Trust Negotiation: Authorization for Virtual Organizations

M. Winslett  University of Illinois at Urbana-Champaign
A. J. Lee  University of Pittsburgh
K. Perano  Sandia National Laboratories

Competitive pressures and market forces are dissolving boundaries between organizations
Trust negotiation can help!

- Authorization policy for every open-system resource
- Digital credentials: verifiable, unforgeable attribute attestations
- Run-time negotiation triggered by access attempt

Trust Negotiation E-business Example

Alice

- BBB Member?
- BBB credential.

Bob

- VISA employee ID.
- Access granted.
Trust negotiation approaches to authorization have a number of advantages

Primary advantage: *reduced maintenance overhead*

Secondary benefits:
- Bilateral establishment of trust
- Iterative protocols
- Automated construction of *machine-verifiable* proofs

TrustBuilder2 is a framework for experimenting with TN

- Open source
- [http://dais.cs.uiuc.edu/tn](http://dais.cs.uiuc.edu/tn)
- Over 300 downloads
A compliance checker determines \textit{if} and \textit{how} some policy can be satisfied

- Credentials returned form a \textit{satisfying set}
- One or more satisfying sets \textit{must} be returned if the policy can be satisfied
- Definition of policy satisfaction depends on policy language semantics

\textbf{Problem: theorem-proving is slow}

Clouseau avoids theorem-proving by compiling policies down into a low-level language that can be checked using RETE

Existing policy languages (e.g., \textit{RT}, \textit{WS-SecurityPolicy})
Pattern matching is much faster than previous approaches to compliance checking.

Traust allows legacy applications to take advantage of trust negotiation.
Traust protocol overview

Client Features:
- User-defined sensitivity levels
- OpenAPI (request classification)
- Subnets
- Credential caching

Server Features:
- No single sign of protection
- High trust or low entropy
- Can provide both static and dynamically acquired credentials

TLS Tunnel

1. TRM to Protect Sensitive Resource Request
2. Resource Request
3. TRM to Determine Client Authorization
4. Credentials Needed to Access Resource

After Alice discloses enough credentials to satisfy the resource access policy, the Trust server issues a one or more credentials that she can use to access the requested resource. These credentials could be, but are not limited to, X.509 certificates, SAML assertions, or Kerberos tickets.

 DisasterNET Login

Pasadena Earthquake

At 8:13am this morning, a powerful earthquake caused the number of homes and businesses in the Pasadena area to collapse. This website acts as a portal to coordinate the efforts of the many groups involved in the effort to locate the survivors still trapped in the wreckage. To log in, click the link corresponding to your skill set, below.

I am a...
- Fire or Rescue worker
- Police Officer
- Rescue Dog Handler
- Veterinarian
- Social Worker
Traust trust negotiation overview

**Step 1:** Handler releases request disclosure policy

**Step 2:** DisasterResponseCoordinator credential

**Step 3:** Request access using role "Handler"

**Step 4:** Handler access policy

**Step 5:** SearchTeam credential and access policies

**Step 6:** Privacy policy and StateDepartment credential

**Step 7:** Medical records and drivers license

**Step 8:** Password sent to Handler

Client establishes trust with previously unknown Traust server via TN

Server establishes trust with previously unknown client via TN
We are looking for funding, partners for a trial deployment of trust negotiation

- Based on TrustBuilder2, Clouseau, possibly Traust
- Potential apps
  - Emergency response @ Sandia
  - Others?

Our goal: identify, fix whatever additional problems may hinder deployment

Contact us at winslett@cs.uiuc.edu