ABSTRACT

Business needs in modern times are more and more tied to the use of Internet. Users and business partners are aware of benefits that are offered by technologies like VPN, partner web, e-banking etc.
Therefore, the importance of data security is becoming more important every day. Data integrity and data confidentiality must be kept intact under all circumstances. Jeopardizing either integrity or confidentiality of business data means loosing customers and their trust in our business. This is the risk that most companies cannot afford.

The first step of keeping our data secure is to make sure that only authorized personnel are accessing them. Authentication is used as part of the authorization process. We must make sure that the user who is accessing our data really is who he says he is. For that purpose we can use different authentication methods. This document is focused on alternative authentication methods and their comparison with the common authentication method using just user name and password.

Document describes the need for authorization process, why it is so important and what can help us to make our authorization process as secure as possible. It includes description of authentication factors that are used by the most common authentication method systems.

By combining these factors we achieve grater security in our authentication process which can have significant impact on information security.

1. Short overview of alternative authentication methods

- **Common authentication method**

Common authentication method describes authentication method which uses user name and password. It is used by the majority of operating systems and applications and it is based on only one authentication factor. Security of this authentication method is dependent of implementation and enforcement of password security policy.

- **Alternative authentication methods**

Alternative authentication methods are authentication methods which use two or three authentication factors for determining user's identity. By using more than one authentication factor, we decrease the possibility of someone impersonating any of authorized personnel and therefore enhance data confidentiality and preserve data integrity.

Alternative authentication methods imply having some kind of hardware or software device which represents second or third authentication factor. Some of these devices are:

- hardware tokens
- software tokens
- smart cards

Tokens are hardware or software devices which generate random numbers, also known as OTP ("One Time Password") numbers.
Smart cards are small plastic cards that can be used for multiple purposes like authentication on local or remote computer, storing passwords and certificates etc.

2. Implementation of alternative authentication methods

As stated, alternative authentication methods are more and more needed in every day business. As such, implementation in existing environment is a very important feature. I will describe the basics of one such system, the most powerful and secure system for alternative authentication methods from RSA Security known as RSA SecureID as well as its integration in Microsoft Active Directory services and VPN access to your network through VPN tunnels with firewalls like Check Point Firewall-1 or Cisco PIX. Using this system will make your users' experience as easy as before, but security aspect of your complete network infrastructure will be enhanced by multiple times.

3. Alternative authentication methods and BS7799

Alternative authentication methods, especially systems like RSA SecureID are one of the best solutions for achieving high security standards requested by BS7799 standard. Since access to your confidential data is one of the most important aspects of BS7799 certification these systems will be more and more implemented in existing and new environments.

BIOGRAPHY

Niko Dukic received his B. Sc. degree on Faculty of Electrical Engineering and Computing, University of Zagreb in 2003. Since April, 2004 he works as System Engineer in CS Computer Systems with primary focus on security products like Check Point, Microsoft, Websense, Trend Micro and RSA.