CSE 127: Intro to Computer Security

WI24

Lecture 17 - Privacy

Slide Credit: Kirill Levchenko, Stefan Savage, Deian Stefan, Nadia Heninger, Earlence Fernandes, Imani Munyaka

Announcements

HW/PA 5 out

Discussion Friday

Let me know if there is a topic I should double back on for Thursday

Lecture outline

- Foundations of privacy
- Privacy-enhancing technologies
  - PGP and modern encrypted messaging
  - Tor and anonymous communication
  - Privacy-respecting browsers (Tor, Firefox, Brave)

What is privacy and why do we care?

Various definitions of privacy:

- Secrecy
- Anonymity
- Solitude

Political and democratic values:

- Liberty of action
- Moral autonomy

Human rights and values:

- Human dignity
- Mental health
- Intimacy/relationships

Privacy

- “Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” – Westin (Privacy and Freedom)
  - Being able to control what information people know about you in a meaningful way

Privacy Taxonomy

- Information collection
- Information processing
- Information dissemination
- Invasion

Privacy Taxonomy

- **Information collection**
  - Surveillance
  - Interrogation
- **Information processing**
  - Aggregation
  - Identification
  - Insecurity
  - Secondary use
  - Exclusion
- **Information dissemination**
  - Breach of confidentiality
  - Disclosure
  - Exposure
  - Blackmail
  - Appropriation
  - Distortion
- **Invasion**
  - Intrusion
  - Decisional interference

Privacy vs Secrecy (dictionary.com)

- Privacy -the state or condition of being free from being observed or disturbed by other people
- Secrecy - the action of keeping something secret or the state of being kept secret.

End to End encryption

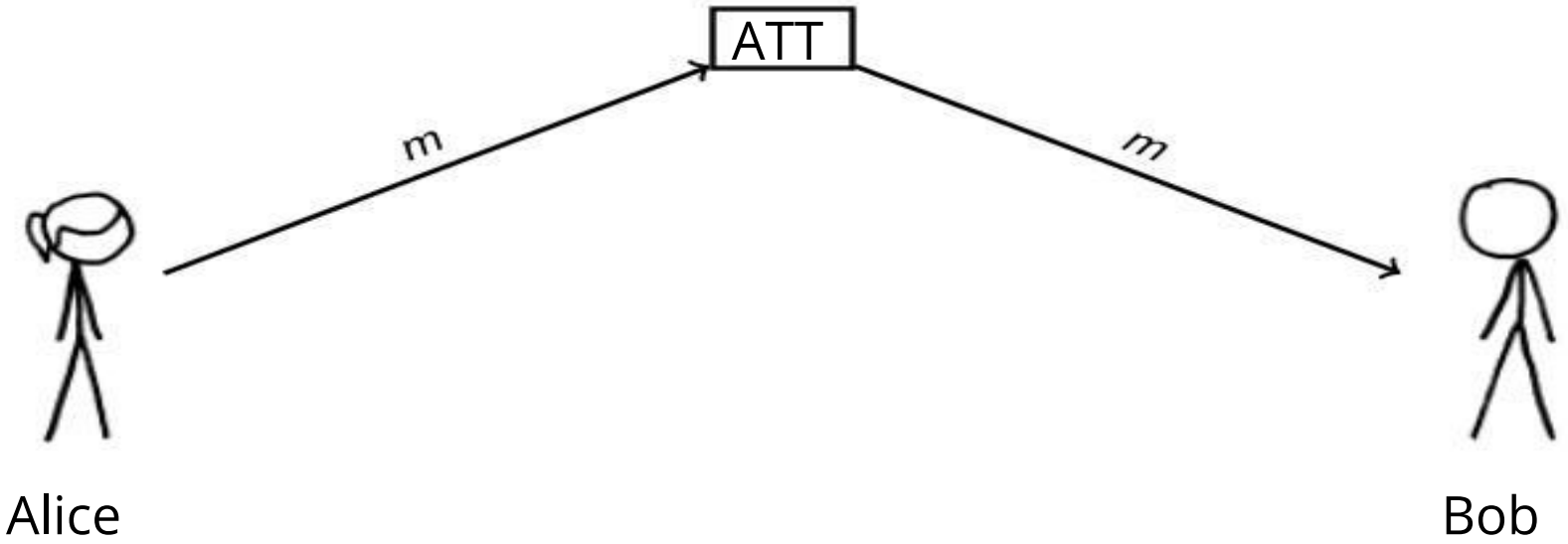
- E2EE - information that is encrypted from one point to another and can only be decrypted by the receiver.

Is HTTPS E2E Encryption?

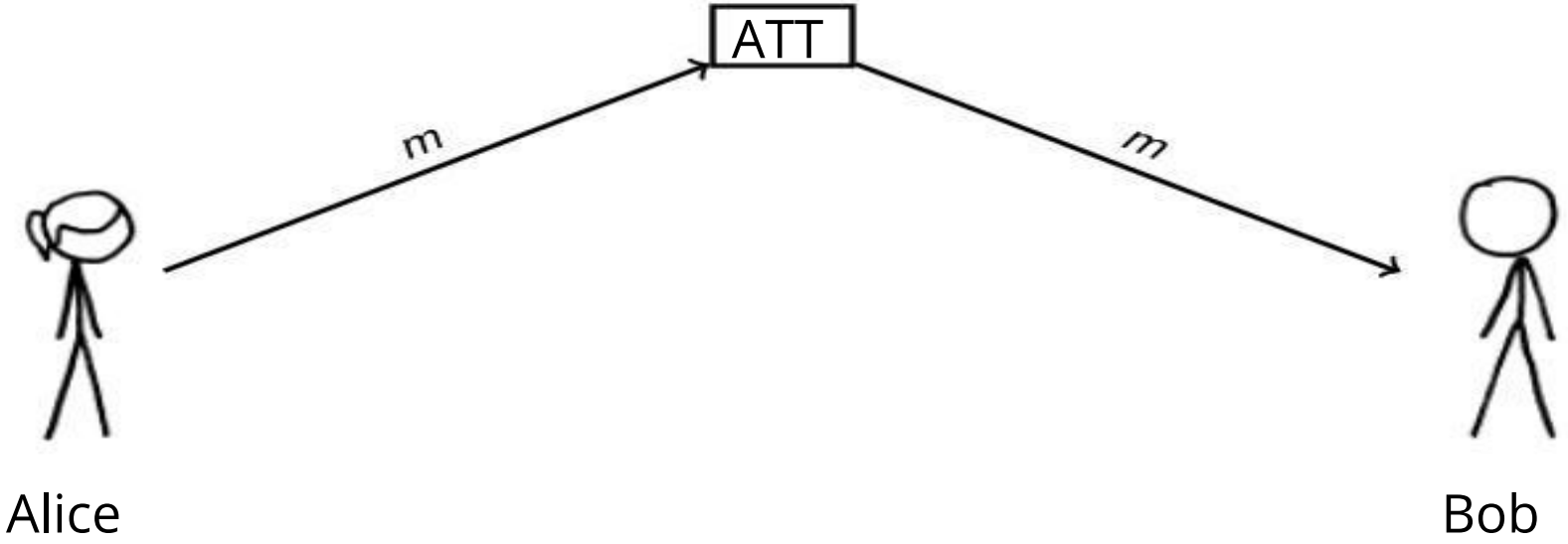
The “crypto wars”: privacy vs. wiretapping

- 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
  - Now
  - Snowden
  - Apple v. FBI • …?
  - Calls for “balance”

The internet was not designed for privacy

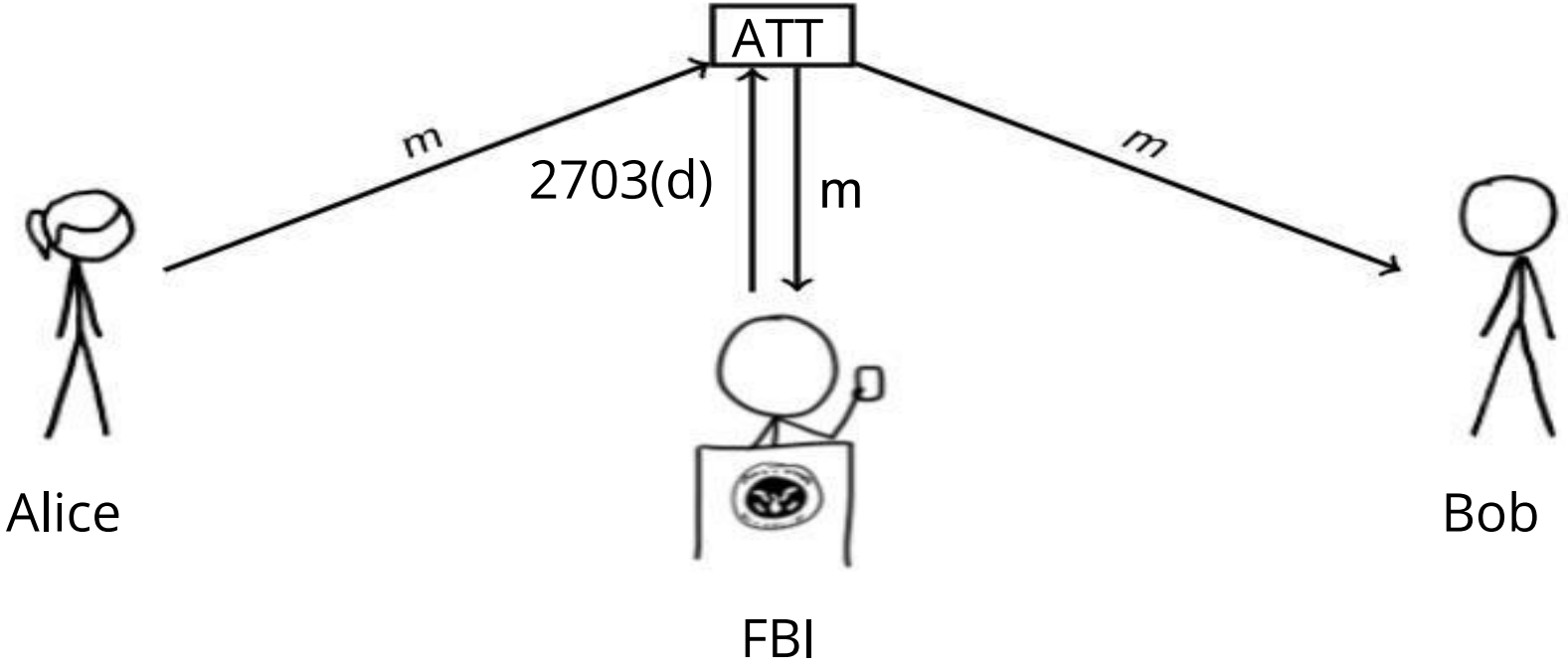


The internet was not designed for privacy



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

The internet was not designed for privacy



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 Catala
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?

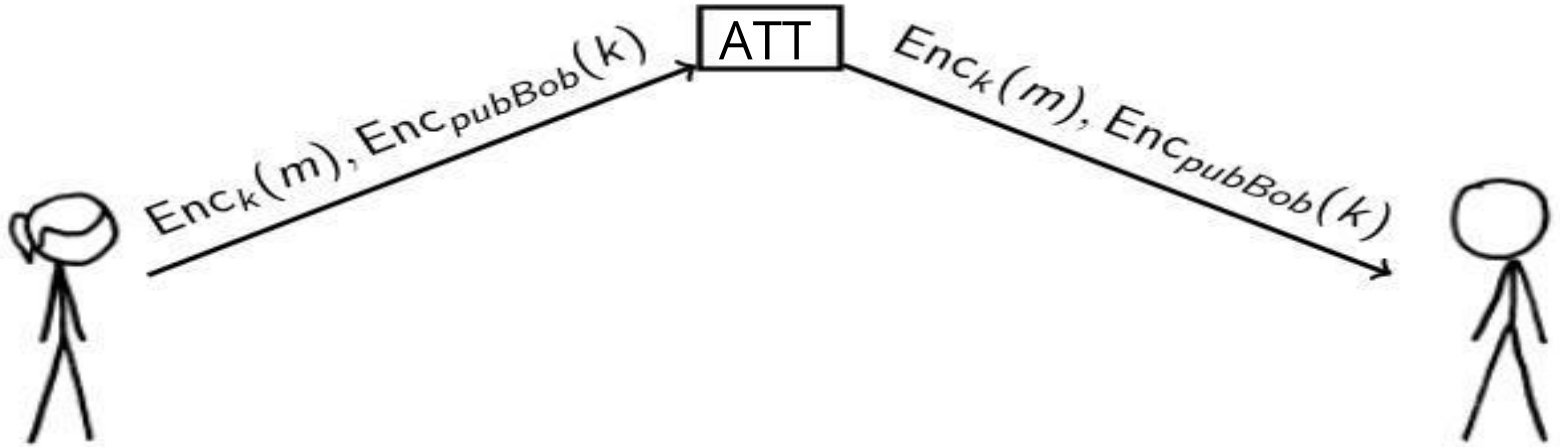
First, don't panic. All your data stored by Riseup is still secure.

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.

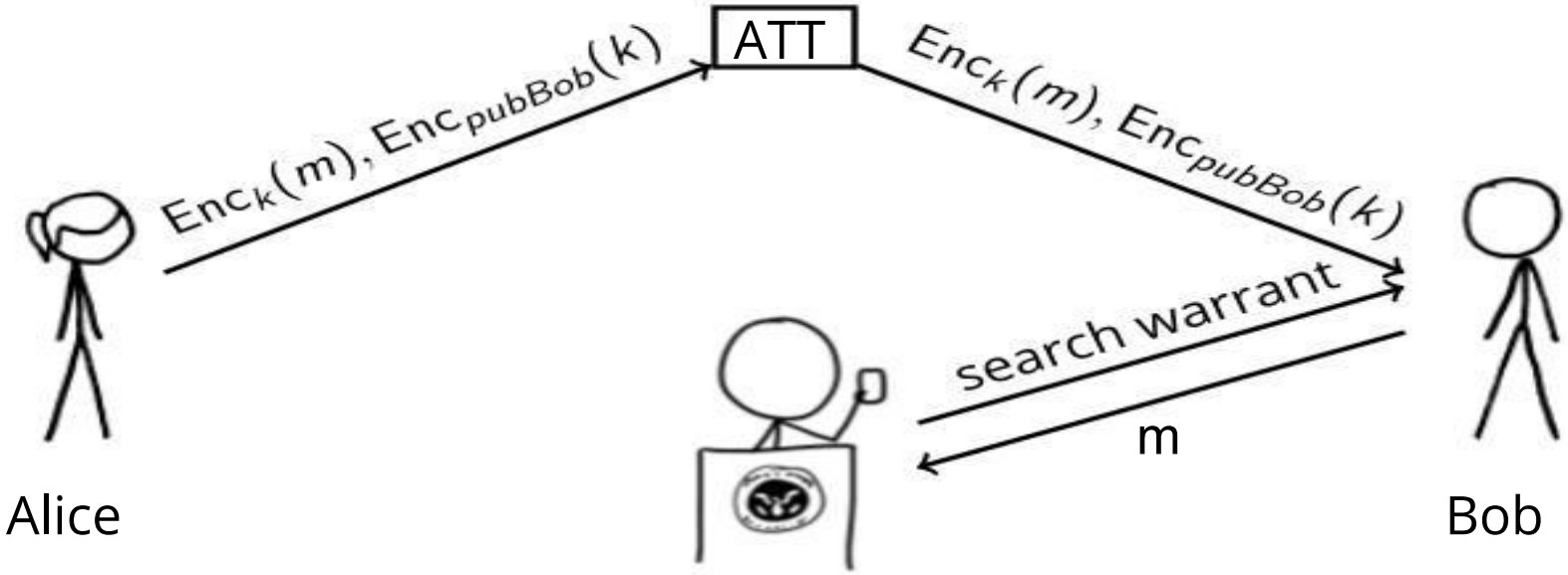
In solidarity,
The Riseup Birds

End-to-end encryption and service providers



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

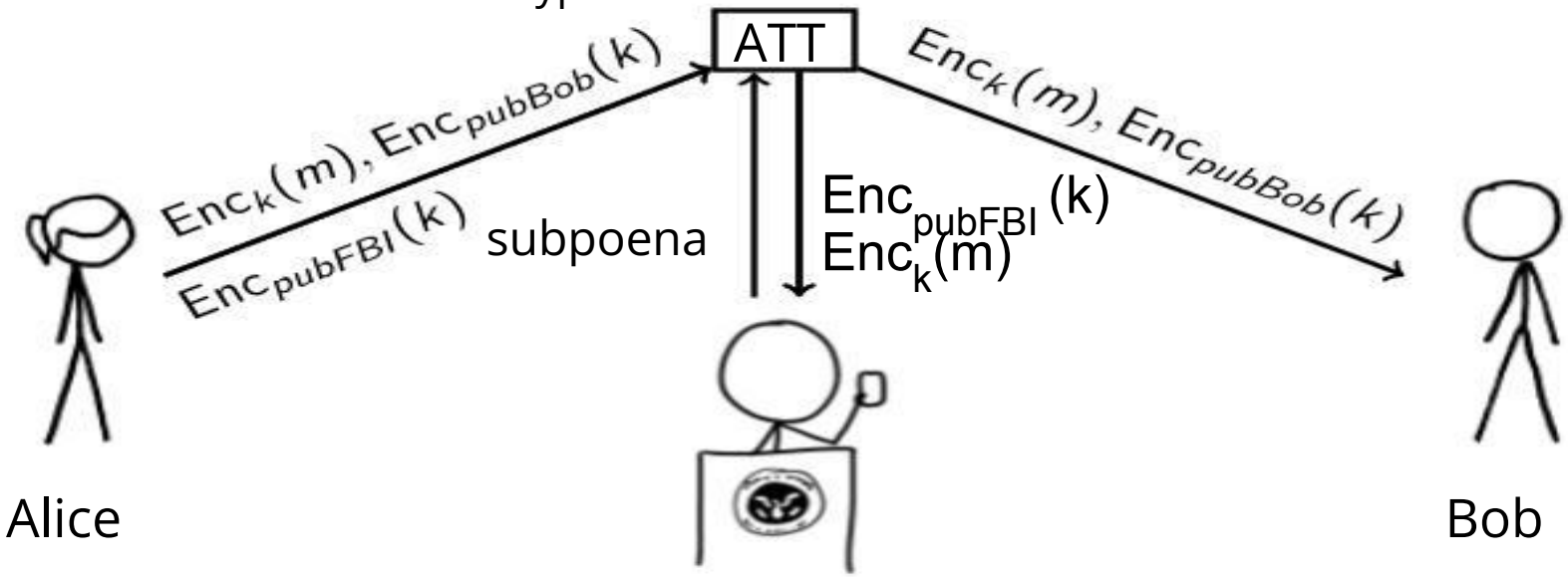
End-to-end encryption and service providers



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.

History of US export controls on cryptography

Pre-1994: Encryption software requires individual export license as a munition.

1994: US State Department amends ITAR regulations to allow export of approved software to approved countries without individual licenses. 40-bit symmetric cryptography was understood to be approved.

1995: Netscape develops initial SSL protocol. Includes weakened “export” cipher suites.

1996: Bernstein v. United States; California judge rules ITAR regulations are unconstitutional because “code is speech”

1996: Cryptography regulation moved to Department of Commerce.

1999: TLS 1.0 standardized. Includes weakened “export” cipher suites.

2000: Department of Commerce loosens regulations on mass-market and open source software.

International Traffic in Arms Regulations

April 1, 1992 version

Category XIII--Auxiliary Military Equipment ...

(b) Information Security Systems and equipment, cryptographic devices, software, and components specifically designed or modified therefore, including:

(1) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, except cryptographic equipment and software as follows:

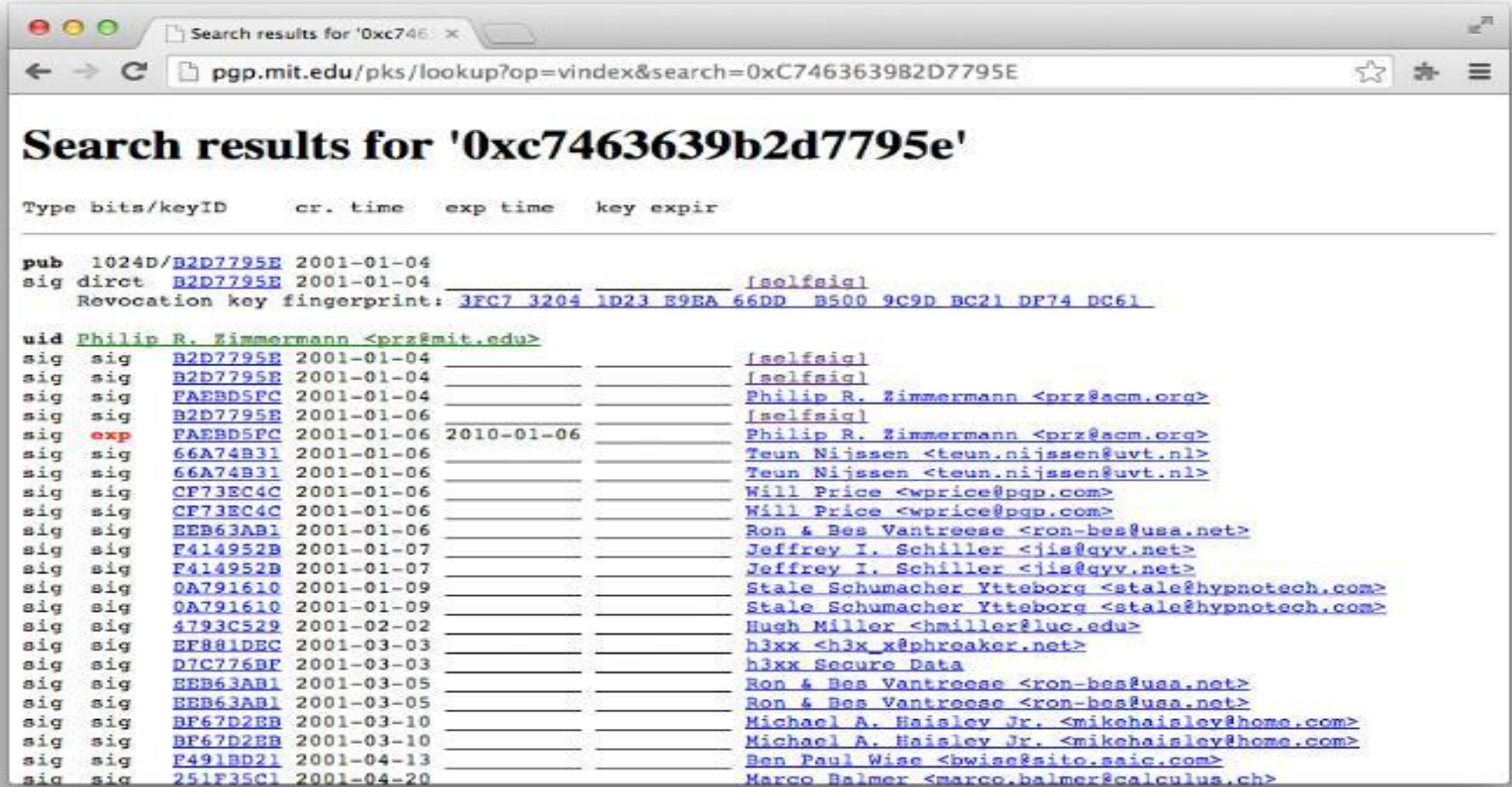
(i) Restricted to decryption functions specifically designed to allow the execution of copy protected software, provided the decryption functions are not user-accessible.

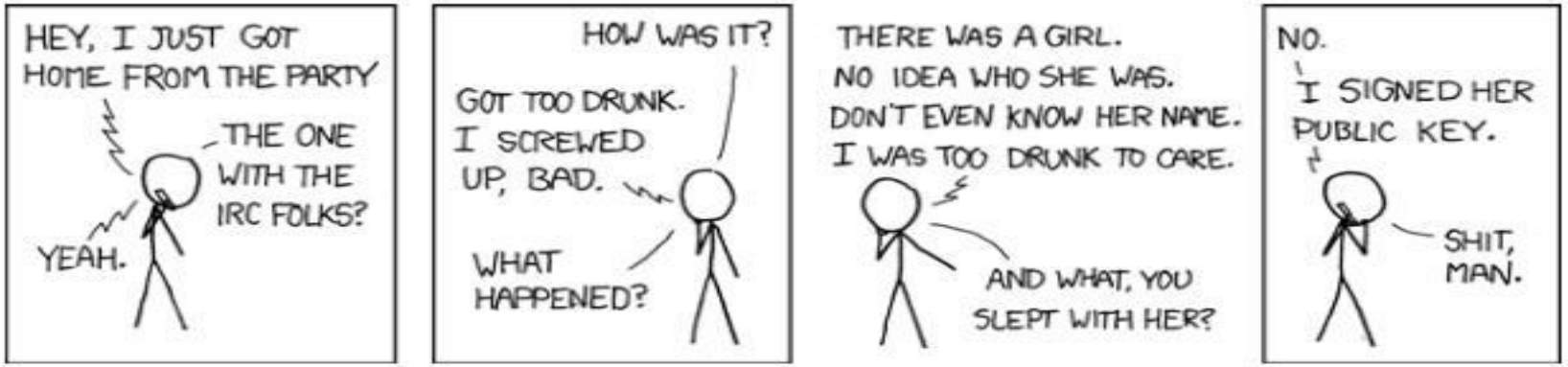
(ii) Specially designed, developed or modified for use in machines for banking or money transactions, and restricted to use only in such transactions. Machines for banking or money transactions include automatic teller machines, self-service statement printers, point of sale terminals or equipment for the encryption of interbanking transactions.

...

Pretty Good Privacy (PGP)

- Written by Phil Zimmermann in 1991 in response to a senate bill requiring crypto backdoors
- Public key email encryption “for the masses”
  - Signatures, public key encryption, or sign+encrypt
- Key management
  - Public keyservers
  - Web of trust: users sign other users’ keys
- Grand jury investigated Zimmermann 1993–1996
  - No indictment issued, but was a subject for violating export controls
- Fundamental insight: Knowledge about cryptography is public. In theory citizens can circumvent government-mandated key escrow by implementing cryptography themselves.


Search results for '0xc746
pgp.mit.edu/pks/lookup?op=vindex&search=0xC746363982D7795E
Search results for '0xc7463639b2d7795e'
Type bits/keyID cr. time exp time key expir
pub 1024D/B2D7795E 2001-01-04
sig dirct B2D7795E 2001-01-04 [selfsig]
Revocation key fingerprint: 3FC7 3204 1D23 E9EA 66DD B500 9C9D BC21 DF74 DC61
uid Philip R. Zimmermann <prz@mit.edu>
sig sig B2D7795E 2001-01-04 [selfsig]
sig sig B2D7795E 2001-01-04 [selfsig]
sig sig FAEBD5FC 2001-01-04 Philip R. Zimmermann <prz@acm.org>
sig sig B2D7795E 2001-01-06 [selfsig]
sig exp FAEBD5FC 2001-01-06 2010-01-06 Philip R. Zimmermann <prz@acm.org>
sig sig 66A74B31 2001-01-06 Teun Nijssen <teun.nijssen@uvt.nl>
sig sig 66A74B31 2001-01-06 Teun Nijssen <teun.nijssen@uvt.nl>
sig sig CF73EC4C 2001-01-06 Will Price <wprice@pgp.com>
sig sig CF73EC4C 2001-01-06 Will Price <wprice@pgp.com>
sig sig EEB63AB1 2001-01-06 Ron & Bes Vantreese <ron-bes@usa.net>
sig sig F414952B 2001-01-07 Jeffrey I. Schiller <jis@qyv.net>
sig sig F414952B 2001-01-07 Jeffrey I. Schiller <jis@qyv.net>
sig sig 0A791610 2001-01-09 Stale Schumacher Ytteborg <stale@hypnotech.com>
sig sig 0A791610 2001-01-09 Stale Schumacher Ytteborg <stale@hypnotech.com>
sig sig 4793C529 2001-02-02 Hugh Miller <hmiller@luc.edu>
sig sig EF881DEC 2001-03-03 h3xx <h3x_x@phreaker.net>
sig sig D7C776BF 2001-03-03 h3xx Secure Data
sig sig EEB63AB1 2001-03-05 Ron & Bes Vantreese <ron-bes@usa.net>
sig sig EEB63AB1 2001-03-05 Ron & Bes Vantreese <ron-bes@usa.net>
sig sig BF67D2EB 2001-03-10 Michael A. Haisley Jr. <mikehaisley@home.com>
sig sig BF67D2EB 2001-03-10 Michael A. Haisley Jr. <mikehaisley@home.com>
sig sig F491BD21 2001-04-13 Ben Paul Wise <bwise@sito.saic.com>
sig sig 251F35C1 2001-04-20 Marco Balmer <marco.balmer@calculus.ch>



https://xkcd.com/364/

“Never bring tequila to a key-signing party.”

PGP in the modern era

- PGP was built before modern cryptographic protocol design was properly understood.
- Numerous vulnerabilities
- GnuPGP and libgcrypt open source and quite widely used
- Usability issues: most experts unable to use PGP properly
  - “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0” by Whitten and Tygar
  - “Why Johnny Still, Still Can’t Encrypt: Evaluating the Usability of a Modern PGP Client” by Ruoti et al.

https://xkcd.com/1181/

“If you want to be extra safe, check that there’s a big block of jumbled characters at the bottom.”

Message Encryption since PGP

- For messaging, Signal, WhatsApp, 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

Message Encryption since PGP

- For messaging, Signal, WhatsApp, 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 revealing plaintext of previous messages
  - If sender or recipient store plaintext, this is more likely point of compromise

t

Message Encryption since PGP

- For messaging, Signal, WhatsApp, 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 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.

t

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.

Apple v. FBI (2016)

- In 2016, the FBI tried to legally compel Apple to break their own encryption scheme to access the iPhone of the San Bernadino bomber.
- The government tried to use the All Writs Act to compel Apple to write a decryption tool.
- Apple publicized the case.
- Eventually the FBI backed down and reportedly used a specialty consulting firm to unlock the phone.

the following three important functions: (1) it will bypass or disable the auto-erase function whether or not it has been enabled; (2) it will enable the FBI to submit passcodes to the SUBJECT DEVICE for testing electronically via the physical device port, Bluetooth, Wi-Fi, or other protocol available on the SUBJECT DEVICE; and (3) it will ensure that when the FBI submits passcodes to the SUBJECT DEVICE, software running on the device will not purposefully introduce any additional delay between passcode attempts beyond what is incurred by Apple hardware.

3. Apple's reasonable technical assistance may include, but is not limited to: providing the FBI with a signed iPhone Software file, recovery bundle, or other Software Image File ("SIF") that can be loaded onto the SUBJECT DEVICE. The SIF will load and run from Random Access Memory ("RAM") and will not modify the iOS on the actual phone, the user data partition or system partition on the device's flash memory. The SIF will be coded by Apple with a unique identifier of the phone so that the SIF would only load and execute on the SUBJECT DEVICE. The SIF will be loaded via Device Firmware Upgrade ("DFU") mode, recovery mode, or other applicable mode


<C>
<C>
<iphone
golden key>

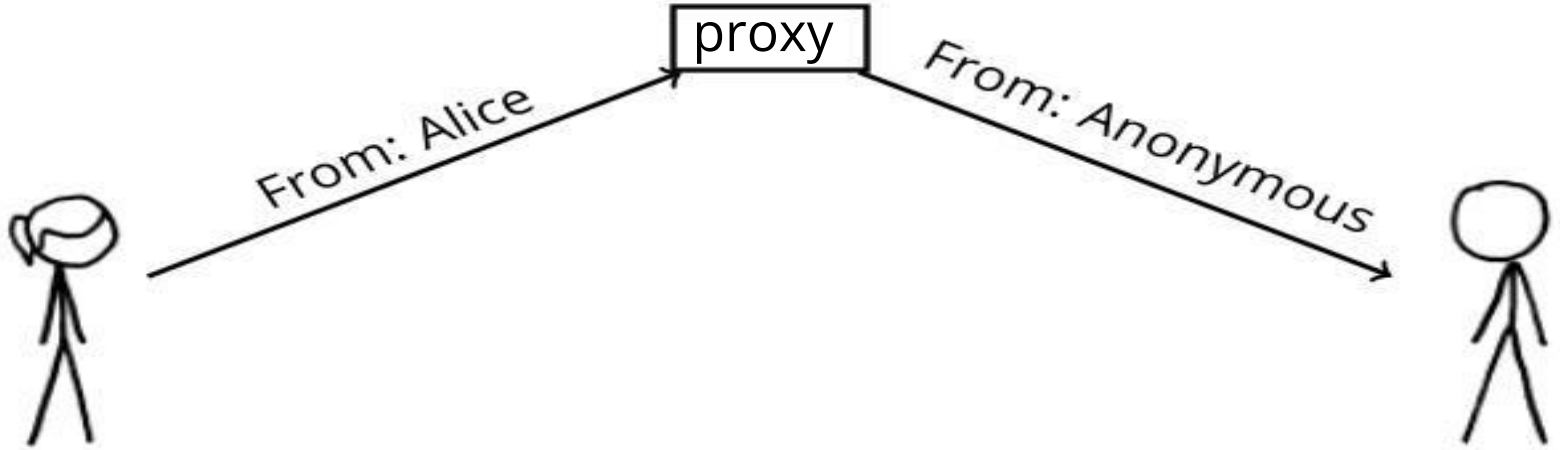
Anonymity

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?

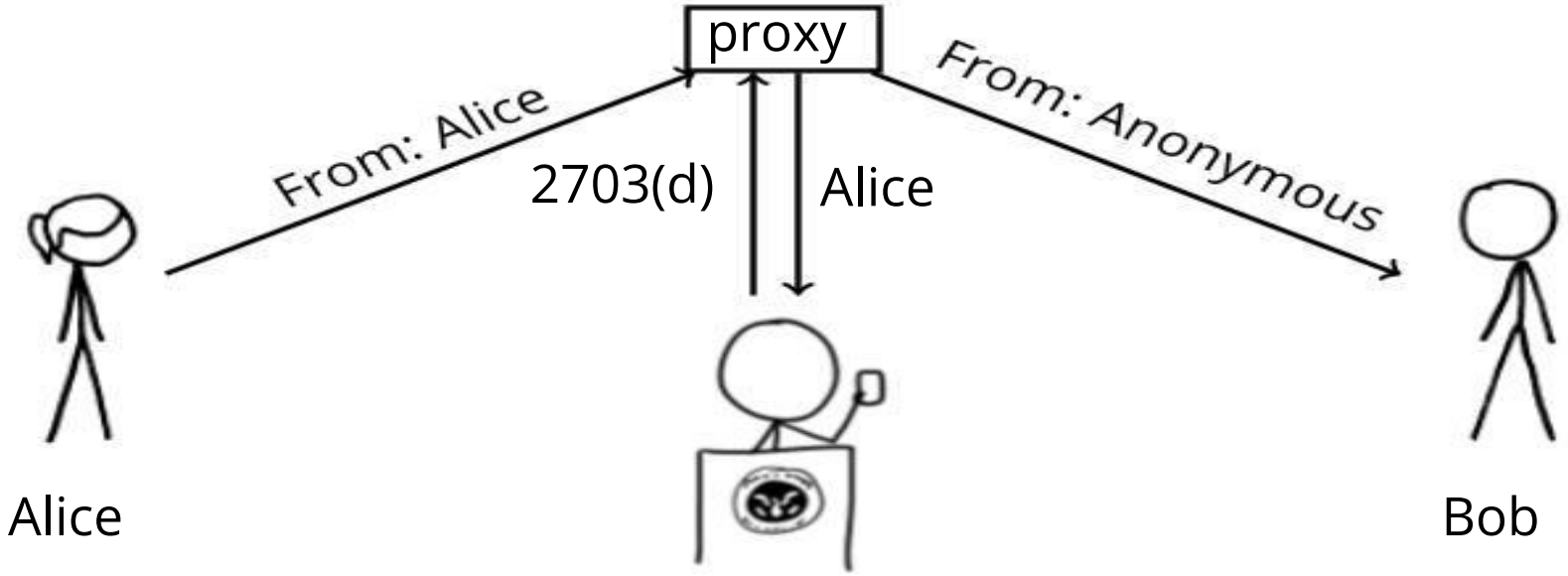
“Anonymity” via tunneling or proxies



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:

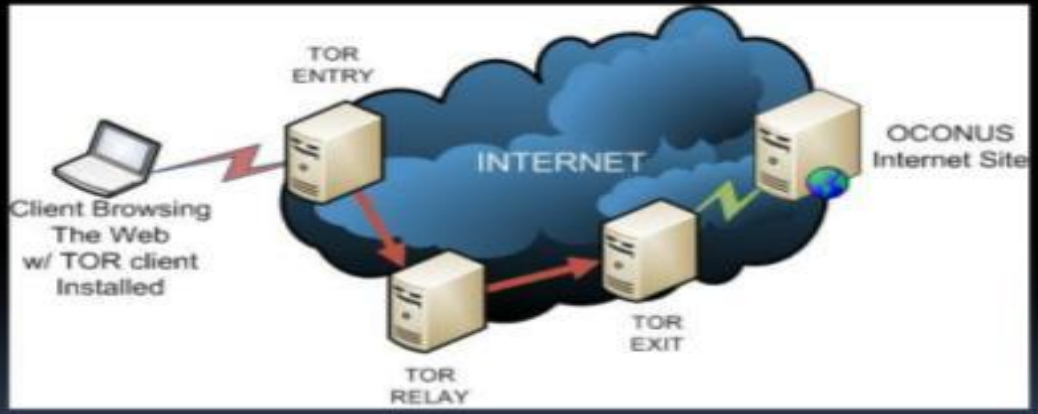
- Network attacker watching client traffic can't see destination.
- Destination server does not see client IP address.
- Network nodes can't link client and server.
- Fast enough to support TCP streams and network applications.

Current state: A nonprofit organization, active academic research, deployed around the world.
Not perfect, but a building block.

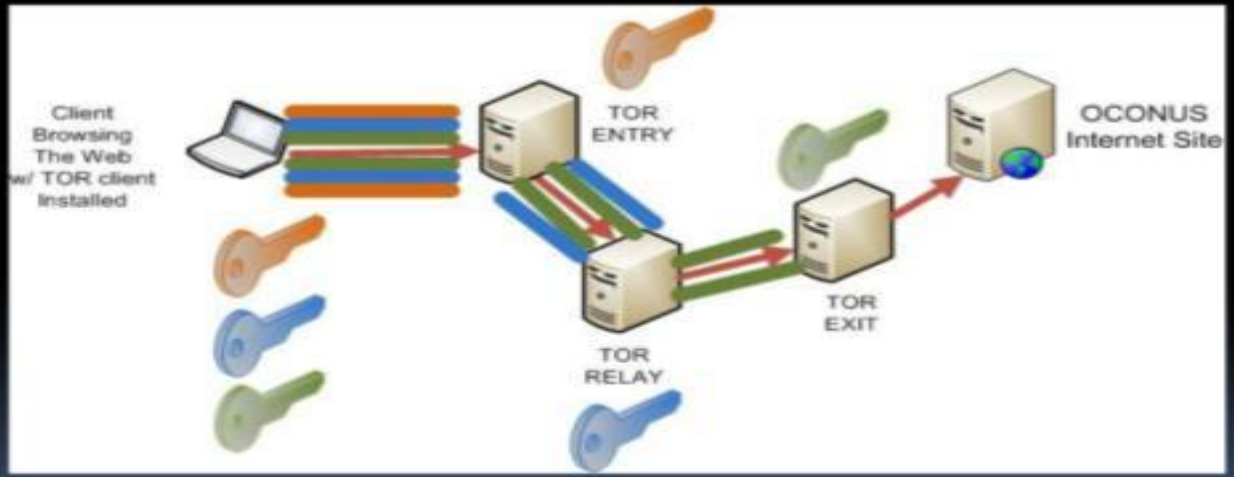
(U) What is TOR?

- (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

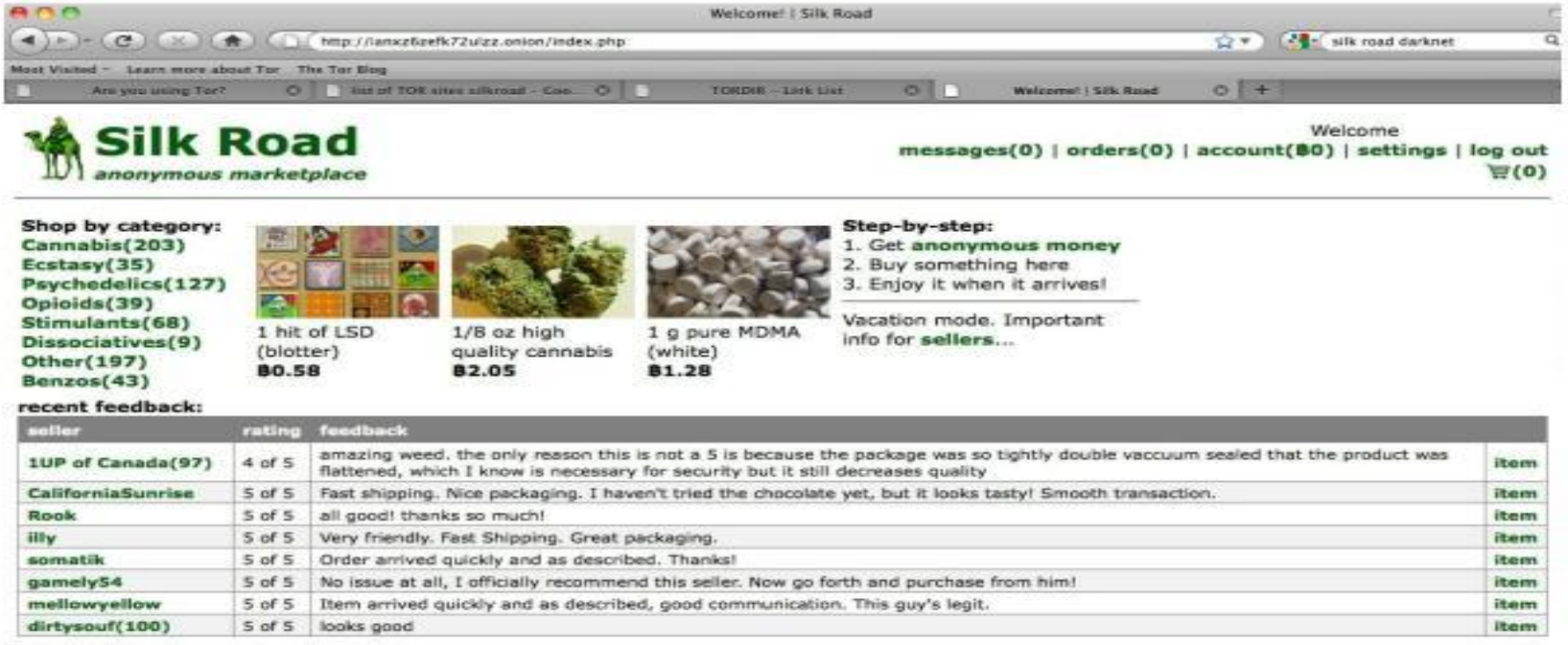
(U) What is TOR?


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

Important to align the security guarantees offered by anonymity systems with threat model.

b. On March 1, 2012, at approximately 5:03 p.m. CST, HAMMOND was seen leaving the CHICAGO RESIDENCE. Almost immediately after, CW-1 (in New York) contacted me to report that the defendant was offline. Pen/Trap data also reflected that TOR network activity and Internet activity from the CHICAGO RESIDENCE stopped at approximately the same time.

c. Later, also on March 1, 2012, at approximately 6:23 p.m. CST, HAMMOND was observed returning to the CHICAGO RESIDENCE. TOR network traffic resumed from the CHICAGO RESIDENCE approximately a minute or so later. Moreover, CW-1 reported to me that the defendant, using the online alias "yohoho," was back online at approximately the same time as physical surveillance in Chicago showed HAMMOND had returned to the CHICAGO RESIDENCE. New York FBI, through a program that remotely monitors the Internet activity of the buddy list on CW-1's jabber program, including when a "buddy" signs on and off, corroborated CW-1's report that the defendant, using "yohoho," was back online. Pen/Trap data reflected extensive TOR-related activity through the night.

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 wireless network.

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

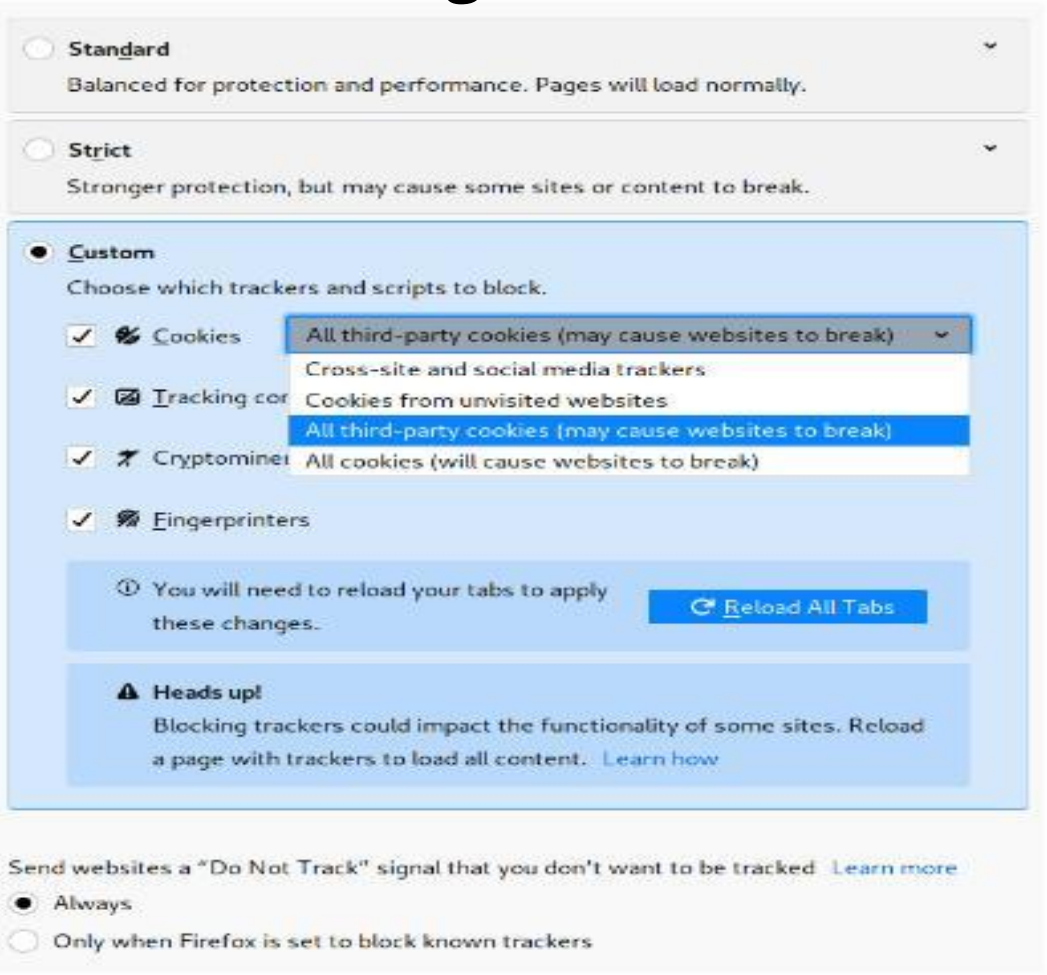
- Companies like Google, Facebook, Twitter, Microsoft, Amazon, Target, Walmart, . . . make a lot of money from tracking users.
- For some of these companies you are the product. So tracking you is their business.
  How do websites track users?
- - Third-party cookies: recall that cookies for trackme.com are sent with any request to trackme.com, 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.


Incognito mode
=private?
NordVPN

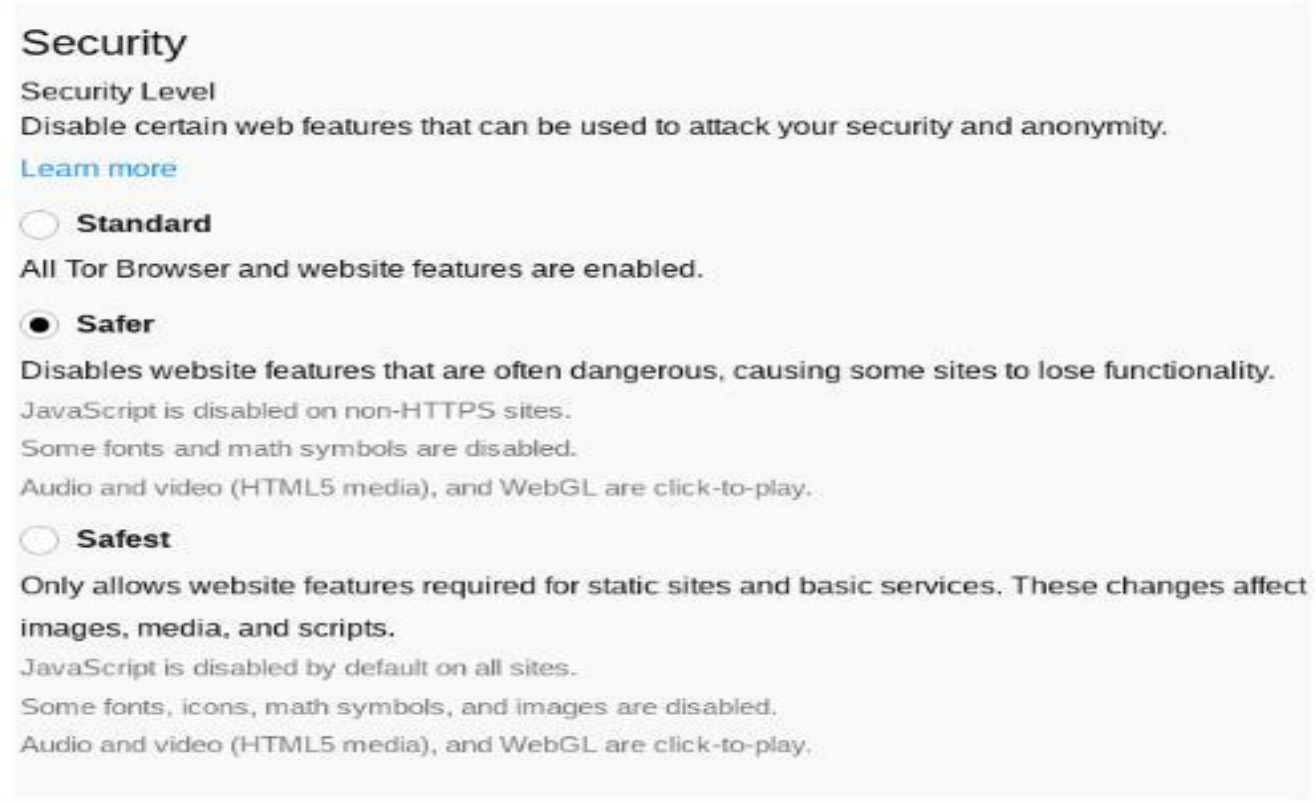
What can you do about this?

- 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

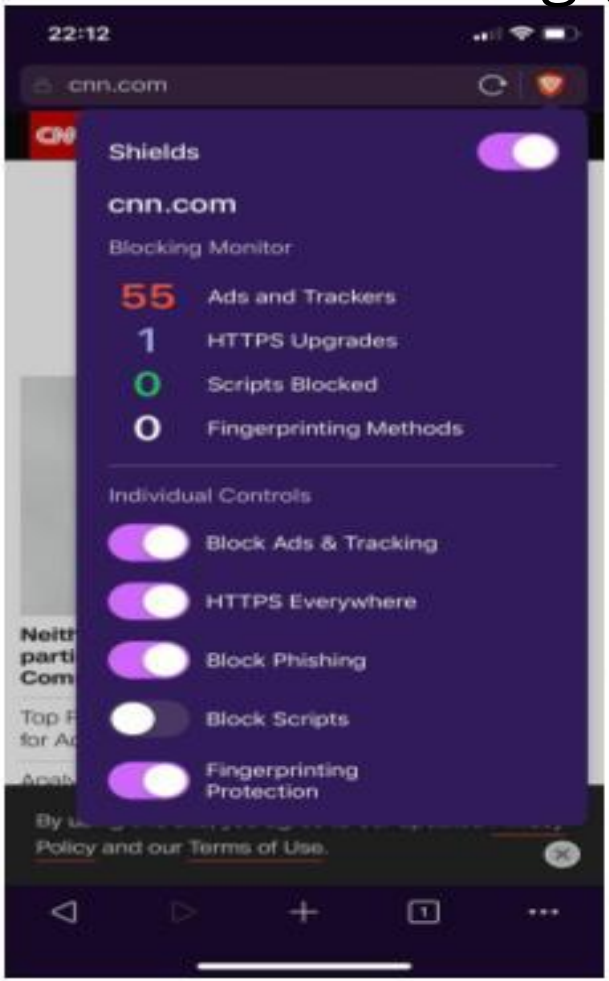
Privacy-enhanced browsing (Firefox)

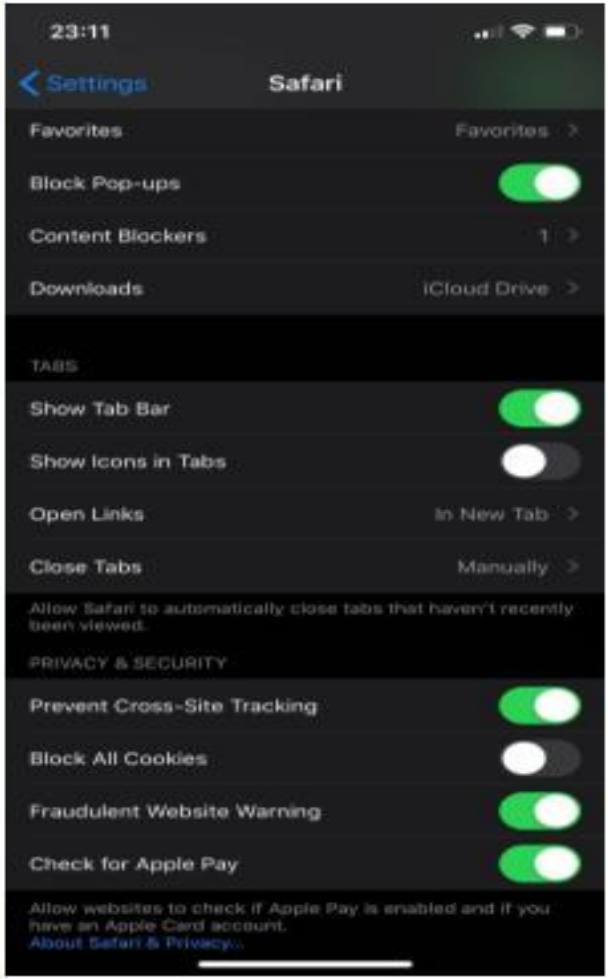


Privacy-enhanced browsing (Tor)



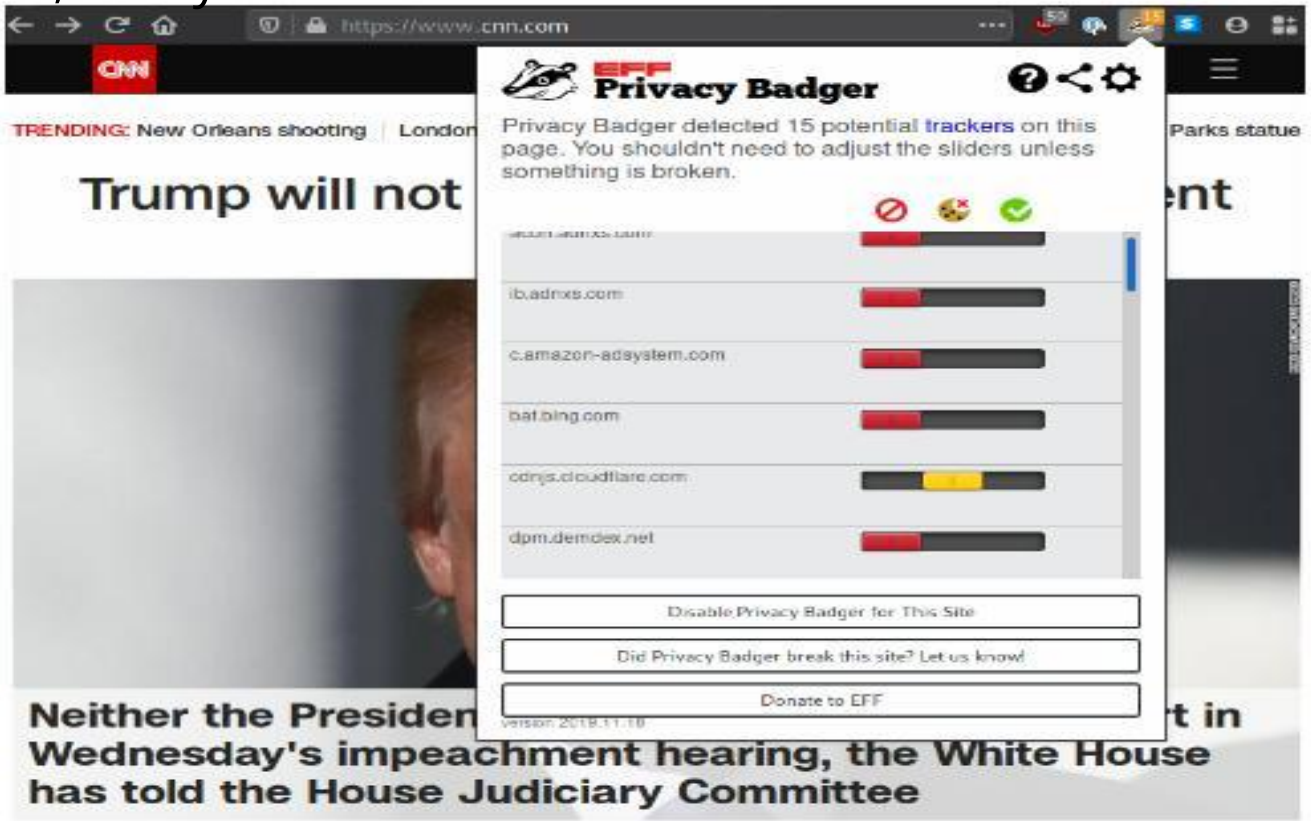
Privacy-enhanced browsing (Brave & Safari)





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)