TrustBuilder: Authorization and Authentication for Open Systems

M. Winslett, A. Lee, L. Olson, M. Rosulek
University of Illinois

K. E. Seamons
Brigham Young University
Motivation: Open System Security

- In open systems, resources are shared across organizational boundaries
  - Examples: supply chain management, web services, grid computing, peer-to-peer systems, semantic web, disaster response, joint military activities

- When users come from outside the organization, their identity is insufficient to determine their access rights
  - The dynamic nature of open systems makes preregistration impractical and unscalable

- Proposed solution: trust negotiation, a new approach to authentication and authorization for open systems
Trust Negotiation Basics

- Every resource in the open system must be protected by an access control policy
  - Policy describes the attributes that users must possess to access the resource, in terms of the digital credentials that they must present to gain access
  - Resources can include services, roles, capabilities, files, directories, credentials themselves, and even access control policies
- Digital credentials are verifiable, unforgeable statements made by the credential issuer about one or more subjects
  - Examples: X. 509 employee IDs, patient cards, driver’s licenses, diplomas
- An attempt to access a resource triggers a negotiation: a bilateral iterative disclosure of credentials and requests for credentials
Step 1: Alice requests a service from Bob

Step 2: Bob discloses his policy for the service

Step 3: Alice discloses her policy for her VISA card

Step 4: Bob discloses his BBB credential

Step 5: Alice discloses her VISA card credential

Step 6: Bob grants access to the service
Research Goal and Strategy

■ Goal: ubiquitous trust negotiation facilities, so trust negotiation is available whenever and wherever needed

■ Strategy for reaching goal
  ● Theory
    ➢ Develop theoretical guidelines to preserve negotiating parties’ autonomy while still guaranteeing that trust will be established whenever possible, for negotiations involving any number of parties
  ● Systems
    ➢ Develop modular, scalable, reusable implementations of trust negotiation
    ➢ Deploy them in every widely used communications protocol: deployed in SSL/TLS, SMTP, SSH, HTTPS; underway in IPSec, GridFTP, and others
Trust Negotiation Architecture

A TrustBuilder Security Agent (left) is deployed everywhere the handshake icon appears above.
Example: Foiling Phishing Attacks

- Phishing attack extracts private information, such as eBay logins and passwords, from unwary users via legitimate-seeming email and web sites.

- Content-triggered trust negotiation filters outgoing content, looking for predetermined types of sensitive information (e.g., logins and passwords) using standard IR techniques (SMTP version shown above at right).

- A trust negotiation session is triggered with the intended recipient of sensitive outgoing information, using predetermined access control policies for that type of information (e.g., eBay login/password only goes to eBay).

- Phishing pirate site cannot satisfy the policy, so the content is not sent.

Possible URL spoofing attack:
http://pages.ebay.com/reactivate[null]@steal_your_identity.com