Federated Identity in OneHealthPort

Ravi Sandhu*
Chief Scientist
NSD Security
www.nsdsecurity.com
sandhu@nsdsecurity.com
703.283.3484

*Also Professor of Information Security and Assurance at George Mason University, Fairfax, Virginia
Outline

• What is security?
• What is OneHealthPort?
• What is OneHealthPort federated identity?
• What is the technology behind OneHealthPort federated identity?
What is Security

• Catastrophic failure is a whole lot worse than occasional failure
• A single multi-functional infrastructure is better than multiple stovepipes
• Good enough security
  – Is all we can achieve
  – Tolerates occasional failure
  – Does not tolerate catastrophic failure
Security is Only One Objective

- Ease of Use
- Security
- Total Cost of Ownership
- Integrated, identity management infrastructure
What is OneHealthPort?

• What is OneHealthPort (OHP)?
The technology behind OneHealthPort

OneHealthPort

Betrusted
Providing Trust Worldwide

NSD Security

Secure Identity Appliance®

FIPS 140-1 COMPLIANT

identrus
COMPLIANT
What is OneHealthPort federated identity?

• **OHP Overview**
• **OHP Process Overview**
• **OHP Registration Flow**
Use case 1: Subscriber has no Cookies
Gets OHP Cookie (planted by OHP at beTRUSTed) and PMI Cookie (planted by Relying Party)
Use case 2: Subscriber has PMI Cookie (planted by Relying Party)
Use case 3: Subscriber has OHP Cookie but no PMI Cookie

User browses to the Relying Party Application via a bookmark.

Does the User have a PMI cookie?

Yes

Web Page Displayed

No

Generate an OHP cookie

Generate an OHP cookie

Redirect to PMI Login Server

Does the User have an OHP cookie?

Yes

Redirect to OHP Login Page

Are credentials correct?

User enters OHP Credentials

User enters PMI Credentials

No

Are credentials correct?

Redirect to OHP Login Page

User enters OHP Credentials

Error Page Displayed

XXX = Stop

XXX = Decision

XXX = Action
Security Appliances

- Dedicated (but COTS) hardware
- Hardened OS
- Managed by restricted protocols (no root access)
- Highly available, scalable and secure
Authentication Ladder

- Weak Password Systems, Catastrophic Dictionary attacks
- Secure Identity Appliance
- Zero Footprint
  Hardened Password
- Roaming PKI
- Two-factor (with optional PKI)
  Password plus USB token or variant
- No change for users
- No change for issuer
- No password file (PKI hardened)

Password Usability
PKI Security
2-Key RSA vs. 3-Key RSA

**Old PKI**

**Keys:**
- a) Alice Public = e
- b) Alice Private = d
- c) Alice Cert = C

**Signing:**
- a) S = Sign(M,d)

Send [S, C] to Bob

**Bob:**
- Gets e from C
- Does Verify(S,e) = M?

**Practical PKI**

**Keys:**
- a) Alice Public = e
- b) Alice password = d1
- c) Alice Cert = C
- d) Alice appliance key = d2

**Signing:**
- a) Alice logs on to appliance using strong authentication and creates secure channel
- b) Spartial = Sign(M,d2)
- c) S = Sign(Spartial,d1)

Send [S, C] to Bob

**Bob:**
- Gets e from C
- Does Verify(S,e) = M?
Role-Based Management

Authorization profiles are managed in terms of roles

Administration is delegated in terms of identity management roles
Appliance Management Roles

- Supermanager
  - Not your usual root user
- Security manager
- System manager

Diagram:

```
Supermanager
  Can-create but
  Cannot do
  
Security manager
  
System manager
```
Consumer Management Roles

Super-csr

Can-create but
Cannot do

Create-csr

Modify-csr

Read-only-csr

Subscriber
Subscriber Management Roles

Create-csr1  Modify-csr1  Read-only-csr1  Modify-csr2  Read-only-csr2

Subscriber1

| userid | user personal profile | org1 roles | org2 roles | ..... |
Conclusion

- Good enough security tolerates occasional failure but does not tolerate catastrophic failure
- Identity management is the most important security issue for organizations
- The authentication ladder is real
- Role-based federated identity management is a proven technology in production today
- NSDS’s Secure Identity Appliance is a multifunctional product that supports these objectives