Role-Based Cascaded Delegation:
A Decentralized Delegation Model for Roles

Roberto Tamassia
Brown University

Danfeng Yao
Brown University

William H. Winsborough
George Mason University
Resource Sharing and Delegation in Distributed Environment
Delegation chain

- Delegation is essential in distributed environment
  - KeyNote (Blaze Feigenbaum Ioannidis Keromytis 1998)
  - Trust Establishment (Herzberg Mass Michaeli et al. 2000)
  - X-Sec (Bertino Castano Ferrari 2001)
  - SPKI/SDSI (Clarke Elien Ellison et al. 2001)
  - OASIS (Bacon Moody Yao 2001)
  - RT framework (Li Winsborough Mitchell 2002)
  - PBDM (Zhang Oh Sandhu 2003)

- Delegation chain
  - Connects the resource owner to unknown ones

- Discovering and verifying delegation chains are two key issues
  - Discovery: find a delegation chain
  - Verification: authenticate the credentials on the chain
Existing role-based delegation model

- Storage of delegation credentials
  - Distributed across the network

- Distributed delegation chain discovery algorithms (Li Winsborough Mitchell 2003)
  - Traverse the graph of delegations

Bob is a member of Hospital.Guest
Credential chain discovery example

Brown -> Brown.prof -> Bob

CompanyA

Brown

UnivA

UnivB

UnivC

UnivD

UnivA.prof

UnivB.prof

UnivC.prof

UnivD.prof

CompanyA.manager -> UnivA.prof

CompanyB.manager -> UnivB.prof

CompanyB.manager -> UnivC.prof

CompanyB.manager -> UnivD.prof

GT.manager -> Brown.prof

H.Guest -> CompanyA.manager

H.Guest -> CompanyB.manager

H.Guest -> GenomeTech.manager
Distributed delegation chain discovery

- Flexible role-based delegation chain discovery
  - Linking arbitrary number of delegations
  - Issuing delegations independently

- Communication among credential servers
  - Complexity increases with the size of the credential graph

- Availability of credential servers
  - Participation of servers in discovery

- Privacy considerations
  - Revealing unrelated delegations
Cascaded delegation

- Efficient verification of a hierarchical delegation chain (Sollins 1988)
  - Accumulates certificates at each delegation transaction
  - Avoids certificate chain discovery
- Does not support the use of roles
  - Low scalability
- **Our approach**: combine Role-Based Access Control (RBAC) with cascaded delegation
  - No need to know role members
  - Unique delegation credential
  - No administrator participation in delegation
  - Low communication costs
Our model: Role-Based Cascaded Delegation (RBCD)

- The member of a role is given a role credential by the administrator

  - **Genome Tech** Manager → **John**

- Delegation of privileges is initialized by the resource owner and issued to a role

  - **Hospital** H.Guest → **GenomeTech.Manager** C₁

- Delegation may be further extended to others by any member of the role (intermediate delegator)

  - **John** H.Guest → **Brown.Professor** C₂

- Extension credential, role credential, and previous delegation credentials are issued (partial delegation credential)
  - **John** forwards C₁, Rⱼ, and C₂ to *professor at Brown*

- Requester submits the partial delegation credential, his role credential, and his signature to the verifier
  - **Bob** submits C₁, Rⱼ, C₂, his role credential Rₜ, and his signature Sₜ to **Hospital**
An example of RBCD

H → H.Guest → GenomeTech.Manager

John → H.Guest → Brown.prof

Request

Delegate

Hospital

Genome Tech Server

Professor

Brown University

Bob

Brown Server

C1

C2

C1

C1

C2

C1

C2

H.Guest

John

Manager

Genome Tech

Manager

GenomeTech.Manager
Advantages of RBCD model

- Avoidance of the distributed delegation chain discovery
  - Delegation chain is stored in the credentials
- High scalability because of the use of roles
  - Delegator does not have to know the members of a role
- Flexible and decentralized delegation
  - Delegation process does not require the participation of administrators
- Improved privacy protection
  - Unrelated credentials are not touched
- Low computation costs even if credentials are stored centrally
Implementing RBCD

- Requirements
  - Compact credential size
  - Efficient storage and transmission
  - Security of the scheme

- Our approach
  - Implementing RBCD model using Hierarchical Certificate-Based Encryption
Hierarchical Certificate-Based Encryption

- **HCBE scheme (Gentry 2003)**
  - Setup, Certify, Aggregate, Encrypt, Decrypt
  - Aggregated decryption key
    - CA signatures + User signature
  - Aggregate multiple signatures into one signature (Boneh et al. 2003)
  - Security

- **Size of signatures and public keys**
  - 170 bits with security comparable to 1024 bit RSA and 320 bit DSA (Boneh et al. 2001)

- **Response and challenge**
Our approach: using HCBE to realize RBCD

- **Genome Tech**
  - Public key: $PK_2$, Secret key: $SK_2$

- **Brown**
  - Public key: $PK_4$, Secret key: $SK_4$

- **Hospital**
  - Public key: $PK_1$, Secret key: $SK_1$

- **John**
  - Delegate
  - Aggregate($C_1$, $R_J$, $C'_2$)

- **Bob**
  - Delegate, Sign
  - Aggregate($C_2$, $R_B$, $S_B$)

- **Aggregate**
  - $C_1$, $R_J$, $C'_2$

- **Aggregate**
  - $C_2$, $R_B$, $S_B$
Performance comparisons between the RBCD implementation using RSA and HCBE

<table>
<thead>
<tr>
<th>Chain length n=20</th>
<th>Credential size (Kbits)</th>
<th>20 Kbit/s connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>RBCD using RSA</td>
<td>&gt; 81</td>
<td>&gt; 4s</td>
</tr>
<tr>
<td>RBCD using HCBE</td>
<td>&lt; 7</td>
<td>&lt; 0.35s</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Sign*</th>
<th>Verify*</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA (d = 1007-bit)</td>
<td>7.9ms</td>
<td>0.4ms</td>
</tr>
<tr>
<td>HCBE</td>
<td>3.57ms</td>
<td>~ 50ms</td>
</tr>
</tbody>
</table>

* Performed on 1GHz Pentium III (Barreto et al. 2002)

- **Verify(Chain) ~ |Chain|**
Conclusions

Contributions
- Role-Based Cascaded Delegation (RBCD) model
  - Eliminating credential chain discovery
  - Supporting decentralized delegation
  - Scalable
  - Minimizing exposure of sensitive credentials
- Implementation of RBCD using HCBE
  - Compact credentials

Future work
- Integration
  - Combining RT framework with RBCD
  - Using XACML as the policy language
- Experimental study
  - Detailed evaluation of communication and computation costs