Handling Identity Agent Compromise in User-Centric Identity Management Systems

Daisuke Mashima and Mustaque Ahamad
College of Computing, Georgia Institute of Technology

[1] Introduction

- User-centric identity management systems rely on local / network-resident identity agents (Local / Remote IdA)
  - Compromise of identity agents is a serious security concern
- User control over identity agents, such as revocation, recovery, and identity-usage monitoring is desirable
- We focus on an identity management architecture in which identity-related transactions require verification of identity owner's signature
  - Microsoft CardSpace, Credentica U-Prove, GUIDE-ME, etc.
- Novelty of our work includes:
  - Integration of threshold signature into user-centric identity management architecture
  - Use of a hardware storage token for the sake of revocation and recovery of identity agents
  - User-controllable usage monitoring by a trusted online agent

[2] Our Approach

- Eliminate a single point of attack
  - Keep user's private key largely off-line
  - Use threshold signature scheme
- Fast revocation of compromised identity agents
  - Do not need to involve CA
- Help users recognize the problem when identity agent compromise is suspected
  - Identity-Usage monitoring feature controllable by users

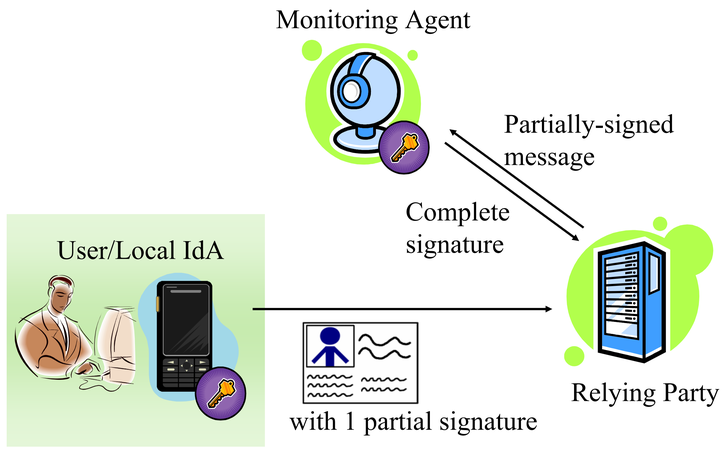
[3] Advantages of Our Approach

- Security
  - Private key can be mostly off-line
  - Compromise of a single entity does not allow identity misuse
  - Revocation can be done immediately by re-generating new key shares from original private key
- User-Centric Identity-Usage Monitoring
  - User has an option to use / not to use monitoring feature
  - When a user intends, Relying Party is required to contact his/her monitoring agent
- Recovery and Higher Availability
  - Even if any one of Local IdA, a storage token, and a monitoring agent is unavailable, users still can continue using services
  - Recovery can be done by re-distributing key shares to newly-configured entity or storage token

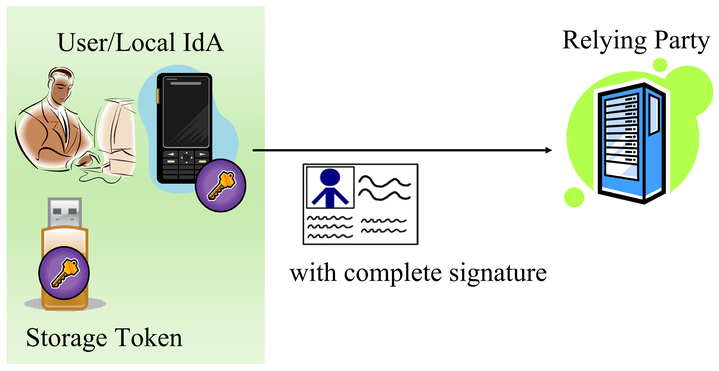
Overview of Our Approach

- Implementation in an architecture involving only Local IdA based on 2-3 threshold signature

In Case Storage Token Is Absent



In Case Storage Token Is Present

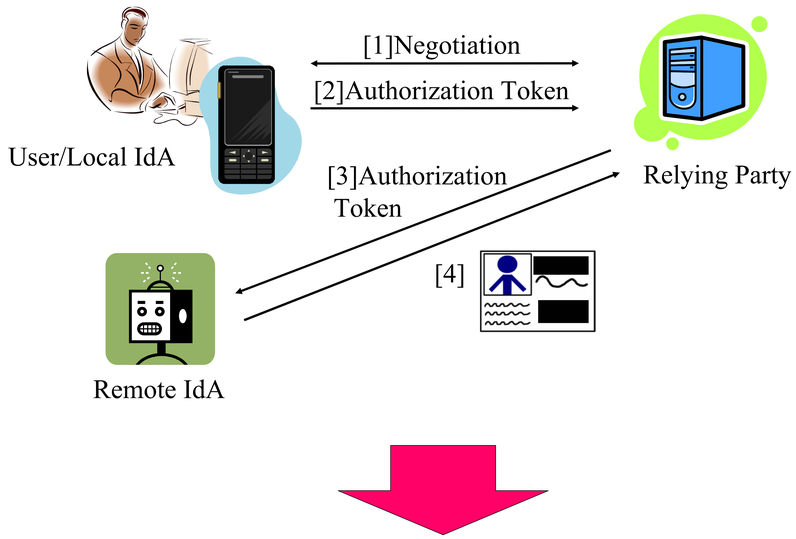


[4] Conclusion

- Demonstrated a novel usage of a storage token for revocation and recovery of identity agents and control over identity-usage monitoring feature
- Achieved robust and flexible user control over identity agents by utilizing threshold signature scheme in user-centric identity management systems
- Balanced security and privacy concerns by user-controllable identity-usage monitoring

[A] Implementation in Hybrid Architecture (GUIDE-ME)

Original GUIDE-ME Identity Management Environment



GUIDE-ME with Proposing Concept Based on 3-4 Threshold Signature