Anonymous Communication

An Introduction

James Lee

jlee23@umbc.edu

University of Maryland, Baltimore County

Outline

- Introduction
- Relays
- Mixes
- Questions
- References

Why Is Anonymity Important?

- A person wants to protect their privacy.
- Fear of retaliation, discrediting, unpopular sentiment, etc.
- Examples:
  - Crime tip lines
  - Political discussion, voting
  - P2P file sharing
- Users are identified by unique addresses (IP, MAC, etc.)

What Is the Goal?

- Make it appear to an outside observer that no communication happened at all.
- However, on the Internet there is spyware, untrusted routers, packet sniffers, trojans, wire tappers.
- Strive for sender anonymity, receiver anonymity, sender-receiver unlinkablity.

Anonymity is the state of being not identifiable within a set of subjects.

Unlinkability means an attacker would not be able to relate two or more subjects by observing the system.

Trusted and Semi-trusted Relays

Relays rely on one central trusted node to provide security.

- The Anon.penet.fi relay
- Anonymizer and SafeWeb
- Type I remailers
- Crowds
- Nym servers

The Anon.penet.fi Relay

- Pseudoanonymous email service started in 1993.
- Kept table mapping pseudonyms to real email addresses.
- Email to a pseudonym would be forwarded to the real address.
- Email from a pseudonym would be stripped of all identifying information and relayed.
- Service shut down in 1996 after being forced to reveal the identity of a user in a copyright trial.

Anonymizer and SafeWeb

- Anonymizer and SafeWeb are both commercial services which offered web proxies.
- Filters out or wraps active content like JavaScript or Java which could be used to identify users.
- Like anon.penet.fi, anonymity depends on the integrity of the company providing the service.
- Less vulnerable to legal attacks since logs don’t have to be kept.

Type I Remailers

- Relay email after stripping all identifying information.
- Many implementations allowed remailers to be chained together.
- Reply information encrypted within the message itself.
- Unlike anon.penet.fi, no database of pseudonyms is kept, but each relay node still has to be trusted.

Crowds

- User downloads a list of participants from a central server.
- User then relays a web request to a randomly selected node in the crowd.
- Any received request is either relayed to another random node or sent to the final recipient randomly.
- Cannot tell if a request was initiated by the previous node or if it was just passing it on.
- Dishonest nodes can collude to discover identity of users.

Nym Servers

- Like remailers, but also give users pseudonyms.
- Routing information encoded within message.
- Nym servers don’t have to be trusted since they can only determine the location of other nym servers.

Mix Systems

These systems use techniques from remailers plus cryptography to ensure anonymity.

- Chaum's original mix
- ISDN mixes, real time mixes, and web mixes
- Onion Routing
- Tor

Chaum's Original Mix

- A "mix" node hides the correspondence between its input messages and output messages using cryptography.
- Messages to be anonymized are encrypted and relayed through a mix which has a well-known public key.
- The mix decrypts the message, strips out identifying information, adds random bits (junk) to the end passes it on to the recipient.
- Mixes also mix together many messages, sending messages out in a different order than they were received.

ISDN Mixes

- Designed for constant, high traffic such as streaming data or voice.
- Uses a cascade of mixes with a persistent route set up before sending data.
- Does not mix message order, uses stream cipher instead of block cipher.
- Based on ISDN infrastructure; not well suited for TCP/IP.

Onion Routing

- Like ISDN mixes in that a route is established before sending messages.
- First message is encrypted in layers that can only be decrypted by a chain of onion routers.
- First message contains keys for the routers for encryption of subsequent messages.
- Vulnerable to “timing attacks.” Adversary can watch the patterns of traffic moving between routers to identify users.

Tor

- An implementation of onion routing for arbitrary TCP streams.
- Any application can route through the Tor network without modification using its SOCKS proxy service.
- Also provides mechanisms for “hidden servers.”

Questions

References

- George Danezis and Claudia Diaz. A Survey of Anonymous Communication Channels. Submitted to the *Journal of Privacy Technology*, 40 pages, 2006.
- Andy Jones. Anonymous Communication on the Internet. http://www10.cs.rose-hulman.edu/Papers/Jones.pdf. Retrieved Feb 17, 2008.