Outline

1. Introduction
   - Background
   - Session Initiation Protocol
2. Continuous authorizations in SIP
   - Architecture
   - Performance evaluation
3. Future work
4. Questions
Background

- Traditional access control models
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)
  - Role-based Access Control (RBAC)
- Usage Control ($\textit{UCON}_{ABC}$)
  - Subject and Object Attributes: mutable and immutable
  - Continuous enforcement of security policy
  - Authorizations (A): pre-Authorizations and ongoing-Authorizations
  - oBligations (B): pre-oBligations and ongoing-oBligations
  - Conditions (C)
- Session Initiation Protocol (SIP)
  - Application-layer signaling protocol for creating, modifying and terminating multimedia sessions
  - Examples: Internet telephone calls, multimedia distribution, and multimedia conferences
INVITE sip:user@aegean.gr SIP/2.0
Via: SIP/2.0/UDP pc33.pisa.it;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: User <sip:user@aegean.gr>
From: Giorgos <sip:gkar@iit.cnr.it>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.pisa.it
CSeq: 314159 INVITE
Contact: <sip:gkar@pc33.pisa.it>
Content-Type: application/sdp
Content-Length: 142
Continuous Authorizations in SIP with Usage Control

Session Initiation Protocol

SIP operation overview

1. INVITE
2. INVITE
3. 100 Trying
4. INVITE
5. 100 Trying
6. INVITE
7. 100 Trying
8. 180 Ringing
9. 180 Ringing
10. 180 Ringing
11. 180 Ringing
12. 200 OK
13. 200 OK
14. 200 OK
15. 200 OK
16. ACK
17. ACK
18. BYE
19. BYE
20. 200 OK
21. 200 OK

G. Karopoulos, P. Mori, F. Martinelli

IIT-CNR
Architecture
Testbed components

- B2BUA: Sippy
- SIP Proxy server: SIP Router
- Authorization server: PDP server supporting the UCON model, developed at IIT-CNR
- Attribute server: scripts that modify attribute values
- User Agents: Sipsak, SIPp

Machine 1 specifications:
- CPU: Dual-core Intel Core 2 6600 running on 2.4 GHz
- Memory: 2 GB
- OS: 32bit openSuSE Linux version 11.3, kernel version 2.6.34
- Software: SIPp user agents, SIP router, Sippy and the scripts for attribute update

Machine 2 specifications:
- CPU: Quad-core Intel Core i5 750 running on 2.67 GHz
- Memory: 8 GB
- OS: 64bit Ubuntu Linux version 10.10, kernel version 2.6.35
- Software: VMWare Player based Virtual Machine with the implementation of the PDP; the virtual machine is running a 32bit Ubuntu Linux version 9.10 with kernel version 2.6.31 using 1 GB of memory
Policy

Example of security policy in POLPA

\[
\text{tryaccess}(\text{user}, \text{net}, \text{sip\_call}(\text{call\_id})). \quad \text{line 1}
\]

\[
[(\text{user.reputation} \geq R)]. \quad \text{line 2}
\]

\[
\text{permitaccess}(\text{user}, \text{net}, \text{sip\_call}(\text{call\_id})). \quad \text{line 3}
\]

\[
( \quad \text{endaccess}(\text{user}, \text{net}, \text{sip\_call}(\text{call\_id})) \quad \text{line 4}
\]

\[
\text{or} \quad \text{or} \quad \text{or} \quad \text{or} \quad \text{or} \quad \text{or} \quad \text{or} \quad \text{or}
\]

\[
((\text{user.reputation} < R)]. \quad \text{line 6}
\]

\[
\text{revokeaccess}(\text{user}, \text{net}, \text{sip\_call}(\text{call\_id})) \quad \text{line 7}
\]

\[
); \quad \text{line 8}
\]
Experimental results

Mean delay of revoking a single SIP session

<table>
<thead>
<tr>
<th>Queue size</th>
<th>Mean delays (msecs)</th>
<th>PDP</th>
<th>SIP</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.9</td>
<td>1.7</td>
<td>2.6</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>1</td>
<td>2.2</td>
<td>3.2</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>1.1</td>
<td>2.7</td>
<td>3.8</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>1.3</td>
<td>2.6</td>
<td>3.9</td>
<td></td>
</tr>
<tr>
<td>400</td>
<td>1.3</td>
<td>2.6</td>
<td>3.9</td>
<td></td>
</tr>
<tr>
<td>500</td>
<td>1.4</td>
<td>2.6</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>600</td>
<td>1.5</td>
<td>2.6</td>
<td>4.1</td>
<td></td>
</tr>
<tr>
<td>700</td>
<td>1.6</td>
<td>2.7</td>
<td>4.3</td>
<td></td>
</tr>
<tr>
<td>800</td>
<td>1.7</td>
<td>3</td>
<td>4.7</td>
<td></td>
</tr>
<tr>
<td>900</td>
<td>1.8</td>
<td>3.3</td>
<td>5.1</td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td>2</td>
<td>2.9</td>
<td>4.9</td>
<td></td>
</tr>
</tbody>
</table>

Mean delay of revoking 5 SIP sessions simultaneously

<table>
<thead>
<tr>
<th>Queue size</th>
<th>Mean delays (msecs)</th>
<th>PDP</th>
<th>SIP</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1.8</td>
<td>8</td>
<td>9.8</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>1.9</td>
<td>8.3</td>
<td>10.2</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>2</td>
<td>9.3</td>
<td>11.3</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>2.1</td>
<td>8.6</td>
<td>10.7</td>
<td></td>
</tr>
<tr>
<td>400</td>
<td>2.3</td>
<td>8.7</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>500</td>
<td>2.3</td>
<td>9.2</td>
<td>11.5</td>
<td></td>
</tr>
<tr>
<td>600</td>
<td>2.4</td>
<td>9</td>
<td>11.4</td>
<td></td>
</tr>
<tr>
<td>700</td>
<td>2.5</td>
<td>9.7</td>
<td>12.2</td>
<td></td>
</tr>
<tr>
<td>800</td>
<td>2.6</td>
<td>10.7</td>
<td>13.3</td>
<td></td>
</tr>
<tr>
<td>900</td>
<td>2.7</td>
<td>9.7</td>
<td>12.4</td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td>2.8</td>
<td>10.9</td>
<td>13.7</td>
<td></td>
</tr>
</tbody>
</table>
Experimental results

Mean delay of revoking a single SIP session

![Graph showing mean delay of revoking a single SIP session](image)
Experimental results

Mean delay of revoking 5 SIP sessions simultaneously

![Graph showing mean delay of revoking 5 SIP sessions simultaneously]
Future work

- Implement scenarios with more complex security policies
- Fully implement UCON (Authorizations, oBligations and Conditions scenarios)
- Usage Control support in AAA/Diameter
Questions?