Role-Based Access Control (RBAC) with SingleSignOn.Net's Secure Identity Appliance™

Prof. Ravi Sandhu
Chief Scientist
RSandhu@SingleSignOn.Net
703-796-0965

State of the Practice

Weak Password Systems
• Relatively Usable and operable
• Insecure: Vulnerable to password guessing
• Insecure: Admin Accounts have carte blanche access to customer data

Strong PKI Systems
• Require smart cards: secure!
• Inoperable, ten years of frustrating pilots
• Unusable, very poor adoption

The hurdle in practice!

Result
Many ‘weak’ 3A systems
Very few strong PKI systems
Result: PKI in Isolated Silo

The PKI project at an issuer is often a non-mission critical "pilot" that is in its own silo.

E.g.: How many on-line banking sites use PKI for authentication? What chance does PKI have of succeeding if it is not usable for retail on-line banking????

The Practical PKI™ Approach

Result
- Phased migration path
- No "quantum jump"
- PKI integral, not siloed

Strong PKI Systems

PKI with Password Convenience

Password usability
PKI security

PKI Hardened Passwords

No change for user
No change for issuer
Eliminate weaknesses
3-Key RSA

- Key 1 = ALICE’S PUBLIC KEY
  - Contained in industry standard X.509v3 digital certificate
- Key 2 = Co-Signor’s KEY FOR ALICE
  - Only known to the Co-Signor
- Key 3 = ALICE’s KEY derived from her password
  - Only known to user Alice
  - In future, could be stored in Alice’s smart card or derived from her biometrics or both

Message signed sequentially with Key 2 and Key 3 is equivalent to one signed by composite private key.

Mathematically proven that the 3-key system is exactly as secure from an attacker as 2-key RSA

Security: Practical PKI™

- Practical PKI™ = Traditional PKI + Passwords
- Invented at Verizon and Bellcore; patents owned by Verizon and licensed exclusively to SingleSignOn.Net
- It can be informally thought of as a network-based “soft” smart card.
- Practical PKI™ uses and interoperates with usual PKI standards
Better Fraud Management

Every signature requires appliance interaction. Appliance logs can be used for velocity checking.

Consumer or CSR can use password to revoke instantly!

Since every signature requires appliance interaction, once revoked, a key cannot be used again! Instant, complete revocation!

Velocity
Easy
ID CANNOT BE USED ANY FURTHER!
INSTANT, COMPLETE, REVOCATION

ID stolen
Theft detected
Theft reported
CA revokes ID
Recipient (we hope) stops accepting ID

Usability: PKI mode

M is hash of the handshake (client-side SSL)

- User only needs to know password.
- User can roam from PC to PC with ease.
- The fact that there is PKI involved is completely hidden from user.
- User has one password for all channels and security functions
- Upward compatible with smart cards, tokens and biometrics.
Usability: Proxy mode

- Zero footprint password mode

Secure Identity Appliance™

Application Service Password

UserID Password (over server-side SSL)

Password

Weak Password Systems

PKI Hardened Passwords (Proxy mode)

PKI with Password Convenience (PKI mode)

Password usability
PKI security

No change for user
No change for issuer
Eliminate weaknesses

The Practical PKI™ Approach

Result
- Phased migration path
- No “quantum jump”
- PKI integral, not siloed

Strong PKI Systems
Operability

- Appliance Architecture:
  - Requires less than an hour to set up by non-expert
  - Off the shelf server with stripped down hardened OS
  - Easy to use tools for management
  - Redundant mirrored configuration
- Monitoring Station:
  - Industry Standard SNMP based monitoring
  - Harness for heartbeat monitoring
  - Application logs stored in relational database
- Role Based Access Control used to enforce least privilege:
  - Manager roles cannot access customer data
  - CSR Roles can only access data they are authorized to see
- Scalability: Single system benchmarked at 1 million users with 60 TPS. Can stack multiple systems.
- Went Beta in Nov 2000, Release 1.5 (March 2001) and is now in Release 2.0 (October 2001) and has been very extensively tested (internally and by major ASPs) for functionality, reliability and performance.

Reusability

- Password auth.
- + single sign-on
- + SSL (PKI) auth.
- + digital sig. (PKI)
- + VPN (PKI) auth.
- + wireless auth.
- + secure vault for private data which can provide a network wallet
- + authorization
Role-Based Access Control

- RBAC enforcement is almost trivial
  - A user's permissions are determined by the user's role
  - Enforcement is responsibility of an application service
- RBAC administration is the real crux of RBAC
  - Separation of user-role and permission-role administration
  - Delegated administration of user identity and profile
  - Separation of user-account administration from system administration
  - Role-based administration
  - Least privilege with respect to administration

Role-Based Administration

- Manager roles manage consumer roles
  - A consumer role can only access its own account
  - A manager role can similarly access its own account
  - All of this is appropriately configurable
- Manager roles also manage manager roles
- Enforcement of role-based administration is done by the Secure Identity Appliance™
RBAC: PKI mode

M is hash of the handshake (client -side SSL)

- Alice’s signature on M is used to authenticate and authorize Alice for some transaction
- Alice’s authorization is determined by her role and other profile information in Alice’s certificate

RBAC: PKI mode

M is hash of the handshake (client -side SSL)

- Consumer roles
- Manager roles

Identity and Profile Management Application

Appliance Management Application
RBAC: PKI mode

M is hash of the handshake (client-side SSL)

Secure Identity Appliance™

RBAC: Proxy mode

• Zero footprint password mode

Secure Identity Appliance™
RBAC: Proxy mode

• Zero footprint password mode

Secure Identity Appliance™

Password

UserID
Password (over SSL)

Application Service

Identity and Profile Management Application

Appliance Management Application

Identity and Profile Management Application

Application Service

Password

Secure Identity Appliance™

• Zero footprint password mode

Password

Application Service

Identity and Profile Management Application

Appliance Management Application
RBAC on Secure Identity Appliance™

- Three kinds of roles
  - Consumer roles
    - Can only access their own data
    - Configurable and modifiable
  - Appliance management roles
    - Built-in and cannot be modified
  - Identity/profile management roles
    - Configurable and modifiable
- Supermanager role
  - Has exclusive control of role definition and modification

Identity/Profile Management Functions

- Create
- Delete
- Revoke
- Suspend/Unsuspend
- Reset
- Read
  - Selective by profile field
- Write
  - Selective by profile field
  - Write implies Read

Role1
  - all of these

Role2

Role1
  - all except
  - Create, Delete

Role2
**Appliance Management Roles**

- **Supermanager**
- **Security Manager**
- **System Manager**

*Appliance management functionality is built into these three roles and cannot be changed*

*Appliance ships with one Supermanager account that cannot be deleted*

---

**Default Identity/Profile Management Roles**

- **Supermanager**
- **Super CSR**
- **Create CSR**
- **Modify CSR**
- **Consumer**
Identity/Profile Management:
Role-to-Role management

Manager Roles
Consumer Roles

Supermanager controls role-to-role management
Create, Delete, Revoke
Suspend/Unsuspend, Reset
Read, Write

Identity/Profile Management:
Role-to-field management

Manager Roles

Supermanager controls role-to-field management
Read, Write
(Write implies Read)
Identity/Profile Management:
Role-to-self-record management

Self-record
Field1 Field2 FieldN

Consumer and Manager Roles

Role_i

Supermanager controls role-to-self-record management

Read, Write (Write implies Read)