

CSRG :: DAA

Ben Smyth

16th October 2006

Note: if you are viewing these slides after the presentation you will have missed the material presented on the whiteboard (i.e. the interesting bits!)

What does TC give us?

- Hardware device called a Trusted Platform Module (TPM)
- Client can make cryptographically strong guarantees about its state (attestation)
- Server can make educated decisions as to whether to trust the client
- Example applications
 - Banking industry/corporate networks (min specs)
 - Grid applications (software/data integrity)

What about privacy?

- TPM can be uniquely identified
- Personal identity can be linked to TPM
- Loss of privacy
- Privacy preserving protocols satisfy:
 - Anonymity: Cannot link action to agent
 - Unlinkability (relationship anonymity): Given two or more actions originating from the same agent it is not possible to link them

Privacy preserving solutions

- Single shared secret
- Trusted Third Party (TTP)–previous spec
 - TTP is bottleneck
 - TTP/verifier collusion (probably fixable using blind signatures)
- Direct Anonymous Attestation (DAA)–spec v1.2
 - Direct (proof): without TTP
 - Anonymous: identity of TPM not revealed
 - Attestation: (trusted) claim from TPM

Cryptographic primitives

- Public key encryption
- Secure hash functions
- Digital signature schemes
 - Blind signatures
 - Group signatures
- Zero knowledge protocols

Group Signatures

- Group signatures
 - Group member can sign on behalf of group
 - Requires trusted *group manager* to add members
 - Group manager can revoke anonymity

Zero knowledge protocols

- Zero knowledge proof (ZKP)
 - Prover A convinces verifier B that an element y is a member of group g
- Zero knowledge proof of knowledge (PK)
 - ZKP leak information, verifier learns y belongs to g
 - Prover shows knowledge of y with respect to g
- PK can be turned into a signature scheme (SPK)

DAA protocol

- Group signature scheme without ability to revoke anonymity
- Mechanism to detect rogue members
- Differing degrees of privacy (unlinkability)
- Minimise computation load on TPM
 - Offload any operation which doesn't compromise security
 - Privacy need only by guaranteed if the host is not corrupt

DAA protocol

- Players

- Issuer (similar to the group manager)
- Host/TPM
- Verifier

- Protocols

- Join: Issuer and host interaction to enable host to become a group member (i.e. obtain attestation)
- Sign/verify: Host and verifier interact to convince the verifier that the host has obtained attestation (i.e. is a group member)

DAA protocol

- Issuer might not want to issue too many credentials to a TPM, re-issue instead
- Verifier wants to be able to detect keys originating from rogue TPMs
- Signer and verifier may agree to enable verifier specific linkability
 - Note: this could allow a service provider to deny requests after n attempts

Summary of issues with DAA

- Extracted EKs can be used to obtain attestation
 - Simple fix requires certificate revocation list (CRL)
- Issuer and Verifier can collude to break anonymity
 - Simple fix requires swapping a 1 for a 0
- (Currently looking into a possible) Man in the middle attack to allow an attacker to convince a verifier that they have attestation

Future work and observations

- Research alternative approaches to remote anonymous attestation to reduce complexity
 - The join protocol essential requires a blind signature on some value along with proofs that values are correctly formed... There must be a simpler way?
- Prove privacy properties using ProVerif