Federated Identity and Single-Sign On

Prof. Ravi Sandhu
Executive Director and Endowed Chair

February 15, 2013

ravi.sandhu@utsa.edu
www.profsandhu.com
The Web Today

User ID, Password
+ maybe:
Personalized image
Cookie
Knowledge based authentication
One-time password

Client

RP1

RP2

RP3

Relying Parties
(Service Providers)

Encrypted channel
Weak RP to client authentication
Susceptible to RP spoofing and man-in-the-middle
The Web Today

Client

User ID, Password
+ maybe:
Personalized image
Cookie
Knowledge based authentication
One-time password

RP1
Private Key
Public Key

RP2
Private Key
Public Key

RP3
Private Key
Public Key

Encrypted channel
**Weak RP to client authentication**
**Susceptible to RP spoofing and man-in-the-middle**

Signature: done by Private Key, Verified by Public Key
Encryption: done by Public Key, Decrypted by Private Key
How to get a public key?
Digital Certificates

PKI: Public Key Infrastructure

Guarantees authentication and integrity
But how does one verify this signature
Need another Public Key
The Web Today

Root certificates are weakly protected in today’s browsers

Multi-rooted Certificate Hierarchy
The PKI Vision (1980s Onwards)

- Relying Parties (Service Providers)
  - RP1
    - Private Key
    - Public Key
  - RP2
    - Private Key
    - Public Key
  - RP3
    - Private Key
    - Public Key

Client
- Private Key
- Public Key

The PKI Vision (1980s Onwards)

- Store as password protected and use in insecure PC
- Store and use in smartcard
- Store and use in Trusted Platform Module (TPM)

Relying Parties (Service Providers)

Client

- Private Key
- Public Key

RP1

- Private Key
- Public Key

RP2

- Private Key
- Public Key

RP3

- Private Key
- Public Key

Store and use in
- well protected server
- hardware security module (HSM)
The PKI Vision (1980s Onwards)

- One authenticator for each client
  - Protected by one or more additional factors

- Usable by every RP who trusts the client’s root

- Built-in out-of-the box Single Sign-On (SSO)

- Massive expense by US DoD on Common Access Card
Kerberos SSO (1980’s onward)

Symmetric Key Technology

Stored client symmetric key $K_c$

Client password $\rightarrow$ client symmetric key $K_c$

1. Client
2. Kerberos also TGS

Client

Kerberos also TGS

$\{T_{c,tgs}, K_{c,tgs}\}^{K_c}$

$C$
Kerberos SSO (1980’s onward)

Symmetric Key Technology

T_{c,tgs}, A_{c,tgs}, s

\{T_{c,s}, K_{c,s}\} K_{c,tgs}

3

4

Client

TGS

Server

T_{c,s}, A_{c,s}
Kerberos SSO (1980’s onward)

- shared symmetric key
- public-private keys
Kerberos SSO (1980’s onward)

- Successful in Enterprise SSO
  - Scales to 10’s or 100’s of thousands of users

- Microsoft Active Directory login is based on Kerberos

- Inter-realm rarely deployed
Microsoft SSO (1990’s)

Failed
Microsoft Infocard Identity Ecosystem (2000’s)

Failed
Liberty Alliance (2000’s)

Failed
NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

Enhancing Online Choice, Efficiency, Security, and Privacy

APRIL 2011