CS 134
Winter 2016

Privacy and Anonymity
Privacy

• Privacy and Society
  • Basic individual right & desire
  • Relevant to corporations & government agencies
  • Recently increased awareness
    • However, general public’s perception of privacy is fickle

• Privacy and Technology in Recent Years
  • >> Information disclosed on the Internet
  • >> Handling and transfer of sensitive information
  • << Privacy and accountability

(Image from geekologie.com)
Privacy on Public Networks

• The Internet is designed as a public network
  • Machines on your LAN may see your traffic, network routers see all traffic that passes through them

• Routing information is public
  • IP packet headers identify source and destination
  • Even a passive observer can easily figure out who is talking to whom

• Encryption (e.g., SSL or IPSec) does not hide identities
  • Encryption hides payload, not routing information
  • Even IP-level encryption (tunnel-mode IPsec/ESP) reveals IP addresses of IPsec gateways
Applications of Anonymity (1)

• Privacy
  • Hide online transactions, Web browsing, etc. from intrusive governments, marketers, archival/search entities (e.g., Google) as well as from criminals and snoops

• Untraceable Electronic Mail
  • Corporate whistle-blowers
  • Political dissidents in oppressive societies
  • Socially sensitive communications (online AA or STD meeting)
  • Confidential business negotiations

• Law Enforcement and Intelligence
  • Sting operations and honeypots
  • Secret communications on a public network
    • Informers, secret agents, etc.
Applications of Anonymity (2)

• Digital/Electronic Cash
  • Electronic currency with properties of paper money (online purchases unlinkable to buyer’s identity)

• Anonymous Electronic Voting

• Censorship-Resistant Publishing

• Crypto-Anarchy
  • “Some people say that “anarchy won't work.” That's not an argument against anarchy; that's an argument against work.” – Bob Black 😊
Applications of Anonymity (3)

- Porn
- Libel
- Disinformation / Propaganda
- Sale of Illegal Substances (e.g., SilkRoad)
- Tax Avoidance (via Untraceable Payments)
- Incitement to Criminal Activity (e.g., Murder, Rioting, Genocide, Terrorism)
What is Anonymity?

• Anonymity: is the inability to identify someone within a set of subjects (size varies)
  • Different from PRIVACY – right to be left alone
  • Hide your activities among similar activities by others
  • One cannot be anonymous alone!
    • Big difference between anonymity and confidentiality

• Unlinkability: of action and identity
  • For example, sender and his email are no more related after observing communication than they were before

• Unobservability: (very hard to achieve)
  • Observer cannot tell whether a certain action took place
Attacks on Anonymity

• Passive Traffic Analysis
  • Infer from network traffic who is talking to whom
  • To hide your traffic, must carry other people’s traffic!

• Active Traffic Analysis
  • Inject packets or put a timing signature on packet flow

• Compromise of Network Nodes (Routers)
  • Not obvious which nodes have been compromised
    • Attacker may be passively logging traffic
  • It’s better not to trust any individual node
    • Assume that some fraction of nodes is good, but do not know which
Chaum’s Mix

• Early proposal for anonymous email

• Public-key crypto + trusted re-mailer (Mix)
  • Untrusted communication medium
  • Public-keys used as persistent pseudonyms

• Modern anonymity systems use Mix as the basic building block
Basic Mix Design

Adversary knows all senders and all receivers, but cannot link a sent message with a received message.
Anonymous Return Addresses

\[ M \text{ includes } \{K_1, A\}_{pk(mix')} , K_2 \text{ where } K_2 \text{ is a fresh public key and MIX’ is possibly different from MIX} \]

\[ \{r_1, \{r_0, M\}_{pk(B)}, B\}_{pk(mix)} \]

\[ \{r_0, M\}_{pk(B)}, B \]

\[ A, \{\{r_2, M'\}_{K_2}\}_{K_1} \]

Response MIX’

\[ \{K_1, A\}_{pk(mix')} , \{r_2, M'\}_{K_2} \]

Secrecy without authentication
(good for an online confession service 😊)
Mix Cascade

• Messages are sent through a sequence of mixes
  • Can also form an arbitrary network of mixes (“mixnet”)

• Some mixes may be controlled by attacker, but even a single good mix guarantees some anonymity

• Pad and buffer traffic to foil correlation attacks
Disadvantages of Basic Mixnets

• Public-key encryption and decryption at each mix are computationally expensive

• Basic mixnets have high latency
  • Ok for email, but not for anonymous Web browsing

• Challenge: low-latency anonymity network
  • Use public-key cryptography to establish a “circuit” with pairwise symmetric keys between hops on the circuit
  • Then use symmetric decryption and re-encryption to move data messages along the established circuits
  • Each node behaves like a mix; anonymity is preserved even if some nodes are compromised
Another Idea: Randomized Routing

- Hide sources by routing messages randomly
  - Popular technique: Crowds, Freenet, Onion routing

- Routers do not know if the apparent source of a message is the true sender or another router
Onion Routing

- Sender chooses a random sequence of routers
  - Some routers are honest, some are not
  - Sender controls path length

[Reed, Syverson, Goldschlag 1997]
Route Establishment

- Routing info for each link encrypted with router’s public key
- Each router learns only the identity of the next router
The Onion Router (Tor)

• Second-generation onion routing network
  • [http://tor.eff.org](http://tor.eff.org)
  • Specifically designed for low-latency anonymous Internet communications (e.g., Web browsing)
  • Running since October 2003

• Hundreds of nodes on all continents

• 1.5 million users as of 2016

• “Easy-to-use” client proxy
  • Freely available, can use it for anonymous browsing
  • Available for smartphones and tablets too
Tor Circuit Setup (1)

- Client proxy establishes a symmetric session key and circuit with Onion Router #1
Tor Circuit Setup (2)

- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #2
  - Tunnel through Onion Router #1
Tor Circuit Setup (3)

- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #3
  - Tunnel through Onion Routers #1 and #2
Using a Tor Circuit

• Client applications connect and communicate over the established Tor circuit (also to multiple dst-s)
  • Datagrams are decrypted and re-encrypted at each link
Tor Management Issues

• Many applications can share one circuit
  • Multiple TCP streams over one anonymous connection

• Tor router do not need root privileges
  • Encourages people to set up their own routers
  • More participants = better anonymity for everyone

• Directory servers
  • Maintain lists of active onion routers, their locations, current public keys, etc.
  • Control how new routers join the network
    • “Sybil attack”: attacker creates a large number of routers
  • Directory servers’ keys ship with Tor code
Location Hidden Servers

• **Goal:** deploy a server on the Internet that anyone can connect to without knowing where it is or who runs it

• Accessible from anywhere

• Resistant to censorship

• Can survive a full-blown DoS attack

• Resistant to physical attack
  • Can not find the physical server!
Creating a Location Hidden Server

Server creates circuits to “introduction points”

Server gives intro points’ descriptors and addresses to service lookup directory

Client obtains service descriptor and intro point address from directory
Using a Location Hidden Server

Client creates a circuit to a "rendezvous point"

Rendezvous point matches the circuits from client & server

If server chooses to talk to client, connect to rendezvous point

Client sends address of the rendezvous point and any authorization, if needed, to server through intro point
Deployed Anonymity Systems

• Free Haven project has an excellent bibliography on anonymity
  • http://www.freehaven.net/anonbib

• Tor (http://tor.eff.org)
  • Overlay circuit-based anonymity network
  • Best for low-latency applications such as anonymous Web browsing

• Mixminion (http://www.mixminion.net)
  • Network of mixes
  • Best for high-latency applications such as anonymous email
Dining Cryptographers

• How to make a message public, but in a perfectly untraceable manner

• Guarantees information-theoretic anonymity for message senders
  • VERY strong form of anonymity: defeats adversary who has unlimited computational power

• Difficult to make practical
  • In group of size N, need N random bits to send 1 bit
Three-Person DC Protocol

• Three cryptographers are having dinner.

• Either NSA is paying for the dinner, or one of them is paying, but wishes to remain anonymous.

1. Each diner flips a coin and shows it to his left neighbor.
   • Every diner sees two coins: his own and his right neighbor’s

2. Each diner announces whether the two coins are the same. If he is the payer, he lies (says the opposite).

3. IF Number of “same” = 1 or 3 \( \Rightarrow \) NSA is paying
   IF Number of “same” = 0 or 2 \( \Rightarrow \) one of them is paying
   • But a non-payer cannot tell which of the other two is paying!
Non-Payer’s View: Same Coins

Without knowing the coin toss between the other two, non-payer cannot tell which of them is lying.

 payer

 payer
Non-Payer’s View: Different Coins

Without knowing the coin toss between the other two, non-payer cannot tell which of them is lying.
Super-posed Sending

• This idea generalizes to any group of size N

• For each bit of the message, every user generates 1 random bit and sends it to ONE neighbor
  • Every user learns 2 bits (his own and his neighbor’s)

• Each user announces own bit XOR neighbor’s bit

• Sender announces own bit XOR neighbor’s bit XOR message bit

• XOR all announcements = message bit
  • Every randomly generated bit occurs in this sum twice (and is canceled by XOR), message bit occurs once