Anonymity

IP address
- When you connect to another computer you send it your IP address.
- It is very hard to communicate without revealing an address on which you can receive traffic.
- Recent court cases have decided that your IP address can be used to identify you in court.

The TCP protocol
- The TCP protocol
  - Requires 2 way communication.
- Uses sequence numbers.

Who could fake your IP?
- If you have 2 way communication:
  - Anyone on the route between the hosts:
  - Sys admins at both ends
  - Your ISP
  - Anyone with access to the routers
  - Anyone on your local wi-fi or Ethernet
  - A hacker that has broken into any of the above.

Most Common Assumption:
- *Your IP always explicitly identifies you.*
- E.g. file sharers are sued by firms that
  - Find their IP and a time.
  - Go to the ISP and ask for the address of the user who had that IP at that time.

More Threats to Anonymity
- Your ISP logs all your web activities.
- Cookies in your browser.
  - Ad. companies profile your web surfing.
- Google knows every search you make.
“You have zero privacy anyway, get over it”
Scott McNealy,
CEO of SUN Microsystems.

With your permission, you give us more information about you, about your friends, and we can improve the quality of our searches. We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about.”
Eric Schmidt
CEO of Google

Proxy: Hotspot Shield VPN
An Internet connection reveals your IP number.
The promises “Anonymity”
Connection made via their servers.
The server never see's your IP address.

Virtual Private Networks
• VPNs securely connect you to another network.
• E.g. you can connect to the schools printers via the schools VPN
• Secured with certificates and encryption, e.g. TLS, or IPsec.

Virtual Private Networks For Anonymity
• To get some anonymity you can route all your traffic via the VPN.
  – Server thinks you are the VPN provider
  – ISP only sees the connection to the VPN
  – A global observer can probably link your connections.
• There is no anonymity to the VPN.

Proxy Example: AnchorFree’s Hotspot Shield VPN
But ...
• HotSpot makes its money from advertising, and will share information with advertisers.
• HotSpot will also share information with governments and law enforcement.
This is not the anonymity we are looking for.
MIXes
- MIXes are proxies that forward messages between them
- A user contacts a MIX to send a message
- The MIX waits until it has received a number of messages, then forwards them in different order

Some types of Mix
- Time delay mixes
  - Fires after a set time
- Threshold mixes
  - Fires when a set number of messages have arrived.
- Pool mixes
  - Like Threshold, but some messages are randomly held back to the next round.

1st Generation: Onion Routing
- Each node publishes a public key.
- The initiator selects the whole route and encrypts the message with all keys in reverse order.
- Each node unwraps a layer and forwards the message to the next one.

Onion Routing
- Onion Routing ensures that your message really is routed via the proxies you want.
  - Presented in the research paper:
  - "Tor: The Second-Generation Onion Router"
    By Roger Dingledine, Nick Mathewson, Paul Syverson

Onion Routing
- Each node only learns the IP of the node before it and the node after it.
- End-users can run their own node
  - Better anonymity
- or use an existing one
  - Easier to use
  - User's identity is revealed to the node
2nd Generation Onion Routing

Tor

- Tor implements this protocol.
- Several hundred volunteer nodes.
- Firefox plug-in.
- Big supporters include:
  - Electronic Frontier Foundation
  - US Naval Research Laboratory

Hidden Services

- Webservers that only accept connections via Tor.
- Server picks 3 nodes to set up connections.
- These nodes and the server’s public key are stored in a secure distributed database.
- The database entry key is the server’s address
  - E.g. http://3g2upl4pq6kufc4m.onion is the duckduckgo anonymous search engine.

Connecting to a Hidden Service via Tor

- Client uses the URL to look up the public key of the server and the introduction nodes.
- Client connects to a “rendezvous” node, tells the server about this via an introduction node.
- The server connects to the rendezvous node. The client and server are connected via Tor.

Example Hidden Service: The Silk Road
Example Hidden Service:
The Silk Road
- Market place for (main) drugs
  - Started early 2011
  - Estimated turnover $90,000 per month.
- Shut down Oct 2013:
  - FBI hacked the service
  - They installed their own software to reveal the users and location of the server.

Bitcoin
- An anonymous currency.
- Makes it easy for anyone (including criminals) to make secure payments over the Internet.
- More on this later in the module.

Problems with Tor
- Tor provides a very high degree of anonymity.
- No anonymity from an attacker that monitors the whole network.
- Some protocols broadcast their IP address
- If all the nodes on the path work together they can break your anonymity.

Poorly Configured Browsers Aren’t Anonymous with Tor
- Browser could give out cookies that identify you.
- Tor is TCP only.
  - server could use Flash to make the client connect to the server using UDP.
  - server then learns users real IP address.
- Need to turn off cookies and flash, JavaScript etc.

Question
- Does Tor keep your data secure?

Groups that did not realise this:
- Embassies of Japan, Russia, Kazakhstan, Uzbekistan, Tajikistan, India, Iran, Mongolia...
- UK Visa Application Centre in Nepal
- The office of the Dalai Lama
- Several Hong Kong Human Rights Groups
- Over 1,000 businesses ...
Monitoring Tor’s Output

• In Dan Egerstad (Security Researcher) ran five Tor nodes.
• He monitored all unencrypted traffic
• But also unencrypted e-mail traffic, including user names and passwords

Monitoring Tor’s Output

• He then tried to contact the embassies involved via the e-mail address.
• Got no or little response
• Finally he posted the login names and passwords on his website.

Some BAD passwords:

• Iranian embassies used their host country or cities name as their password.
• Hong Kong Liberal Party used “123456” and “12345678”.
• An Indian embassy used “1234”.
• An India Ministry of Defence account used “password+1”
• The Mongolian embassy in the U.S. used “temp”

Reactions

• India, Iran and Uzbekistan were “friendly” and acted quickly to fix the problem,
• China filed a criminal complaint over the posting,
• U.S. authorities had his website taken down,
• ... and the Swedish authorities arrested him.

The real story:

Further research found Tor nodes that:

• only accept unencrypted traffic for: DNS, POP3, IMAP, MSN Messenger, VNC and IRC.
• only accept HTTP packets bound for MySpace and Google (N.B. not HTTPS).
• A Tor Node that replaces any SSL certificate with a self signed certificate.

Conclusion

• Lots of different kinds and levels of anonymity.
• Key anonymity technologies include:
  – Proxy
  – Onion routing (e.g. Tor)
  – Mix networks