Annals of DAAAM for 2010 & Proceedings of the 21st International DAAAM Symposium, Volume 21, No. 1, ISSN 1726-9679
ISBN 978-3-901509-73-5, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2010
Make Harmony Between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals of DAAAM International

USE OF ACTIVE DIRECTORY IN SECURING THE CLIENT APPLICATIONS

PALKA, J[iri]; PALKA, J[an] & MOTYL, I[vo]

Abstract: *Nowadays developers change their view on applications from web oriented to thick or even smart clients. The reason of this change is more and more rising demands of the users for technologies. As thin clients are more enhanced by modern technologies these days, they are still quite limited against the opposites. Rise of these clients arise questions how to solve better authentification, authorization and securing of the whole communication between these clients and their servers. The main goal of this paper is analyze the possibilities of using the LDAP technology Active Directory in this process.*
Key words: *Active Directory, LDAP, authentification, authorization*

1. INTRODUCTION

Active directory is a central component of the Windows platform, Active Directory directory service provides the means to manage the identities and relationships that make up network environments. It is an implementation of a directory services LDAP by company Microsoft for use in system Microsoft Windows environment. Active directory allows administrators to set up politics, install programs on many stations and apply the critical updates in whole organisation structure. One of the main advantages is that the Active Directory stores the information and data in central organized database.

Active Directory is extendable and scalable directory service, which allows efectively manage network resources. Many applications no more require separate, distinct directory and userID/password to be managed for each application or service. (Desmond B., 2008)

- In Windows NT 4.0, for example, a directory was required for the domain itself, a separate directory for Exchange mailboxes and distribution lists, and separate directories for remote access, database, and other applications.

The administrator of the organization can add a user to Active Directory and enable remote access to the network through this one single entry. He can enable the same user account for database access for accounting, client relationship management, or other applications. Active Directory can work as a multi-purpose directory and doing so a company enables single sign-on for its users. Once a user logs in to Windows their Active Directory credential is the key that will automatically unlock all of the applications or services that they have been enabled for.

Creation of a link between user accounts, mailbox accounts, and applications means that Active Directory simplifies the task of adding, modifying, and deleting user accounts. For example when some information has to be changed in a user data, it can be done at one place, in central database. This change is displayed in all application, services the user is connected to. (Price, B., 2008)

- Based on standard internet protocols
- Needs a DNS service instalation.
- Organizes computer and domains groups
- Defines definity network structure

2. SECURITY OF THE ACTIVE DIRECTORY DIRECTORY SERVICES

Nowaday, when organizations and companies insist on better securiness the Active Directory has been dramatically enhanced to meet the requests of the user community and provide a solid defense in the increasingly hostile internet connected environment. Thera are a number of tools which facilitate applying additional levels of security to the server and the network environment to meet the stringent rules and regulations of current government laws. The most common reason for decreasing in security is of course organizations budget granted on security. Active Directory solves this problem in helping organizations achieve the goal of having a more secured environment without having to specifically allocate funds for a security project.

2.1 Protection againts unauthorized or undesired access to data

Against unauthorized or undesired access to data is used in Active Directory file-level encryption. The data stored on the server is encrypted, so a potentiall attacker gaining the access to a file server through unauthorized access, can be able to download files, but will be unable to open or access the content of the files unless they have a key to decrypt the data.
Encrypted File System (EFS) is especially useful for securing sensitive data on portable computers. For example if a laptop is stolen and the thief removed the hard drive and attempted to read the encrypted files on another computer, they would not be accessible. This type of encryption has satisfied many organizations requirements to comply with current laws and regulations on data encryption and information privacy such as HIPAA, California SB-1386, and FISMA.
With Windows Server EFS encrypted data and Windows XP EFS encrypted hard drives, information can be copied from a server to the client system, or from the client system to a server and retain the encryption through the process. This encryption gives a confidence to the organization that information is stored, managed, and accessed secure and that the integrity and privacy of the information is not be compromised.

2.2 IP Security

Using the Windows Server 2003 and later is for administrator very easy to configure a server to send all communications in 168-bit encrypted format. For encrypting is used mechanism of the IP security called IPSec, it is used for establishing end-to-end encryption of all data packets send between computers. IPSec is built-in to Windows Server 2003 and later. The only individuals that can access the IPSec enabled server are users that have workstations running. With a

matched client and server encryption connection, users can be assured that the conversations and data transmitted between the IPSec server and client system are as private and secure as possible. Additionally, IPSec ensures that messages are not modified in transit and are unreadable to network intruders.

2.3 IPSec and Network-Based Attacks

Through network services is possible to attack the organisation infratructure. Clients and servers with Windows operation system have a number of services which are network-aware this way.

These services can be attacked various attacks:

- Denial of service attack, or data corruption
- Data theft, use credential theft
- Administrative control of the server
- Administrative control of other computers and the network

Easiest way to protect against these attacks is to disable all not used services, but what to do with services the organization needs, like authentication domain users, providing network based application such as web hosting, databases, file sharing.

The security against network-based attacks is not provided at TCP and UDP level. Authentication, authorization, data confidentiality, and data integrity are typically provided by applications at the security services layer.

- Internet e-mail program uses Secure Sockets Layer (SSL) to help protect data that is transmitted during user account logons and during the upload and download of e-mail messages from a mail server.

To reduce weaknesses of applications is possible to use IPSec. It is helping to secure network communications through policies between clients and their mail servers or between mail servers. (Dixon, W., Wong, D. & Scambray, J., 2008)

2.4 Attacks against Internal Network Server

There are two ways of attacks:

- Pasive – Is based on capturing communications between internal server and other computers in the network.
- Active – Is based on connecting attackers computer straight to the attacked server or modifying communication

Attacks can be divided into three variants:

- Inside - Within the internal network, an attacker can use a physical port to make a connection to the internal network, or malicious users can use computers on the internal network.
- Near - outside of the internal network, but within range of the organisation wireless LAN
- Outside - The Internet

Finally, the attacker might have or gain knowledge of legitimate, internal user account passwords before attempting to access an internal corporate network server

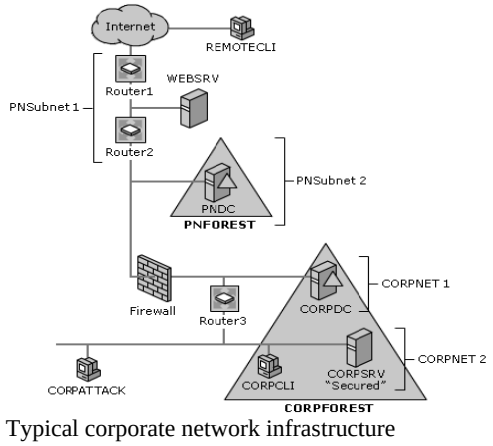

Fig. 1. Typical corporate network infrastructure

2.5 Benefits of using IPsec as a defense against Network-based attacks

It is possible to use IPSec to defend against network-based attacks from untrusted computers. IPSec is also useful as a means of auditing communication, to assist in network security investigations.

IPSec is a security protocol that provides defense against network-based attacks from untrusted computers. IPSec provides data confidentiality, data integrity, data origin authentication, and anti-replay for unicast IP packets sent between trusted hosts. It offers a cryptographic-based authentication and encryption that is especially useful for securing traffic that must go through untrusted network paths, such as on a large intranet or the Internet. IPSec can be succesfully used for securing traffic that uses protocols and applications that do not provide sufficient security for communications.

Use of the IPSec reduces the risk of a network attack against that server in the following ways:

- Attack opportunity is reduced to trusted computers. It is possible to reduce the risk of attack from compromised user credentials and other unmanaged or untrusted computers on the network by granting inbound network access only to a group of trusted computers that are explicitly specified.
- Attacks can come from the communication paths, protocols, and ports that you explicitly specified in an IPSec policy only.
- The cryptographic protection that IPSec provides, greatly reduce possibility of sophisticated attacks based on capturing or manipulating network traffic.

By providing these benefits, Windows IPSec brings a high level of security for the traffic and the servers in network. (Johansson M. & Riley S., 2002)

3. CONCLUSION

As showed in this paper using the Active Directory brings more secure networks with more secured applications in these networks which are so important nowaday. Second reason for using the active directory directory services is in its cost demands, which are for the organisation much less in the case of establishing Active Directory into the network than use of an adhoc security solution. It is foresightfull these days to implement solutions like Active directory into the corporal networks, because of its qualities and possibility to use its features like group policy, or IPSec which can be at the least the answer to the problems which cannot be solved alternatively or in the cases of the specific laws and regulations. However this technology is limited because of its implementation complexity into the existing infrastructure.

4. REFERENCES

Desmond B.: (2008): *Active Directory: Designing, Deploying, and Running Active Directory*, O'Reilly Media, 978-0596520595

Dixon, W., Wong, D. & Scambray, J. (2008), *Using Microsoft Windows IPSec to Help Secure an Internal Corporate Network Server*, Microsoft Corporation

Johansson M. & Riley S.: (2002): *Protect your windows network from perimeter to data*, The Addison-Wesley, 0-201-61621-1

Kouti, S. & Seitsonen, M.: (2001): *Inside Active Directory*. Addison-Wesley, 978-0321228482

Price, B. (2008): *Mastering Active Directory for Windows Server*, Sybex Press, 978-0470249833