CSE 127: Introduction to Security

Privacy and Anonymity / Policy and Ethics

Deian Stefan

UCSD

Fall 2021

Some material from Nadia Heninger

Lecture outline

- Foundations of privacy
- Privacy-enhancing technologies
  - Modern encrypted messaging
  - Tor and anonymous communication
  - Privacy-respecting browsers (Tor, Firefox, Brave)
- Ethical principles
- Basic hygiene

What is privacy and why do we care?

Various definitions of privacy:

- Secrecy
- Anonymity
- Solitude

Human rights and values:

- Human dignity
- Mental health
- Intimacy/relationships

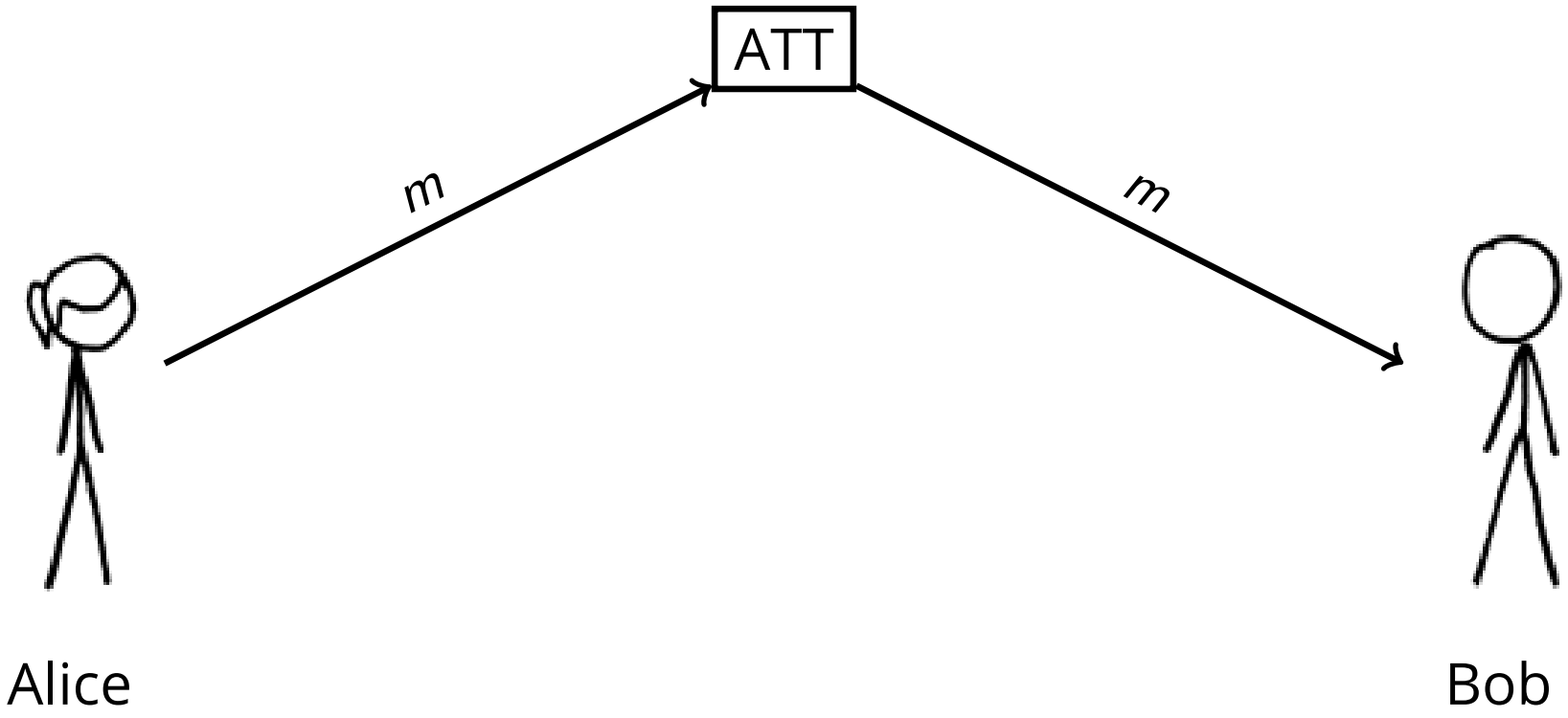
Political and democratic values:

- Liberty of action
- Moral autonomy

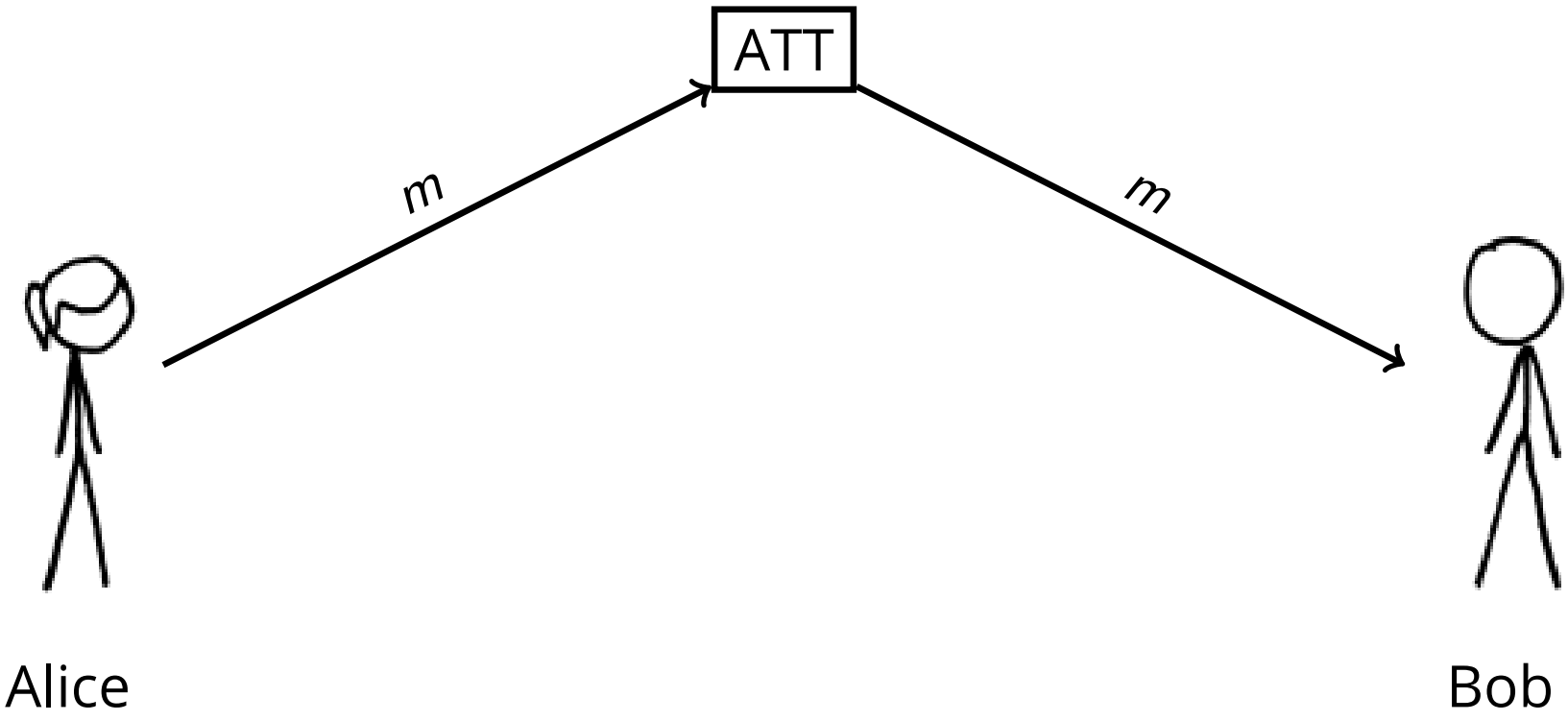
The “crypto wars”: privacy vs. wiretapping

- Crypto wars 1.0
  - Late 1970s,
  - US government threatened legal sanctions on researchers who published papers about cryptography.
  - Threats to retroactively classify cryptography research.
- Crypto wars 2.0
  - 1990s
  - Main issues: Export control and key escrow
  - Several legal challenges
- Crypto wars 3.0
  - Snowden
  - Apple v. FBI
  - Calls for “balance”
  - Apple’s CSAM
  - …?

Why is anonymous communication hard?

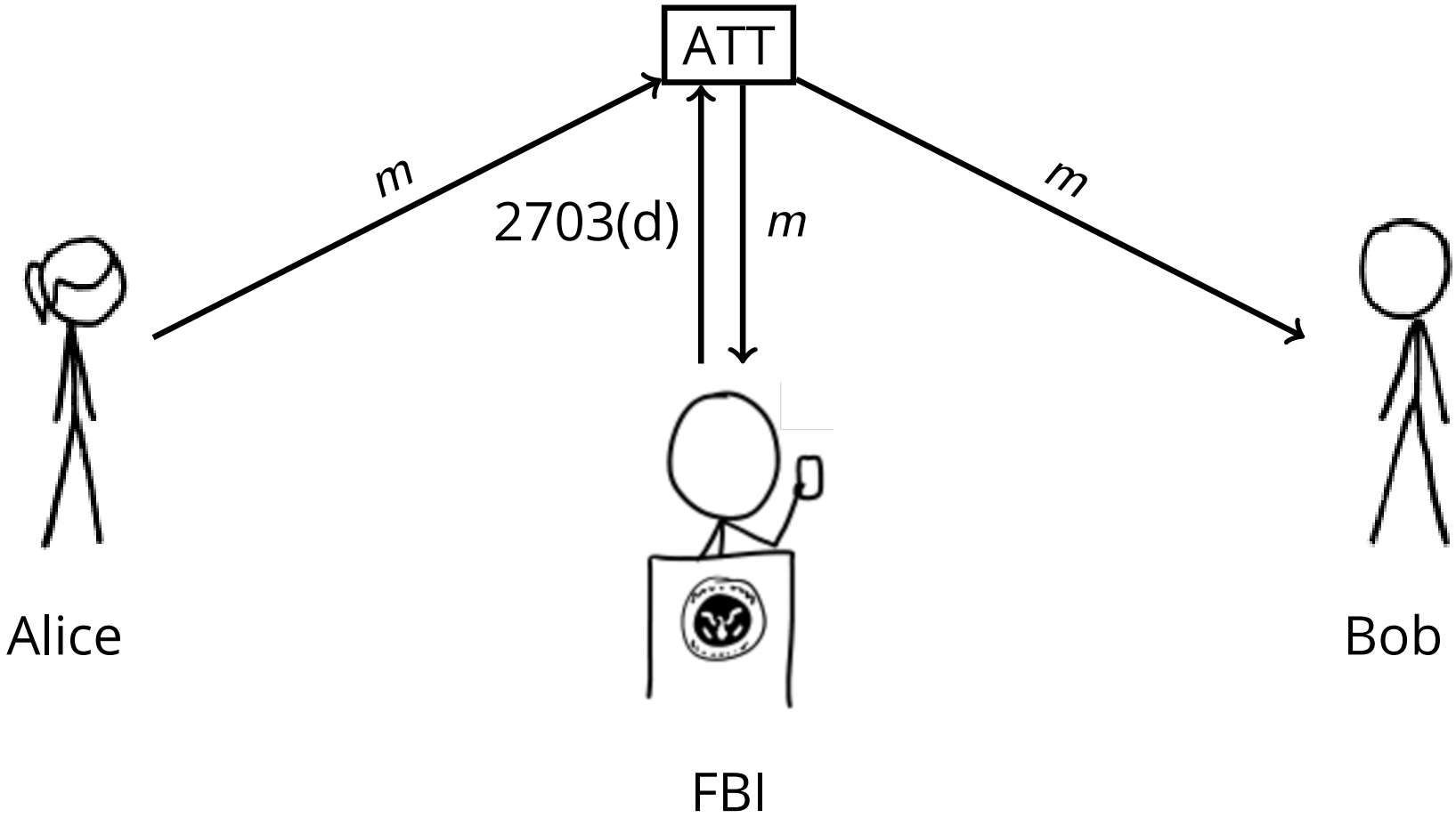


Why is anonymous communication hard?



Communications/network service providers (ISPs, Google, Facebook, etc.) can generally see all traffic or communications they handle.

Why is anonymous communication hard?



Under the Stored Communications Act (1986), the US government can compel service providers to turn over customer communications. Only requires a subpoena for “storage” or communications held longer than 180 days.

Canary
Contact
Newsletters
Donate
Policy
Political Principles
Press
Projects

Search

□□ Español English
Português Русский
Deutsch Français Italiano
Polski Ελληνικά Català
Hindi

Support Riseup!

Bavarian raids

4 Jul, 2018

On June 20th, in order to gather data on a Riseup user, our fiscal sponsor in the EU was raided by the Bavarian police. This extreme overreach included raids on several homes, a hackerspace, a social center, and a lawyer's office. The police took all the computers, cell phones, disks, and records that they could. Several people were arrested and are now out and safe. However, as a consequence of these raids, the police have filed a number of unrelated charges.

What caused the police-state to raise up its ugly head? In this case, the justification was a website created to organize against a rally of an extreme right political party. It seems in Bavaria, you cannot make a website that tries to get people to come protest neo-fascists without also offending the police. The website had a riseup.net email address listed for a contact, and knowing they cannot get information from Riseup, the police looked at Riseup's donate page and found we accept donations in Europe through a non-profit organization ("Verein") based in Germany called Zwiebelfreunde. They decided this meant that Riseup was run by this organization (it is not), and so aggressively targeted this organization.

What does this mean for you, dear Riseup user?

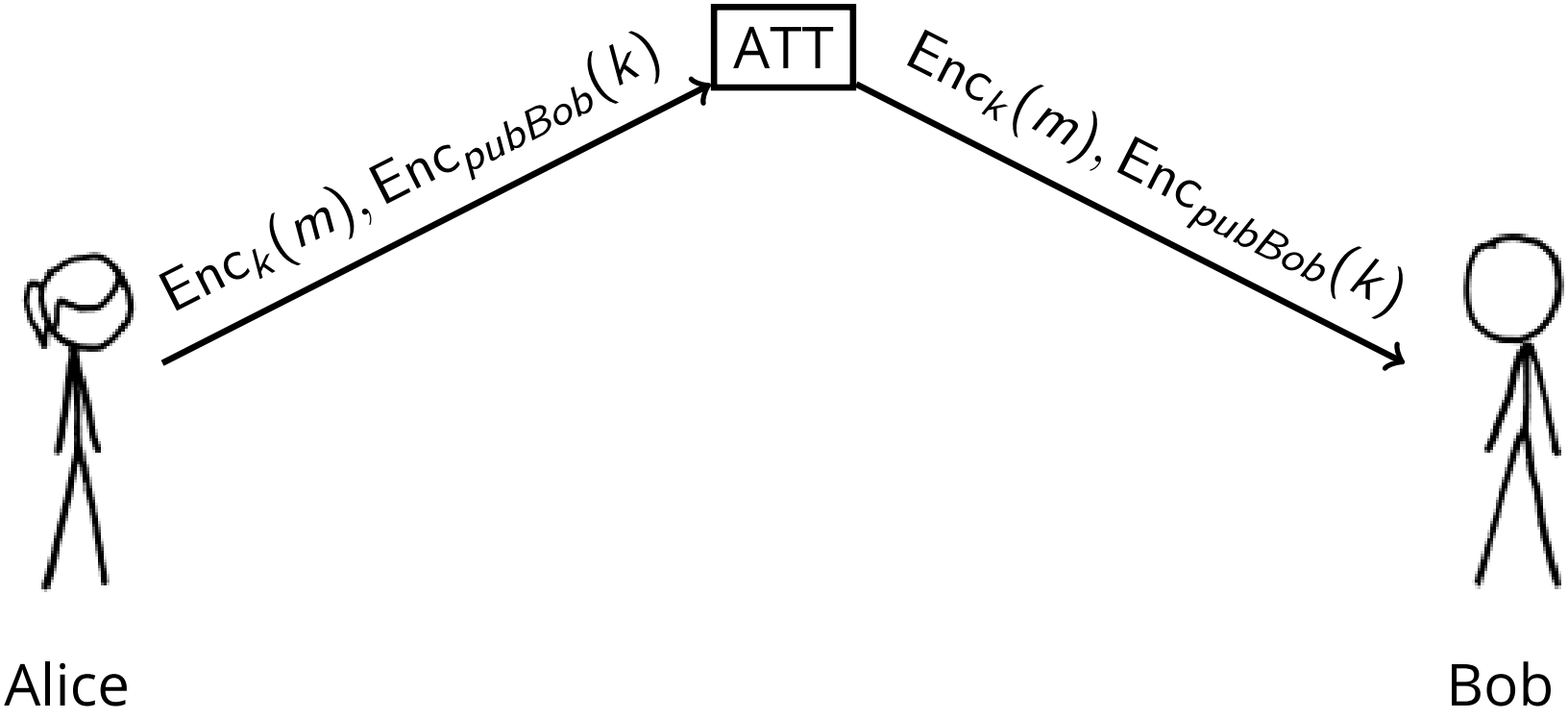
First, don't panic. All your data stored by Riseup is still secure.

Second, if you donated to Riseup via our European IBAN mechanism then there is a good chance the German police now have a record of your bank account number, name, amount you donated, and the date of the donation.

Third, please join us in supporting our friends and allies at Zwiebelfreunde[0]. They are amazing and need your support. In the coming weeks, information will be posted to their website detailing ways that you can help.

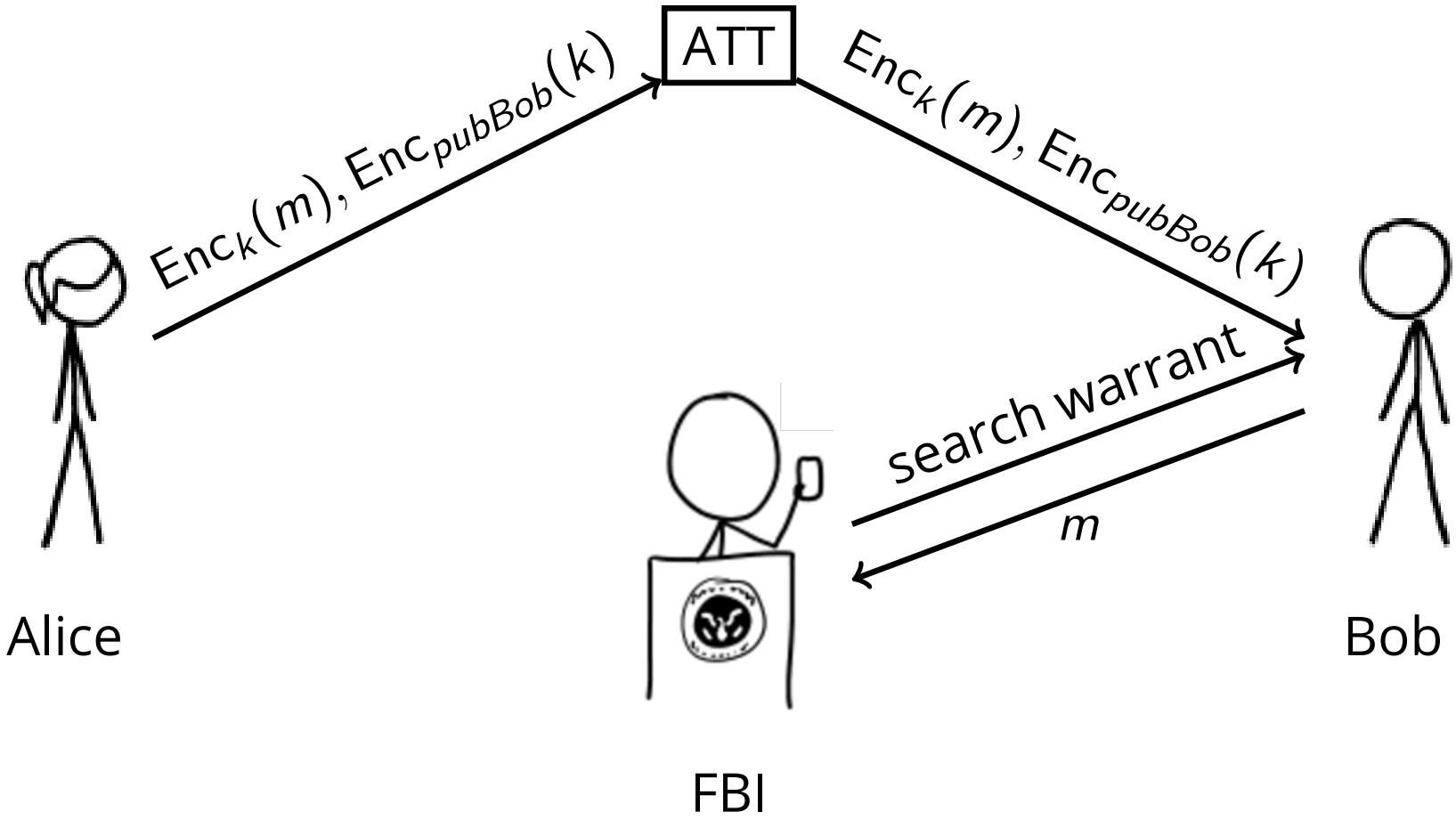
In solidarity,
The Riseup Birds

End-to-end encryption and service providers



If a message is end-to-end encrypted, the service provider may not have the plaintext.

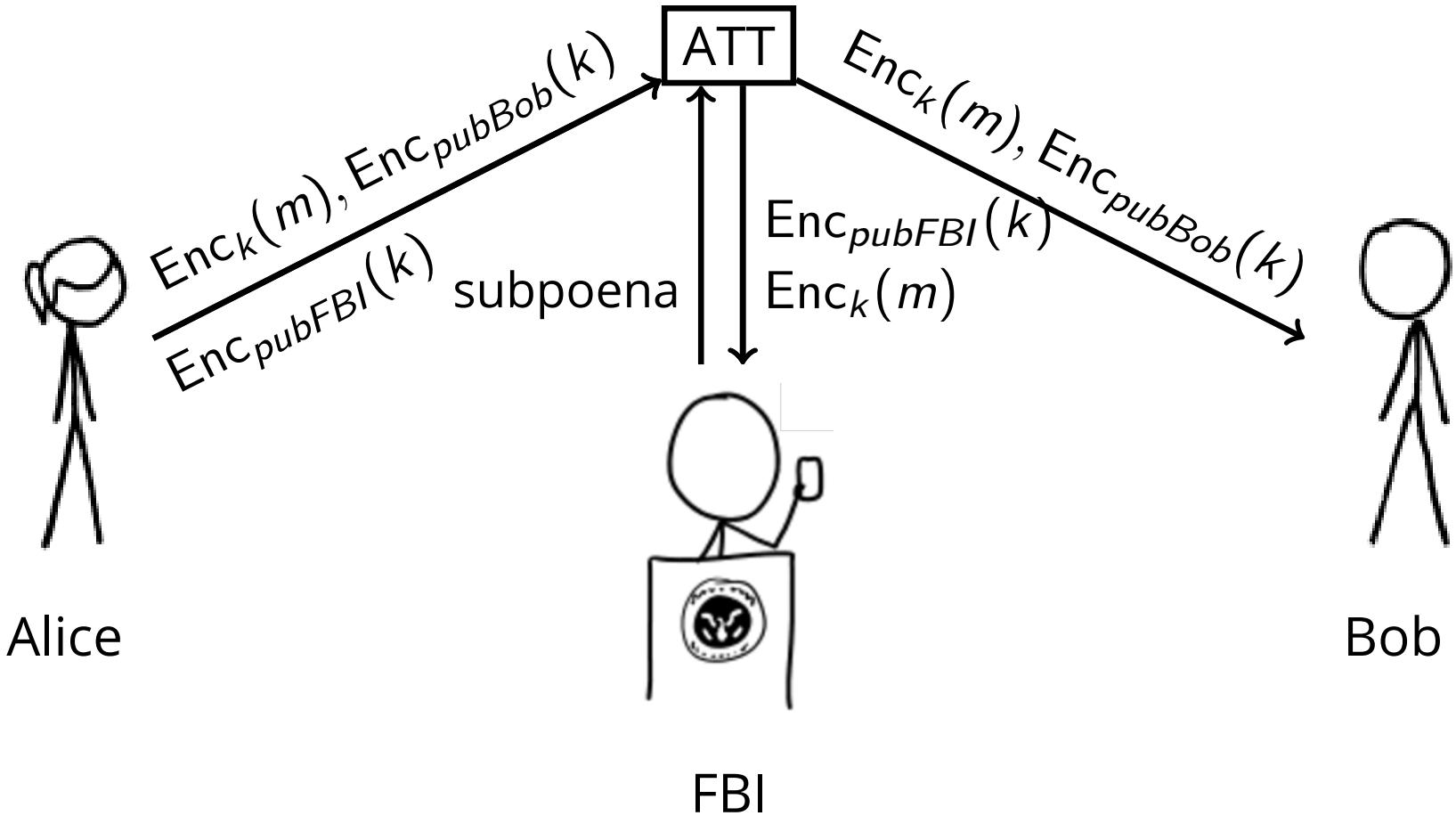
End-to-end encryption and service providers



Law enforcement can always serve the customer with a search warrant for the decrypted communications.

End-to-end encryption and service providers

"Key escrow" or "backdoored encryption"



The US government has been asking service providers to design ways to overcome encryption for decades. Most reasonable proposals work something like this.

End-to-end encryption for messaging

- It all started with PGP (before cryptographic protocol design was properly understood.
- Signal, WhatsApp, Keybase, or iMessage offer modern end-to-end encryption.
- Modern protocols typically:
  - Use Diffie-Hellman to negotiate ephemeral keys
  - Use long-term authentication keys with out-of-band fingerprint verification

End-to-end encryption for messaging

- It all started with PGP (before cryptographic protocol design was properly understood.
- Signal, WhatsApp, Keybase, or iMessage offer modern end-to-end encryption.
- Modern protocols typically:
  - Use Diffie-Hellman to negotiate ephemeral keys
  - Use long-term authentication keys with out-of-band fingerprint verification
  - Offer “forward secrecy”:
    - In theory, protects against key compromise at time t revealing plaintext of previous messages
    - If sender or recipient store plaintext, this is more likely point of compromise

End-to-end encryption for messaging

- It all started with PGP (before cryptographic protocol design was properly understood.
- Signal, WhatsApp, Keybase, or iMessage offer modern end-to-end encryption.
- Modern protocols typically:
  - Use Diffie-Hellman to negotiate ephemeral keys
  - Use long-term authentication keys with out-of-band fingerprint verification
  - Offer “forward secrecy”:
    - In theory, protects against key compromise at time t revealing plaintext of previous messages
    - If sender or recipient store plaintext, this is more likely point of compromise
  - Offer “deniability”:
    - Message recipient can verify message integrity without a third party being able to “cryptographically prove” that sender sent the message.
    - Cryptographically interesting, but likely legally irrelevant.

Crypto Wars 2.0

In the current debates about government-mandated weakening of cryptography, there are two scenarios of interest:

- Message encryption.
  - This is what we've talked about so far in lecture.

- Storage encryption.
  - For example, unlocking iPhones.
  - This is what the Apple v. FBI case was about.

In Apple v. FBI, the question was whether the government could compel Apple to break their own encryption mechanism with the All Writs Act. The government backed down and reportedly used a specialty consulting firm to unlock the phone.

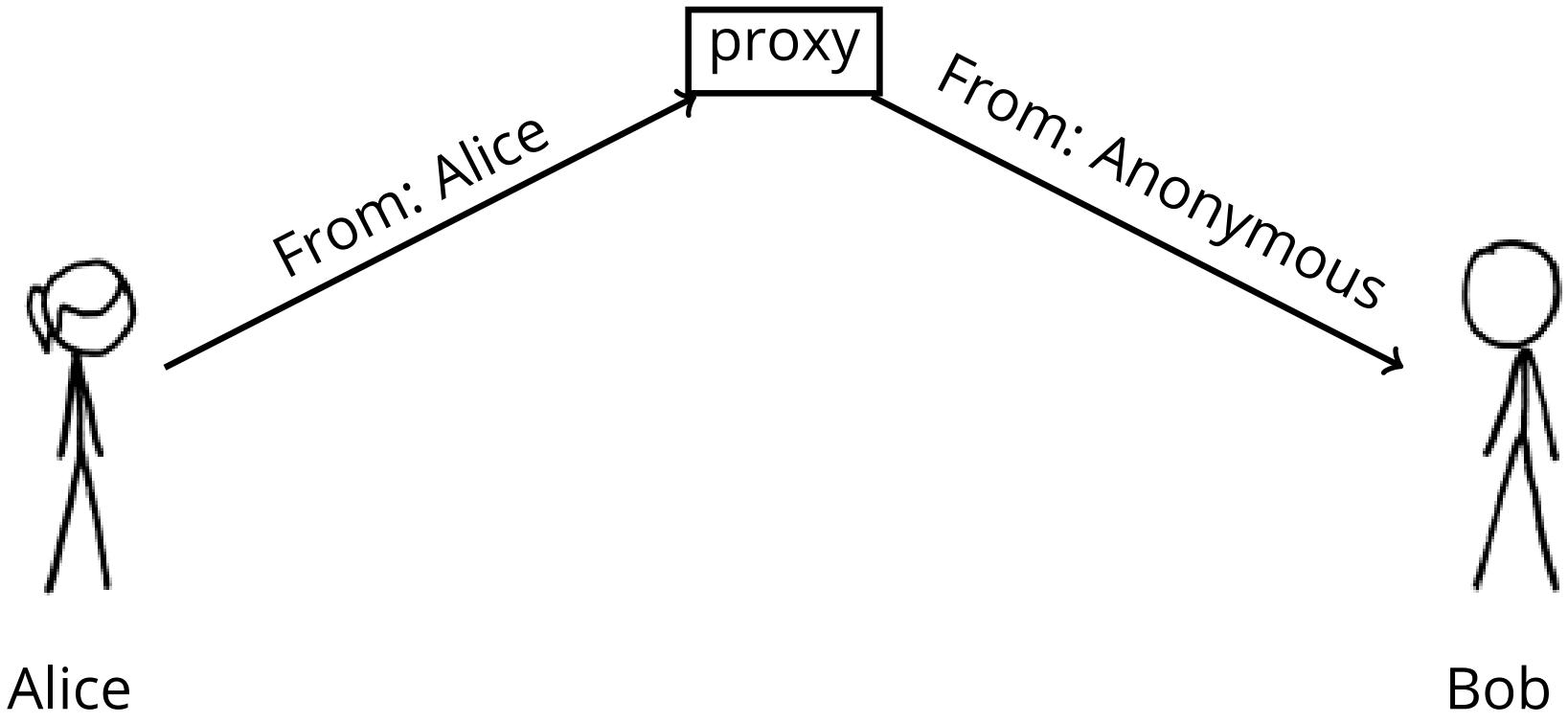
Anonymity

Michael Hayden, former NSA director: “We kill people based on metadata.”

- Long history of anonymous communication in US democracy
- e.g. Revolutionary war anonymous political pamphlets

Technical question: Is anonymous communication still feasible on the internet?

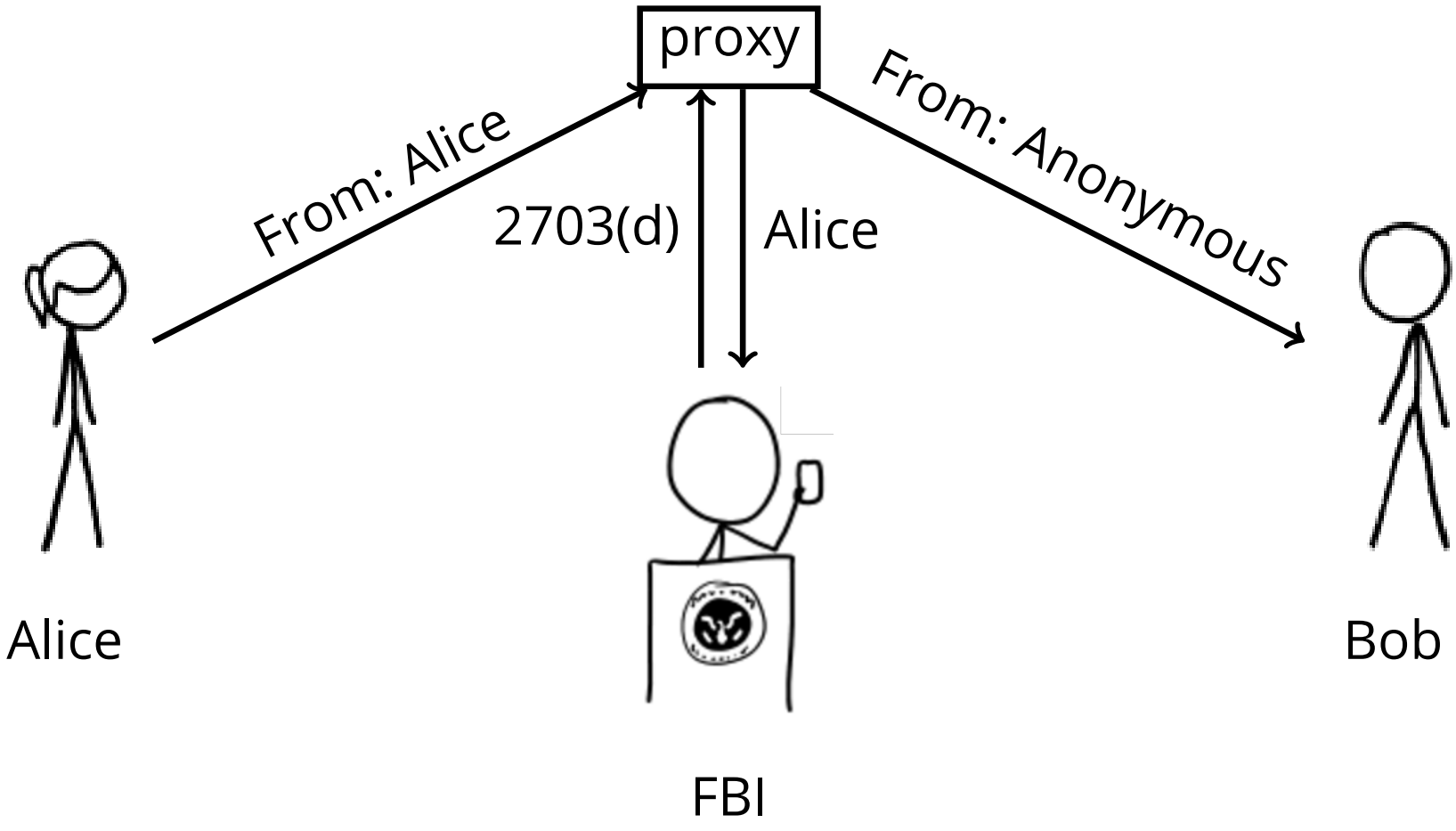
“Anonymity” via tunneling or proxies



A proxy can rewrite metadata. Examples:

- Early “anonymous remailers” forwarded email.
- VPN services allow users to tunnel traffic

“Anonymity” via tunneling or proxies



One-hop proxies have a single point of failure, must see both sides of communication.

Tor: Anonymous communication for TCP sessions

Desired properties:

- Network attacker watching client traffic can't see destination.
- Destination server does not see client IP address.
- Network nodes can't link client and server.
- Fast enough to support TCP streams and network applications.

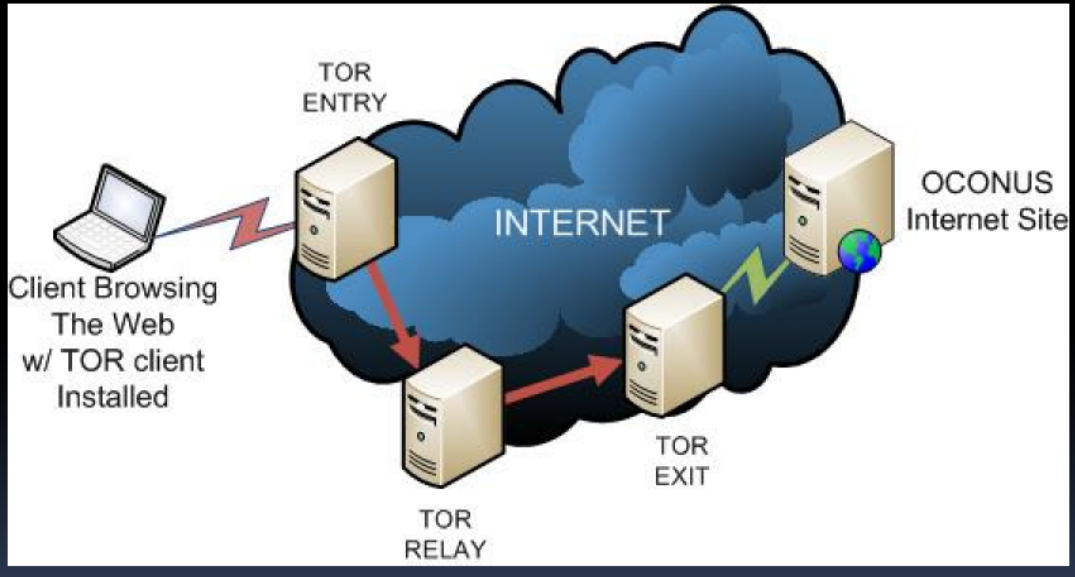
Current state: A nonprofit organization, active academic research, deployed around the world.

Not perfect, but a building block.

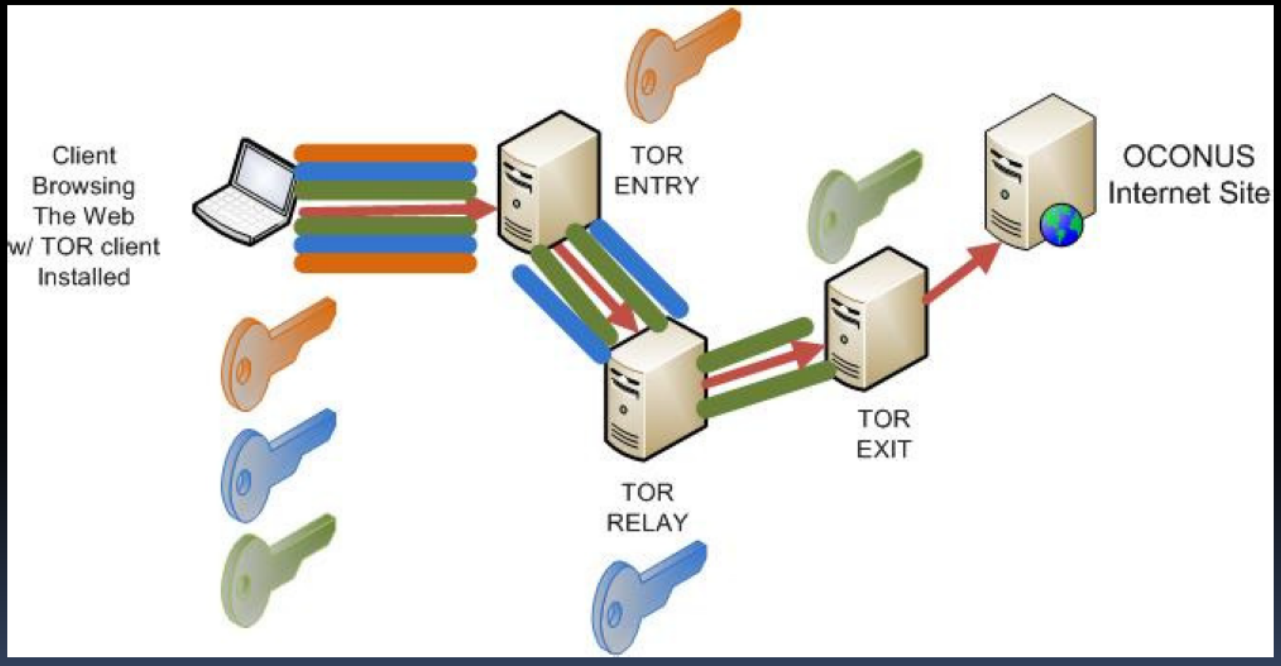
(U) What is TOR?

- (U) "The Onion Router"
- (U) Enables anonymous internet activity
  - General privacy
  - Non-attribution
  - Circumvention of nation state internet policies
- (U) Hundreds of thousands of users
  - Dissidents (Iran, China, etc)
  - (S//SI//REL) **Terrorists!**
  - (S//SI//REL) Other targets too!

(U) What is TOR?


TOR
ENTRY
INTERNET
OCONUS
Internet Site
Client Browsing
The Web
w/ TOR client
Installed
TOR
EXIT
TOR
RELAY

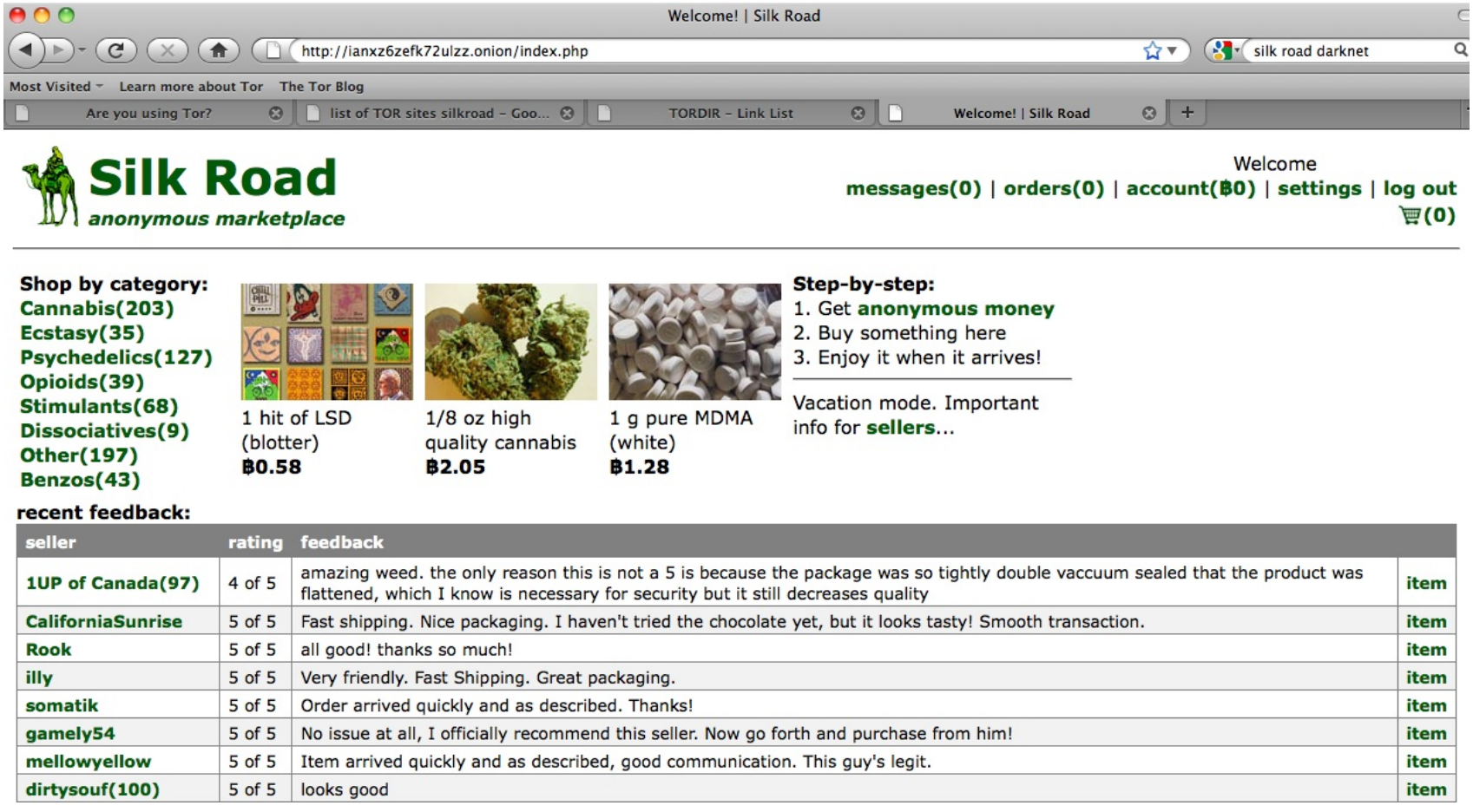
(U) What is TOR?


Client
Browsing
The Web
w/ TOR client
Installed
TOR
ENTRY
TOR
RELAY
TOR
EXIT
OCONUS
Internet Site

(U) What is TOR?

- (U) TOR Browser Bundle
  - Portable Firefox 10 ESR (tbb-firefox.exe)
  - Vidalia
  - Polipo
  - TorButton
  - TOR
  - "Idiot-proof"

Tor also allows “anonymous” servers



vice.com

In practice, prominent “hidden services” deanonymized through real-world metadata, browser 0days, misconfigured servers.

Stinks (U)

[redacted]

CT SIGDEV

[redacted]

JUN 2012

Tor Stinks… (U)

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a **very small fraction** of Tor users, however, **no** success de-anonymizing a user in response to a TOPI request/on demand.

[redacted]

Traffic correlation

8. In the course of this investigation, I have learned that the person who sent the e-mail messages described above took steps to disguise his identity. Specifically, Harvard received the e-mail messages from a service called Guerrilla Mail, an Internet application that creates temporary and anonymous e-mail addresses available free of charge. Further investigation yielded information that the person who sent the e-mail messages accessed Guerrilla Mail by using a product called TOR, which is also available free of charge on the Internet and which automatically assigns an anonymous Internet Protocol ("IP") address that can be used for a limited period of time. Every computer attached to the Internet uses an IP address, which is a unique numerical identifier, to identify itself to other computers on the Internet and direct the orderly flow of electronic information between them. IP addresses typically consist of four numbers between 0 and 255 separated by periods (*e.g.*, 216.239.51.99). Both TOR and Guerilla Mail are commonly used by Internet users seeking to communicate anonymously and in a manner that makes it difficult to trace the IP address of the computer being used.

9. Harvard University was able to determine that, in the several hours leading up to the receipt of the e-mail messages described above, ELDO KIM accessed TOR using Harvard's

Anonymity on the web

- Companies like Google, Facebook, Twitter, Microsoft, Amazon, Target, Walmart, . . . make a lot of money from tracking users.
- For some of these companies you are the product. So tracking you is their business.

Anonymity on the web

- Companies like Google, Facebook, Twitter, Microsoft, Amazon, Target, Walmart, . . . make a lot of money from tracking users.
- For some of these companies you are the product. So tracking you is their business.
- How do websites track users?

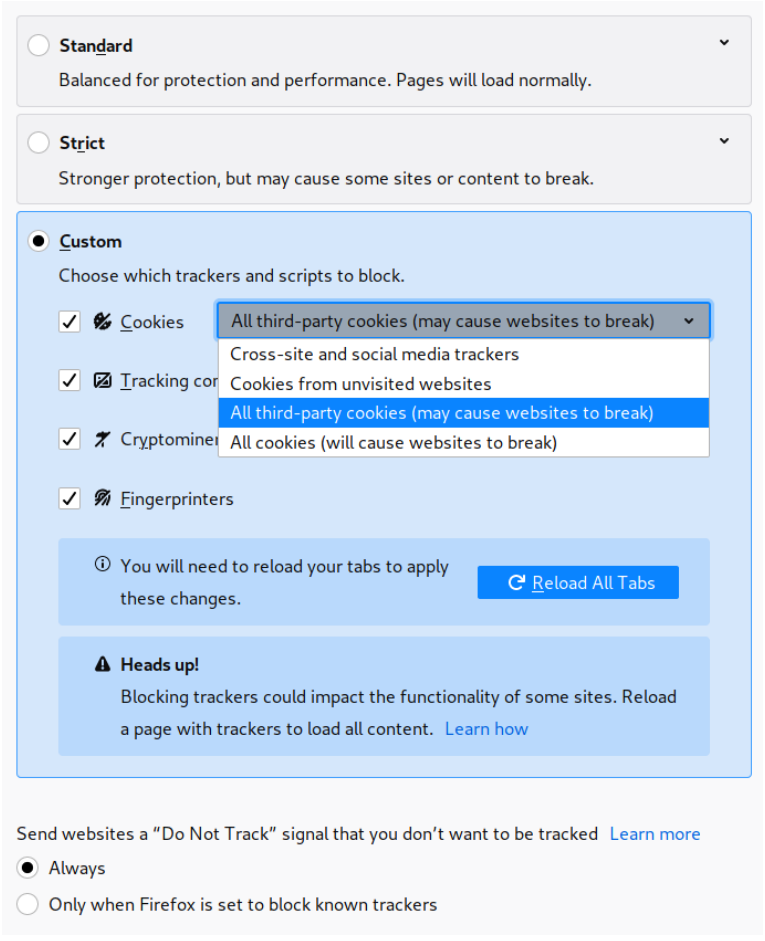
Anonymity on the web

- Companies like Google, Facebook, Twitter, Microsoft, Amazon, Target, Walmart, . . . make a lot of money from tracking users.
- For some of these companies you are the product. So tracking you is their business.
- How do websites track users?
  - Third-party cookies: cookies for `trackme.com` are sent with any request to `trackme.com` if `SameSite=None`, even if you're on `cnn.com`.
  - Tracking content: Sites include tracking code into URLs (e.g., advertisements, videos, marketing emails, etc.)
  - Fingerprinting: sites profile your browser, extensions, OS, hardware, screen resolution, fonts you have installed, etc.

What can you do about this?

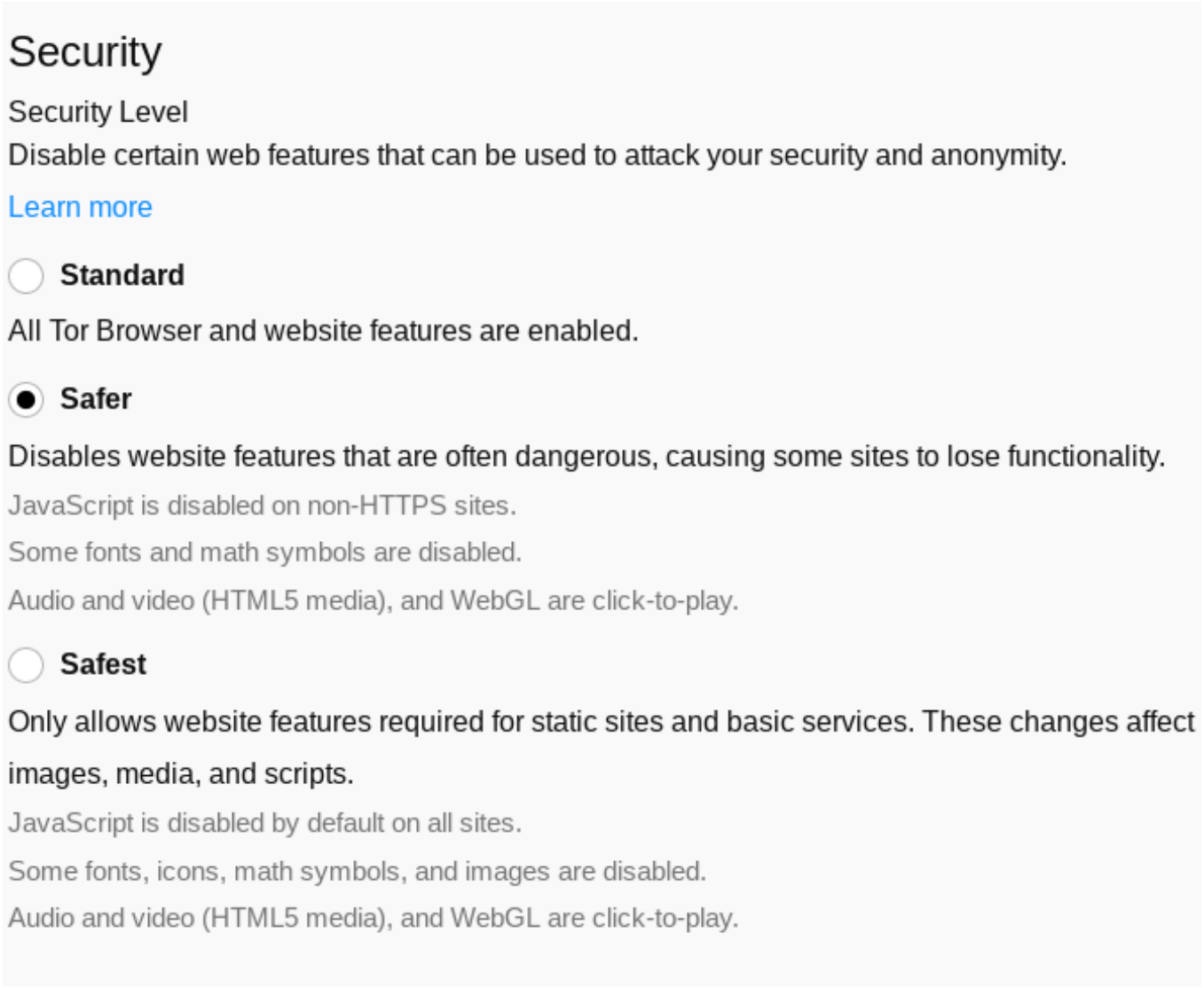
- Can’t really avoid these platforms (e.g., Facebook profiles you even if you don’t have an account).
- Use a browser that cares about your privacy (e.g., Firefox, The Tor Browser, Brave, Safari)
- Use privacy-enhancing browser extensions

Privacy-enhanced browsing (Firefox)

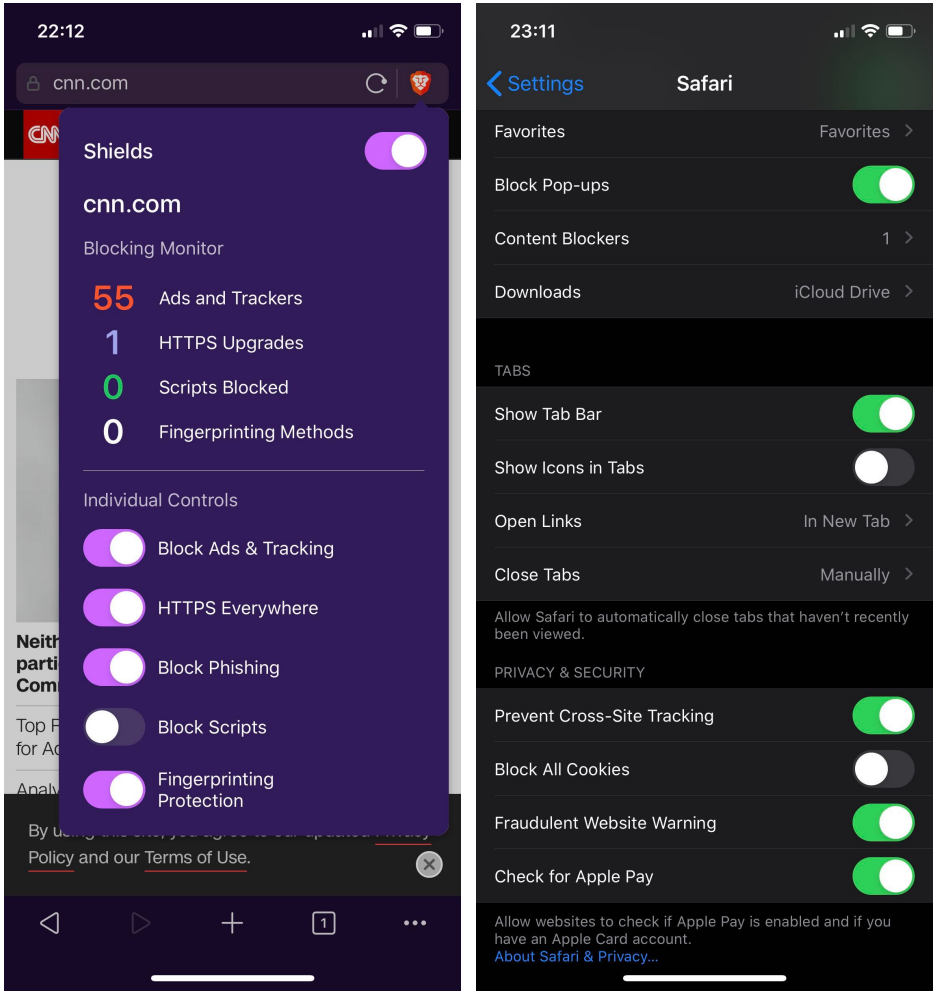


+ Firefox containers!

Privacy-enhanced browsing (Tor)

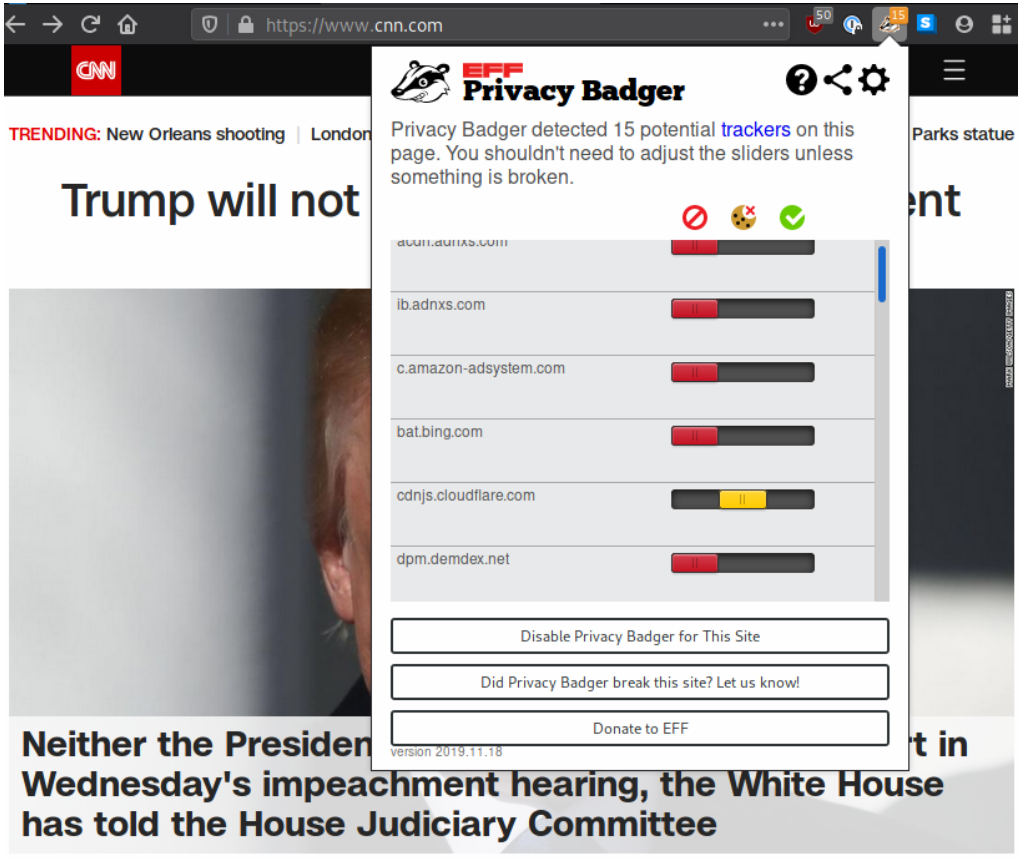


Privacy-enhanced browsing (Brave & Safari)



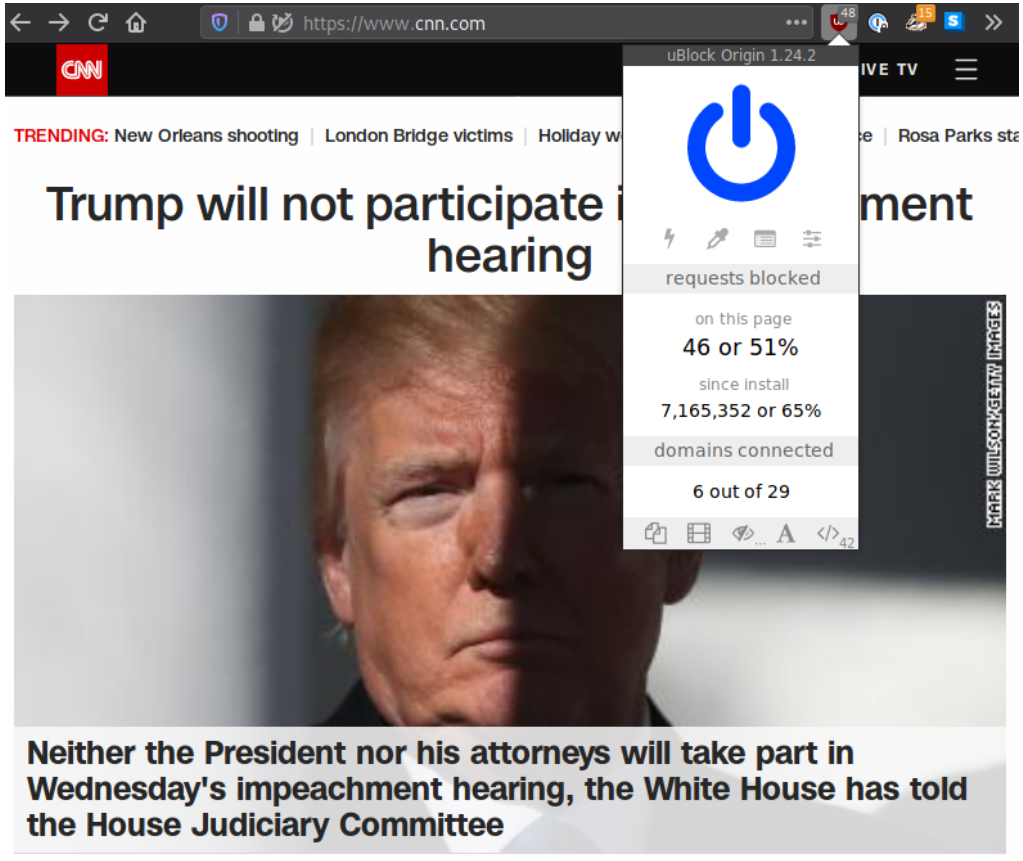
Privacy-enchaning extensions

- Privacy Badger blocks trackers; uBlock Origin blocks ads; many others



Privacy-enchaning extensions

- Privacy Badger blocks trackers; uBlock Origin blocks ads; many others



Lecture outline

- Foundations of privacy
- Privacy-enhancing technologies
  - PGP and modern encrypted messaging
  - Tor and anonymous communication
  - Privacy-respecting browsers (Tor, Firefox, Brave)
- Ethical principles
- Laws relevant to security research and practice

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.)

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

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
- 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?

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?

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.

4th amendment and electronic search

"The right of the people to be secure in their . . . effects, against unreasonable searches and seizures . . . , and no warrants shall issue, but upon probable cause, . . . describing the . . . things to be seized."

- 1928 Olmstead v. US: Wiretapping is not seizure for 4th amendment purposes.
- 1967 Katz v. US: Physical intrusion isn't necessary for a 4th amendment search
- 1968 Omnibus Crime Control and Safe Streets Act: Wiretapping is legal with a search warrant
- 1986 Electronic Communications Privacy Act:
  - Law enforcement can get customer records or stored email (> 6 months) with a subpoena
  - Email contents in storage for < 6 months require a search warrant
- 1994 CALEA: Telecom providers must build wiretapping infrastructure
- 2018 Carpenter v. US: Law enforcement needs a warrant to obtain cell phone location information.

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 13-80

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 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

TOP SECRET//SI//NOFORN

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

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.

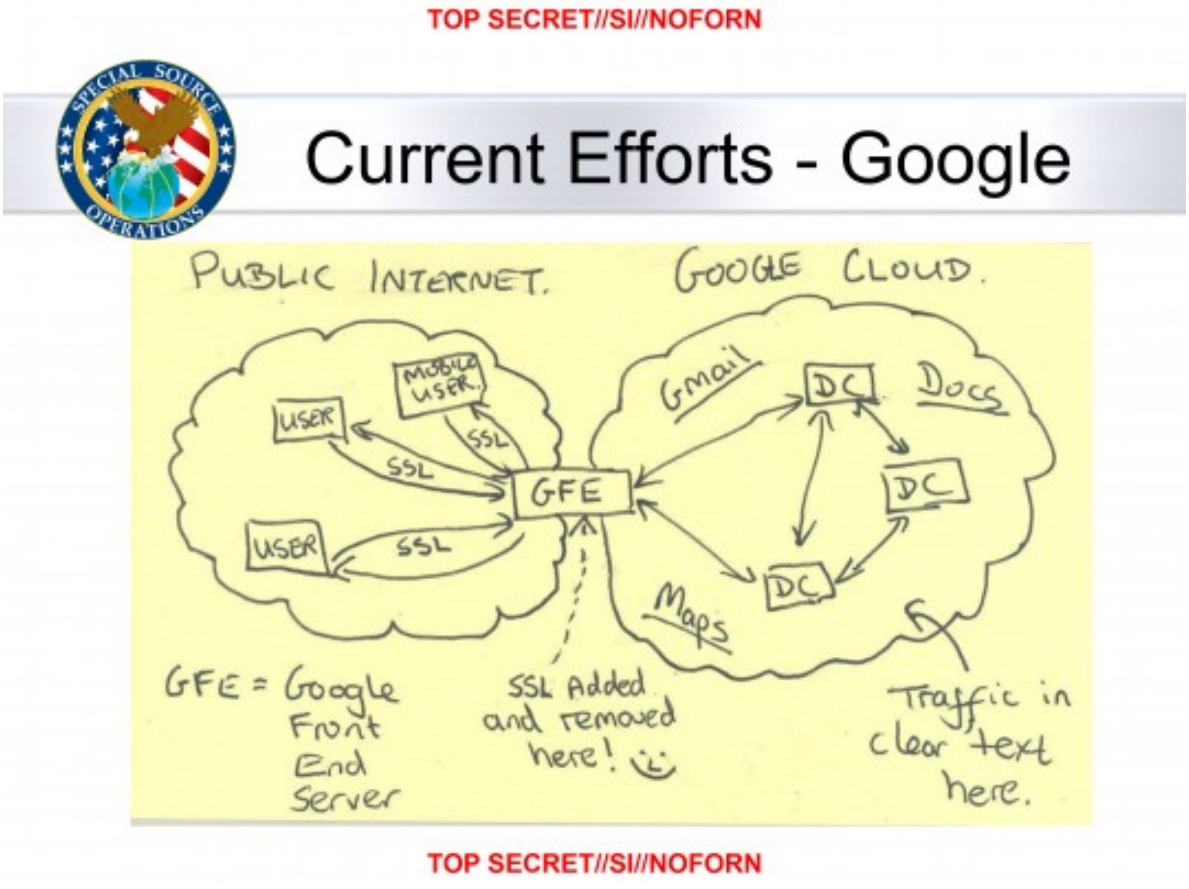
Enlarge This Image

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.

October 2013: MUSCULAR



Official Google statement:
“We are outraged”

Unofficial Google statement: “**** you.”

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

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
- 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
- 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
- Students have made $3-10K per bug!

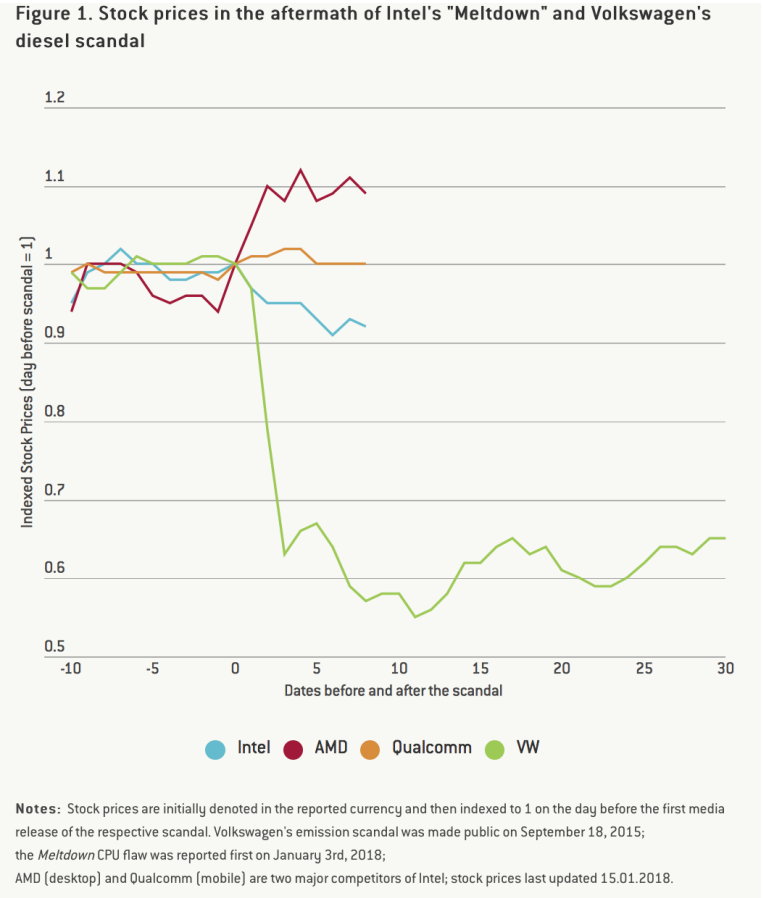
	High-quality report with functional exploit	High-quality report	Baseline
Sandbox escape / Memory corruption in a non-sandboxed process	$30,000	$20,000	$5,000 - $15,000
Universal Cross Site Scripting	$20,000	$15,000	$2,000 - $10,000
Renderer RCE / memory corruption in a sandboxed process	$10,000	$7,500	$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	See below		
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

Stock market says not really:



nakedcapitalism.com

Policy questions around security research

- Should exploit sales be legal?
  - Code as speech principle says yes
  - Is publishing exploits ethical?
    - Today's news: Researcher publishes Microsoft Exchange exploit code to Github.
    - Github (owned by Microsoft) takes it down.
- How about mixed-use tools?
  - Privacy tools like Tor or encrypted messengers used by criminals, normal people, activists
  - Random darknet shopper art piece?

Personal security hygiene.

Back up your computers

- If you can, keep a local (auto-backup to external drive) and a remote (rsync, Dropbox, Github) backup.

What threats does this help mitigate?

Password security

- Use a different password for every single web site.
- Use a password manager to store your passwords for you.
- Turn on two-factor authentication whenever it is available.
- Use public-key authentication for SSH servers.
- Be careful about phishing attempts.

What threats does this help mitigate?

Encrypt your laptop and phone hard drive

- OS X: Filevault; Windows: BitLocker; Linux: luks, dm-crypt, etc.
- Also set a lock screen with a password.

What threats does this help mitigate?

Maintaining computer hygiene

- Keep your OS and software up to date.
- Don’t install random software or apps.
- Use browser to preview files.
- Use a VM to open sketchy files or run software you don’t trust.

What threats does this help mitigate?

Web privacy

- Keep your browser up to date (largely done for you).
- Consider using a privacy-focused browser like Tor, Firefox, or Brave.
- Use containers if your browser supports it (Firefox).
- Use an ad-blocker like uBlockOrigin.
- Consider DNS sinkholing.

What threats does this help mitigate?

Travel and transit

- Consider using a VPN or Tor when on untrusted WiFi.
- You can also use a SSH tunnel in a pinch.
- Consider having a minimal travel laptop.

What threats does this help mitigate?

Encryption applications

- Encrypted chat: Signal; WhatsApp also uses Signal protocol
- Make sure your web sites support HTTPS
- PGP (ugh) is probably still the best option for sending encrypted email or files

What threats does this help mitigate?

Wed: Invited talk + short review.

Fri: Final review.