CSE 127: Introduction to Security

Lecture 17: Privacy and Anonymity

Nadia Heninger

UCSD

Winter 2021

Some material from Deian Stefan
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

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

$\text{Alice}$

$\text{ATT}$

$\text{Bob}$

$\text{FBI}$

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

$\text{Enc}_k(m), \text{Enc}_{\text{pubBob}}(k)$

$\text{Enc}_k(m), \text{Enc}_{\text{pubBob}}(k)$

search warrant

$m$
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.
- 1996: Bernstein v. United States; California judge rules ITAR regulations are unconstitutional because “code is speech”
- 1996: Cryptography regulation moved to Department of Commerce.
- 2000: Department of Commerce loosens regulations on mass-market and open source software.
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.
(1) CJ 191-92
61. On or about June 30, 1992, Plaintiff submitted a CJ Request to Defendant STATE DEPARTMENT to determine whether publication of 1) the paper entitled "The Snuffle Encryption System," 2) source code for the encryption portion of Snuffle, and 3) source code for the decryption portion of Snuffle required a license under the ITAR. Filed under seal herewith as Exhibit "A" is a true and correct copy of the cover letter accompanying CJ 191-92.
62. Plaintiff is informed and believes and based upon such information and belief alleges that his request, labelled CJ 191-92 by the Defendant STATE DEPARTMENT, was referred to, among others, Defendants MARK KORO and GREG STARK acting under color of authority of Defendant NATIONAL SECURITY AGENCY for determination of whether a license was required prior to publication of the Items.
63. On or about August 20, 1992, Defendant WILLIAM G. ROBINSON, acting under color of authority of Defendant STATE DEPARTMENT, informed Plaintiff that he would need a license in order to publish the items included in CJ 191-92. Attached hereto as Exhibit "B" is a true and correct copy of Defendant ROBINSON’s letter to Plaintiff.
Pretty Good Privacy (PGP)

- Written by Phil Zimmermann in 1991
  - Response to US Senate bill requiring crypto backdoors (didn’t pass)
- 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 '0xc7463639b2d7795e'

<table>
<thead>
<tr>
<th>Type</th>
<th>bits/keyID</th>
<th>cr. time</th>
<th>exp time</th>
<th>key expir</th>
</tr>
</thead>
<tbody>
<tr>
<td>pub</td>
<td>1024/D/2B2D7795E</td>
<td>2001-01-04</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>B2D7795E</td>
<td>2001-01-04</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>B2D7795E</td>
<td>2001-01-04</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>B2D7795E</td>
<td>2001-01-06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>3FC7 3204 1D23 E9EA 66DD B500 9C9D BC21 DF74 DC61</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>uid</td>
<td>Philip R. Zimmermann <a href="mailto:prz@mit.edu">prz@mit.edu</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>B2D7795E</td>
<td>2001-01-04</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>B2D7795E</td>
<td>2001-01-04</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>B2D7795E</td>
<td>2001-01-04</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>FAEBD5FC</td>
<td>2001-01-04</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>FAEBD5FC</td>
<td>2001-01-06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>66A74B3E</td>
<td>2001-01-06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>66A74B3E</td>
<td>2001-01-06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>CF73EC4C</td>
<td>2001-01-06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>CF73EC4C</td>
<td>2001-01-06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>66A74B3E</td>
<td>2001-01-06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>66A74B3E</td>
<td>2001-01-06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>CF73EC4C</td>
<td>2001-01-06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>CF73EC4C</td>
<td>2001-01-06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>FAEBD5FC</td>
<td>2001-01-07</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>FAEBD5FC</td>
<td>2001-01-07</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>0A791610</td>
<td>2001-01-09</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>0A791610</td>
<td>2001-01-09</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>4793C529</td>
<td>2001-02-02</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>EF881DEC</td>
<td>2001-03-03</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>251F35C1</td>
<td>2001-04-20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>251F35C1</td>
<td>2001-04-20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sig</td>
<td>251F35C1</td>
<td>2001-04-20</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Revocation key fingerprint: 3FC7 3204 1D23 E9EA 66DD B500 9C9D BC21 DF74 DC61
“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.
"If you want to be extra safe, check that there's a big block of jumbled characters at the bottom."

https://xkcd.com/1181/
Government requests for crypto keys: Lavabit

Lavabit was an email provider that offered encryption, who in 2013 happened to have Edward Snowden as a customer.

Lavabit employed two stages of encryption for its paid subscribers: storage encryption and transport encryption. Storage encryption protects emails and other data that rests on Lavabit’s servers. Theoretically, no person other than the email user could access the data once it was so encrypted. By using storage encryption, Lavabit held a unique market position in the email industry, as many providers do not encrypt stored data.
YOU ARE COMMANDED to appear and testify before the United States district court at the time, date, and place shown below to testify before the court's grand jury. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Place: UNITED STATES DISTRICT COURT
401 Courthouse Square
Alexandria, Virginia 22314

Date and Time: July 16, 2013  9:30 AM

You must also bring with you the following documents, electronically stored information, or objects (blank if not applicable):

In addition to your personal appearance, you are directed to bring to the grand jury the public and private encryption keys used by lavabit.com in any SSL (Secure Socket Layer) or TLS (Transport Security Layer) sessions, including HTTPS sessions with clients using the lavabit.com web site and encrypted SMTP communications (or Internet communications using other protocols) with mail servers;

Any other information necessary to accomplish the installation and use of the pen/trap device ordered by Judge Buchanan on June 28, 2013, unobtrusively and with minimum interference to the services that are accorded persons with respect to whom the installation and use is to take place;

If such information is electronically stored or unable to be physically transported to the grand jury, you may provide a copy of the information to the Federal Bureau of Investigation. Provision of this information to the FBI does not excuse your personal appearance.

Date: July 11, 2013

CLERK OF COURT

Signature of the Clerk or Deputy Clerk
UNDER SEAL

UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

INFORMATION ASSOCIATED WITH
THAT IS STORED AT PREMISES
CONTROLLED BY LAVABIT, LLC

Case No. 1:13SW522

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the ______ Northern ______ District of ______ Texas ______

(identify the person or describe the property to be searched and give its location):

See Attachment A
ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Lavabit, LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All information necessary to decrypt communications sent to or from the Lavabit email account [blacked out] including encryption keys and SSL keys;

b. All information necessary to decrypt data stored in or otherwise associated with the Lavabit account [blacked out].
The owner of Lavabit tried to resist the legal order without a lawyer.

It did not go well.

Despite the unequivocal language of the August 1 Order, Lavabit dallied and did not comply. Just before the 5:00 pm August 2 deadline, for instance, Levison provided the FBI with an 11-page printout containing largely illegible characters in 4-point type, which he represented to be Lavabit’s encryption keys. The Government instructed Lavabit to provide the keys in an industry-standard electronic format by the morning of August 5. Lavabit did not respond.
My Fellow Users,

I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit. After significant soul searching, I have decided to suspend operations. I wish that I could legally share with you the events that led to my decision. I cannot. I feel you deserve to know what's going on—the first amendment is supposed to guarantee me the freedom to speak out in situations like this. Unfortunately, Congress has passed laws that say otherwise. As things currently stand, I cannot share my experiences over the last six weeks, even though I have twice made the appropriate requests.

What's going to happen now? We've already started preparing the paperwork needed to continue to fight for the Constitution in the Fourth Circuit Court of Appeals. A favorable decision would allow me resurrect Lavabit as an American company.

This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would _strongly_ recommend against anyone trusting their private data to a company with physical ties to the United States.

Sincerely,
Ladar Levison
Owner and Operator, Lavabit LLC
• Levison was eventually represented by the EFF
• He lost the case on appeal for failing to raise the defense the EFF tried to use in the first place

We reiterate that our review is circumscribed by the arguments that Lavabit raised below and in this Court. We take this narrow course because an appellate court is not a freestanding open forum for the discussion of esoteric hypothetical questions. See Swann v. Charlotte-Mecklenburg Bd.
“Actual actual reality: nobody cares about his secrets. Also, I would be hard-pressed to find that wrench for $5.”
The server's security certificate is revoked!

You attempted to reach lavabit.com, but the certificate that the server presented has been revoked by its issuer. This means that the security credentials the server presented absolutely should not be trusted. You may be communicating with an attacker.

Back to safety

Help me understand
Secure email for the world

Because everyone has the right to communicate privately.

SIGN UP
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 $t$ revealing plaintext of previous messages
    - If sender or recipient store plaintext, this is more likely point of compromise
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 $t$ 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.
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 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.
pursuant to a warrant of this Court by providing reasonable technical assistance to assist law enforcement agents in obtaining access to the data on the SUBJECT DEVICE.

2. Apple's reasonable technical assistance shall accomplish 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 available to the FBI. Once active on the SUBJECT DEVICE, the SIF will accomplish the three functions specified in paragraph 2. The SIF will be loaded on the SUBJECT DEVICE at either a government facility, or alternatively, at an Apple facility; if the latter, Apple shall provide the government with remote access to the SUBJECT DEVICE.
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?
(U) What is TOR?
(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

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

- **Standard**: Balanced for protection and performance. Pages will load normally.
- **Strict**: Stronger protection, but may cause some sites or content to break.
- **Custom**: Choose which trackers and scripts to block.
  - **Cookies**: All third-party cookies (may cause websites to break)
  - **Tracking cookies**: Cookies from unvisited websites
  - **Cryptominers**: All third-party cookies (may cause websites to break)
  - **Fingerprinters**

You will need to reload your tabs to apply these changes.

**Heads up!**
Blocking trackers could impact the functionality of some sites. Reload a page with trackers to load all content. Learn more

Send websites a “Do Not Track” signal that you don’t want to be tracked. Learn more
- **Always**
- **Only when Firefox is set to block known trackers**
Privacy-enhanced browsing (Tor)

Security
Security Level
Disable certain web features that can be used to attack your security and anonymity.
Learn more

☐ Standard
All Tor Browser and website features are enabled.

● Safer
Disables website features that are often dangerous, causing some sites to lose functionality.
JavaScript is disabled on non-HTTPS sites.
Some fonts and math symbols are disabled.
Audio and video (HTML5 media), and WebGL are click-to-play.

☐ Safest
Only allows website features required for static sites and basic services. These changes affect images, media, and scripts.
JavaScript is disabled by default on all sites.
Some fonts, icons, math symbols, and images are disabled.
Audio and video (HTML5 media), and WebGL are click-to-play.
Privacy-enhanced browsing (Brave & Safari)
Privacy-enchanting extensions

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