CS 134

Privacy and Anonymity

1

Privacy

•(Image from geekologie.com)

- 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

2

Privacy on Public Networks

- 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

3

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.

4

Applications of Anonymity (2)

- Digital 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 `anarchy won't work'. That's not an argument against anarchy; that's an argument against work." – Bob Black
  - ☺

5

Applications of Anonymity (3)

- Porn
- Libel
- Disinformation / Propaganda
- Sale of illegal substances
- Tax avoidance (via untraceable payments)
- Incitement to criminal activity (e.g., genocide, terrorism)

6

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 (hard to achieve)
  - Observer cannot tell whether a certain action took place or not

7

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, don't know which

8

Chaum's Mix

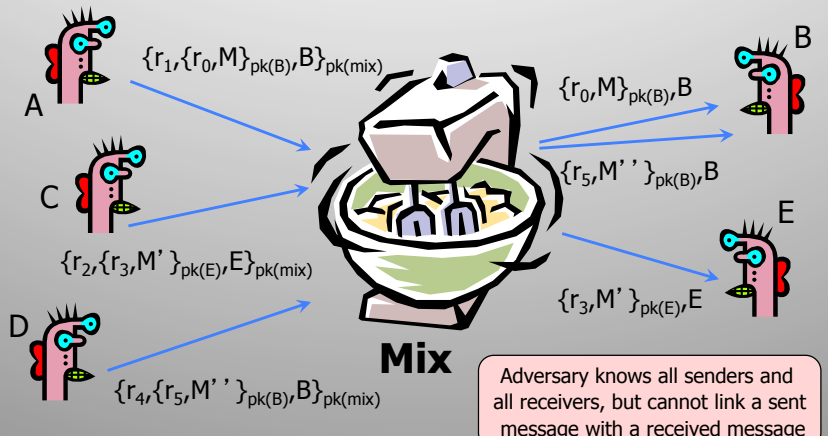
- Early proposal for anonymous email
  - David Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". Communications of the ACM, February 1981.

Before spam, people thought anonymous email was a good idea ☺

- 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

9

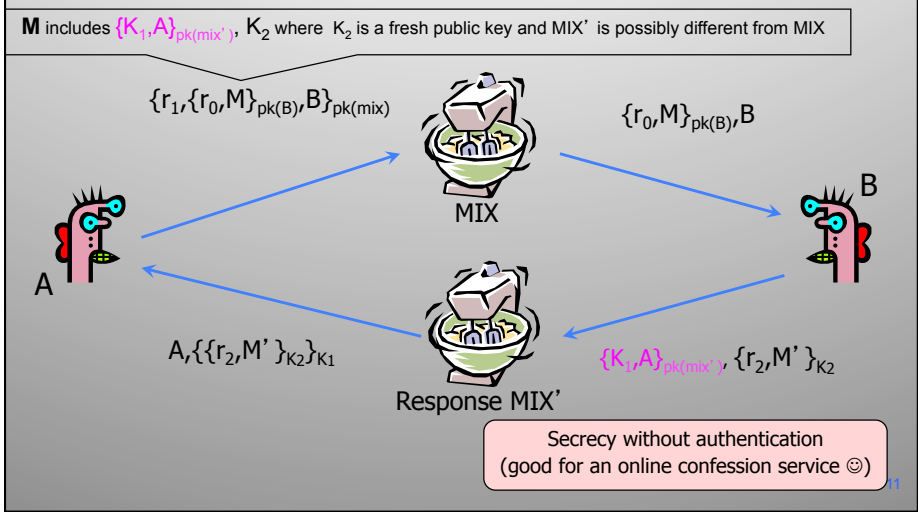
Basic Mix Design



Adversary knows all senders and all receivers, but cannot link a sent message with a received message

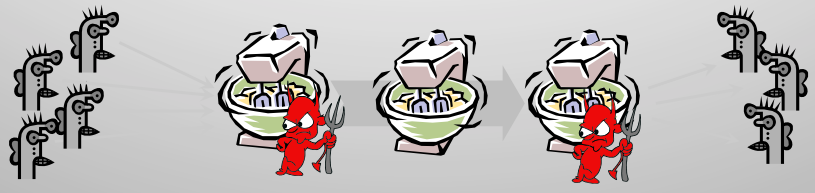
10

Anonymous Return Addresses



11

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

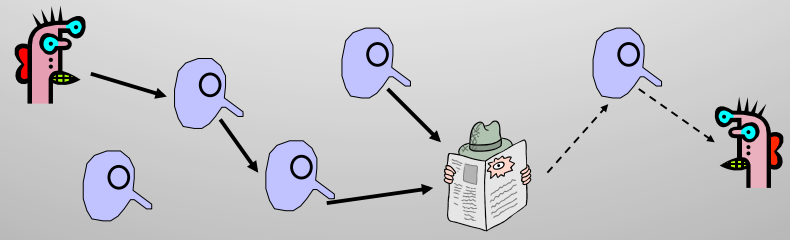
12

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

13

Another Idea: Randomized Routing

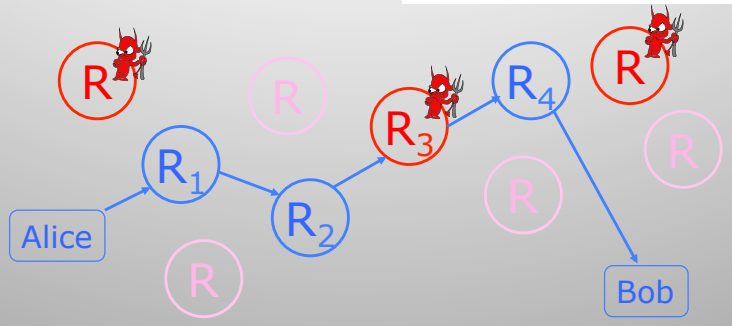


- Hide message source by routing it randomly
  - Popular technique: Crowds, Freenet, Onion routing
- Routers don't know for sure if the apparent source of a message is the true sender or another router

14

Onion Routing

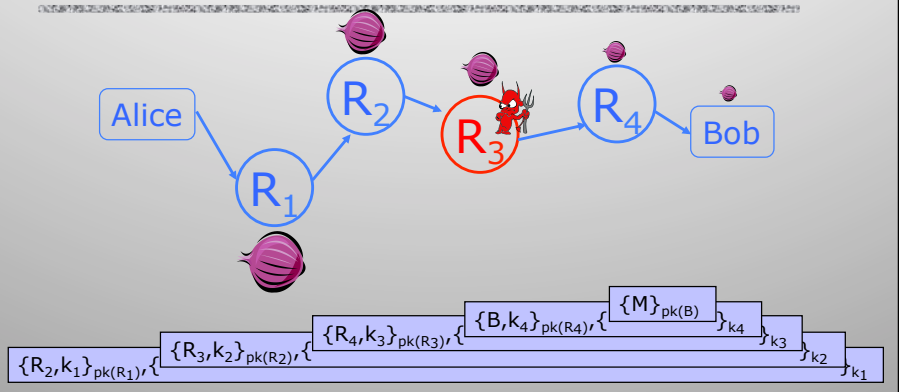
[Reed, Syverson, Goldschlag 1997]



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

15

Route Establishment



- Routing info for each link encrypted with router's public key
- Each router learns only the identity of the next router

16

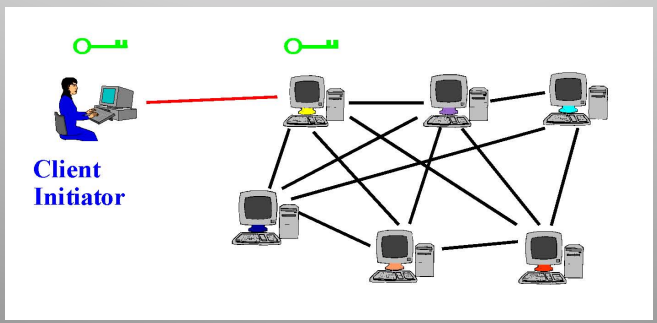
Tor

- Second-generation onion routing network
  - 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
- Approximately 300,000 users as of 2009
- "Easy-to-use" client proxy
  - Freely available, can use it for anonymous browsing

17

Tor Circuit Setup (1)

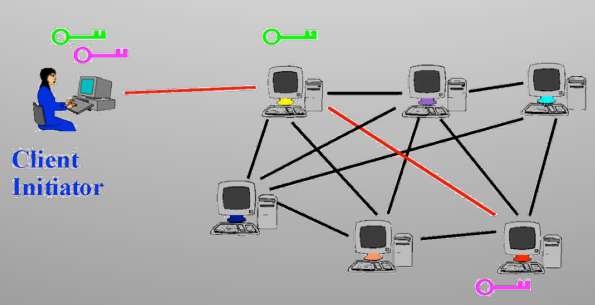
- Client proxy establishes a symmetric session key and circuit with Onion Router #1



18

Tor Circuit Setup (2)

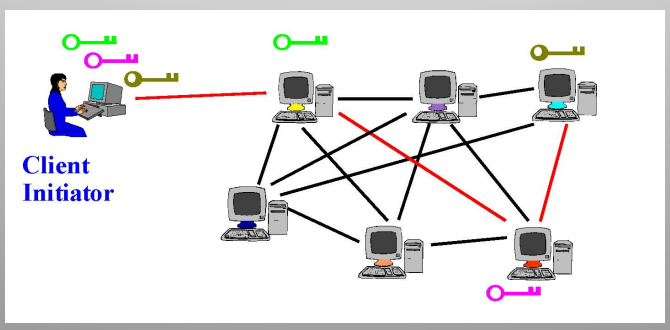
- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #2
  - Tunnel through Onion Router #1



19

Tor Circuit Setup (3)

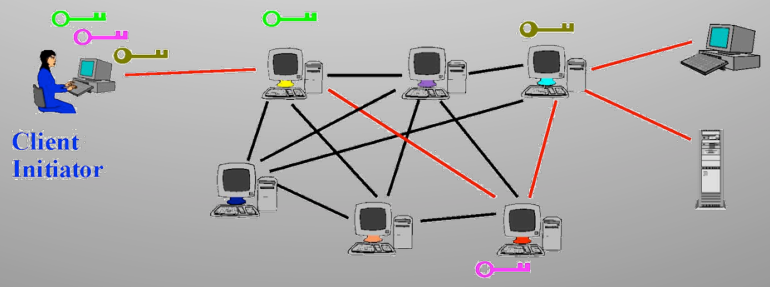
- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #3
  - Tunnel through Onion Routers #1 and #2



20

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



21

Tor Management Issues

- Many applications can share one circuit
  - Multiple TCP streams over one anonymous connection
- Tor router doesn't 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 --- PoV

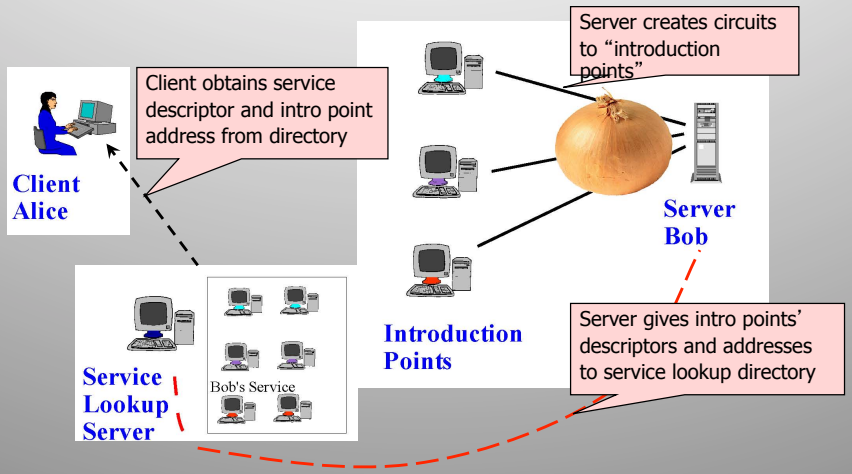
22

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't find the physical server!

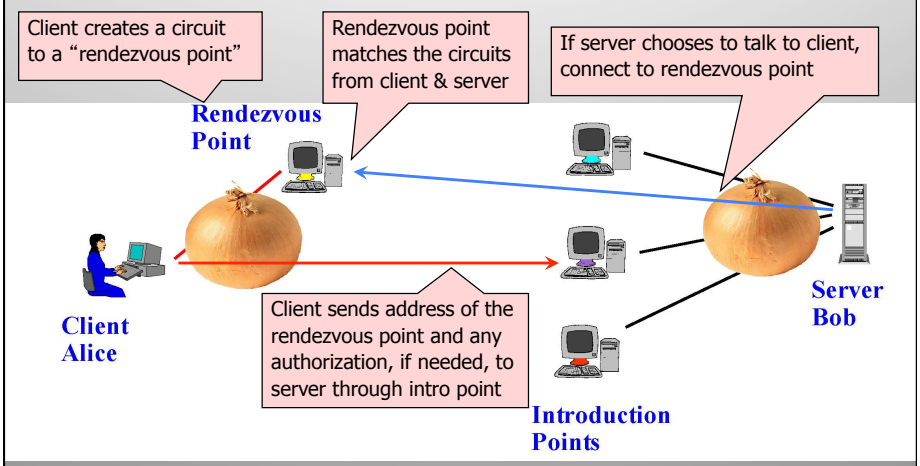
23

Creating a Location Hidden Server



24

Using a Location Hidden Server



25

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

26

Dining Cryptographers

- Clever idea how to make a message public in a perfectly untraceable manner
  - David Chaum. "The dining cryptographers problem: unconditional sender and recipient untraceability." Journal of Cryptology, 1988.
- Guarantees information-theoretic anonymity for message senders
  - This is 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

27

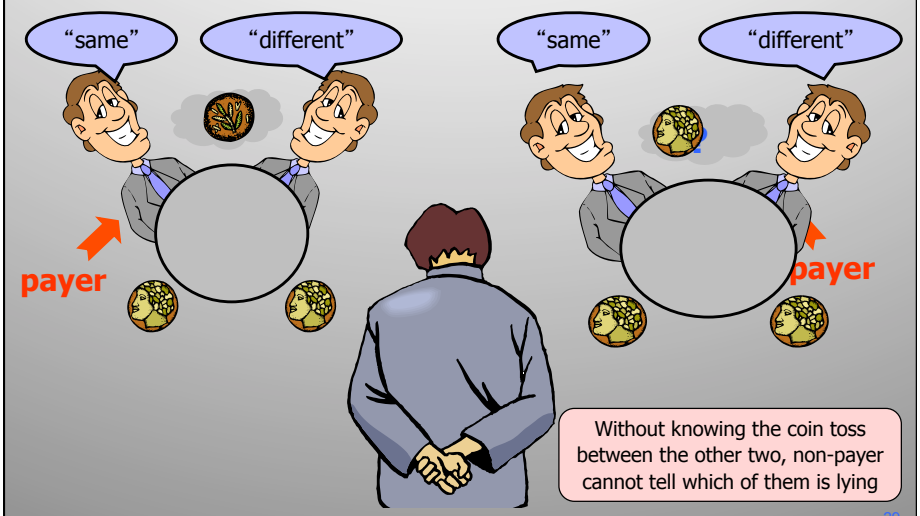
Three-Person DC Protocol

- 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 ⇒ NSA is paying
   IF Number of "same" = 0 or 2 ⇒ one of them is paying
   - But a non-payer cannot tell which of the other two is paying!

28

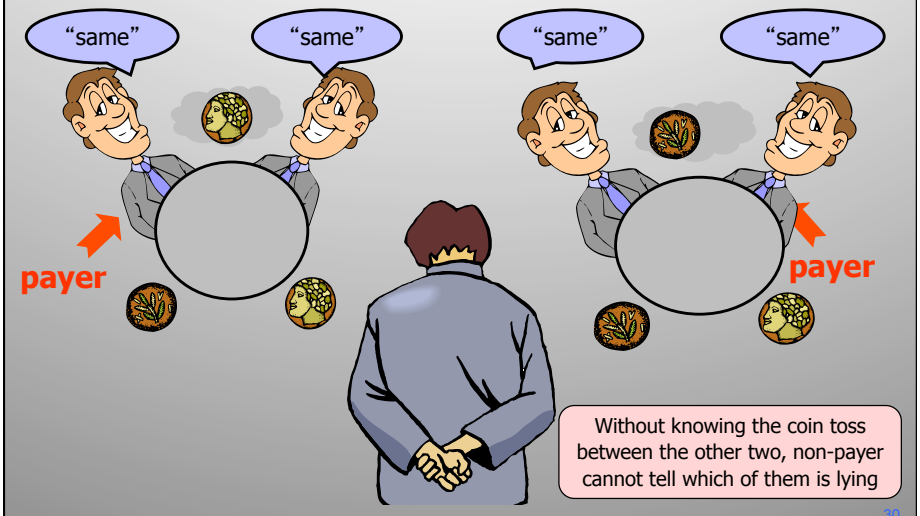
Non-Payer's View: Same Coins



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

29

Non-Payer's View: Different Coins



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

30

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

31