Securing Information Transfer in Distributed Computing Environments

AbdulRahman A. Namankani
Out Line

- What does it mean?
- Identity Information
- Identity Trust Domain
- Security Analysis
- Security Requirement
- A suggestive solution
- Conclusion
What does it mean?

Securing Information Transfer in Distributed Computing Environment ...

A collection of loosely coupled processors interconnected by a communication network
Identity Information

- Cryptographic key
- Unsigned credentials
- Signed credentials
- Hypride credentials
User credentials

High-Level
- Credit-card info
- Digitally signed XML
- X.509 attribute certificate

Low-Level
- Hybrid credentials
- Unsigned credentials
- Signed credentials
- Protected keys
- Platform secrets
- Storage keys used to encrypt data
- Simple PKI certificate
- Pseudonyms to control access to resources
- Word document embedded with signed credential
- Salary documentation
Identity Trust Domain

Presistent
Mobile
Shared
Do we need to transfer Identity informations?
Call For a Solution

1. Maintain data conf.
3. Perform in a controlled manner
4. Prevent the policies corruption
5. Ensure the solution’s accountability and compliance with policy
Key Approaches

- Policy-based encryptions
- Tamper-resistant hardware during the migration
- Use a third parties to provide a basis for trust, accountability and policy checking
- Audited access to data, based on stated policy
Detour
• Security Policy
  – A statement of what is, and what is not, allowed
• Security Mechanism
  – Methods used to enforce the policy
• Threat
  – A potential violation of security
• Confidentiality: Keeping data and resources hidden
• Integrity: Preventing unauthorized modification
Encryptions

• Most computer encryption systems belong in one of two categories:
  – Symmetric-key encryption
  – Public-key encryption
## Control Access

<table>
<thead>
<tr>
<th></th>
<th>file1</th>
<th>file2</th>
<th>file3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andy</td>
<td>rx</td>
<td>r</td>
<td>rwo</td>
</tr>
<tr>
<td>Betty</td>
<td>rwxo</td>
<td>r</td>
<td></td>
</tr>
<tr>
<td>Charlie</td>
<td>rx</td>
<td>rwo</td>
<td>w</td>
</tr>
</tbody>
</table>
Back to the main topic ...
TCG

- Not-for-profit organization formed to
  - Develop
  - Define
  - and promote open standards
for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices.
TPM

• Trusted Platform Module
• Low-Cost TPMs are becoming commodities in business computing devices, laptops and desktops
• Act as a root of trust
• Used mainly to protect keys and other platform secrets and to exe cryptography operations
But ...

- TCG specifications are based on a monolithic platform
- TPM is bounded to that platform
- Requires the platform owner to explicitly authorize credential migration to specific destination platform
Additional requirement is needed !!
A Policy-Driven Migration

- Providing a mechanism to migrated user-credentials associated with policy that govern there use, security, accountability and privacy during the migration
- Adding a Trusted Third Party (TTP)
  - Address the problem of not knowing the dest. in advance
Credential-Management System (CMS)

- Security mechanism
- Running in local platform to protect credential
- Define how to migrate data
- Also, adding a trusted HW for encryption
- And adding the policy mech. to ensure that the target meet the required policy to receive data and key
The Root of Trust

[Diagram showing a network of resources and a credential management service (CMS).]
Policy

- Remotely verify the software state and identify the target platform as belonging to a known partner
- Migrate only within a given set of platforms
- Check for stated purposes for which data will be used in the new system
- TTP will be used as an interpreter for the policy
• We can relay on TCG protocols to migrate low-level user-credentials
• TPM act as a local credential and as a source for used authenticate
• TTP will be working as trusted authority and used to generate IBE decryption keys, the same entity as CMS
Example ...
Summary

• What does it mean?
• Identity Information
• Identity Trust Domain
• Security Analysis
• Security Requirement
• A suggestive solution
In Conclusion