Anonymity on the Internet

Cunsheng Ding

HKUST

Hong Kong

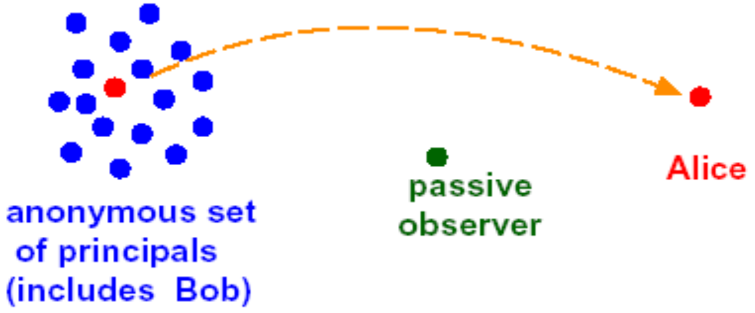
Part I: Introduction to Anonymity

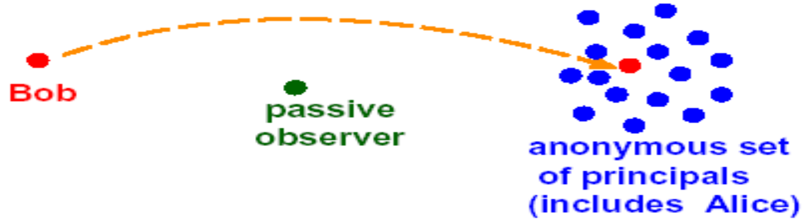
Definition of Anonymity

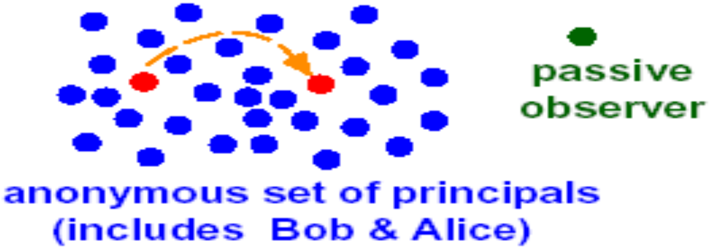
- According to Wikipedia, anonymity is derived from the Greek word ἀνωνυμία, anonymia, meaning "without a name" or "namelessness".
- Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set.
- The anonymity set may vary from time to time.

Types of Anonymity

- Sender
  - Receiver / observer can’t identify sender
- Receiver
  - Observer can’t identify receiver
- Sender-receiver
  - Observer can’t identify that communication has been sent







Pseudonymity

- Though the identity of the message sender may seem anonymous because it is not easily to uncovered or make readily available by definition, it is possible to discover the identity of the pseudonymous message sender.
- This kind of anonymity has significant benefits: it enables citizens of a democracy to voice their opinions without fear of retaliation against their personal reputations, but it forces them to take ultimate responsibility for their actions should the need somehow arise.

The Demand of Anonymity: Before the Internet

- It is as old as identity and goes along with humankind from the dawn of history.
- Many acts of charity are performed anonymously, as benefactors do not wish, for whatever reason, to be acknowledged for their action.
- Journalists frequently use anonymous sources to help investigate news stories. As fear of the retaliation or persecution, the whistle-blowers do not want to disclose their identities. Then journalists report using the anonymous sources but quoting informants who were unwilling to reveal their identities as an “anonymous sources”.

The Demand of Anonymity: The Internet Era

- The appeal of Internet communication depends in part on its capacity to support anonymity.
- Internet users can make political claims as well as non-political comments, engage in whistle-blowing, conduct commercial transactions, receive counseling and consume sexual materials without apparently disclosing their identities.
- Anonymous communication encourages Internet communications, and the Internet in turn may encourage anonymous communication.

The Negative Sides of Anonymity

- Spam
- DoS -
- Illegal activity – anonymous bribery, copyright infringement, harassment, financial scams, disclosure of trade secrets

Part II: Anonymity Mechanisms

Proxy (1)

- An anonymous proxy or anonymizer which makes activities on the Internet to be untraceable.
- Between source and destination, it acts as an intermediary and privacy shield to protect personal information by hiding the identity information of sender or receiver.
- It is used to protect the privacy and anonymity of web browsers from web site operators, Internet snoops, and even unfriendly governments.
- It is the most commonly used.

Proxy (2)

- Web client <-> Proxy Server <-> Web server
- The web server does not know the client, but the proxy server.
- The proxy server does know who the client is.
- A good web proxy will allow users to setup a TLS or SSL tunnel. This will prevent packet sniffers from eavesdropping while surfing anonymously.

Proxy (3)

In addition to hiding IP address, an anonymous proxy server will typically remove traffic such as:

- Cookies
- Pop-ups
- Banners
- Scripts
- Referrer information

Mix: Brief Introduction

- It was invented by David Chaum in 1981.
- It is the basic building block of nearly all modern high-latency anonymous communication systems.
- It is a process that
  - accepts encrypted messages as input,
  - then decrypts them;
  - finally sends the decrypted version to the receiver

Mix: Technical Idea

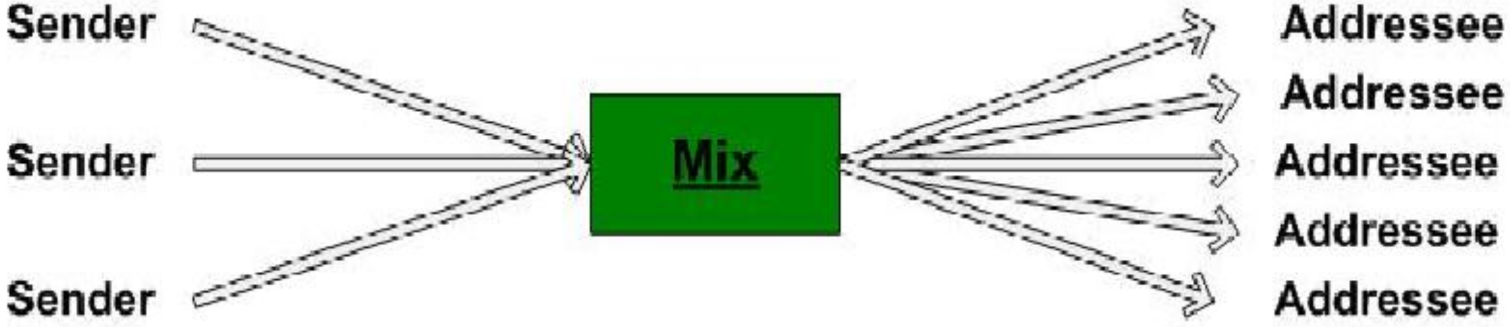
- Participant A prepares a message for delivery to participant B by appending a random value to the message, sealing it with the addressee's public key Kb, appending B’s address, and then sealing the result with the mix's public key Km. M opens it with his private key, now he knows B’s address, and he sends Kb(message,R) to B

$$K_m(R1, K_b(R0, message), B) \longrightarrow (K_b(R0, message), B)$$

- R1 and R0 are random values (strings).
- Question: What are the roles played by R1 and R0?

Mix: How to Use It

- The Mix will wait for a number of input messages, i.e., buffer them.
- The Mix then decrypts the messages.
- The decrypted messages will then be sent out in a different order

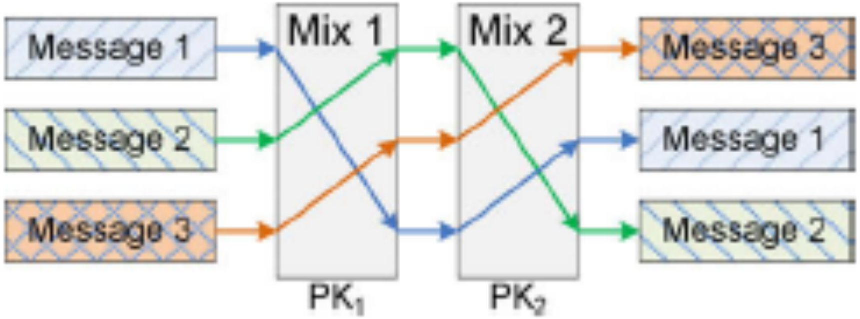


Mix: Security Questions

- Does it provide sender anonymity?
- What will happen if one only one sender is active for a period of time?
- Does it provide receiver anonymity?

Mix Network

- It is a network of mixes, and used for providing better anonymity.
- In case one of the mixes is not trustful, anonymity can still be achieved.



Mix Networks: Problems

- Fine for non real-time applications (email)
- Not sufficient for VoIP, video, web
- Mix waits to accumulate inputs to process as a batch (especially slow for low traffic)

Mix Networks: Enhancements

- Messages all the same length by padding
- Dummy messages inserted
  - Between mixes
  - Between mixes and user
- Balance end to end throughput with anonymity
  - Duration to wait for mixes to accumulate traffic
  - Percentage of dummy traffic

Onion Routing (1)

- It is a distributed overlay network designed to anonymous TCP-based communications over a computer network.
- It is based on the principle of Chaum’s mix
- Encrypt message in layers, one for each hop on the path.

Onion Routing (2)

- Each onion router is a store-and-forward device that accepts fixed length messages, performs cryptographic operations on the messages, and then forwards the messages to the next node in the routing path, called onion router.
- When an onion router receives a message, it knows the immediate predecessor of this message and to whom it should be passed.
- Each onion router removes a layer of encryption using its own private key, which will also uncover routing instructions of the next onion router.

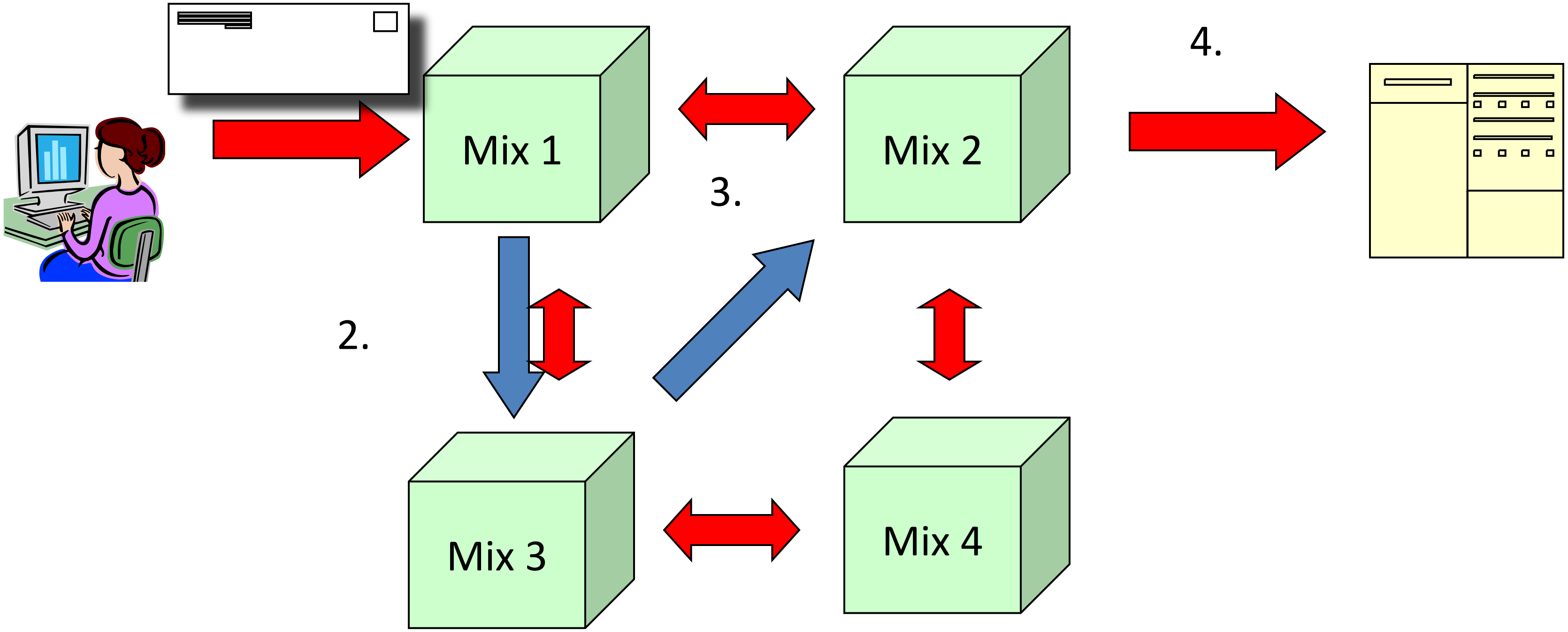
Ai = Next Hop Address

Ci = Message encrypted with public key of Mix i

S = Destination Host address

M = Original message

Each Mix is called an onion router



1. A1, C1(A3, C3(A2, C2(S, M, r2), r3), r1)
2. A3, C3(A2, C2(S, M, r2), r3)
3. A2, C2(S, M, r2)
4. S, M

Other Anonymity Mechanisms

- Tor: the most recent evolution of onion routing.
- Crowds: defense against internal receiver and a corrupted receiver, used for anonymous web browsing.
- DC-nets:
  - It is a secure multi-party computation protocol.
  - It provides sender and receiver anonymity without relying on a trusted third party.

Part III: Applications

Applications of Internet Anonymity

- Anonymous remailer
  - Anon.penet.fi, Cypherpunk, Mixmaster, Mixminion
- Anonymous electronic voting system
- Digital cash

Part IV: Regulations on Anonymity

EU Regulations

- A user should not be required to justify anonymous use.
- Anonymity should not be used as a cloak to protect criminals.
- Various countries have laws both protecting and forbidding anonymity.
- Different countries in EU have different laws.

Hong Kong Regulations

- Government agents are allowed to perform real identity trace in any communication channel including cyberspace if the anonymity is likely connected with crime or security measure.
- In general, persevering anonymity is recognized as a human right.
- Anonymity is not allowed for the sender for commercial purpose (no anonymous commercial emails).