Providing Anonymity Services in SIP

PIMRC 2008
Sept. 15, Cannes, France

L. Kazatzopoulos, K. Delakouridis, G.F. Marias
lkazatzo@aueb.gr, kodelak@aueb.gr, marias@aueb.gr
Session Initiation Protocol - SIP

- widely used for setting up and tearing down multimedia communication sessions (voice and video calls) over the Internet.

- Applications: video conferencing, streaming multimedia distribution, instant messaging, presence information

- creates, modifies, terminates two-party or multiparty sessions consisting of one or several media streams
SIP – Levels of anonymity

- **caller’s absolute anonymity**,  
  - the caller identity cannot be exposed by any other entity, or the attacker

- **caller’s eponymity only to the callee**,  
  - the identity of the caller should be revealed only to the callee

- **caller’s eponymity only to her/his provider**,  
  - the identity of the caller should be revealed only to the his/her provider

- **caller’s eponymity only to callee’s provider**,  
  - same as above, but for the peer’s provider
Candidate PETs

- Mixes
  - Pool Mixes
  - Stop and Go Mixes
  - Mixe-Nets
- DC-Networks
- Crowds
- Hordes
- Onion Routing
- Routing Through the Mist
Evaluation criteria of PETs

- Call establishment delay
- Cost
  - Computational
  - Communication overhead
- Scalability
- Protection level – robustness
  - Threats against anonymity
- Anonymity
  - of both caller and receiver
- Authentication
  - Supported or not?
## Evaluation criteria of PETs

<table>
<thead>
<tr>
<th></th>
<th>Scalability</th>
<th>Robustness</th>
<th>Call Delay</th>
<th>Anonymity</th>
<th>Authentication</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIXES</td>
<td>M</td>
<td>N</td>
<td>H</td>
<td>L</td>
<td>N</td>
<td>L</td>
</tr>
<tr>
<td>POOL MIXES</td>
<td>M</td>
<td>N</td>
<td>H</td>
<td>M</td>
<td>N</td>
<td>M</td>
</tr>
<tr>
<td>S &amp; G MIXES</td>
<td>M</td>
<td>N</td>
<td>M</td>
<td>M</td>
<td>N</td>
<td>M</td>
</tr>
<tr>
<td>MIXNETS</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>N</td>
<td>M</td>
</tr>
<tr>
<td>DC-NETS</td>
<td>L</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>N</td>
<td>M</td>
</tr>
<tr>
<td>CROWDS</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>L</td>
<td>N</td>
<td>L</td>
</tr>
<tr>
<td>HORDES</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>L</td>
<td>N</td>
<td>M</td>
</tr>
<tr>
<td>O.R</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>N</td>
<td>H</td>
</tr>
<tr>
<td>R.T.T.M</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>Y</td>
<td>H</td>
</tr>
</tbody>
</table>

- **H**: High
- **M**: Medium
- **L**: Low
- **Y**: Yes
- **N**: No
Best candidate: Mist

- Mist Routers is Hierarchical Structure
- Handle based communication
- Portal:
  - Mist Router – leaf node
  - Knowledge of user’s positions but not user’s ID
- Lighthouse:
  - Mist Router – Portal’s ancestor
  - Semi-trusted intermediate
  - Knowledge of user’s ID but not user’s physical position
Best candidate: Mist

- Mist Communication
  - Hierarchy definition and initialization
  - Registration to Portal
  - Registration to Lighthouse
  - Mist circuit establishment
  - Data Exchange
Mist Hierarchies

L: Lighthouse
P: Portal
R: Mist Router

User's A
Lighthouse

User's B
Lighthouse

User's A
Portal

User's B
Portal

User B

User A

Providing Anonymity Services in SIP
AUEB/Dept of Informatics/MMLAB
IEEE PIMRC 2008
Mist Initialization

Alice

Request for Registration

List of Mist Routers

Tokens for Selecting
Alice’s Lighthouse

Confirmation

Portal
Applying Mist on SIP

- Assumptions:
  - SIP Home Server acts as Mist Lighthouse
  - SIP Remote servers act as Mist Portals
  - SIP location service instead of user’s physical location will know the way to route packets to him.
  - Mist Hierarchy has been applied as overlay to the SIP Network
    - Add connections between the siblings of each level of the hierarchy
Establishing of a SIP Session through MIST

1. MIST [SIP [INVITE mother@dpi.com]]
2. MIST [mother@dpi.com]
3. MIST [Lighthouse Alice]
4. MISTe [SIP [INVITE mother@dpi.com]]
5. MIST [SIP [INVITE mother@dpi.com]]
6. MIST [P_Father (SIP [302: Moved temporarily])]
   contact: 3572@ffs.com
7. MIST [P_Father (SIP [302: Moved temporarily])]
   contact 3572@ffs.com
8. MIST [P_Father (SIP [302: Moved temporarily])]
   contact: 3572@ffs.com
9. MIST [SIP [ACK]]
10. MIST [SIP [ACK]]
11. MIST [SIP [ACK]]
12. SIP [INVITE 3572@ffs.com]
13. SIP [200: ACK]
14. SIP [ACK]
Advantages

- support untraceability of the packets routed through the Mist due to the distribution of knowledge (i.e., Portals know “where”, LIGs know “who”)
  - This preserves the privacy of the location of the users.
- For the users registered to the system using their nickname, assuming that the private keys have been issued based on this nickname:
  - anonymous communications are actually supported.
Further work

- Evaluate the proposal against privacy threats and vulnerabilities
- Measure anonymity
- Evaluate the proposal
  - Quantitative (delay, overhead, etc)
  - Real implementations under going
  - SIPp call generator
  - Soft clients
thank you

PIMRC 2008
Sept. 15, Cannes, France

L. Kazatzopoulos, K. Delakouridis, G.F. Marias
lkazatzo@aueb.gr, kodelak@aueb.gr, marias@aueb.gr