Anonymous Mixes

As Proposed by David Chaum

James Lee

jlee23@umbc.edu

University of Maryland, Baltimore County

Outline

- Introduction
- Public Key Cryptography
- Assumptions
- Mixes
- Return Addresses
- Digital Pseudonyms
- Conclusion
- Questions
- References

“The Traffic Analysis Problem”

- Anyone along a physical circuit can watch traffic flow.
- Trying to keep confidential who converses with whom and when.
- Solution based on public key cryptography.
- Previous work required common authority.
- Now all participants are authorities.

Public Key Cryptography

- Solves the key distribution problem.
- User creates two keys: public K and private K^{-1}.
- Public and private keys are inverses of each other.

Sealing a Message

- A message is *sealed* by any user so that only a certain user can decrypt it.
- $K(R, X) = Y$
- Append random bits R before message X to make brute-force attacks harder.
- Designated user can decrypt using their private key: $K^{-1}(Y) = R, X$.

Signing a Message

- A message is *signed* so that any user can verify its source.
- $K^{-1}(C, X) = Y$
- Any user can decrypt using the public key of the claimed source: $K(Y) = C, X$.
- If C matches expected value, then X is actually from the claimed source.

Assumptions

1. The cryptographic algorithm is strong.
2. Anyone may watch the underlying communication system. Anyone may interfere.

Mixes

- A *mix* is a computer which accepts and delivers messages.
- A user wishing to remain anonymous to the recipient will send a message through the mix.
- Every participant in the system has a known public key.
- User seals message for the recipient, then seals the sealed message with the recipient's address for the mix.
- Mix will send the original sealed message to the designated address.
- $K_{mix}(R_{mix}, K_{dest}(R_{dest}, M), A) \rightarrow K_{dest}(R_{dest}, M), A$

Mixes (cont.)

- Purpose of mixes is to hide correspondences between the items in the input and output.
- Order of arrival is hidden by outputting messages in uniformly sized, lexicographically ordered batches.
- Special care must be taken to make sure duplicate messages are never sent twice.

Signed Receipts

- How does a user know if the mix discarded the message?
- Mix sends the signed batch back to the user.
- User checks the signature.
- Checks if original message exists in the batch.

Cascades

- Series of mixes.
- Prevents any single mix from knowing both the source and destination of a message.
- $K_{mix_1}(R_{mix_1}, K_{mix_2}(R_{mix_2}, K_{dest}(R_{dest}, M), A), A_{mix_2})$

Return Addresses

- Alice can form an untraceable return address: $K_{mix}(R_{mix}, A_{alice}), K_{alice}$.
- Alice can send the address to Bob in an anonymous message.
- For Bob to send a reply, he forms a message for a mix like: $K_{mix}(R_{mix}, A_{alice}), K_{alice}(R_{bob}, M)$.

Digital Pseudonyms

- Public key used to identify a user.
- A authority holds a *roster* of trusted pseudonyms.
- Applicant sends his public key, K, to the authority through a mix.
- Example: Registered voters can submit a signed, anonymous ballot $K_{mix}(R_{mix}, K, K^{-1}(C, Vote))$.
- Recipient of ballot checks K against roster and records the vote.

Questions

References

- David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. In *Communications of the ACM 4(2)*, February 1981.
- George Danezis and Claudia Diaz. A Survey of Anonymous Communication Channels. Submitted to the *Journal of Privacy Technology*, 40 pages, 2006.