International Journal of Information Technology and Knowledge Management (ISSN: 0973-4414) July-December 2012, Volume 5, No. Issues 2, pp. 501-506.

Analysis of Security Criteria For Partner Network

*Chaman Verma[1], Dr.Ashish Chaturvedi[2] ,Mandeep Singh Tinna[3]
[1]*Department of Computer Science & Engineering, Eternal University, Baru Sahib, H.P.173101, India*
[2]*Arni University,Kangra.H.P,india*
[3]*Department of Computer Science & Engineering, Chandigargh University,, India*

Abstract

We are allowing people outside our organization access to proprietary data and applications - over the Internet. The objectives of this research are to form a secured infrastructure between partner network and Internet. In today's competitive business landscape, organizations are compelled to share data, files, and applications with external partners, customers, and remote workers. Primarily, they are doing this over extranets. In this paper we define some security criteria for maintain the security in Extranet and also elaborate latest technologies & products for forming a secure dynamic architecture for partner network.

KEYWORDS: Authentication, Extranet, Partner Network, Security.

1. INTRODUCTION

In todays digital environment completely business deals are executing on internet. So each organizationis directly in contact with internet. Like an Intranet, an extranet is a private network. But rather than being directed internally for staff needs, it is an outward facing network used to securely collaborate, share information or integrate operations with suppliers, vendors, partners, customers or other businesses. So it is variously titled "customer extranet" or "vendor extranet" or "Partner Extranet". In our connected society, the lines between an organization's intranet and the Internet are blurring. Almost every organization possesses some need to extend limited access to business partners, suppliers, vendors and/or customers via an extranet. In this tip, we take a look at four important strategies for securing extranets: isolation, strong authentication, granular access controls and use of adequate encryption. The secure framework aims to answer these needs, by providing a framework for dynamically setting up and running secure extranets.

* Corresponding author. Tel.: +91 8894379601; fax: +91 1799276006
E-mail: chaman.verma@gmail.com

2. BACKGROUND

Organizations depend on information more and more nowadays. For the information to be easily accessed and exchanged, it is stored in computer systems. New business models and out-sourcing of services require much more flexible exchange of information than before. The offices of an organisation are often geographically distributed all over the world (see Figure 1 below), yet the information should be easily accessed and exchanged

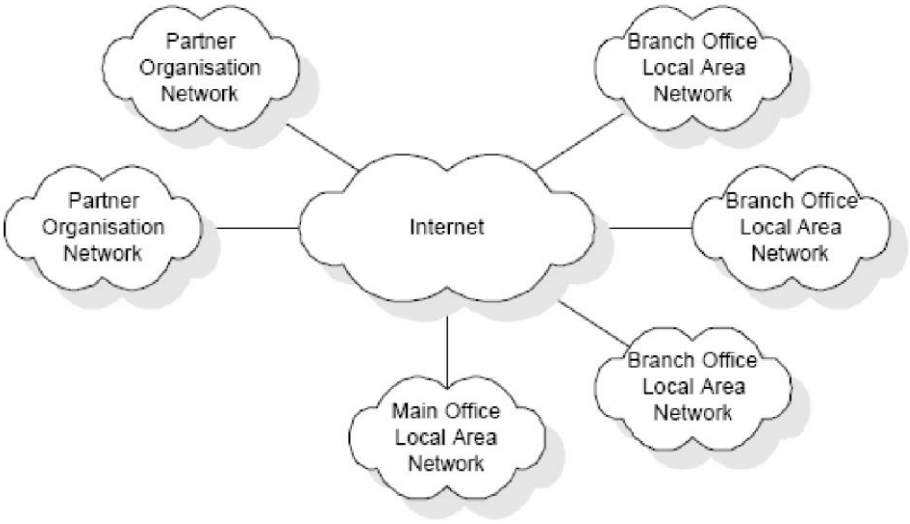

Figure 1. Organization's network and partner networks distributed over the Internet.

Since the above mentioned parties are spread over diverse locations, extranets use the internet as a vehicle to connect to these parties. A company might have multiple dedicated extranets for different key partners or clients. It can sometimes also be seen as an extension of an "intranet" where external parties are brought into the fold of the company's private network.

The Internet is a public, insecure network. Anyone can connect to the Internet. Basically all information sent to the Internet is public.

3. REASON FOR STUDY

The problem is to authenticate users and services from other partner networks in a structured manner. Structured manner means that an organisation may define an individual access policy for each partner organisation. Different partner organizations have different business needs. Different partners require access to different parts of the information system or require different access rights to the information system. Still, for simplicity, there should be only one authentication mechanism for all partner organisations.

4. METHDOLOGY

The Dynamic framework must be based on the following criteria to be a useful and successful system. In this thesis, there will be define some basic criteria that supposed to be fulfilling the requirement of security on Extranet. The Reference System would be helpful for Network Security Manager to implement security on any Extranet. In this methodology, study of technologies and products that are used for authentication, encryption and secure network connections over any Extranet. The secondary descriptive approach of Research Methodology will be used.

4.1 Security Criteria

Algorithm Criteria 1: - The algorithms must use strong cryptography. The specifications of the algorithm must be public. The security of the algorithm must not rely on the secrecy of the specifications i.e. security through obscurity. Secret specifications have the tendency that they will not stay secret for long.

Algorithm Criteria 2:- The algorithms must use strong keys. The key length must be so long that it is unfeasible to make a brute force attack against the algorithm. The brute force attack can be either a known plaintext or a chosen plaintext attack. The required computational resources or the required memory resources must be several orders of magnitudes higher than the estimated resources that any organization could have.

Protocol Criteria 3:- The protocol must implement Virtual Private Network at IP level. The easiest way to introduce security to any system is when the users do not have to do any additional actions to enhance the security. All old applications work the same way as they have worked before. The only way to do this is to implement the Virtual Private Network at IP level. After the Virtual Private Network is set up, it will be completely transparent to the end user.

Protocol Criteria 4:- No plaintext authentication tokens (passwords etc.) must pass across insecure networks. The protocol must not rely on the security of the network. The protocol must be secure even if the attacker can listen to the network traffic. If an unauthorized party can acquire the authentication tokens for example by eavesdropping the communications channel, it could use the authentication tokens to impersonate as legitimate user and gain unauthorized access.

Protocol Criteria 5:- The protocol must provide confidentiality, integrity and protection against replay attacks. Unauthorised parties must not be able to eavesdrop the information that is transmitted to the network. The information must be encrypted to ensure confidentiality. The information sent to the network must be tamper-proof. The integrity of the information must be maintained. This is accomplished by authenticating the data.

Protocol Criteria 6:- The protocol must provide authenticated keying material that is kept confidential. The protocol must provide keying material. The keying material is used to initialize the encryption and authentication algorithms. The keying material must be kept confidential against eavesdroppers.

Implementation Criterion 7:- The complexity of key management must be at most linear as the number of parties increase. In small systems the connections between end points can be configured manually. The number of configured connections grows exponentially as the number of end points increase. Large systems require easy key management. The connections must be configured automatically. When setting up a large system the complexity of the key management must be based on the number of end points, not on the number of separate connections.

Implementation Criterion 8:- The protocol must provide Perfect Forward Secrecy. Perfect Forward Secrecy means that the compromise of a single key restricts the security breach only to data protected by that key. To facilitate Perfect Forward Secrecy the key used to protect transmission of data is not used to derive any additional keys.

Implementation Criterion 9:- The administrator of a network must be able to decide which partner networks are permitted access. Organization offering its intranet to the partner organizations must have the means to define what partners have access to what information. The authentication mechanism can be quite complex because the trust relationships of each partner are different.

Implementation Criterion 10:- The system must be built using already existing products. It is very important that security products do not contain any bugs that would result in a security breach. Companies that produce security products have comprehensive experience about secure coding and testing guidelines. It would be infeasible for the inexperienced to try to make such a critical product from scratch.

5. Dynamic framework

A dynamic framework which meets each criteria or requirements specify by human being or user is called the completely secure system In this paper reference system will be made by use of different security products, technologies which supposed to be meet each criteria.

Criterion 1 The algorithms must use strong cryptography. The specifications for cryptographic algorithms are public (3DES, HMAC-SHA-1-96 and RSA [2]). The algorithms are also very widely used and have no known weaknesses.

Criterion 2 The algorithms must use strong keys. The reference system uses 3DES for symmetric encryption, SHA-1-96 for keyed Hash Message Authentication Code (HMAC) and 1024-bit RSA keys for asymmetric encryption. The best known attack against 3DES requires 22 known plaintext cipher text pairs, 2112 encryptions and requires 256 words of memory. [22] HMAC-SHA-1-96 uses 96-bit key and has no known weaknesses [14]. HMAC-MD5-96 has been shown to be vulnerable to collision search attack and is not used in the reference system.

The complexity a brute force attack against 1024-bit RSA asymmetric key is equivalent to 96-bit symmetric key (effective key length of 3DES is 112 bits). Estimated time to break 96-bit symmetric key or 1 024-bits asymmetric key using brute force attack is 3 000000 years. Recommended effective key length for symmetric algorithms is 96 bits and 1 024 bits for asymmetric algorithms, just to be sure.

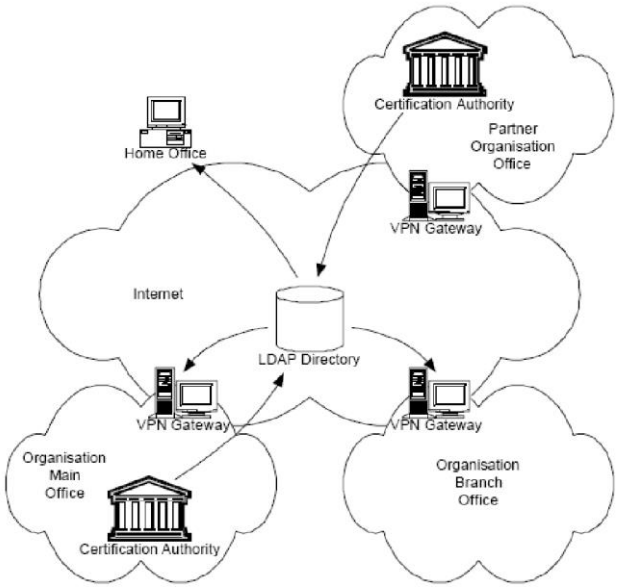

Figure 2 Dynamic Framework

Criterion 3 The protocol must implement Virtual Private Network at IP- level. VPN is based on IPsec standards that provide the security services at the IP level. The VPN is completely transparent to users after it is built.

Criterion 4 No plaintext authentication tokens (passwords etc.) must pass across insecure networks. Authentication is based on public keys using X.509 digital certificates. No private keys or secret keys are sent to the network unprotected. Secret keys may be used in VPN client authentication, but in that case the connection is already secured with IPsec using X.509 digital certificate.

Criterion 5 The protocol must provide confidentiality, integrity and protection against replay attacks. IPsec Encapsulating Security Payload (ESP) is used to provide confidentiality using symmetric encryption with a session key, which is generated when establishing the Security Association (SA). IPsec Authentication Header (AH) is used to provide integrity and protection against replay attacks using keyed Hash Message Authentication Code and Sequence Number.

Criterion 6 The protocol must provide authenticated keying material that is kept confidential. Internet Security Association and Key Management Protocol (ISAKMP) provide authenticated confidential keying material using random no's and public key encryption.

Criterion 7 The complexity of key management must be at most linear as the number of parties increase. Each VPN gateway and each end user require one certificate. Thus the complexity of key management grows linearly. If pre-shared secrets would be used, each pair of end points would need its own secret key. The number of pre-shared secrets would grow exponential as the number of end points increase. Pre-shared secrets are not a feasible authentication method in large systems.

Criterion 8 The protocol must provide Perfect Forward Secrecy. Internet Key Exchange (IKE) provides Perfect Forward Secrecy (PFS) for both the keying material and the identities. PFS for keying material is established by specifying a Diffie-Hellman group and passing public key values in the key exchange payload. PFS for identities is established by using encryption keying material in the ISAKMP SA.

Criterion 9 The administrator of a network must be able to decide which partner networks are permitted access. Access control is achieved by defining specific rules for different

partner organizations and different local area network combinations. The CheckPoint VPN-1 administration GUI has an easy-to-use interface to perform this task.

Criterion 10 The system must be built using already existing products. CheckPoint VPN-1 is a commercial product from CheckPoint Software Technologies Ltd. CheckPoint VPN-1 was introduced several years ago and is widely used.

RSA Keon Sentry CA is a commercial product from RSA Security. Sentry CA was developed by Xcert Software, which was purchased by RSA Security in 2001. Xcert Software was founded in 1996. Sentry CA was introduced several years ago and is also widely used.

6. Conclusion

Extranet that is based on IPsec VPN technology are in many ways a good solution. IPsec is a widely adopted standard, which has also been proved in practice. There are many software vendors that have IPsec compliant VPN gateways and VPN client software. The support covers a wide range of platforms and operating systems. In most cases there is even freedom of choice between similar products so that the product matches the organization's individual preferences best. The dynamic framework described in this paper uses IPsec VPN for creating extranets and digital certificates for authentication. The reference system fulfils all of the criteria specified for a useful system.

References:-

Books:

[1] Amoroso, E., Fundamentals of Computer Security Technology, Prentice Hall, 1994, 404 p

[2] Schneier, B., Applied Cryptography Second Edition: protocols, algorithms, and Source code in C, John Wiley & Sons, 1996, 758 p.

[3] Charless P.Pflager, Security in Computing, Third Edition, Pearson Education, PHI, 2006.

[4] Cryptography and Network Security: Principles & Practices, Fourth Edition, PHI, 2007

Websites:

[5] CheckPoint, VPN-1 Certificate Manager,
http://www.checkpoint.com/products/vpn1/certificate.html

[6] CheckPoint, VPN-1 Product Family, ,
http://www.checkpoint.com/products/vpn1/index.html

[7] Entrust, Entrust/PKI,
http://www.entrust.com/entrust/index.htm

[8] Federal Information Process Standards, Digital Signature Standard (DSS),
U.S. Department of Commerce, National Institute of Standards and
Technology, http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf

[9] Free On-Line Dictionary Of Computing,
http://foldoc.doc.ic.ac.uk/foldoc/

[10] FreeS/WAN,
http://www.freeswan.org/

[11] F-Secure, F-Secure VPN+, http://www.f-
secure.com/products/vpnplus/

[12] iPlanet, iPlanet Certificate Management System,
http://www.iplanet.com/products/iplanet_certificate/home_2_1_1ad.html

[13] iPlanet, iPlanet Directory Server,
http://www.iplanet.com/products/iplanet_directory/home_2_1_1z.html

[14] Knudsen, L. R. & Rijmen, V., The Block Cipher Lounge,
http://www.esat.kuleuven.ac.be/~rijmen/bc.html

[15] National Institute of Standards and Technology, Advanced Encryption Standard, http://csrc.nist.gov/encryption/aes/

[16] PGP Security, Gauntlet VPN,
http://www.pgpinternational.com/products/vpnsuite/default.shtml

[17] RSA Security, Keon,
http://www.rsa.com/products/keon/index.html

[18] RSA Security, SecurID,
http://www.rsasecurity.com/products/securid/index.html

[19] SmartTrust,

http://www.smarttrust.com/

[20] Stonesoft, StoneGate,

http://www.stonesoft.com/document/143.html

[21] Symantec, Symantec Enterprise Firewall 6.5,

http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=47&PI

D=5718284

[22] Tivoli, IBM SecureWay Directory,

http://www.ibm.com/software/network/directory/index.html

[23] Tivoli, IBM SecureWay Firewall,

http://www.tivoli.com/products/index/secureway_firewall/index.html

Journals:-

[24] ”Extras - Security for Intranets and Extranets” Jerry Lawson Published on November 18, 1998.

[25] “Protecting Confidential Information in a Corporate Intranet or Extranet” Dovetail Internet Technologies, LLC 906 Boston Turnpike Shrewsbury, MA 01545

[26] “PKI Security in The New Extranet Marketplace - Industry Trend or Event” Peter J. Hussey, President of GTE Cyber Trust (Needham Heights, MA) Oct 1999.

[27] “Extranet security: A Technical Overview from a Business Perspective” Jennifer Jordan, University of Maryland, Graduate School of Business May 1’1997

[28] “Security Considerations for Extranets” Security Considerations for Extranets by Karen A. Korow Diks December 18, 2001

[29] “Intra, Extra, and Internets in Franchise Network Organizations" Audhesh K. Paswan C.

Michael Wittmann Joyce A. Young, a Department of Marketing and Logistics, College of Business Administration, University of North Texas, Denton, TX b School of Business, Indiana State University, Terre Haute, 2004

[30] “Extranet Implementation: A Case Study of a Community Healthcare Information Network” Dr.

Steven Ross, Dr. Deepinder Bajwa, Dr. Christopher Sandvig,Western Washington University, IACIS 2003

[31] “Extranet Access Control Issues” Tim Grance, Joan Hash, Steven Peck Jonathan Smith, Karen

Korow-Diks in Harold F. Tipton and Micki Krause, ed., Information Security Management Handbook, Vol. 2, 4th edition (New York: Auerbach, 2000), 99-114.