

Protecting our Online Privacy

Michalis Polychronakis
Stony Brook University

October 23, 2015

Login

Our digital interactions are being threatened

Systems get compromised

- Malware

- Malicious websites

- Targeted attacks

Private information is exposed to third parties

- Social networking

- Cloud services

- Eavesdropping

BUSINESS DAY

Millions of Anthem Customers Targeted in Cyberattack

By REED ABELSON and MATTHEW GOLDSTEIN FEB. 5, 2015



Outside the Anthem facility in Indianapolis. Anthem said it detected a data breach on Jan. 29, and that it was working with the Federal Bureau of Investigation. Aaron P. Bernstein/Getty Images

Anthem, one of the nation's largest health insurers, said late

National Security

Hackers breach some White House computers



Get the WorldViews newsletter

Sign up for daily updates from WorldViews.

Sign Up

Most Read World

1 Michelle Obama forgoes a headscarf and sparks a backlash in Saudi Arabia



2 The Islamic State's Dragunov sniper rifles, in photos

home > tech

Malware

International Space Station attacked by 'virus epidemics'

Malware spread from infected devices in orbit, proving not even computers in space are safe from viruses



Featured comment

In space, no one can see your blue screen.

alanredangel
12 Nov 2013

See more comments

THREAT LEVEL

cyberwar cyberwarfare stuxnet

FOLLOW WIRED



An Unprecedented Look at Stuxnet, the World's First Digital Weapon

BY KIM ZETTER 11.03.14 | 6:30 AM | PERMALINK

Share 4.3k Tweet 1,485 +1 129 in Share 693 Pin it



MOST RECENT WIRED POSTS



Facebook Just Had Another Record Quarter, and It Has Apple to Thank



Comcast Renames Man 'Asshole Brown' After He Tries to Cancel Cable



A Heroin Dealer Tells the Silk Road Jury What It Was Like to Sell Drugs Online



Amazon Challenges Google and Microsoft With Its Own Email Service



These Are the Hottest New Open Source Projects Right Now



Canada Joins World Powers in...

home > tech

Computing

US police force pay bitcoin ransom in Cryptolocker malware scam

Unprepared officials blindsided by sophisticated virus call experience 'an education'





New Rules in China Upset Western Tech Companies



STATE OF THE ART Uber's Business Model Could Change Your Work



ECONOMIC SCENE Job Licenses in Spotlight as Uber Rises



DEALBOOK After Alibaba Spinoff, Yahoo May Become a Takeover Target

Bits

Search Bits

SEARCH

SECURITY

Apple Says It Will Add New iCloud Security Measures After Celebrity Hack

By BRIAN X. CHEN SEPTEMBER 4, 2014 11:32 PM 21 Comments

PREVIOUS POST
Microsoft Introduces Three New Smartphones

NEXT POST
Daily Report: Apple Expected to Unveil Smartwatch and Larger iPhones

THE BITS DAILY UPDATE

Every weekday, **get the latest technology news**, analysis and buzz from around the web — delivered to your inbox.

[SIGN UP FOR OUR NEWSLETTER](#) See a Sample »

SCUTTLEBOT News from the Web, annotated by our staff

Netflix's Secret Special Algorithm Is a Human

NEW YORKER | His name, writes Tim Wu, is Ted Sarandos. - *Natasha Singer*

Uber Releases Study on Drunk Driving and Transportation

UBER BLOG | A new study released by the ride-hailing company claims it is having a "measurable impact on driving down alcohol-related crashes." - *Mike Isaac*



SAVE BIG SUBSCRIBE TODAY



Get The Atlantic on Facebook

- POLITICS
- BUSINESS
- TECH**
- ENTERTAINMENT
- HEALTH
- EDUCATION
- SEXES
- NATIONAL
- GLOBAL
- VIDEO
- MAGAZINE

JUST IN How Insurance Companies Still Discriminate Against the Sick PHOTO | FEATURES | APPS | BOOKS | NEWSLETTERS | EVENTS | SUBSCRIBE



The Netanyahu Disaster
By Jeffrey Goldberg



The Effects of Forgiveness
By Olga Khazan



Rural America's Silent Housing Crisis
By Gillian B. White



Introducing the Supertweet
By Ian Bogost

Armed With Facebook 'Likes' Alone, Researchers Can Tell Your Race, Gender, and Sexual Orientation

REBECCA J. ROSEN | MAR 12 2013, 2:59 PM ET

But the deeper aspects of your personality remain hard to detect.

- f
- t
- in
- ✉
- 📄
- 💬





VIDEO



How to Build a Tornado
A Canadian inventor believes his tornado machine could solve the world's energy crisis.

MORE IN TECHNOLOGY

 **Introducing the Supertweet**
IAN BOGOST

 **My Parents' Facebook Will**
JAKE SWEARINGEN



TECH 2/16/2012 @ 11:02AM | 2,698,356 views

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

+ Comment Now + Follow Comments

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. [Target](#), for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.



Target has got you in its aim

Charles Duhigg outlines in the [New York Times](#) how Target tries to hook parents-to-be at that crucial moment before they turn into rampant — and



Share



Next Post

BUSINESS DAY

410 COMMENTS

Attention, Shoppers: Store Is Tracking Your Cell

By STEPHANIE CLIFFORD and QUENTIN HARDY JULY 14, 2013

Email

Share

Tweet

Save

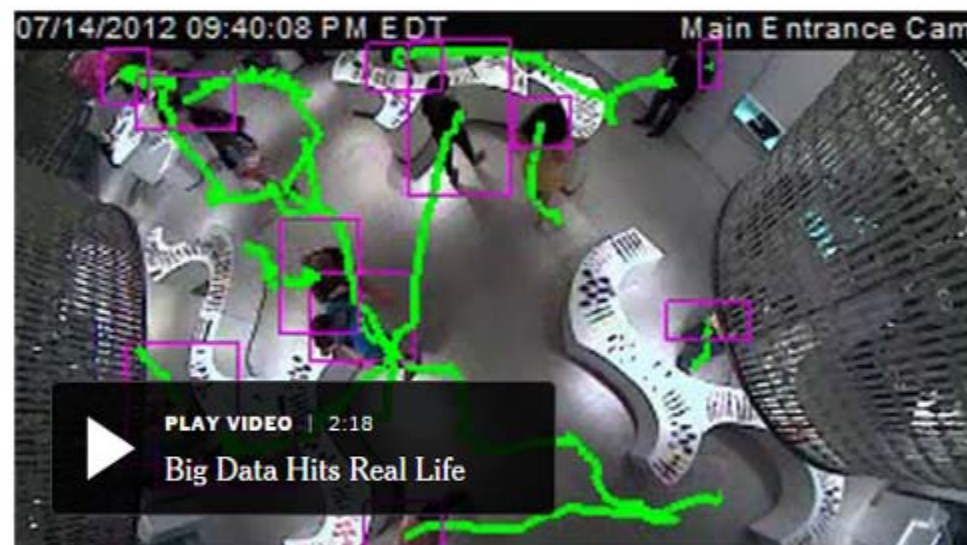
More

Like dozens of other brick-and-mortar retailers, [Nordstrom](#) wanted to learn more about its customers — how many came through the doors, how many were repeat visitors — the kind of information that e-commerce sites like Amazon have in spades. So last fall the company started testing new technology that allowed it to track customers' movements by following the Wi-Fi signals from their smartphones.

But when Nordstrom posted a sign telling customers it was tracking them, shoppers were unnerved.

"We did hear some complaints," said Tara Darrow, a spokeswoman for the store. Nordstrom ended the experiment in May, she said, in part because of the comments.

Nordstrom's experiment is part of a movement by retailers to gather data about in-store shoppers' behavior and moods, using video surveillance and signals from their cellphones and apps to learn



Brick-and-mortar stores are looking for a chance to catch up with their online competitors by using software that allows them to watch customers as they shop, and gather data about their behavior. Video by Erica Berenstein on July 14, 2013.

MINISTRY OF INNOVATION / BUSINESS OF TECHNOLOGY

AT&T charges \$29 more for gigabit fiber that doesn't watch your Web browsing

AT&T goes head to head against Google in KC on fiber and targeted ads.

by Jon Brodtkin - Feb 16, 2015 12:38pm EST

Share Tweet 205



AT&T

AT&T's gigabit fiber-to-the-home service has just **arrived in Kansas City**, and the price is the same as Google Fiber—if you let AT&T track your Web browsing history.

LATEST FEATURE STORY



FEATURE STORY (2 PAGES)

Battlefield Hardline review: an odd, cops-and-robbers facade

New twists on old formula help in multiplayer, baffle in single player.

WATCH ARS VIDEO



DONATE



Journalism in the Public Interest

Receive our top stories daily

Email address

SUBSCRIBE



Search ProPublica



Dragnets

Tracking Censorship and Surveillance



Verizon's Zombie Cookie Gets New Life

Verizon is merging its cellphone tracking supercookie with AOL's ad tracking network to match users' online habits with their offline details.

by *Julia Angwin and Jeff Larson*
ProPublica, Oct. 6, 2015, 1:15 p.m.

15 Comments | Print



This is part of an ongoing investigation:

Dragnets

ProPublica investigates the threats to privacy in an era of cellphones, data mining and cyberwar.



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

Enable Social Reading

Latest Stories in this Project



RISK ASSESSMENT / SECURITY & HACKTIVISM

SSL-busting code that threatened Lenovo users found in a dozen more apps

"What all these applications have in common is that they make people less secure."

by Dan Goodin - Feb 22, 2015 3:45pm EST

Share Tweet 126



LATEST FEATURE STORY



FEATURE STORY (2 PAGES)

Battlefield Hardline review: an odd, cops-and-robbers facade

New twists on old formula help in multiplayer, baffle in single player.

WATCH ARS VIDEO





GREATFIRE.ORG

SEARCH

TEST URL

TEST KEYWORD

FAQ

NEWS

中文

All Search

AUTHORITIES LAUNCH MAN-IN-THE-MIDDLE ATTACK ON GOOGLE

Submitted by percy on Thu, Sep 04, 2014

WHAT HAPPENED?

From August 28, 2014 reports appeared on Weibo and Google Plus that users in China trying to access google.com and google.com.hk via CERNET, the country's education network, were receiving warning messages about invalid SSL certificates. The evidence, which we include later in this post, indicates that this was caused by a man-in-the-middle attack.



While the authorities have been [blocking access to most things Google](#) since June 4th, they have kept their hands off of [CERNET](#), China's nationwide education and research network. However, in the lead up to the new school year, the Chinese authorities launched a man-in-the-middle (MITM) attack against Google.

We broke the news about the MITM attack on Github in January 2013. To borrow from that

Subscribe to our blog using [RSS](#).

COMMENTS

Submitted by Marty on Mon, Sep 22, 2014

It's amazing too pay a quick visit this site and reading

the views of all colleagues on tthe topic of this post, while I am also eager of gettingh knowledge.

Here is my page; effective weight, [Marty](#)

Submitted by subway surfers ... on Sat, Sep 27, 2014

I'm gone to convey my little brother, that he should also pay a quick visit this web site on regular basis to obtain updated from most recent gossip.

Submitted by Merissa on Sun, Sep 28, 2014

I think the admin of this site is genuinely working hard in support of his website, because here every stuff is





RISK ASSESSMENT / SECURITY & HACKTIVISM

French agency caught minting SSL certificates impersonating Google

Unauthorized credentials for Google sites were accepted by many browsers.

by Dan Goodin - Dec 9 2013, 2:05pm EST

Share Tweet 61



LATEST FEATURE STORY



FEATURE STORY (2 PAGES)

Want high-end flight sim pedals? Put \$500 in a Polish bank account and contact Slaw

Review: "Wait—\$500 for *just* the Slaw Device BF 109?" Well, yes, but what pedals!

WATCH ARS VIDEO





SECURITY 2/24/2015 @ 7:18AM | 13,489 views

How Hackers Abused Tor To Rob Blockchain, Steal Bitcoin, Target Private Email And Get Away With It

[+ Comment Now](#) [+ Follow Comments](#)

Across October and November of last year, some unlucky users of the world's most popular Bitcoin wallet, [Blockchain.info](#), and one of the better-known exchanges, [LocalBitcoins](#), had their usernames and passwords silently pilfered. They were robbed of significant sums, probably tens of thousands of dollars worth of the virtual currency, possibly more. Security-focused email services, [Riseup](#) and [Safe-mail](#) were also targeted by the same crew. And according to the man who witnessed the attacks go off last year, Digital Assurance director Greg Jones, it looks like buyers and sellers of [dark markets](#) were the targets.

The attackers used a tried-and-tested method to begin with, setting up a number of malicious [exit relays on Tor](#). Legitimate exit relays act as the final jump from the anonymising Tor network, which loops users through a number of randomly-chosen servers across the world to protect their identity, onto the clear web. But any nefarious type who runs a malicious relay can use an encryption removal technique known as [SSL stripping](#), where connections are



Share



Next Post

THREAT LEVEL

FOLLOW WIRED [Twitter] [Facebook] [RSS]

FBI Admits It Controlled Tor Servers Behind Mass Malware Attack

BY KEVIN POULSEN 09.13.13 | 4:17 PM | PERMALINK

[Share] 222 [Tweet] 98 [g+] 730 [in Share] 1 [PinIt]



MOST RECENT WIRED POSTS



Facebook Just Had Another Record Quarter, and It Has Apple to Thank



Comcast Renames Man 'Asshole Brown' After He Tries to Cancel Cable



A Heroin Dealer Tells the Silk Road Jury What It Was Like to Sell Drugs Online



Amazon Challenges Google and Microsoft With Its Own Email Service



These Are the Hottest New Open Source Projects Right Now



Canada Joins World Powers in

Privacy

“The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others.” [RFC2828]

Anonymity

“The state of being not identifiable within a set of subjects, the anonymity set.” [Pfitzmann and Köhntopp]

Very different from privacy:

An anonymous action may be public, but the actor's identity remains unknown (e.g., vote in free elections)

Real-world Privacy

Large-scale data collection examples

Credit cards, Metrocards, Loyalty cards

Street/public space cameras

E-ZPass

Named tickets

...

Part of our everyday activities and personal information is (voluntarily or compulsorily) recorded

Information from different sources can be **correlated**

Did you buy your Metrocard with your credit card?

The same happens in the online world...

Third parties have access to...

Our email (Gmail, Yahoo, ...)

Our files (Dropbox, Google Drive, ...)

Our communication (Skype, Facebook, ...)

Our traffic (WiFi hotspots, ISPs, ...)

Our location (3/4G, GPS, WiFi, ...)

Our preferences ("Likes," Amazon, Netflix, ...)

Our health (Fitbit, iWatch, 23andMe, ...)

...

What can we do?

Technical solutions exist

- Encryption

- Self-hosted services

- Anonymous communication

- ...



But they are not enough

- Privacy vs. usability tradeoff

- Wrong assumptions

- Implementation flaws

Many users are not even aware of privacy issues, let alone solutions

**Minimizing information disclosure
in social login platforms**

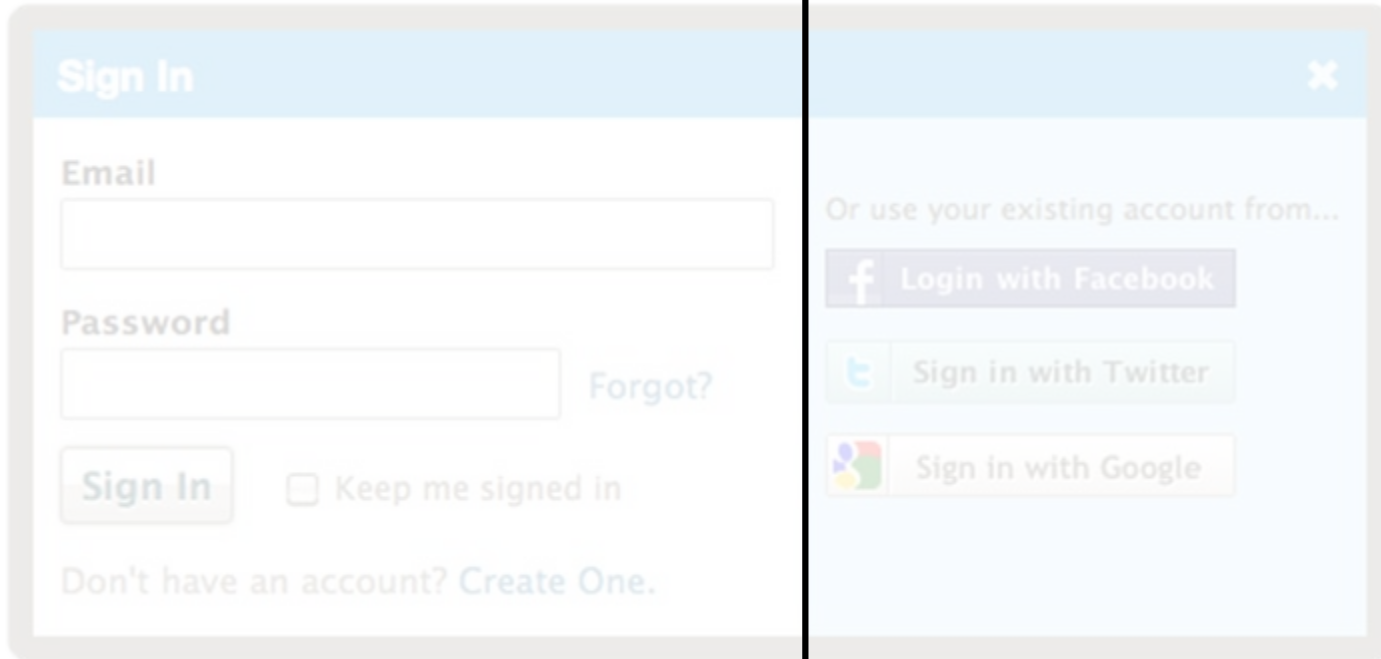
Privacy-preserving social plugins

Detecting traffic snooping in Tor using decoys

Minimizing information disclosure in social login platforms

Privacy-preserving social plugins

Detecting traffic snooping in Tor using decoys



Create yet another account...

Sign in with a single click...

Social Login







- ✓ Convenience – fewer passwords to remember
- ✓ Rich experience through social features
- ✓ Outsource user registration and management

Request for Permission - Google Chrome

https://www.facebook.com/dialog/permissions.request?api_key=d2730cb3e9daeef4b171f669af4231e5&app_id=d2730cb3e9d

f Request for Permission

surfingneighbors.com is requesting permission to do the following:

-  **Access my basic information**
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've made public.
-  **Send me email**
surfingneighbors.com may email me directly at diego.ridaz@yahoo.com · Change
-  **Post to Facebook as me**
surfingneighbors.com may post status messages, notes, photos, and videos on my behalf.
-  **Access posts in my News Feed**
-  **Access my data any time**
surfingneighbors.com may access my data at any time for this application.
-  **Access my profile information**
Birthday and Facebook Status

Report App

Logged in as Diego Ridaz · Log Out

surfingneighbors.com

Take it or leave it

Allow **Don't Allow**

SudoWeb

Bring the least privilege paradigm to social login platforms

Primary profile == root account

Use carefully! Contains sensitive private information!

Secondary profile == normal user account

Does not contain any sensitive information – *disposable*

Open source project (browser extension):

<https://code.google.com/p/sudoweb/>

Minimizing information disclosure
in social login platforms

Privacy-preserving social plugins

Detecting traffic snooping in Tor using decoys

Who knows I visited wired.com?



WIRED SCIENCE

NEWS FOR YOUR NEURONS

PREVIOUS POST

NEXT POST

Wired Science Space Photo of the Day

By [Wired Science](#) July 31, 2012 | 3:36 pm | Categories: [Space](#)

[Like](#) [Send](#) [f](#) 25 likes. Sign Up to see what your friends like.

141	6	2
Twitter	Google +1	in Share

Facebook

Twitter

Google

LinkedIn

The Problem

Social plugins are prevalent

1.23bn Facebook users

33% of the top 10K websites have Like Buttons

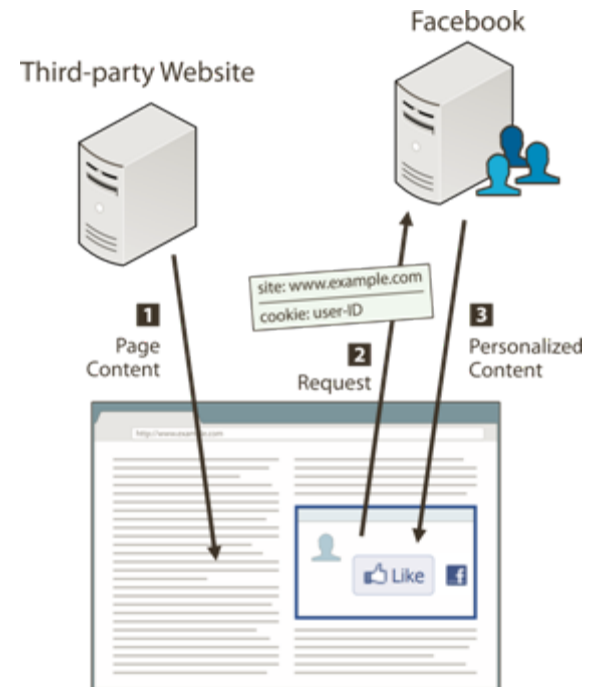
Twitter, Google+, LinkedIn, Pinterest, AddThis, ...

OS integration

A growing part of users' browsing history can be tracked

Not merely anonymous visitors,
but ***named persons***

By just visiting the page
(no interaction needed)



Existing Solutions

Log out

Some cookies persist

Block third-party cookies

Not always effective

Block social widgets completely

All existing solutions disable content personalization

Privacy vs. functionality dilemma

- (a)  43 likes. Sign Up to see what your friends like.
- (b)  43 people like this.
- (c)  Jane Doe, John Doe and 41 others like this.



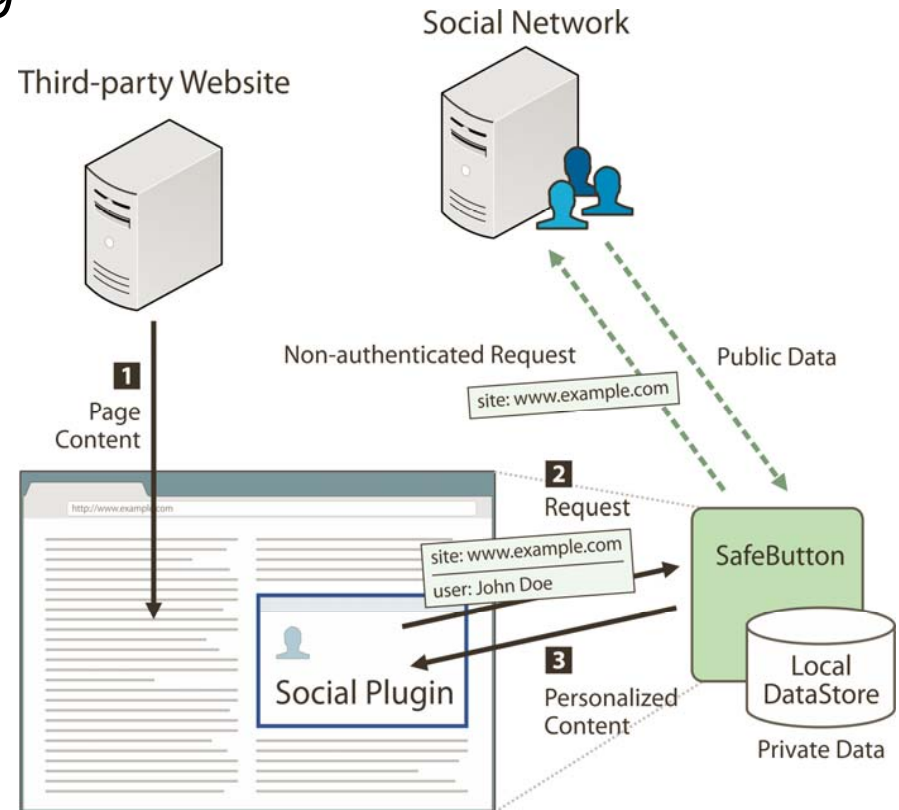
Privacy-Preserving Social Plugins

Decouple the retrieval of private information from the rendering of personalized content

Asynchronous content prefetching

Personalized content is synthesized *locally*

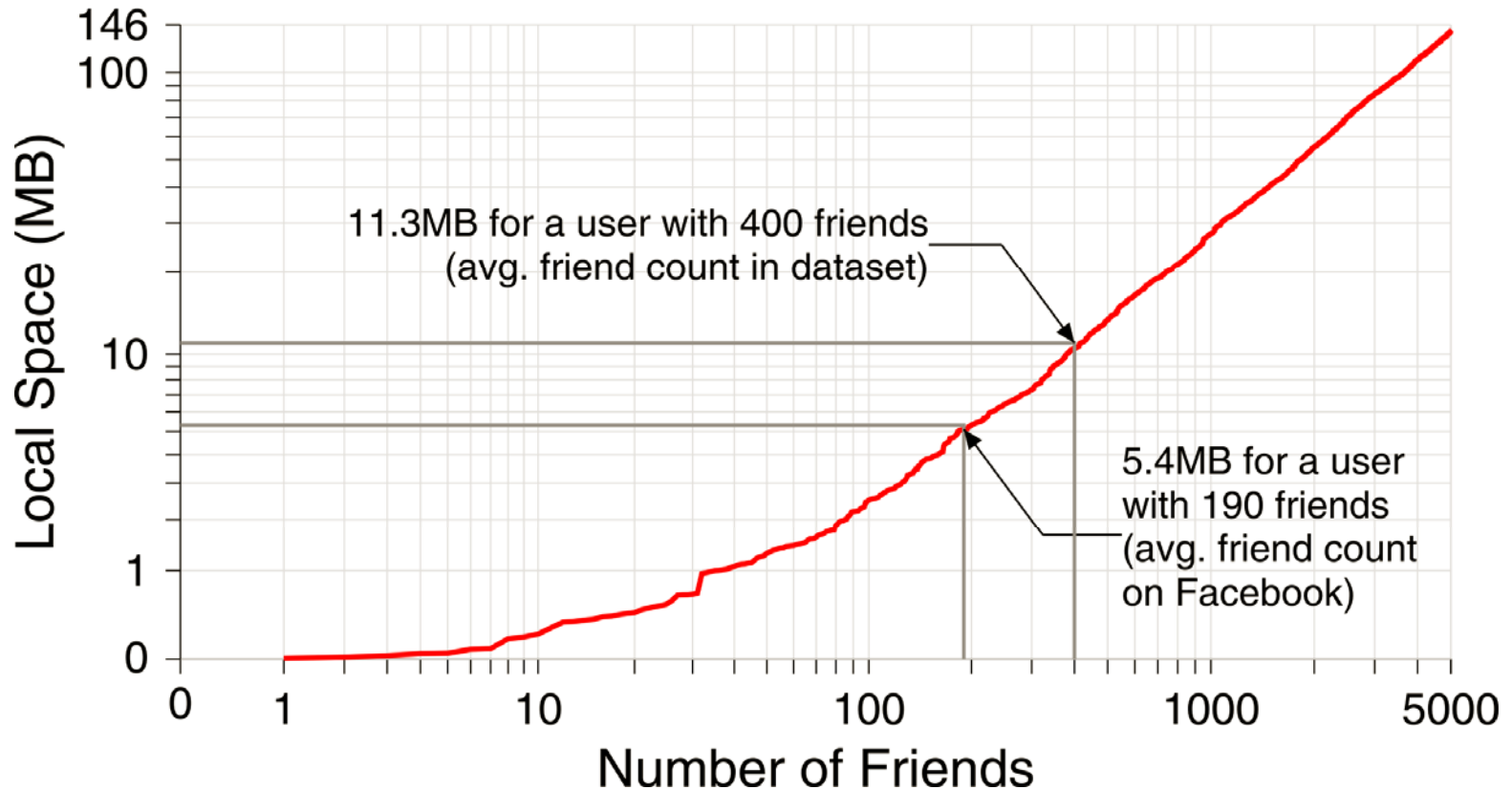
Same user experience



Open source project (browser extension):

<http://www.cs.columbia.edu/~kontaxis/safebutton/>

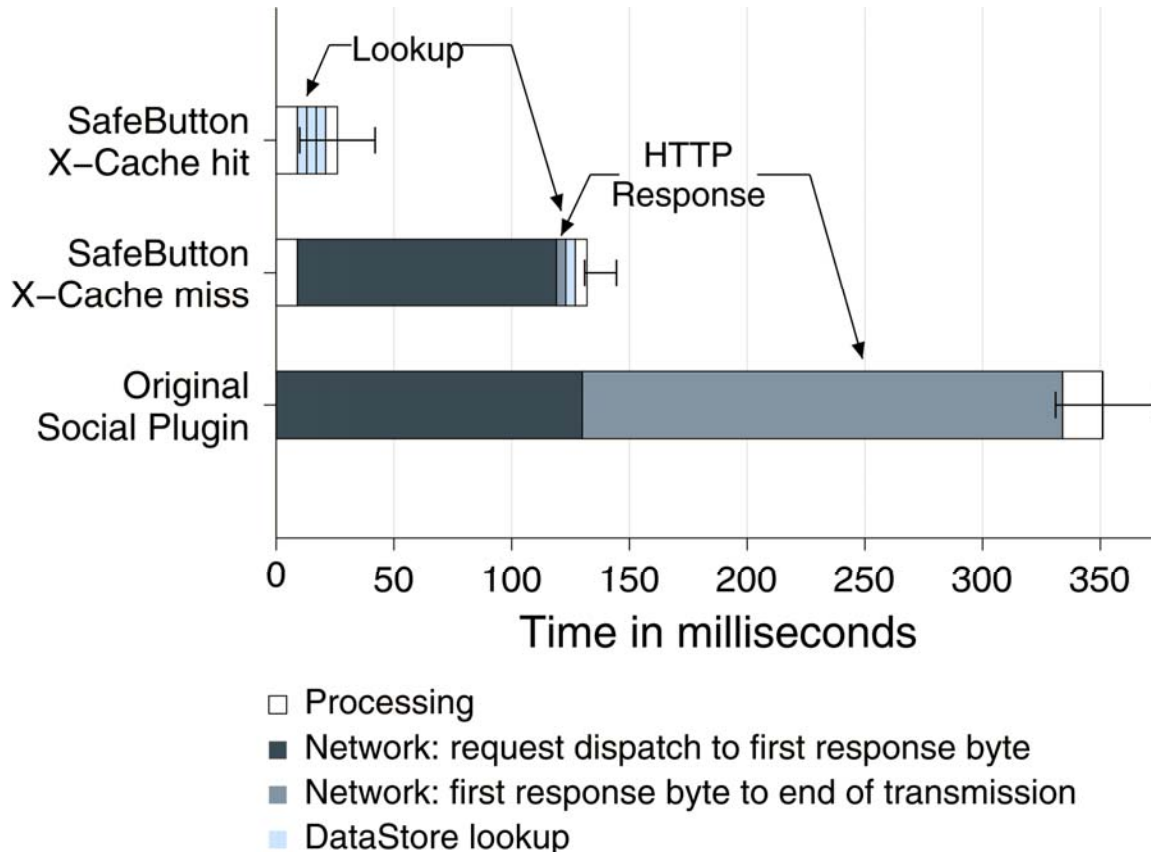
SafeButton Storage Requirements



Average user (190 friends): 5.4MB (Incl. names, profile photos, "likes", "shares" of all friends)

Extreme case (5,000 friends): 145.7MB (reasonable even for mobile devices)

SafeButton Performance



Caching frequently used data enables almost instantaneous rendering due to the absence of network requests:
x14.6 faster

SafeButton downloads only raw data, instead of HTML/CSS/JS content:
x2.8 faster

Minimizing information disclosure
in social login platforms

Privacy-preserving social plugins

Detecting traffic snooping in Tor using decoys

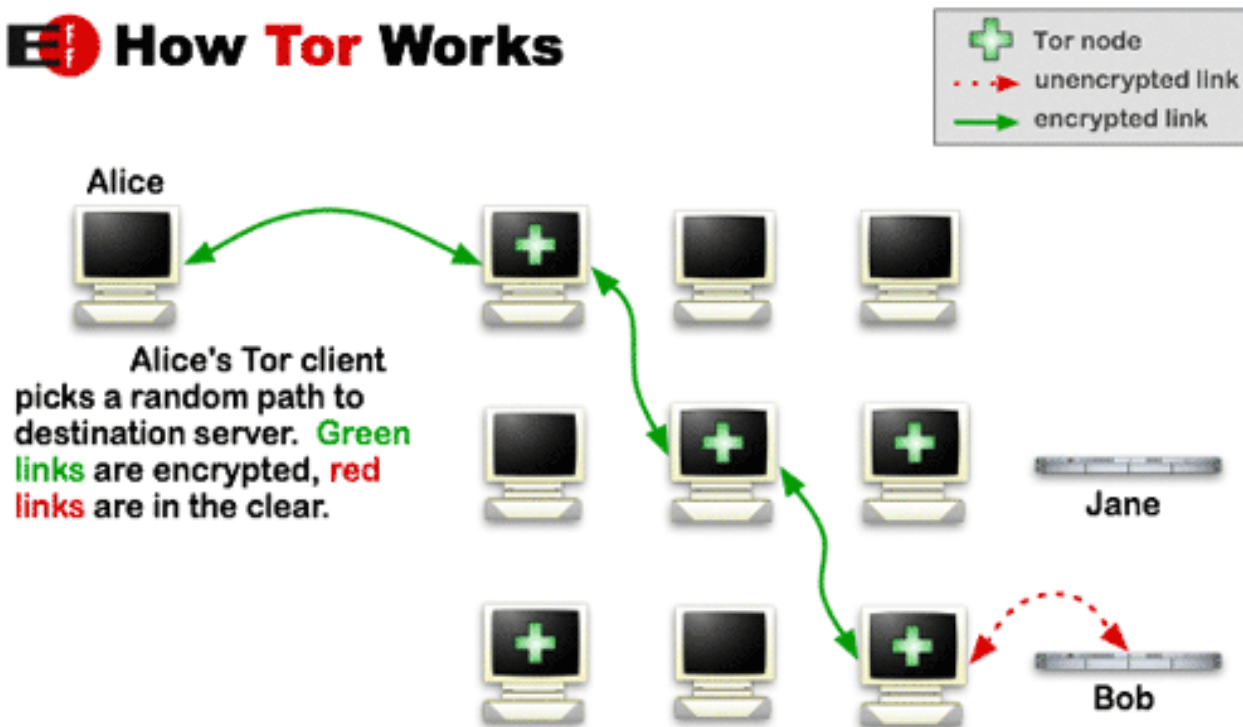
Tor (aka. the Onion Router)

Low-latency anonymous communication network

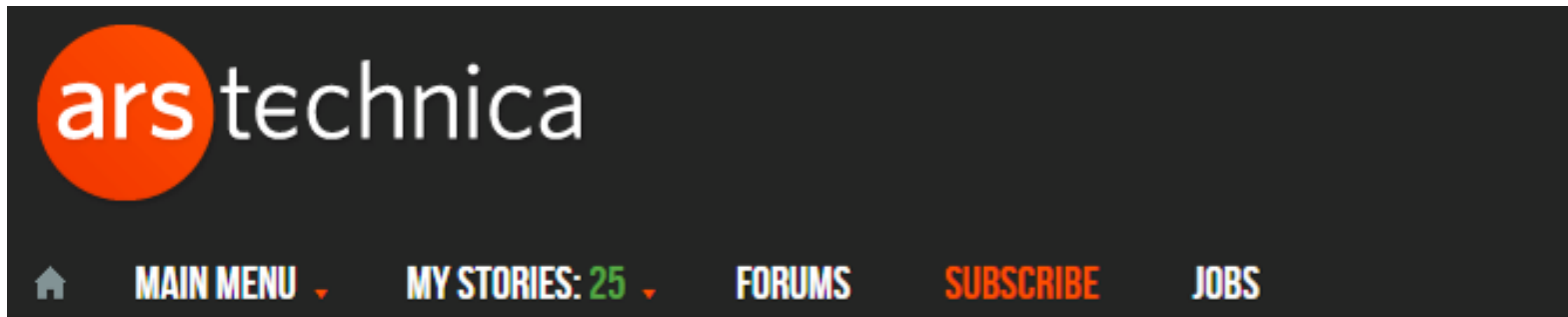
Layered encryption: each relay decrypts a layer of encryption to reveal only the next relay

Worldwide volunteer network of ~6K relays

How Tor Works



Who can see my traffic?



RISK ASSESSMENT / SECURITY & HACKTIVISM

For a year, gang operating rogue Tor node infected Windows executables

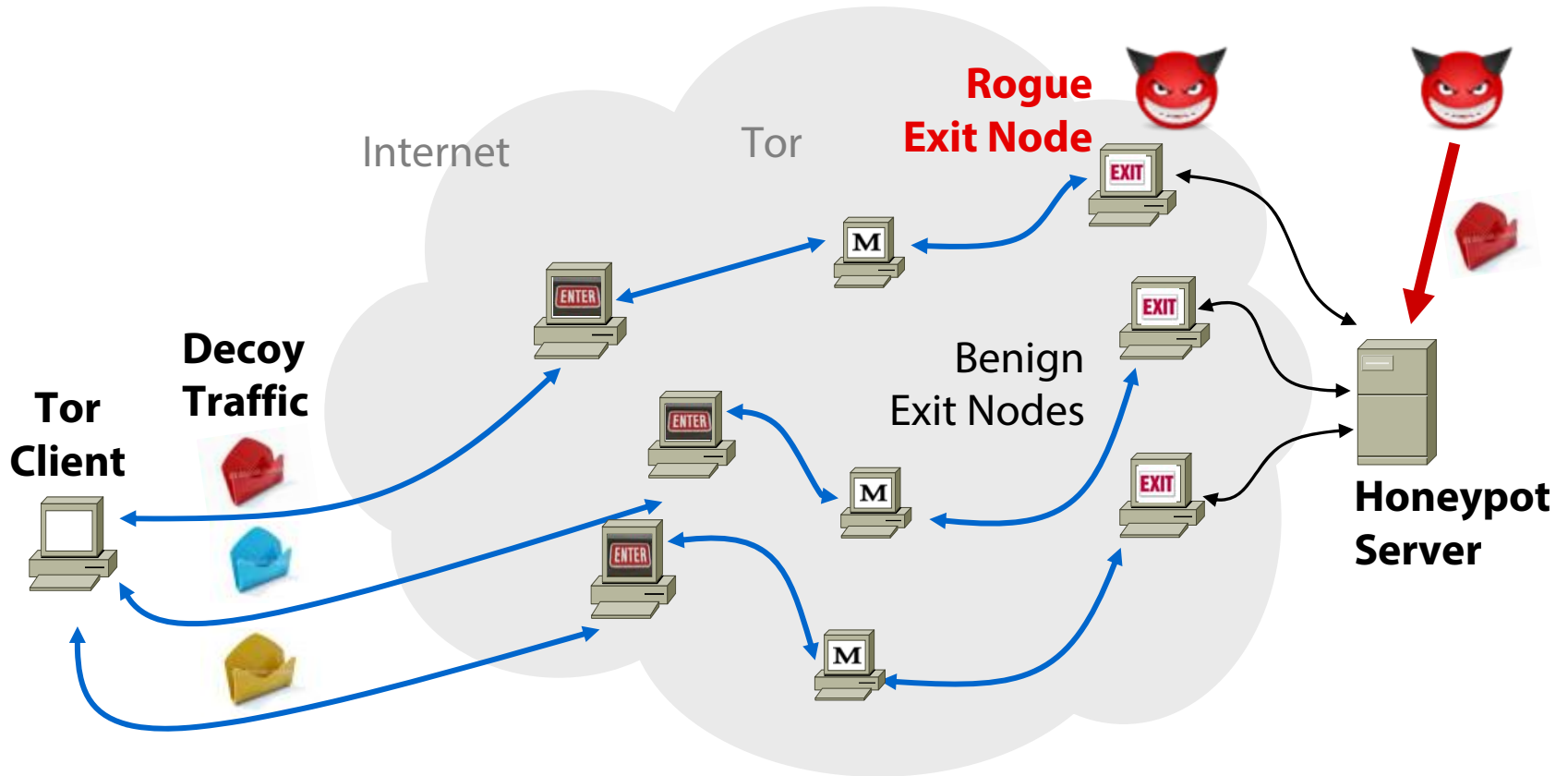
Attacks tied to gang that previously infected governments with highly advanced malware.

by Dan Goodin - Nov 14 2014, 10:30am EST

[Share](#) [Tweet](#) 57



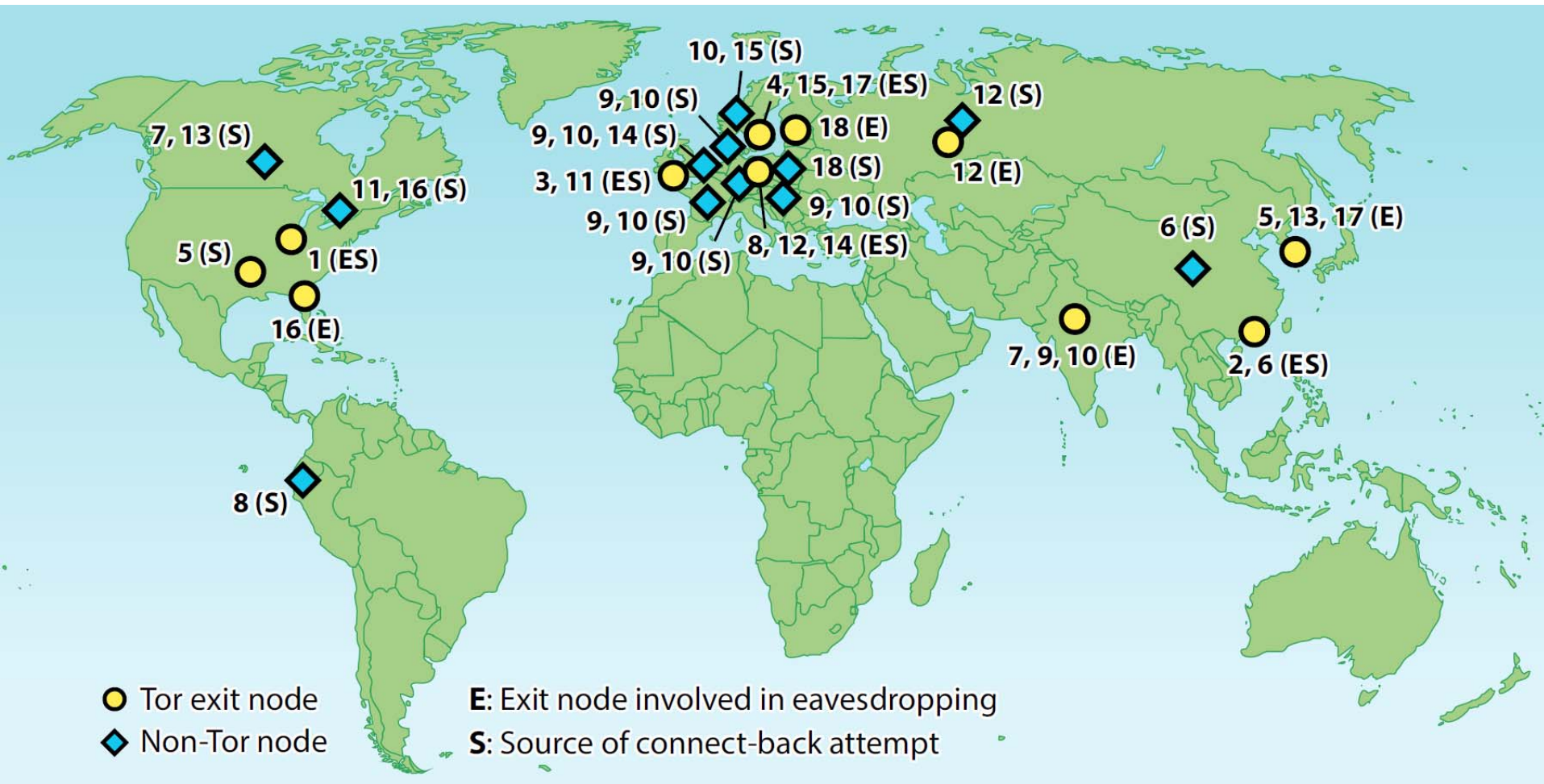
Detecting Traffic Snooping in Tor using Decoys



Expose unique decoy username+password through each exit node

Wait for unsolicited connections to the honeypot server using any of the exposed bait credentials

Detected Rogue Exit Nodes



30-month period: detected **18 cases** of traffic eavesdropping that involved **14 different Tor exit nodes**