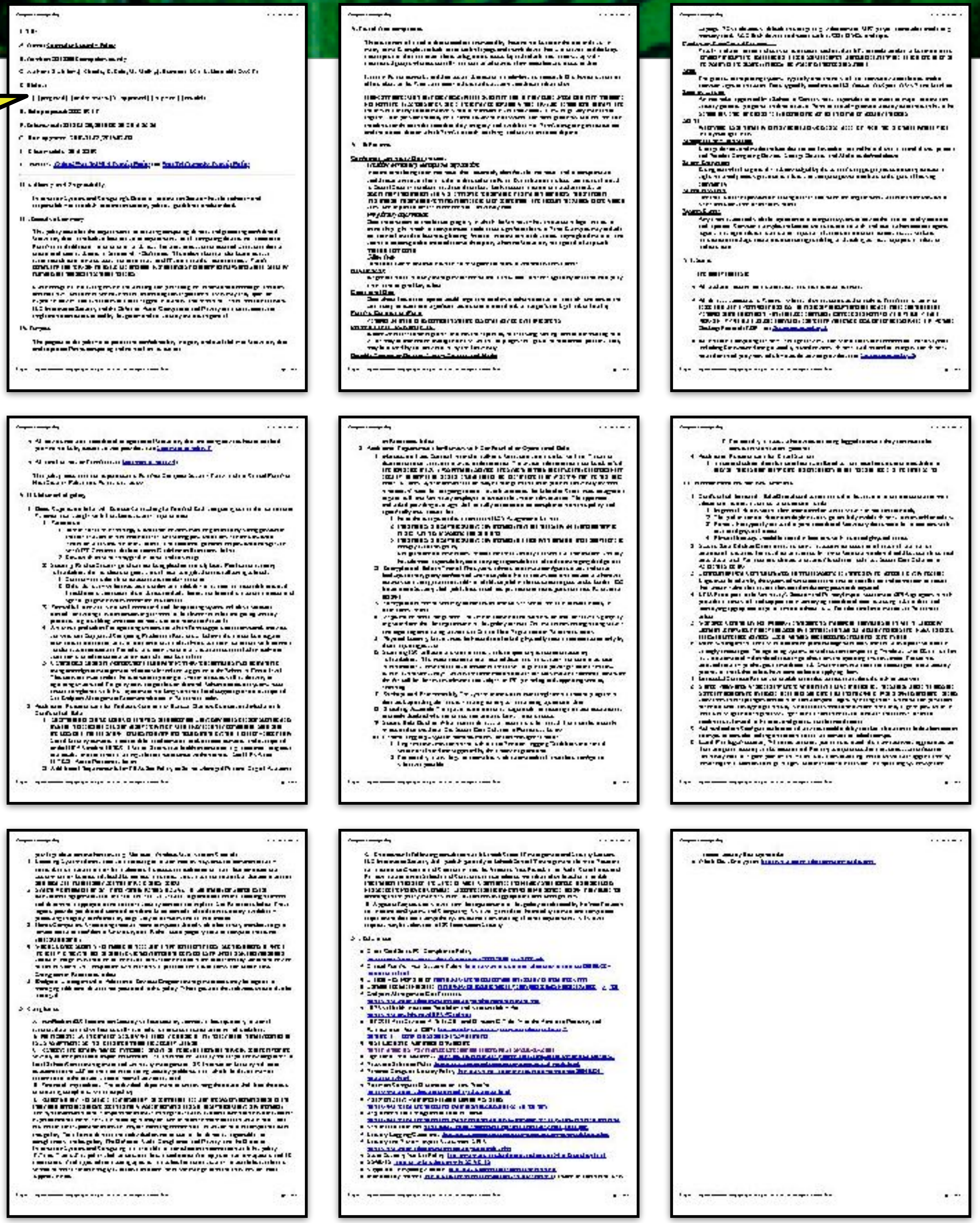
E. Date proposed: 2008-09-17

F. Date revised: 2010-03-23, 2010-05-20, 2015-05-25

G. Date approved: 2010-03-08, 2016-02-09

H. Effective date: 2016-02-09

I. Obsoletes: *Critical PennNet Host Security Policy* and *PennNet Computer Security Policy*



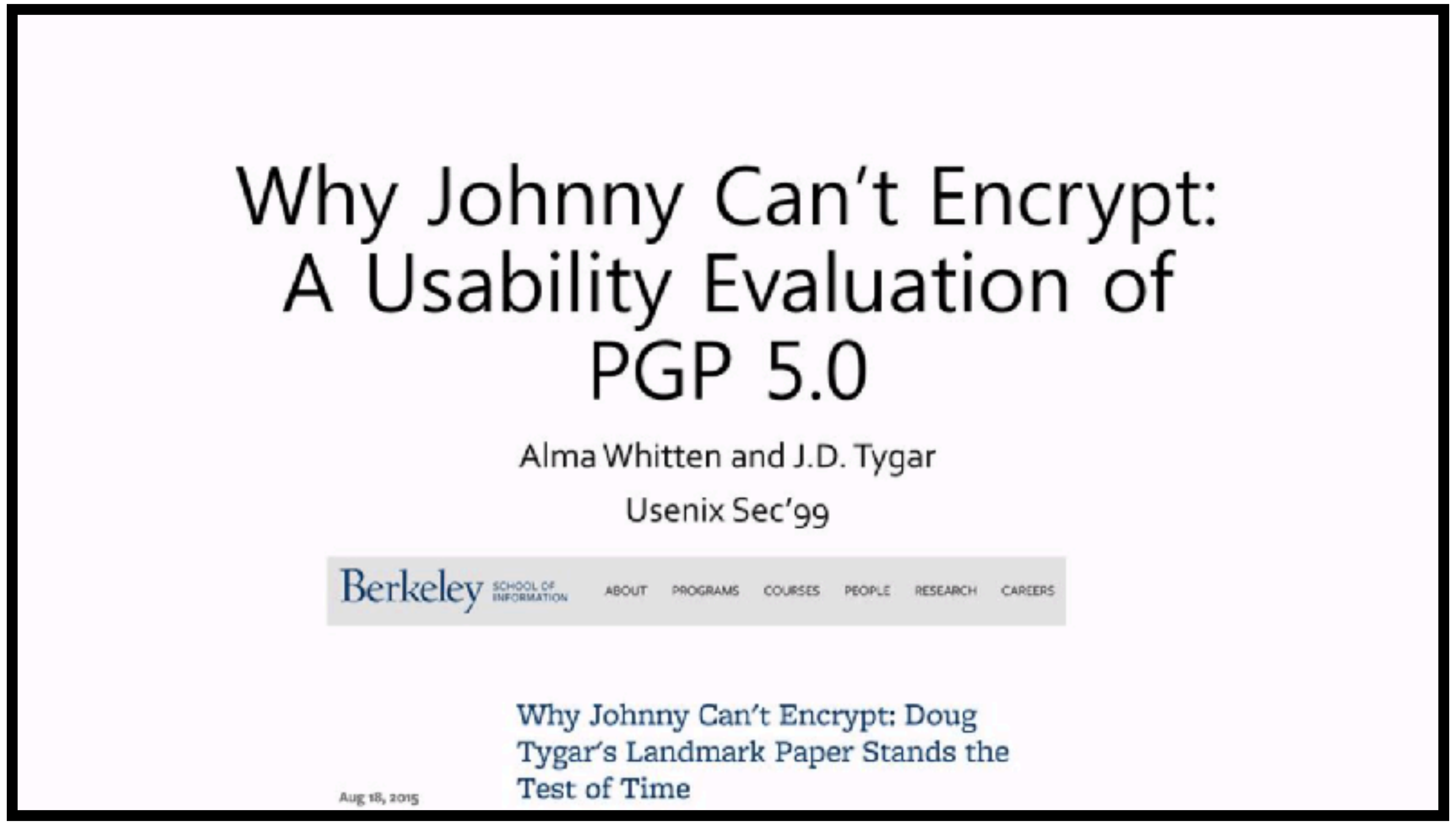
http://www.upenn.edu/computing/group/npc/approved/20100308-computersecurity.html

In 1999, "Why Johnny Can't Encrypt" created the notion of usability of "security software."

"Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0"

Alma Whitten and J.D. Tygar
Usenix Security '99

2015 USENIX Security "Test of Time" Award



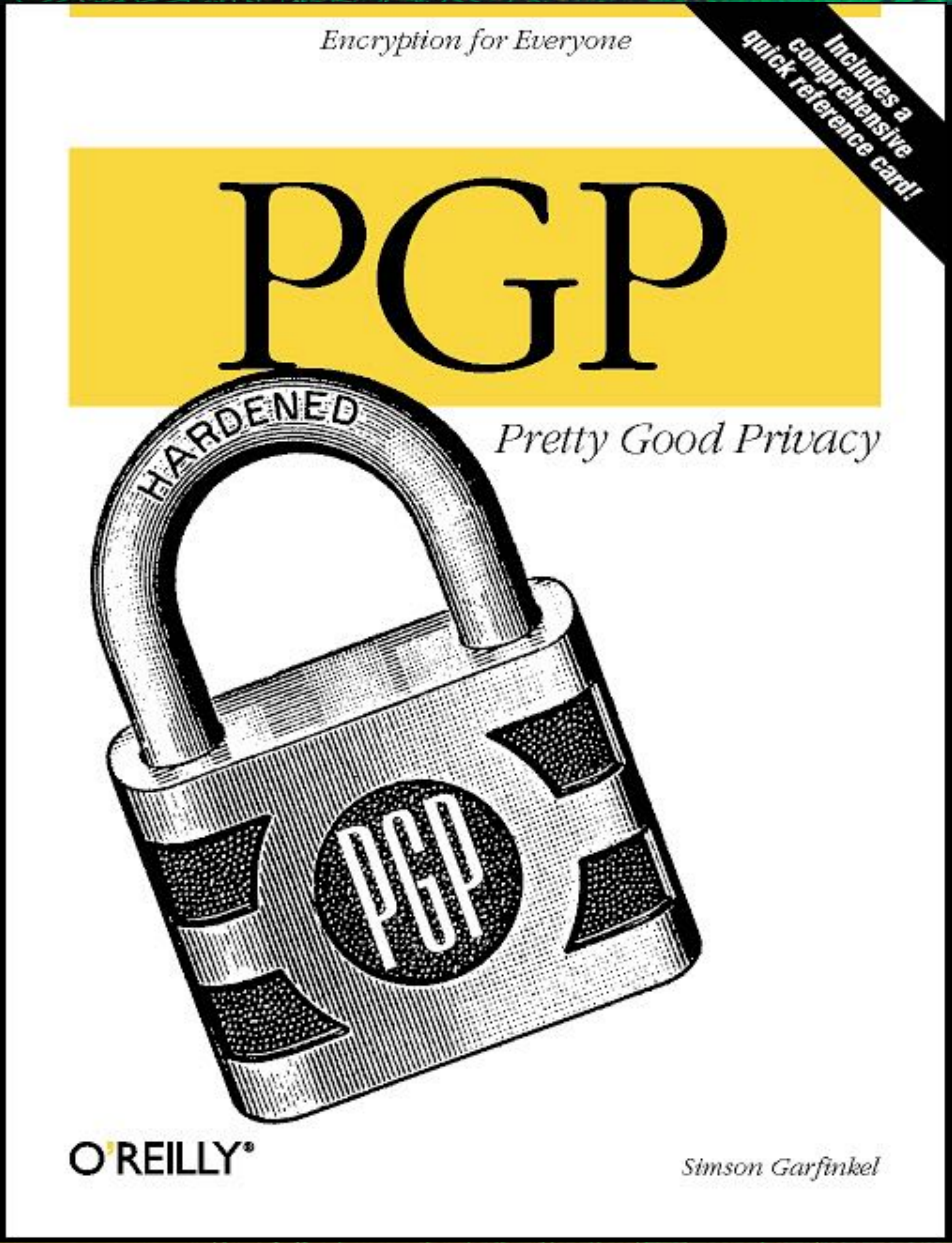
1991

Pretty Good Privacy (PGP)

Phil Zimmermann

PGP was a command-line tool.

Whitten & Tygar reviewed the 1998 MacPGP version.



PGP: Pretty Good Privacy, Garfinkel, O'Reilly, 1994

Whitten & Tygar actually analyzed the 1998 Macintosh PGP program.

Definition: Security software is usable if the people who are expected to use it:

- **Are reliably made aware of the security tasks they need to perform**
- **Are able to figure out how to successfully perform those tasks**
- **Don't make dangerous errors**
- **Are sufficiently comfortable with the interface to continue using it**

—Whitten & Tygar, 1999

When it comes to cybersecurity, many non-experts can compromise security.

Cybersecurity researchers that study non-experts have found that usability problems dominate *all aspects* of the security chain

Users — Don't make sensible choice, put everyone at risk

Programmers — Develop software with cybersecurity vulnerabilities

System Administrators — Errors in configuration, deployment, incident response

Managers and Leadership — Errors in priority setting, resource allocation

With active adversaries,
all software is security software,
all programmers are security programmers.

For example: As compilers get better at optimizing, security bugs are emerging in old code. [2012]

Undefined Behavior: What Happened to My Code?*

Xi Wang   Haogang Chen   Alvin Cheung   Zhihao Jia[†]
Nickolai Zeldovich   M. Frans Kaashoek
MIT CSAIL   [†]*Tsinghua University*

APSys '12, July 23-24, 2012

```
struct timeval tv;
unsigned long junk;          /* XXX left uninitialized
                                on purpose */
gettimeofday(&tv, NULL);
srandom((getpid() << 16)
        ^ tv.tv_sec ^ tv.tv_usec ^ junk);
```

Figure 8: An uninitialized variable misuse for random number generation, in `lib/libc/stdlib/rand.c` of the FreeBSD libc, where the seed computation will be optimized away.

For example: Bugs in CPU silicon are remotely exploitable! [2008]
So every team working on a modern CPU must have security engineer.

Programs that are “secure” on one CPU may be vulnerable on another.

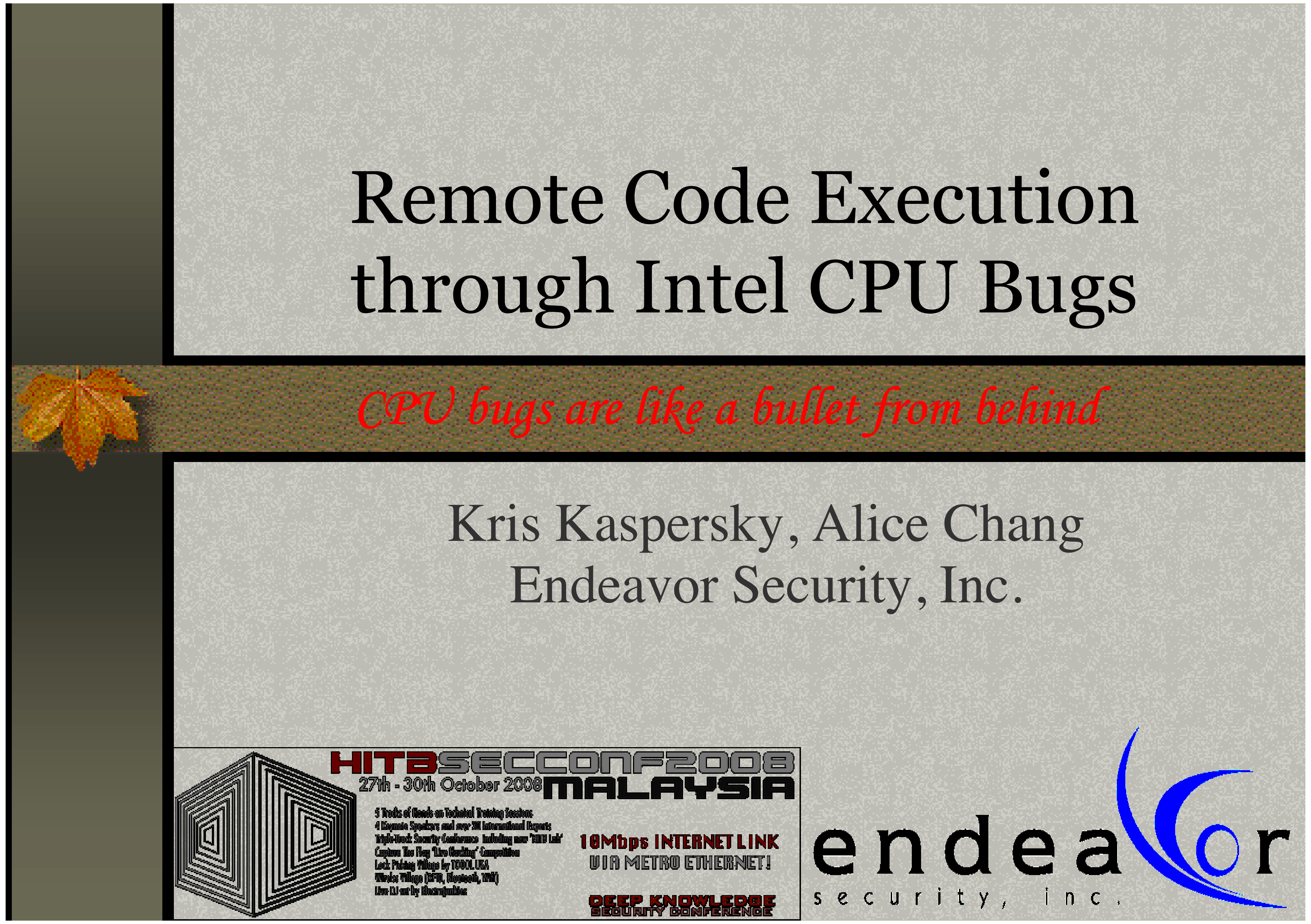
Auditing the code & the compiler isn’t enough.

Kris Kaspersky (1976-2017)

“Fact: malware that uses CPU bugs really does exist;”

"nobody can catch it, since nobody knows how it works or how it looks;"

“not apocalypse, just a new threat;”



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

For example: increasingly complex CPUs reveal previously unrealized security assumptions about CPU architecture. [2018]

Meltdown

Spectre

```
if (x < array1_size)
    y = array2[array1[x] * 4096];
```

Listing 1: Conditional Branch Example

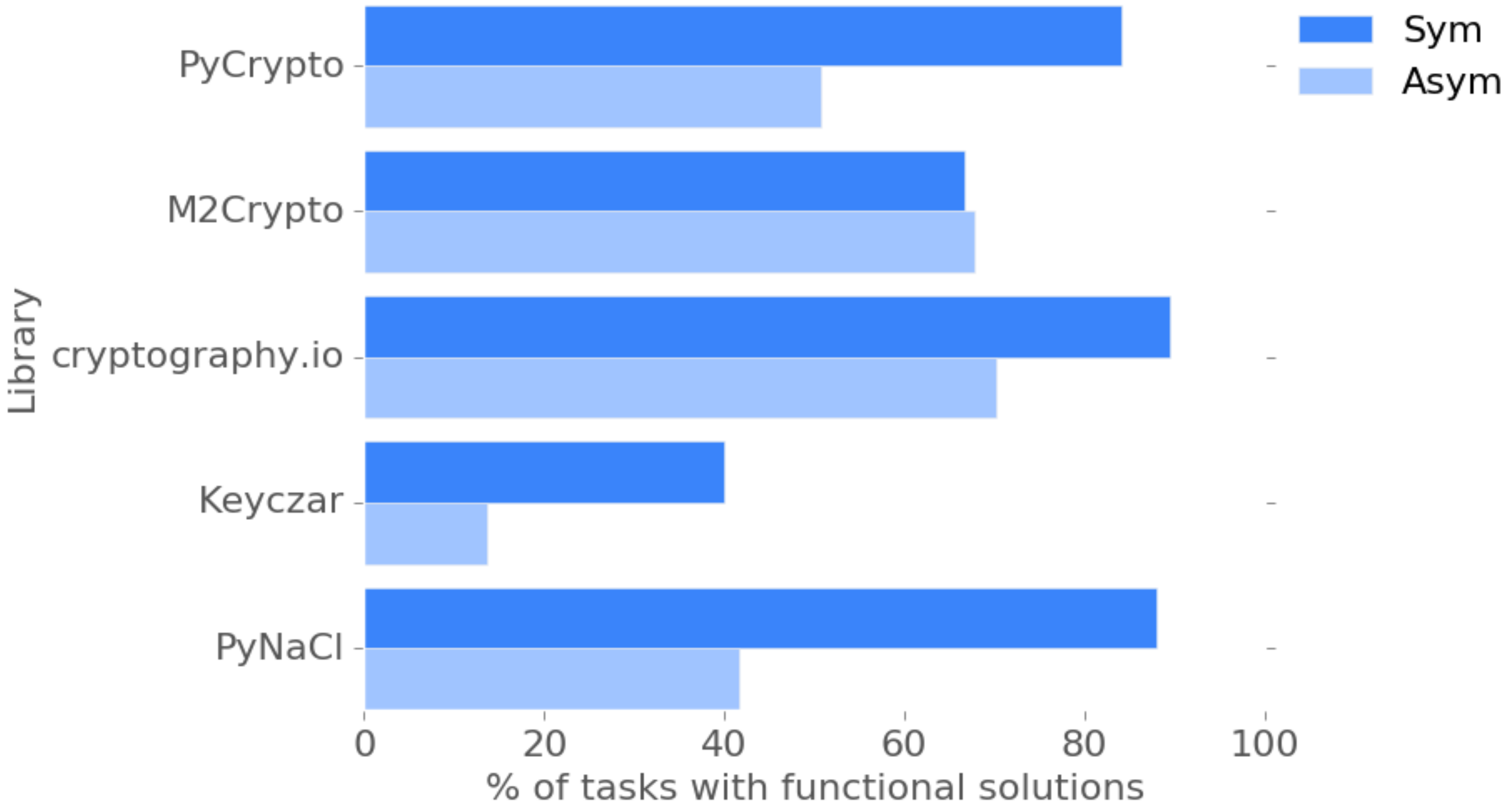
```
if (index < simpleByteArray.length) {
  index = simpleByteArray[index | 0];
  index = (((index * 4096)|0) & (32*1024*1024-1))|0;
  localJunk ^= probeTable[index|0]|0;
}
```

Listing 2: Exploiting Speculative Execution via JavaScript.

These attacks use timing side-channel to bypass memory protection.
Spectre can even be exploited by JavaScript!

Programmers writing security software optimize for functionality, not for security—their tools don't tell them when the code is secure.

We conducted a 256-person, between-subjects online study comparing five Python cryptographic libraries:



In 20% of functionally correct tasks (across libraries), participants believed that their code was secure when it was not

Yasemin Acar (CISPA, Saarland University), Michael Backes (CISPA, Saarland University & MPI-SWS), Sascha Fahl (CISPA, Saarland University), Simson Garfinkel (National Institute of Standards and Technology), Doowon Kim (University of Maryland), Michelle Mazurek (University of Maryland), Christian Stransky (CISPA, Saarland University), Comparing the Usability of Cryptographic APIs, IEEE Security and Privacy 2017, San Jose, CA

Organizations developing cryptographic products face significant challenges. [Haney, Garfinkel, Theofanos 2017]

We surveyed 121 individuals.

78%	Use test vectors
11%	Don't do formal testing, but just look at the data to observe that it's being encrypted
74%	Use crypto standards
6%	Don't use standards
64%	Have problems recruiting talent
40%	Think security professionals are harder to manage
33%	Have challenges finding adequate development tools
93%	Have challenges explaining products to potential customers.

The marketplace does not incentivize cryptographic products that are actually secure!

Table I
PARTICIPANT JOB FUNCTIONS

Job Function Category	n=	%[a]
Managerial (e.g. executive, program or department manager)	17	14%
Cryptographer	11	9%
Developer/Software Engineer	17	14%
Researcher/Educator	9	7%
Security Professional (e.g. security architect, security engineer)	10	8%
Technical - Executive (e.g. CTO, Chief Scientist, Technical Director)	12	10%
Technical - Other (e.g. architect, engineer, certifications)	21	17%
Unknown/not specified	24	20%

[a]Note: percentages do not sum to 100% due to rounding.

Haney, Julie M., Simson L. Garfinkel, Mary F. Theofanos, Organizational Practices in Cryptographic Development and Testing, 2017 IEEE Conference on Communications and Network Security (CNS).

We reviewed 10 years of usable security research [2014]

User Authentication

Email Security and PKI

Anti-Phishing

Storage

Device Pairing

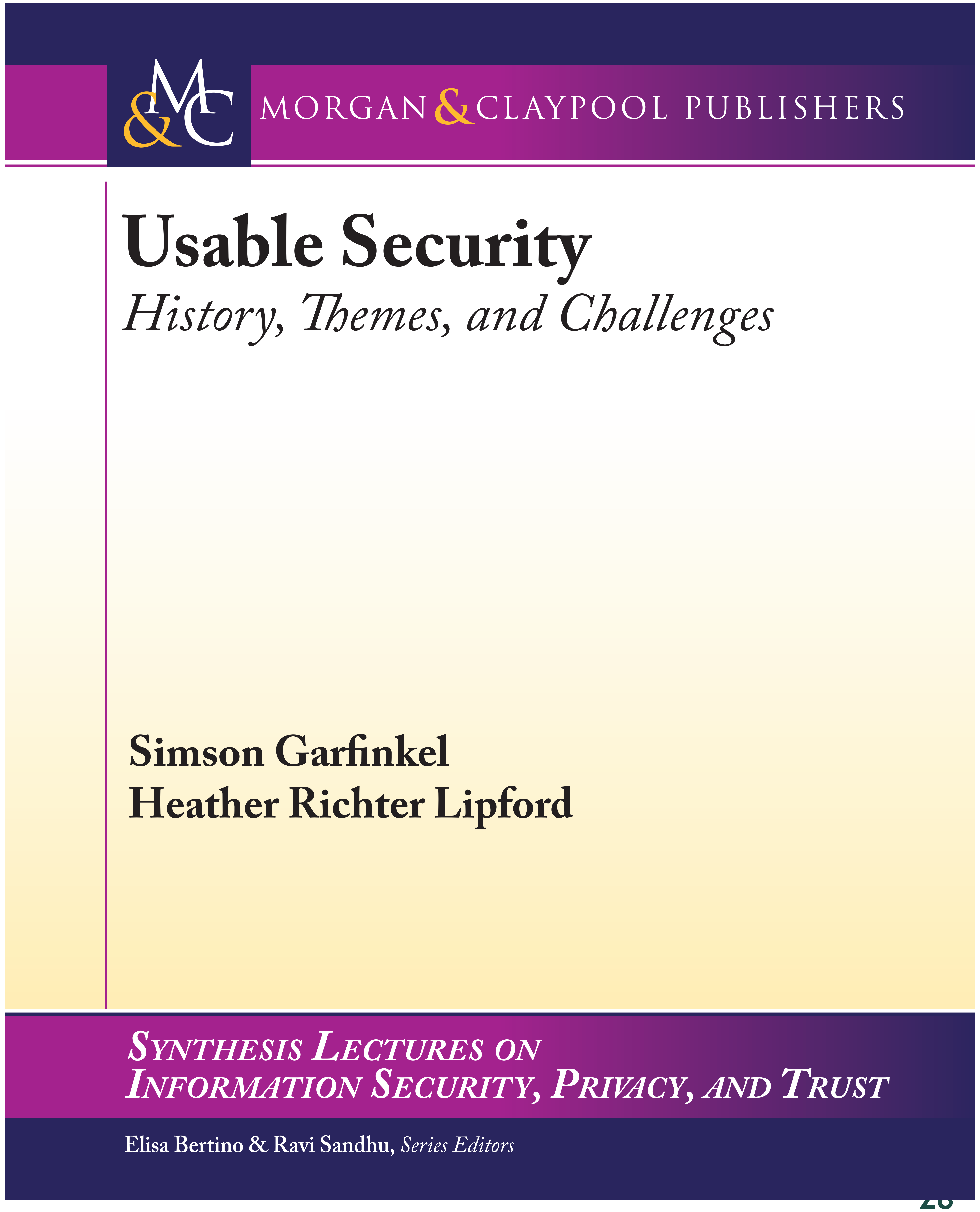
Web Privacy and Information Information Practice

Policy Specification and Interaction

Mobile Security and Privacy

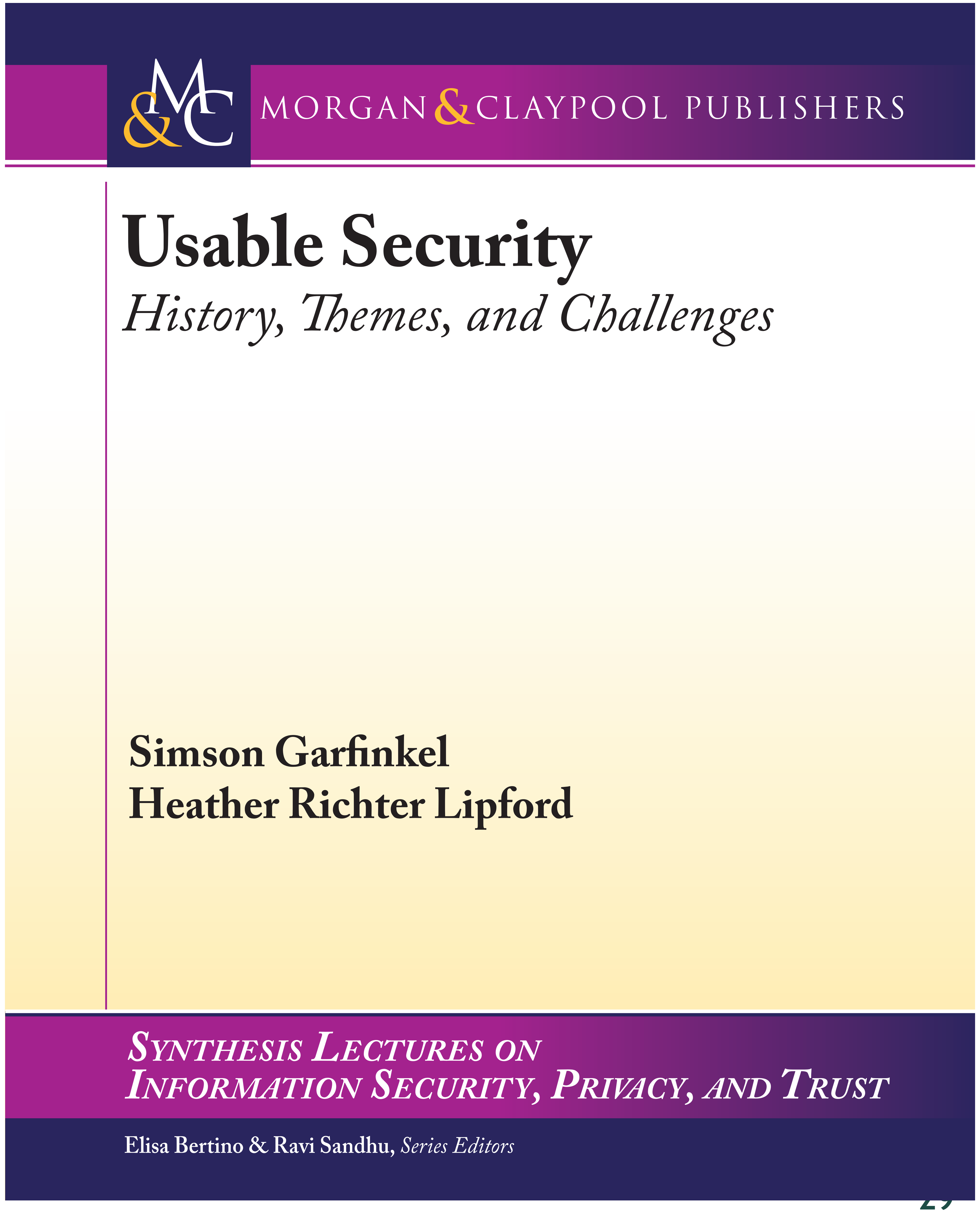
Social Media Privacy

Security Administrators



Key Lessons

1. Reduce Decisions
2. Safe and Secure Defaults
3. Provide Users with Better Information, not More Information
4. Users Require Clear Context to Make Good Decisions
5. Information Presentation is Critical
6. Education Works, But Has Limits



Research Challenges

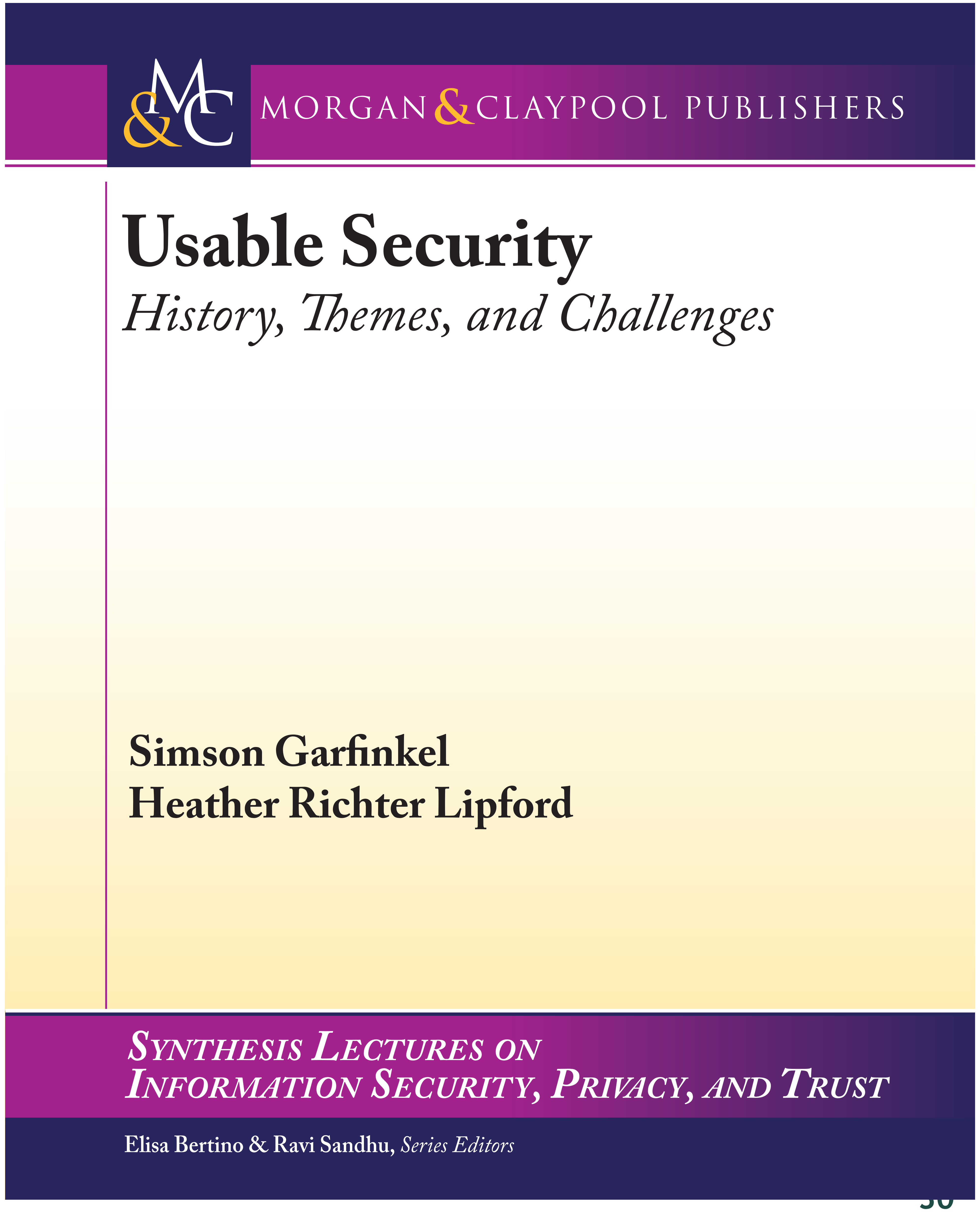
Subject Challenges:

1. Authentication
2. Adversary Modeling
3. Consumer Privacy
4. Social Computing

Domain Challenges:

1. Ecological Validity
2. Teaching

Cybersecurity is too hard for average users, but with research we could change that.



2

Cybersecurity experts make mistakes, too.

New technologies seem secure because nobody has attacked them. Remember Wi-Fi?

1985 - FCC Approves Unlicensed Spread Spectrum

1991 - NCR Corporation starts selling WaveLAN

1999 - Wi-Fi Alliance Created

"Spread Spectrum" technology ... makes the signal both difficult to intercept and less susceptible to interference."
— *The Economist, "A brief history of Wi-Fi", June 10th, 2004*

Today we know that nothing could be further from the truth!

The expert managers of the world's most secure networks can't get cybersecurity right.

Practical systems for multi-factor authentication have been available since 1980s

The US Government mandated them in 2004

DoD's CAC "provides two-factor authentication that's largely immune to social engineering and phishing."

We found:

- 97% of DoD respondents use a CAC to log into at least one work-related system.
- 56% of DoD employees used systems requiring a "character string" password. (Average of 3 accounts accessed frequently, 2 occasionally.)

DoD's success depended on a $30 million allocation by Congress for coordinating activities

Fall 2012 Survey of 28,481 DoD and 4,573 DoC employees

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

 Copublished by the IEEE Computer and Reliability Societies 1540-7993/16/$33.00

IEEE Security & Privacy Magazine
September/October 2016

June 2015: Office of Personnel Management (OPM) Data Breach 19.7 million individuals applying for security clearances

www.opm.gov/cybersecurity/cybersecurity-incidents/

A–Z Index | Contact Us | Forms | FAQs | OPERATING STATUS: OPEN | Search All of OPM...

OPM.GOV

ABOUT POLICY INSURANCE RETIREMENT INVESTIGATIONS AGENCY SERVICES NEWS

CPM.gov Main > Cybersecurity Resource Center > Cybersecurity Incidents

IN THIS SECTION

- Sign Up for Services
- Cybersecurity Incidents
  - What Happened
  - How You May Be Affected
  - What You Can Do
  - What We Are Doing to Help
- Recent Updates
- Frequently Asked Questions
- Stay Informed

PRINT PAGE

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

Display a menu

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

OPM had 0% Strong Authentication deployment in 2013

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

DOD had 89% deployment of two-factor

DOD's experts prioritized two-factor, OPM's didn't. OPM got hacked.

Strong authentication doesn't protect against hostile insiders.

Most cybersecurity approaches are designed to deny access to bad actors

Some of the most devastating publicized cybersecurity incidents were perpetrated by insiders

(Typically only attacks on government systems are publicized.)


Ames


Hanssen


Manning

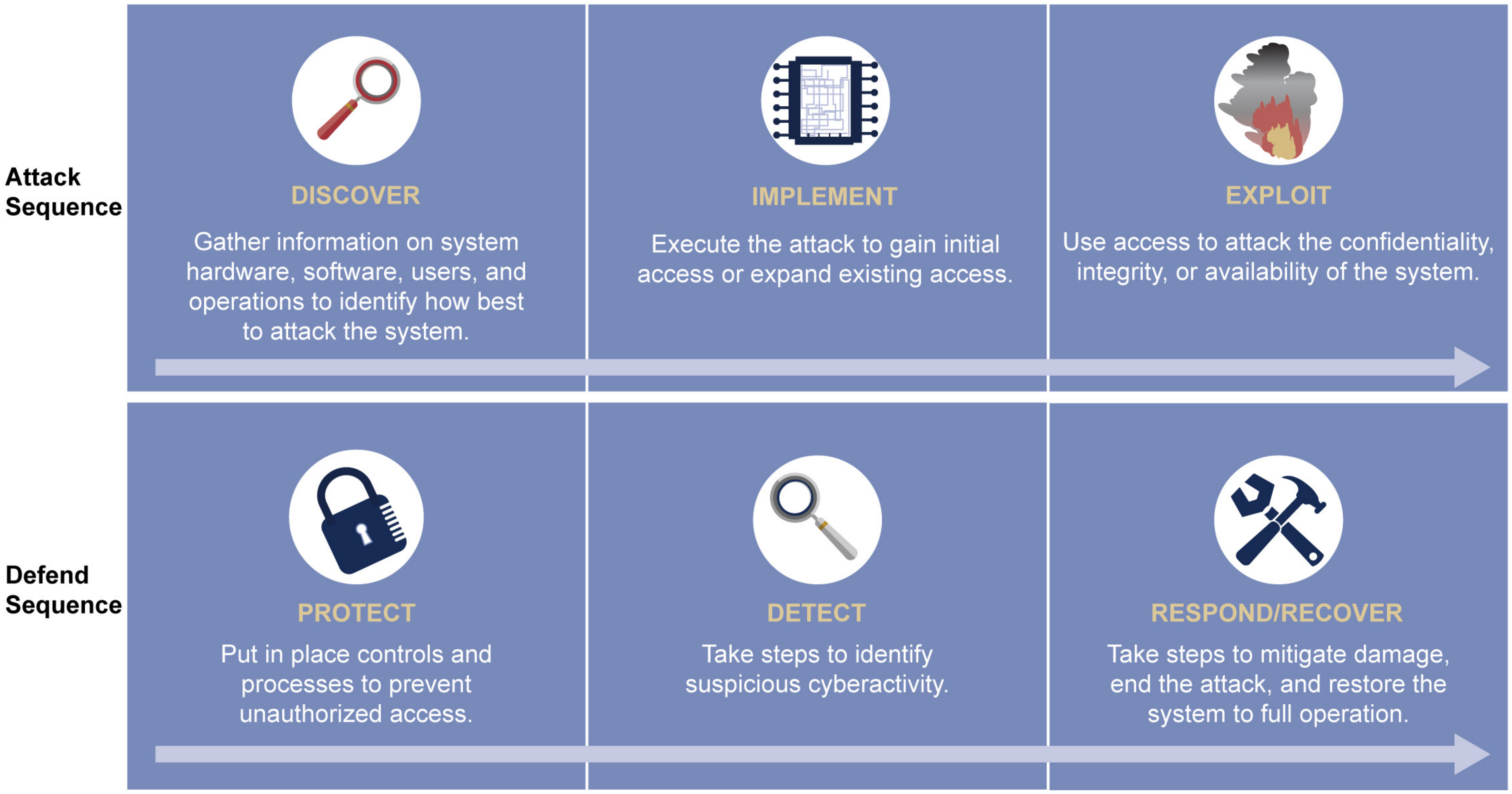

Snowden

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

As Spectre and Meltdown demonstrate, much of today's cybersecurity research is attack research.

The "cyber kill chain" is driven by the quest for new exploits.

Figure 1: Key Activities in Cyber Attacks and Cyber Defense



Source: GAO analysis of Department of Defense information. | GAO-19-128

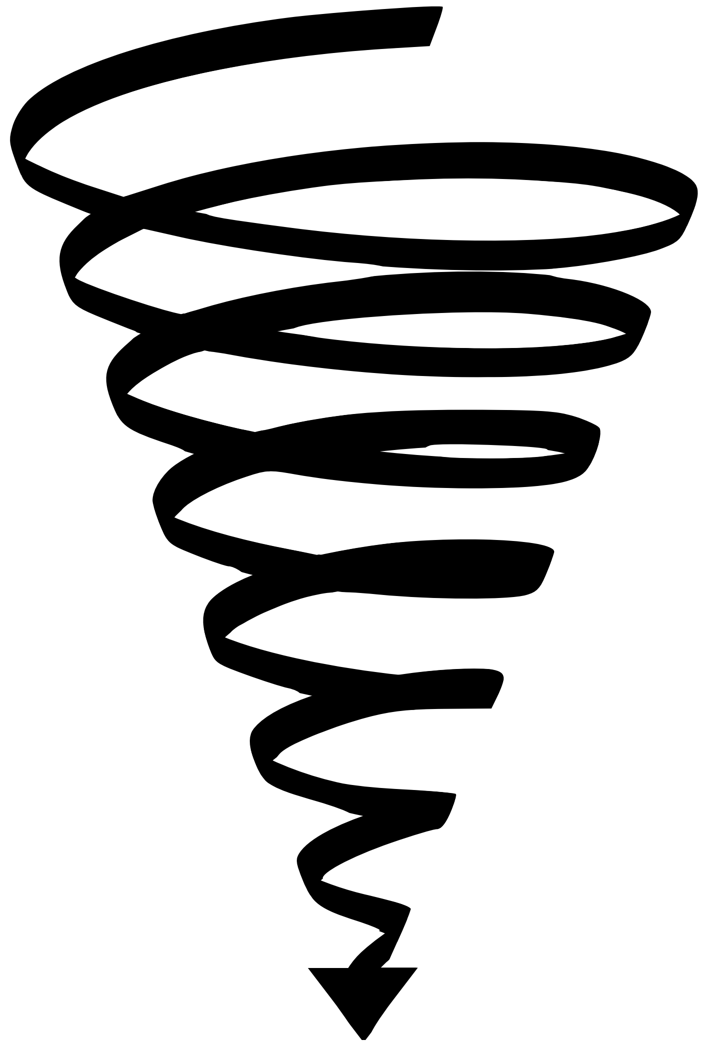
Offensive cybersecurity research changes business "risks" into "issues."

Cybersecurity researchers find new things to attack

Today's computers are incredibly complex:

Data • Encoding • Apps • Architectures • OS • Network & VPNs • DNS (DNSSEC) • IPv4 (IPv6) • Embedded Systems • Human operators • Hiring process • Supply chain • Family members

The more we look, the more vulnerabilities we find



Icon credit
downward spiral,
By Davo Sime, AU

Cybersecurity is a “wicked problem”

Wicked Problems: Rittel and Webber,
“Dilemmas in a General Theory of Planning,” 1973

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

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

Cybersecurity is too hard for both users *and* experts!

Chatham House • Oct. 2011
"Cyber Security as a Wicked Problem"

3

Despite talk, leadership does not value cybersecurity.

October 2018: GAO-19-128

Hot new report!

DOD has been concerned about its information networks for years

DOD has only recently evaluated the security of its weapons systems

GAO has audited what DOD has done.

This report is fascinating reading!

GAO

United States Government Accountability Office

Report to the Committee on Armed Services, U.S. Senate

October 2018

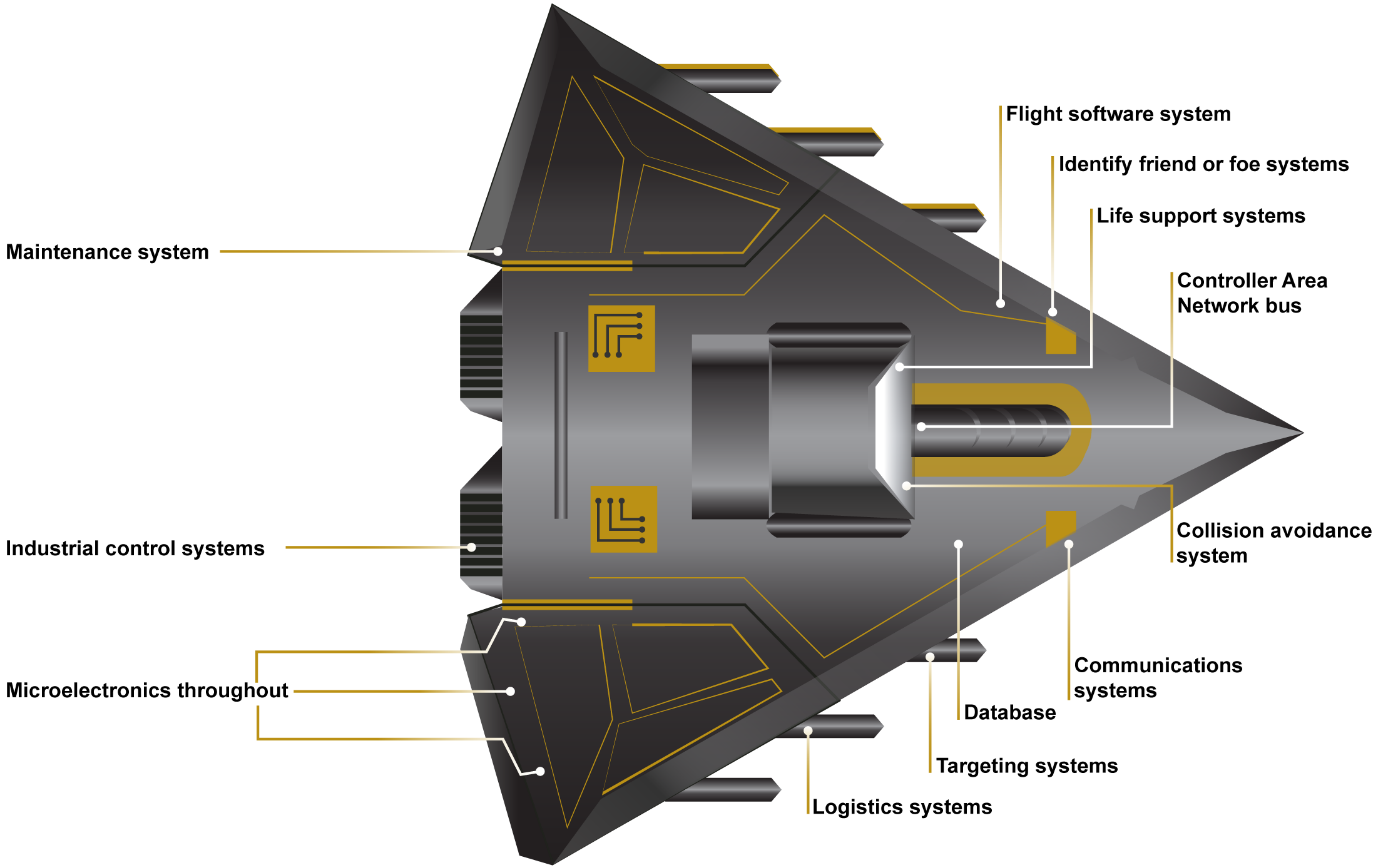
WEAPON SYSTEMS CYBERSECURITY

DOD Just Beginning to Grapple with Scale of Vulnerabilities

GAO-19-128

Today's weapons are cyberphysical systems

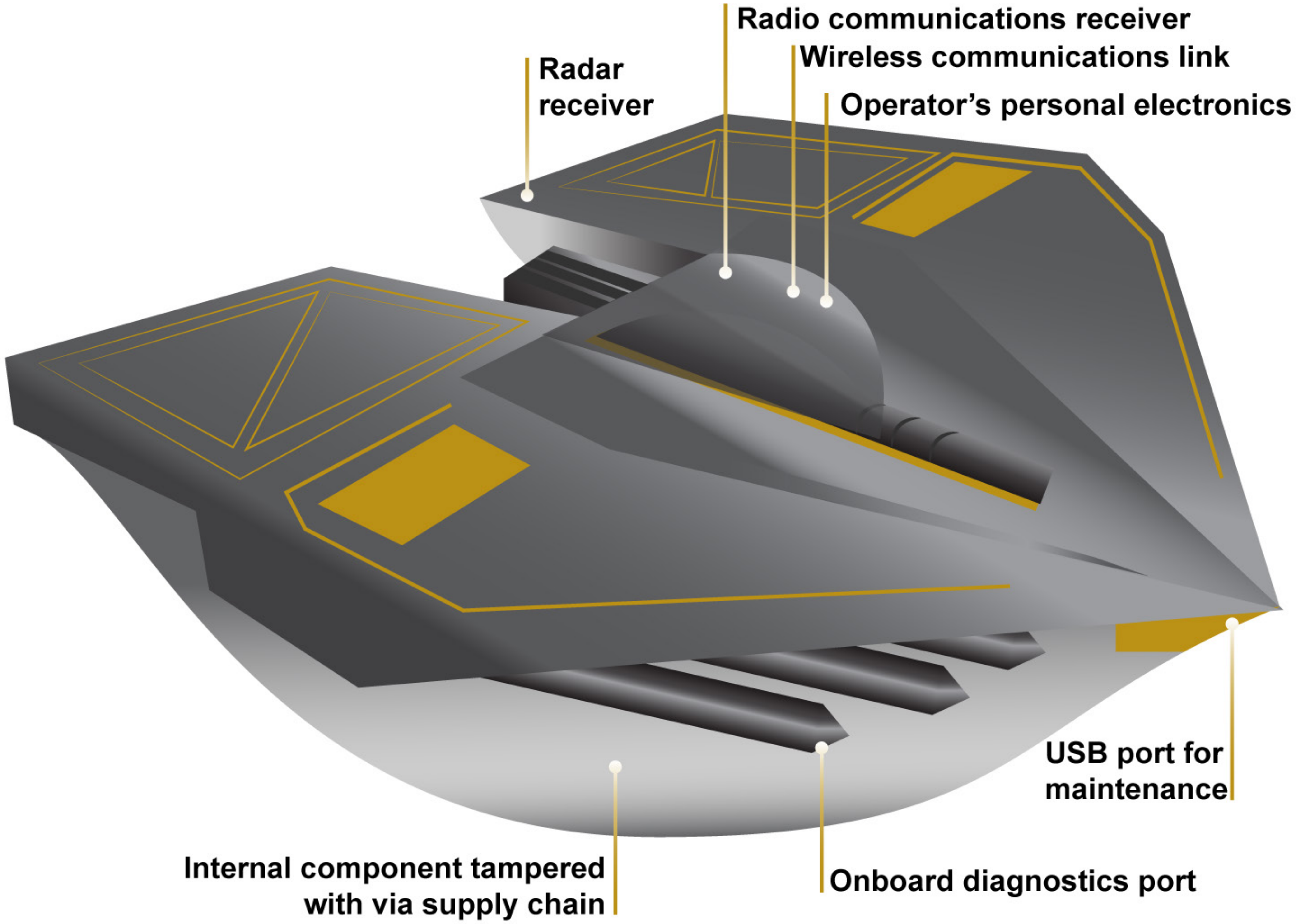
Figure 2: Embedded Software and Information Technology Systems Are Pervasive in Weapon Systems (Represented via Fictitious Weapon System for Classification Reasons)



Source: GAO analysis of Department of Defense information. | GAO-19-128

A fighter is really flying laptop with weapons.

Figure 3: Weapons Include Numerous Interfaces That Can Be Used as Pathways to Access the System (Represented via Fictitious Weapon System for Classification Reasons)



Source: GAO analysis of Department of Defense information. | GAO-19-128

Here's what GAO found.

Officials from one program... said they are supposed to apply patches within 21 days of when they are released, but fully testing a patch can take months due to the complexity of the system." (p. 20)

Here's what GAO found.

We found that from 2012 to 2017, DOD testers routinely found mission-critical cyber vulnerabilities in nearly all weapon systems that were under development.

Using relatively simple tools and techniques, testers were able to take control of these systems and largely operate undetected. In some cases, system operators were unable to effectively respond to the hacks.

Furthermore, DOD does not know the full scale of its weapon system vulnerabilities because, for a number of reasons, tests were limited in scope and sophistication." (p. 25)

DOD's test teams easily took control of weapons systems.

One test team emulated a denial of service attack by rebooting the system, ensuring the system could not carry out its mission for a short period of time. 41 Operators reported that they did not suspect a cyber attack because unexplained crashes were normal for the system." (p. 24)

It wasn't hard.

In one case, it took a two-person test team just one hour to gain initial access to a weapon system and one day to gain full control of the system they were testing." (p. 25)

Leadership literally does not "value" cybersecurity [enough].

"DOD **struggles to hire and retain cybersecurity personnel**, particularly those with weapon systems cybersecurity expertise.

"Our prior work has shown that maintaining a cybersecurity workforce is a challenge government-wide and that this issue has been a high-priority across the government for years.

"Program officials from a majority of the programs and test organizations we met with said they have difficulty hiring and retaining people with the right expertise, due to issues such as a shortage of qualified personnel and private sector competition.

"Test officials said that **once their staff members have gained experience in DOD, they tend to leave for the private sector, where they can command much higher salaries**.

"According to a 2014 RAND study, **personnel at the high end of the capability scale**, who are able to detect the presence of advanced threats, or finding the hidden vulnerabilities in software and systems, **can be compensated above $200,000 to $250,000 a year**, which **greatly exceeds DOD's pay scale**." (p.34)

Underfunding is not a new problem. We narrowly missed World War III because the production system was used for development and testing.

Mitigation:

"A **software development and testing facility was constructed** in Colorado Springs that **allows the development and testing** of all software at an offsite facility **removed from the operational missile warning system** in the Cheyenne Mountain Complex.

"This should prevent errors such as that of November 9, 1979, **when test data was inadvertently injected into the operational mission warning system**." (p. ii)

RESTRICTED — Not to be released outside the General Accounting Office except on the basis of specific approval by the Office of Congressional Relations.

115265

BY THE COMPTROLLER GENERAL

Report To The Chairman

Committee On Government Operations

House Of Representatives

OF THE UNITED STATES

RELEASED

NORAD's Missile Warning System: What Went Wrong?

The importance and criticality of the North American Air Defense Command's (NORAD's) computer system have recently been emphasized when false missile warning messages were generated and the Nation's nuclear retaliatory forces alerted.

The Air Force began a computer upgrade program for NORAD computers in 1968 which is expected to reach initial operational capability in November 1981. Due to poor management causing program delays and the attempt to adapt inadequate computers to the NORAD mission, the system falls short of meeting the requirements of the growing missile warning mission.

NORAD will replace these computers by the late 1980s, but it needs to do more to improve management and warning capability.

115265

UNITED STATES GENERAL ACCOUNTING OFFICE

Has Form 46

MASAD-81-30
MAY 15, 1981

516922

1983

WarGames

Lawrence Lasker, Walter F. Parkes, John Badham

After seeing the movie, President Ronald Reagan asked the chairman of the Joint Chiefs of Staff it it was really possible to break into sensitive US government computers.

"Mr. President, the problem is much worse than you think."

Cybersecurity 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.

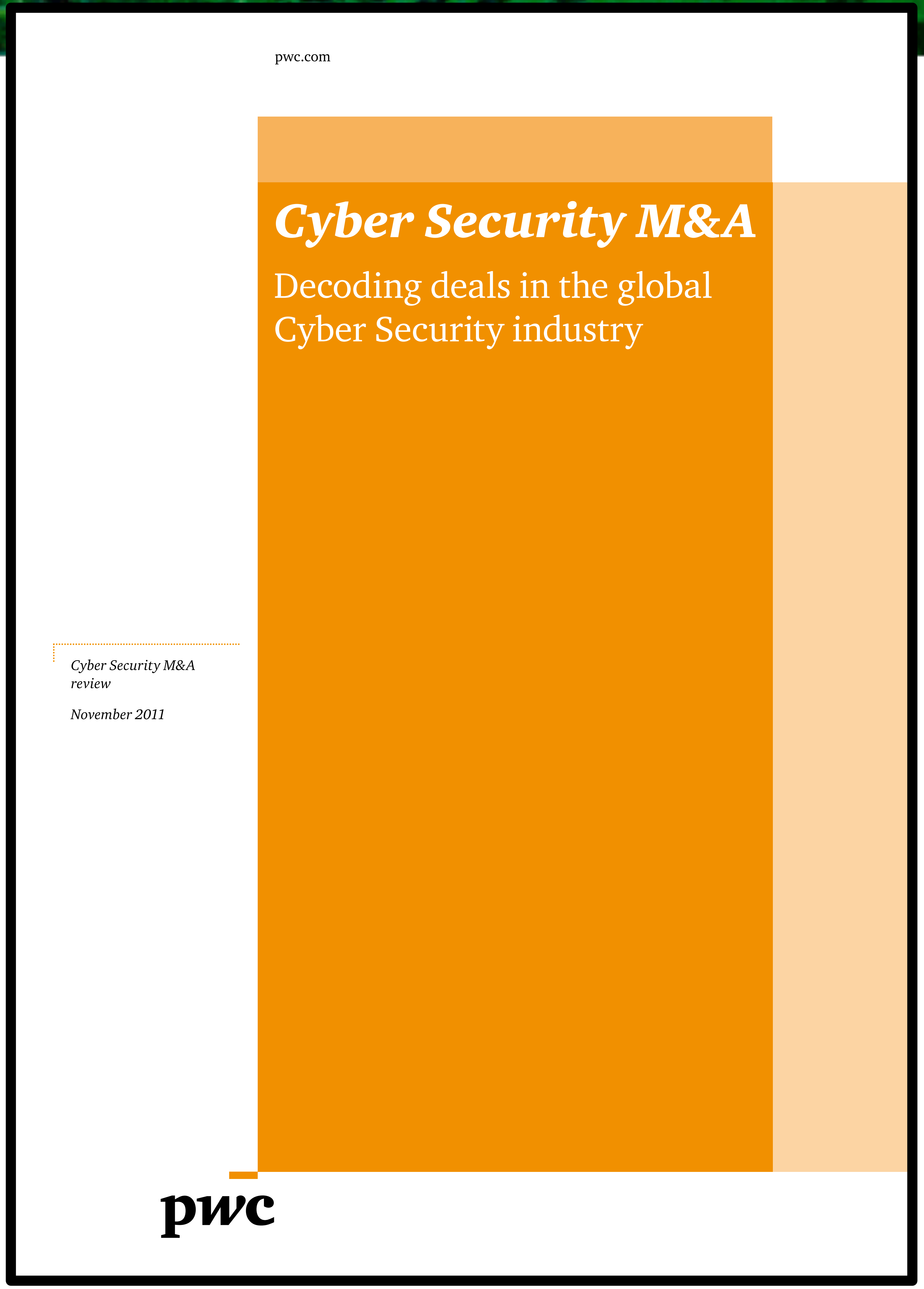
If they raise spending...

$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

Cybersecurity expenditures continue to rise.

$73.7 billion in 2016

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

$1 trillion spent globally from 2015 to 2021

$200B/year!

Source: Cybersecurity Ventures, http://cybersecurityventures.com/

Is money spent on
cybersecurity
an investment or a cost?

Cybersecurity researchers want money spent on cybersecurity to be an *investment.*

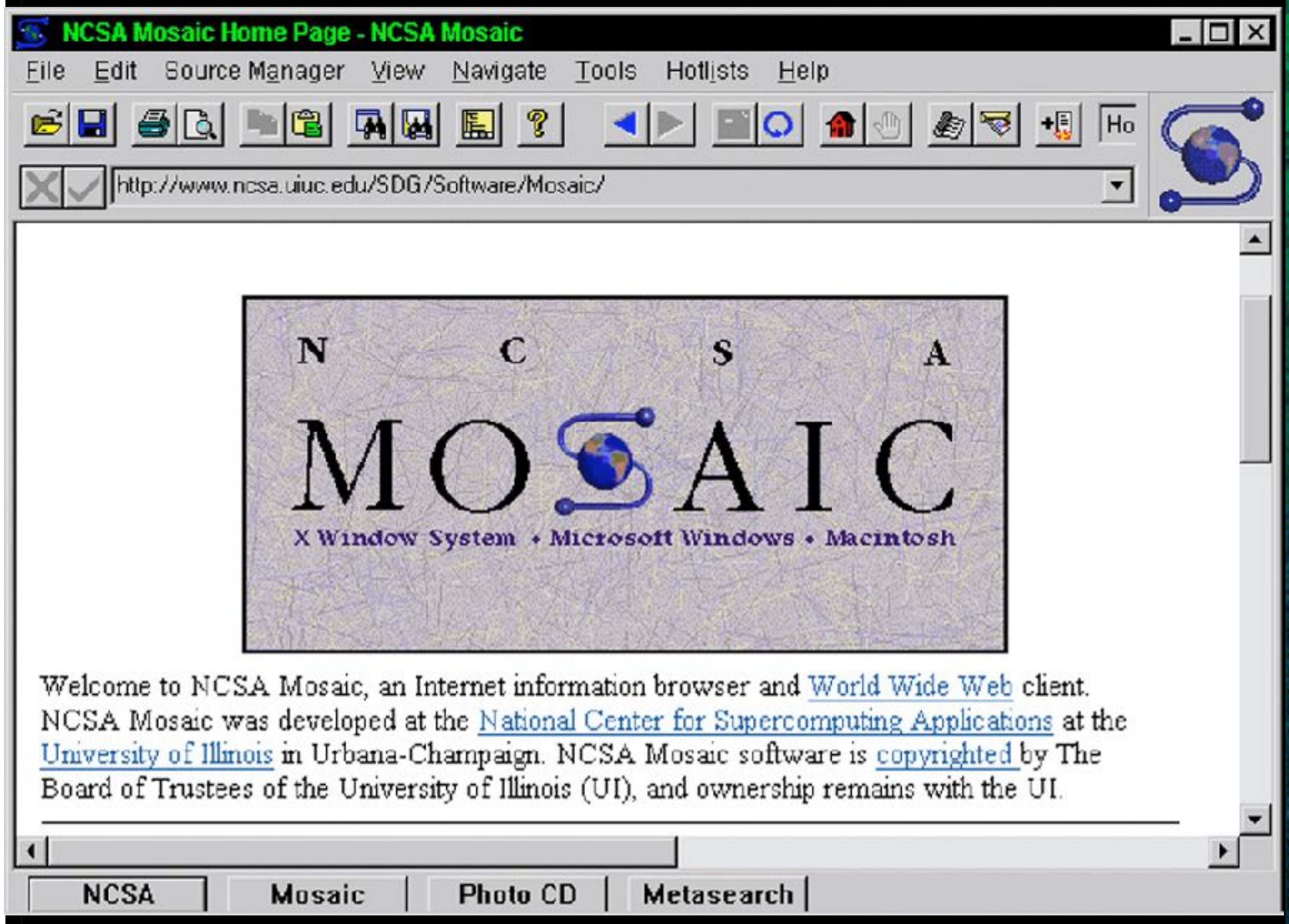
1992

Mass-Marked Web Browser

Marc Andressen, Eric Bina

No security.

"Experts" said not to send credit cards over the Web.



1995

E-Commerce

- — Netscape SSL (1994)
- — Verisign®
- — NSFNET commercial traffic
- — Network Solutions charges for domain names
- — eBay
- — Amazon
- — DoubleClick®

Cybersecurity experts told American business that encryption and good security were necessary to let them use the Internet.... We were wrong.

Consider Paypal — send money by email.

Established December 1998 — No email encryption!

IPO 2002 — valuation $847 million

Acquired by eBay in July 2002 — $1.5 billion

2018 revenue: $13 billion

2018 income: $2 billion

Companies that prioritize cybersecurity:

- Are late to market and miss market opportunities.
- Miss sales that could fund security patches.
- They are not the market winners.

Spending money on cybersecurity does not prevent incidents. Companies are rarely penalized for cybersecurity problems.

Yahoo breach:
2013-2014: 3 billion accounts, revealed Sept. 2016

eBay breach:
May 2014: 145 million users,

Equifax breach:
July 2017: 143 million consumers

The three largest breaches in history.

∴ Cybersecurity appears to be a cost that is best minimized or avoided.

	Unlucky	**Lucky**
Good Cybersecurity	Company is attacked. Attack is repulsed. High cost.	Company is not attacked. Cybersecurity is wasted. CISO gets budget cut.
Poor Cybersecurity	Company is attacked. Company suffers lost. Company recovers.	Company is not attacked. Low cost = higher profits. "Simson's Magic Quadrant"

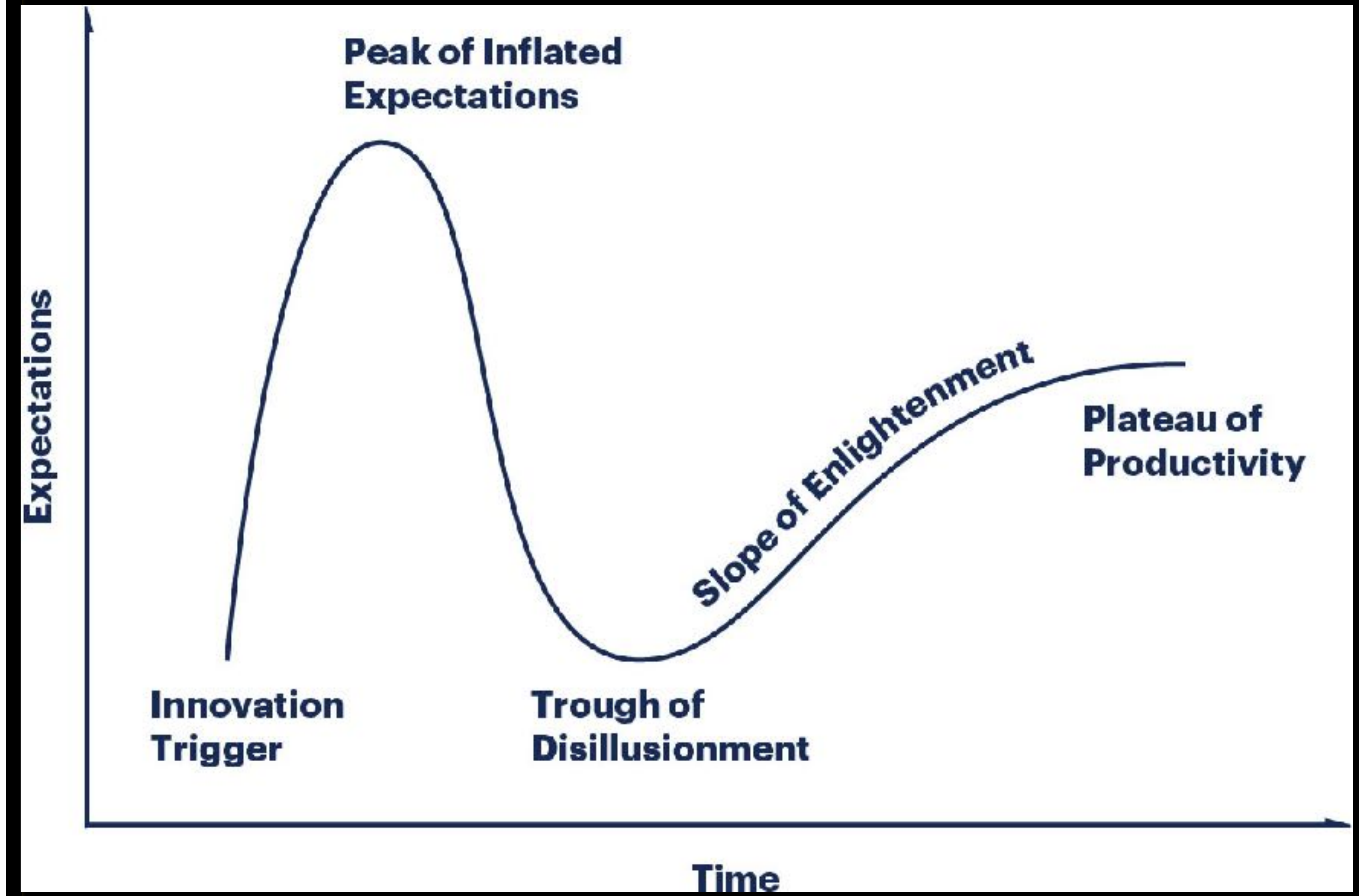
Micro-economics analysis from the point of view of the surviving companies.

1995

Gartner Hype Cycle

The Hype Cycle applies to information technology.

Cybersecurity never reaches the Plateau of Productivity because the environment keeps changing.



Leadership is not economically accountable for valuing cybersecurity, so leadership doesn't.

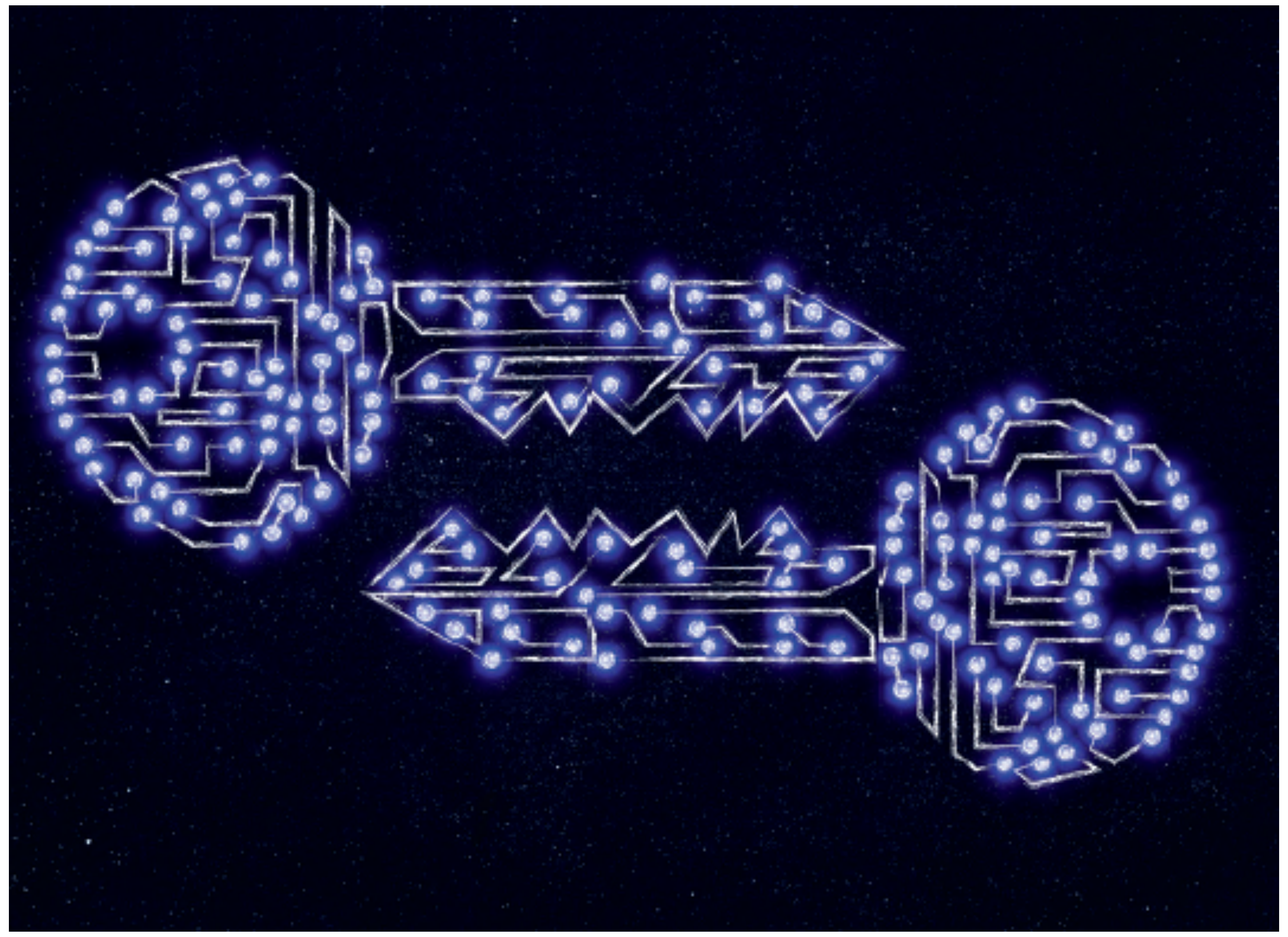
4

Research is needed on how to transition research

Cybersecurity research has made major advances in the past 30 years.

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)
- BAN logic
- Fuzzing



Most of these breakthroughs are crypto & theory

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

We have been less successful deploying applied cybersecurity research.

Sandboxing (Java, C# and virtualization)

- Not very successful on desktop
- Highly successful on mobile — it was the only choice in the new OS
- Highly successful in cloud — it was the only choice at AWS

Firewalls

- Highly successful in regulated environments
- Mostly successful in small markets but only when incorporated into access devices

Network Monitoring

- Hard to get statistics on this.
- Many organizations seem to monitor, but it's not clear if they look at their logs.

Removing user choice has been a powerful tool for improving security.

Browser vendors (Google, Firefox, etc.) are increasingly forcing good cybersecurity practices:

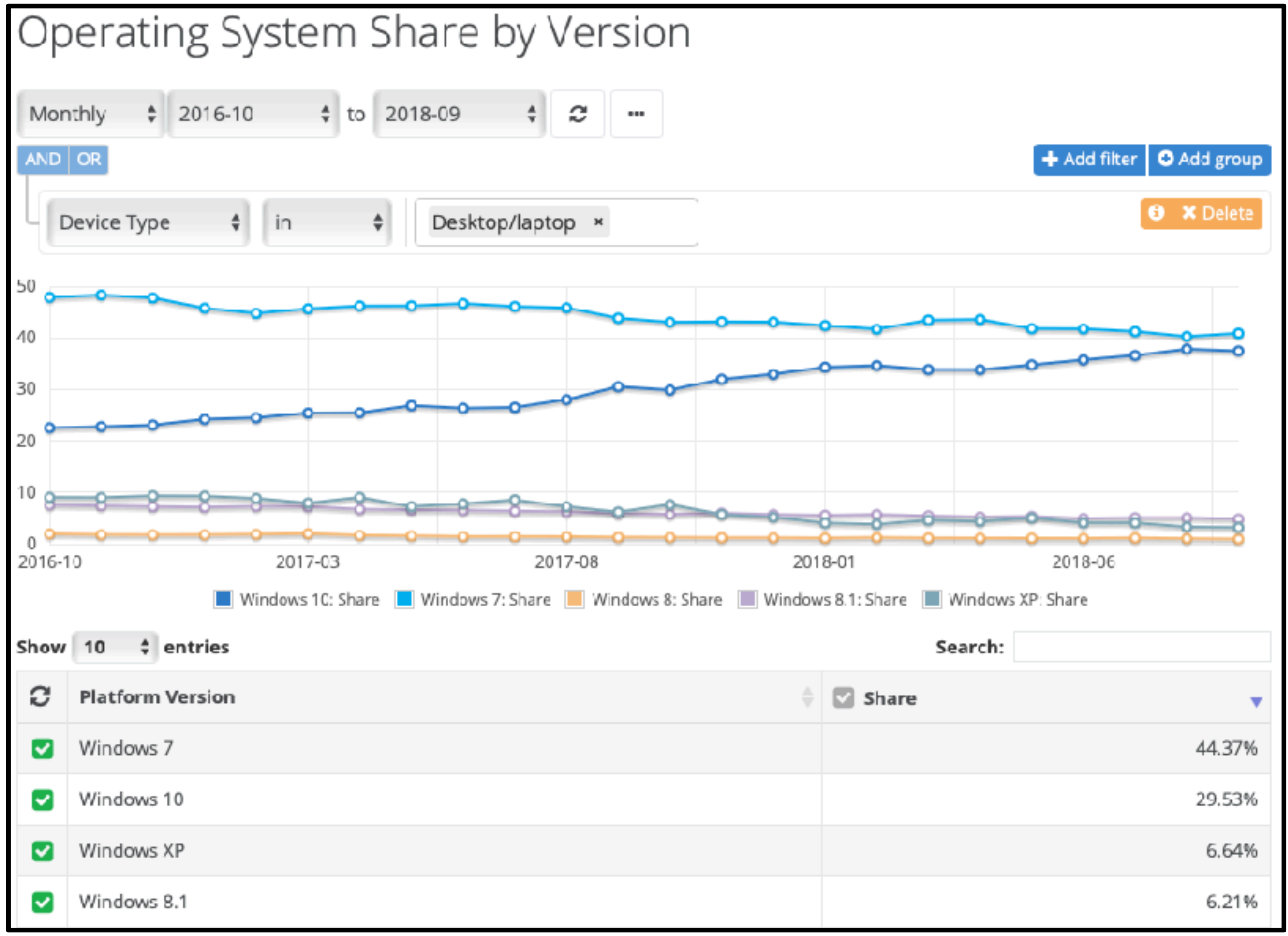
- HTTPS everywhere
- Elimination of SSL 3.0, TLS 1.0, etc.

Microsoft's elimination of support for Windows XP has been less successful.

- In the past 2 years, market share of Windows XP has dropped from 9% to 6.6%
- Support was ended in 2014!
- Microsoft gives users choice!
- 6.6% of users chose to be not secure.

DNSSEC appears dead in the water.

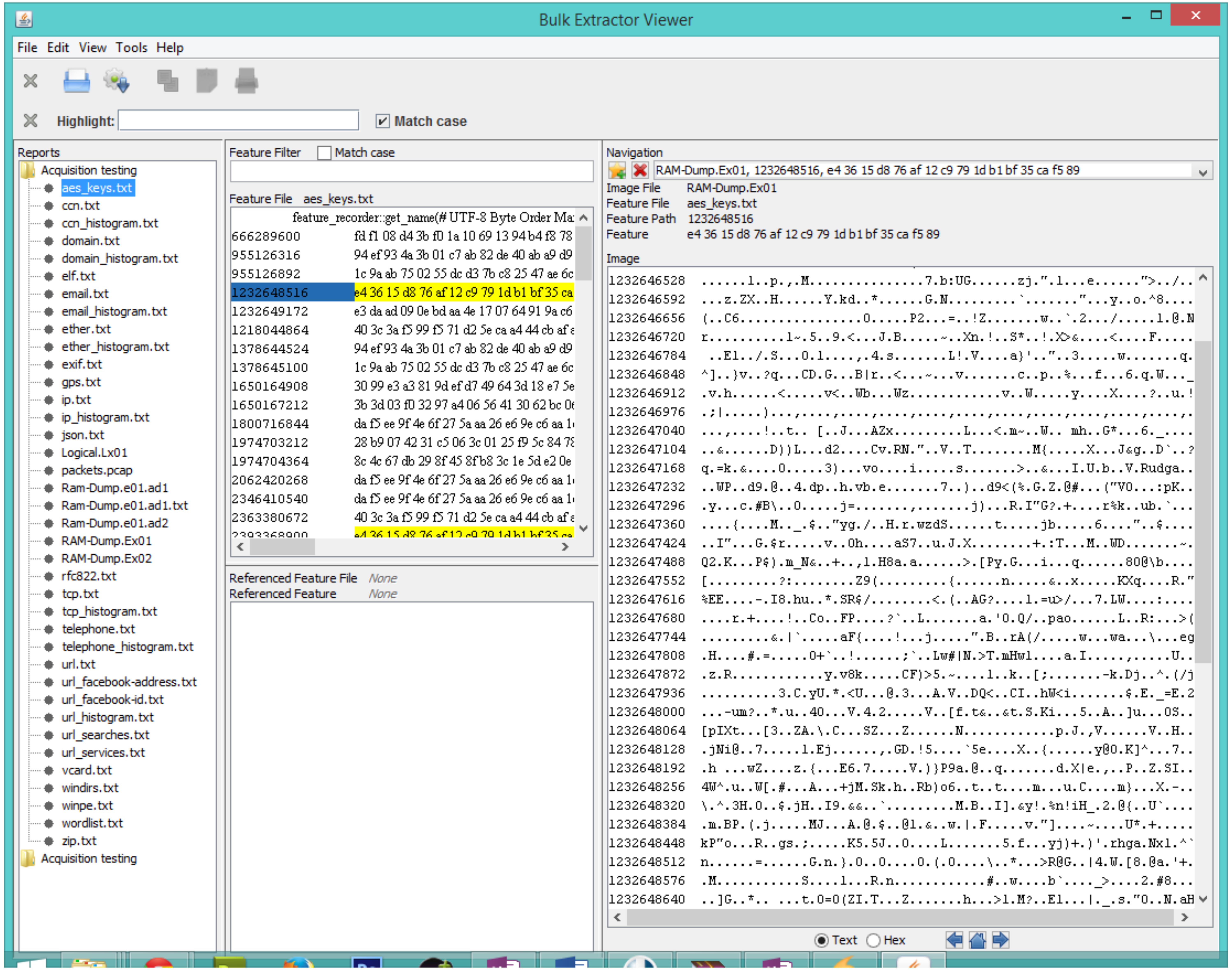
- Users want to go to websites when DNSSEC is misconfigured.
- There is no match in incentives.



http://netmarketshare.com/

Bulk_Extractor Digital Forensics Tool 2006-2014

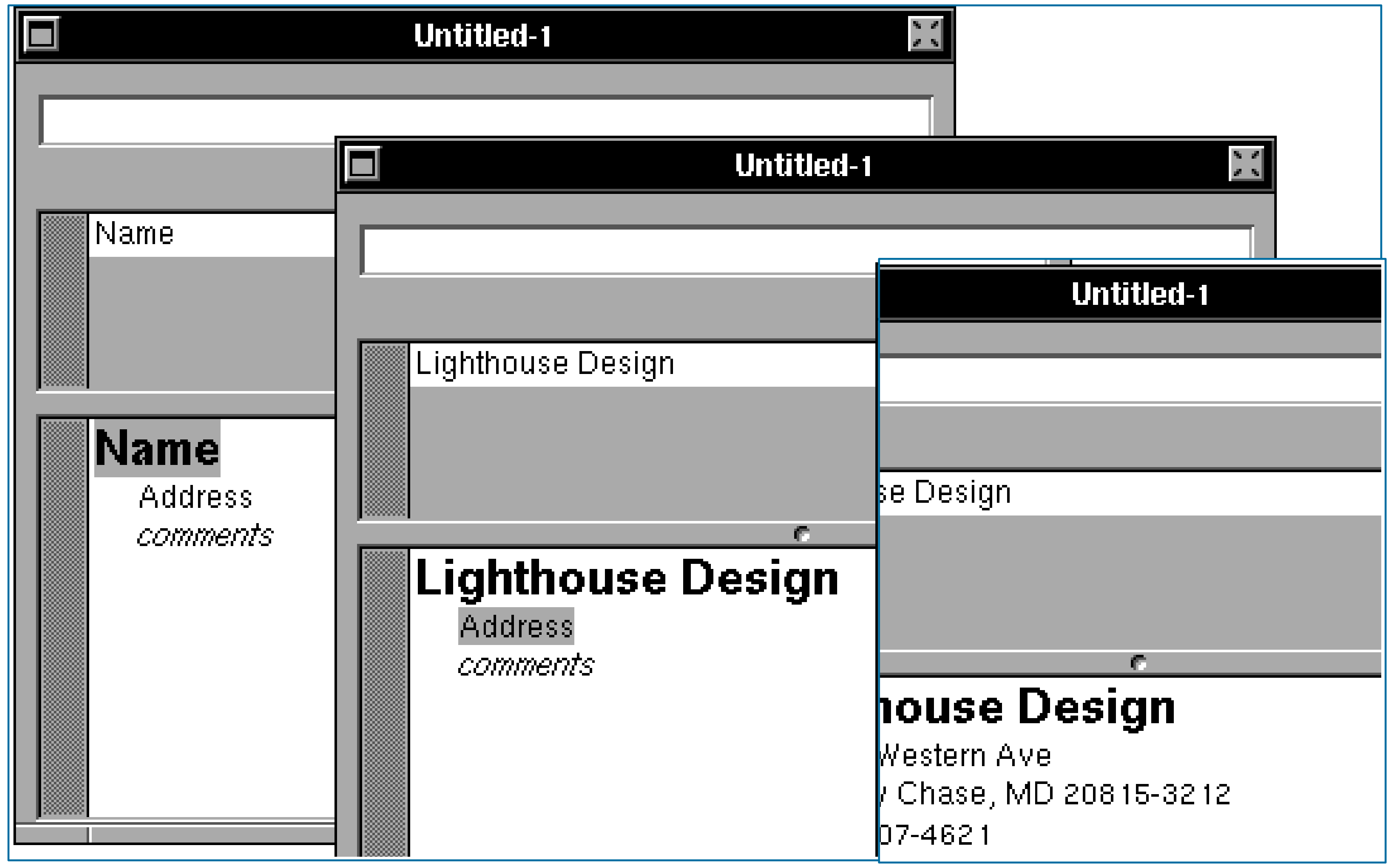
Based on cybersecurity research at:
MIT 1989-1990
MIT 2002-2005
Harvard CRCS 2005-2006
NPS 2006-2014



A brief history of bulk_extractor

1989 — Named Entity Recognizer (NER) developed at MIT Media Lab

1991 — Transitioned to free-format address book for NeXT computers.



2003 — Used technology to find email addresses, phone numbers and other information on hard drives that I had purchased *without first recovering the files.*

We purchased 3000 used hard drives, memory sticks, digital cameras and cell phones between 1998 and 2010 for their data.

Center for Research on Computation and Society
Harvard School of Engineering and Applied Sciences, 2006
≈ 600 hard drives

In 2009, I was at the Naval Postgraduate School.
I had a vision for using the data analysis tool for threat correlation.

Most of this data is analyzed using trained personnel and off-the-shelf software.

DOMEX in Iraq

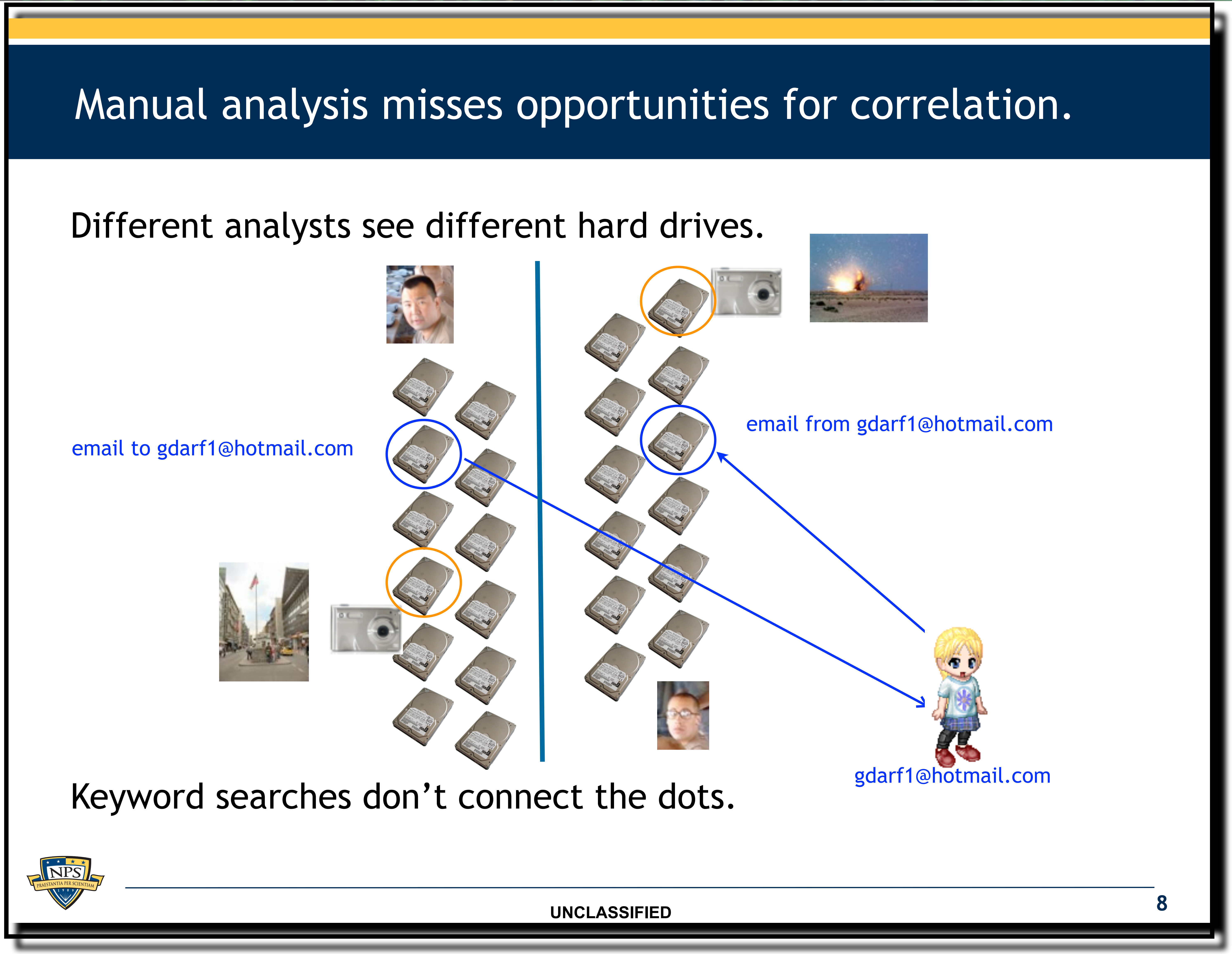
NPS PRAESTANTIA PER SCIENTIAM

UNCLASSIFIED

6

Actual slide from a presentation I used trying to raise money from a sponsor.

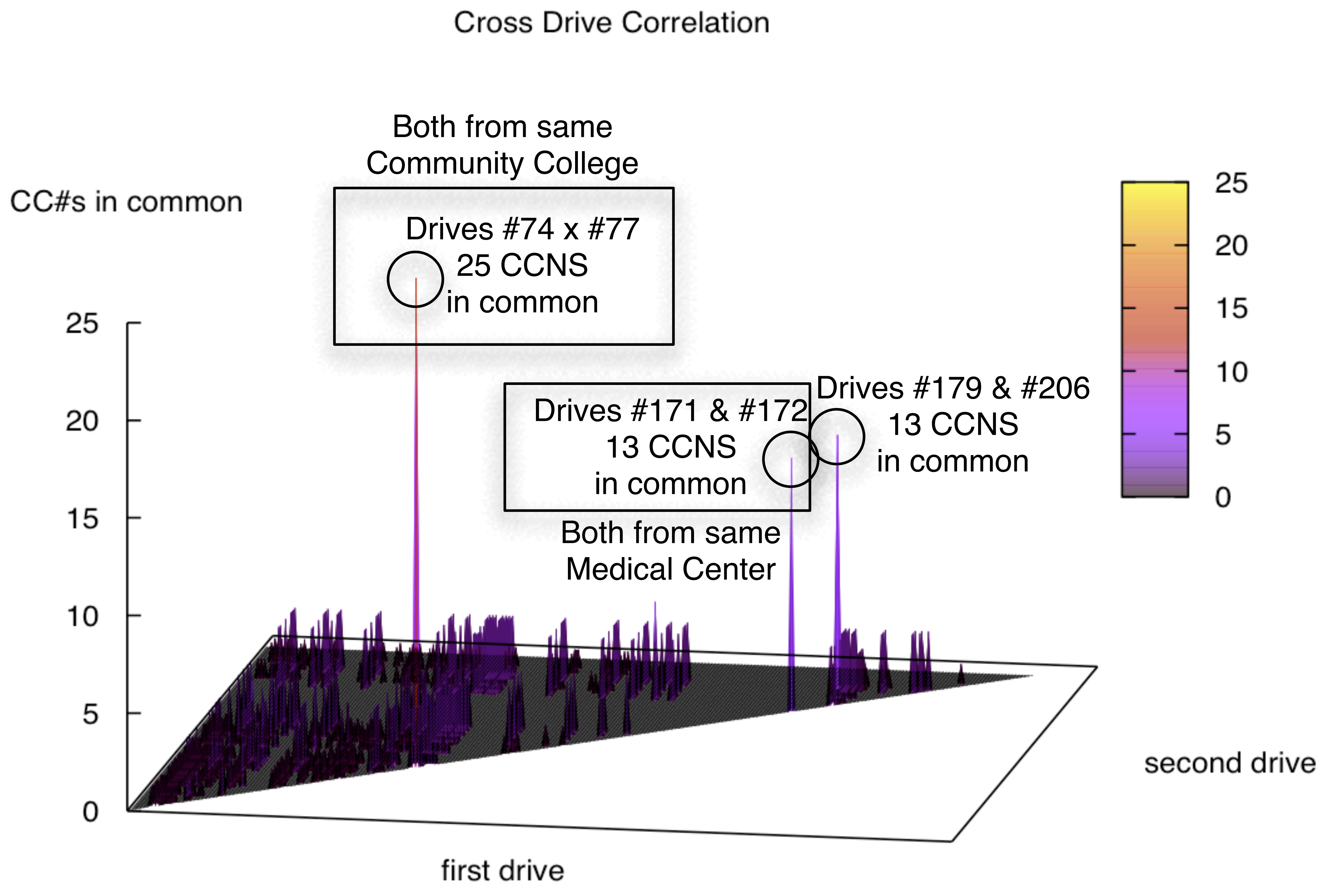
My vision was to automatically correlate information discovered on different drives.



Actual slide from a presentation I used to raise money from a sponsor.

I knew this would work, because I had done it during my postdoc at Harvard three years before!

Manual analysis of on-drive data reveals that these drives are from the same organization.



66

Actual slide from a presentation from my 2006 job talk.

Cross-drive correlation was *too sophisticated* for my intended users.

The customer didn't want some fancy new cyber approach.

The customer just wanted to get email addresses and phone numbers off the hard drives.

We were prepared. Between 2005 and 2008, we interviewed law enforcement regarding their use of forensic tools.

Law enforcement officers wanted a *highly automated* tool for finding:

- Email addresses
- Credit card numbers (including track 2 information)
- Search terms (extracted from URLs)
- Phone numbers
- GPS coordinates
- EXIF information from JPEGs
- All words that were present on the disk (for password cracking)

The tool had to:

- Run on Windows, Linux, and Mac-based systems
- Run with *no* user interaction
- Operate on every kind of evidence file they might have.
- Automatically extract features from compressed data such as gzip-compressed HTTP
- Run at maximum I/O speed of physical drive
- **Never crash**

Moving the technology from the lab to the field was challenging.

The tool had to:

- plug-in to existing processes (technical, managerial)
- require no training to get immediate results.
- run on limited hardware.
- run faster when run on a faster, more expensive hardware.
- produce text files *and* have a graphical user interface.

We learned that:

- If a tool doesn't work, we would not be given a chance to fix it.
- Users frequently coudln't provide data when a program crashed.
- Users are not engineers or programmers.

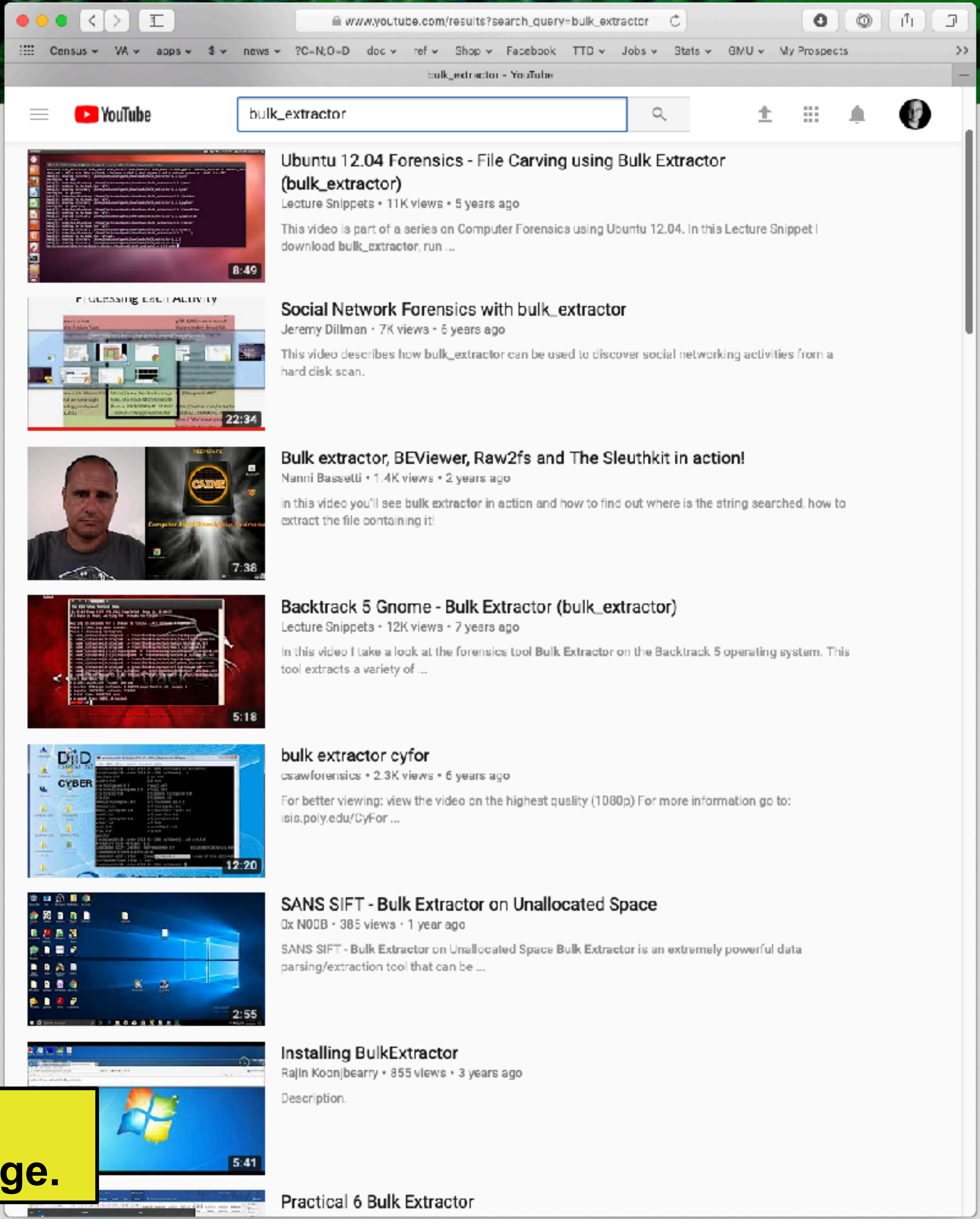
We were highly successful.

bulk_extractor is used in research and law enforcement operations.

bulk_extractor is packaged with many open source digital forensics distributions.

Over 960 Internet videos specifically mention bulk_extractor (mostly tutorials).

3 master's theses
3 journal articles
11 conference papers



This project was successful because it is cheap for organizations to adopt bulk_extractor and the ROI is huge.

Lessons from bulk_extractor

Importance of product engineering

Not an accident that the tool *precisely matched* the requirements of the users

Tool economics are incredibly important

Bulk_Extractor is a force multiplier for its users

Like many cybersecurity tools, it became *more expensive maintain over time*

Economics of cybersecurity tools depends on constantly expanding the user base

Technology Impedance

The sophistication of the technology must match the sophistication of the users

We developed a lot of clever technology that we could never deploy

Good news:
DHS has prioritized funding of cybersecurity economics issues.

DHS announces new research and technology guides

By Andrew Wagner | Published Thursday, March 22, 2018

A A A

__Douglas Maughan__, director of the Cyber Security Division at the DHS Science and Technology Directorate, discusses guides that his agency put out to promote cybersecurity development, and how they are looking to the private sector to put their tech solutions on the market.

The Department of Homeland Security's Science and Technology Directorate has released two new guides to the public. The 2018 Cyber Security Division Portfolio Guide aims to drive industry adoption of DHS cybersecurity solutions, and the 2018 Cyber Security Division Technology Guide hopes to spur a conversation about the agency's research and development agenda.

Cyber Risk Economics Capability Gaps Research Strategy

2018

Homeland Security
Science and Technology

Conclusion: Cybersecurity is not making us more secure because that's not where the incentives are.

We didn't set out to create a tool that was more reliable. We were told to create a tool that *never crashed*.

Few if any cybersecurity researchers are being incentivized to create systems that are "unhackable."

- Users want systems that are unhackable. We don't even have a definition.

Many researchers are focused on attacking or defending existing systems.

- Malware • Access controls • Authentication • Supply chain

Non-technical issues are equally important

- Education • career paths • salaries
- Economic incentives • Regulation

[Not discussed in this talk]
I'm hopeful about:

- Increasing use of formal methods.
- Clean-Slate approaches (e.g. DARPA CRASH).
- iOS, Android, and Chromebooks show that this a workable approach.
- Regulation — it's coming.

Contact Information:
Simson Garfinkel
simsong@acm.org