International Journal of Advanced Science and Technology
Volume 8, July, 2009

Vulnerabilities of VPN using IPSec and Defensive Measures

[1]Byeong-Ho Kang and [2]Maricel O. Balitanas

[1]University of Tasmania, Australia
[2]Hannam University, Department of Multimedia Engineering, Postfach, 306-791
jhe_c1756@yahoo.com[2]

Abstract

Data security plays a crucial role in modern times most business is transacted over the internet and even to wireless devices. This paper presents the vulnerabilities found in VPN using IPsec and suggested a set of Policy as a Defensive measure. Such policy suggested applies to implementations of VPN that are directed through an IPsec concentrator and to all company's employee, contractors, consultants, temporaries and other workers including all personnel affiliated with the third parties utilizing VPNs to access the company's network.

Keywords: *Virtual Private Network, Internet Key Exchange, IPSec, Aggressive mode*

1. Introduction

People have been searching for ways to hide valuable information from each other. In earlier times man would make a simple pattern changes to an alphabet or substitute other letters or numbers into their written messages, to successfully hide private information. The use of encryption in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet. VPNs (Virtual Private Networks) are private networks using private lines but rely on having the same encryption system at both ends. The encryption may be performed by firewall software or possibly by routers.

All too frequently, the default "out of the box" configuration for a VPN server is geared towards usability rather than security. Typically the default authentication method for remote access VPNs is IKE Aggressive Mode with pre-shared keys, even when stronger authentication methods such as Main Mode with certificates are available. IKE Aggressive Mode with pre-shared key authentication has known issues, which have been detailed in previous sections. The end-users generally assume that the default configuration is secure because they trust the vendor to choose sensible defaults, and there is nothing to indicate to them that there is any security vulnerability unless they get tested or hacked.

The default configurations also normally include support for many different ciphers and modes, so you will often see a combination of strong and weak ciphers or both Encapsulating Security Payload (ESP) and Authentication Header (AH) (which does not encrypt the traffic when used alone) being supported. In these cases, someone with access to the client system (either directly, or over the network) could re-configure the client to use a weak cipher that could be easily cracked (it would not take long to crack a 40-bit export-grade cipher with modern equipment), or worse to use AH which passes the traffic in the clear [1]. The user would almost certainly never notice the change because the VPN works just the same, and no

one would bothers to manually check the tunnel mode and encryption ciphers after every connection.

The rest of this paper is organized as follows. We first review and present what is VPN and using IPsec. Then in third section we made a scenario and layout the vulnerabilities if VPN using IPsec, while Section 4 is the proposed policy as a defensive measure. And 5th section draws the main conclusions of this paper.

2. VPN using IPsec

Virtual Private Network is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger networks, such as the internet, as opposed to running across a single private network. The link layer protocols of thevirtual network are said to be tunneled through the transport network. [2]

In mid 1990s, the rise of the Internet and the increase of speed for cheap Internet connections paved the way for new technologies. Many developers, administrators, and, last but not the least, managers had discovered that there might be better solutions than spending several hundreds of dollars, if not thousands of dollars, on dedicated and dial-up access lines.

The idea was to use the Internet for communication between branches and at the same time ensure safety and secrecy of the data transferred. In other words: providing secure connections between enterprise branches via low-cost lines using the Internet. This is a very basic description of what VPNs are all about.

Taking into account literally the acronym VPN (Virtual Private Network) Virtual means there is no direct network connection between the two communication partners, but only a virtual connection provided by VPN. Software, realized normally over public internet connection. And considered to be private because only the members of the company connection by the VPN software are allowed to read data transform.[3] With a VPN The network entities are described as a set of logical connections secured by special software that establishes privacy of safeguard the connection endpoint. As depicted in the Today the Internet is a work medium used, and privacy is achieved by modern cryptographic methods.

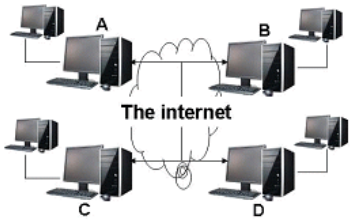

Figure 1. Virtual Private Network

2.1. VPN Scenario

How this VPN works is of the following: For instance, if the Australian branch in Sydney decides to contract a supplier, then the London office might need to know that immediately. The main part of IT infrastructure is set up data hosted on Seoul. In Singapore

there are twenty people whose work depends on the availability of the data hosted on Seoul servers. The said scenario is depicted in Figure 2. Both sites are equipped with a permanent Internet line. An internet gateway router is set up to provide Internet access for the staff. This router is configured to protect the local network of the site from unauthorized access from the other side, which is the "culprit"Internet. Such a router set up to block special traffic san be called firewall and must be found in every branch that is supposed to take part in the VPN.

The software used for VPN must be installed on this firewall. Many modern firewall appliances from manufacturers like Bin Tec or Cisco includes this feature and there is VPN software for all hardware and software platform.

Once connection has been established, the company has a working Virtual Network. The two branches are connected via internet and can work together in a real network. Here, a VPN without privacy, because any internet router between Seouland Singapore can read the data exchanged. A competitor gaining control over an internet router could read all relevant business data going through the virtual network.

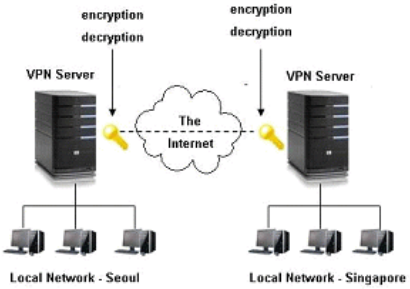

Figure 2. Scenario layout

How to make Virtual Network Private? The VPN traffic between two branches is locked with special keys, and only computers or persons owning this key can open this lock and look at the data sent.[3]

All data sent from Singapore to Seoul or from Seoul to Singapore must be encrypted before and decrypted after transmission. The encryption safeguards the data in the connection like the walls of the tunnel protect the train from the mountain around it.This explains why Virtual Private Networks are often simply known as tunnels or VPN tunnels, and the technology is often called tunneling-even if there is no quantum mechanics involved [4]

The exact method of encryption and providing the keys to all parties involved makes one of the main distinguishing factors between different VPN solutions.

2.2. IPsec

IPsec is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect

data flows between a pair of hosts (e.g. computer users or servers), between a pair of security gateways (e.g. routers or firewalls), or between a security gateway and a host. [5]

A critical aspect of IPsec, is automatic key management current being used to negotiate in behalf of IPsec operations, keying material and security suite requirements defined in the VPN communication policy. IPsec encompasses several interesting technologies, many of which can be very complicated and open to interpretation, such as IKE (the automatic key management). However, IPsec-specific operations, such asthe use of security protocols, are fairly straightforward and the implementation options, with regard to automatic key management are what need to bed conveyed.

Figure 3 shows the seven groups of documents that allow the separate aspects of the IPsec protocol suite to be developed independently while providing a functioning relationship that can be easily managed.

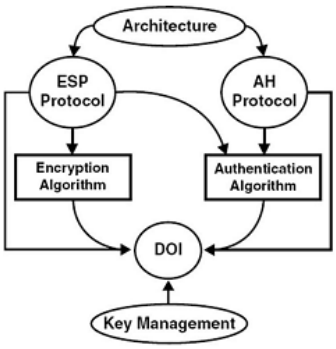

Figure 3. Document Road Map [6]

2.3. IKE (Internet Key Exchange)

Internet Key Exchange is the automatic key management protocol used for IPSec. IKE was created from several other key management protocols and is the default for IPSec, but other key management protocols can be used. In reality, no key management is required for IPSec functions and the keys can be manually managed. However, manual key management is not desirable for all implementations due to the administrative overhead and the fact that keys never expire. Having keys that never expire represents a plethora of security vulnerabilities.

The general key material within IKE is primarily for IKE encryption and authentication, and is not directly responsible for the key material for the underlying protocol-IPSec. During the creation of the keys for the various IKE Phase I authentication types (shared secret, digital signatures, and public key encryption), a pseudorandom function is used to assist in combining the material to create the keys. Because no pseudo-random functions are currently defined for use within IKE, the HMAC portion of the negotiated authentication algorithm is used such as HMAC-MD5.Each HMAC function is a message authentication code based on a keyed hash function. Hence, when the creation of the keys are defined, there is a key identified within the process itself as shown in the following: [7]

Result = prf (key, attribute1 | attribute2)

Due to hashing of HMAC function, they are restricted to certain block sizes that will have an effect on the resulting key size. If a hash algorithm has a block size of 8 bytes, but the requirement of the final key is 30 bytes, the PRF has to be used four times into itself, combining the results and taking the most significant bits to produce the necessary key. The following is an example based on the creation of the pre-shared secret SKEYID, in which each Bx is one resulting block of 8 bytes.

B1 = prf (pre-shared-key, nonce_i | nonce_r)

Such operation was previously defined as equaling the SKEYID. However, that would result in a key 4 times too small.

B2 = prf (pre-shared-key, B1 | nonce_i | nonce_r)

B3 = prf (pre-shared-key, B2 | nonce_i | nonce_r)

B4 = prf (pre-shared-key, B3 | nonce_i | nonce_r)

With four 8-byte keys, one can combine them and use the most significant number of bits necessary to create the final key. In this example, the final key is equal to 32 bytes; therefore, one takes the first 30 bytes of the result of combining the pre-calculated blocks of 8 bytes:

SKEYID = (!30 (B1 | B2 | B3 | B4))

The same process is applicable to other key generation operations. As the three constant keys are created (_a, _e, and _d), they must be increased to accommodate the encryption algorithm. For example, the creation of SKEYID_d, the first of the three to be computed:

B1 = prf (SKEYID, DH_key | cookie_i | cookie_r | 0)

B2 = prf (SKEYID, B1 | DH_key | cookie_i | cookie_r | 0)

B3 = prf (SKEYID, B2 | DH_key | cookie_i | cookie_r | 0)

B4 = prf (SKEYID, B3 | DH_key | cookie_i | cookie_r | 0)

Once the blocks are created, one can combine the results and take the first 30 bytes for a key.

SKEYID_d = (!30 (B1 | B2 | B3 | B4))

2.4. IKE and IPsec Relationship

IPSec and IKE are compared to PKI (Public Key Infrastructure) and in theuse of Certificates. Certificates, by themselves, are quite simple and can be used for encryption, signing, authenticating, and a multitude of other services. IPSec is similar to the application that uses the Certificate to execute the desired actions, such as signing an e-mail message. Simply stated, the application is virtually unaware or concerned about the maze of trusts and policies governing the entirePKI from which the Certificate was created. IPSec is much like the application that uses the Certificate, and IKE is much like the PKI that creates and manages the Certificate. Inevitably, IKE is more complicated and subject to constant functionality and security concerns. IPSec is more concerned with properly implementing the security services and maintaining various forms of communication options.

3. VPN Vulnerabilities

3.1. IKE Aggressive Mode

In IKE Aggressive mode the authentication hash based on a preshared key (PSK) is transmitted as response to the initial packet of a vpn client that wants to establish an IPSec Tunnel (Hash_R). This hash is not encrypted. It's possible to capture these packets using a sniffer, for example tcpdump and start dictionary or brute force attack against this hash to recover the PSK. Using IKECrack [8]

This attack only works in IKE aggressive mode because in IKE Main Mode the hash is already encrypted. Based on such facts IKE aggressive mode is not very secure.

To capture and crack the PSK, IKE aggressive mode must be able to capture the traffic from the wire. Also the IP address of the VPN client must be acceptable by the VPN gateway. Figure 4 shows the setup of PSK Cracking

Figure 4. PSK Cracking

3.2 Common VPN Issues

3.2.1 VPN fingerprinting : VPN servers can be finger printed buts User Datagram Protocol (UDP) backoff fingerprinting, Vendor Identity (ID) fingerprinting or other fingerprinting methods.[9] While this is not a problem by itself (and some vendors do not consider it a problem at all), it does give useful information to potential attackers. Some systems will reveal the general type of device, e.g. "Cisco PIX" or "Nortel Contivity", whereas others will show the software version details as well. Knowledge of the device type and software version allows an attacker to target any known weaknesses in that particular product. Here is an example showing both backoff fingerprinting and Vendor ID fingerprinting. The backoff pattern indicates that the system is Checkpoint Firewall-1, and the Vendor ID confirms this and also identifies the version as NGX.

Most VPN client program offer to store come or all of the authentication credentials, and for some clients, this is the default setting. This makes VPN easier to use and also introduces security risks, especially if the credentials are not well protected.

The common client issues that have been seen are as follows:

1. Storing the password in a scrambled form

This is often referred to as "encryption", but it is really obfuscation rather than encryption because there is no unique key needed to decrypt it. If the obfuscation algorithm becomes known, then it is a simple matter to obtain the password if you have access to the client computer. The folowing screenshot shows an example of both the plain-text username and also the obfuscated password stored in the registry.

2. Storing the plain-text password in memory. If storing an obfuscated version of the password in a file or registry is not bad enough, many clients decrypt this password when they start up, and store a plaintext version of the password in memory. In this case, anyone with access to the

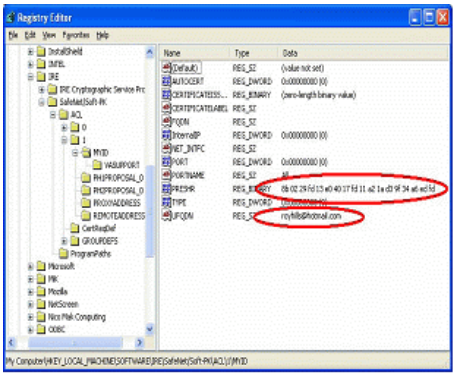

Figure 5. Example of plain-text username and also the obfuscated password stored in the registry. [10]

Client computer can obtain the password by starting the VPN client and then dumping the process memory with a tool such as pmdump, or crashing the computer to get a dump of physical memory. The figure 6 shows an example memory dump from a VPN client with the clear-text password 7W0ntGu355Th15 highlighted. Notice that the last two characters of the

Password are repeated in the memory dump. This is repeatable behaviour for this VPN client, and may give some insight into the obfuscation mechanism

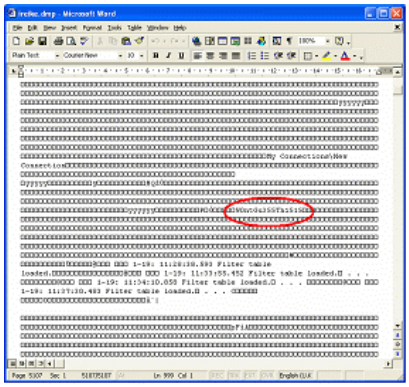

Figure 6. example memory dump from a VPN client with the clear-text password 7W0ntGu355Th15 highlighted.[9][10]

4. Proposed Policy

Due to the attack scenario, it would put VPNs at risk that uses pre shared keys for authentication and accepts VPN connections from anywhere like access for traveling users.

Possible solutions would be one, use pre shared keys for authentication even with routers, second disable aggressive mode it its supported like firewall checkpoint and third don't allow dynamic IP addresses in VPNs and don't use dynamic crypto maps. As a suggestion a Policy is layout in the following section to provide guidelines for remote access IPSec virtual private network (VPN) connections to a corporate network.

1. Only InforSec-approved VPN clients may be used
2. User of computers that are not company-own equipment must configure the equipment to comply with the company's VPN and network policies
3. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of company's network and as such are subject to the same rules and regulations that apply to the company-owned equipment.
4. It is the responsibility of employee with VPN privileges to ensure that unauthorized users are not allowed access to company's internal networks.
5. When actively connected to the corporate network, VPN will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped
6. VPN use is to be controlled using either a one-time password authentication such as a token device or public/private key system with a strong passphrase.
7. VPN gateway will be set up and managed by company's network operational groups
8. All computers connected to the company's internal network via VPN or any other technology must use the most up-to-date anti virus software that is the corporate standard; this includes personal computers
9. VPN concentrator is limited to an absolute connection time of 24 hours
10. Dual tunneling is not permitted; only one network connection is allowed

5. Conclusion

The described attack puts all VPNs at risk that uses preshared keys for authentication and accepts VPN connections from anywhere like access for traveling users. The authors have also suggested policy for to provide guidelines for remote access IPsec virtual private network connections to the company's corporate network.

Acknowledgements

This work was supported by the Security Engineering Research Center, granted by the Korean Ministry of Knowledge Economy.

References

[1] http://www.linuxsecurity.com/content/view/117363/49/.
[2] http://en.wikipedia.org/wiki/vpn

[3]http://openvpn.net/easyrsa.html.

[4] http://www.tunnelblick.net/.

[5] S. Kent (BBN Corp) and R. Atkinson (@Home Network). "RFC 2406 IP Encapsulating Security Payload (ESP)"". Internet Engineering Task Force (IETF). http://www.ietf.org/rfc/rfc2406.txt.

[6] Perkins, C., IP Encapsulation within IP, RFC 2003, IBM, September 1996

[7] Deering, S. and R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 1883, Xerox PARC, Ipsilon Networks, December 1995.

[8] (http://ikecrack.sourceforge.net

[9] R. Hills, "NTA Monitor UDP Backoff Pattern Fingerprinting White Paper", http://www.nta-monitor.com/posts/2003/01/udp-backoff-whitepaper.pdf, January 2003.

[10] R. Hills, "Firewall-1 Vendor ID Fingerprinting", http://www.nta-monitor.com/posts/2004/01/checkpoint-vid-fingerprinting.html, January 2004.

[11] R. Morris and K. Thompson, "Password Security: A Case History", Communications of the ACM, Vol.22, No.11, November, 1979, pp.594-597.

[12] H. Krawczyk, M Bellare and R. Canetti, RFC 2104 "HMAC: Keyed-Hashing for Message Authentication", February 1997.