

# CSE 127: Introduction to Security

Lecture 18: Ethics, law, and policy

**Nadia Heninger and Deian Stefan**

UCSD

Fall 2019

# Lecture Outline

- Ethical principles
- Laws relevant to security research and practice
- Example cases

# Overarching principles/lessons

- Ethics: Try to be a good person. Be thoughtful about your actions and their effects on yourself and others.
- Legal issues: Don't violate laws.
- If lawyers or law enforcement are involved, you have already lost. It doesn't matter if you could in theory win the case in the end.

# Legal/ethical principle: Property rights

Respect other people's property.

**Example:** Hacking your own password.

- On your own machine: Probably ok. (Possible exception: DMCA.)
- On someone else's machine: Get permission or else it's probably not ok. (Might be CFAA violation under Terms of Service interpretation.)

# Computer Fraud and Abuse Act (CFAA)

18 U.S. CODE §1030 - FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS

Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer...

The punishment for an offense...

- a fine under this title or imprisonment for not more than one year, or both...,
- a fine under this title or imprisonment for not more than 5 years, or both... if—
  - (i) the offense was committed for purposes of commercial advantage or private financial gain;
  - (ii) the offense was committed in furtherance of any criminal or tortious act...; or
  - (iii) the value of the information obtained exceeds \$5,000

# Prominent CFAA cases: Aaron Swartz

- Scraped JStor from MIT's network and evaded numerous blocking attempts.
- Prosecuted for violating the Terms of Service of JStor even though JStor did not want to prosecute.
- Property owners: MIT, JStor, article authors
- Swartz had already been investigated for scraping public court records (PACER)



# Prominent CFAA cases: Weev

- Found a vulnerability in 2010 that allowed AT&T iPad owners email addresses to be scraped.
- Enumerated URLs with a numeric identifier to scrape.
- Convicted, won on appeal in the US 3rd District in 2014 but on venue grounds, question of whether enumerating URLs is exceeding authorized access unresolved.

## Apple's Worst Security Breach: 114,000 iPad Owners Exposed



Ryan Tate

Filed to: EXCLUSIVE 6/09/10 4:50pm

1,072,918 2 ★ ~



# Ethical Principle: Minimizing harm

Ethical research involves trying to minimize harm.

## **Example:** SYN scanning

- Scanning public hosts is legal, but generates many complaints.
- Depends on intended use: Used by attackers to find vulnerable hosts, used by researchers to measure networks.
- Doing research on open networks means understanding and following best practices:
  - Publicly identifying the purpose of the research
  - Providing an opt-out mechanism
  - Not launching attacks
  - Avoiding overwhelming your or others' networks or crashing hosts
  - Etc.



# Ethical principle: Minimizing harm

## **Example:** Botherding

- Botherding is taking over a botnet
- Is this ethical or not?
  - Interfering with a legal botnet is definitely illegal.
  - Marcus Hutchins was celebrated for activating a kill switch in WannaCry malware that halted infections.
  - Is taking over a botnet for research purposes ethical? It is pursuing illegal activity to study illegal activity.
  - What is harm minimization?

## **Your Botnet is My Botnet: Analysis of a Botnet Takeover**

Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna

University of California, Santa Barbara

[bstone,marco,sullivan,rgilbert,msz,kemm,chris,vigna]@cs.ucsb.edu

### **ABSTRACT**

Botnets, networks of malware-infected machines that are controlled by an adversary, are the root cause of a large number of security problems on the Internet. A particularly sophisticated and insidious type of bot is Torpig, a malware program that is designed to

One approach to study botnets is to perform *passive analysis* of secondary effects that are caused by the activity of compromised machines. For example, researchers have collected spam mails that were likely sent by bots [47]. Through this, they were able to make indirect observations about the sizes and activities of different spam botnets. Similar measurements focused on DNS queries [34, 35]

# Digital Millennium Copyright Act (DMCA)

## 17 U.S. Code § 1201 - Circumvention of copyright protection systems

Current through Pub. L. [113-86](#), except [113-79](#). (See [Public Laws for the current Congress](#).)

US Code

Notes

Updates

### (a) Violations Regarding Circumvention of Technological Measures.—

(1)

(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.

# DMCA cases

- 2010 US v. Crippen, rare criminal DMCA prosecution of Xbox modder
- 2002 Bunnie Huang Xbox key extraction
  - MIT did not support his work, AI Lab published his work and reached an agreement with Microsoft

## % Hacking the Xbox\_

### A Brief History of the Book

"Hacking the Xbox" was originally a work commissioned by the respected technical publisher Wiley & Sons. Shortly after completing the final chapters, Wiley & Sons notified the author that publishing of the book had been cancelled, due to their concerns regarding the Digital Millennium Copyrights Act (DMCA). This happened despite the author taking special care not to include any Microsoft-copyrighted material or materials that could be directly applied to copyright circumvention.

Furthermore, on the second day of book pre-sales, the original e-commerce provider Americart elected to decline offering cart services due to concerns over the DMCA:

Now for the bad news. We are going to have to decline to offer you cart service for selling hacker materials, which is our right to do so per the Americart Merchant Service agreement. It's too risky for us to be involved in, especially in light of the fact that now I know about it. \$15 per month doesn't pay for us to take the risk of being named in a DMCA suit. From what I understand, Microsoft is pretty aggressive on such matters. It is nothing personal on our part.

# DMCA Exemptions

Every three years, the Library of Congress considers exemptions to the DMCA.

- 2010: Phone jailbreaking
- 2016: Security research

Accordingly, based on the Register's recommendation, the Librarian adopts the following exemption:

(i) **Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good-faith security research and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code; and provided, however, that, except as to voting machines, such circumvention is initiated no earlier than 12 months after the effective date of this regulation, and the device or machine is one of the following:**

(2) **Permissible acts of encryption research.**— Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if—

(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;

(B) such act is necessary to conduct such encryption research;

(C) the person made a good faith effort to obtain authorization before the circumvention; and

(D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section [1030](#) of title [18](#) and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

# **Petition for Proposed Exemption Under 17 U.S.C. § 1201**

## **Item 1. Submitter and Contact Information**

The submitters are a group of academic security researchers comprised of Prof. Steven M. Bellovin (Columbia University), Prof. Matt Blaze (University of Pennsylvania), Prof. Edward W. Felten (Princeton University), Prof. J. Alex Halderman (University of Michigan), and Prof. Nadia Heninger (University of Pennsylvania) (the “Submitters”).

## **Item 2. Brief Overview of Proposed Exemption**

Literary works, including computer programs and databases, protected by access control mechanisms that potentially expose the public to risk of harm due to malfunction, security flaws or vulnerabilities when

(a) circumvention is accomplished for the purpose of good faith testing for, investigating, or correcting such malfunction, security flaws or vulnerabilities in a technological protection measure or the underlying work it protects; OR

(b) circumvention was part of the testing or investigation into a malfunction, security flaw or vulnerability that resulted in the public dissemination of security research when (1) a copyright holder fails to comply with the standards set forth in ISO 29147 and 30111; or (2) the finder of the malfunction, security flaw or vulnerability reports the malfunction, security flaw or vulnerability to the copyright holder by providing the information set forth in Form A\* in advance of or concurrently with public dissemination of the security research.

# Trade Secrets and Reverse Engineering

- RC4 trade secret
  - RC4 stream cipher algorithm was originally a trade secret of RSA company
  - Reverse engineered in 1994 and code posted anonymously to Cypherpunks mailing list and sci.crypt newsgroup
  - Used afterward and referred to as “ARC4”
- Megamos Crypto
  - In 2013 European researchers reverse engineered a car unlocking system used by Volkswagen
  - Volkswagen got an injunction in the UK against the researchers publishing based on the “murky” origins of the publicly available code they reverse engineered
  - It took two years for the final paper to be able to be published
  - Injunction would not likely have succeeded in US

# Personal and Privacy Rights

## Principle: Informed consent

- Human subjects research should go through ethical review
  - At a university, this is done by IRB
  - Some companies now have review processes (Example: Facebook happiness research)
- Human subjects research includes any collection of Personally Identifiable Information

# Judge Confirms Government Paid CMU Scientists to Hack Tor Users for FBI

📅 February 25, 2016    👤 Swati Khandelwal



Everything is now crystal clear:

The security researchers from Carnegie Mellon University (CMU) were hired by the federal officials to discover a technique that could help the FBI [Unmask Tor users](#) and [Reveal their IP addresses](#) as part of a criminal investigation.

Yes, a federal judge in Washington has recently confirmed that the computer scientists at CMU's Software Engineering Institute (SEI) were indeed behind a hack of the TOR project in 2014, according to court documents [\[PDF\]](#) filed Tuesday.

In November 2015, The Hacker News reported that Tor Project Director *Roger Dingledine* accused the Federal Bureau of Investigation (FBI) of paying the CMU, at least, [\\$1 Million for providing information](#) that led to the criminal suspects identification on the [Dark Web](#).

After this news had broken, the [FBI denied the claims](#), saying *"The allegation that we paid [CMU] \$1 Million to hack into TOR is inaccurate."*



# Informed consent

**Example:** Jason Fortuny posted fake sex ad on Craigslist as a woman in 2006

- Received hundreds of replies, posted them all online
- Unethical? Yes.
- Illegal? Unclear.
  - Encyclopedia Dramatica received DMCA takedown notice.
  - Sued in Illinois by anonymous victim, default \$75k judgement

# Legal foundations of privacy

In US, 14th amendment: “nor shall any state deprive any person of life, liberty, or property without due process of law”

Interpreted as right to privacy by 20th century supreme court:

- Legality of contraception
- Roe v. Wade

# Wiretapping

## 18 U.S. Code § 2511 - Interception and disclosure of wire, oral, or electronic communications prohibited

Current through Pub. L. [113-296](#), except [113-287](#), [113-291](#), [113-295](#). (See [Public Laws for the current Congress](#).)

US Code

Notes

[prev](#) | [next](#)

- (1) Except as otherwise specifically provided in this chapter any person who—
- (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
  - (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—
    - (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
    - (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
    - (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or
    - (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

California is a “two-party consent” state. All parties in a conversation must consent for it to be recorded.

# FISA background

## 1978 Foreign Intelligence Surveillance Act

- Passed in response to Church Committee investigation of COINTELPRO scandals
- Codified separation between domestic law enforcement activities and international intelligence activities
- FISA Court established to handle surveillance warrants for intelligence investigations in the US

After 2001, PATRIOT Act weakened some of these separations.

# Snowden leaked FISA order for all Verizon Business customer information in 2013

---

IN RE APPLICATION OF THE  
FEDERAL BUREAU OF INVESTIGATION  
FOR AN ORDER REQUIRING THE  
PRODUCTION OF TANGIBLE THINGS  
FROM VERIZON BUSINESS NETWORK SERVICES,  
INC. ON BEHALF OF MCI COMMUNICATION  
SERVICES, INC. D/B/A VERIZON  
BUSINESS SERVICES.

---

Docket Number: BR

13 - 8 0

## SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

TOP SECRET//SI//NOFORN

Derived from: Pleadings in the above-captioned docket  
Declassify on: 12 April 2038

on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. This Order does not require Verizon to produce telephony metadata for communications wholly originating and terminating in foreign countries. Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

IT IS FURTHER ORDERED that no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order, other than to: (a) those persons to whom disclosure is necessary to comply with such Order; (b) an attorney to obtain legal advice or assistance with respect to the production of things in

## Updated FISA orders have continued to be approved.

# Verizon Government Transparency Report

## National security demands

The table below sets forth the number of national security demands we received in the applicable period. Under section 603 of the USA Freedom Act we are now able to report the number of demands in bands of 500.

	Jan 1, 2016 – Jun. 30, 2016	Jul. 1, 2016 – Dec. 31, 2016	Jan 1, 2017 – Jun. 30, 2017	July 1, 2017 – Dec. 31, 2017	Jan 1, 2018 – Jun. 30, 2018	Jul. 1, 2018 – Dec. 31, 2018	Jan 1, 2019 – Jun. 30, 2019
National Security Letters	1-499	5-499	1-499	501-999	1-499	0-499	0-499
Number of customer selectors	500-999	1000-1499	1500-1999	1500-1999	2000-2499	2000-2499	1500-1999
FISA Orders (Content)	0-499	0-499	0-499	0-499	0-499	0-499	*
Number of customer selectors	2000-1499	2000-2499	1500-1999	2000-2499	2000-2499	1500-1999	*
FISA Orders (Non-Content)	0-499	0-499	0-499	0-499	0-499	0-499	*
Number of customer selectors	0-499	0-499	0-499	0-499	0-499	0-499	*

\* The government has imposed a six month delay for reporting this data.

“In the first half of 2019, we received between 0 and 499 NSLs from the FBI. Those NSLs sought information regarding between 1500 and 1999 ‘selectors’ used to identify a Verizon customer. ”

# N.S.A. Able to Foil Basic Safeguards of Privacy on Web

By NICOLE PERLROTH, JEFF LARSON and SCOTT SHANE

Published: September 5, 2013 | 1466 Comments

The [National Security Agency](#) is winning its long-running secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age, according to newly disclosed documents.


 [Enlarge This Image](#)





Associated Press

This undated photo released by the United States government shows the National Security Agency campus in Fort Meade, Md.

The agency has circumvented or cracked much of the encryption, or digital scrambling, that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and automatically secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world, the documents show.

 FACEBOOK

 TWITTER

 GOOGLE+


 SAVE

 EMAIL

 SHARE

 PRINT

 SINGLE PAGE

 REPRINTS



# September 2013: NSA Bullrun program

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.
- (TS//SI//REL TO USA, FVEY) Collect target network data and metadata via cooperative network carriers and/or increased control over core networks.
- (TS//SI//REL TO USA, FVEY) Leverage commercial capabilities to remotely deliver or receive information to and from target endpoints.
- (TS//SI//REL TO USA, FVEY) Exploit foreign trusted computing platforms and technologies.
- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.
- (TS//SI//REL TO USA, FVEY) Make specific and aggressive investments to facilitate the development of a robust exploitation capability against Next-Generation Wireless (NGW) communications.



# September 2013: NSA Bullrun program

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.
- (TS//SI//REL TO USA, FVEY) Collect target network data and metadata via cooperative network carriers and/or increased control over core networks.
- (TS//SI//REL TO USA, FVEY) Leverage commercial capabilities to remotely deliver or receive information to and from target endpoints.
- (TS//SI//REL TO USA, FVEY) Exploit foreign trusted computing platforms and technologies.
- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.
- (TS//SI//REL TO USA, FVEY) Make specific and aggressive investments to facilitate the development of a robust exploitation capability against Next-Generation Wireless (NGW) communications.

New York Times names US standardized random number generator as a target.

# September 2013: NSA Bullrun program

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.
- (TS//SI//REL TO USA, FVEY) Collect target network data and metadata via cooperative network carriers and/or increased control over core networks.
- (TS//SI//REL TO USA, FVEY) Leverage commercial capabilities to remotely deliver or receive information to and from target endpoints.
- (TS//SI//REL TO USA, FVEY) Exploit foreign trusted computing platforms and technologies.
- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.
- (TS//SI//REL TO USA, FVEY) Make specific and aggressive investments to facilitate the development of a robust exploitation capability against Next-Generation Wireless (NGW) communications.

New York Times names US standardized random number generator as a target.

NIST re-opens discussions on SP800.90; recommends against use.

RSA suggests changing default in BSAFE.

2015: Juniper discovers Dual EC DRBG backdoor in ScreenOS.

(Reuters) - Security industry pioneer RSA adopted not just one but two encryption [tools](#) developed by the U.S. National Security Agency, greatly increasing the spy agency's ability to eavesdrop on some Internet communications, according to a team of academic researchers.

Reuters reported in December that the NSA had paid RSA \$10 million to make a now-discredited cryptography system the default in [software](#) used by a wide range of Internet and computer security programs. The system, called Dual Elliptic Curve, was a random number generator, but it had a deliberate flaw - or "back door" - that allowed the NSA to crack the encryption.

A group of professors from Johns Hopkins, the University of Wisconsin, the University of Illinois and elsewhere now say they have discovered that a second NSA tool exacerbated the RSA software's vulnerability.

The professors found that the tool, known as the "Extended Random" extension for secure websites, could help crack a version of RSA's Dual Elliptic Curve [software](#) tens of thousands of times faster, according to an advance copy of their research shared with Reuters.

While Extended Random was not widely adopted, the new research sheds light on how the NSA extended the reach of its surveillance under cover of advising companies on protection.

## **2015-12 Out of Cycle Security Bulletin: ScreenOS: Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756)**

VPN Decryption (CVE-2015-7756) may allow a knowledgeable attacker who can monitor VPN traffic to decrypt that traffic. It is independent of the first issue.

This issue affects ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20. **No other Juniper products or versions of ScreenOS are affected by this issue.**

There is no way to detect that this vulnerability was exploited.

This issue has been assigned [CVE-2015-7756](#).

## 2015-12 Out of Cycle Security Bulletin: ScreenOS: Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756)

VPN Decryption (CVE-2015-7756) may allow a knowledgeable attacker who can monitor VPN traffic to decrypt that traffic. It is independent of the first issue.

This issue affects ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20. **No other Juniper products or versions of ScreenOS are affected by this issue.**

There is no way to detect that this vulnerability was exploited.

This issue has been assigned [CVE-2015-7756](#).

### A Systematic Analysis of the Juniper Dual EC Incident

Stephen Checkoway,<sup>\*</sup> Shaanan Cohney,<sup>\*\*</sup> Christina Garman<sup>†</sup> Matthew Green,<sup>‡</sup> Nadia Heninger,<sup>\*\*</sup>

Jacob Maskewicz,<sup>††</sup> Eric Rescorla,<sup>††</sup> Hovav Shacham,<sup>††</sup> Ralf-Philipp Weinmann  
<sup>††</sup>*UC San Diego*, <sup>\*\*</sup>*University of Pennsylvania*, <sup>†</sup>*Johns Hopkins University* <sup>\*</sup>*University of Illinois at Chicago*

# 2015-12 Out of Cycle Security Bulletin: ScreenOS: Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756)

VPN Decryption (CVE-2015-7756) may allow a knowledgeable attacker who can monitor VPN traffic to decrypt that traffic. It is independent of the first issue.

This issue affects ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20. **No other Juniper products or versions of ScreenOS are affected by this issue.**

There is no way to detect that this vulnerability was exploited.

This issue has been assigned [CVE-2015-7756](#).

## A Systematic Analysis of the Juniper Dual EC Incident

Stephen Checkoway,<sup>\*</sup> Shaanan Cohney,<sup>\*\*</sup> Christina Garman<sup>†</sup> Matthew Green,<sup>‡</sup> Nadia Heninger,<sup>\*\*</sup>

Jacob Maskewicz,<sup>††</sup> Eric Rescorla,<sup>††</sup> Hovav Shacham,<sup>††</sup> Ralf-Philipp Weinmann  
<sup>††</sup>*UC San Diego*, <sup>\*\*</sup>*University of Pennsylvania*, <sup>†</sup>*Johns Hopkins University* <sup>\*</sup>*University of Illinois at Chicago*



emptywheel @emptywheel · 23h

Ted Lieu: That Juniper did not come to testify "insinuates they have something to hide."



21



16



emptywheel @emptywheel · 23h

Juniper refused to come to Oversight hearing on cyber.



4

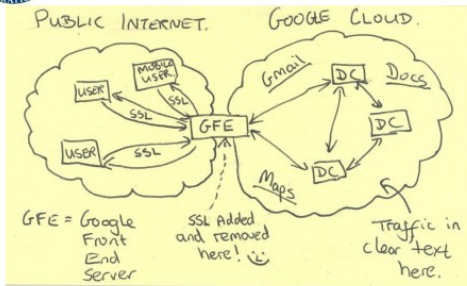


# October 2013: MUSCULAR

TOP SECRET//SI//NOFORN



## Current Efforts - Google



TOP SECRET//SI//NOFORN

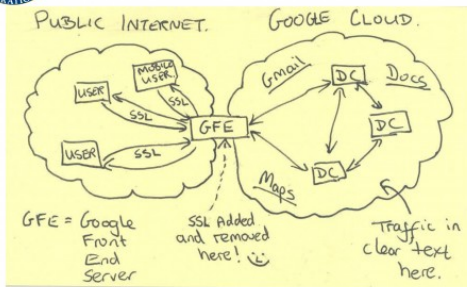
Official Google  
statement:  
"We are outraged"

# October 2013: MUSCULAR

TOP SECRET//SI//NOFORN



## Current Efforts - Google



TOP SECRET//SI//NOFORN

Official Google statement:  
"We are outraged"

Unofficial Google statement: "Fuck these guys."



# Key Escrow and Law Enforcement Backdoors Redux

Recently, the head of the National Security Agency provided a rare hint of what some U.S. officials think might be a technical solution. Why not, suggested Adm. Michael S. Rogers, require technology companies to create a digital key that could open any smartphone or other locked device to obtain text messages or photos, but divide the key into pieces so that no one person or agency alone could decide to use it?

“I don’t want a back door,” Rogers, the director of the nation’s top electronic spy agency, said during a speech at Princeton University, using a tech industry term for covert measures to bypass device security. “I want a front door. And I want the front door to have multiple locks. Big locks.”

# Law Enforcement Access Policy

Policy/ethics question: Is it preferable to have law enforcement/intelligence:

- Stockpile software vulnerabilities, write targeted malware, and hack into targets when desired
- Mandate encryption backdoors or otherwise enable mass surveillance

# The FBI's Firefox Exploit

By **Nicholas Weaver** Thursday, April 7, 2016, 8:43 AM



DayZero: Cybersecurity Law and Policy

Lawfare contributors are having an [interesting debate](#) (with dinners and drinks on the line) about whether and why the FBI might reveal the details of the exploit used to unlock the San Bernardino iPhone. My guess is that the FBI will inadvertently release so many details in aiding local law enforcement that the question becomes moot: we will at least learn whether the exploit uses the USB connection or attacks through the cellular "baseband," as well as whether the exploit works on current versions or has already been patched by Apple.

But another fight over vulnerability disclosure is far more interesting and getting far less attention. The FBI is apparently hoarding a Tor Browser exploit which it used to target visitors of the "Playpen" child porn site. I've previously discussed [how the FBI wrote the warrant to hack over a thousand targets](#). Now the FBI is [fighting defense efforts to examine the exploit itself](#) despite an order [requiring the FBI to reveal the exploit to the defense](#).

The Tor Browser is simply Firefox running in a hardened mode. While many Firefox exploits will not work against the Tor browser—particularly those relying on Flash—the converse is not necessarily true. To the contrary, any Tor browser exploit is almost certainly a Firefox exploit too.

# Unintended Consequences of Law Enforcement Access

- 2004 Greek wiretapping scandal
  - Greek politicians wiretapped through law enforcement access system present on phone network
  - System was present because of US CALEA law, not used in Greece
- 2010 China Google hack
  - Came in through law enforcement access portal

# Disclosure options for security flaws

- Develop fully weaponized malware and distribute on black market
- Tell no one
- Sell vulnerability to middleman and don't report to vendor
- Report to vendor only
- Report to vendor and receive bug bounty
- Report to vendor, wait for fix, report to public ("responsible disclosure")
- Report in full to public immediately ("full disclosure")

# The process of reporting vulnerabilities

- Some vendors have sensible reporting process
  - E.g., Firefox and Chrome teams respond and react quickly, easy to work with on fixing bugs, etc.
- Some vendors less so
  - E.g., Send email through an intermediary, receive ACK, no real conversation.
  - E.g., Send email, poke individual folks for replies, no replies. Give up.
- Some vendors are playing catch up
  - E.g., Reported OOB write vulnerability, security “team” replied with “not a security bug.” Later freaked out about public disclosure of OOB read vulnerability. Now there is a working group dedicated to security, slightly better definition of an attacker model, and reasonable reporting method: HackerOne.
- Some vendors are the worst: they will try to gag/sue you

# Bug bounty programs

- Many vendors have bug bounty programs: \$\$ for bugs
  - Mozilla and Google will even run your checkers and pay you if the checkers find real bugs
- Our students made \$3-10K on some papers!

	High-quality report with functional exploit	High-quality report	Baseline
Sandbox escape / Memory corruption in a non-sandboxed process	\$30,000	\$20,000	\$5,000 - \$15,000
Universal Cross Site Scripting	\$20,000	\$15,000	\$2,000 - \$10,000
Renderer RCE / memory corruption in a sandboxed process	\$10,000	\$7,500	\$2,000 - \$5,000
Security UI Spoofing	\$7,500	N/A [1]	\$500 - \$3,000
User Information disclosure	\$5,000 - \$20,000	N/A [1]	\$500 - \$2,000
Web Platform Privilege Escalation	\$5,000	\$3,000	\$500 - \$1,000
Exploitation Mitigation Bypass	\$5,000	\$3,000	\$500 - \$1,000
Chrome OS	<a href="#">See below</a>		
Chrome Fuzzer Bonus	\$1,000		
Chrome Patch Bonus	\$500 - \$2,000		

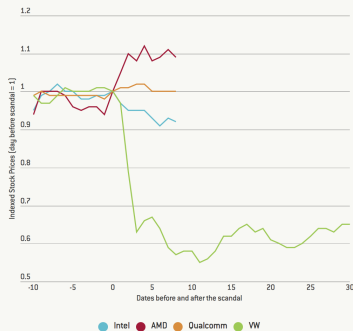
# Are companies liable for security flaws?

The FTC says yes.

- 2011 Facebook settlement for deceptive privacy policies
- 2013 HTC settlement for security flaws in phones
- 2016 LabMD liable for failure to institute reasonable security practices to protect consumer data

The stock market says not really:

Figure 1. Stock prices in the aftermath of Intel's "Meltdown" and Volkswagen's diesel scandal



Notes: Stock prices are initially denoted in the reported currency and then indexed to 1 on the day before the first media release of the respective scandal. Volkswagen's emission scandal was made public on September 18, 2015; the Meltdown CPU flaw was reported first on January 3rd, 2018; AMD (desktop) and Qualcomm (mobile) are two major competitors of Intel; stock prices last updated 15.01.2018.



# Policy questions around security research

- Should exploit sales be legal?
  - Code as speech principle says yes
  - Is publishing exploits ethical?
- How about mixed-use tools?
  - Privacy tools like Tor or encrypted messengers used by criminals, normal people, activists
  - Random darknet shopper art piece?

Have a great end of quarter!

Good luck on the final!