ADAPID E-GOVERNMENT APPLICATION:

PRIVACY-ENHANCED E-PETITIONS

Claudia Diaz

COSIC – K.U. Leuven

2nd ADAPID Workshop
28/09/2007
Petitions in the physical world

- Formal request addressed to an authority and signed by numerous individuals
- Typically citizens provide
  - Unique identifier (name, national ID number)
  - Signature
- Verification:
  - Validating that the signatures correspond to the identifiers
  - Discarding multiple/invalid signatures
Electronic petitions

- Benefits of going electronic:
  - Many resources are needed in order to physically collect the signatures
  - Manual signature verification is a costly and tedious process
  - Good example of ICT enabling participatory e-democracy
  - Electronic petitions have technically challenging requirements that make it an interesting application
The naive e-petition implementation

- Have users sign the petitions with their e-ID
  1. Select petition
  2. Sign using the e-ID (2-factor authentication)
  3. Check that the petition has not yet been signed with that e-ID
  4. Count (or discard) the signature

- Privacy risks
  - Leak sensitive information on political beliefs, religious inclinations, etc.
  - Through unique identifiers, petition signatures can be linked to other data
Basic requirements

- Authentication: citizen is who claims to be (i.e., no impersonation)
- Required attributes: citizen is entitled to sign (e.g., age > 18)
- Uniqueness: citizens sign a petition only once
- Correctness: all valid signatures are counted

Privacy requirements

- Citizen unlinkable to petition (i.e., not possible to identify who are the signers)
Anonymous credential protocols

- Active area of research in cryptography
- They rely on cryptographic protocols and Zero-Knowledge proofs to reduce to the bare minimum the amount of information disclosed
- Flexible protocols, many options possible
- Example:
  - CI issues a credential to U that encodes U’s age
  - U can prove to V that his age is above/below a threshold
  - V does not learn U’s exact age
  - V can check that this is certified by CI
## PKI vs anonymous credentials

<table>
<thead>
<tr>
<th>PKI</th>
<th>Anonymous credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signed by a trusted issuer</td>
<td>Signed by a trusted issuer</td>
</tr>
<tr>
<td>Certification of attributes</td>
<td>Certification of attributes</td>
</tr>
<tr>
<td>Authentication (secret key)</td>
<td>Authentication (secret key)</td>
</tr>
<tr>
<td>Double-signing detection</td>
<td>Double-signing detection</td>
</tr>
<tr>
<td>No data minimization</td>
<td>Data minimization</td>
</tr>
<tr>
<td>Users are identifiable</td>
<td>Users are anonymous</td>
</tr>
<tr>
<td>Users can be tracked (Signature linkable to other contexts where e-ID is used)</td>
<td>Users are unlinkable in different contexts</td>
</tr>
</tbody>
</table>
Protocol 1: obtaining a credential

1. Challenge

2. Valid?
   - PIN code
   - PIN blocked
   - Retry

3. Interactive credential generation

4. Credential storage
   - Check no credential has been issued to that e-ID
   - Check attributes
Protocol 2: signing the petition

5. Credential show + Petition signing

6. Multiple signing?
   - Yes
   - No

7. Count signature and store transcript
Properties

- Only citizens entitled to sign can do so
  - Possession of e-ID + knowledge of PIN
  - Attribute verification (e.g., age, locality)
  - One credential per citizen
- Citizens can sign only once (multiple signing is detectable so that repeated signatures can be deleted)
- Collusion of credential issuer and e-Petition server does not reveal the identity of a signer
Implemented in Java

Components:
- E-ID card, car reader and middleware
- SSL/TLS client-server communication
- Anonymous credential protocols (extension of currently available primitives provided by Idemix)
- Graphical user interfaces

Proof-of-concept
- Security with lowest required level of identification
- e-ID can be used to bootstrap secure and privacy friendly identity management
Open issues

- Improved implementation
- Allow citizens to add petitions
- Secure storage for the user master secret
- Prevent timing and traffic analysis attacks
Summary and conclusions

- Motivated the choice of e-petition applications
- Combined and extended various building blocks to implement privacy-enhanced e-petitions
- Overview of protocols and properties
- Security properties can be achieved without identifiability
Thank you!