Privacy Enhancing Technologies (BSc)

Lecture II: Internet and Privacy in the Web

Univ.-Prof. Dr. Dominique Schröder

October 14, 2024

This Lecture's Questions

- What is Privacy?
- Why Privacy in the Internet?
- How does the internet work?
- What are privacy-enhancing technologies?

This Lecture's Questions

- What is Privacy?
- Why Privacy in the Internet?
- How does the internet work?
- What are privacy-enhancing technologies?

Protocols → network

This Lecture's Questions

- What is Privacy?
- Why Privacy in the Internet?
- How does the internet work?
- What are privacy-enhancing technologies?

This Lecture's Questions

- What is Privacy?
- Why Privacy in the Internet?
- How does the internet work?
- What are privacy-enhancing technologies?

Privacy

What is Privacy? (1)

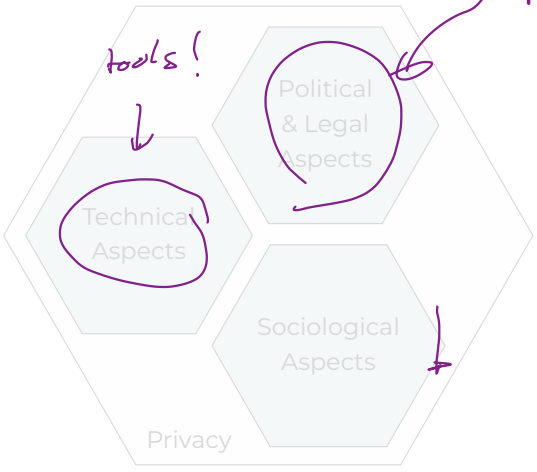
Definition (Warren, Brandweis 1890)

The right to be left alone.

Definition (Westin, 1970)

The right of the individual to decide what information about himself should be communicated to others and under what circumstances.

What is Privacy? (2)



Sociological Aspects

I have nothing to hide

Everyone Needs Privacy

- **Physical privacy** (curtains, doors)
- **Health-related issues**
- **Work-related issues** (unions, religion, salary)
- **Political views**
- **Financial privacy** (bank details, credit scores)
- **Online activities** (browsing history, social media)
- **Communication privacy** (messages, calls, emails)
- **Family matters** (relationships, personal life)
- **Location data** (whereabouts, movements)
- **Intellectual property** (creative works, research)
- …

Everyone Needs Privacy

- **Physical privacy** (curtains, doors)
- **Health-related issues**
- **Work-related issues** (unions, religion, salary)
- **Political views**
- **Financial privacy** (bank details, credit scores)
- **Online activities** (browsing history, social media)
- **Communication privacy** (messages, calls, emails)
- **Family matters** (relationships, personal life)
- **Location data** (whereabouts, movements)
- **Intellectual property** (creative works, research)
- …

Everyone Needs Privacy

- **Physical privacy** (curtains, doors)
- **Health-related issues**
- **Work-related issues** (unions, religion, salary)
- **Political views**
- **Financial privacy** (bank details, credit scores)
- **Online activities** (browsing history, social media)
- **Communication privacy** (messages, calls, emails)
- **Family matters** (relationships, personal life)
- **Location data** (whereabouts, movements)
- **Intellectual property** (creative works, research)
- …

Everyone Needs Privacy

- **Physical privacy** (curtains, doors)
- **Health-related issues**
- **Work-related issues** (unions, religion, salary)
- **Political views**
- **Financial privacy** (bank details, credit scores)
- **Online activities** (browsing history, social media)
- **Communication privacy** (messages, calls, emails)
- **Family matters** (relationships, personal life)
- **Location data** (whereabouts, movements)
- **Intellectual property** (creative works, research)
- …

Everyone Needs Privacy

- **Physical privacy** (curtains, doors)
- **Health-related issues**
- **Work-related issues** (unions, religion, salary)
- **Political views**
- **Financial privacy** (bank details, credit scores)
- **Online activities** (browsing history, social media)
- **Communication privacy** (messages, calls, emails)
- **Family matters** (relationships, personal life)
- **Location data** (whereabouts, movements)
- **Intellectual property** (creative works, research)
- …

Everyone Needs Privacy

- **Physical privacy** (curtains, doors)
- **Health-related issues**
- **Work-related issues** (unions, religion, salary)
- **Political views**
- **Financial privacy** (bank details, credit scores)
- **Online activities** (browsing history, social media) → profile
- **Communication privacy** (messages, calls, emails)
- **Family matters** (relationships, personal life)
- **Location data** (whereabouts, movements)
- **Intellectual property** (creative works, research)
- …

Everyone Needs Privacy

- **Physical privacy** (curtains, doors)
- **Health-related issues**
- **Work-related issues** (unions, religion, salary)
- **Political views**
- **Financial privacy** (bank details, credit scores)
- **Online activities** (browsing history, social media)
- **Communication privacy** (messages, calls, emails)
- **Family matters** (relationships, personal life)
- **Location data** (whereabouts, movements)
- **Intellectual property** (creative works, research)
- …

Everyone Needs Privacy

- **Physical privacy** (curtains, doors)
- **Health-related issues**
- **Work-related issues** (unions, religion, salary)
- **Political views**
- **Financial privacy** (bank details, credit scores)
- **Online activities** (browsing history, social media)
- **Communication privacy** (messages, calls, emails)
- **Family matters** (relationships, personal life)
- **Location data** (whereabouts, movements)
- **Intellectual property** (creative works, research)
- …

Everyone Needs Privacy

- **Physical privacy** (curtains, doors)
- **Health-related issues**
- **Work-related issues** (unions, religion, salary)
- **Political views**
- **Financial privacy** (bank details, credit scores)
- **Online activities** (browsing history, social media)
- **Communication privacy** (messages, calls, emails)
- **Family matters** (relationships, personal life)
- **Location data** (whereabouts, movements)
- **Intellectual property** (creative works, research)
- …

Everyone Needs Privacy

- **Physical privacy** (curtains, doors)
- **Health-related issues**
- **Work-related issues** (unions, religion, salary)
- **Political views**
- **Financial privacy** (bank details, credit scores)
- **Online activities** (browsing history, social media)
- **Communication privacy** (messages, calls, emails)
- **Family matters** (relationships, personal life)
- **Location data** (whereabouts, movements)
- **Intellectual property** (creative works, research)
- ...

Everyone Needs Privacy

- **Physical privacy** (curtains, doors)
- **Health-related issues**
- **Work-related issues** (unions, religion, salary)
- **Political views**
- **Financial privacy** (bank details, credit scores)
- **Online activities** (browsing history, social media)
- **Communication privacy** (messages, calls, emails)
- **Family matters** (relationships, personal life)
- **Location data** (whereabouts, movements)
- **Intellectual property** (creative works, research)
- …

Privacy vs. Security

Less privacy = more security?

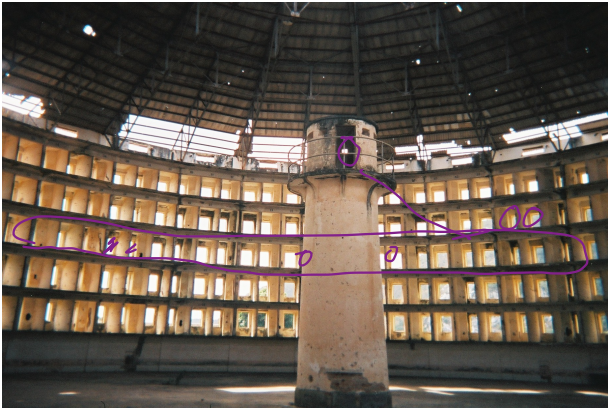
Panopticism (1)

Definition (Panopticism, Michel Foucault)

A social theory describing a system of power where individuals, aware of possible surveillance, self-regulate their behavior. The concept comes from the Panopticon, a prison design where a central watchtower allows constant observation without inmates knowing when they are being watched.

- **Key Idea**: The uncertainty of being watched results in self-discipline and self-censorship among individuals.
- **Implications**: Extends beyond prisons to workplaces, schools, and digital surveillance, where behavior is influenced by the perceived presence of observation.

Panopticism (2)



https://en.wikipedia.org/wiki/Panopticon

Paternalism

Definition (Paternalism)

Paternalism refers to an "action that limits a person's or group's liberty or autonomy and is intended to promote their own good."

- **Examples**: Seat belts, non-smoking regulations, mandatory vaccinations.
- **Social Behavior**: Regulation of activities like online gaming, shopping, religious practices, etc.

Paternalism

Definition (Paternalism)

Paternalism refers to an "action that limits a person's or group's liberty or autonomy and is intended to promote their own good."

- **Examples**: Seat belts, non-smoking regulations, mandatory vaccinations.
- **Social Behavior**: Regulation of activities like online gaming, shopping, religious practices, etc.

Surveillance

Definition (Surveillance)

Surveillance involves monitoring activities or communications to gather information, often for security or control purposes.

- **Scope**:
  - **Mass-surveillance**: "Let's collect location data of all mobile phones in our country in order to catch terrorists."
  - **Targeted-surveillance**: "Let's wiretap people we suspect of planning a terror attack."
- **Common Technologies**: Internet/phone surveillance, CCTV cameras.

Surveillance

Definition (Surveillance)

Surveillance involves monitoring activities or communications to gather information, often for security or control purposes.

- **Scope**:
  - **Mass-surveillance**: "Let's collect location data of all mobile phones in our country in order to catch terrorists."
  - **Targeted-surveillance**: "Let's wiretap people we suspect of planning a terror attack."
- **Common Technologies**: Internet/phone surveillance, CCTV cameras.

Surveillance

Definition (Surveillance)

Surveillance involves monitoring activities or communications to gather information, often for security or control purposes.

- **Scope**:
  - **Mass-surveillance**: “Let’s collect location data of all mobile phones in our country in order to catch terrorists.”
  - **Targeted-surveillance**: “Let’s wiretap people we suspect of planning a terror attack.”
- **Common Technologies**: Internet/phone surveillance, CCTV cameras.

Surveillance

Definition (Surveillance)

Surveillance involves monitoring activities or communications to gather information, often for security or control purposes.

- **Scope**:
  - **Mass-surveillance**: “Let’s collect location data of all mobile phones in our country in order to catch terrorists.”
  - **Targeted-surveillance**: “Let’s wiretap people we suspect of planning a terror attack.”
- **Common Technologies**: Internet/phone surveillance, CCTV cameras.

Documented Cases of Abuse

Video Surveillance at Schwedenplatz

- **Location**: Austria, 2005
- **Incident**: Out of boredom, operators used video surveillance to watch people in their homes.

NSA Analysts Stalked Ex-Partners:

- **Incident**: Dubbed **LOVEINT**.
- **Details**: Willful misconduct by NSA employees to spy on their ex-partners.

References and Resources

“Why privacy matters”
(TED Talk by Alessandro Acquisti)

“How the NSA betrayed the world’s trust”
(TED Talk by Mikko Hypponen)

Zero
(Book by Mark Elsberg)

1984
(Book by George Orwell)

Legal and Political Aspects

Privacy as a Universal Human Right

Privacy is recognized as a fundamental human right. According to the UDHR:

Definition (Universal Declaration of Human Rights (UDHR))

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence."

Article 8 of the European Convention on Human Rights

Definition (Article 8, European Convention on Human Rights)

"Everyone has the right to respect for his private and family life, his home and his correspondence."

- **Exceptions**: This right may be limited if it is in accordance with the law and necessary in a democratic society, including:
  - National security, public safety, or the economic well-being of the country.
  - Prevention of disorder or crime.
  - Protection of health or morals.
  - Protection of the rights and freedoms of others.

Article 8 of the European Convention on Human Rights

Definition (Article 8, European Convention on Human Rights)

"Everyone has the right to respect for his private and family life, his home and his correspondence."

- **Exceptions**: This right may be limited if it is in accordance with the law and necessary in a democratic society, including:
  - National security, public safety, or the economic well-being of the country.
  - Prevention of disorder or crime.
  - Protection of health or morals.
  - Protection of the rights and freedoms of others.

Article 8 of the European Convention on Human Rights

Definition (Article 8, European Convention on Human Rights)

"Everyone has the right to respect for his private and family life, his home and his correspondence."

- **Exceptions**: This right may be limited if it is in accordance with the law and necessary in a democratic society, including:
  - National security, public safety, or the economic well-being of the country.
  - Prevention of disorder or crime.
  - Protection of health or morals.
  - Protection of the rights and freedoms of others.

Article 8 of the European Convention on Human Rights

Definition (Article 8, European Convention on Human Rights)

"Everyone has the right to respect for his private and family life, his home and his correspondence."

- **Exceptions**: This right may be limited if it is in accordance with the law and necessary in a democratic society, including:
  - National security, public safety, or the economic well-being of the country.
  - Prevention of disorder or crime.
  - Protection of health or morals.
  - Protection of the rights and freedoms of others.

Article 8 of the European Convention on Human Rights

Definition (Article 8, European Convention on Human Rights)

"Everyone has the right to respect for his private and family life, his home and his correspondence."

- **Exceptions**: This right may be limited if it is in accordance with the law and necessary in a democratic society, including:
  - National security, public safety, or the economic well-being of the country.
  - Prevention of disorder or crime.
  - Protection of health or morals.
  - Protection of the rights and freedoms of others.

Political Aspects of Privacy

- **Surveillance**:
  - Mass surveillance vs. targeted attacks
  - Attacks against people, organizations, industry
  - Insights since Snowden revelations and hacked providers (e.g., Phineas Fisher)
  - Examples: NSO Group, Candiru, HackingTeam, FinFisher
- **Censorship**:
  - Hack and track down political opposition
- **Conformity (Panopticism/Paternalism)**:
  - Social Credit System in China (since 2013): travel bans, social status, exclusion from school admissions, etc.

Political Aspects of Privacy

- **Surveillance**:
  - Mass surveillance vs. targeted attacks
  - Attacks against people, organizations, industry
  - Insights since Snowden revelations and hacked providers (e.g., Phineas Fisher)
  - Examples: NSO Group, Candiru, HackingTeam, FinFisher
- **Censorship**:
  - Hack and track down political opposition
- **Conformity (Panopticism/Paternalism)**:
  - Social Credit System in China (since 2013): travel bans, social status, exclusion from school admissions, etc.

Political Aspects of Privacy

- **Surveillance**:
  - Mass surveillance vs. targeted attacks
  - Attacks against people, organizations, industry
  - Insights since Snowden revelations and hacked providers (e.g., Phineas Fisher)
  - Examples: NSO Group, Candiru, HackingTeam, FinFisher
- **Censorship**:
  - Hack and track down political opposition
- **Conformity (Panopticism/Paternalism)**:
  - Social Credit System in China (since 2013): travel bans, social status, exclusion from school admissions, etc.

Political Aspects of Privacy

- **Surveillance**:
  - Mass surveillance vs. targeted attacks
  - Attacks against people, organizations, industry
  - Insights since Snowden revelations and hacked providers (e.g., Phineas Fisher)
  - Examples: NSO Group, Candiru, HackingTeam, FinFisher
- **Censorship**:
  - Hack and track down political opposition
- **Conformity (Panopticism/Paternalism)**:
  - Social Credit System in China (since 2013): travel bans, social status, exclusion from school admissions, etc.

Political Aspects of Privacy

- **Surveillance**:
  - Mass surveillance vs. targeted attacks
  - Attacks against people, organizations, industry
  - Insights since Snowden revelations and hacked providers (e.g., Phineas Fisher)
  - Examples: NSO Group, Candiru, HackingTeam, FinFisher
- **Censorship**:
  - Hack and track down political opposition
- **Conformity (Panopticism/Paternalism)**:
  - Social Credit System in China (since 2013): travel bans, social status, exclusion from school admissions, etc.

Political Aspects of Privacy

- **Surveillance**:
  - Mass surveillance vs. targeted attacks
  - Attacks against people, organizations, industry
  - Insights since Snowden revelations and hacked providers (e.g., Phineas Fisher)
  - Examples: NSO Group, Candiru, HackingTeam, FinFisher
- **Censorship**:
  - Hack and track down political opposition
- **Conformity (Panopticism/Paternalism)**:
  - Social Credit System in China (since 2013): travel bans, social status, exclusion from school admissions, etc.

Political Aspects of Privacy

- **Surveillance**:
  - Mass surveillance vs. targeted attacks
  - Attacks against people, organizations, industry
  - Insights since Snowden revelations and hacked providers (e.g., Phineas Fisher)
  - Examples: NSO Group, Candiru, HackingTeam, FinFisher
- **Censorship**:
  - Hack and track down political opposition 
- **Conformity (Panopticism/Paternalism)**:
  - Social Credit System in China (since 2013): travel bans, social status, exclusion from school admissions, etc.

Political Aspects of Privacy

- **Surveillance**:
  - Mass surveillance vs. targeted attacks
  - Attacks against people, organizations, industry
  - Insights since Snowden revelations and hacked providers (e.g., Phineas Fisher)
  - Examples: NSO Group, Candiru, HackingTeam, FinFisher
- **Censorship**:
  - Hack and track down political opposition 
- **Conformity (Panopticism/Paternalism)**:
  - Social Credit System in China (since 2013): travel bans, social status, exclusion from school admissions, etc.

Political Aspects of Privacy

- **Surveillance**:
  - Mass surveillance vs. targeted attacks
  - Attacks against people, organizations, industry
  - Insights since Snowden revelations and hacked providers (e.g., Phineas Fisher)
  - Examples: NSO Group, Candiru, HackingTeam, FinFisher
- **Censorship**:
  - Hack and track down political opposition 
- **Conformity (Panopticism/Paternalism)**:
  - Social Credit System in China (since 2013): travel bans, social status, exclusion from school admissions, etc. 

Why Privacy Matters on the Internet

- **Global Access**: Data is accessible from anywhere.
- **Digital Footprint**: Online actions are permanent.
- **Behavioral Ads**: Data is used to manipulate preferences.
- **Data Breaches**: Centralized data attracts hackers.
- **Surveillance**: Cross-border monitoring is easy.

Why Privacy Matters on the Internet

- **Global Access**: Data is accessible from anywhere.
- **Digital Footprint**: Online actions are permanent.
- **Behavioral Ads**: Data is used to manipulate preferences.
- **Data Breaches**: Centralized data attracts hackers.
- **Surveillance**: Cross-border monitoring is easy.

Why Privacy Matters on the Internet

- **Global Access**: Data is accessible from anywhere.
- **Digital Footprint**: Online actions are permanent.
- **Behavioral Ads**: Data is used to manipulate preferences.
- **Data Breaches**: Centralized data attracts hackers.
- **Surveillance**: Cross-border monitoring is easy.

Why Privacy Matters on the Internet

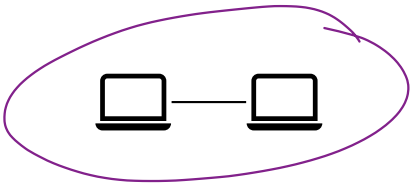
- **Global Access**: Data is accessible from anywhere.
- **Digital Footprint**: Online actions are permanent.
- **Behavioral Ads**: Data is used to manipulate preferences.
- **Data Breaches**: Centralized data attracts hackers. → IBM → Data Breach Report
- **Surveillance**: Cross-border monitoring is easy.

Why Privacy Matters on the Internet

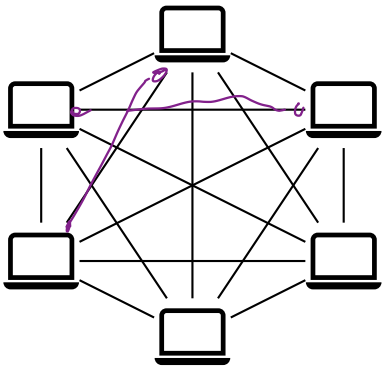
- **Global Access**: Data is accessible from anywhere.
- **Digital Footprint**: Online actions are permanent.
- **Behavioral Ads**: Data is used to manipulate preferences.
- **Data Breaches**: Centralized data attracts hackers.
- **Surveillance**: Cross-border monitoring is easy.

The Internet

Network Topology

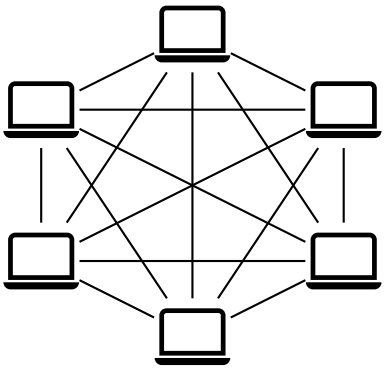


Network Topology



- **Scalability**: Too many connections as more computers join.
  (n^2 connections for n computers.)
- **Complexity**: Hard to manage and maintain all connections.
- **Inefficiency**: Wastes bandwidth and processing power.

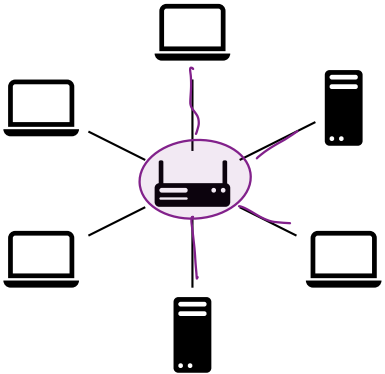
Network Topology



- **Scalability**: Too many connections as more computers join.
  (n^2 connections for n computers.)
- **Complexity**: Hard to manage and maintain all connections.
- **Inefficiency**: Wastes bandwidth and processing power.

Network Topology

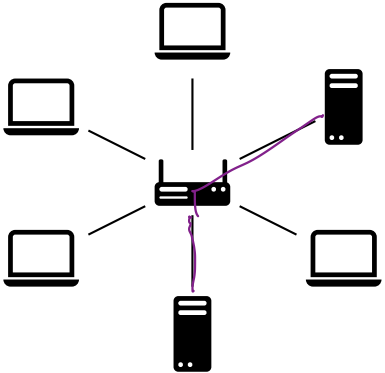
Routers and Servers



- **Routers**:
  - Direct data between networks efficiently.
  - Reduce the need for direct connections between all devices.
  - Optimize data paths to minimize delays.
- **Servers**:
  - Centralize resources and data storage.
  - Handle requests from multiple devices.
  - Enable scalable, shared access to resources.

Network Topology

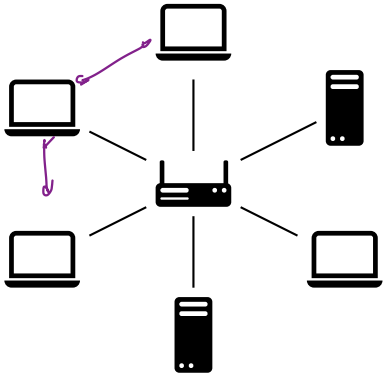
Routers and Servers



- **Routers**:
  - Direct data between networks efficiently.
  - Reduce the need for direct connections between all devices.
  - Optimize data paths to minimize delays.
- **Servers**:
  - Centralize resources and data storage.
  - Handle requests from multiple devices.
  - Enable scalable, shared access to resources.

Network Topology

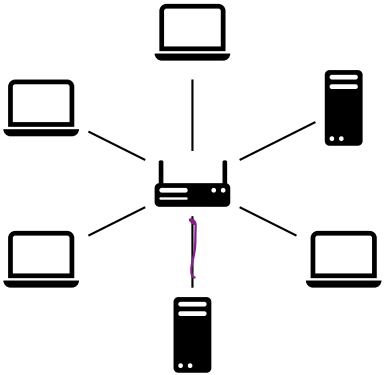
Routers and Servers



- **Routers**:
  - Direct data between networks efficiently.
  - Reduce the need for direct connections between all devices.
  - Optimize data paths to minimize delays.
- **Servers**:
  - Centralize resources and data storage.
  - Handle requests from multiple devices.
  - Enable scalable, shared access to resources.

Network Topology

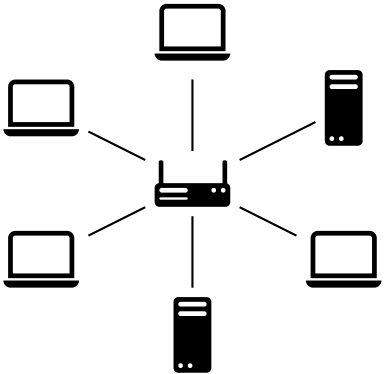
Routers and Servers



- **Routers**:
  - Direct data between networks efficiently.
  - Reduce the need for direct connections between all devices.
  - Optimize data paths to minimize delays.
- **Servers**:
  - Centralize resources and data storage.
  - Handle requests from multiple devices.
  - Enable scalable, shared access to resources.

Network Topology

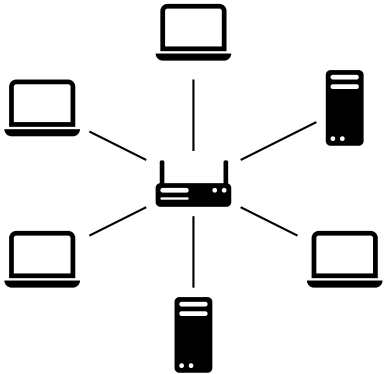
Routers and Servers



- **Routers**:
  - Direct data between networks efficiently.
  - Reduce the need for direct connections between all devices.
  - Optimize data paths to minimize delays.
- **Servers**:
  - Centralize resources and data storage.
  - Handle requests from multiple devices.
  - Enable scalable, shared access to services.

Network Topology

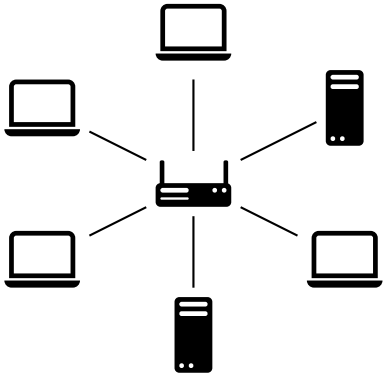
Routers and Servers



- **Routers**:
  - Direct data between networks efficiently.
  - Reduce the need for direct connections between all devices.
  - Optimize data paths to minimize delays.
- **Servers**:
  - Centralize resources and data storage.
  - Handle requests from multiple devices.
  - Enable scalable, shared access to services.

Network Topology

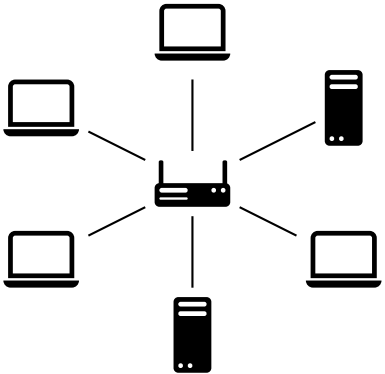
Routers and Servers



- **Routers**:
  - Direct data between networks efficiently.
  - Reduce the need for direct connections between all devices.
  - Optimize data paths to minimize delays.
- **Servers**:
  - Centralize resources and data storage.
  - Handle requests from multiple devices.
  - Enable scalable, shared access to services.

Network Topology

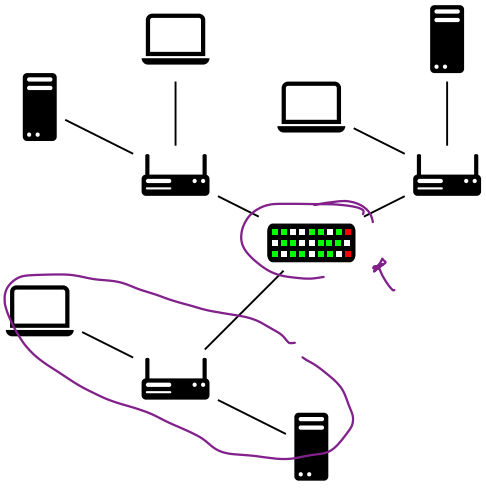
Routers and Servers



- **Routers**:
  - Direct data between networks efficiently.
  - Reduce the need for direct connections between all devices.
  - Optimize data paths to minimize delays.
- **Servers**:
  - Centralize resources and data storage.
  - Handle requests from multiple devices.
  - Enable scalable, shared access to services.

Network Topology

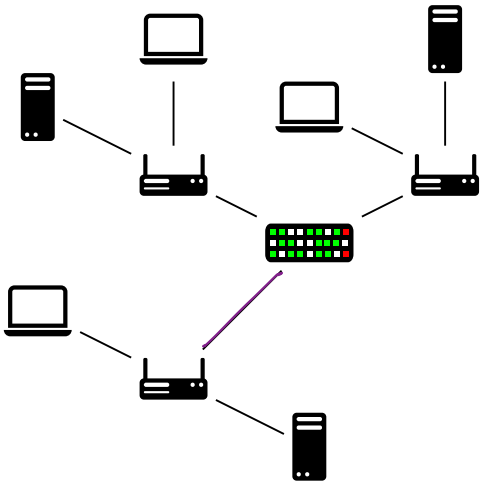
Internet Service Providers



- **Connect local networks**:
  - Link homes, businesses, and organizations.
  - Enable *communication between networks*.
- **Provide Internet Access**:
  - Offer broadband, fiber, mobile data
  - Route data to the global internet

Network Topology

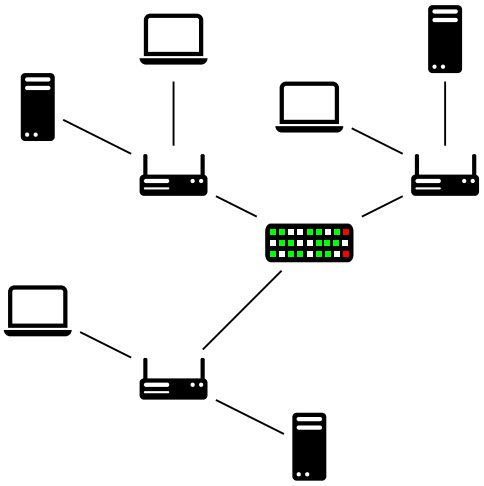
Internet Service Providers



- **Connect local networks**:
  - Link homes, businesses, and organizations.
  - Enable *communication between networks*.
- **Provide Internet Access**:
  - Offer broadband, fiber, mobile data
  - Route data to the global internet

Network Topology

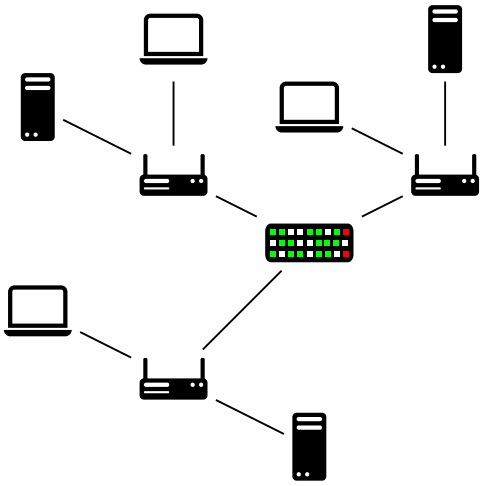
Internet Service Providers



- **Connect local networks**:
  - Link homes, businesses, and organizations.
  - Enable *communication between networks*.
- **Provide Internet Access**:
  - Offer broadband, fiber, mobile data
  - Route data to the global internet

Network Topology

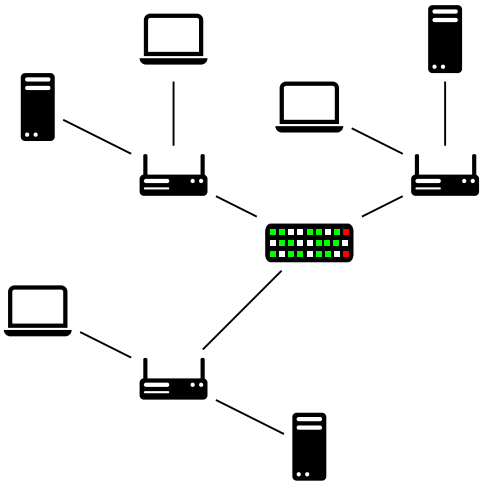
Internet Service Providers



- **Connect local networks**:
  - Link homes, businesses, and organizations.
  - Enable *communication between networks*.
- **Provide Internet Access**:
  - Offer broadband, fiber, mobile data.
  - Route data to the global internet.

Network Topology

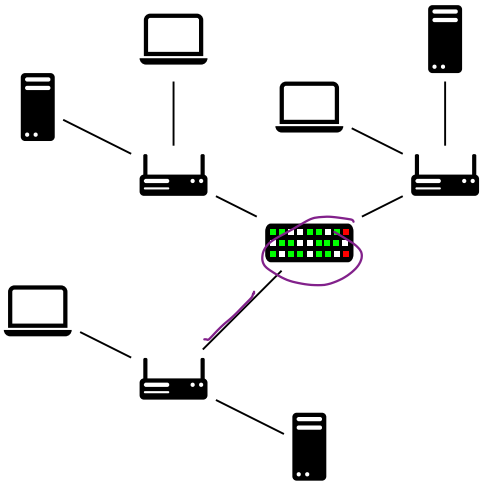
Internet Service Providers



- **Connect local networks**:
  - Link homes, businesses, and organizations.
  - Enable *communication between networks*.
- **Provide Internet Access**:
  - Offer broadband, fiber, mobile data.
  - Route data to the global internet.

Network Topology

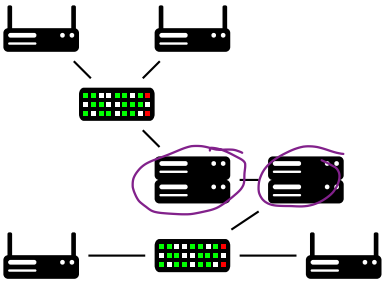
Internet Service Providers



- **Connect local networks**:
  - Link homes, businesses, and organizations.
  - Enable *communication between networks*.
- **Provide Internet Access**:
  - Offer broadband, fiber, mobile data.
  - Route data to the global internet.

Network Topology

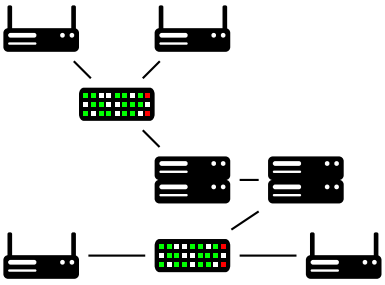
Network Service Providers



- **Internet Backbone**:
  - Connect ISPs and major networks.
  - Handle high-speed global data flow.
- **Global Coverage**:
  - Use fiber-optic cables and satellites.
  - Link networks across continents.

Network Topology

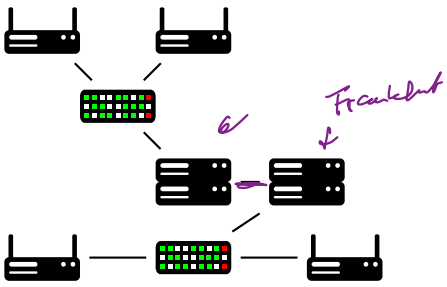
Network Service Providers



- **Internet Backbone**:
  - Connect ISPs and major networks.
  - Handle high-speed global data flow.
- **Global Coverage**:
  - Use fiber-optic cables and satellites.
  - Link networks across continents.

Network Topology

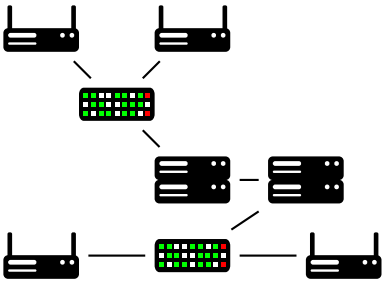
Network Service Providers



- **Internet Backbone**:
  - Connect ISPs and major networks.
  - Handle high-speed global data flow.
- **Global Coverage**:
  - Use fiber-optic cables and satellites.
  - Link networks across continents.

Network Topology

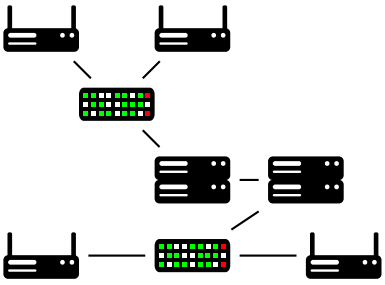
Network Service Providers



- **Internet Backbone**:
  - Connect ISPs and major networks.
  - Handle high-speed global data flow.
- **Global Coverage**:
  - Use fiber-optic cables and satellites.
  - Link networks across continents.

Network Topology

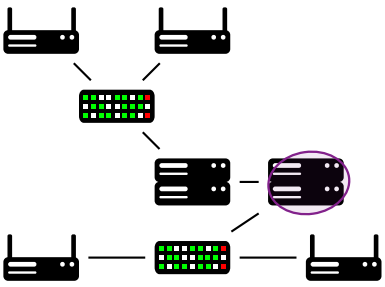
Network Service Providers



- **Internet Backbone**:
  - Connect ISPs and major networks.
  - Handle high-speed global data flow.
- **Global Coverage**:
  - Use fiber-optic cables and satellites.
  - Link networks across continents.

Network Topology

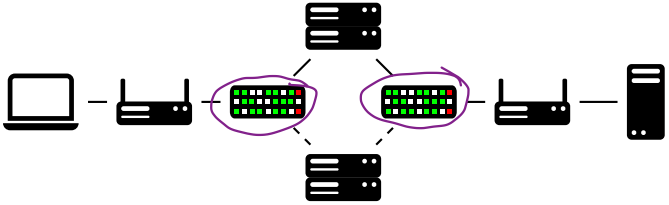
Network Service Providers



- **Internet Backbone**:
  - Connect ISPs and major networks.
  - Handle high-speed global data flow.
- **Global Coverage**:
  - Use fiber-optic cables and satellites.
  - Link networks across continents.

Network Topology

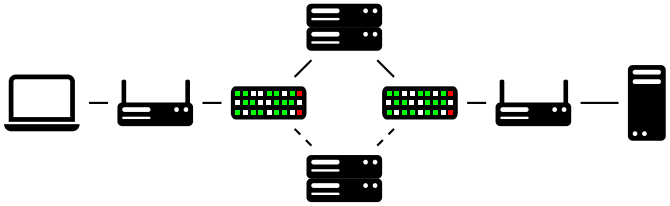
Sending Messages



- **Redundant Design**:
  - Multiple paths ensure reliability.
  - Avoids single points of failure.
- **Dynamic Routing**:
  - Message paths change with network conditions.
  - Route taken is not always predictable.
- **Lack of Privacy**:
  - Intermediaries can see the traffic.

Network Topology

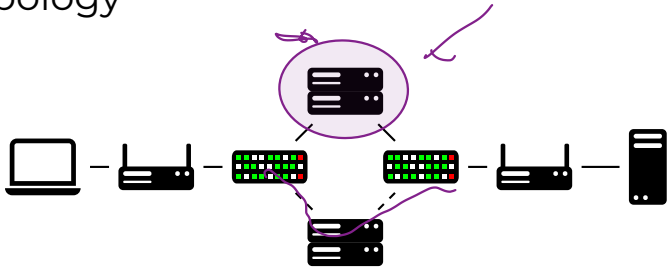
Sending Messages



- **Redundant Design**:
  - Multiple paths ensure reliability.
  - Avoids single points of failure.
- **Dynamic Routing**:
  - Message paths change with network conditions.
  - Route taken is not always predictable.
- **Lack of Privacy**:
  - Intermediaries can see the traffic.

Network Topology

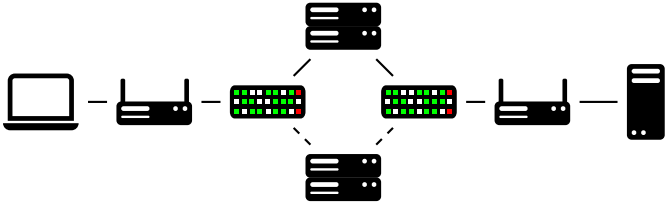
Sending Messages



- **Redundant Design**:
  - Multiple paths ensure reliability.
  - Avoids single points of failure.
- **Dynamic Routing**:
  - Message paths change with network conditions.
  - Route taken is not always predictable.
- **Lack of Privacy**:
  - Intermediaries can see the traffic.

Network Topology

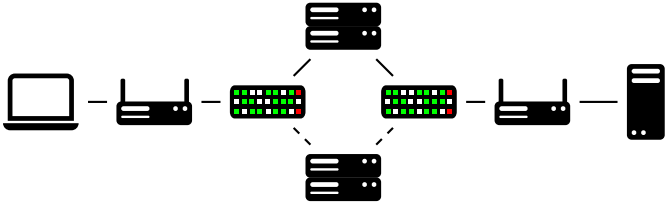
Sending Messages



- **Redundant Design**:
  - Multiple paths ensure reliability.
  - Avoids single points of failure.
- **Dynamic Routing**:
  - Message paths change with network conditions.
  - Route taken is not always predictable.
- **Lack of Privacy**:
  - Intermediaries can see the traffic.

Network Topology

Sending Messages

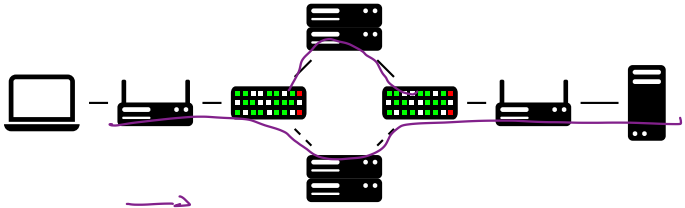


- **Redundant Design**:
  - Multiple paths ensure reliability.
  - Avoids single points of failure.
- **Dynamic Routing**:
  - Message paths change with network conditions.
  - Route taken is not always predictable.
- **Lack of Privacy**:
  - Intermediaries can see the traffic.

→ TCP/IP

Network Topology

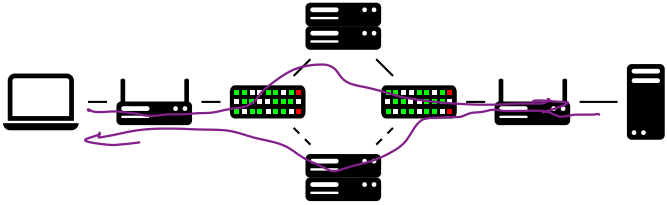
Sending Messages



- **Redundant Design**:
  - Multiple paths ensure reliability.
  - Avoids single points of failure.
- **Dynamic Routing**:
  - Message paths change with network conditions.
  - Route taken is not always predictable.
- **Lack of Privacy**:
  - Intermediaries can see the traffic.

Network Topology

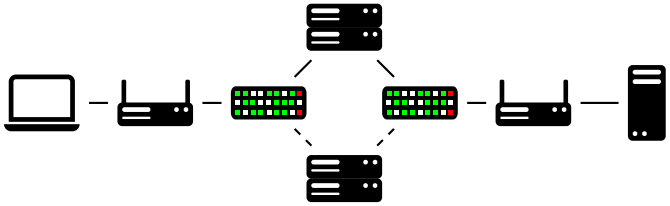
Sending Messages



- **Redundant Design**:
  - Multiple paths ensure reliability.
  - Avoids single points of failure.
- **Dynamic Routing**:
  - Message paths change with network conditions.
  - Route taken is not always predictable.
- **Lack of Privacy**:
  - Intermediaries can see the traffic.

Network Topology

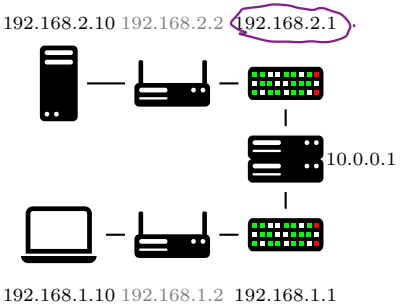
Sending Messages



- **Redundant Design**:
  - Multiple paths ensure reliability.
  - Avoids single points of failure.
- **Dynamic Routing**:
  - Message paths change with network conditions.
  - Route taken is not always predictable.
- **Lack of Privacy**:
  - Intermediaries can see the traffic.

Internet Adresses

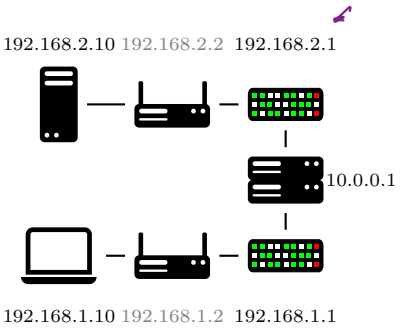
The IP Protocol



- **Unique Identifiers**:
  - Every device on the internet has an IP address.
  - Allows devices to communicate with each other.
- **Two Versions**:
  - **IPv4**: 32-bit, e.g., 192.168.1.1.
  - **IPv6**: 128-bit, e.g., 2001:0db8:1.

Internet Adresses

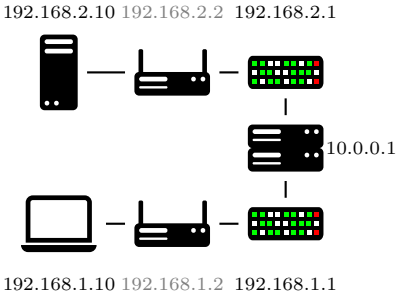
The IP Protocol



- **Unique Identifiers**:
  - Every device on the internet has an IP address.
  - Allows devices to communicate with each other.
- **Two Versions**:
  - **IPv4**: 32-bit, e.g., 192.168.1.1.
  - **IPv6**: 128-bit, e.g., 2001:0db8:1.

Internet Adresses

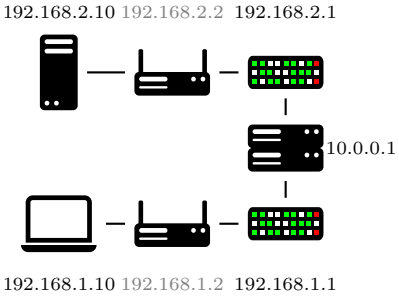
The IP Protocol



- **Unique Identifiers**:
  - Every device on the internet has an IP address.
  - Allows devices to communicate with each other.
- **Two Versions**:
  - **IPv4**: 32-bit, e.g., 192.168.1.1.
  - **IPv6**: 128-bit, e.g., 2001:0db8:1.

Internet Adresses

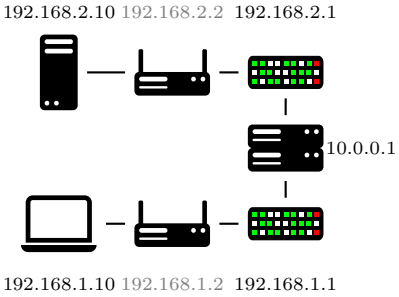
The IP Protocol



- **Unique Identifiers**:
  - Every device on the internet has an IP address.
  - Allows devices to communicate with each other.
- **Two Versions**:
  - **IPv4**: 32-bit, e.g., 192.168.1.1.
  - **IPv6**: 128-bit, e.g., 2001:0db8::1.

Internet Adresses

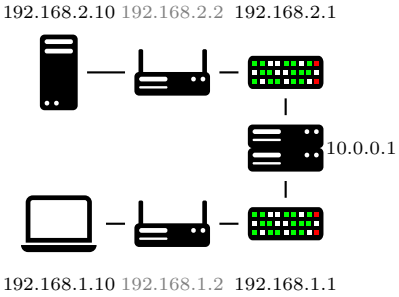
The IP Protocol



- **Unique Identifiers**:
  - Every device on the internet has an IP address.
  - Allows devices to communicate with each other.
- **Two Versions**:
  - **IPv4**: 32-bit, e.g., 192.168.1.1.
  - **IPv6**: 128-bit, e.g., 2001:0db8::1.

Internet Adresses

The IP Protocol



- **Unique Identifiers**:
  - Every device on the internet has an IP address.
  - Allows devices to communicate with each other.
- **Two Versions**:
  - **IPv4**: 32-bit, e.g., 192.168.1.1.
  - **IPv6**: 128-bit, e.g., 2001:0db8::1.

Internet Adresses (2) (1)

The IP Protocol

```
traceroute tuwien.at
    traceroute to tuwien.at (128.130.35.76), 64 hops max, 40 byte packets
    1  winnetou-794.kom.tuwien.ac.at (128.130.224.1) 4.512 ms 3.962 ms 4.001 ms
    2  sw-warp-2.kom.tuwien.ac.at (128.131.5.129) 4.248 ms 4.360 ms *
    3  sw-dc-1.kom.tuwien.ac.at (192.35.243.86) 9.417 ms 4.345 ms 4.397 ms
    4  info.zserv.tuwien.ac.at (128.130.35.76) 4.537 ms !X 4.660 ms !X 4.239 ms !X
```

Name Resolution

The DNS Protocol

- **What is DNS?**
  - Translates human-readable domain names (e.g., `example.com`) into IP addresses (e.g., `93.184.216.34`).
  - Acts like the internet's phonebook.
- **How DNS Works**:
  - User types a domain name into their browser.
  - DNS server finds the corresponding IP address.
  - The browser uses the IP address to communicate with the server.
- **DNS Structure**:
  - Hierarchical with **root servers**, **TLD (Top-Level Domain) servers**, and **authoritative servers**.
  - Examples of TLDs: `.com`, `.org`, `.edu`.

Name Resolution

The DNS Protocol

- **What is DNS?**
  - Translates human-readable domain names (e.g., `example.com`) into IP addresses (e.g., `93.184.216.34`).
  - Acts like the internet's phonebook.
- **How DNS Works**:
  - User types a domain name into their browser.
  - DNS server finds the corresponding IP address.
  - The browser uses the IP address to communicate with the server.
- **DNS Structure**:
  - Hierarchical with **root servers**, **TLD (Top-Level Domain) servers**, and **authoritative servers**.
  - Examples of TLDs: `.com`, `.org`, `.edu`.

Name Resolution

The DNS Protocol

- **What is DNS?**
  - Translates human-readable domain names (e.g., `example.com`) into IP addresses (e.g., `93.184.216.34`).
  - Acts like the internet's phonebook.
- **How DNS Works**:
  - User types a domain name into their browser.
  - DNS server finds the corresponding IP address.
  - The browser uses the IP address to communicate with the server.
- **DNS Structure**:
  - Hierarchical with **root servers**, **TLD (Top-Level Domain) servers**, and **authoritative servers**.
  - Examples of TLDs: `.com`, `.org`, `.edu`.

Name Resolution

The DNS Protocol

- **What is DNS?**
  - Translates human-readable domain names (e.g., `example.com`) into IP addresses (e.g., `93.184.216.34`).
  - Acts like the internet's phonebook.
- **How DNS Works**:
  - User types a domain name into their browser.
  - DNS server finds the corresponding IP address.
  - The browser uses the IP address to communicate with the server.
- **DNS Structure**:
  - Hierarchical with **root servers**, **TLD (Top-Level Domain) servers**, and **authoritative servers**.
  - Examples of TLDs: `.com`, `.org`, `.edu`.

Name Resolution

The DNS Protocol

- **What is DNS?**
  - Translates human-readable domain names (e.g., `example.com`) into IP addresses (e.g., `93.184.216.34`).
  - Acts like the internet's phonebook.
- **How DNS Works:**
  - User types a domain name into their browser.
  - DNS server finds the corresponding IP address.
  - The browser uses the IP address to communicate with the server.
- **DNS Structure**:
  - Hierarchical with **root servers**, **TLD (Top-Level Domain) servers**, and **authoritative servers**.
  - Examples of TLDs: `.com`, `.org`, `.edu`.

Name Resolution

The DNS Protocol

- **What is DNS?**
  - Translates human-readable domain names (e.g., `example.com`) into IP addresses (e.g., `93.184.216.34`).
  - Acts like the internet's phonebook.
- **How DNS Works**:
  - User types a domain name into their browser.
  - DNS server finds the corresponding IP address.
  - The browser uses the IP address to communicate with the server.
- **DNS Structure**:
  - Hierarchical with **root servers**, **TLD (Top-Level Domain) servers**, and **authoritative servers**.
  - Examples of TLDs: `.com`, `.org`, `.edu`.

Name Resolution

The DNS Protocol

- **What is DNS?**
  - Translates human-readable domain names (e.g., `example.com`) into IP addresses (e.g., `93.184.216.34`).
  - Acts like the internet's phonebook.
- **How DNS Works**:
  - User types a domain name into their browser.
  - DNS server finds the corresponding IP address.
  - The browser uses the IP address to communicate with the server.
- **DNS Structure**:
  - Hierarchical with **root servers**, **TLD (Top-Level Domain) servers**, and **authoritative servers**.
  - Examples of TLDs: `.com`, `.org`, `.edu`.

Name Resolution

The DNS Protocol

- **What is DNS?**
  - Translates human-readable domain names (e.g., `example.com`) into IP addresses (e.g., `93.184.216.34`).
  - Acts like the internet's phonebook.
- **How DNS Works**:
  - User types a domain name into their browser.
  - DNS server finds the corresponding IP address.
  - The browser uses the IP address to communicate with the server.
- **DNS Structure**:
  - Hierarchical with **root servers**, **TLD (Top-Level Domain) servers**, and **authoritative servers**.
  - Examples of TLDs: `.com`, `.org`, `.edu`.

Name Resolution

The DNS Protocol

- **What is DNS?**
  - Translates human-readable domain names (e.g., `example.com`) into IP addresses (e.g., `93.184.216.34`).
  - Acts like the internet's phonebook.
- **How DNS Works**:
  - User types a domain name into their browser.
  - DNS server finds the corresponding IP address.
  - The browser uses the IP address to communicate with the server.
- **DNS Structure**:
  - Hierarchical with **root servers**, **TLD (Top-Level Domain) servers**, and **authoritative servers**.
  - Examples of TLDs: `.com`, `.org`, `.edu`.

Name Resolution

The DNS Protocol

- **What is DNS?**
  - Translates human-readable domain names (e.g., `example.com`) into IP addresses (e.g., `93.184.216.34`).
  - Acts like the internet's phonebook.
- **How DNS Works**:
  - User types a domain name into their browser.
  - DNS server finds the corresponding IP address.
  - The browser uses the IP address to communicate with the server.
- **DNS Structure**:
  - Hierarchical with **root servers**, **TLD (Top-Level Domain) servers**, and **authoritative servers**.
  - Examples of TLDs: `.com`, `.org`, `.edu`. af

Name Resolution (1)

The DNS Protocol

```
host tuwien.at
    tuwien.at has address 128.130.35.76
    tuwien.at mail is handled by 20 mri2.tuwien.ac.at.
    tuwien.at mail is handled by 10 mri3.tuwien.ac.at.
    tuwien.at mail is handled by 20 mri1.tuwien.ac.at.
```

Internet Browsing

The HTTP Protocol

- **What is HTTP?**
  - Stands for **HyperText Transfer Protocol**.
  - Protocol for transferring data between a web server and a web client (browser).
  - Operates over TCP/IP.
- **How HTTP Works**:
  - Client sends an **HTTP request** to a server (e.g., GET, POST).
  - Server responds with an **HTTP response**, including status code and content.
- **Common HTTP Methods**:
  - **GET**: Request data from a server.
  - **POST**: Send data to a server.
  - **PUT**, **DELETE**: Update or delete resources.

Internet Browsing

The HTTP Protocol

- **What is HTTP?**
  - Stands for **HyperText Transfer Protocol**.
  - Protocol for transferring data between a web server and a web client (browser).
  - Operates over TCP/IP.
- **How HTTP Works**:
  - Client sends an **HTTP request** to a server (e.g., GET, POST).
  - Server responds with an **HTTP response**, including status code and content.
- **Common HTTP Methods**:
  - **GET**: Request data from a server.
  - **POST**: Send data to a server.
  - **PUT**, **DELETE**: Update or delete resources.

Internet Browsing

The HTTP Protocol

- **What is HTTP?**
  - Stands for **HyperText Transfer Protocol**.
  - Protocol for transferring data between a web server and a web client (browser).
  - Operates over TCP/IP.
- **How HTTP Works**:
  - Client sends an **HTTP request** to a server (e.g., GET, POST).
  - Server responds with an **HTTP response**, including status code and content.
- **Common HTTP Methods**:
  - **GET**: Request data from a server.
  - **POST**: Send data to a server.
  - **PUT**, **DELETE**: Update or delete resources.

Internet Browsing

The HTTP Protocol

- **What is HTTP?**
  - Stands for **HyperText Transfer Protocol**.
  - Protocol for transferring data between a web server and a web client (browser).
  - Operates over TCP/IP.
- **How HTTP Works**:
  - Client sends an **HTTP request** to a server (e.g., GET, POST).
  - Server responds with an **HTTP response**, including status code and content.
- **Common HTTP Methods**:
  - **GET**: Request data from a server.
  - **POST**: Send data to a server.
  - **PUT**, **DELETE**: Update or delete resources.

Internet Browsing

The HTTP Protocol

- **What is HTTP?**
  - Stands for **HyperText Transfer Protocol**.
  - Protocol for transferring data between a web server and a web client (browser).
  - Operates over TCP/IP.
- **How HTTP Works**:
  - Client sends an **HTTP request** to a server (e.g., GET, POST).
  - Server responds with an **HTTP response**, including status code and content.
- **Common HTTP Methods**:
  - **GET**: Request data from a server.
  - **POST**: Send data to a server.
  - **PUT**, **DELETE**: Update or delete resources.

Internet Browsing

The HTTP Protocol

- **What is HTTP?**
  - Stands for **HyperText Transfer Protocol**.
  - Protocol for transferring data between a web server and a web client (browser).
  - Operates over TCP/IP.
- **How HTTP Works**:
  - Client sends an **HTTP request** to a server (e.g., GET, POST).
  - Server responds with an **HTTP response**, including status code and content.
- **Common HTTP Methods**:
  - **GET**: Request data from a server.
  - **POST**: Send data to a server.
  - **PUT**, **DELETE**: Update or delete resources.

Internet Browsing

The HTTP Protocol

- **What is HTTP?**
  - Stands for **HyperText Transfer Protocol**.
  - Protocol for transferring data between a web server and a web client (browser).
  - Operates over TCP/IP.
- **How HTTP Works**:
  - Client sends an **HTTP request** to a server (e.g., GET, POST).
  - Server responds with an **HTTP response**, including status code and content.
- **Common HTTP Methods**:
  - **GET**: Request data from a server.
  - **POST**: Send data to a server.
  - **PUT**, **DELETE**: Update or delete resources.

Internet Browsing

The HTTP Protocol

- **What is HTTP?**
  - Stands for **HyperText Transfer Protocol**.
  - Protocol for transferring data between a web server and a web client (browser).
  - Operates over TCP/IP.
- **How HTTP Works**:
  - Client sends an **HTTP request** to a server (e.g., GET, POST).
  - Server responds with an **HTTP response**, including status code and content.
- **Common HTTP Methods**:
  - **GET**: Request data from a server.
  - **POST**: Send data to a server.
  - **PUT**, **DELETE**: Update or delete resources.

Internet Browsing

The HTTP Protocol

- **What is HTTP?**
  - Stands for **HyperText Transfer Protocol**.
  - Protocol for transferring data between a web server and a web client (browser).
  - Operates over TCP/IP.
- **How HTTP Works**:
  - Client sends an **HTTP request** to a server (e.g., GET, POST).
  - Server responds with an **HTTP response**, including status code and content.
- **Common HTTP Methods**:
  - **GET**: Request data from a server.
  - **POST**: Send data to a server.
  - **PUT**, **DELETE**: Update or delete resources.

Internet Browsing

The HTTP Protocol

- **What is HTTP?**
  - Stands for **HyperText Transfer Protocol**.
  - Protocol for transferring data between a web server and a web client (browser).
  - Operates over TCP/IP.
- **How HTTP Works**:
  - Client sends an **HTTP request** to a server (e.g., GET, POST).
  - Server responds with an **HTTP response**, including status code and content.
- **Common HTTP Methods**:
  - **GET**: Request data from a server.
  - **POST**: Send data to a server.
  - **PUT**, **DELETE**: Update or delete resources.

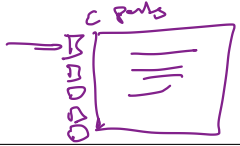
Internet Browsing

The HTTP Protocol

- **What is HTTP?**
  - Stands for **HyperText Transfer Protocol**.
  - Protocol for transferring data between a web server and a web client (browser).
  - Operates over TCP/IP.
- **How HTTP Works**:
  - Client sends an **HTTP request** to a server (e.g., GET, POST).
  - Server responds with an **HTTP response**, including status code and content.
- **Common HTTP Methods**:
  - **GET**: Request data from a server.
  - **POST**: Send data to a server.
  - **PUT**, **DELETE**: Update or delete resources.

Internet Browsing (1)

The HTTP Protocol (2)



```
curl -v tuwien.at
    * Host tuwien.at:80 was resolved.
    * IPv6: (none)
    * IPv4: 128.130.35.76
    *   Trying 128.130.35.76:80...
    * Connected to tuwien.at (128.130.35.76) port 80
    > GET / HTTP/1.1
    > Host: tuwien.at
    > User-Agent: curl/8.7.1
    > Accept: */*
```

Internet Browsing (2)

The HTTP Protocol (2)

```
15      >
16      * Request completely sent off
17      < HTTP/1.1 301 Moved Permanently
18      < content-length: 0
19      < location: https://tuwien.at/
20      <
21      * Connection #0 to host tuwien.at left intact
```

- HTTP connections are **unencrypted**, making data visible to intermediaries.

Email Communication

The SMTP, IMAP, and POP3 Protocols

- **What is SMTP, IMAP, and POP3?**
  - **SMTP** (Simple Mail Transfer Protocol): Used to send emails from a client to a mail server.
  - **IMAP** (Internet Message Access Protocol): Allows clients to retrieve messages and manage mail directly on the server.
  - **POP3** (Post Office Protocol 3): Downloads emails from a server to a client, typically removing them from the server.
- **How Email Transmission Works**:
  - Client sends an **SMTP request** to the server to send an email.
  - **IMAP** or **POP3** is used by the client to retrieve incoming emails.
  - SMTP servers communicate with each other to deliver emails to the recipient's mail server.

Email Communication

The SMTP, IMAP, and POP3 Protocols

- **What is SMTP, IMAP, and POP3?**
  - **SMTP** (Simple Mail Transfer Protocol): Used to send emails from a client to a mail server.
  - **IMAP** (Internet Message Access Protocol): Allows clients to retrieve messages and manage mail directly on the server.
  - **POP3** (Post Office Protocol 3): Downloads emails from a server to a client, typically removing them from the server.
- **How Email Transmission Works**:
  - Client sends an **SMTP request** to the server to send an email.
  - **IMAP** or **POP3** is used by the client to retrieve incoming emails.
  - SMTP servers communicate with each other to deliver emails to the recipient's mail server.

Email Communication

The SMTP, IMAP, and POP3 Protocols

- **What is SMTP, IMAP, and POP3?**
  - **SMTP** (Simple Mail Transfer Protocol): Used to send emails from a client to a mail server.
  - **IMAP** (Internet Message Access Protocol): Allows clients to retrieve messages and manage mail directly on the server.
  - **POP3** (Post Office Protocol 3): Downloads emails from a server to a client, typically removing them from the server.
- **How Email Transmission Works**:
  - Client sends an **SMTP request** to the server to send an email.
  - **IMAP** or **POP3** is used by the client to retrieve incoming emails.
  - SMTP servers communicate with each other to deliver emails to the recipient's mail server.

Email Communication

The SMTP, IMAP, and POP3 Protocols

- **What is SMTP, IMAP, and POP3?**
  - **SMTP** (Simple Mail Transfer Protocol): Used to send emails from a client to a mail server.
  - **IMAP** (Internet Message Access Protocol): Allows clients to retrieve messages and manage mail directly on the server.
  - **POP3** (Post Office Protocol 3): Downloads emails from a server to a client, typically removing them from the server.
- **How Email Transmission Works**:
  - Client sends an **SMTP request** to the server to send an email.
  - **IMAP** or **POP3** is used by the client to retrieve incoming emails.
  - SMTP servers communicate with each other to deliver emails to the recipient's mail server.

Email Communication

The SMTP, IMAP, and POP3 Protocols

- **What is SMTP, IMAP, and POP3?**
  - **SMTP** (Simple Mail Transfer Protocol): Used to send emails from a client to a mail server.
  - **IMAP** (Internet Message Access Protocol): Allows clients to retrieve messages and manage mail directly on the server.
  - **POP3** (Post Office Protocol 3): Downloads emails from a server to a client, typically removing them from the server.
- **How Email Transmission Works**:
  - Client sends an **SMTP request** to the server to send an email.
  - **IMAP** or **POP3** is used by the client to retrieve incoming emails.
  - SMTP servers communicate with each other to deliver emails to the recipient's mail server.

Email Communication

The SMTP, IMAP, and POP3 Protocols

- **What is SMTP, IMAP, and POP3?**
  - **SMTP** (Simple Mail Transfer Protocol): Used to send emails from a client to a mail server.
  - **IMAP** (Internet Message Access Protocol): Allows clients to retrieve messages and manage mail directly on the server.
  - **POP3** (Post Office Protocol 3): Downloads emails from a server to a client, typically removing them from the server.
- **How Email Transmission Works**:
  - Client sends an **SMTP request** to the server to send an email.
  - **IMAP** or **POP3** is used by the client to retrieve incoming emails.
  - SMTP servers communicate with each other to deliver emails to the recipient's mail server.

Email Communication

The SMTP, IMAP, and POP3 Protocols

- **What is SMTP, IMAP, and POP3?**
  - **SMTP** (Simple Mail Transfer Protocol): Used to send emails from a client to a mail server.
  - **IMAP** (Internet Message Access Protocol): Allows clients to retrieve messages and manage mail directly on the server.
  - **POP3** (Post Office Protocol 3): Downloads emails from a server to a client, typically removing them from the server.
- **How Email Transmission Works**:
  - Client sends an **SMTP request** to the server to send an email.
  - **IMAP** or **POP3** is used by the client to retrieve incoming emails.
  - SMTP servers communicate with each other to deliver emails to the recipient's mail server.

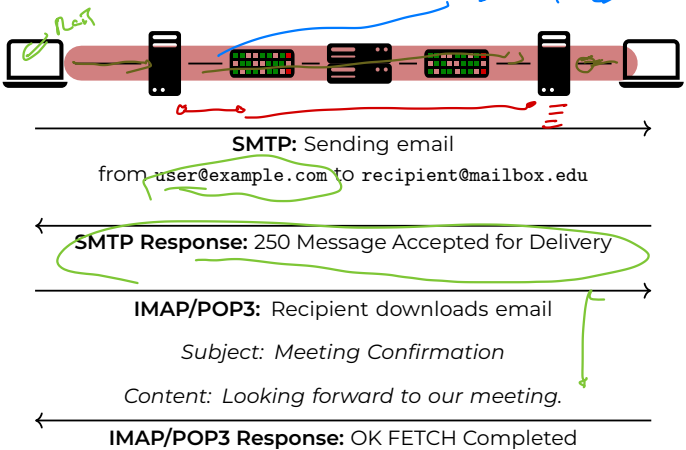
Email Communication

The SMTP, IMAP, and POP3 Protocols

- **What is SMTP, IMAP, and POP3?**
  - **SMTP** (Simple Mail Transfer Protocol): Used to send emails from a client to a mail server.
  - **IMAP** (Internet Message Access Protocol): Allows clients to retrieve messages and manage mail directly on the server.
  - **POP3** (Post Office Protocol 3): Downloads emails from a server to a client, typically removing them from the server.
- **How Email Transmission Works**:
  - Client sends an **SMTP request** to the server to send an email.
  - **IMAP** or **POP3** is used by the client to retrieve incoming emails.
  - SMTP servers communicate with each other to deliver emails to the recipient's mail server.

Email Communication (1)

The SMTP, IMAP, and POP3 Protocols



SMTP Server
Routes email from sender to recipient's domain

ISP
Transfers data between SMTP servers

Email Client
Retrieves emails using IMAP or POP3

Email Communication (2)

The SMTP, IMAP, and POP3 Protocols

```
telnet mail.example.com 25
    Trying 203.0.113.2...
    Connected to mail.example.com.
    Escape character is '^]'.
    220 mail.example.com ESMTP Postfix
    HELO mydomain.com
    250 mail.example.com Hello mydomain.com
    MAIL FROM:<user@mydomain.com>
    250 2.1.0 Ok
    RCPT TO:<recipient@example.com>
    250 2.1.5 Ok
    DATA
    354 End data with <CR><LF>.<CR><LF>
    Subject: Test Email
```

Email Communication (3)

The SMTP, IMAP, and POP3 Protocols

```
15      This is a test message.
16      .
17      250 2.0.0 Ok: queued as 12345
```

- **Encryption**: Use **TLS/SSL** for secure transmission over SMTP, IMAP, and POP3 to protect data.

Warning

TLS/SSL does not encrypt the content of the message. The email servers can still access the data.

Internet vs. Web

- **Internet:** Global network of connected computers; supports data exchange (e.g., email, online games).
- **Web:** A service using the internet; accesses websites through HTTP/HTTPS (e.g., Wikipedia, social media).

Difference: The internet is the infrastructure; the web is a service on top of it.

Internet vs. Web

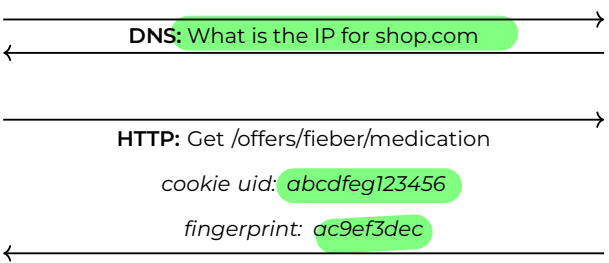
- **Internet:** Global network of connected computers; supports data exchange (e.g., email, online games).
- **Web:** A service using the internet; accesses websites through HTTP/HTTPS (e.g., Wikipedia, social media).

Difference: The internet is the infrastructure; the web is a service on top of it.

Privacy in the Web

Privacy in the Web

Overview



ISP

Domains visited (+ site content) by specific customer

Website

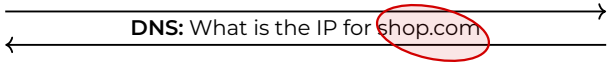
Site content visited by specific user

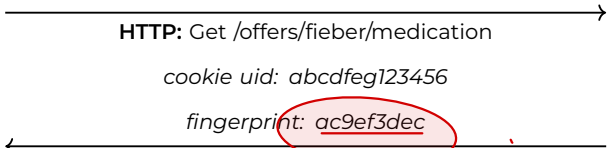
Ad networks, Social Media, ...

Content on different Websites visited by specific User

Privacy in the Web

Overview





Note

We will talk about fingerprinting next week.

ISP

Domains visited (+ site content) by specific customer

Website

Site content visited by specific user

Ad networks, Social Media, ...

Content on different Websites visited by specific User

DNS Tracking (1)

- **DNS is a plaintext protocol (UDP port 53)**
  - Requests are visible within the same WiFi, to ISP, and in transit.
  - **DNS hijacking:** 
    censorship, injecting advertising, attacks.
- **Monitoring independent of DNS provider with:**
  - Deep-packet inspection for Public DNS (e.g., 8.8.8.8), recursive DNS resolver.

DNS Tracking (2)

Filter: dns and ip.addr == 10.190.38.85 Expression... Clear Apply Save Only-BA Only-Data

No.	Time	Source	Destination	Length	Info
451	1.113258	10.190.38.85	10.190.12.27		Standard query 0x91a0 A abs.twimg.com
492	1.175555	10.190.12.27	10.190.38.85		Standard query response 0x91a0 CNAME cs472.wac.edgecastcdn.net A 192.229.237.25
563	1.321328	10.190.38.85	10.190.12.27		Standard query 0x2f65 A o.twimg.com
614	1.391930	10.190.12.27	10.190.38.85		Standard query response 0x2f65 CNAME wildcard.twimg.com.tw.map.fastly.net A 199.96.57.7
6441	38.518478	10.190.38.85	192.168.19.1		Standard query 0x7932 A twitter.com
6470	39.518215	10.190.38.85	192.168.19.1		Standard query 0x7932 A twitter.com
6487	40.521448	10.190.38.85	192.168.19.1		Standard query 0x7932 A twitter.com
6516	42.521437	10.190.38.85	192.168.19.1		Standard query 0x7932 A twitter.com
6555	44.517697	10.190.38.85	192.168.19.1		Standard query 0xc69b A twitter.com
6575	45.517245	10.190.38.85	192.168.19.1		Standard query 0xc69b A twitter.com
6596	46.517220	10.190.38.85	192.168.19.1		Standard query 0xc69b A twitter.com
6597	46.521307	10.190.38.85	192.168.19.1		Standard query 0x7932 A twitter.com
6640	48.517546	10.190.38.85	192.168.19.1		Standard query 0xc69b A twitter.com
6706	51.708351	10.190.38.85	192.168.19.1		Standard query 0x1301 A dns.msftncsi.com
6727	52.517390	10.190.38.85	192.168.19.1		Standard query 0xc69b A twitter.com
6730	52.708537	10.190.38.85	192.168.19.1		Standard query 0x1301 A dns.msftncsi.com
6754	53.708553	10.190.38.85	192.168.19.1		Standard query 0x1301 A dns.msftncsi.com

Encrypted DNS

- **Popular standards to encrypt DNS**
  - DNS over TLS (DoT) from 2016
  - DNS Queries over HTTPS (DoH) from 2018
- **DoT:** DNS wrapped with TLS (new port `tcp/853`)
  - Potential issue: blocking / detection
  - Supported by Android $\geq$ 9 (“Private DNS”), iOS $\geq$ 14, Windows 10, systemd
- **DoH:** HTTPS for transporting DNS queries
  - HTTPS is commonly used for web services / browser APIs
  - Supported by major web browsers and mobile apps

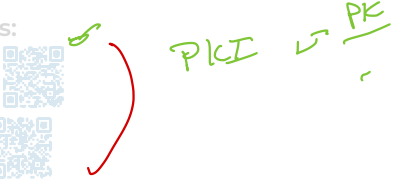
Encrypted DNS (2)

Remaining Problems:

- Recursive DNS resolver
- Malicious DNS provider

Our Recommendations:

- appliedprivacy.net
- usableprivacy.com



Encrypted DNS (2)

Remaining Problems:

- Recursive DNS resolver
- Malicious DNS provider

Our Recommendations:

- `appliedprivacy.net`
- `usableprivacy.com`

Network HTTP(S) Leaks

- **Unencrypted HTTP:**
  - Website(s) requested: `http://shop.com/offers/fieber/medication`
  - Entire page content, including authentication tokens, etc.
  - Straightforward to monitor with transparent HTTP proxies.
- **HTTPS (covered in detail in the TLS lecture):**
  - Hostname leaks in initial TLS handshake.
  - Deep packet inspection can be used to monitor/censor HTTPS.
  - Example: `https://shop.com/offers/fieber/medication`

Network HTTP(S) Leaks

- **Unencrypted HTTP:**
  - Website(s) requested: `http://shop.com/offers/fieber/medication`
  - Entire page content, including authentication tokens, etc.
  - Straightforward to monitor with transparent HTTP proxies.
- **HTTPS (covered in detail in the TLS lecture):**
  - Hostname leaks in initial TLS handshake.
  - Deep packet inspection can be used to monitor/censor HTTPS.
  - Example: `https://shop.com/offers/fieber/medication`

Network HTTP(S) Leaks

- **Unencrypted HTTP:**
  - Website(s) requested: `http://shop.com/offers/fieber/medication`
  - Entire page content, including authentication tokens, etc.
  - Straightforward to monitor with transparent HTTP proxies.
- **HTTPS (covered in detail in the TLS lecture):**
  - Hostname leaks in initial TLS handshake.
  - Deep packet inspection can be used to monitor/censor HTTPS.
  - Example: `https://shop.com/offers/fieber/medication`

Network HTTP(S) Leaks

- **Unencrypted HTTP:**
  - Website(s) requested: `http://shop.com/offers/fieber/medication`
  - Entire page content, including authentication tokens, etc.
  - Straightforward to monitor with transparent HTTP proxies.
- **HTTPS (covered in detail in the TLS lecture):**
  - Hostname leaks in initial TLS handshake.
  - Deep packet inspection can be used to monitor/censor HTTPS.
  - Example: `https://shop.com/offers/fieber/medication`

Network HTTP(S) Leaks

- **Unencrypted HTTP:**
  - Website(s) requested: `http://shop.com/offers/fieber/medication`
  - Entire page content, including authentication tokens, etc.
  - Straightforward to monitor with transparent HTTP proxies.
- **HTTPS (covered in detail in the TLS lecture):**
  - Hostname leaks in initial TLS handshake.
  - Deep packet inspection can be used to monitor/censor HTTPS.
  - Example: `https://shop.com/offers/fieber/medication`

Network HTTP(S) Leaks

- **Unencrypted HTTP:**
  - Website(s) requested: `http://shop.com/offers/fieber/medication`
  - Entire page content, including authentication tokens, etc.
  - Straightforward to monitor with transparent HTTP proxies.
- **HTTPS (covered in detail in the TLS lecture):**
  - Hostname leaks in initial TLS handshake.
  - Deep packet inspection can be used to monitor/censor HTTPS.
  - Example: `https://shop.com/offers/fieber/medication`

Network HTTP(S) Leaks

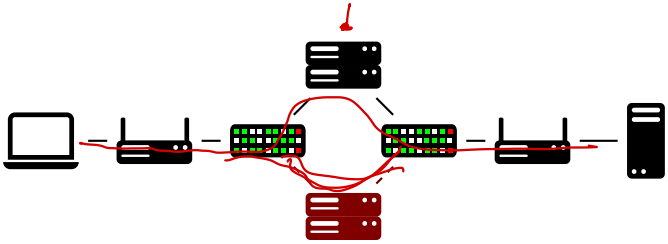
- **Unencrypted HTTP:**
  - Website(s) requested: `http://shop.com/offers/fieber/medication`
  - Entire page content, including authentication tokens, etc.
  - Straightforward to monitor with transparent HTTP proxies.
- **HTTPS (covered in detail in the TLS lecture):**
  - Hostname leaks in initial TLS handshake.
  - Deep packet inspection can be used to monitor/censor HTTPS.
  - Example: `https://shop.com/offers/fieber/medication`

Network HTTP(S) Leaks

- **Unencrypted HTTP:**
  - Website(s) requested: `http://shop.com/offers/fieber/medication`
  - Entire page content, including authentication tokens, etc.
  - Straightforward to monitor with transparent HTTP proxies.
- **HTTPS (covered in detail in the TLS lecture):**
  - Hostname leaks in initial TLS handshake.
  - Deep packet inspection can be used to monitor/censor HTTPS.
  - Example: `https://shop.com/offers/fieber/medication`

Network HTTP(S) Leaks (1)

Rerouting Attacks



Rerouting Attacks:

- The internet's decentralized architecture enables data to take multiple paths.
- BGP (Border Gateway Protocol) allows ISPs to dynamically choose the best path.
- Even HTTPS traffic exposes metadata, like destination servers and data volume.

Network HTTP(S) Leaks (2)

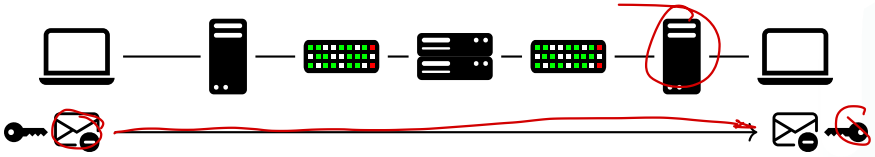
Rerouting Attacks

Example of a Rerouting Attacks:

- **China Reroute Attack (2010):** A Chinese ISP used BGP hijacking to reroute global internet traffic, including U.S. government data, through China, exposing sensitive information.
- **Amazon Route 53 Hijack (2018):** Attackers used BGP hijacking to redirect Amazon Route 53 traffic, stealing cryptocurrency from an Ethereum wallet.
- **Google Traffic Hijack (2018):** A BGP leak rerouted Google traffic through China and Russia, disrupting access and raising security concerns.

Encrypted Emails (1)

Why Encryption Matters and Usability Challenges



Why is Email Encryption Important?

- **Confidentiality:** Protects the content of emails from being read by unauthorized parties during transmission.
- **Integrity:** Ensures that the email content is not altered during transit.
- **Authentication:** Verifies the identity of the sender, preventing email spoofing.

Encrypted Emails (2)

Why Encryption Matters and Usability Challenges

Examples of Email Encryption Standards:

- **PGP/GPG (Pretty Good Privacy):** Uses public-key cryptography for encrypting and signing emails.
- **S/MIME (Secure/Multipurpose Internet Mail Extensions):** Uses digital certificates for encryption and signing.

Encrypted Emails (3)

Why Encryption Matters and Usability Challenges

Why Poor Usability?

- **Complex Setup:** Requires users to generate, share, and manage encryption keys or certificates.
- **Compatibility Issues:** Not all email clients support encryption standards like PGP or S/MIME natively.
- **Key Management:** Losing private keys means losing access to encrypted emails, while sharing keys securely can be difficult.
- **User Awareness:** Users may lack knowledge about how encryption works, leading to improper use or bypassing security measures.

Privacy Enhancing Technologies

What are Privacy Enhancing Technologies?

A Definition

Definition (PETS; van Blarkom, Borking & Olk 2003)

Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system."

What are Privacy Enhancing Technologies?

Goals & Examples

- **Definition (short):** Tools and methods designed to protect user privacy and minimize data exposure.
- **Goals:**
  - Ensure confidentiality and anonymity of user data.
  - Protect against tracking and profiling.
  - Enable secure communication.
- **Examples:**
  - End-to-end encryption (e.g., TLS).
  - Secure DNS solutions (e.g., DNS over HTTPS).
  - Private Communication (e.g., Signal).
  - Anonymization networks (e.g., Tor).

Note

We cover TLS, Signal, and Tor in subsequent lectures.

What are Privacy Enhancing Technologies?

Goals & Examples

- **Definition (short):** Tools and methods designed to protect user privacy and minimize data exposure.
- **Goals:**
  - Ensure confidentiality and anonymity of user data.
  - Protect against tracking and profiling.
  - Enable secure communication.
- **Examples:**
  - End-to-end encryption (e.g., TLS).
  - Secure DNS solutions (e.g., DNS over HTTPS).
  - Private Communication (e.g., Signal).
  - Anonymization networks (e.g., Tor).

Note

We cover TLS, Signal, and Tor in subsequent lectures.

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=2440289

PRIVACY
ENHANCING
TECHNOLOGIES