Alternative authentication methods

Niko Dukić/Mario Šale
CS Computer Systems
Table of contents:

• Authentication and why is it important
• Authentication methods
• RSA SecureID solutions for authentication
• Implementation of RSA SecureID solution into Microsoft Active Directory enviroment
• Authentication and BS7799
Authentication
Authentication

• “Is user really the one he is claiming to be?”
• 3 factors for confirmation of user’s identity
  – “Something I know”
  – “Something I have”
  – “Something I am”
• Authentication selection criteria
  – Cost (acquisition, deployment, support)
  – Level of security
  – Ease of use/convenience
Authentication methods
Authentication methods

• Common method:
  – User name and password

• Alternative methods:
  – Tokens ("one-time-password" devices)
  – Digital certificates
  – Smart Cards
  – Biometric devices
Passwords

• Simple and most common method
• One-factor authentication
• Very low cost of acquisition
• Very high cost of support and administration
• Balance of security policy (not too tight!)
• User is not aware that his password is stolen!
Tokens

- Pseudo-random number generation
- Two-factor authentication:
  - PIN
  - Token code
- Passcode (PIN + token code)
- Higher acquisition cost, lower support cost
- Offer higher security without security policies
- User is aware when his token is stolen!
Tokens

• Two kinds:
  – Hardware
    • Key-fob
    • Card
    • PIN Pad
  – Software
Digital certificates

- High level of security
- High acquisition cost, low administration cost
- Central administration
Smart Cards

• Two-factor authentication
• Storage container for various passwords and certificates
• Multi-functionality
  – Desktop authorization
  – Physical access to areas
  – Photo ID
Authentication methods

No Password Policy

PIN

Password Policy

PIN

PIN

Security

Weaker

Stronger
RSA SecureID solutions for authentication
RSA Authentication Manager

- Central component of RSA SecureID
- High level of compatibility (Microsoft, Cisco, Check Point)
- Integrated RADIUS server
- Unique database of all users
  - Windows domain users
  - RADIUS users (for dial-up access)
  - remote access users (RRAS, VPN)
  - web application users
RSA Authentication Manager

Authentication agent

User name and passcode

User name and passcode

RSA Authentication Manager
RSA Authentication Manager

• Fail over and load balancing
  – Primary server and replica
  – If primary server becomes inoperative, replica server can be promoted to primary server very quickly

• Two license options:
  – Base license
  – Enterprise (advanced) license
Implementation of RSA SecureID solution
Implementation in AD environment

- Increased security and simplicity
- Configuration:
  - RSA Authentication Manager
  - RSA SecureID for Microsoft Windows
  - RSA Authentication Agent
- All user names and passwords from AD are stored in RSA Authentication Manager database
Implementation in AD environment

- Installation of clients and agents
  - Agents
    - Windows 2000 Server
    - Windows 2003 Server
  - Clients
    - Windows 2000
    - Windows XP
    - Windows 2003
Implementation in AD environment

- Standard windows log-on

- RSA SecureID Windows log-on
Implementation in AD environment

5. User name and Windows password are sent to AD
6. AD sends “kerberos ticket” to the client

User name and passcode

Domain Controller

2. User name and password are sent to RSA Authentication Manager

3. Authentication Manager checks data and sends answer to request

4. Authentication Manager decrypts the password and sends it to OS

7. Authentication Manager makes preparations for offline authentication

RSA offline module

RSA Authentication Manager
Implementation in AD environment

1. User name and passcode

2. User name, Passcode

3. RSA offline module decrypts Windows password and sends it to operating system

Stored Microsoft passwords

RSA offline module

Client

RSA Authentication Server

User name and passcode

Windows password

Operating system
Authentication and BS7799

- BS7799-2:2002 - international standard for security by BSI
- Authentication - one of the most important aspects of BS7799
For those who want to know more...

- www.rsasecurity.com
- www.rsasecured.com
- www.microsoft.com
- www.checkpoint.com