

the hard thing

(about the hard things)



what with the stupid title?



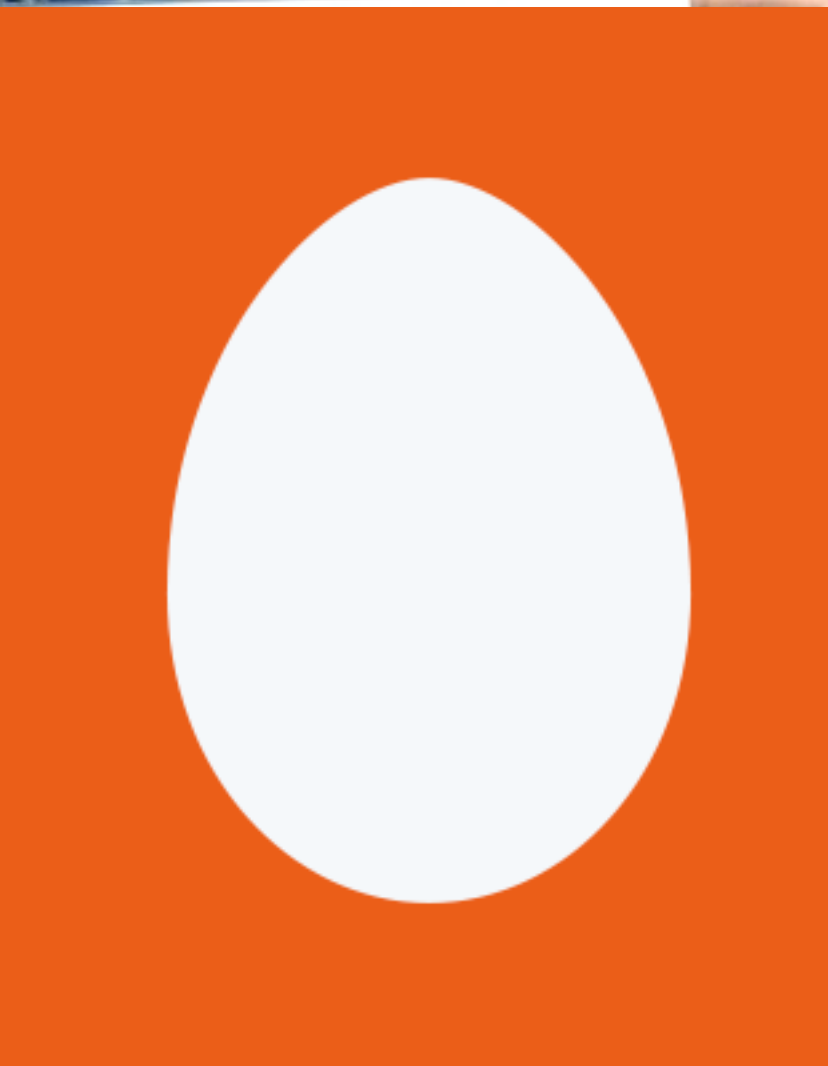
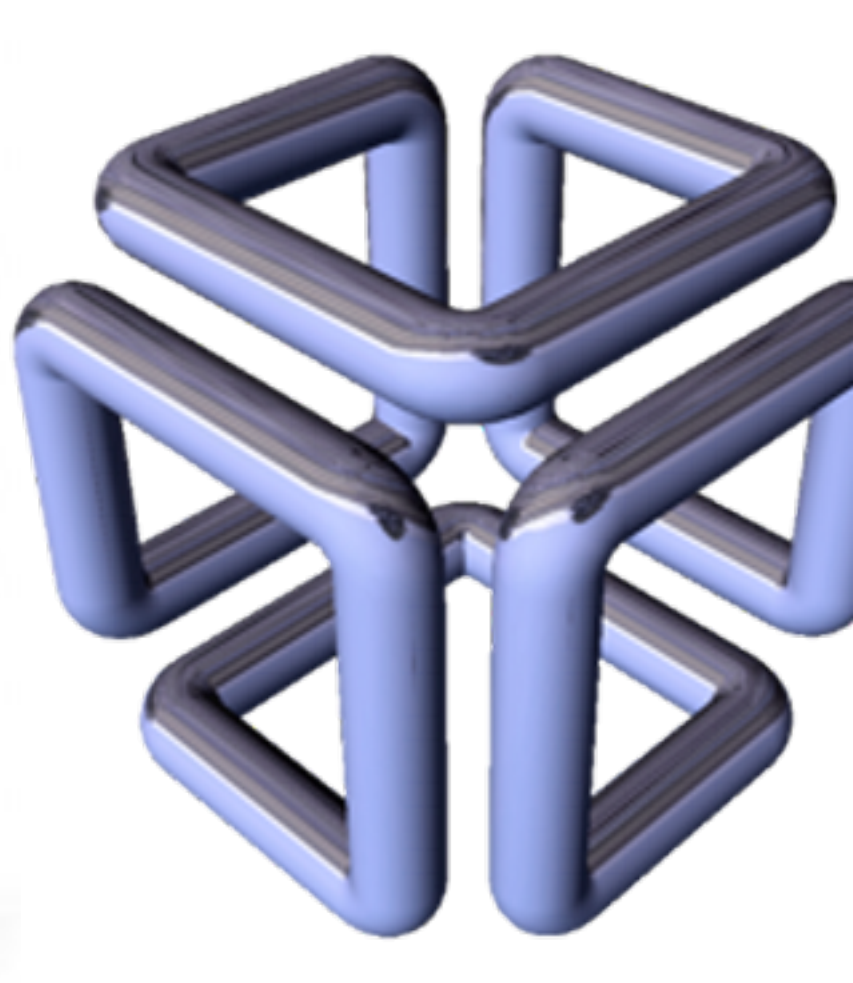
What do startups and Security
have in common ?



"I couldn't sleep, I had cold sweats, I threw up, and I cried"



the plan for this talk





Lets go back..

<http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html>



20 years ago:
Management don't buy in!!



<http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html>



<http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html>



<http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html>

“But one of the often unspoken truths of security is that large areas of it are currently unsolved problems. We don't know how to write large applications securely yet. We don't know how to secure entire organizations with reasonable cost effective measures yet.”

“The honest answer to almost any security question is: "it's complicated!". But there is no shortage of gung-ho salesmen in expensive suits peddling their security wares and no shortage of clients willing to throw money at the problem (because doing something must be better than doing nothing, right?)”

“Wrong. Peddling hard in the wrong direction doesn't help just because you want it to”



14 Apr

If our industry is so broken, why are you still in it? Become a cook or a truck driver then! [#infosec](#)

Expand  Reply  Retweet  Favorite

“You must never confuse faith that you will prevail in the end—which you can never afford to lose—with the discipline to confront the most brutal facts of your current reality, whatever they might be”

Admiral James Stockdale

(un)fortunately we don't have to
convince people anymore



haroon meer

@haroonmeer

Lulzsec hacks embarrassed the sec community by showing we were outclassed as defenders. NSA leaks show we were outclassed as attackers too

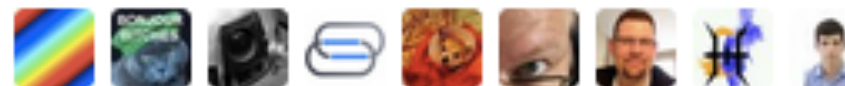


RETWEETS

82

FAVORITES

13



3:12 PM - 7 Sep 2013

“I’m here to tell you that your cyber systems continue to function and serve you not due to the expertise of your security staff but solely due to the sufferance of your opponents”

Brian Snow - 2012

different people have raised their
explanations for our woes



Sentient Opponents & Rate of Change





focus on the bug parade vs secure engineering





RICHARD BEJTlich
Chief Security Strategist, FireEye

BBC WORLD NEWS USE AFTER THE COUNTRY'S FOOD INSPECTORS COMPLAIN





You don't have a malware problem
You have an adversary problem

YOU DON'T HAVE A MALWARE PROBLEM, YOU HAVE AN ADVERSARY PROBLEM

Haroon

← → ↺

https://trademarks.justia.com/856/23/you-don-t-have-a-malware-problem-you-have-an-advers...

☆ ⓘ 📱 I ☰

Justia.com Find a Lawyer Legal Answers Law More ▾

Sign In

JUSTIA Trademarks

Search

Serial Number

85623622

Word Mark

YOU DON'T HAVE A MALWARE PROBLEM, YOU HAVE AN ADVERSARY PROBLEM

Status

819 - SU - Registration Review Complete

Status Date

2015-02-06

Filing Date

2012-05-11

Mark Drawing

4000 - Standard character mark Typeset

Published for Opposition Date

2013-06-18

Attorney Name

Nathan E. Ferguson

Law Office Assigned Location Code

L60

Examiner Name

KIM GODDARD CHUN

Arizona independent Redistricting case before the U.S. Supreme Court.

By [Vikram David Amar](#)

ASK A LAWYER

Question:

Please Ask Your Question Here.
e.g., Do I need a Bankruptcy Lawyer?

Add details 120

Ask Question

FIND A LAWYER

Legal Issue or Lawyer Name

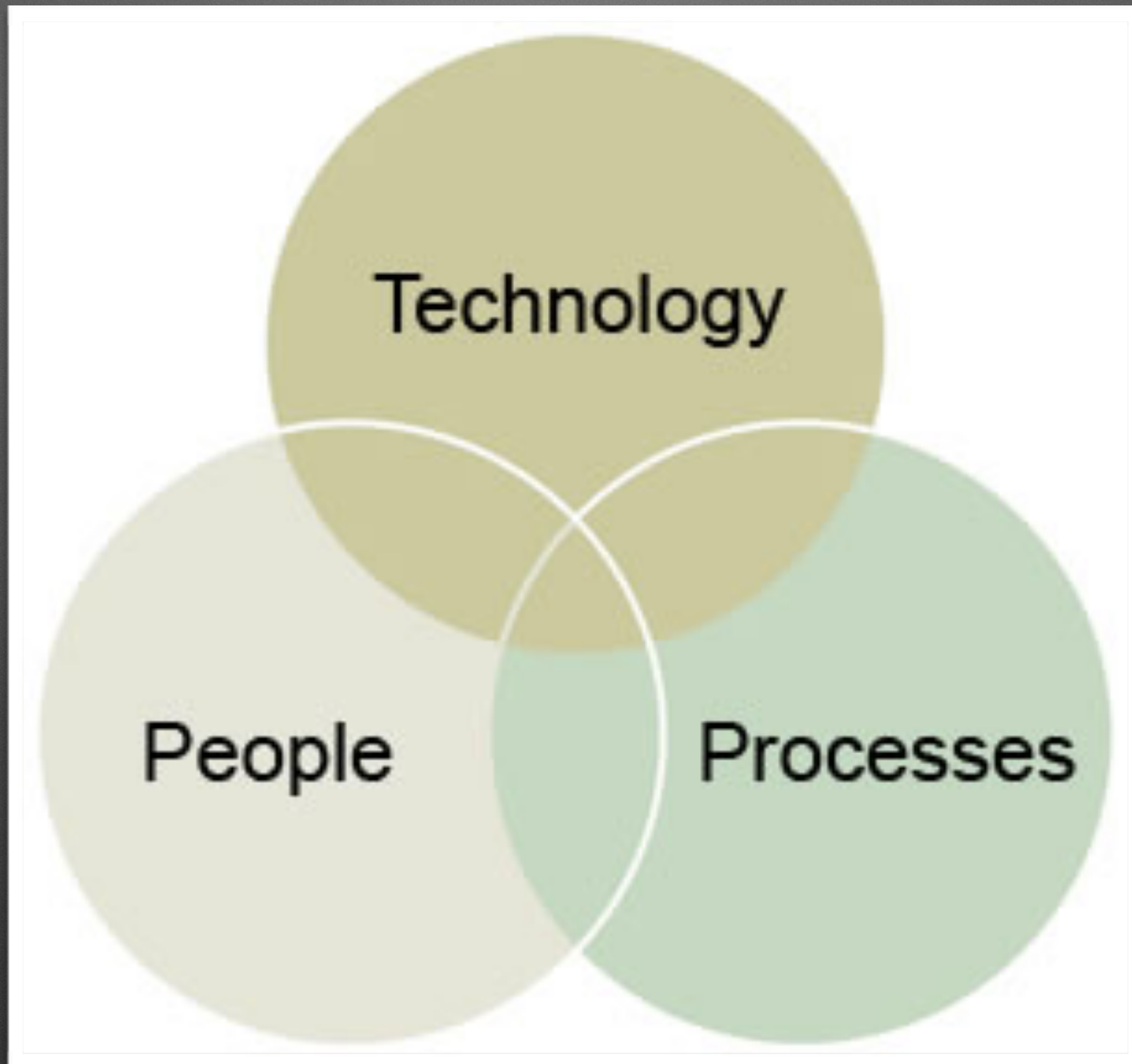
City, State

Search

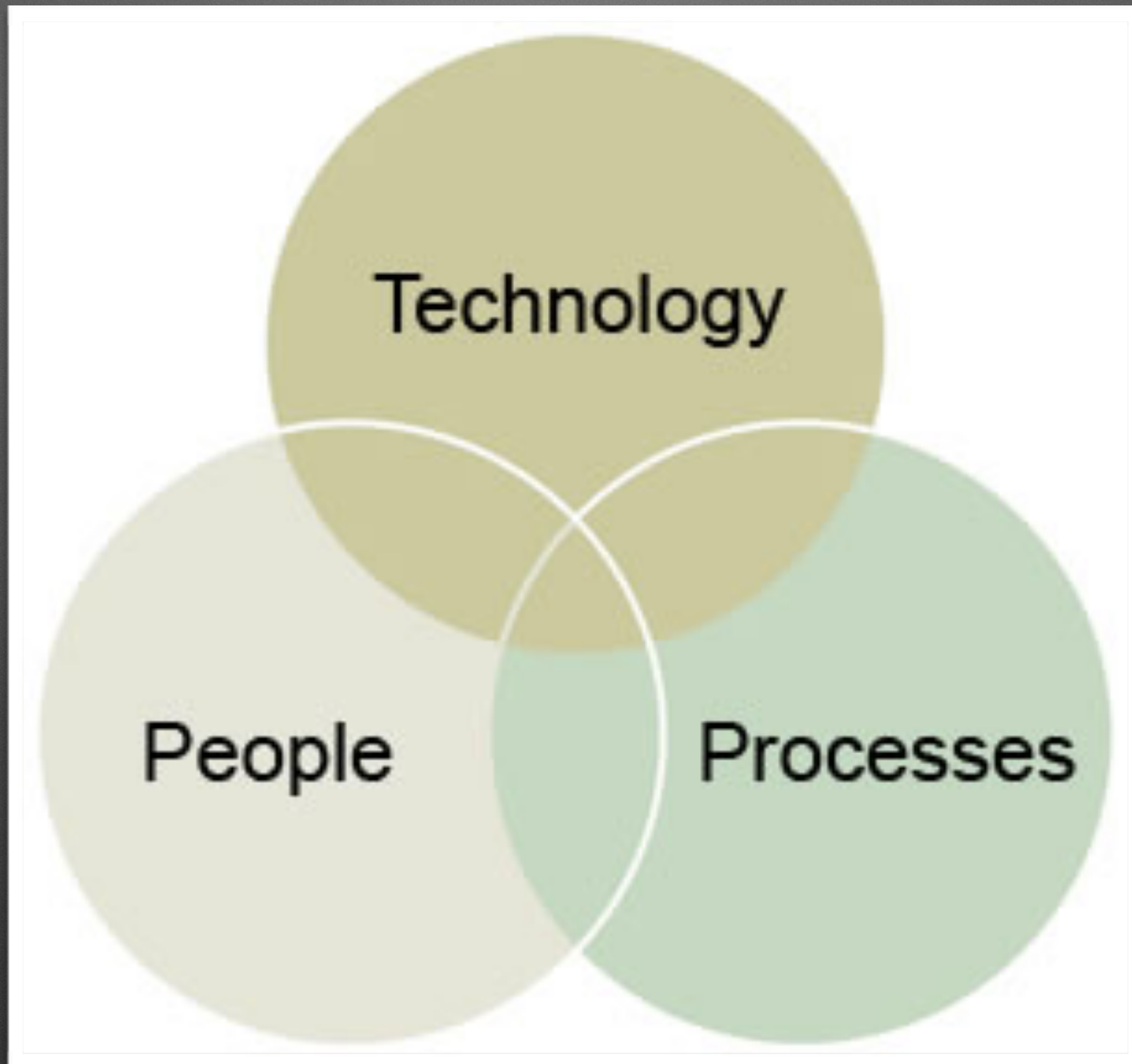
Browse Lawyers



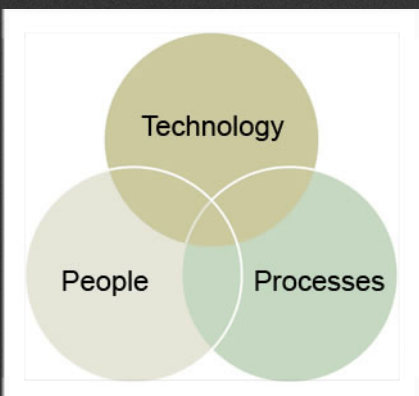
You don't have a malware problem
You have an adversary problem



horrible abuse of Venn Diagrams!



We have some genuinely hard
problems to solve..





**COMPLEXITY
SOFTWARE**

PEOPLE

**ORGANIZATIONS
MARKETS**

**COMPLEXITY
SOFTWARE**

**ORGANIZATIONS
MARKETS**

PEOPLE

COMPLEXITY

Schneier on Security



[Blog](#) [Newsletter](#) [Books](#) [Essays](#) [News](#) [Schedule](#) [Crypto](#) [About Me](#)

A Plea for Simplicity

You can't secure what you don't understand.

Bruce Schneier
Information Security
November 19, 1999

Ask any 21 experts to predict the future, and they're likely to point in 21 different directions. But whatever the future holds--IP everywhere, smart cards everywhere, video everywhere, Internet commerce everywhere, wireless everywhere, agents everywhere, AI everywhere, *everything* everywhere--the one thing you can be sure of is that it will be complex. For consumers, this is great. For security professionals, this is terrifying. The worst enemy of security is complexity. This has been true since the beginning of computers, and it's likely to be true for the foreseeable future.

We all know the amount of testing that goes into any major software product, and we all know the number of bugs that still slip through. The testing process--implement, test, fix, test, repeat--is imperfect, but it's the best we've found. Security doesn't lend itself to this process, because security properties cannot be "tested" in the same way as functional properties. Products are useful for what they do, while security products are useful solely because of what they *prevent* from being done. A security product may work fine, but you have no idea if it is secure. No amount of beta testing can uncover a security flaw. Ever.

The only way to evaluate the security of a system is to analyze it. This is a time-consuming and expensive process, and almost no one bothers to go through it. If they did, they would quickly realize that most systems are far more complex to analyze, and that there are security flaws everywhere.

We've seen security bugs in almost everything: operating systems, applications programs, network hardware and software, and security products themselves. This is a direct result of the complexity of these systems. The more complex a system is--the more options it has, the more functionality it has, the more interfaces it has, the more interactions it has--the harder it is to analyze. Everything is more complicated: the specification, the design, the implementation, the use. And everything is relevant to security analysis.

This complexity isn't limited to single systems, but includes interactions *between* systems as well. For years we knew that Internet applications like sendmail and rlogin had to be secure, but the recent epidemic of macro viruses shows that Microsoft Word and Excel need to be secure too. Rogue printer drivers can compromise Windows NT. Malicious attachments can tunnel through firewalls. Maintenance ports on routers can compromise networks, as can random modems. DSL and satellite modems can completely compromise security. So can Java or Microsoft Outlook. Or your recycling bin.

The networks of the future will be necessarily more complex, and therefore less secure. The technology industry is driven by the demand for features, for options, for speed. There are no standards for quality or security, and there is no liability for insecure software. Hence, there is no economic incentive to build in high quality. In fact, it's just the opposite. There is an economic incentive to create the lowest quality the market will bear. Unless customers demand higher quality and better security, this will never change.

I see two alternatives. The first is to recognize that the digital world will be one of ever-expanding features and options, of ever-faster product releases, of ever-increasing complexity and of ever-decreasing security. This is the world we have today, and we can decide to embrace it knowingly.

The other choice is to slow down, simplify and try to add security. Customers won't demand this--the issues are too complex for them to understand--so a consumer advocacy group is required. This solution might not be economically viable for the Internet, but it is the only way to get security.

BRUCE SCHNEIER is CTO of Counterpane Internet Security Inc., a company trying to bring managed security solutions to complex networks. He writes the *CryptoRhythms* column for Information Security, and is the author of Applied Cryptography and the Blowfish and Twofish encryption algorithms.

Predictions

- As systems get more complex, security will get worse.
- As systems become more interconnected, security will get worse.
- Unless manufacturers are held liable for security failures, security will get worse.
- The only long-term solutions are to either embrace insecurity or eschew "Internet-years" style complexity.
- In the short term, the best course of action for enterprises is to outsource security to companies that have the expertise to understand the systems being secured.

Categories: [Business of Security](#), [Computer and Information Security](#)

Tags: [Information Security](#)

Like Tweet +1

[← DVD Encryption Broken](#)

[The 1999 Crypto Year-in-Review →](#)

Photo of Bruce Schneier by Per Ervand.
Schneier on Security is a personal website. Opinions expressed are not necessarily those of [Resilient Systems, Inc.](#)

About Bruce Schneier



I've been writing about security issues on my blog since 2004, and in my monthly newsletter since 1998. I write books, articles, and academic papers. Currently, I'm the Chief Technology Officer of Resilient Systems, a fellow at Harvard's Berkman Center, and a board member of EFF.

Featured Essays

[It's Time to Break Up the NSA](#)
[How the NSA Threatens National Security](#)
[Terrorists May Use Google Earth, but Fear is No Reason to Ban It](#)
[In Praise of Security Theater](#)
[The Eternal Value of Privacy](#)
[Terrorists Don't Do Movie Plots](#)

[more essays](#)

Essay Archives

[Archives by Date](#)
[Restaurant Reviews](#)

Essay Categories

[Airline Travel](#)
[Business of Security](#)
[Computer and Information Security](#)
[Cyberwar and Cyberterrorism](#)
[Disasters](#)
[Economics of Security](#)
[Elections](#)
[ID Cards](#)
[Identity Theft](#)
[Internet and Society](#)
[Laws and Regulations](#)
[National Security Policy](#)
[Non-Security Articles](#)
[Physical Security](#)
[Privacy and Surveillance](#)
[Psychology of Security](#)
[Social Engineering](#)
[Terrorism](#)
[Theory of Security](#)
[Trust](#)

Essay Tags

[Wired](#) / [The Guardian](#) / [Information Security](#) / [CNN](#) / [IEEE Security & Privacy](#) / [MacWEEK](#) / [The Atlantic](#) / [Communications of the ACM](#) / [Forbes](#) / [Minneapolis Star Tribune](#) / [The Wall Street Journal](#) / [InternetWeek](#) / [Computerworld](#) / [Network World](#) / [The Sydney Morning Herald](#) / [CNET News.com](#) / [New York Daily News](#) / [New York Times Room for Debate](#) / [Dark Reading](#) / [eWeek](#) / [Newsday](#) / [Salon](#) / [San Francisco Chronicle](#) / [Threatpost](#) / [ZDNet](#) / [AOL News](#) / [Dr. Dobb's Journal](#) / [IEEE Computer](#) / [Macworld](#) / [MPR NewsQ](#)

[more tags](#)

[Blog](#) [Newsletter](#) [Books](#) [Essays](#) [News](#) [Schedule](#) [Crypto](#) [About Me](#)



We've seen security bugs in almost everything: operating systems, applications programs, network hardware and software, and security products themselves. This is a direct result of the complexity of these systems. The more complex a system is--the more options it has, the more functionality it has, the more interfaces it has, the more interactions it has--the harder it is to analyze. Everything is more complicated: the specification, the design, the implementation, the use. And everything is relevant to security analysis.

The networks of the future will be necessarily more complex, and therefore less secure. The technology industry is driven by the demand for features, for options, for speed. There are no standards for quality or security, and there is no liability for insecure software. Hence, there is no economic incentive to build in high quality. In fact, it's just the opposite. There is an economic incentive to create the lowest quality the market will bear. Unless customers demand higher quality and better security, this will never change.

I see two alternatives. The first is to recognize that the digital world will be one of ever-expanding features and options, of ever-faster product releases, of ever-increasing complexity and of ever-decreasing security. This is the world we have today, and we can decide to embrace it knowingly.

The other choice is to slow down, simplify and try to add security. Customers won't demand this--the issues are too complex for them to understand--so a consumer advocacy group is required. This solution might not be economically viable for the Internet, but it is the only way to get security.

Schneier on Security

[Blog](#)[Newsletter](#)[Books](#)[Essays](#)[News](#)[Schedule](#)

A Plea for Simplicity

You can't secure what you don't understand.

Bruce Schneier

Information Security

November 19, 1999

predictably - we are far worse

linux kernel
1991 - 10,239 (loc)

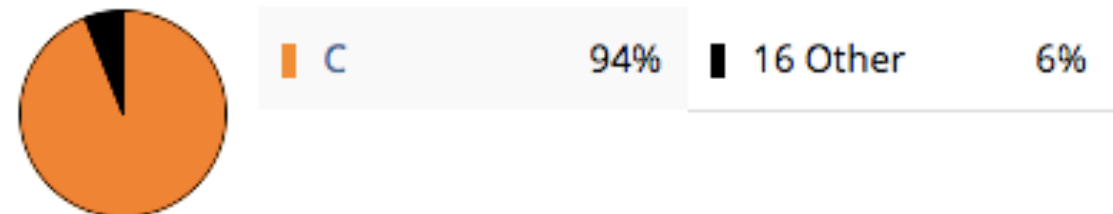
linux kernel

1991 - 10,239 (loc)

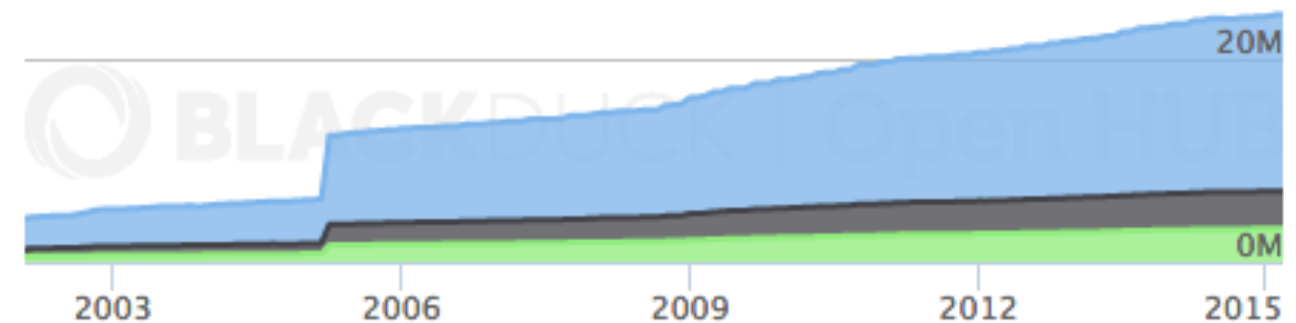
In a Nutshell, Linux Kernel...

- ... has had 569,762 commits made by 13,912 contributors representing 17,284,904 lines of code
- ... is mostly written in C with an average number of source code comments
- ... has a well established, mature codebase maintained by a very large development team with stable Y-O-Y commits
- ... took an estimated 5,618 years of effort (COCOMO model) starting with its first commit in February, 2002 ending with its most recent commit 5 days ago

Languages



Lines of Code



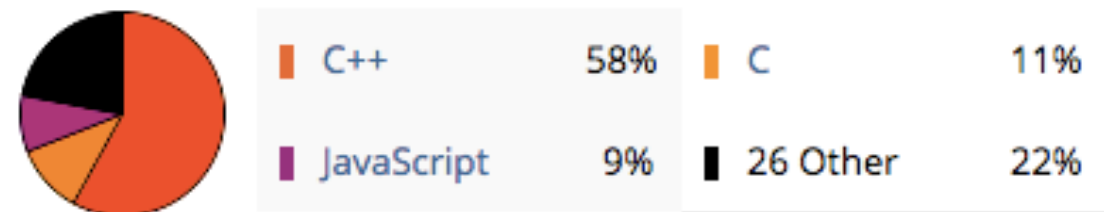
Kernel 3.3 shipped on 18 March, 2012, and in the 13 months since, 3,172 developers have contributed some 68,000 change sets into the mainline kernel. The kernel is now 1.53 million lines bigger than it was a year ago.

Chrome

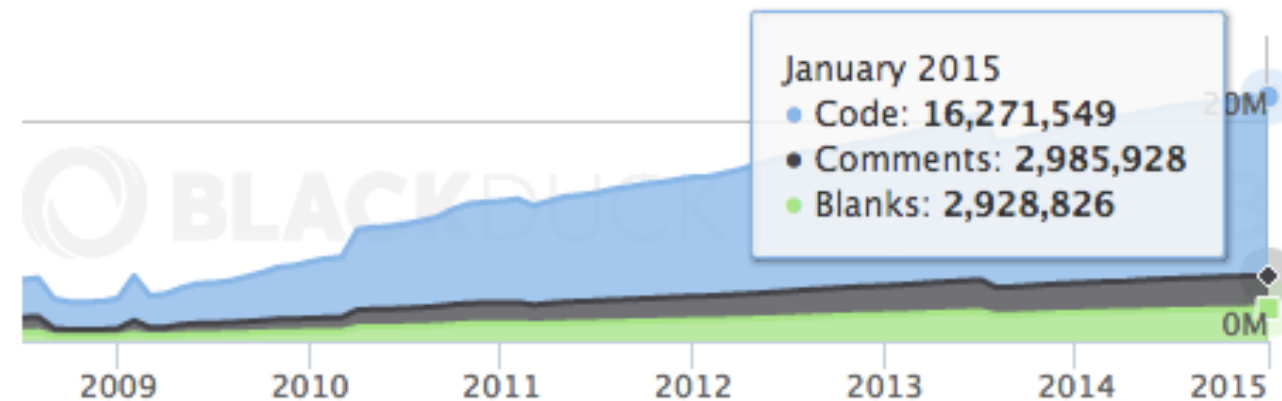
In a Nutshell, Chromium (Google Chrome)...

- ... has had 533,479 commits made by 3,347 contributors representing 16,271,549 lines of code
- ... is mostly written in C++ with an average number of source code comments
- ... has a well established, mature codebase maintained by a very large development team with decreasing Y-O-Y commits
- ... took an estimated 5,160 years of effort (COCOMO model) starting with its first commit in July, 2008 ending with its most recent commit 2 months ago

Languages



Lines of Code







“You have three fairly capable CPU cores, with a pretty big amount of RAM connected to it. There's also an uart, for the serial port, and at least two SPI interfaces; one to the flash rom and one to the spindle controllers. You can load the code for the processor by updating an external flash chip, or even by using the serial port in the bootloader”

```
ROXTerm
jeroen@spritesws:~/hddfw$ sudo mount /dev/sdal /mnt
jeroen@spritesws:~/hddfw$ echo 'HD, live' > /mnt/home/jeroen/dummy
jeroen@spritesws:~/hddfw$ cp linux/kernel.sect /mnt/home/jeroen/
jeroen@spritesws:~/hddfw$ cp linux/initrd.sect /mnt/home/jeroen/
jeroen@spritesws:~/hddfw$ sync
jeroen@spritesws:~/hddfw$ echo 'HD, lnx!' > /mnt/home/jeroen/dummy
jeroen@spritesws:~/hddfw$

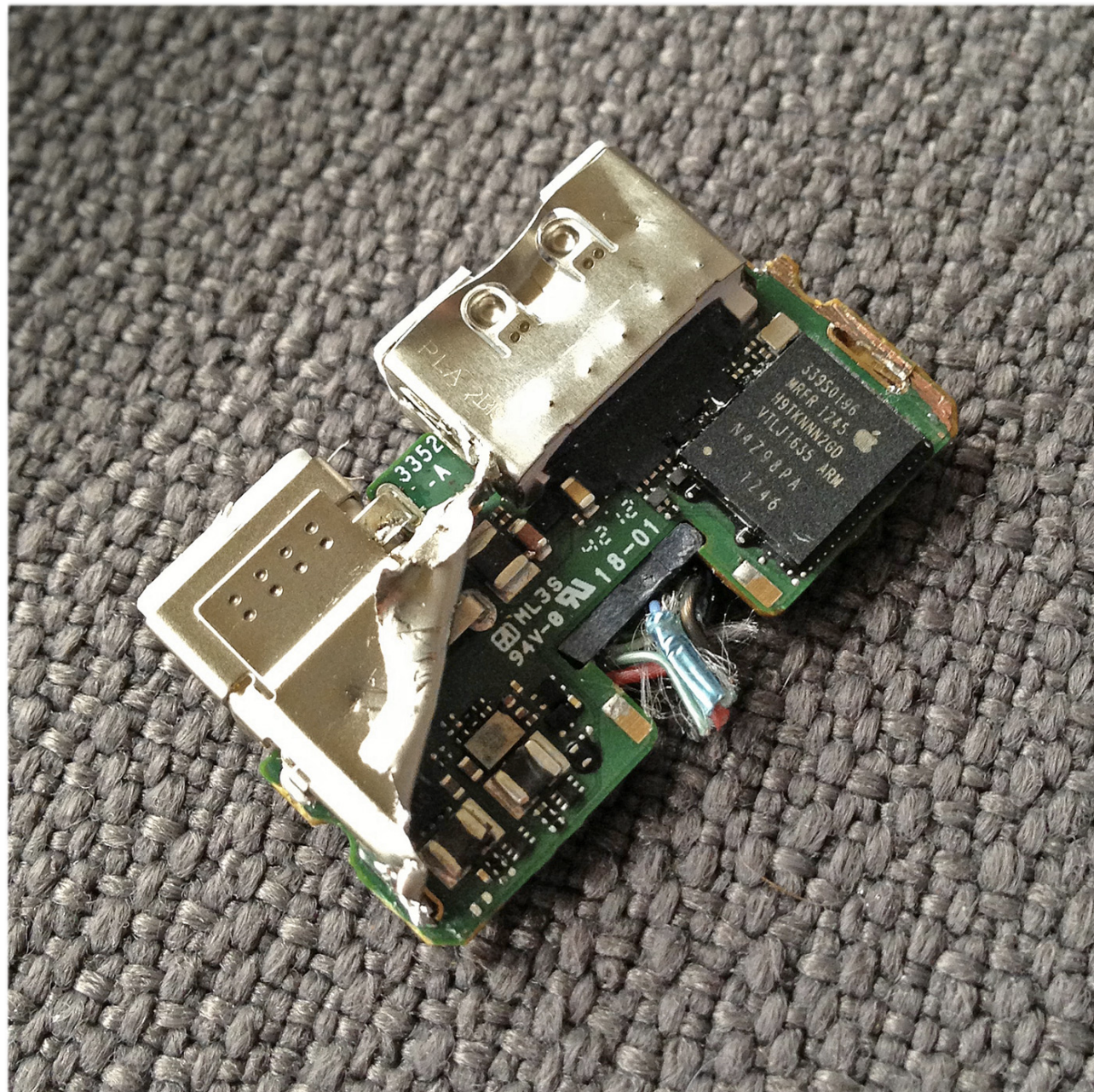
.data : 0x29128000 - 0x29133dc0    ( 48 kB)
.bss : 0x29133dc0 - 0x2915b7e8    ( 159 kB)
NR_IRQS:16
sched_clock: 32 bits at 100 Hz, resolution 100000000ns, wraps every 4s
Console: colour dummy device 80x30
console [tty0] enabled
Calibrating delay loop... 0.13 BogoMIPS (lpj=669)
pid_max: default: 32768 minimum: 301
Mount-cache hash table entries: 512
Failed to create a rootfs
msgmni has been set to 90
Serial: 8250/16550 driver, 4 ports, IRQ sharing enabled
Warning: unable to open an initial console.
Freeing init memory: 60K
```




<http://www.panic.com/blog/the-lightning-digital-av-adapter-surprise/>



<http://www.panic.com/blog/the-lightning-digital-av-adapter-surprise/>

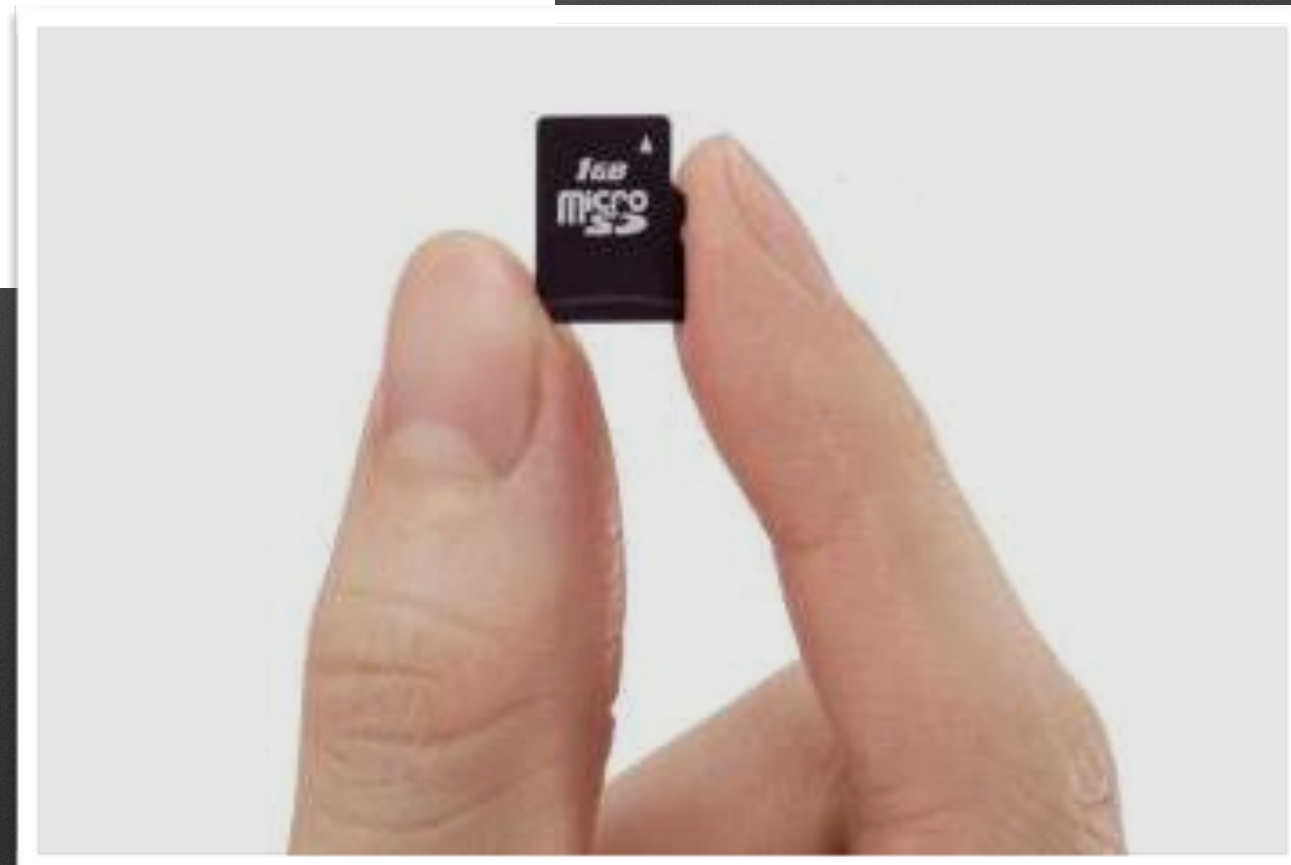


<http://www.panic.com/blog/the-lightning-digital-av-adapter-surprise/>

SD Card Hacking

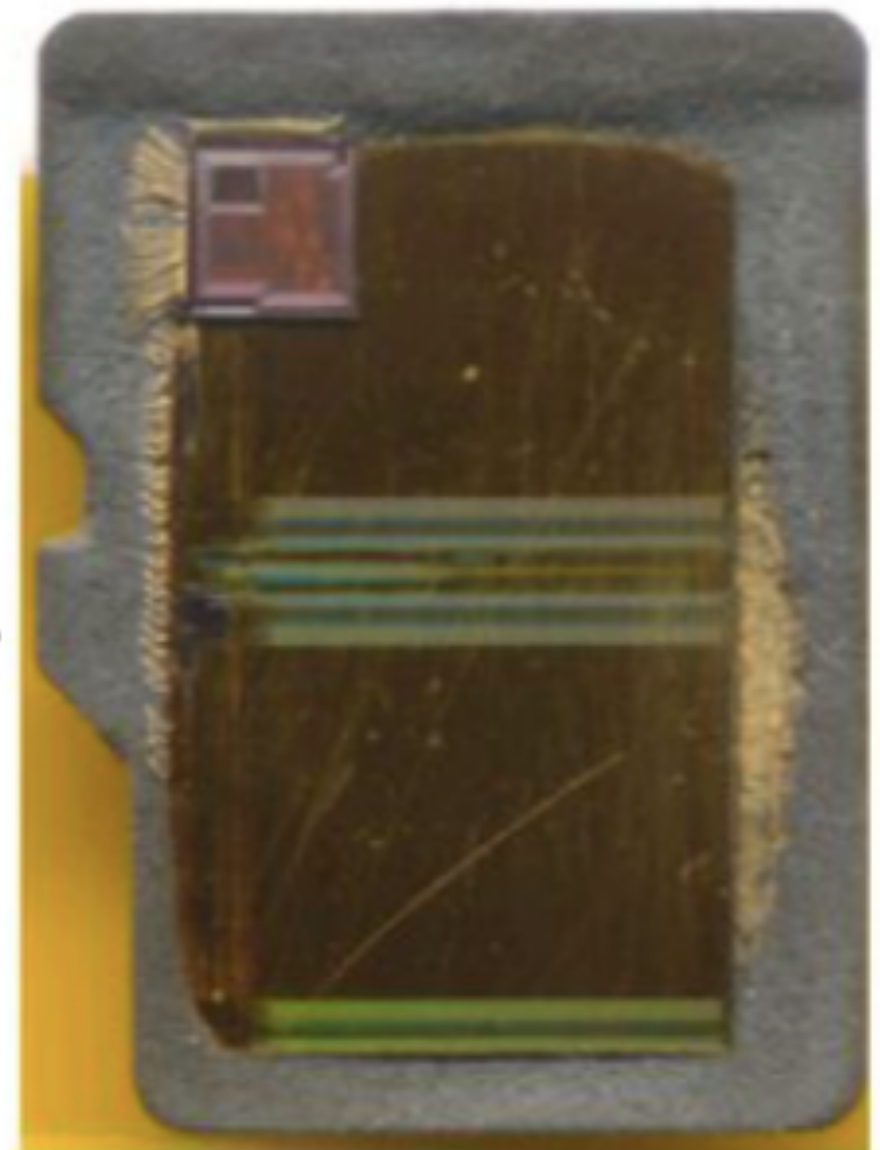
The Exploration and Exploitation of an SD Memory Card

bunnie & xobs
30c3



Solution: managed Flash

- Small embedded controller in every “managed Flash” device
 - 8051 or ARM7 CPU
 - 4-8mm² silicon = ~\$0.15-\$0.30 cost add-on
 - Compare to Flash die area = 100mm², \$2.90 cost
 - Compare to test cost, wafer-scale tester = \$1mm = ~\$0.45 for a 30 second test (assuming 24 month lifetime and usage 24x7x365)



Wrap-up

- SD cards contain fully programmable microcontrollers
- Controller program modifiable via special host commands
 - Potential for MITM attack scenarios 😊
 - Potential for extremely cheap microcontroller for fun projects 😊

*“You have dropped into the abyss
and you may never get out.”*





In a quite similar fashion, computer security developed other focal points at which to implement security. The guiding principle in this case was usually one of minimally invasive measures, applied *ad hoc* to a specific system along with other needs. These measures were applied in a surgical manner to only a very few places, which had been the most common vectors of attacks, so no other ‘critical’ specified function was disturbed.

This approach, however, is dangerously flawed from the outset. Attackers are not like natural catastrophes. They can analyze their targets for vulnerable elements. Isolating single, selected vectors only shifts them onto a different, less observed, and less protected vector.

An example is encryption. Even today lay people and encryption technology salesmen tend to think that encryption can solve everything—if simply everything could be encrypted, everything would be safe. This reasoning, again, pays little heed to the composite nature of information technology. Encryption can only protect certain content under certain conditions. It will not protect the operating system in charge of the encryption process and in charge of holding the keys. Thus, selling encryption as a critical guard at a critical gate for overall system protection is clearly mistaken, just like any other kind of protection focused on selected vectors. In a composite system, there is no critical gate: everything is a gate.

Baseline checks

Verify signatures
on all **userspace**
binaries

Verify signatures
on all **kernel**
space binaries

Verify signatures
on all **BIOS**
components

Verify signatures
on all **device**
firmwares

Verify signatures
on the **Intel ME**
code

Verify **that the signers**
know about their
signatures

Verify origin of
privileged scripts

Baseline checks

Verify signatures
on a **FAILURE** ice
binaries

Verify signatures
of **FAILURE** el
space binaries

Verify signatures
of **FAILURE** \$
components

Verify signatures
of **FAILURE** e
firmwares

Verify signatures
on **FAILURE** ME
code

Verify ~~that the signers~~
know **FAILURE** their
signatures

Ve **FAILURE** of
privileged scripts

Failure on all levels

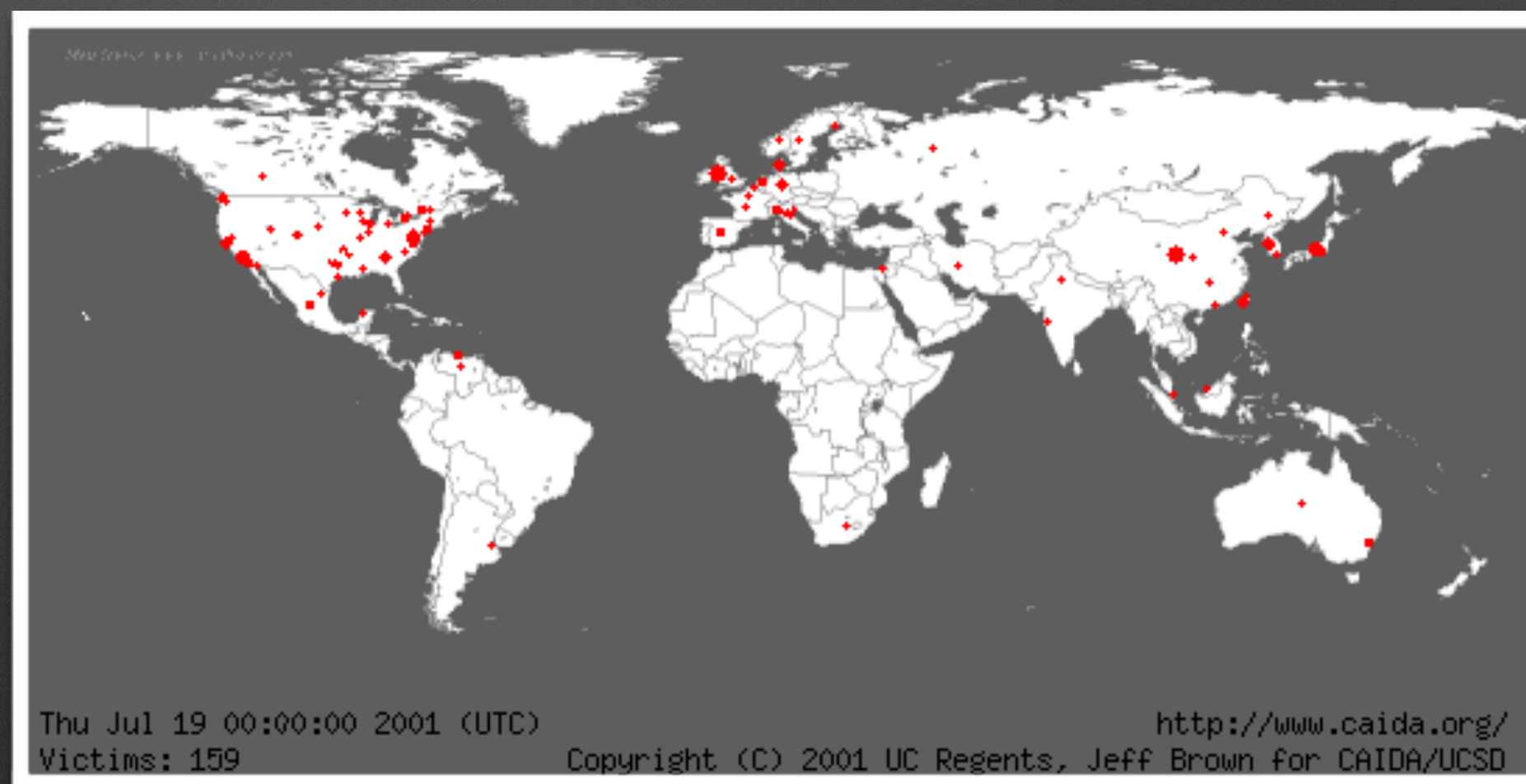
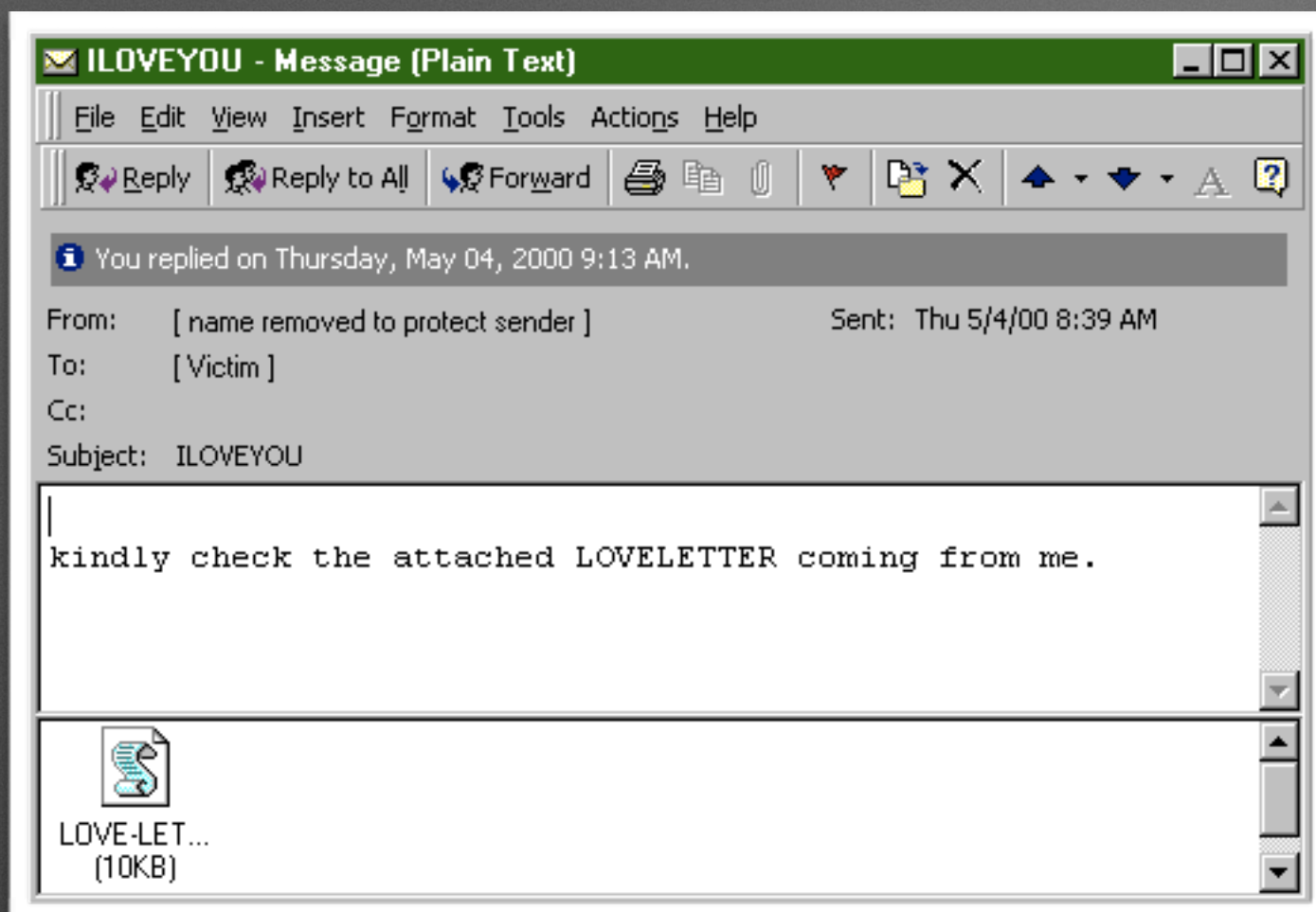
Given modern infrastructure, it is nearly impossible to determine if a machine is compromised

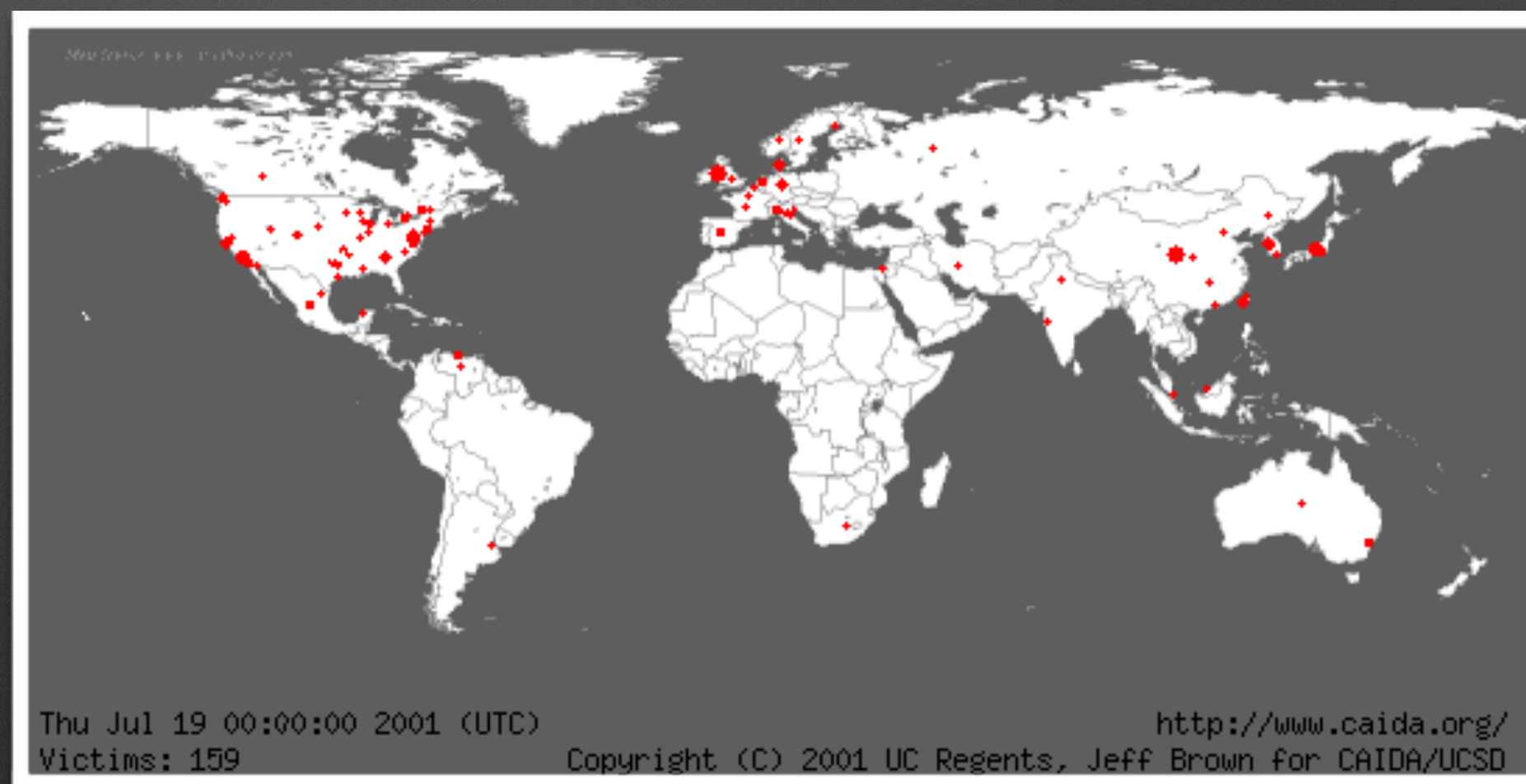
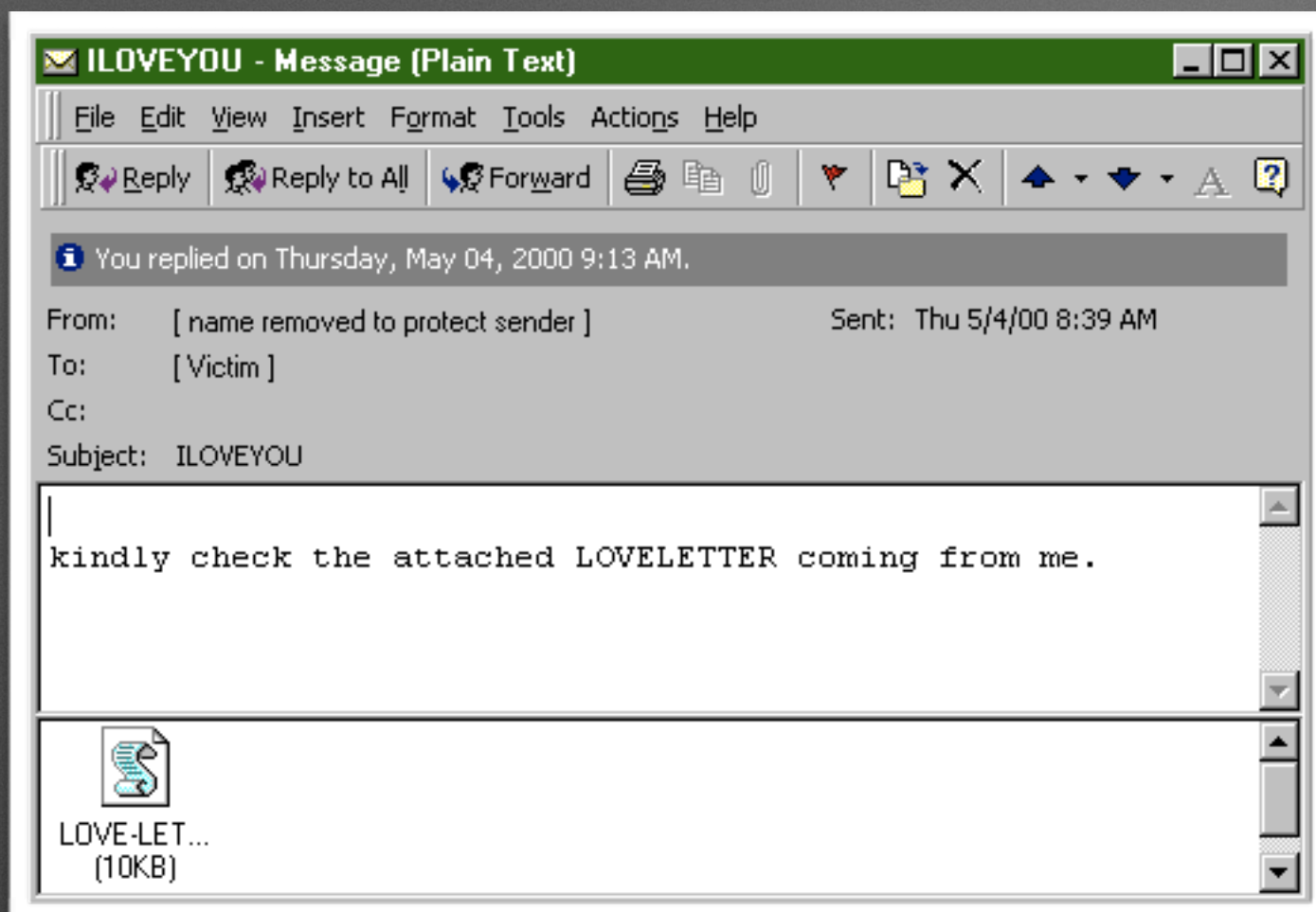
It is also nearly impossible to “un-infect” a machine once it has been infected

SOFTWARE

provably bad at writing secure
software at scale

provably ?





-----Original Message-----

From: Bill Gates

Sent: Tuesday, January 15, 2002 2:22 PM

To: Microsoft and Subsidiaries: All FTE

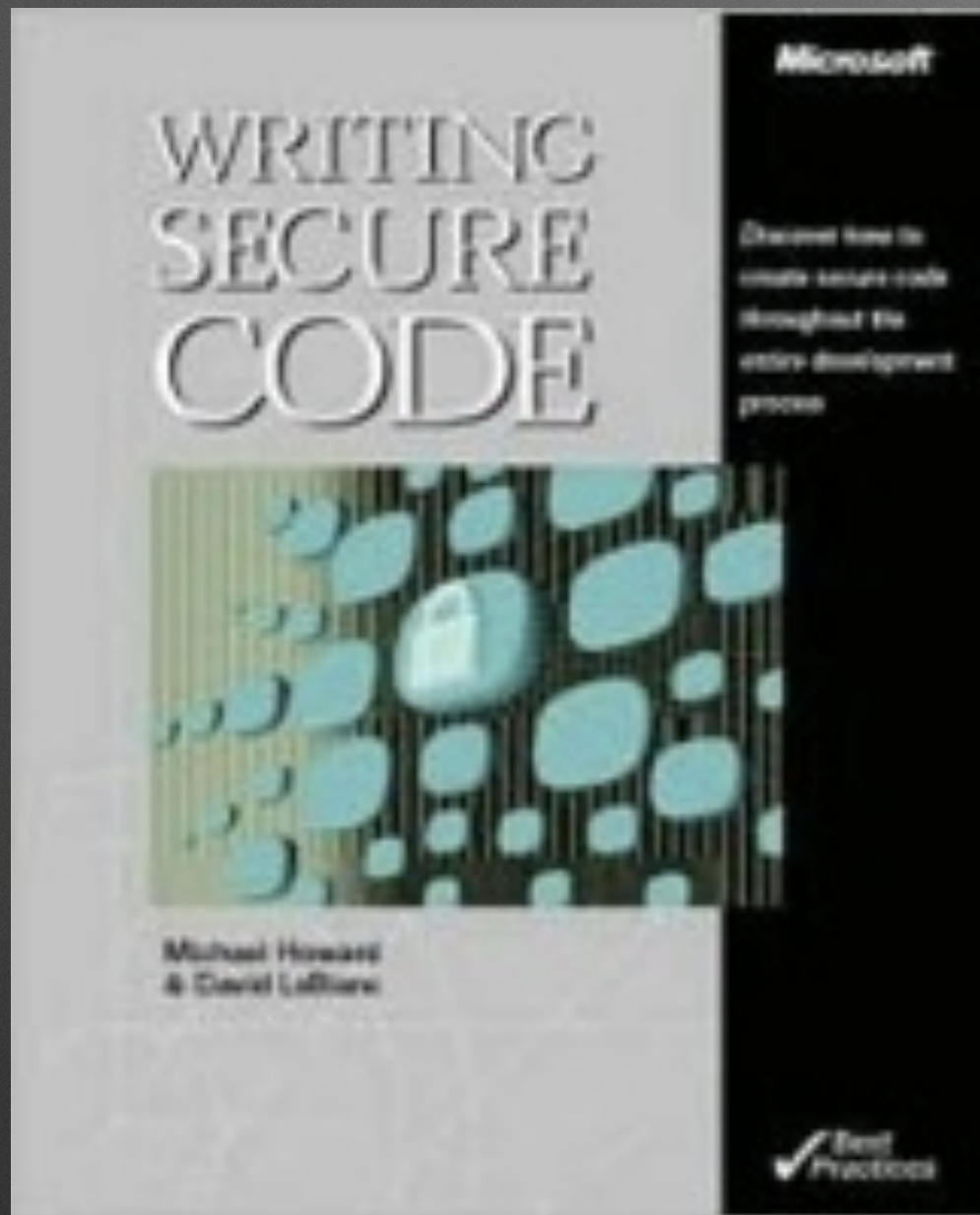
Subject: Trustworthy computing

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing – or able – to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.

When we started work on Microsoft .NET more than two years ago, we set a new direction for the company – and articulated a new way to think about our software. Rather than developing standalone applications and Web sites, today we're moving towards smart clients with rich user interfaces interacting with Web services. We're driving the XML Web services standards so that systems from all vendors can share information, while working to make Windows the best client and server for this new era.

There is a lot of excitement about what this architecture makes possible. It allows the dreams about e-business that have been hyped over the last few years to become a reality. It enables people to collaborate in new ways, including how they read, communicate, share annotations, analyze information and meet.

However, even more important than any of these new capabilities is the fact that it is designed from the ground up to deliver Trustworthy



Did things change?

Microsoft Security Bulletin Summary for February 2015

[local copy]

FLOSS to the Rescue ?

“given enough eyeballs, all bugs are shallow”

OpenSSLTM

Cryptography and SSL/TLS Toolkit



ShellShock
{bashbug}

even people with every incentive
to do it right...

THIS PHONE IS AN NSA-FREE, SECRET-STORING BLACK BOX

MEET THE BLACKPHONE, BROUGHT TO YOU BY THE CREATOR OF ENCRYPTION SERVICE PGP.

By Colin Lecher Posted January 15, 2014

With \$50M Boost, Silent Circle Aims Blackphone At Enterprise Security

Posted Feb 26, 2015 by [Natasha Lomas \(@riptari\)](#)

World's most secure Android phone vows to 'replace' and 'dominate' BlackBerry

THE BLACKPHONE 2 IS AN ULTRA-SECURE SMARTPHONE MADE FOR SECRET AGENTS



While exploring my recently purchased BlackPhone, I discovered that the messaging application contains a serious memory corruption vulnerability that can be triggered remotely by an attacker. If exploited successfully, this flaw could be used to gain remote arbitrary code execution on the target's handset. The code run by the attacker will have the privileges of the messaging application, which is a standard Android application with some additional privileges. Specifically, it is possible to:



Mark Dowd is clearly a genius,
but..

multiple critical vulnerabilities in sophos products

From: Tavis Ormandy <taviso () cmpxchg8b com>

Date: Mon, 5 Nov 2012 16:14:17 +0100

List, I've completed the second paper in my series analyzing Sophos Antivirus internals, titled "Practical Attacks against Sophos Antivirus". As the name suggests, this paper describes realistic attacks against networks using Sophos products.

The paper includes a working pre-authentication remote root exploit that requires zero-interaction, and could be wormed within the next few days. I would suggest administrators deploying Sophos products study my results urgently, and implement the recommendations.

I've also included a section on best practices for Sophos users, intended to help administrators of high-value networks minimise the potential damage to their assets caused by Sophos.

The paper is available to download at the link below.

<https://lock.cmpxchg8b.com/sophailv2.pdf>

IV. Conclusion

As demonstrated in this paper, installing Sophos Antivirus exposes machines to considerable risk. If Sophos do not urgently improve their security posture, their continued deployment causes significant risk to global networks and infrastructure.

In response to early access to this report, Sophos did allocate some resources to resolve the issues discussed, however they were clearly ill-equipped to handle the output of one co-operative, non-adversarial security researcher. A sophisticated state-sponsored or highly motivated attacker could devastate the entire Sophos user base with ease.

Sophos claim their products are deployed throughout [healthcare](#), [government](#), [finance](#) and even the military⁶. The chaos a motivated attacker could cause to these systems is a realistic global threat. For this reason, Sophos products should only ever be considered for low-value non-critical systems and never deployed on networks or environments where a complete compromise by adversaries would be inconvenient.

The author is often asked what he recommends existing Sophos users migrate to. The author currently recommends Parity Suite, from Bit9 software⁷, an easily defensible solution.



Retweeted by Ben Nagy



Joxean Koret @matalaz · 30m

It took me longer to install your AV, Comodo, than finding the first bug on it.
Thanks for playing, wait for results...

RETWEETS

8

FAVORITES

4



2:02 PM - 25 Aug 2014 · Details

Software Sub-segment Performance on First Submission

■ Acceptable ■ Not Acceptable

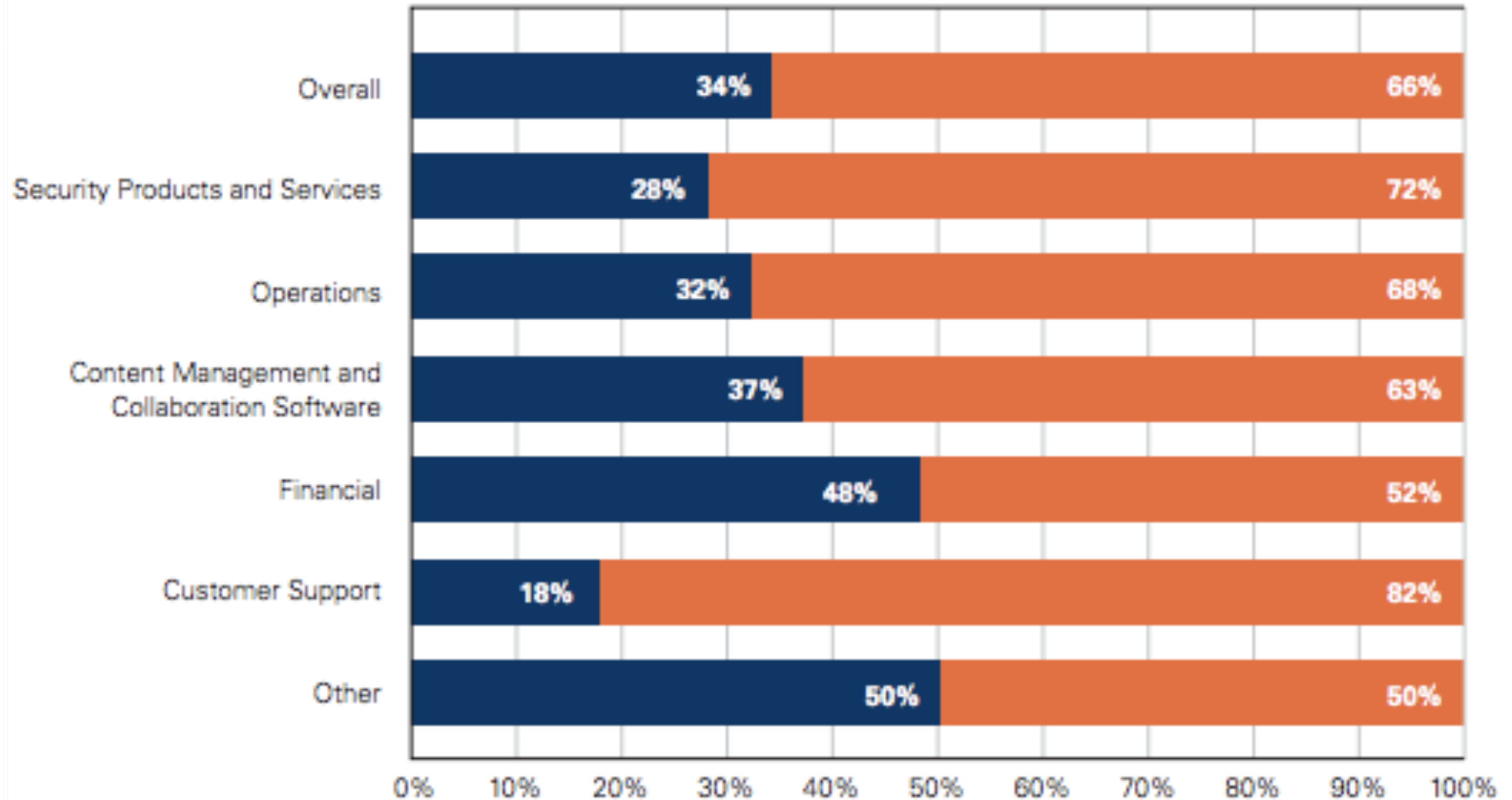
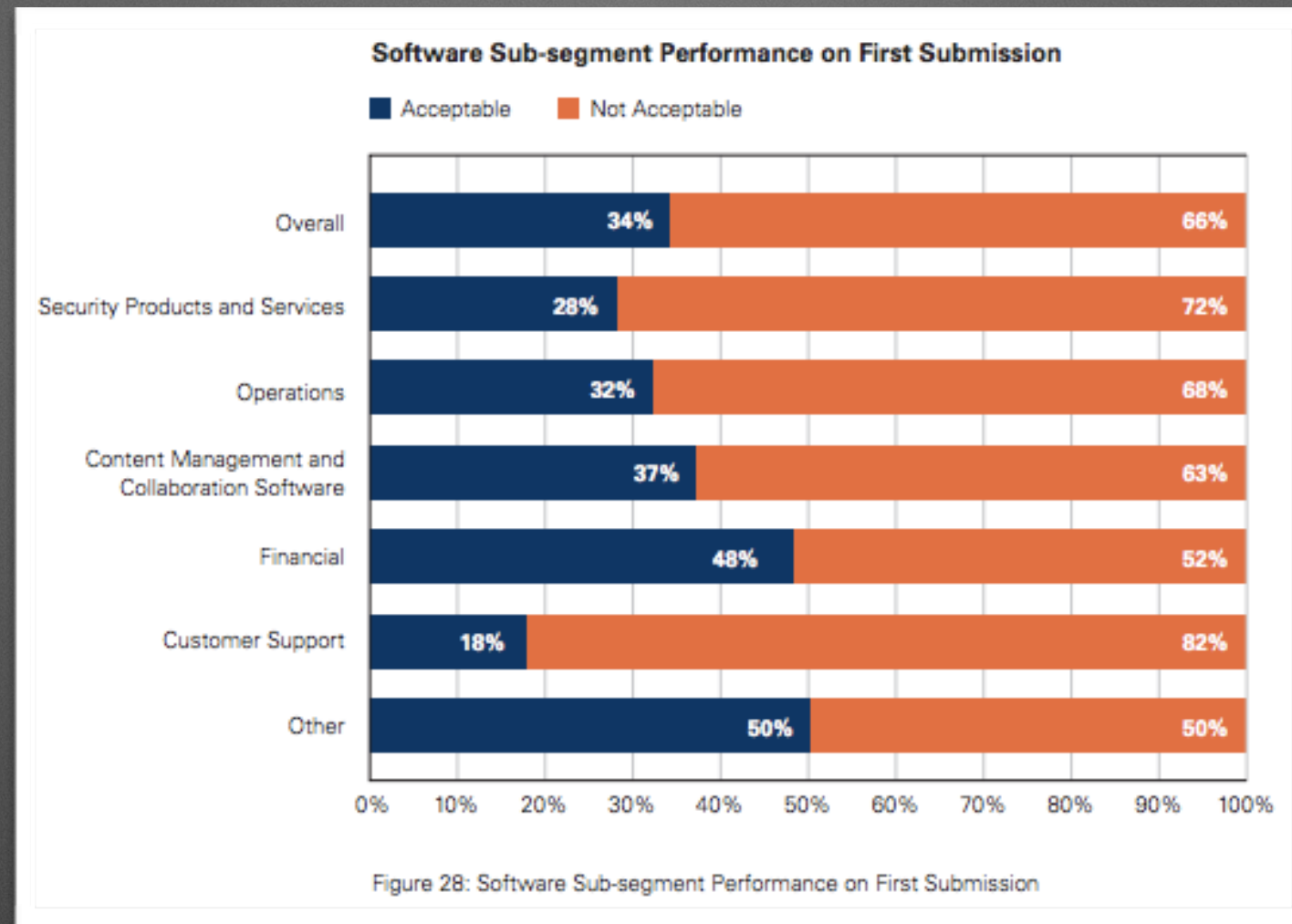


Figure 28: Software Sub-segment Performance on First Submission



“basically by quality level you would be better off defending your network with microsoft word than a checkpoint firewall”

-fx

Enigmail PGP plugin forgets to encrypt mail sent as blind copies

"Such functionality is missing in version 1.7. Even when marked to be encrypted, an email with only BCC recipients is sent in plain text!"

The email was sent in plaintext after users check boxes to encrypt their message.

MARKETS

One of our great (possible)
contributions to the world

a number of beautiful examples
of market failures



Journalism in the Public Interest



Receive our top stories daily

Email address

SUBSCRIBE

Home

Our Investigations

Data

MuckReads

Get Involved

About Us



Search ProPublica



The World's Email Encryption Software Relies on One Guy, Who is Going Broke

Werner Koch's code powers the email encryption programs around the world. If only somebody would pay him for the work.

by [Julia Angwin](#)

ProPublica, Feb. 5, 2015, 11:24 a.m.

262 Comments | Print



Connect with Facebook to share articles you read on ProPublica. [Learn more »](#)



Enable Social Reading

KEEP YOUR CLOUD
TO YOURSELF

<https://gnupg.org/blog/20141214-gnupg-and-g10.html>







62,642

backers

\$13,285,226

pledged of \$50,000 goal



MAIN MENU ▾

MY STORIES: 0 ▾

FORUMS

SUBSCRIBE

JOBS

ARS CONSORTIUM

RISK ASSESSMENT / SECURITY & HACKTIVISM

Once-starving GnuPG crypto project gets a windfall. Now comes the hard part

With project understaffed for a decade, code has fallen into disrepair. What now?

by Dan Goodin - Feb 6, 2015 9:35pm SAST

Share

Tweet

81



It's encouraging to see the GnuPG project benefitting from similar largess. But it also raises the question: how is the money best spent? Matt Green, a professor specializing in cryptography at Johns Hopkins University, said he has looked at the GnuPG source code and found it in such rough shape that he regularly assigns chunks of it to his students for review.



6,911

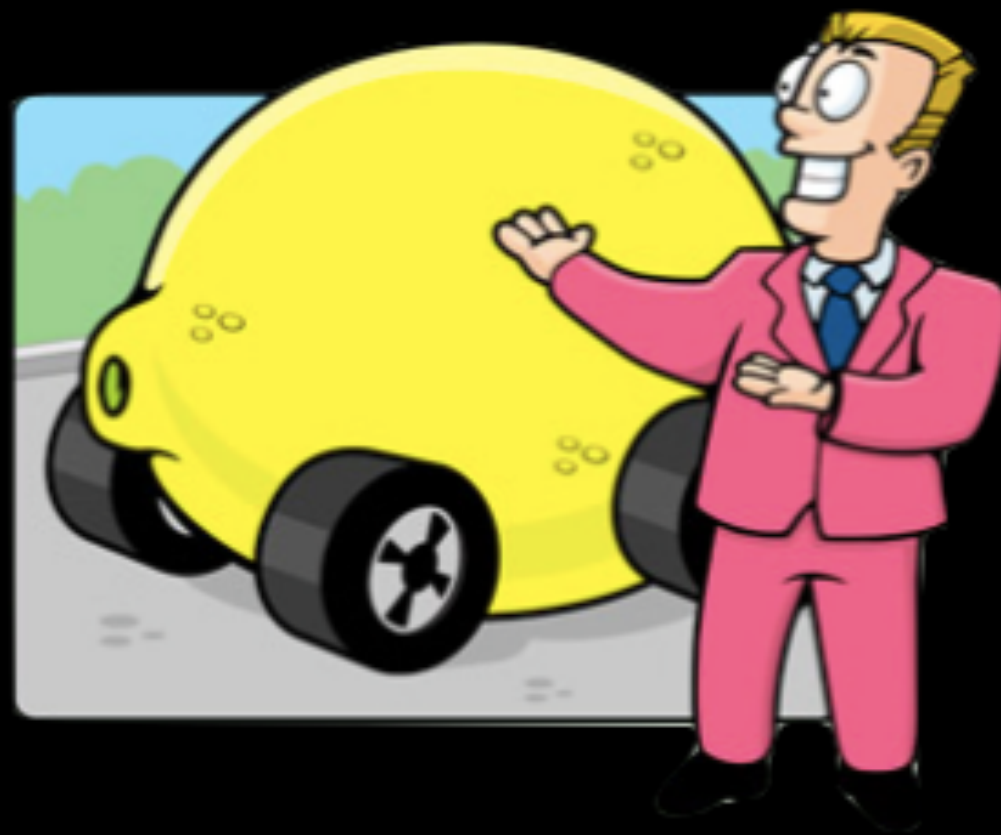
backers

\$55,492

pledged of \$10 goal

Information Asymmetry

Pen-Testing Companies a “market for lemons”



<http://hydrogen.its.ucdavis.edu/eec/education/EEC-classes/eeclimate/class-readings/akerlof-the%20market%20for%20lemons.pdf>



For Sale



For Sale
(Customer View)



For Sale



For Sale






For Sale





Twitter / telegram: 4.95 m x


Twitter, Inc. [US] <https://twitter.com/telegram/status/437743435395514368>

Home Connect Discover Me Search

 **Telegram Messenger** @telegram  




4.95 million people signed up for Telegram today. Telegram is #1 most downloaded iPhone app in 48 countries. To the bad news...

 Reply  Retweet  Favorite  More

RETWEETS 978 FAVORITES 276 







2:19 AM - 24 Feb 2014







Related headlines


-  **Millions Flock to Telegram Messaging App After WhatsApp Outage**
Mashable @mashable
-  **WhatsApp-kaupat olivat onnenpotku kilpailevalle sovellukselle**
Yleisradio @Yleisradio
-  **This Messaging App Added 5 Million New Members One Day After ...**
BI: Tech @SAI

Show 2 more

Reply to @telegram

 **Reynald Lelong** @ReynaldLelong · 22h
@telegram Very bad news.. ^^
 Details  Reply  Retweet  Favorite  More

 **@99xc** صوت مصر الليبرالي · 22h
@telegram We need a BB version plz!
 Details  Reply  Retweet  Favorite  More

 **AKA jemas** @jtseros · 22h

TextSecure Private Messenger

https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en

Apps

My apps

Shop

Games

Editors' Choice

My wishlist

Redeem

Using TextSecure, you can communicate instantly while avoiding SMS fees, create groups so that you can chat in real time with all your friends at once, and share media or attachments all with complete privacy. The server never has access to any of your communication and never stores any of your data.

- ★ Private. TextSecure uses an advanced end to end encryption protocol for all of your messages that provides privacy for every message every time.
- ★ Open Source. TextSecure is Free and Open Source, enabling anyone to verify its security by auditing the code. TextSecure is the only private messenger that uses open source peer-reviewed cryptographic protocols to keep your messages safe.
- ★ Group Chat. TextSecure allows you to create encrypted groups so you can private conversations with all your friends at once. Not only are the messages encrypted, but the TextSecure server never has access to any group metadata such as the membership list, group title, or group icon.
- ★ Group Chat. TextSecure allows you to create encrypted groups so you can private conversations with all your friends at once. Not only are the messages encrypted, but the TextSecure server never has access to any group metadata such as the membership list, group title, or group icon.
- ★ Fast. The TextSecure protocol is designed to operate in the most constrained environment possible. Using TextSecure, messages are instantly delivered to friends.

Please file any bugs, issues, or feature requests at:
<https://github.com/whispersystems/textsecure/issues>

More details:
http://www.whispersystems.org/#encrypted_texts

Read more

Reviews

4.4

★ ★ ★ ★ ★

2,301 total

★ 51,445


★ 4487

★ 3201

★ 288


★ 180

Write a Review




Silent failure When it works, it works well: this is as user-friendly an encryption system as I've ever seen.

Phillip de Wet ★ ★ ★ ★ ★




Awesome Awesome. Just live it, especially alder new visual UI refresh. It's lovely and works great. Well done

Dominik Bieszczad ★ ★ ★ ★ ★



Great so far, just a few suggestions! I'm loving it so far, just a couple of suggestions: 1) Add a '+' for

Ben Silber ★ ★ ★ ★ ★



Fairly easy to use. Love the encryption. Ui could New update: better look but the color green should

Jeremy Wiedemann ★ ★ ★ ★ ★

What's New

Changes in 2.0:

- ★ Support for push messages.
- ★ Encrypted group chat.
- ★ Large visual refresh.

Changes in 1.0.6:

- ★ Display notifications for encrypted messages even when not default messaging app on KitKat+.
- ★ Fix for MMS messages that could get dropped on KitKat in some cases.
- ★ Minor style adjustments and improvements.

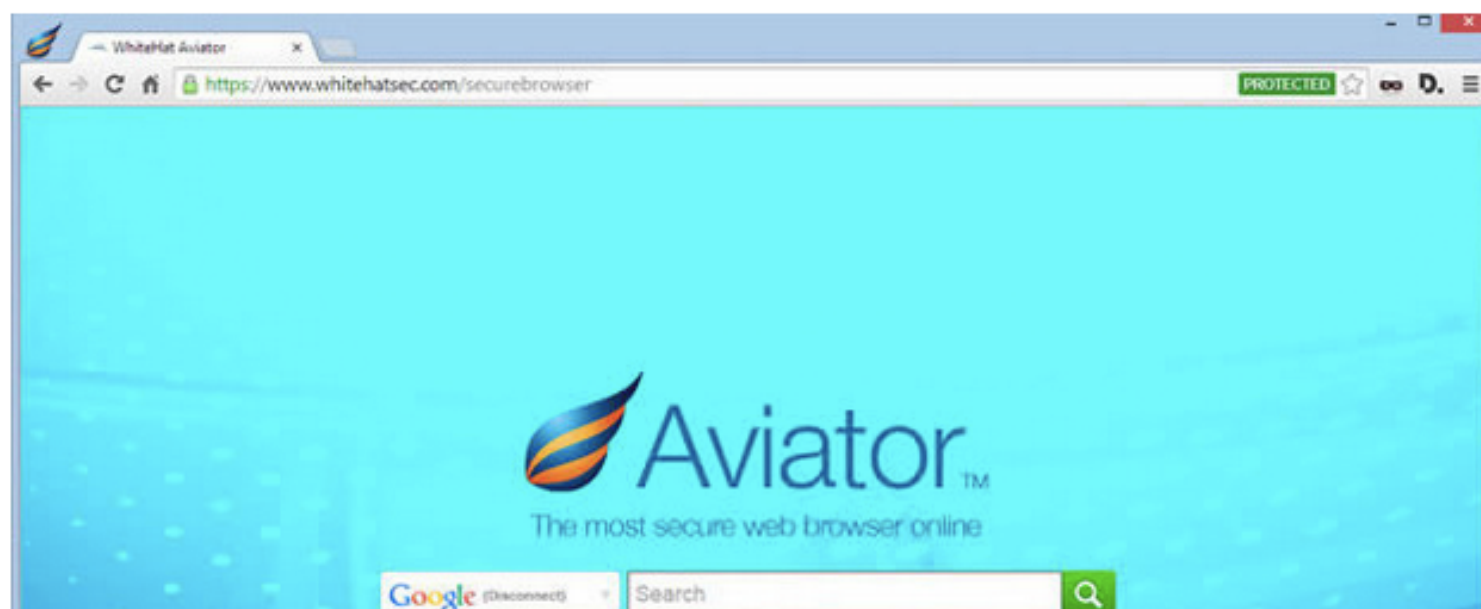
Additional information

Updated	Size	Installs	Current Version	Requires Android	Content Rating
February 24, 2014	3.6M	100,000 - 500,000	2.0	2.3 and up	Everyone

Contact Developer

NEWS ANALYSIS

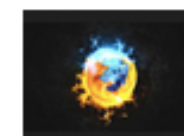
Are you using the most secure and private web browser?



MORE LIKE THIS



The paranoid's survival guide, part 1: How to protect your personal data



Mozilla tells Google, it's not you (anymore), it's Yahoo



5 clouds for building mobile apps

tom'sGUIDE
TECH FOR REAL LIFE

SEARCH TOM'S GUIDE



Sign In with

Facebook Twitter Google+
Sign up | Sign in

TAGS: Android Security Wearables Apps Gaming TVs Cameras Smartphones Tablets Software 3D Printing More ▼

Aviator: Hands-On With the Most Secure Web Browser

16
COMMENTS

By Jill Scharr FEBRUARY 12, 2014 5:00 AM



Tavis Ormandy @taviso · Jan 9

Well that didn't take long ;-)
github.com/WhiteHatSecuri... =>
google.com/;/Applications...



149



118



[View summary](#)



Justin Schuh

Shared publicly - Jan 9, 2015

[#chrome](#)

You probably shouldn't be using the WhiteHat Aviator browser if you're concerned about security and privacy.

I want to be clear that I'm very happy people can take Chromium and build something better on top of it. That's a big part of why Chromium is open source—to encourage community contributions and third-party innovation. And I want to commend WhiteHat on releasing the source to their fork, because that allows more honest discussion and the potential for shared innovations. But I also feel compelled to stress that building a safe browser is a very hard thing to do, which is why Chrome Security has roughly 30 full-time members and Chrome Privacy has another dozen or so themselves—and none of us are ever short on work.



Tavis Ormandy @taviso · Jan 9

Well that didn't take long ;-)
github.com/WhiteHatSecuri... =>
google.com/;/Applications...



149



118



[View summary](#)



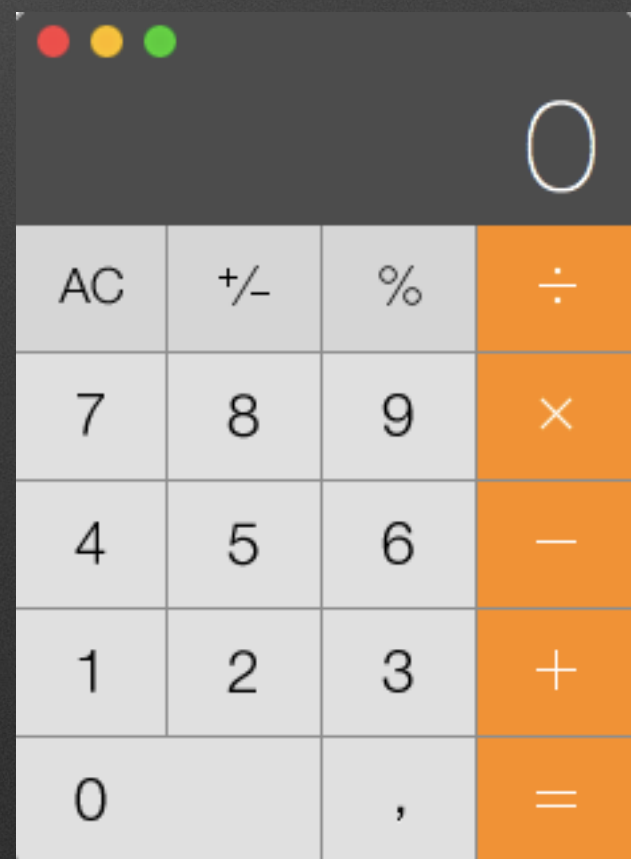
Justin Schuh

Shared publicly - Jan 9, 2015

[#chrome](#)

You probably shouldn't be using the WhiteHat Aviator browser if you're concerned about security and privacy.

I want to be clear that I'm very happy people can take Chromium and build something better on top of it. That's a big part of why Chromium is open source—to encourage community contributions and third-party innovation. And I want to commend WhiteHat on releasing the source to their fork, because that allows more honest discussion and the potential for shared innovations. But I also feel compelled to stress that building a safe browser is a very hard thing to do, which is why Chrome Security has roughly 30 full-time members and Chrome Privacy has another dozen or so themselves—and none of us are ever short on work.





Intelligence Feeds

Incentives

part of the reason for the market
failures



halvarflake

@halvarflake



Following

Managers get promoted by shipping software. By the time horrific security debt becomes evident, years have passed.



RETWEETS

40

FAVORITES

23



6:56 PM - 13 Feb 2015



Unbreakable
Linux





Emile Trombetti @EmileTrombetti · 4h

Oracle's data redaction security trashed at Defcon 22
siliconangle.com/blog/2014/08/1...

Retweeted by Frank Koehntopp and 1 other



iarce @4Dgifts · Aug 7

Oracle isnt unbreakable but it consistently wins every race to the bottom there is in infosec disclosures.house.gov/ld/ldxmlreleas...
No Pwnie for this?

Expand

← Reply ↻ Retweet ★ Favorite ... More



Followed by Tom Keetch and 1 other



Threatpost @threatpost · Aug 7

Oracle Database Redaction 'Trivial to Bypass' - threatpost.com/oracle-databas...

Expand

← Reply ↻ Retweet ★ Favorite ... More

Retweeted by David Litchfield



DennisF @DennisF · Aug 7

The triumphant return of @dlitchfield threatpost.com/oracle-databas...

Expand

← Reply ↻ Retweet ★ Favorite ... More

Retweeted by Stefano Zanero and 2 others



David Litchfield @dlitchfield · Aug 6

I'll be discussing why **Oracle** get a F for security (with demos) at 2:15pm in Lagoon K. Swing by if you're interested. [#blackhat](#)

Expand

← Reply ↻ Retweet ★ Favorite ... More



Dheeraj Pandey

@trailsfootmarks

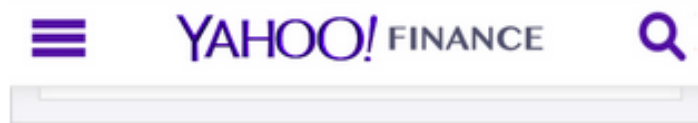
Share



Follow

One of the best comebacks in tech history.
#Oracle

Reply Retweet Favorite More



After Hours 41.69 0.00 (0.00%) 5:51PM EDT

As of 4:00PM EDT

ORCL ★ Follow

41.69

Oracle Corporation

-0.24 -0.57%



Prev Close	41.93	High	41.97
Open	41.89	Low	41.32
Volume	15.5m	52 Wk High	42.17
Mkt Cap	185.89B	52 Wk Low	29.86

RETWEETS

113

FAVORITES

87



11:51 PM - 4 Aug 2014

Flag media

Impact on Company Stock following Data Breaches

Posted on [July 21, 2014](#) by [Sean Mason](#) · [1 Comment](#)

Over the years I've seen a disturbing trend, where there must be a school where vendors and information security professionals are taught to invoke fear into business leaders by claiming that an incident will have a severe impact on its stock price. Considering most companies and its leaders are measured on the stock price, this is a very strong statement. I've personally never quite believed this and decided to take some time out to dive into the stock impact of some breaches to see if this truly is a concern. Keep in mind there is nothing scientific about this data and it doesn't take into account repercussions over the long haul from incidents stemming related to nation state espionage (Perhaps that is another research endeavor).

Company	Stock	Breach Announcement				Week After				Today	
		Date	Open	Close	% Change	Low	High	Close	% Change	Close	% Change
RSA/EMC	EMC	3/17/2011	25.84	25.56	1.08%	25	26.53	25.63	0.27%	26.11	2.15%
Lockheed	LMT	3/17/2011	79.79	80.41	0.78%	78.2	81.49	80.53	0.15%	200.24	149.02%
Sony ('11)	SNE	4/20/2011	30.03	30.14	0.37%	27.85	30.26	28.31	6.07%	25.71	14.70%
Google	GOOG	1/10/2012	298.74	294.94	1.27%	286.66	301.93	289.71	1.77%	554.16	87.89%
LinkedIn	LNKD	6/6/2012	93.17	93.08	0.10%	88	96.35	96.26	3.42%	258.17	177.36%
Adobe	ADBE	10/3/2013	51.61	50.88	1.41%	50.02	52.48	51.57	1.36%	77.98	53.26%
Target	TGT	12/18/2013	62.52	63.55	1.65%	61.44	63.59	62.49	1.67%	80.44	26.58%
eBay	EBAY	5/21/2014	50.86	51.88	2.01%	50.3	52.46	52.02	0.27%	59.79	15.25%
JP Morgan	JPM	8/27/2014	59.85	59.59	0.43%	58.81	59.95	59.45	0.23%	61.63	3.42%
Home Depot	HD	9/2/2014	93.04	91.15	2.03%	88.98	93.31	91.61	0.50%	115.93	27.19%
Staples	SPLS	10/20/2014	11.99	12.3	2.59%	11.93	12.6799	12.505	1.67%	16.01	30.16%
Sony ('14)	SNE	11/24/2014	21.22	21.63	1.93%	21.22	22.05	21.99	1.66%	25.71	18.86%

<https://docs.google.com/a/thinkst.com/spreadsheets/d/1IJYWaJLJ8IPTcjabUr1d4ZOaNeHnIbcwgufaQgLtKqE/edit#gid=0>



infosec
ISLAND

SECURITY
INTERNET AND ENT

[Front Page](#)

[Blog Posts](#)

[Resources](#)

[Media](#)

[Whitepapers](#)

[Visit SecurityWeek](#)

Sony Stock Hammered in Wake of Security Breaches

Monday, June 06, 2011

The Washington Post

Search



[Sign In](#)

[Economy](#)

Home Depot's profits rise, suggesting data breach hasn't led customers to flee



A



0

November 18, 2014

RETAIL

Home Depot reports increased profits

Home Depot's third-quarter profit rose 14 percent as comparable-store

Get Today's Headlines

Daily updates delivered just for you.

E-mail address

[Add](#)

Advertisement

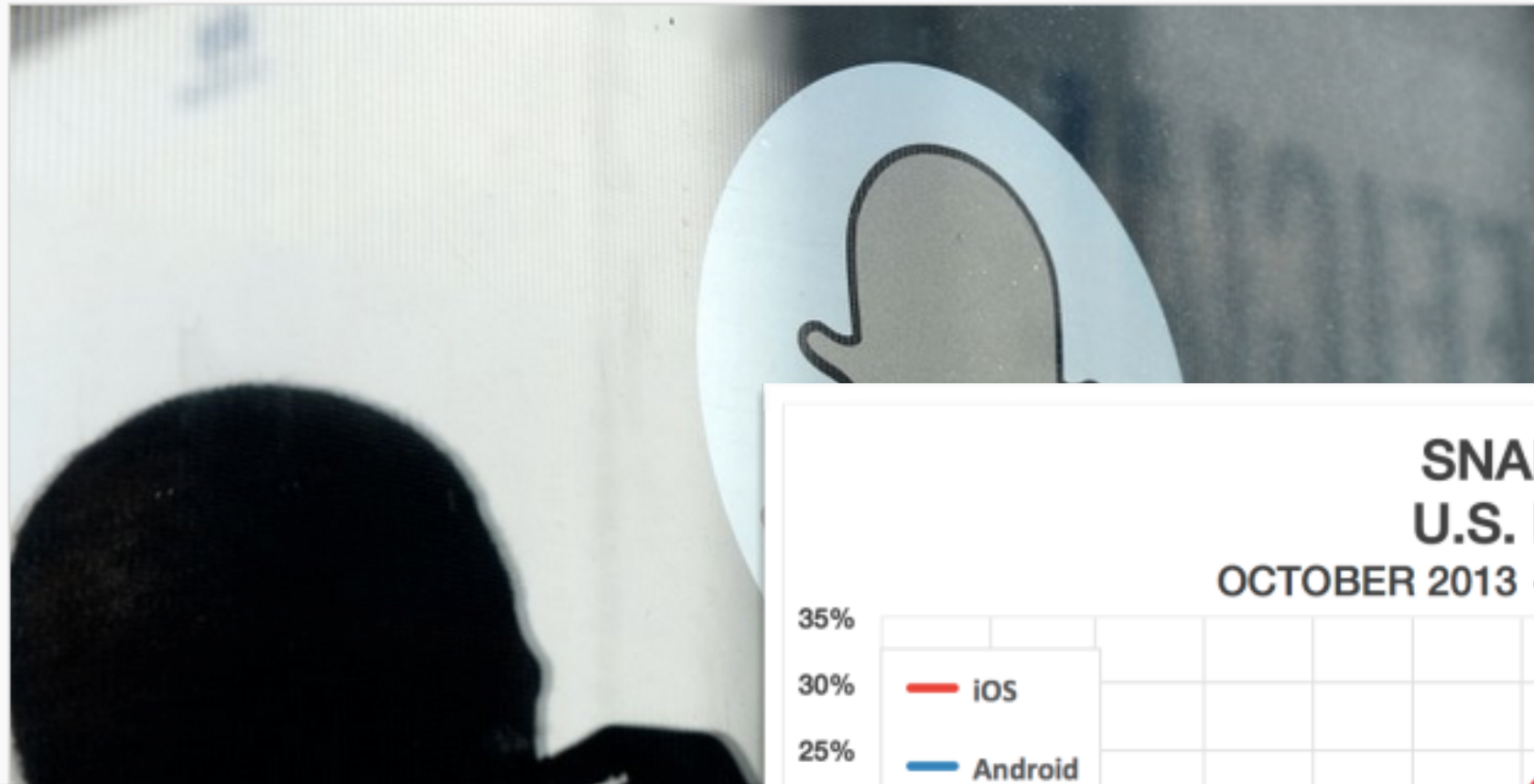


The “Snappening” Had No Impact On Snapchat Growth, Usage Or Engagement

Posted Dec 23, 2014 by [Sarah Perez \(@sarahintampa\)](#)

531

SHARES

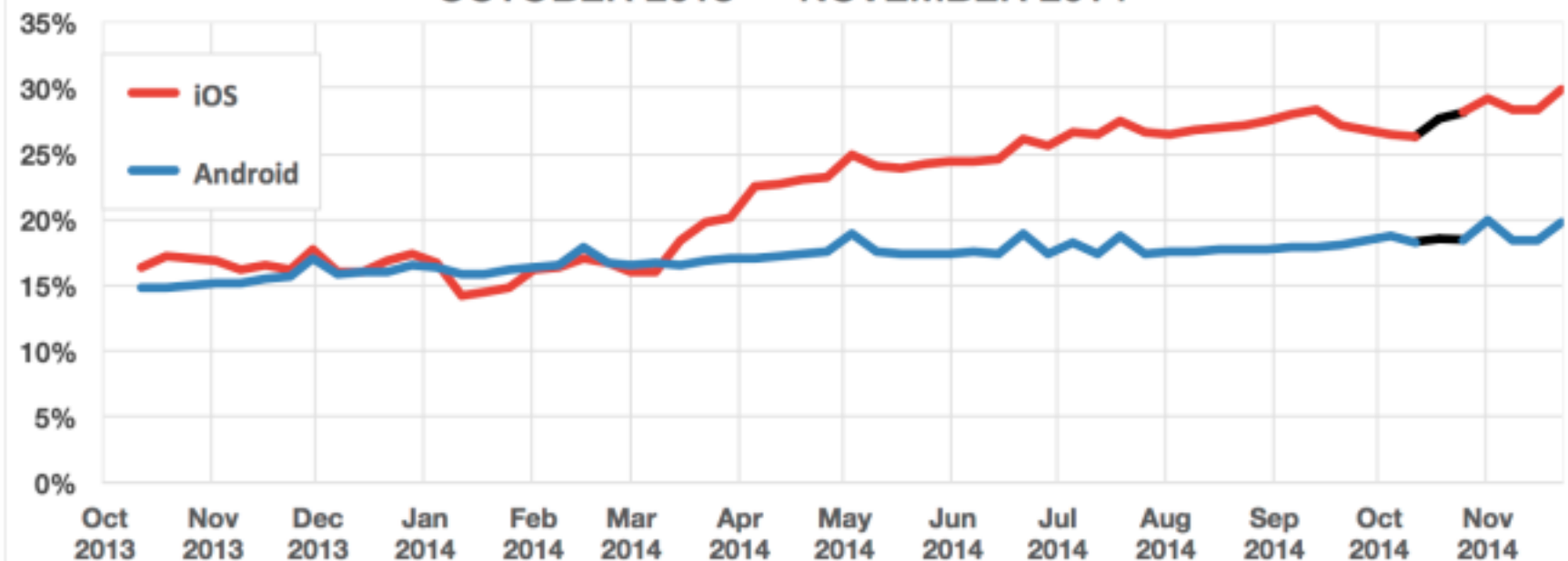


ADVERTISEMENT



SNAPCHAT U.S. REACH OCTOBER 2013 — NOVEMBER 2014

7PARK
DATA



Data: Monthly active users (MAU) of SnapChat as a percentage of millions of iOS and Android users in the U.S. between October 2013 and November 2014. Data sources include Mobidia.

7Park Data's App Intelligence Platform leverages international panels of millions of anonymous iOS and Android device users to deliver meaningful and actionable insights into mobile app usage and engagement with unparalleled granularity and scale. Sourced from independent data providers and cross-referenced to ensure quality and accuracy, businesses around the world rely on exclusive 7Park Data intelligence to inform strategic business decisions. Learn more at www.7parkdata.com.

ORGANIZATIONS

CSO Role Complexity

For people accustomed to think that plans of campaign and battles are made by generals—as any one of us sitting over a map in his study may imagine how he would have arranged things in this or that battle—the questions present themselves: Why did Kutúzov during the retreat not do this or that? Why did he not take up a position before reaching Fili? Why did he not retire at once by the Kaluga road, abandoning Moscow? and so on. People accustomed to think in that way forget, or do not know, the inevitable conditions which always limit the activities of any commander in chief. The activity of a commander in chief's does not at all resemble the activity we imagine to ourselves when we sit at ease in our studies examining some campaign on the map, with a certain number of troops on this and that side in a certain known locality, and begin our plans from some given moment. A commander in chief is never dealing with the *beginning* of any event—the position from which we always contemplate it. The commander in chief is always in the midst of a series of shifting events and so he never can at any moment consider the whole import of an event that is occurring. Moment by moment the event is imperceptibly shaping itself, and at every moment of this continuous, uninterrupted shaping of events the commander in

A commander in chief's business, it would seem, is simply to choose one of these projects. But even that he cannot do. Events and time do not wait. For instance, on the twenty-eighth it is suggested to him to cross to the Kalúga road, but just then an adjutant gallops up from Milorádovich asking whether he is to engage the French or retire. An order must be given him at once, that instant. And the order to retreat carries us past the turn to the Kalúga road. And after the adjutant comes the commissary general asking where the stores are to be taken, and the chief of the hospitals asks where the wounded are to go, and a courier from Petersburg

how do we calculate risk?

most parts of the business cant
evaluate the risks (because they
don't know whats possible)

reporting breach costs by social
security numbers lost

security is often hilariously bad
at business thinking



RISKY.BIZ

It's a jungle out there

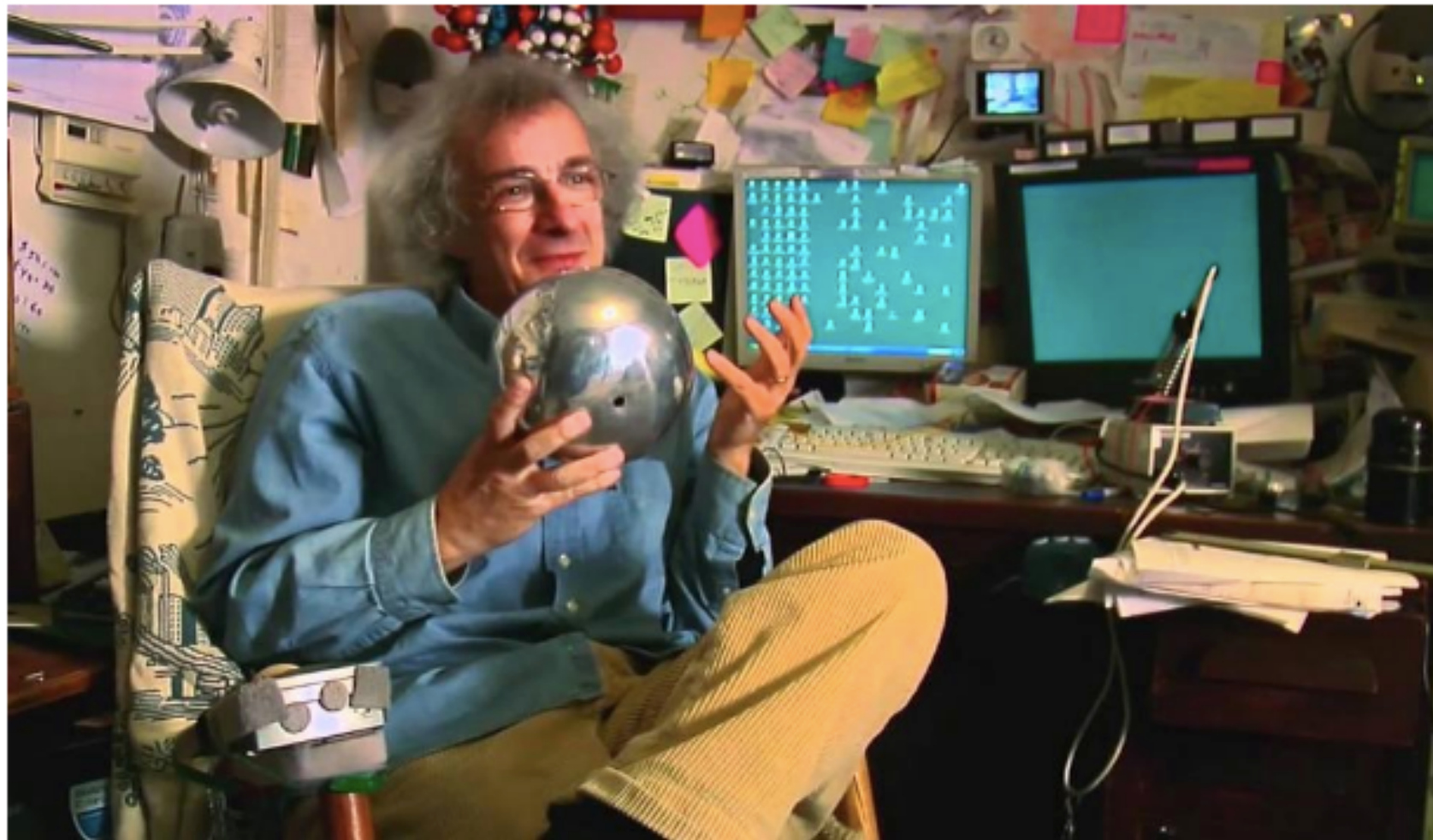


Square



Why the Web Won't Be Nirvana

BY **CLIFFORD STOLL** 2/26/95 AT 7:00 PM



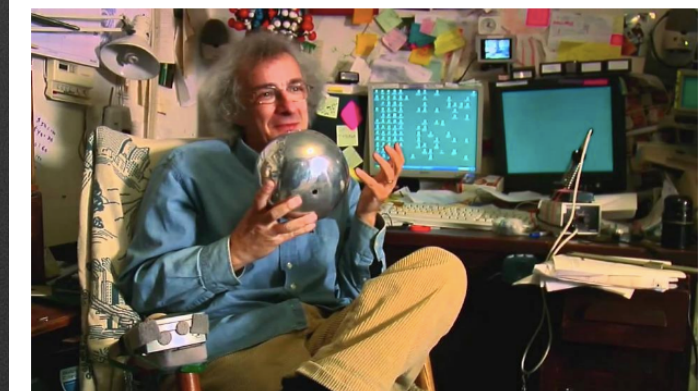
Clifford Stoll YOUTUBE

Visionaries see a future of telecommuting workers, interactive libraries and multimedia classrooms. They speak of electronic town meetings and virtual communities. Commerce and business will shift from offices and malls to networks and modems. And the freedom of digital networks will make government more democratic.

Baloney. Do our computer pundits lack all common sense? The truth is no online database will replace your daily newspaper, no CD-ROM can take the place of a competent teacher and no computer network will change the way government works.

Why the Web Won't Be Nirvana

BY CLIFFORD STOLL 2/26/95 AT 7:00 PM

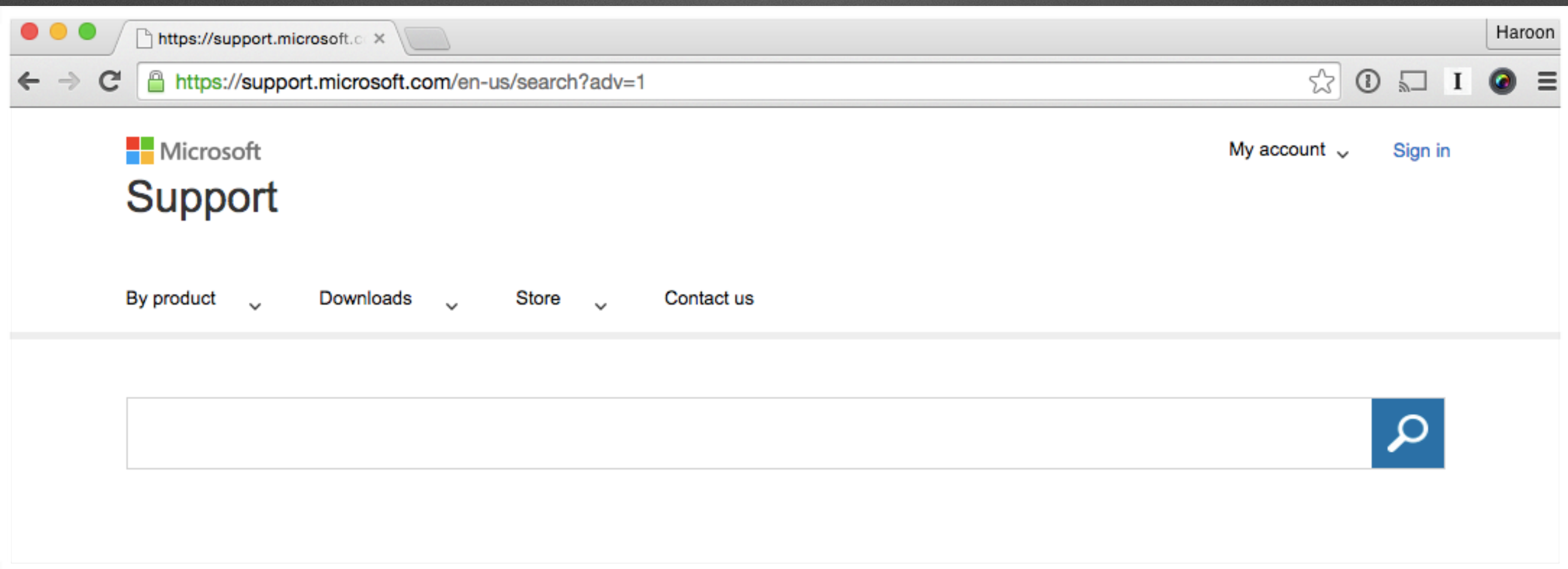


Clifford Stoll YOUTUBE

most everyone shouts, few listen. How about electronic publishing? Try reading a book on disc. At best, it's an unpleasant chore: the myopic glow of a clunky computer replaces the friendly pages of a book. And you can't tote that laptop to the beach. Yet Nicholas Negroponte, director of the MIT Media Lab, predicts that we'll soon buy books and newspapers straight over the Internet. Uh, sure.



mixed reporting lines



You can't buy security!

PEOPLE

expertise is niche

overview is rare

the bigger problem, is that you
never really know what you have?



openssl is wr



openssl is written by monkeys

openssl wrong number of fields on line 1

openssl wrong final block length

openssl wrong version number

Press Enter to search.



thinkst
applied research

Please Put OpenSSL Out of Its Misery - ACM Queue

queue.acm.org/detail.cfm?id=2602816 ▼

by PH Kamp - Cited by 3 - Related articles

Apr 12, 2014 - The **OpenSSL** software package is around 300,000 lines of **code**, ... If those bugs were unique to your computer, that wouldn't be too **bad**.

OpenSSL code beyond repair, claims creator of "LibreSSL ...

lwn.net/Articles/595639/ ▼

Apr 22, 2014 - Since the goal of LibreSSL is thoroughly overhaul **OpenSSL code** it may well be OpenVMS also is blamed for **bad code** in **OpenSSL**.

Post-Heartbleed: Is it time to kill OpenSSL? - TechRadar

www.techradar.com/.../post-heartbleed-is-it-time-to-consider-an-alternati... ▼

May 12, 2014 - "And that brings me back to **OpenSSL** — which **sucks**. The **code** is a mess, the documentation is misleading, and the defaults are deceptive.

OpenSSL insecure and has been for two years. - Industry ...

vpsboard.com › [vpsBoard](#) › [Industry News](#) ▼

Apr 8, 2014 - 8 posts - 8 authors

Should be new updates for **OpenSSL** pushed out today... and other ... Just call it a

Please Put OpenSSL Out of Its Misery - ACM Queue

queue.acm.org/detail.cfm?id=2602816 ▼

by PH Kamp - Cited by 3 - Related articles

Apr 12, 2014 - The **OpenSSL** software package is around 300,000 lines of **code**, ... If those bugs were unique to your computer, that wouldn't be too **bad**.

OpenSSL code beyond repair, claims creator of "LibreSSL ...

lwn.net/Articles/595639/ ▼

Apr 22, 2014 - Since the goal of LibreSSL is thoroughly overhaul **OpenSSL code** it may well be OpenVMS also is blamed for **bad code** in **OpenSSL**.

Post-Heartbleed: Is it time to kill OpenSSL? - TechRadar

www.techradar.com/.../post-heartbleed-is-it-time-to-consider-an-alternati... ▼

May 12, 2014 - "And that brings me back to **OpenSSL** — which **sucks**. The **code** is a mess, the documentation is misleading, and the defaults are deceptive.

OpenSSL insecure and has been for two years. - Industry ...

vpsboard.com › [vpsBoard](#) › [Industry News](#) ▼

Apr 8, 2014 - 8 posts - 8 authors

Should be new updates for **OpenSSL** pushed out today... and other ... Just call it a

Home

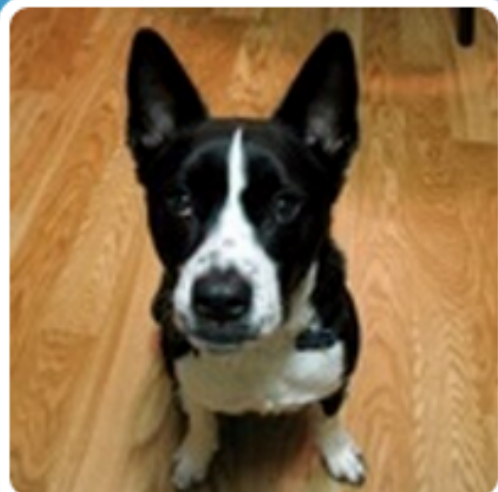
Notifications

Messages

Discover



Search Twitter



Justin Schuh

@justinschuh

I work on Google Chrome Security.
(Disclaimer: My views are my own, but
they are available for license under
FRAND terms)

📍 Silicon Valley

🔗 google.com/+JustinSchuh

🕒 Joined September 2009

✉ Tweet to Justin Schuh

👤 234 Followers you know

TWEETS
1,001

FOLLOWING
223

FOLLOWERS
3,170

FAVORITES
102



Following

Tweets

Tweets & replies

Photos & videos



Justin Schuh @justinschuh · 4h

Wow, yahoo.com went HSTS. Had to switch
to microsoft.com for a captive portal login
[#HTTP4EVER](https://twitter.com/hashtag/HTTP4EVER)



16



27

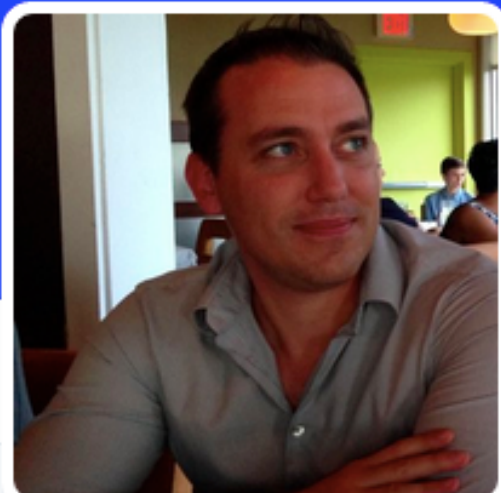


Justin Schuh retweeted



John Lambert @JohnLaTwC · Mar 15

If you hide your analysts from your competition, remember that you share
adversaries. Cooperate on adversaries, compete on business.

TWEETS
2,660FOLLOWING
550FOLLOWERS
17.6KFAVORITES
32

Follow

RSnake

@RSnake

Computer security enthusiast, defender of others' privacy, VP of labs, often found joking.

Austin, TX

detectmalice.com

Joined July 2008

Tweet to RSnake

492 Followers you know



Tweets

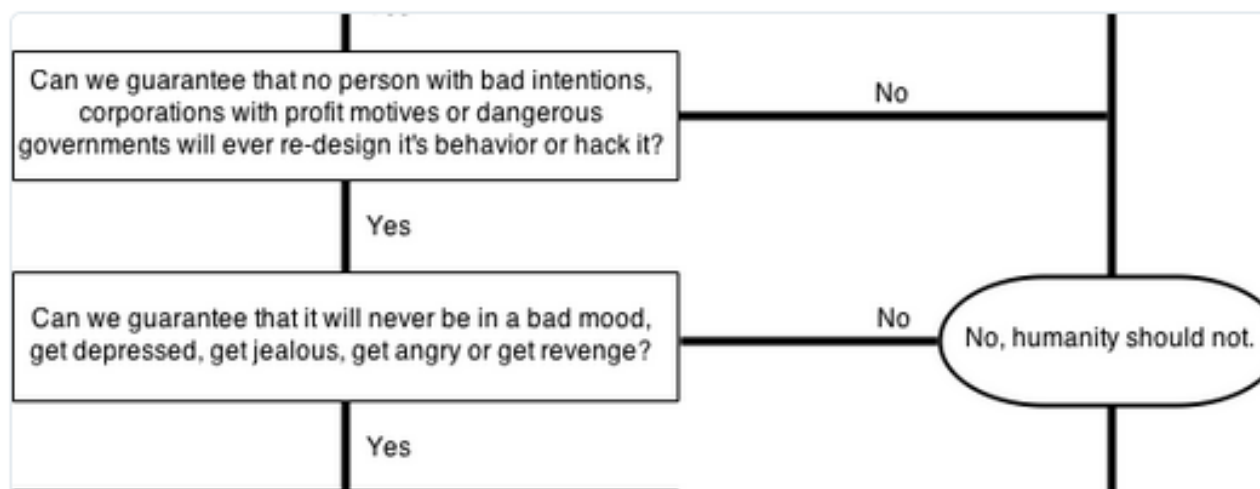
Tweets & replies

Photos & videos



RSnake @RSnake · Mar 16


Some thoughts on AI and if humanity should pursue it:



Jeremiah Grossman (@jeremiahg)


Twitter, Inc. [US] https://twitter.com/jeremiahg/

HomeNotificationsMessagesDiscoverSearch Twitter



SENTINEL
WE SECURE THE WEB
APPLICATION VULNERABILITIES BEFORE THE BAD GUYS EXPLOIT THEM

SENTINEL ELITE
GUARANTEE YOUR SECURITY



TWEETS23.5K

FOLLOWING270

FOLLOWERS58.1K

FAVORITES58

Following

Jeremiah Grossman
@jeremiahg
FOLLOWS YOU

Founder & iCEO of WhiteHat Security, Hacker, Black Belt in Brazilian Jiu-Jitsu, and Off-Road Race Car Driver.


Maui, Hi

facebook.com/jeremiahgrossm...

Joined March 2008

TweetsTweets & repliesPhotos & videos


Jeremiah Grossman retweeted

**chenxi wang** @chenxiwang · now
@jeremiahg This is an "imply" op. Imply is only true if the contraposition is true. U can see clearly the contraposition of this isn't true.

11

View conversation

Jeremiah Grossman retweeted

**Mary Branson** @marybranson · now

we don't have enough people

The Scarcity Problem

Employee scarcity is the term that describes employers being unable to recruit sufficient talent in a given niche to fill their requirements. Employee scarcity is generally said to occur if, adjusting for lower-than-market wages and other recruiting path issues, positions remain unfilled for more than one month.¹² This measure of scarcity has been repeatedly validated through peer-reviewed study since the 1980s.

In the cybersecurity arena, there is a general sense that hiring is difficult, and the numbers back that conclusion up. With more than one million cybersecurity positions unfilled worldwide,³ currently-identified security needs couldn't be met if every employee at GM,⁴ Costco,⁵ Home Depot,⁶ Delta,⁷ and Procter & Gamble⁸ became security experts tomorrow. Those one million positions span industries, specializations, and requirements; in addition, approximately 25,000 of them are in the United States' federal civil service.⁹ These non-military government agencies, in addition to the general difficulty of hiring security personnel at this time, have the added complicating factor of not being able to raise their salaries in response to market conditions. While some authors tout the idea that working for the government brings side benefits that private industry cannot match (such as a sense of giving back to the community and country), these benefits are apparently insufficient to meet the current demand. The military is also interested in locating additional cybersecurity experts, but their approach is to produce them internally (through rating schools and other educational methods), rather than sourcing them externally, so their numbers and internal recruiting concerns are not included in this analysis.

To be clear, this is a global problem which affects every country, regardless of apparent level of technological integration. Few countries' governments can match private salaries, and even private industry is unable to hire sufficient security expertise to meet the demand.

WITH MORE THAN ONE MILLION
CYBERSECURITY POSITIONS
UNFILLED WORLDWIDE,
CURRENTLY-IDENTIFIED SECURITY
NEEDS COULDN'T BE MET
IF EVERY EMPLOYEE AT GM,
COSTCO, HOME DEPOT, DELTA,
AND PROCTER & GAMBLE
BECAME SECURITY EXPERTS
TOMORROW.



...With more than one million cyber security positions unfilled worldwide, currently identified security needs couldn't be met if every employee at GM, Costco, Home Depot, Delta, and Procter & Gamble became security experts tomorrow.

The Scarcity Problem

Employee scarcity is the term that describes employers being unable to recruit sufficient talent in a given niche to fill their requirements. Employee scarcity is generally said to occur if, adjusting for above-market wages and other recruiting path issues, positions remain unfilled for more than one month.¹¹ This measure of scarcity has been repeatedly validated through peer-reviewed study since the 1960s.

In the cybersecurity arena, there is a general sense that hiring is difficult, and the numbers back that conclusion up. With more than one million cybersecurity positions unfilled worldwide,¹² currently identified security needs couldn't be met if every employee at GM,¹³ Costco,¹⁴ Home Depot,¹⁵ Delta,¹⁶ and Procter & Gamble¹⁷ became security experts tomorrow. These one million positions span industries, specializations, and requirements; in addition, approximately 25,000 of them are in the United States' federal civil service.¹⁸ These non-military government agencies, in addition to the general difficulty of hiring security personnel at this time, have the added complicating factor of not being able to raise their salaries in response to market conditions. While some authors tout the idea that working for the government brings side benefits that private industry cannot match (such as a sense of giving back to the community and country), these benefits are apparently insufficient to meet the current demand. The military is also interested in locating additional cybersecurity experts, but their approach is to produce them internally through rising schools and other educational methods, rather than sourcing them externally, so their numbers and internal recruiting concerns are not included in this analysis.

To be clear, this is a global problem which affects every country regardless of apparent level of technological integration. Few countries' governments can match private salaries, and even private industry is unable to hire sufficient security expertise to meet the demand.

WITH MORE THAN ONE MILLION CYBERSECURITY POSITIONS UNFILLED WORLDWIDE, CURRENTLY IDENTIFIED SECURITY NEEDS COULDN'T BE MET IF EVERY EMPLOYEE AT GM, COSTCO, HOME DEPOT, DELTA, AND PROCTER & GAMBLE BECAME SECURITY EXPERTS TOMORROW.



don't get better like craftsmen



We lose great people:

We lose great people:

- leave the Industry
- to offense
- to “the scene”

losing ppl to “offence”

offense _is_ “easier”

defenders need to give a lot of
bad news

fewer competing goals

We lose great people:

- leave the Industry
- to offense
- to “the scene”

our scene:

who have we been solving for?

we have a huge part to play in
the whole NSA/IC mess

conference talks & stunt hacking

the 0day rule
(instead of the golden rule!)

XSS - Lame!
STUXNET - Lame!
Client Side Exploits - Lame!

OMG CHINA!!!1 1!!

So in Summary so far..

We have really hard problems..

from fundamental computer
science problems,

to pathological market failure

to deep rooted sociology
problems

“I think information security is quite possibly the most intellectually challenging profession on the planet”

-Dan Geer

“but you are probably conning
yourself if you think this applies to
what you are doing!”

-me

so the central thesis of this talk..

infosec can be really hard..

&&

infosec can be really important..

but many of us are not working on
the problems that are really hard or
really important

the problems we chose to focus
on, are not necessarily the
problems we needed to focus on

dopamine hits with conference talks

http://thinkst.com/stuff/44Con_2013/talk_about_talks.pdf

<https://www.youtube.com/watch?v=BIVjdUkrSFY>

feeling good about ourselves
doing pen-testing

<http://www.youtube.com/watch?v=GvX52HPAfBk>

<http://thinkst.com/resources/slides/44con-final.pdf>



but we are not significantly moving
the needle on the real problems

Conducted a Pen-Test in
the past 2 years ?

How many 0-days would I
need to access your crown
jewels?

Most Common Answer: 1

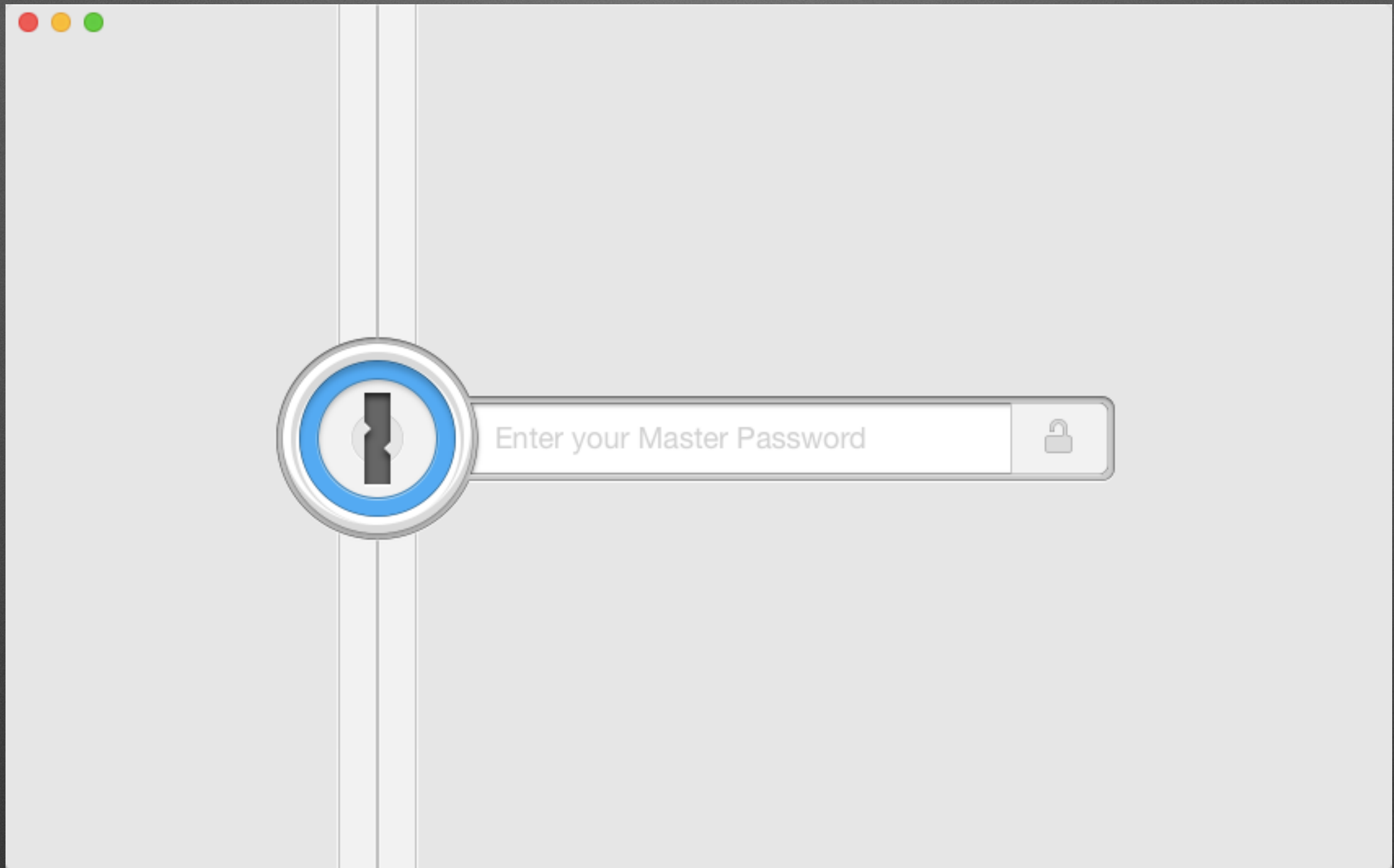


we need to get over our
entitlement

Security needs to be included

why ?

we need to refocus some
research



Killing the Rootkit

By Shane Macaulay

Cross-platform, cross-architecture DKOM detection

To know if your system is compromised, you need to find everything that could run or otherwise change state on your system and verify its integrity (that is, check that the state is what you expect it to be).

“Finding everything” is a bold statement, particularly in security, rootkits, and advanced threats. Is it possible the short answer is no, it’s not. Strangely, the long and

By defining the execution environment at any point in through the use of hardware-based hypervisor or virtual verify the integrity of that specific environment using of hashing.

Process-based Page Table Detection

Any given page of memory could be a page table. Typically a page table is organized as a series of page table entries (PTEs). These entries are usually traversed by selecting some bits from a virtual address and converting them into a series of table lookups.

The magic of this technique comes from the propensity of all OS (at least **Windows**, **Linux**, and BSD) to organize their page tables into virtual memory. That way they can use virtual addresses to edit PTEs instead of physical memory addresses.

```
7: kd> .formats FFFFF6FB7DBEDF68
```

```
Binary: 111111111111111111110110111101101111011011110110111101101000
```

Sign extend	1111111111111111	
PML4 offset	111101101	== 0x1ED
PDP offset	111101101	== 0x1ED
PD offset	111101101	== 0x1ED
Page table offset	111101101	== 0x1ED
Physical page offset	111101101000	== 0xF68 (0xF68 / 8 == 0x1ED)

there is a beautiful gap in the
market here!

between the customers we
have and ones we wish we had

we need to build the tools that
solve actual user problems

this gives us an opportunity to
make a difference & be relevant



Pinned Tweet



Dino A. Dai Zovi @dinodaizovi · Aug 16

"You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete."



41



29



thinkst
applied research

not slating offence..

back in 1999.. it was cool

today..

our future _is_ currently being
decided

- We are at an important inflection point
- We simultaneously face a crisis of relevance and a crisis of confidence
- We have important problems that need solving
- Our best ad brightest shouldn't be spending their time creating sideshows to distract and entertain the rest

we need you to show up and
choose a side..

throw your hat into the ring..

Questions?

@haroonmeer

<http://thinkst.com>