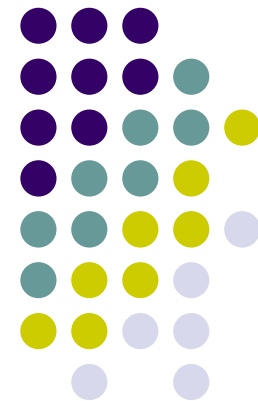


Delegation and Proxy Services in Digital Credential Environments

Carlisle Adams
School of Information Technology and Engineering
University of Ottawa



Outline



- Digital Credentials technology
- Additional Real-World Entities to Consider
- Delegation (Business Users)
- Proxy Service (“Ordinary” Users)
- Conclusions & Future Work

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; i.e., through authentication)
 - 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, h
 - 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 (h becomes h'), and you show that you know the private key corresponding to this modified public key, h'

Issuing Protocol



Alice

CA

a, PK

Random a , public key PK



$h = \text{Alice's public key} = f(\text{Alice's attribute values}, PK)$

$c = f(h, a)$

$c, \text{ attribute values}$



$r = f(c, \text{CA's private key})$

r



$c' = f(c)$

$r' = f(r)$

Alice's digital credential is h and the CA's signature on h is (c', r')

Showing Protocol



Alice

Bob

m

Nonce m



$r_i = f(\text{Alice's secret attribute values}, m)$

$h, (c', r'), r_i$ claimed attribute values



$h' = f(h, m)$

Are r_i and the *claimed attributes* a private key for h' ?

Our Research



- Our work has focused on modifying / extending Brands' protocols to make them more suitable for two practical, real-world types of people
 - Business users (delegation of credentials in a corporate setting)
 - *Joint work with David Knox*
 - “Ordinary” users (use of a constrained device with limited memory and processing power)
 - *Joint work with Daniel Shapiro and Vishal Thareja*

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 business environments, there are legitimate requirements for constrained credential delegation (e.g., manager on vacation)

Delegation of Credentials



- Delegator (A), Delagatee (D), Verifier (B)
 - Key pairs are created for the delagatee and the verifier; these have a mathematical relationship to the delagator's key pair. All three public keys are certified by the authority.

Digital Credential “Triples”



$$h_A = \left(g_1^{x_1} \square g_2^{x_2} \square \dots \square g_l^{x_l} \square h_1 \right)^{\beta\delta}$$

$$h_D = \left(g_1^{(x_1-m_1)} \square g_2^{(x_2-m_2)} \square \dots \square g_l^{(x_l-m_l)} \square h_2 \right)^{\delta}$$

$$h_B = \left(g_1^{m_1} \square g_2^{m_2} \square \dots \square g_l^{m_l} \square h_3 \right)^{\beta}$$

Where $h_1 \square h_2 \square h_3$

So that $h_D^{\beta} \square h_B^{\delta} = h_A$

Delegation of Credentials



- Delegator (A), Delagatee (D), Verifier (B)
 - A gives the (x_i, m_i) values to Del along with the secret value *delta*, and gives the secret value *beta* to Bob
 - **Scenario 1:**
 - A reveals some credentials to D (by revealing the corresponding m_i values). D can now prove ownership of any subset of these to B (using D 's certificate, A 's certificate, and B 's certificate), without revealing others
 - **Scenario 2:**
 - A reveals m_i values to B but not to D . D is able to prove ownership of (x_i, m_i) values to B so that B learns x_i values but D does not
 - **Scenario 3:**
 - A reveals m_i values to B but not to D . D is able to prove properties of corresponding credentials to B without either entity being able to determine the actual credential values
- Any of these may be useful in a corporate environment
- **A decides who she wants to trust, and to what extent**

Our Research



- Our work has focused on modifying / extending Brands' protocols to make them more suitable for two practical, real-world types of people
 - Business users (delegation of credentials in a corporate setting)
 - *Joint work with David Knox*
 - Ordinary users (use of a constrained device with limited memory and processing power)
 - *Joint work with Daniel Shapiro and Vishal Thareja*

Constrained Devices

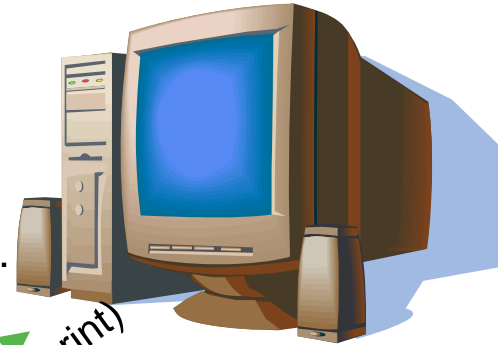


- In many real-world situations,
 - Alice may not have her digital credentials physically with her (and/or may not have the protocol engine and processing power to engage in the required showing protocol)
 - In particular, Alice may have only a cell phone or PDA with her (very common scenario these days)
- How can we incorporate digital credentials in such environments?
 - Use a proxy service...

Overall Architecture



Proxy stores (blinded) dig. cred.



1
Biometric (voice print)
over SSL to Login

2
Normal showing
protocol, but giving
proof of blinded
credentials

3
Graphical pwd
over SSL
to unblind cred.
(authorize trans.)



Proxy Service



- Alice has a proxy service to store her (blinded) digital credential, and to engage in the showing protocol on her behalf
- Alice uses her constrained device (e.g., cell phone) to log into / initiate the proxy, and to authorize the completed transaction (unblind the relevant attributes) at the verifier
- **Alice is able to use digital credentials technology without a powerful laptop and without having to place undue trust in the proxy**

Conclusions



- Digital Credentials
 - Allow entities to choose which attributes to reveal to whom in particular situations (potentially an important tool in helping to prevent identity theft)
- 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
 - An entity may wish / need to “outsource” storage and processing to a proxy service and use only a constrained device (such as a cell phone or PDA)
- Goal of this work:
 - To combine the above notions: **to maintain user choice in what attributes are revealed, even when they are held by another entity**

Directions for Further Work



- Implementation and analysis of proposals
 - Complexity, usability, performance impact, etc.
- Other extensions for additional environments
 - What other real-world entities may be able to usefully employ digital credential technology?