Anonymity and Anti-censorship

Kai Shen
Dept. of Computer Science, University of Rochester

Security-related Issues

- Anonymity and anti-censorship
- Trust and reputation
- Distributed denial-of-service attacks

Background knowledge:
- Cryptography/encryption – symmetric key and public key
- Data integrity – message digest

Anonymous Email

Why anonymous email?
- Protection from prejudice
- Privacy

Why is it difficult?
- Every email has a header including a list of computers it passed through

How to deal with it?
- Use anonymous email relay servers: mixmaster remailers

Roles in our study:
- Bob – the sender
- Alice – the receiver

Mixmaster Remailers

Starting point
- Remailer 1.0: The remailer receives mail from Bob, removes all headers except the subject and then forwards it to Alice.

What if Alice (or anybody else) sniffs in your network?
- Remailer 2.0: Bob encrypts the message to remailer using remailer’s public key.

What if Alice wants to reply?
- Remailer 3.0: The remailer adds a return address block in message to Alice. The return address is encrypted using remailer’s public key. Alice can send reply message back the remailer with the address block intact.
Mixmaster Remailers (cont.)

- What if attackers do traffic analysis?
  - Remailer 4.0: The remailer holds each message for a random period of time before forwarding to Alice. The remailer can even randomly send some junk to someone to hide the real messages.
- What if the remailer could be compromised?
  - Remailer 5.0: Bob employs a chain of remailers, each of which only knows its immediate predecessor and successor.

Anything missing?

Anonymity and Anti-censorship in Document Publishing

- Anonymity
  - protect the author
  - documents are distributed under a name called "Document Locator"
  - documents can be looked up using peer-to-peer lookup protocol, query flooding
- Anti-censorship
  - protect the publisher
  - one way to protect the publisher is to make the publisher unaware of the content unless it knows the "Document Locator"
  - how?

Anti-censorship in Document Publishing

Publius:
- Documents are encrypted
- The encryption key contains 30 shares, any 3 shares can decrypt the document
- Encrypted document and each share of the key is distributed under separate IDs.
- "Document Locator" contains the ID of the encrypted document and the IDs of all the key shares.