Lecture 7.1: Privacy and Anonymity Using Anonymizing Networks - I

CS 436/636/736
Spring 2012

Nitesh Saxena

Some slides borrowed from Philippe Goillé, Markus Jacobson
Course Admin

• Mid-term graded
  – Scores posted
  – To be distributed today
  – Stats: Mean 87.75; Median 92.5

• HW3 to be posted in the next few days
A Case History: AOL Web Search Query Log Leakage

• **AOL's disturbing glimpse into users' lives, CNET News, August 7, 2006**
  – 21 million search queries posed over a 3-month long period; 650,000 users
  – No user identification information released per se, but??

• Search Log still available:
Other Scenarios where privacy is important

- Location-based search
- Web browsing
- Electronic voting
- Electronic payments
- Email conversation
- ...
Today’s Outline

• Anonymizing Network (or Mix Network)
• Anonymizing Network Applications
• Requirements
• Robustness
• Types of Anonymizing Networks
  – Decryption based (Onion Routing)
  – Re-encryption based
Definition: Mix Server (or Relay)

A mix server:
- Receives inputs
- Produces “related” outputs
- The relationship between inputs and outputs is secret

A mix server receives a set of inputs and produces related outputs so that the relationship between inputs and outputs can not be learned by anyone but the mix server.
a mix server receives a set of inputs and produces related outputs so that the relationship between inputs and outputs can not be learned by anyone but the mix server.
Applications

• Hide:
  ➔ “who voted for whom?”
  ➔ “who paid whom?”
  ➔ “who communicated with whom?”
  ➔ “what is the source of a message?”

• Good for protecting privacy for
  election and communication

• Used as a privacy building block
Electronic Voting Demonstration

1. “Who do you like best?”
   - Washington
   - Lincoln
   - Roosevelt

2. Put your ballot into a WHITE envelope and put again in a RED one and sign on it.

Jerry
Electronic Voting Demo. (Cont’d)

Administrators will
1. Verify signatures together
2. 1st Admin. shuffles and opens RED envelopes
3. Send them to 2nd Admin.
4. 2nd Admin. shuffles again and opens WHITE envelopes
5. Count ballots together
A real system for elections

\[
\text{Sign}_{\text{voter} \, 1} \left( \text{encr} (\text{encr} (\text{vote}_1)) \right) \to \text{Mix Net} \\
\text{Sign}_{\text{voter} \, 2} \left( \text{encr} (\text{encr} (\text{vote}_2)) \right) \\
\text{...} \\
\text{Sign}_{\text{voter} \, n} \left( \text{encr} (\text{encr} (\text{vote}_n)) \right) \\
\]

\[
\text{Mix Net} \to \left\{ \begin{array}{l}
\text{vote}_1 \\
\text{vote}_2 \\
\text{vote}_3 \\
\text{...} \\
\text{vote}_n
\end{array} \right\}
\]
Electronic Payment Demo.

- “Choose one person you like to pay $5”

  Name of the person
  (__________)

- Put your ballot into an **WHITE** envelope and put again in a **RED** one and sign on it
Electronic Payment Demo. (Cont’d)

Administrators will

1. Verify signatures together
2. Deduct $5 from each account
3. 1st Admin. shuffles and opens RED envelopes
4. Send them to 2nd Admin.
5. 2nd Admin. shuffles again and opens WHITE envelopes
6. Credit $5 to recipients
For email communication

\[\text{encr (email}_1, \text{ addressee}_1)\]
\[\text{encr (email}_2, \text{ addressee}_2)\]
\[\ldots\]
\[\text{encr (email}_n, \text{ addressee}_n)\]

Mix
Net

\{\ldots\}

To: Jerry
Don’t forget to have lunch.

Deliver
Other Uses

- Anonymous web browsing; web searching (Anonymizer)

From LPWA homepage
Other Uses (Cont’d)

- Location privacy for cellular devices
  - Location-based service is GOOD!
    - Landline-phone calling to 911 in the US, 112 in Europe
    - All cellular carrier since December 2005
  - RISK!
    - Location-based spam
    - Harm to a reputation
Other Uses

• Anonymous VoIP calls
• Anonymous acquisition of security patches
Other uses (Cont’d)

Sometimes abuses
• Avoid legislation (e.g., piracy)
• P2P sharing of copyright content
• Terrorism: communication with media
  – Mumbai attacks
Principle

Chaum ’81

Message 1

server 1

server 2

server 3

Message 2

Requirements: Privacy  
Efficiency  
Trust  
Robustness
Requirements

1. Privacy
   Nobody knows who said what

2. Efficiency
   Mixing is efficient (= practically useful)

3. Trust
   How many entities do we have to trust?

4. Robustness
   Will replacement cheaters be caught? What if a certain number of mix servers fail?
But what about robustness?

encr(Berry) →
encr(Kush) →
encr(Kush) →

STOP

There is no robustness!

I ignore his output

and produce my own

Kush → Kush → Kush

Kush
Zoology of Mix Networks

- Decryption Mix Nets [Cha81,...]:
  - Inputs: ciphertexts
  - Outputs: decryption of the inputs.

- Re-encryption Mix Nets [PIK93,...]:
  - Inputs: ciphertexts
  - Outputs: re-encryption of the inputs
First Solution

Chaum ’81, implemented by Syverson, Goldschlag

Not robust
(or: tolerates 0 cheaters for correctness)

Requires every server to participate
(and in the “right” order!)