Towards Measuring Anonymity

Claudia Diaz, Stefaan Seys, Joris Claessens, Bart Preneel

Presented By: Chris Coakley

Overview

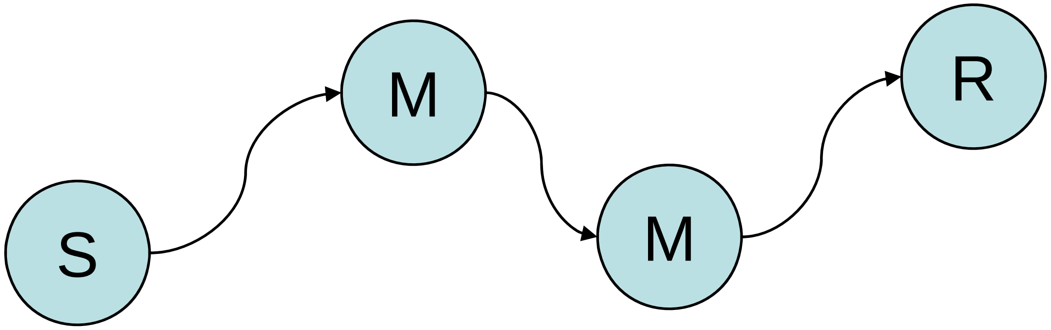
- Background
  - Topic Area
  - Problem
- Research
  - Threat and Privacy Models
- Results
- Examples
- Pro/Con

Background

- Topic Area
  - Anonymous routing protocols
  - Keeping the sender secret
  - Secret data is a separate problem
- Problem
  - How much anonymity does a system provide?
  - What does that mean, anyway?

System Model

- Senders
- Recipients
- Mixes
- Anonymity Set - the “honest” Senders



Threat Model

- Attacker Properties
  - Internal - External
  - Passive - Active
  - Local - Global
- Probabilistic Attack
  - With probability p, A is the sender
- Maximum Anonymity: All senders equally probable

Degree of Anonymity

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

What does it mean?

- d = 0 - it was YOU!
- d = 1 - it could be anyone

Example - Crowds

- Sender submits web request to Mixes
- With probability:
  - p_f - forward to another mix
  - 1-p_f - make request
- Property Missing: Mix doesn’t try to hide correlation of incoming and outgoing traffic

Crowds - Attack

- Corrupted Mixes (C Collaborators)
- Internal, Passive, Local

Attack

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

Attack

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

Sender’s Point of View

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

Example - Onion Routing

- Sender routes message through Mixes
- Sender determines path

Onion Routing - Attack

- Attack method is indeterminate
- Somehow identifies a subset of possible senders S
  - Each has probability 1 / S

Onion Routing - Attack

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

Pros

- Easy to see contributions to previous work
    - Precise Definition of Degree of Anonymity
- Crowds Example is nice

Cons

- Change of Language
  - Mix becomes Jondo, User
  - 3 becomes C+1
- Useless Examples
  - Anonymous Email (elided)
  - Onion Routing
- Pulls numbers from anus

Done

- Questions?
  - 42
  - true