

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



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 aplication users



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



- 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



- Instalation of clients and agents
 - Agents
 - Windows 2000 Server
 - Windows 2003 Server
 - Clients
 - Windows 2000
 - Windows XP
 - Windows 2003



Standard windows log-on

RSA SecureID Windows log-on

Log On to W	/indows
Copyright © 1985- Microsoft Corporal	-2001 tion Microsoft Professional Microsoft
User name:	ndukic
– Password:	
– Log on to:	domena
HR	OK Cancel Shut Down Options <<
Log On to V	Mindows [®] with RSA SecurID
	SA SecurID [®]
	Copyright 1990-2004 RSA Security Im
Log on with token, ente User name:	your RSA SecurID token. If you have not been issued a r your Windows password in the "Passcode" box.
Passcode:	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Passcode:	Help using tokens





5. User name and Windows password are sent to AD

6. AD sends "kerberos ticket" to the client

User name and passcode









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





CS Computer Systems d.o.o. | Prečko 1a | HR-10000 Zagreb T. +385 (0)1 3885 555 | F. +385 (0)1 3882 555 W. www.cs.hr E. **ndukic@cs.hr**

