Modelling and Analysing of Security Protocol: Lecture 9

Anonymous Protocols: Theory

Today’s Lecture

- Practical course issues.
- Theoretical anonymity.
  - Dinning Cryptographers Protocol
  - Definitions of Anonymity
  - The Crowds Protocol

BREAK

- Practical anonymous systems
  - Onion Routing and the Tor System
  - Mix Networks
  - Anonymous File-sharing Systems: MUTE
  - Anonymous Publishing: Freenet

The rest of the course

- Today: 12th Oct, Protocols for anonymity (homework)
- 19th Oct moved to 22nd Oct 11:15 to 13:00:
  - Model Checking & Fair exchange protocols.
- 26th Oct: Summary Lecture (Homework due)
- 2nd, 9th, 16th, 23rd and 30th Nov
  - Student presentations

Homework

- You have only got questions 1 and 2 back. You have not been told your mark for question 3.
- Attacks exist against some of your protocols.
- As part of the current homework you have to analysis your own protocol using ProVerif.
- If you can find and correct a fault in your protocol you will win back half the marks lost for that fault in homework 1.

Qu. 1: Typing attack

1. A → B : A
2. B → A : Nb
3. A → B : { A, B, Nb }Kas
4. B → S : { A, B, { A, B, Nb }Kas }Kbs
5. S → B : { A, B, Nb }Kbs

Qu. 2: Early SSL

1. A → B : E_{B}^{E}(Kab)
2. B → A : { Nb }_{Kab}
3. A → B : { CA, SignA( Nb ) }_{Kab}
Today's Lecture

- Practical course issues.
- Theoretical anonymity.
  - Dining Cryptographers Protocol
  - Definitions of Anonymity
  - The Crowds Protocol

BREAK

- Practical anonymous systems
  - Onion Routing and the Tor System
  - Mix Networks
  - Anonymous File-sharing Systems: MUTE
  - Anonymous Publishing: Freenet

IP address

- When you connect to another computer you send its IP address.
- It is ever hard to communicate well without revealing your real IP address.
- Recent court case (last week) decided that your IP address can be used to identify you in court.

“You have zero privacy anyway, get over it”

Scott, CEO of SUN microsystems.

Dining Cryptographers

- Nodes form a ring
- Each adjacent pair picks a random number
- Each node broadcasts the sum (xor) of the adjacent numbers
- The user who wants to send a message also adds the message
- The total sum (xor) is:

\[ r_1 + r_2 + r_3 + r_4 + r_5 + r_6 + r_7 + m = m \]

Dining Cryptographers

- It's impossible to tell who added m.
- Beyond suspicion even to a global attacker.
- Very inefficient: everyone must send the same amount of data as the real sender.

A Hierarchy of Goals
The Theory of Anonymity

Anonymity means different things to different users.
The right definitions are key to understand any system.

"On the Internet nobody knows you’re a dog"

The Theory of Anonymity

- Anonymity is a difficult notion to define.
  - Systems have multiple agents
  - which have different views of the system
  - and wish to hide different actions
  - to variable levels.
- Sometimes you just want some doubt, sometimes you want to act unseen.

The Theory of Anonymity

- In a system of anonymous communication you can be:
  - A sender
  - A receiver / responder
  - A helpful node in the system
  - An outsider (who may see all or just some of the communications)
- We might want anonymity for any of these, from any of these.

Some Kinds of Anonymity

- Sender anonymity.
- Receiver anonymity.
- Sender-receiver unlinkability.

For the
- Sender
- Receiver
- Another participant in the protocol.
- Outside observer that can see all/some of the network

Levels of Anonymity

Reiter and Rubin provide the classification:

- **Beyond suspicion**: the user appears no more likely to have acted than any other.
- **Probable innocence**: the user appears no more likely to have acted than to not to have.
- **Possible innocence**: there is a nontrivial probability that it was not the user.

Beyond suspicion

- All users are Beyond suspicion:

<table>
<thead>
<tr>
<th>Prob</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Beyond suspicion
• Not Beyond Suspicion:

Prob

A B C D E

Users

Probable Innocence
• All users are Probably Innocence

Prob

A B C D E

Users

Probable Innocence
• All users are Probably Innocence

Prob

A B C D E

Users

Probable Innocence
• All users are Probably Innocence

Prob

A B C D E

Users

Probable Innocence
• All users are Probably Innocence

Prob

A B C D E

Users
Possible Innocence

• There a small change it is not you.

<table>
<thead>
<tr>
<th>Prob</th>
<th>50%</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
</tr>
</tbody>
</table>

Users

Definitions

• These definitions do not take into account how likely each principal is to be guilty to start off with.

• Or quantify what the attack learns from a run of the protocol.

• This is currently a hot research topic, so far there are lots of complicated definitions but no clear winner.

Example: The Anonymizer

An Internet connection reveals your IP number.

The server knows The Anonymizer is being used.

The sender is Beyond Suspicion to the server.

The global observer knows you are using the "The Anonymizer"

There is no anonymity to the "The Anonymizer"

Example: The Anonymizer

A crowd is a group of n nodes

• The initiator selects randomly a node (called forwarder) and forwards the request to it

• A forwarder:
  - With prob. 1-p, selects randomly a new node and forwards the request to him
  - With prob. p, sends the request to the server

Example: The Anonymizer

• From the small print:
  • … we disclose personal information only in the good faith belief that we are required to do so by law, or that doing so is reasonably necessary …
  • … Note to European Customers: The information you provide us will be transferred outside the European Economic Area
Crowds

- The sender is beyond suspicion to the server.
- Some of the nodes could be corrupted.
- The initiator could forward the message to a corrupted node.
- The sender has probable innocence to other nodes.

Today’s Lecture

- Practical course issues.
- Theoretical anonymity.
  - Dimming Cryptographers Protocol
  - Definitions of Anonymity
  - The Crowds Protocol
- Practical anonymous systems
  - Onion Routing and the Tor System
  - Mix Networks
  - Anonymous File-sharing Systems: MUTE
  - Anonymous Publishing: Freenet

BREAK