CARMA: Composable-Adaptive Resource Management Authorization for Ubiquitous Environments

Roberto Morales
Technical University of Catalonia
SPEDA
August, 2010
Outline

• Introduction
• CARM middleware
• CARM security
• CARM Authorization module
• Conclusions
• Diversity
  Mobile phones, PDAs, MP3, etc.

• Constraint resources or limited:
  CPU processing, memory, storage
  Built-in WiFi, Bluetooth, GPS, etc.
CARM: Composable-Adaptive Resource Manager

- The set of local resources can be shared spontaneously with other devices in the vicinity.
- Devices can improve local resources: by using more capable resources.
- Or, can augment their resources (limited devices): by using resources that are locally missing.
CARM: Composable-Adaptive Resource Manager

- CARM provides the infrastructure necessary to share and use resources according to its availability and user’s needs.
- Currently communications are done via Bluetooth, but CARM is flexible and is able to support additional communication technologies.
CARM: Composable-Adaptive Resource Manager

Display promotions

Ubiquitous displays

m-business

m-health
Owners are reluctant to allow the use of their shared resources for fear of potential adverse effects;
The use of peripherals is more likely to be granted if it’s under owner’s control and causes not ill effects.

CARMA: CARM Authorization model enables resource’s access control under user’s predefined conditions.
CARMA: CARM Authorization model

- Credential Validator (CV)
- Policy Manager (PM)
- Attribute Certificate Manager (ACM)
- Alerting System (AS)
- Blacklist

The *Messaging Manager* serves as the communication channel between CARMA and CARM’s core. Once user’s credentials have been validated (if granted) - resources will be delivered by the CARM’s core.
CARMA: mobile devices interaction
CARMA: AC and Policy format examples

a) AC basic format

```
IssueInstant="2010-05-10T09:37:56Z" Version="2.0"
<Subject>
  <SubjectctID>
    IMEI: AA-BBBBBB-CCCCCD
  </SubjectID>
</Subject>
<Issuer>
  BOB
</Issuer>
<Signature>
  <SignatureValue>
    BOB's signature :
    hq4zk+ZknjggCQgZm7ea8fI7...Hr7wHxvCCRwu
    bfZ6RqVIL+wNmeWI4=
  </SignatureValue>
</Signature>
<Conditions NotValidBefore="2010-05-10T09:38:45Z"
  NotValidAfter="2010-05-10T09:40:45Z">...
</Conditions>
<Attribute>
  <attributeValue>
    (group|guest)
  </attributeValue>
  ...
</Attribute>
```

b) Audio Resource Policy example

```
<policy policyId="audio resource policy"
  <policyIssuer>
    <value>Bob</value>
  </policyIssuer>
  <rule ruleId="audio rule" effect="permit">
    <target>
      <subject>
        <value>IMEI</value>
      </subject>
      <resource>
        <value>audio</value>
      </resource>
      <action>
        <value>play</value>
      </action>
    </target>
  </rule>
</policy>
```
CARMA: Communication protocol

MM: resource_req → resource_den

CV: Cert_validation yes → Res_req → AC_validation yes → Res_req → IMEI in blacklist? yes → res_denied

ACM: AC_denied → issued_AC → AC_req → Cert_validation no → Res_req → IMEI in blacklist? no → res_granted

PM: policy matching no → res_denied

Blacklist:

AS:
CARMA: Performance (initial evaluation)

<table>
<thead>
<tr>
<th>Action</th>
<th>Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>2644.8</td>
</tr>
<tr>
<td>Request</td>
<td>169.5</td>
</tr>
<tr>
<td>Relinquish</td>
<td>21.5</td>
</tr>
<tr>
<td>Disconnection</td>
<td>30.3</td>
</tr>
<tr>
<td>A/C Transmission</td>
<td>111.9</td>
</tr>
</tbody>
</table>

Nokia E65
Symbian OS v9.1
Series 60 3rd Edition
Audio speakers (medium quality)

Nokia 6600
Symbian OS v7.0s
Series 60 2nd Edition
Audio speakers (low quality)
Conclusions

• A security solution that enables automatic device authentication and authorization for resource sharing in pervasive environments was proposed.

• The security model does not represent a time consuming process, but due to power consumption constraints we need to test additional policy formats that requires less computing.
Thank you,

Questions?

Roberto Morales
rmorales@ac.upc.edu