The Quest for Single-Sign On

Prof. Ravi Sandhu
Executive Director and Endowed Chair

February 8, 2013

ravi.sandhu@utsa.edu
www.profsandhu.com
We will discuss SSO separately.

- Initial authentication
- Session establishment and maintenance to authentication server
- Authentication to multiple servers
- Session establishment and maintenance at multiple servers
- Single logout
User-Authenticator-Attribute Triangle

User

Attribute

Authenticator
User-Authenticator-Attribute Triangle

1990s

User

X.509 attribute certificate

Attribute

SPKI certificate

Authenticator

X.509 identity certificate
Taxonomy 2003

Pseudo SSO  
Identity to SP is n to 1

True SSO  
Identity to SP is n to m

SSO: single sign on  
SP: service provider (also called relying party)  
ASP: authentication service provider
Local: to user platform
Proxy: provided by external platform

- Local, Pseudo
- Proxy, Pseudo
- Local, True
- Proxy, True

3.1 and 3.2
Pseudo SSO: authenticate
True SSO: pass assertions
PKI (Public Key Infrastructure) does not fall neatly into this characterization.

Authenticated, confidential channels
2-way SSL also known as mutually authenticated SSL