Prospects for Using Privacy-Enhancing Technologies in the NSTIC Ecosystem

NIST Workshop on Privacy-Enhancing Crypto

Panel on Privacy in the Identification Domain

Francisco Corella

Pomcor

Pros and Cons of U-Prove

- Provides issue-show unlinkability
- Does NOT provide multi-show unlinkability
- Provides selective disclosure of attributes, but no proof that integer lies in interval
  - That would require many auxiliary proofs
- No revocation by issuer

Revocation Methods Mentioned by U-Prove Documents

- Blacklist the Token Id
  - Id not visible to issuer => issuer cannot revoke
- Blacklist serial # included in Token Info Field
  - Info field visible to all => full linkability
- Blacklist serial # stored in undisclosed attribute
  - Would require one NOT proof per revoked credential
- Revoke smart card rather than token
  - Smart card must be tamper proof against user
  - CRL increment must be downloaded to smart card
- On-demand token
  - Impacts presentation performance
  - Allows issue-show linkability by timing correlation

Pros and Cons of Idemix

- Full privacy features
  - Issue-show and multi-show unlinkability
  - Selective disclosure of attributes
  - Proof that integer lies in interval
- Performance?
  - Only available figures: presentation takes 12-28s

    2002, 1.1GHz, 1024-bit modulus, possible optimizations mentioned
- No revocation
  - Instead: short term credential, update of expiration time

Idemix Java Card

- “Idemix light”: very different crypto properties
- Security relies on card being tamper proof against user
- Presentation takes 10-12s
- Revocation requires knowledge of private key, which is kept in the tamper proof card and known to no one

Are PETs really needed for NSTIC?

Yes, but only for limited use cases

- Not needed for anonymous login to Web site
  - Site can issue its own PK certificate
- Not useful if disclosed attributes uniquely identify user
  - User can be tracked by attributes
- Useful if disclosed attributes do not uniquely identify user
  - Examples?

Deployment and Usability

Credentials:

- Must reside in browser
- Must be supported by core Web protocols: HTTP, TLS
- Must be issued and imported into browser automatically

Recap of Revocation Methods and Alternatives

- Dynamic accumulators
  - [Camenish,Lysyanskaya-2002]
  - [Boneh,Boyen,Shacham-2004]
  - Proven that witness is not accumulated adds time to presentation proof
  - Prover must access issuer periodically to update witness
- Dynamic accumulator, fast witness update by issuer
  - [Camenisch,Kohlweiss,Soriente-2009]
  - Issuer needs very large data structure
- Dynamic universal accumulator
  - [Li,Li,Xue-2007]
  - [Au,Tsang,Susilo,Mu-2009]
  - Accumulator changes less frequently
- Split dynamic universal accumulator (+delegation)
  - [Acar,Nguyen-2011]
  - Less frequent witness updates

- Proof that undisclosed serial # not in CRL, O(R)
  - Mentioned in [Brands,Demuynck,DeDecker-2007]
  - Suggested in U-Prove documentation, not implemented
  - One proof per serial # in list
- Proof that undisclosed serial # not in CRL, O($\sqrt{R}$)
  - [Brands,Demuynck,DeDecker-2007]
  - Verifier-driven, issuer can’t revoke
  - Prover must retrieve CRLs from all verifiers
  - Adds non-constant time to presentation proof
- Proof that undisclosed serial # not in CRL, O(1)
  - [Nakanishi,Fujii,Hira,Funabiki-2010]
  - Prover must obtain entire revocation list (no increments)
- Verifier-local revocation
  - [Boneh,Shacham-2004]
  - Requires knowledge of private key
  - Revoking credentials become linkable

- On-demand credentials
  - U-PROVE
  - Expensive presentation: requires issuing a new token
  - Issue-show linkability by timing correlation
- Short term credentials with expiration update
  - [Camenisch,Kohlweiss,Soriente-2010]
  - IDEMIX
  - Expensive for issuer