

Privacy-Preserving Delegation of Digital Credentials

Carlisle Adams

Auth'n and Auth'z

- Authentication: *who you are*
- Authorization: *what you're allowed to do*
 - Need to prove to the guard that you own the credentials required for access
 - Often, this proof is done implicitly (through the medium of identity)
 - Privacy-preserving authorization: no identity
 - Login to a members-only website anonymously?

Digital Credentials

- Brands (*Rethinking PKIs and Dig. Certs*)
 - Your credentials: encoded into your public key
 - Your public key: certified by a trusted authority
 - Digital signature on public key means that the authority warrants that (i) there are credentials encoded into this key, and (ii) whoever knows the private key corresponding to this public key is the legitimate owner of these credentials
 - In a transaction: you prove credential ownership
 - You reveal your certificate (i.e., public key and authority's signature on this public key) to the guard
 - The guard removes the required credentials from the public key (pk becomes pk'), and you show that you know the private key corresponding to this modified public key, pk'

Delegation

- Original proposal for digital credentials ensures that credentials cannot be passed on (e.g., sensitive information encoded into key so that you can't give any credentials to another entity without also giving this information)
- However, in many environments (e.g., business), there are legitimate requirements for constrained credential delegation (e.g., mgr. on vacation)

Delegation of Digital Credentials

- Delegator (A), Delagatee (D), Guard (G)
 - Key pairs are created for the delagatee and the guard; these have a mathematical relationship to the delagator's key pair. All three public keys are certified by the authority
 - Scenario 1:
 - A reveals some credentials to D , who can now prove ownership of any subset of these to G (using D 's certificate, A 's certificate, and G 's certificate), without revealing others
 - Scenario 2:
 - A reveals some information to G but not to D , such that D is able to prove ownership of certain credentials to G without either entity knowing the actual credential values

Importance

- Digital Credentials
 - Allow entities to choose which attributes to reveal to whom in particular situations
- In many environments
 - An entity may wish / need to “lend” some attributes to another entity (typically subject to some constraints) so that specific transactions can occur
- Goal of this work:
 - To marry the above two notions, to maintain user choice in what attributes are revealed, even when they are temporarily given to another entity