Privacy Enhancing Technologies (BSc)

Lecture III: Fingerprinting & Censorship

Univ.-Prof. Dr. Dominique Schröder

October 21, 2024

Overview

KW	Type	Lectures
42	**Lecture**	Internet and Privacy in the Web
43	**Lecture**	**Fingerprinting & Censorship**
44	**Exercise**	Introduction to Rust
45	**Lecture**	Cryptographic Preliminaries
46	**Lecture**	DDH Key Exchange, Security Reductions
47	**Exercise**	Proofs and Theoretical Deepening
48	**Lecture**	TLS
49	**Exam**	**Midterm Exam**
50	**Exercise**	Rust Key Exchange
51	**Lecture**	Messaging I
3	**Lecture**	Messaging II (Forward Security, Post Compromise Security)
4	**Lecture**	Onion
5	**Lecture**	Q & A
6	**Exam**	**Final Exam**
9	**Exam**	**Reexam** (Both for Midterm and Final)

This Lecture's Questions

- Hiding IP address and erasing cookies, are we still tracked?
- What are tracking protection techniques?
- Censorship, what's going on?
- How to circumvent censorship

This Lecture's Questions

- Hiding IP address and erasing cookies, are we still tracked?
- What are tracking protection techniques?
- Censorship, what's going on?
- How to circumvent censorship

This Lecture's Questions

- Hiding IP address and erasing cookies, are we still tracked?
- What are tracking protection techniques?
- Censorship, what's going on?
- How to circumvent censorship

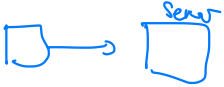
This Lecture's Questions

- Hiding IP address and erasing cookies, are we still tracked?
- What are tracking protection techniques?
- Censorship, what's going on?
- How to circumvent censorship

Fingerprinting

Fingerprinting

Definitions



Definition (Fingerprinting; Eckersley, 2010)

Fingerprinting is the process of collecting information about a device, browser, or connection to create a unique identifier, allowing tracking or identification without the use of cookies.

Definition (Fingerprinting Circumvention; Zuckerman, 2010)

Fingerprinting circumvention refers to the use of privacy tools or techniques to limit or obscure the information gathered for fingerprinting, preventing unique identification.

Fingerprinting

Definitions

Definition (Fingerprinting; Eckersley, 2010)

Fingerprinting is the process of collecting information about a device, browser, or connection to create a unique identifier, allowing tracking or identification without the use of cookies.

Definition (Fingerprinting Circumvention; Zuckerman, 2010)

Fingerprinting circumvention refers to the use of privacy tools or techniques to limit or obscure the information gathered for fingerprinting, preventing unique identification.

How would you fingerprint users on the internet?

→ Information you can't hide → open tech browser

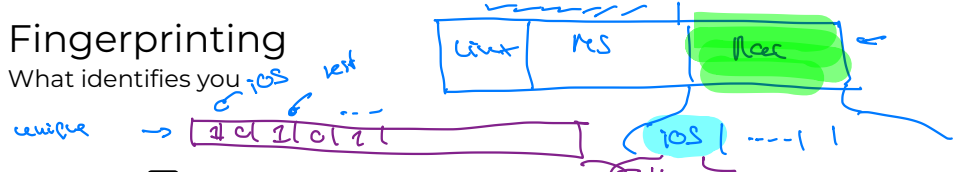
→ size, font, hardware

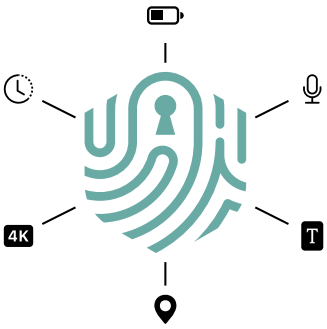
→ tracking browser history ?

↳ ?

Fingerprinting

What identifies you

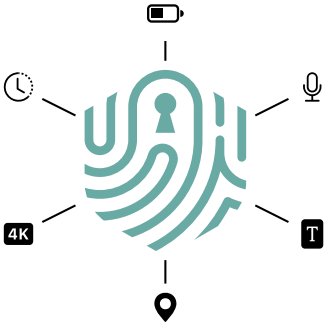




- Users can be **tracked persistently** even without an IP address or cookies.
- **Identification is based on unique system properties:**
  - Geolocation, clock skew (system time differences).
  - Battery status, audio settings.
  - Screen resolution, installed fonts.
  - Operating system, browser language.
- These properties create a **unique device fingerprint**, allowing for continuous tracking across sessions and websites.

Fingerprinting

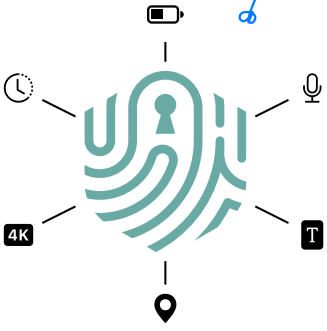
What identifies you



- Users can be **tracked persistently** even without an IP address or cookies.
- **Identification is based on unique system properties:**
  - Geolocation, clock skew (system time differences).
  - Battery status, audio settings.
  - Screen resolution, installed fonts.
  - Operating system, browser language.
- These properties create a **unique device fingerprint**, allowing for continuous tracking across sessions and websites.

Fingerprinting

What identifies you



- Users can be **tracked persistently** even without an IP address or cookies.
- **Identification is based on unique system properties:**
  - Geolocation, clock skew (system time differences).
  - Battery status, audio settings.
  - Screen resolution, installed fonts.
  - Operating system, browser language.
- These properties create a **unique device fingerprint**, allowing for continuous tracking across sessions and websites.

Why Fingerprinting is Possible

- **Device and Browser Diversity:**
  - Every device and browser has unique characteristics (e.g., fonts, screen resolution, GPU).
  - These differences allow the creation of a "fingerprint" that is unique to the user.
- **Technical Information Leak:**
  - Web browsers often reveal detailed technical information such as plugins, fonts, and even battery status.
  - JavaScript, HTML5 APIs, and WebRTC can expose additional details about the user's setup.
- **Legal and Regulatory Gaps:**
  - Unlike cookies, fingerprinting doesn't require user consent in many jurisdictions.
  - No robust global regulations are in place to prevent fingerprinting techniques across borders.

Why Fingerprinting is Possible

- **Device and Browser Diversity:**
  - Every device and browser has unique characteristics (e.g., fonts, screen resolution, GPU).
  - These differences allow the creation of a "fingerprint" that is unique to the user.
- **Technical Information Leak:**
  - Web browsers often reveal detailed technical information such as plugins, fonts, and even battery status.
  - JavaScript, HTML5 APIs, and WebRTC can expose additional details about the user's setup.
- **Legal and Regulatory Gaps:**
  - Unlike cookies, fingerprinting doesn't require user consent in many jurisdictions.
  - No robust global regulations are in place to prevent fingerprinting techniques across borders.

Why Fingerprinting is Possible

- **Device and Browser Diversity:**
  - Every device and browser has unique characteristics (e.g., fonts, screen resolution, GPU).
  - These differences allow the creation of a "fingerprint" that is unique to the user.
- **Technical Information Leak:**
  - Web browsers often reveal detailed technical information such as plugins, fonts, and even battery status.
  - JavaScript, HTML5 APIs, and WebRTC can expose additional details about the user's setup.
- **Legal and Regulatory Gaps:**
  - Unlike cookies, fingerprinting doesn't require user consent in many jurisdictions.
  - No robust global regulations are in place to prevent fingerprinting techniques across borders.

Let’s Fingerprint

Canvas Fingerprinting (1)

A Modern Tracking Technique

- **What is Canvas Fingerprinting?**
  - A technique used to track users by rendering images or text on an HTML5 canvas element.
  - Differences in how the content is rendered (due to variations in device, browser, and GPU) create a unique “fingerprint” for each user.
- **How it Works:**
  - JavaScript instructs the browser to draw invisible images or text using the HTML5 canvas.
  - The browser’s rendering differences (such as anti-aliasing or font smoothing) generate a unique rendering output.

Canvas Fingerprinting (2)

A Modern Tracking Technique

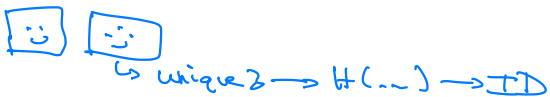
- **Why it Matters:**
  - More difficult to block than traditional cookies since no data is stored on the device.
  - Enables cross-site tracking of users without their explicit consent.
- **Countermeasures:**
  - Use privacy-focused browsers or extensions that block canvas access.
  - Tor Browser, for instance, alerts users whenever a website tries to use canvas fingerprinting.

Canvas Fingerprinting

Can You See the Fingerprint?

Canvas Fingerprinting (1)

- **Rendering on the Canvas:**
  - JavaScript instructs the browser to draw text or images on the HTML5 <canvas> element.
  - Factors like the operating system, browser, and GPU affect how the content is rendered.
- **Pixel Data Extraction:**
  - Once rendered, the **pixel data** of the canvas (RGB color values) is extracted.
  - This pixel data varies slightly between devices due to system differences (fonts, resolution, anti-aliasing, etc.).



Canvas Fingerprinting (2)

- **Hashing the Data:**
  - The extracted pixel data is then hashed (e.g., using SHA-256) to produce a unique fingerprint.
  - This fingerprint identifies a user across websites, even without cookies or IP addresses.
- **Why It's Unique:**
  - Each device renders the same canvas content slightly differently, producing a unique hash.
  - Differences in operating systems, graphic card drivers, and browser configurations contribute to this uniqueness.
- **Popular technique**: Detected on over 14,000 websites in a study of 1 million sites by Princeton University.

Canvas Fingerprinting (3)

An Example

Canvas Fingerprint

```
<canvas id="myCanvas" width="300" height="150">
    Your browser does not support the HTML5 canvas tag.
</canvas>

<script>
    var canvas = document.getElementById("myCanvas");
    var ctx = canvas.getContext("2d");
    ctx.font = "20px Arial";
    ctx.fillText("Canvas Fingerprinting", 50, 50);
    ctx.strokeStyle = "red";
    ctx.lineWidth = 3;
    ctx.strokeRect(40, 25, 250, 40);
</script>
```

Canvas Fingerprinting (4)

An Example

Rendering the same canvas results in different hashes for each device.

- **Device 1 (Windows PC):**
  - Rendering result: `"acbd18db4cc2f85cedef654fccc4a4d8"`
- **Device 2 (MacBook):**
  - Rendering result: `"37b51d194a7513e45b56f6524f2d51f2"`

Canvas Fingerprinting (4)

An Example

Rendering the same canvas results in different hashes for each device.

- **Device 1 (Windows PC):**
  - Rendering result: `"acbd18db4cc2f85cedef654fccc4a4d8"` → unique tracking ID
- **Device 2 (MacBook):**
  - Rendering result: `"37b51d194a7513e45b56f6524f2d51f2"`

HSTS Fingerprinting (1)

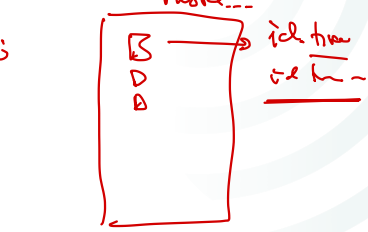
- **What is HSTS?**
  - *HSTS (HTTP Strict Transport Security)* is a security feature that forces browsers to always connect over HTTPS, ensuring secure connections.
  - Websites send a header that instructs the browser to remember this preference for future visits.
- **How Fingerprinting Works:**
  - Websites track users by checking whether the browser has cached the HSTS setting for specific domains.
  - Different browsers store HSTS data differently, contributing to unique fingerprinting.

HSTS Fingerprinting (2)

- **HSTS Fingerprinting Process:**
  - A website sends requests to a series of test domains (e.g., `id-1.tracker-domain.de`, `id-2.tracker-domain.de`).
  - If the browser forces HTTPS (due to HSTS caching), it indicates whether the user has previously visited these domains.
- **Tracking via HSTS SuperCookies:**
  - Tracking agencies can create HSTS entries for various subdomains, which are cached in the browser to form a persistent identifier (SuperCookie).
  - By using different combinations of subdomains, agencies can generate unique fingerprints for each user.
  - Example: 32 subdomains can create over 4 billion combinations for a highly unique fingerprint.

HSTS Fingerprinting (3)

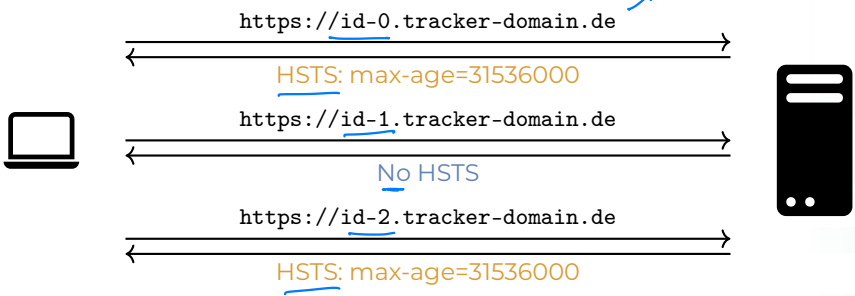
- **Why It's Effective:**
  - The cached HSTS state remains even if cookies are cleared, allowing long-term tracking across sites.
  - Any website can check these entries by requesting resources from the subdomains, enabling continuous tracking.
- **Reference:**
- **Proof of Concept Implementation:**



HSTS Fingerprinting (1)

An Example

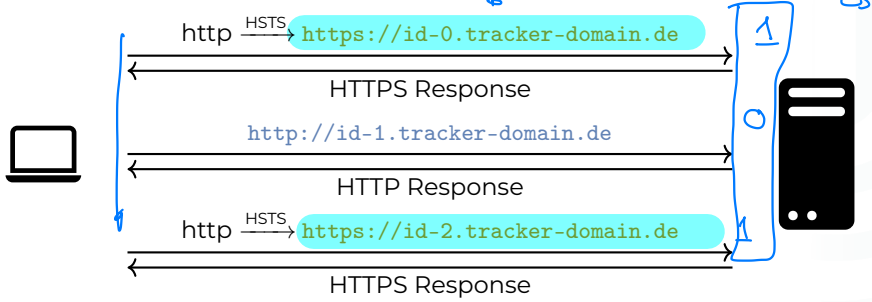
First Visit: We create the effective fingerprint 101



HSTS Fingerprinting (2)

An Example

Second Visit: The user sends the fingerprint 101



Mitigate Fingerprinting

Fingerprinting Protection

Browsers

- **Mozilla Firefox**
  - Tracking prevention based on Disconnect ruleset 
  - Enhanced tracking prevention (separate cookie context)
  - Multi-Account Containers (e.g., separate your browsing for bank, work and personal)
- **Brave**
  - Randomizing fingerprints 
  - Tor-browser tabs (improvement over private mode)
  - "Brave Rewards": privacy-respecting ad ecosystem

Fingerprinting Protection

Browser-Extensions I

- **AdBlock Plus (ABP)**
  - Was the most popular extension to block online advertisements
  - Advertisement is blocked and set invisible (CSS)
  - Issue: Since 2012, "Acceptable Ads"
  - Issue: Acceptable Ads are enabled by default
- **Ghostery**
  - Detection and blocking of web trackers
  - Overlay for social plug-ins
  - Issue: Usability
  - Issue: Business model (now owned by Cliqz)

Browser-Extensions II

- **EFF Privacy Badger**
  - Based on heuristics
  - Tests if DNT header is honored
  - Challenge: Maintain whitelist
  - Overlays for social plug-ins
- **Disconnect.me**
  - Similar to Ghostery but with open-source ruleset
  - VPN service for mobile devices (paid subscription)
  - Basis for tracker blocking in Firefox private mode
- **uBlock (Origin)**
  - Open-Source “wide-spectrum” blocker
  - Focus on performance
  - Challenge: Overblocking, filter rule maintenance

Fingerprinting

Adblock Detection

	Web Dataset						
	Plain	Adblock Plus	Discon-nect	Ghostery	Privacy Badger	uBlock Origin	All Combined
FP-Detective							
IOVATION	98	97	97	1	97	4	1
ThreatMetrix	39	39	39	1	37	-	-
BlueCava	27	5	-	-	25	-	-
...							
OpenWPM: Canvas Font Fingerprinting							
mathid.mathtag.com/d/ijs	437	374	2	1	2	3	-
admicro1.vcmedia.vn/core/fipminjs	39	1	-	3	41	1	-
.*.online-metrix.net	39	39	39	1	37	-	-
...							
OpenWPM: Canvas Fingerprinting							
doubleverify.com/dvtp src internal.*js	4118	78	8	6	37	9	-
ap.lijit.com/www/delivery/fp	826	27	296	3	349	1	-
tags.bkrtx.com/js/bk-coretagjs	631	391	134	-	449	6	-
...							
OpenWPM: WebRTC Local IP discovery							
cdn.augur.io/augur.minjs	111	31	4	43	57	21	-
click.sabavision.com/*/jsEnginejs	78	54	81	84	77	56	-
static.fraudmetrix.cn/fmjs	11	11	11	11	14	11	-
...							

Number of pages with detected fingerprinting services per blocking extension and without any (plain), Merzdovnik et al.

Paradox of Fingerprintable PETs

- Idealized browsers: Firefox, Brave; extensions: Ghostery, uBlock origin
- **Paradox of Fingerprintable Privacy Enhancing Technologies**
  (Peter Eckersley, PETS 2010)
  - Some anti-fingerprinting techniques can be self-defeating if not used by a sufficient number of people.
  - Some fall to this paradox while others do not.

References and Resources

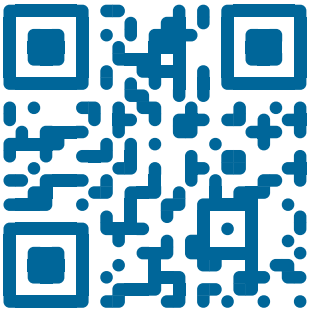
"Cover Your Track"
Sources of fingerprinting and a browser test
(The Electronic Frontier Foundation - EFF)

“Online Tracking: A 1-million-site Measurement and Analysis”
(Steven Englehardt and Arvind Narayanan, paper at ACM CCS 2016)

“Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools”
(Merzdovnik et al, paper at EuroS&P’17)

Any further recommendations?

Check Your Fingerprint



https://amiunique.org

Censorship

Outline

- Internet Censorship
- Censorship Concepts & Techniques
- Detection & Measurement
- Censorship Events Worldwide
- Countermeasures & Circumvention

“There is more than one way to burn a book.
And the world is full of people running about with lit matches.”

– Ray Bradbury, *Fahrenheit 451*

“The Net interprets censorship as damage and routes around it.”

– John Gilmore, 1993

Definitions

Definition (Siebert, 1952)

Censorship is the suppression or prohibition of speech, communication, or other information that may be considered harmful, sensitive, or inconvenient by authorities or institutions.

Definition (Zuckerman, 2010)

Circumvention is the use of tools, technologies, and techniques to bypass censorship and gain access to restricted or controlled information.

Definitions

Definition (Siebert, 1952)

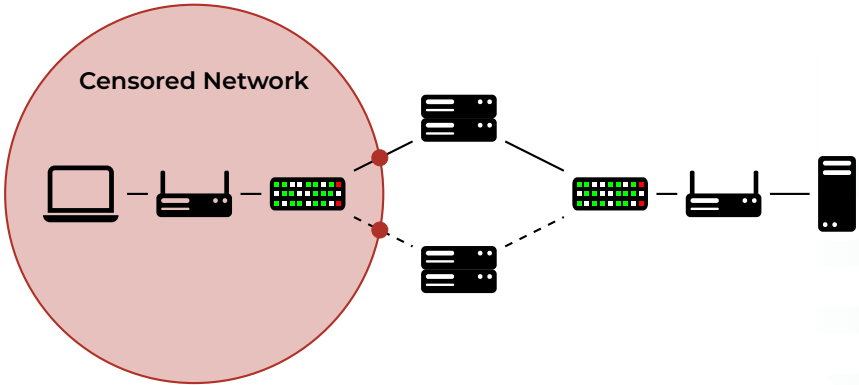
Censorship is the suppression or prohibition of speech, communication, or other information that may be considered harmful, sensitive, or inconvenient by authorities or institutions.

Definition (Zuckerman, 2010)

Circumvention is the use of tools, technologies, and techniques to bypass censorship and gain access to restricted or controlled information.

How would you censor in the internet?

Why Internet Censorship is Possible (1)



Why Internet Censorship is Possible (2)

- **Centralized Control:**
  - Governments and ISPs control key internet infrastructure.
  - Ability to block or filter traffic at choke points.
- **Technical Vulnerabilities:**
  - DNS manipulation and IP blocking.
  - Deep packet inspection to monitor and filter content.
- **Legal and Regulatory Frameworks:**
  - Laws enforce content regulation.
  - Cooperation from tech companies and ISPs.
  - Different jurisdictions enable censorship across borders.

Motivations and Consequences of Internet Censorship

- **Motivations:**
  - Moral, Military, Political, Religious, Corporate
- **Legitimate Interest of Democratic Society:**
  - Illegal content (e.g., Holocaust denial laws)
- **Political Suppression:**
  - Limiting free press and free information
- **Who Decides?**
  - Governments, regimes, or corporations?
  - Example: Facebook censors breast cancer campaign
  - Related issue: Net Neutrality

Motivations and Consequences of Internet Censorship

- **Motivations:**
  - Moral, Military, Political, Religious, Corporate
- **Legitimate Interest of Democratic Society:**
  - Illegal content (e.g., Holocaust denial laws)
- **Political Suppression:**
  - Limiting free press and free information
- **Who Decides?**
  - Governments, regimes, or corporations?
  - Example: Facebook censors breast cancer campaign
  - Related issue: Net Neutrality

Motivations and Consequences of Internet Censorship

- **Motivations:**
  - Moral, Military, Political, Religious, Corporate
- **Legitimate Interest of Democratic Society:**
  - Illegal content (e.g., Holocaust denial laws)
- **Political Suppression:**
  - Limiting free press and free information
- **Who Decides?**
  - Governments, regimes, or corporations?
  - Example: Facebook censors breast cancer campaign
  - Related issue: Net Neutrality

Motivations and Consequences of Internet Censorship

- **Motivations:**
  - Moral, Military, Political, Religious, Corporate
- **Legitimate Interest of Democratic Society:**
  - Illegal content (e.g., Holocaust denial laws)
- **Political Suppression:**
  - Limiting free press and free information
- **Who Decides?**
  - Governments, regimes, or corporations?
  - Example: Facebook censors breast cancer campaign 
  - Related issue: Net Neutrality 

Who Controls Internet Censorship?

- **Scope of Control:**
  - **Individuals:** Users who choose what content to share or censor themselves.
  - **Corporations:** Internet service providers, social media platforms, and tech companies that regulate and filter content.
  - **State-Level Actors:** Governments that enforce laws and impose regulations on internet usage and access.
- **Influence and Visibility:**
  - The degree to which different entities can shape what content is accessible and how visible it is to the public.
- **Physical, Political, and Economic Dynamics:**
  - The geopolitical landscape, economic interests, and infrastructure that allow certain actors to control or restrict access to information.

Who Controls Internet Censorship?

- **Scope of Control:**
  - **Individuals:** Users who choose what content to share or censor themselves.
  - **Corporations:** Internet service providers, social media platforms, and tech companies that regulate and filter content.
  - **State-Level Actors:** Governments that enforce laws and impose regulations on internet usage and access.
- **Influence and Visibility:**
  - The degree to which different entities can shape what content is accessible and how visible it is to the public.
- **Physical, Political, and Economic Dynamics:**
  - The geopolitical landscape, economic interests, and infrastructure that allow certain actors to control or restrict access to information.

Who Controls Internet Censorship?

- **Scope of Control:**
  - **Individuals:** Users who choose what content to share or censor themselves.
  - **Corporations:** Internet service providers, social media platforms, and tech companies that regulate and filter content.
  - **State-Level Actors:** Governments that enforce laws and impose regulations on internet usage and access.
- **Influence and Visibility:**
  - The degree to which different entities can shape what content is accessible and how visible it is to the public.
- **Physical, Political, and Economic Dynamics:**
  - The geopolitical landscape, economic interests, and infrastructure that allow certain actors to control or restrict access to information.

Censorship Techniques

Censorship Techniques Overview

Censorship relies on two main components:

Detection Methods:

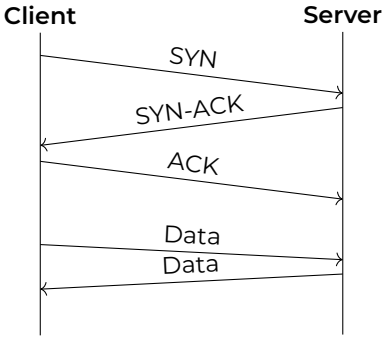
- Monitoring destination IP addresses
- Analyzing Server Name Indication
- Inspecting DNS query contents
- Detecting proxy protocol signatures
- Filtering based on plaintext keywords
- Many more techniques

Blocking Methods:

- IP null routing
- *TCP RST (Reset) injection*
- DNS response injection
- HTTP redirect injection
- Packet dropping
- Various other methods

Connection Reset Attacks

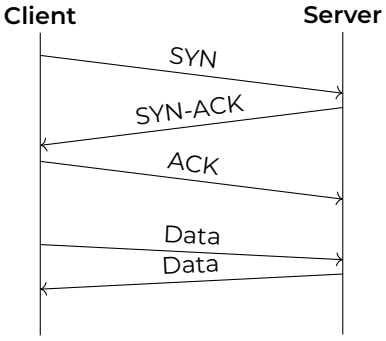
TCP 3 Way Handshake



- **SYN**: The client sends a SYN (synchronize) packet to initiate a connection.
- **SYN-ACK**: The server responds with a SYN-ACK (synchronize-acknowledge) packet to acknowledge the request.
- **ACK**: The client sends an ACK (acknowledge) packet to establish the connection, completing the handshake.
- **Data Transmission**: Once the connection is established, data is exchanged between the client and server.
- **Acknowledgment**: Each data packet is acknowledged by the receiver to ensure reliable delivery.

Connection Reset Attacks

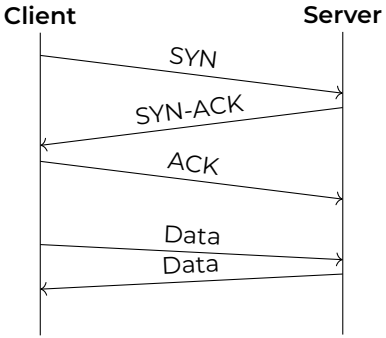
TCP 3 Way Handshake



- **SYN**: The client sends a SYN (synchronize) packet to initiate a connection.
- **SYN-ACK**: The server responds with a SYN-ACK (synchronize-acknowledge) packet to acknowledge the request.
- **ACK**: The client sends an ACK (acknowledge) packet to establish the connection, completing the handshake.
- **Data Transmission**: Once the connection is established, data is exchanged between the client and server.
- **Acknowledgment**: Each data packet is acknowledged by the receiver to ensure reliable delivery.

Connection Reset Attacks

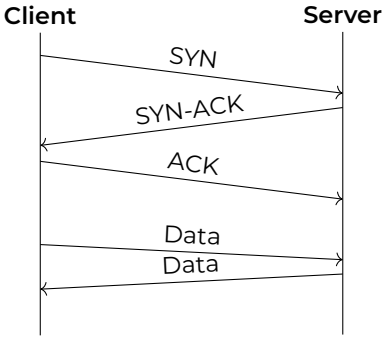
TCP 3 Way Handshake



- **SYN**: The client sends a SYN (synchronize) packet to initiate a connection.
- **SYN-ACK**: The server responds with a SYN-ACK (synchronize-acknowledge) packet to acknowledge the request.
- **ACK**: The client sends an ACK (acknowledge) packet to establish the connection, completing the handshake.
- **Data Transmission**: Once the connection is established, data is exchanged between the client and server.
- **Acknowledgment**: Each data packet is acknowledged by the receiver to ensure reliable delivery.

Connection Reset Attacks

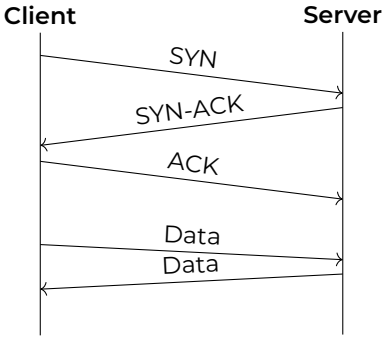
TCP 3 Way Handshake



- **SYN**: The client sends a SYN (synchronize) packet to initiate a connection.
- **SYN-ACK**: The server responds with a SYN-ACK (synchronize-acknowledge) packet to acknowledge the request.
- **ACK**: The client sends an ACK (acknowledge) packet to establish the connection, completing the handshake.
- **Data Transmission**: Once the connection is established, data is exchanged between the client and server.
- **Acknowledgment**: Each data packet is acknowledged by the receiver to ensure reliable delivery.

Connection Reset Attacks

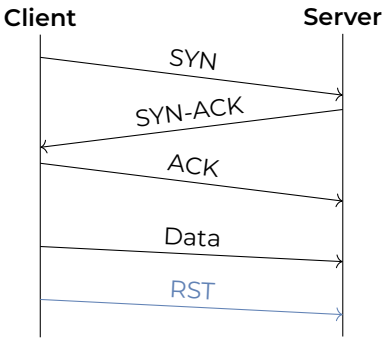
TCP 3 Way Handshake



- **SYN**: The client sends a SYN (synchronize) packet to initiate a connection.
- **SYN-ACK**: The server responds with a SYN-ACK (synchronize-acknowledge) packet to acknowledge the request.
- **ACK**: The client sends an ACK (acknowledge) packet to establish the connection, completing the handshake.
- **Data Transmission**: Once the connection is established, data is exchanged between the client and server.
- **Acknowledgment**: Each data packet is acknowledged by the receiver to ensure reliable delivery.

Connection Reset Attacks

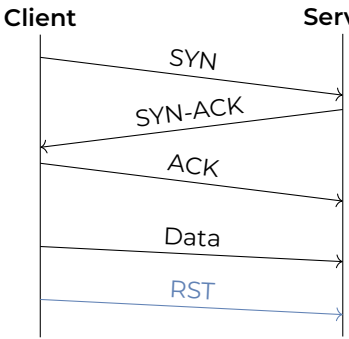
TCP: Resetting Connections



- The connection starts with a normal handshake (SYN, SYN-ACK, ACK) and data exchange.
- When the client or server no longer needs the connection or detects an issue, a legitimate TCP **Reset (RST)** packet is sent to terminate it.
- The reset packet immediately halts communication and frees up system resources, ensuring no further data transmission.

Connection Reset Attacks

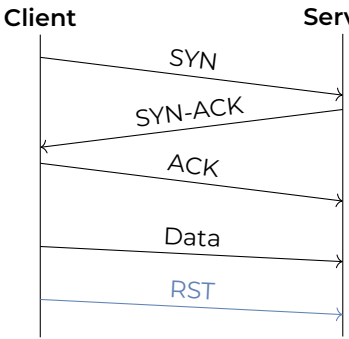
TCP: Resetting Connections



- The connection starts with a normal handshake (SYN, SYN-ACK, ACK) and data exchange.
- When the client or server no longer needs the connection or detects an issue, a legitimate TCP **Reset (RST)** packet is sent to terminate it.
- The reset packet immediately halts communication and frees up system resources, ensuring no further data transmission.

Connection Reset Attacks

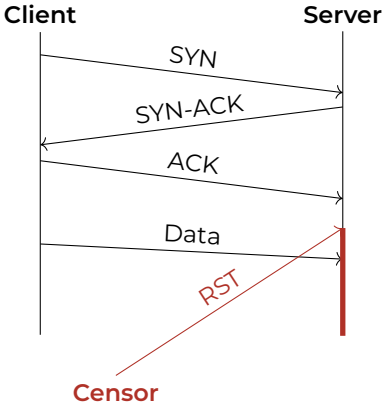
TCP: Resetting Connections



- The connection starts with a normal handshake (SYN, SYN-ACK, ACK) and data exchange.
- When the client or server no longer needs the connection or detects an issue, a legitimate TCP **Reset (RST)** packet is sent to terminate it.
- The reset packet immediately halts communication and frees up system resources, ensuring no further data transmission.

Connection Reset Attacks

Running a TCP Reset Attack



- The client initiates a TCP connection with a **SYN**, the server responds with **SYN-ACK**, and the client completes the handshake with **ACK**.
- Data is exchanged between the client and server after the handshake.
- The censor monitors traffic and injects a forged **RST** (Reset) packet.
- The **RST** packet terminates the connection.
- Any data sent after the reset is dropped, ending interaction between the client and server.

Network and Routing Attacks

Censors may use advanced network manipulation to control access:

- **Denial of Service (DoS) Attacks:**
  - Overloading targeted servers to disrupt services.
- **BGP Hijacking:**
  - Redirecting internet traffic through compromised routes.
- **Network Disconnection:**
  - Cutting off entire regions or countries from the internet.

Special Software for Censorship

Governments may enforce the use of specific software to censor or monitor:

- **TomSkype:** Modified Skype client for censorship in China.
- **GreenDam:** Software required by Chinese users to filter and block content.

Censorship at Service Providers

Internet service providers and platforms can be direct agents of censorship:

- **Search Engine Indexing:** Excluding certain websites from search results.
- **Deplatforming:** Removing accounts or users from platforms like social media.

Cross-Site Scripting (XSS) (1)

What is XSS?

- Cross-site scripting (XSS) is a vulnerability that allows attackers to inject malicious scripts into web pages viewed by others.
- Normally used for stealing data or session cookies, XSS can also be repurposed for censorship.

How XSS is Used for Censorship:

- Censors exploit XSS vulnerabilities to inject scripts that modify or block access to certain content on targeted websites.
- By injecting malicious JavaScript, censors can redirect users away from restricted content or modify the page to hide or replace the content.

Cross-Site Scripting (XSS) (2)

- XSS-based censorship works at the browser level, affecting individual users rather than blocking content at the network level.
- This technique allows censors to target specific users or groups, making it harder to detect than traditional censorship methods.

Examples:

- **Tunisia (2011):** During the Arab Spring, login credentials for Gmail, Yahoo, and Facebook were injected to seize control of regime-critical groups.
- **Comcast (USA, 2014):** Injected ads into user traffic for subscribers on Xfinity WiFi.

URL Filtering

One of the most commonly used censorship methods worldwide:

- Primarily implemented at the ISP level.
- Also used in corporate networks, often paired with TLS interception.

URL Filtering

One of the most commonly used censorship techniques worldwide:

- **Implemented at the ISP level:** Internet Service Providers block access to specific URLs, often based on government blacklists or regulatory demands.
- **Commonly used in institutions:** Schools, workplaces, and libraries apply URL filtering to control access to certain sites (e.g., social media, adult content).
- **Combined with other techniques:** URL filtering is frequently paired with DNS tampering or TLS interception to block encrypted websites.
- **Bypass methods:** Circumvention tools like VPNs, Tor, or DNS-over-HTTPS are often used to evade URL filtering.

Censorship Measurement (1)

- **Large-Scale Measurement Studies:**
  - These studies analyze how censors block or filter content across different regions and platforms.
  - Techniques include inspecting packet traffic, detecting DNS tampering, and identifying IP blacklisting or keyword filtering methods.
- **Longitudinal Data:**
  - Censorship evolves over time as new methods are developed and deployed.
  - These studies track changes to understand how censors adapt to circumvention tools and emerging technologies.
  - **Example:** China's Great Firewall initially relied on basic IP blocking but has evolved into sophisticated techniques like deep packet inspection (DPI) and HTTPS interception.

Censorship Measurement (2)

- **Tools for Measurement:**
  - **OONI (Open Observatory of Network Interference):** A global platform that collects real-time data on internet censorship worldwide.
  - **Censorship Analyzer Tools:** Used by researchers to detect censorship techniques like IP filtering, DNS poisoning, and deep packet inspection, helping to identify censorship patterns.

The Great Firewall of China 

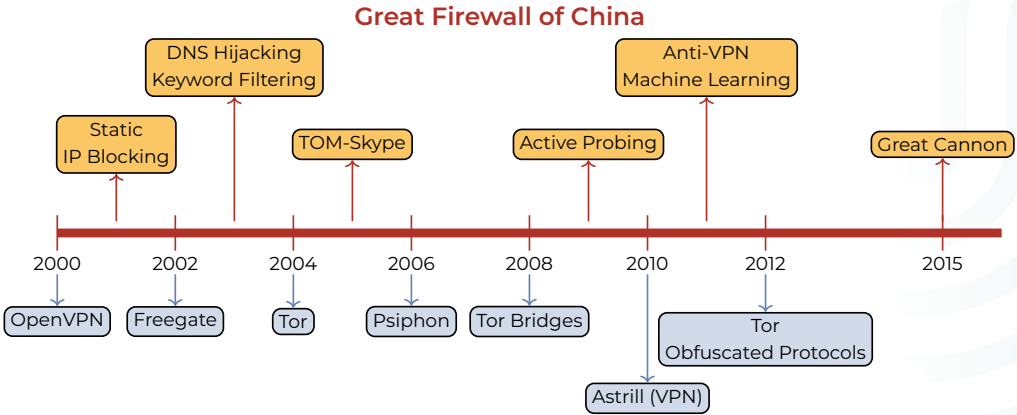
The Great Firewall of China

An Overview

- **Purpose:** A large-scale system of censorship and surveillance employed by the Chinese government to control and restrict access to online content.
- **Key Mechanisms:**
  - Blocking of websites and content (e.g., social media platforms, news outlets).
  - Keyword filtering to prevent specific search terms or phrases.
  - IP blocking and domain overblocking.
  - Traffic analysis and manipulation (e.g., injecting forged IP addresses).
- **Targets:** Foreign websites, politically sensitive content, and encrypted traffic (Tor or VPNs).
- **Noteworthy Challenge:** Ongoing cat-and-mouse game with censorship circumvention tools like VPNs, Tor, and other anonymizing technologies.

The Great Firewall of China

Censor me if you can



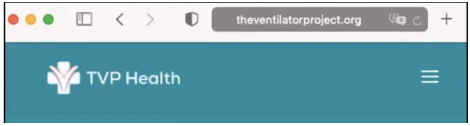
Overblocking

Great Firewall of China

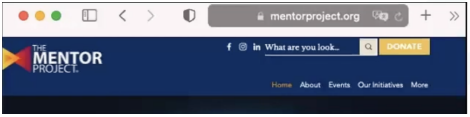
The Tor Project's domain "torproject.org" is blocked under the rule:

***torproject.org**

⟶ Any domains ending with "torproject.org" are censored



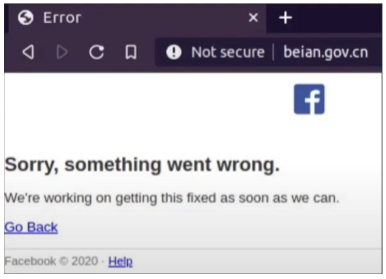
theventilatorproject.org



mentorproject.org

Geoblocking

Great Firewall of China



View from outside China

View from inside China

Forged IP Addresses

Great Firewall of China

- **Censorship Method:** The Great Firewall injects *forged IP addresses* to mislead or block user access to certain websites.
- **Inconsistent Injection:** Not all forged IPs are injected equally; some are used more frequently, causing inconsistent censorship.
- **Circumvention:** By identifying patterns in the injected forged IP addresses, researchers can detect and bypass censorship with a 99% success rate.

Censorship Counter-Measures

Censorship Circumvention

- **Network Methodology**
  - **Domain Fronting:** A technique that allows users to bypass censorship by routing traffic through a different domain, making it appear like they are accessing a legitimate service
  - 
- **Cryptographic Methodology**
  - **Fully Encrypted Protocols (FEPs):** These protocols encrypt *all data in transit*, preventing interception and analysis by censors. They ensure user privacy and secure communications
  -

Censorship Circumvention

- **Network Methodology**
  - **Domain Fronting:** A technique that allows users to bypass censorship by routing traffic through a different domain, making it appear like they are accessing a legitimate service
  - 
- **Cryptographic Methodology**
  - **Fully Encrypted Protocols (FEPs):** These protocols encrypt *all data in transit*, preventing interception and analysis by censors. They ensure user privacy and secure communications
  - 

Domain Fronting (1)

- **What is Domain Fronting?**
  - A technique used to bypass censorship by routing traffic through a different domain than the one the user intends to access.
  - Involves sending requests to a front domain (e.g., `example.com`) that appears legitimate, while accessing a hidden target domain (e.g., `blocked.com`).
  - Works only if both domains are hosted by the same content delivery network (CDN).
- **Benefits Against Censorship:**
  - **Traffic Obfuscation:** By masking the true destination, it becomes challenging for censors to identify and block specific sites.
  - **Resilience to Blocking:** Even if the target domain is blacklisted, users can still connect through the front domain without interruption.

Domain Fronting (2)

- **Real-World Applications:**
  - Activists in repressive regimes use domain fronting to communicate and access information that is otherwise censored.
  - In 2023, 22 out of 30 CDNs still allow domain fronting .
  - Unfortunately, Google stopped supporting domain fronting in 2018 .

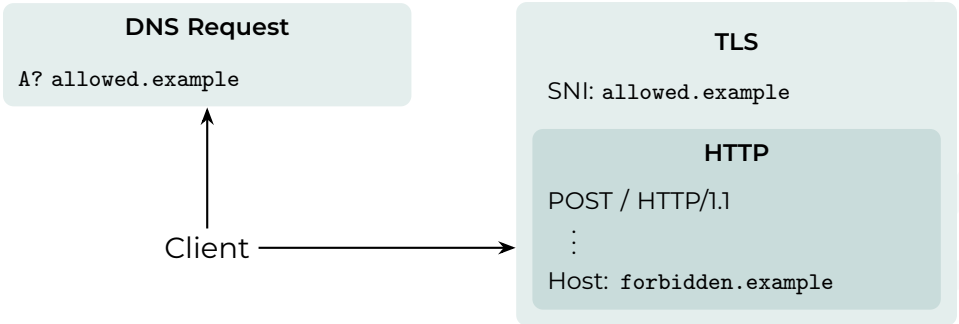
Domain Fronting (1)

How to Domain Front

- **Client requests allowed IP address:** The client resolves an allowed domain through DNS and receives the IP address of a CDN or cloud service.
- **Client connects to CDN:** The client establishes a connection to the CDN using the allowed domain in the DNS and TLS handshake, visible to any network observer.
- **Encrypted request contains forbidden domain:** Within the encrypted HTTPS request, the client specifies the forbidden domain in the HTTP Host header, hidden from censorship tools.

Domain Fronting (2)

How to Domain Front



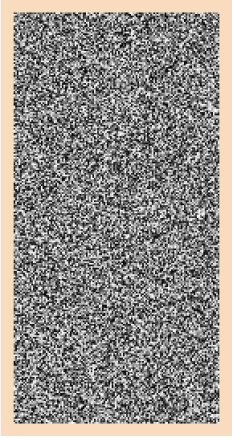
Fully Encrypted Protocols (FEPs) (1)

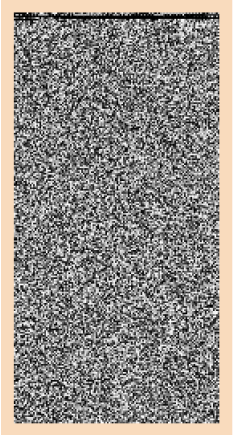
Preventing Censorship

- **What are Fully Encrypted Protocols?**
  - FEPs are specialized protocols designed to ensure that all data is encrypted end-to-end, preventing unauthorized access and inspection.
  - Examples include:
    - **Obfs4**: An obfuscation protocol used to disguise traffic.
    - **Meek**: A transport method that disguises traffic by routing it through cloud services.
    - **Shadowsocks**: A secure socks5 proxy that provides privacy and security.
- **How They Work:**
  - Encrypt data at the application layer before it leaves the user's device, making it unreadable to interceptors.
  - Use obfuscation techniques to disguise the nature of the traffic, making it harder for censors to detect.

Fully Encrypted Protocols (FEPs)

Which Picture Shows TLS and which obfs4?

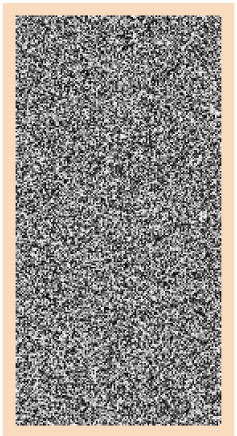




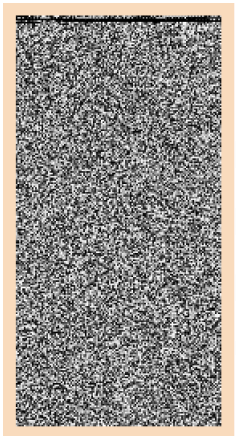
Fully Encrypted Protocols (FEPs)

Which Picture Shows TLS and which obfs4?

obfs4:



TLS:



Fully Encrypted Protocols (FEPs)

Benefits Against Censorship:

- **Traffic Obfuscation:**
  - By disguising the nature of the traffic, FEPs make it difficult for censors to differentiate between legitimate and malicious traffic.
  - The censor can only block everything or allo everything.
  - In the end, it has more incentive to allow everything.
  - Censorship mechanisms rely on identifying specific patterns or keywords, which FEPs effectively mask.
- **Bypassing Network Filters:**
  - FEPs can circumvent network-level filtering that targets specific IP addresses or domain names.
  - Even if a specific site is blocked, users can access it through an FEP without detection.

Fully Encrypted Protocols (FEPs)

Benefits Against Censorship:

- **Traffic Obfuscation:**
  - By disguising the nature of the traffic, FEPs make it difficult for censors to differentiate between legitimate and malicious traffic.
  - The censor can only block everything or allo everything.
  - In the end, it has more incentive to allow everything.
  - Censorship mechanisms rely on identifying specific patterns or keywords, which FEPs effectively mask.
- **Bypassing Network Filters:**
  - FEPs can circumvent network-level filtering that targets specific IP addresses or domain names.
  - Even if a specific site is blocked, users can access it through an FEP without detection.

Fully Encrypted Protocols (FEPs)

Furhter References

“Security notions for fully encrypted protocols"
(Ellis Fenske, Aaron Johnson. FOCI 2023)

“Bytes to Schlep? Use a FEP: Hiding Protocol Metadata with Fully Encrypted Protocols"
(Ellis Fenske, Aaron Johnson, 2024)

“Obfuscated Key Exchange”
(Shannon Veitch. Talk at RWC 2024)

Feedback

Your *anonymous feedback* is invaluable to us, and we are truly grateful for your time and insights.

Thank you for helping us improve!

https://tuwel.tuwien.ac.at/mod/feedback/view.php?id=2442869

PRIVACY
ENHANCING
TECHNOLOGIES