Privacy and Censorship

CS 166: Introduction to Computer Security
Privacy online?

Source: www.pinterest.com%2Fpin%2F393994667380474128%2F&psig=AOvVaw0jS7Y6JZKVSxyEaJfXk2_F&ust=1523630943607084

4/16/18 Anonymous & Censorship
Online Privacy

• Eavesdropping on the Internet
  – Sender's organization or ISP
  – Recipient's organization or ISP
  – Intermediate routers
  – Governments

• Encryption
  – E.g., TLS
  – Protects the data transmitted
  – Does not hide sender and recipient IP addresses
Privacy Importance

• "You have nothing to fear, if you have nothing to hide" attributed to:
  – George Orwell in "1984" book
  – Joseph Goebbels - Minister of Propaganda in Nazi Germany

• "Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance."
  – Bruce Schneier

• Main privacy threats?
  – User Tracking
  – Personal privacy
  – Device Fingerprinting
User Tracking

Technology

- Cookies
  - Http (third party e.g. Google Analytic Doubleclick, etc.)
  - Supercookies (flash)
  - Evercookies (javascript)

Analysis/Protection Tools

- Browser addons focused on cookies management
  - Ghostery
  - lightbeam
  - UBlock
1. **First Party**

   - **Cookie 1:**
     - Amazon
     - Desktop
     - Chrome

2. **Third Party**

   - **Cookie 2:**
     - Weather.com
     - Desktop
     - Chrome
   - **Cookie 3:**
     - Amazon
     - Desktop
     - Chrome
Pageviews
5,606
% of Total 100.00% (5,606)

Pageviews by Age
<table>
<thead>
<tr>
<th>Age</th>
<th>Pageviews</th>
</tr>
</thead>
<tbody>
<tr>
<td>25-34</td>
<td>1,854</td>
</tr>
<tr>
<td>18-24</td>
<td>793</td>
</tr>
<tr>
<td>35-44</td>
<td>744</td>
</tr>
<tr>
<td>45-54</td>
<td>318</td>
</tr>
<tr>
<td>55-64</td>
<td>122</td>
</tr>
<tr>
<td>65+</td>
<td>68</td>
</tr>
</tbody>
</table>

Pageviews by Gender
<table>
<thead>
<tr>
<th>Gender</th>
<th>Pageviews</th>
</tr>
</thead>
<tbody>
<tr>
<td>male</td>
<td>2,033</td>
</tr>
<tr>
<td>female</td>
<td>1,883</td>
</tr>
</tbody>
</table>

Google Analytics

Pageviews by Age and Gender

Pageviews by Age

Pageviews by Gender

Pageviews by Location

Map of pageviews globally.
### Personal Privacy

#### Technology
- Social network (photographs)
- GPS (maps)
- Search engine (google vs. duckduckgo.com)

#### Analysis/Protection Tools
- Facebook stored data
- Google maps stored places
- Search Engine differences
- Protections?

"I want to make and receive mobile calls; in exchange, I allow this company to know where I am at all times.”

Bruce Schneier - Data and Goliath
Device Fingerprinting

Technology
- User agent
- Fonts installed
- Plugins (versions)
- Canvas size

Analysis/Protection Tools
- panopticlick.eff.org
  - Electronic Frontier Foundations
- Tails
Tails

• Privacy for anyone anywhere
• Linux live distro focused on Privacy
• Use the Internet anonymously and circumvent censorship
  – Tor network
• Leave no trace
  – No persistent data on the computer you are using unless you ask it explicitly
• Use state-of-the-art cryptographic tools
  – E.g. Https everywhere addons
The Onion Router
Overview

- First the US Naval Research Laboratory, then the EFF and now the Tor Project (www.torproject.org)
- Access normal Internet sites anonymously, and Tor hidden services.
- Locally run SOCKS proxy that connects to the Tor network.
- “Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis.” On TOR project web site
Anonymity

• Preventing identification within a group
  – E.g., departmental VPN, home NAT router
  – Group should be as large as possible

• Preventing association of action and identity
  – E.g., distributed denial of service by hidden attacker
Mix

• Trusted router, Rose
• Public-key encryption
• Message from Alice to Bob via Rose
  \[ E_{KR}(Bob, E_{KB}(M)) \]
• Precautions
  – Fixed message size
  – Continuous communication
  – Dummy messages
  – Chain of mixes
Step 1: Alice’s Tor client obtains a list of Tor nodes from a directory server.
Onion Routing

- Group of routers
- Message sent via random sequence of routers
- Layered encryption
  - Build onion inside out
- Routing
  - Peel onion outside in
- Each router knows previous and next
How Tor Works: 2

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Onion Routing in Practice

- Do not encrypt final hop
  - Encryption may be done by application (e.g., https)

- Source sets up
  - Random circuit (route)
  - Symmetric keys shared with routers

- Data tunneled to final router over circuit
How Tor Works: 3

Step 3: If the user wants access to another site, Alice’s Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
TOR Analysis

Advantages
• Tunnel, through a SOCKS proxy, allows to work any protocol.
• Three nodes of proxying, each node not knowing the one before last, makes very difficult to find the source.

Problems
• Slow (high latency)
• exit node?
• Semi-fixed Infrastructure: Sept 25th 2009, Great Firewall of China blocks 80% of Tor relays listed in the Directory. Bridged node.
  https://blog.torproject.org/blog/tor-partially-blocked-china
  http://yro.slashdot.org/story/09/10/15/1910229/China-Strangles-Tor-Ahead-of-National-Day
• Fairly easy to tell someone is using it from the server side
Identify TOR traffic

(default configuration)

- Local
  9050/tcp Tor SOCKS proxy
  9051/tcp Tor control port
  8118/tcp Privoxy

- Remote
  443/tcp and 80/tcp mostly
  Servers may also listen on port 9001/tcp, and directory information on 9030.
Applications/Sites

• Hidden services
  Normally websites, but can be just about any TCP connection

• Tor Hidden Service Example (Hiddenwiki) :
  http://zqktlwi4fecvo6ri.onion

• .onion TLD:
  – non-mnemonic,
  – 16-character alpha-semi-numeric hashes
  – automatically generated based on a public key when a hidden service is configured
  – "vanity address" possible with expensive computation
How To Block Tor?

• Attackers can block users from connecting to the Tor network
  – By blocking the directory authorities
  – By blocking all the relay IP addresses in the directory
  – By filtering based on Tor's network fingerprint
  – By preventing users from finding the Tor software
Bridge relays

• Rather than signing up as a normal relay, you can sign up as a special “bridge” relay that is not listed in any directory.

• No need to be an “exit” (so no abuse worries), and you can rate limit if needed

• Integrated into Vidalia (our GUI)

• https://bridges.torproject.org/ will tell you a few based on time and your IP address

• Mail bridges@torproject.org from a gmail address and we'll send you a few
Censorship

The Golden Firewall Project
Internet Censorship

- Control or suppression of the publishing or accessing of information on the Internet
- Carried out by governments or by private organizations either at the behest of government or on their own initiative
- Individuals and organizations may engage in self-censorship on their own or due to intimidation and fear.
Internet Censorship in the World
2012

- No censorship
- Some censorship
- Under surveillance
- Heavy surveillance (Internet “black holes”)
Proxy Servers

- A proxy receives requests for certain applications
  - For example, an HTTP request for a particular URL
- The proxy passes the requests on to target server
  - The target server views the proxy as the source of the request
The Great Firewall of China

- Censorship system to control internet connections to/from China
  - Development began in 1998
  - Deployed in 2003
  - More than 30K people estimated to have worked on it
- All Chinese websites need an Internet Content Provider (ICP) license
- It is difficult for an individual to obtain an ICP license
Golden Shield Project Architecture

• China seems to have just three gateways with the rest of the world:
  – Beijing in the north
  – Shanghai on the central coast
  – Guangzhou in the south, to connect Hong Kong
• The alternative Internet Satellite is slow and expensive
• A **firewall** is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system.

• A network firewall is similar to firewalls in building construction, because in both cases they are intended to **isolate** one "network" or "compartment" from another.
Inside the Golden Shield

• Censorship blocks different kinds of information:
  – News items not approved by regime
  – Open collaborative sites
  – Technical information on how to bypass firewalls
  – https connections

• Understandable information is more dangerous for political regime
  
  Ignorance is the night of the mind, but a night without moon and stars  
  (Confucius)
Filtering vs. Censoring

Your request has been blocked by ContentBarrier.

This web site has been blocked because it matches the following forbidden category: Sex/Pornography.

If you think this web site does not match this category, please submit this URL.

You can ask your parent or your administrator to unlock this web site (a password will be required).

Submit this link  Allow this web site

The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer’s network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again
Golden Shield Internals

- TCP Reset connection

```
47709 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=2265105 TSER=0 WS=7
http > 47709 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1300 TSV=782449585 TSER=2265105 WS=7
47709 > http [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=2265201 TSER=782449585
GET http://en.wikipedia.org/w/index.php?title=Special%3ASearch&search=falun&go=Go HTTP/1.1
http > 47709 [RST, ACK] Seq=1 Ack=1 Win=11520 Len=0
http > 47709 [RST, ACK] Seq=1 Ack=1 Win=11520 Len=0
http > 47709 [RST, ACK] Seq=1 Ack=1 Win=11520 Len=0
http > 47709 [RST] Seq=1 Win=3545218 Len=0
http > 47709 [ACK] Seq=1 Ack=469 Win=6912 Len=0 TSV=782449801 TSER=2265201
47709 > http [RST] Seq=469 Win=0 Len=0
http > 47709 [RST, ACK] Seq=1 Ack=469 Win=4977024 Len=0
http > 47709 [RST] Seq=1 Win=2271104 Len=0
```
How to Bypass the Firewall

• A web-proxy is usually enough to bypass the great firewall
• However, proxies may be monitored
Internet Global Market

- United States: 280m users (4.5% of world population)
- United Kingdom: 57m users (0.9%)
- France: 55m users (0.9%)
- Germany: 72m users (1.1%)
- Russia: 84m users (2%)
- China: 649m users (19%)
- India: 243m users (17%)
- Brazil: 107m users (2.8%)
- Nigeria: 67m users (2.5%)

(Source: Internet Live Stats | All data are estimated)
Detection Techniques

• **DNS blacklist**
  - DNS does not resolve domain names, or returns incorrect IP addresses i.e., www.google.com returns 'page not found'

• **IP blacklist**
  - For sites on a blacklist, the firewall prevents connection attempts

• **Keyword blacklist**
  - The firewall scans the URL string (e.g., search terms) and interrupts the connection if it contains keywords from a blacklist