Case Study – VPN implementation with Smart Token for Company XYZ

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b Option 2

Tan Chee Horng

April 2003

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b Option 2
Tan Chee Horng

Case Study – VPN implementation with Smart Token for Company XYZ

Note: This assignment was based on a real company example, identifying facts; IP address and information have been masked to safeguard the confidentiality of the company.

Abstract

Company XYZ has a number of servers including e-mail, file, database, public web server, internal web server, etc and is protected by a firewall. The company has branches office over a few locations and a regional office. Some staffs are given Remote Access account for them to work at home, some staffs are station oversea for a few months on oversea project and we call them “mobile users”.

Presently all the mobile users are connected to the company resources via VPN using ADSL or dial-up communication channel. They are issued with a Remote Access ID and password. The main objective of this document is to conduct a study of implementing two-factor authentication using smart token with digital certificates, it include evaluation of current environment (before), define current issues and risks (during) and recommendation for management to consider (after).

Evaluation of current environment (before)

I will begin by looking at what Company XYZ presently network infrastructure had in place. The network consist of several switches, a few Window 2000 servers functioning as file, database, email, and authentication. A few Win NT servers functioning as proxy, print, anti-virus and WINS servers.

Like many other corporate perimeter defenses, Company XYZ have protected the networks from vulnerability probes and any type of attacks by configuring firewall with DMZ for public access, internal zone for internal staffs to access and close DMZ.

The networks employed two tiers of virus scanning. The first tier is an anti-virus server that will scan all email and all attachments for virus free before deliver to user mailboxes. When any email that is found to contain virus it will clean the virus, delete the attachment or email if it fails to clean the virus. The second tier is all workstation (PCs or notebooks) have to install with anti-virus client and configure for centrally managed with real time protection. The anti-virus server will update itself with new virus definition file and is done automatically daily. The anti-virus server will push the latest virus definition file to the workstation when user logon to the LAN.

Company XYZ has been rapidly expanding and there are several branch office located across the country and is undergoing a lot of changes to the way it conduct business. The few branch office users were issue with remote access account (other author may name it as VPN account) for them to access the company resources. A group of staffs (we call them mobile users) can work at home, and some of the staffs' station oversea on oversea projects need to access the company resources are given Remote Access account.

Presently the authentication method for remote access account is user ID and password. There are a few questions when using password base authentication and they are:

Is this a strong authentication method to defense again attacker?
Is there any issues or risks currently facing when using password base authentication?

This paper will discuss, current issues and risks currently are facing, and tools and technique attackers can use to perform an unauthorized logon. Ways to mitigate current issues and risks. Finally I will recommend the best way to mitigate current issues and risks.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Current Issues and Risks

1. Users created password that is easily guessed.

Users usually choose passwords that are easily guessed (spouse's name, birth date, or dog's name, etc)

If a technically savvy attacker is after a password, there are a few techniques she can try such as electronic monitoring, accessing the password file, brute force attacks, dictionary attacks, and social engineering.

In most case, the attacker develops a list of possible passwords and makes successive attempts to log on using the different passwords, this general attack as a *trial-and-error* attack.

2. Some users write down password on a sticky note.

After successfully created the password, many times user will write the passwords down on a sticky note and leave it under the keyboard, near their workstation, etc.

The attacker can easily logon without trial-and-error or using any sophisticate method to crack the password. The audit log will not be able to show any unauthorized access, as the attacker is able to logon with the first attempt.

> *The 2002 NTA Monitor password survey revealed that 49 percent of heavy computer users write their password down, or store them in a file of their PC. For lighter users with an average of 31 percentages of all users storing their password.*

> *A survey of user names and passwords conducted recently by SearchSecurity.com on 2003 revealed that 64 percent of respondents admitted to writing down passwords at lease once. The survey results point to the inherent insecurity of the most commonly used authentication mechanisms, user name and passwords.*

3. Regional office staffs are issued with Remote Access ID, the administrator locally assigns their password, users are not prompt to change password at first login.

Either the user or the password generator should create passwords. If it is impossible the user should be able to change the password at the first logon.

When using password base authentication most of the time the administrator often selects a password for a new user of a system. This can be used for the first access to the system. The system will then require the user replace this password, which the administrator had created.

In this situation when any problem surface we cannot enable nonrepudiation as there are two parties (user and administrator) know the password. The user can deny of his action, as the administrator know his password. The user can claim someone else was using their password at the time of unauthorized login and so forth.

4. System do not automatically validated a new created password meet all criteria of same password as the previous password, password complexity requirements.

The system should check that a new password is not the same as the previous password. Very sensitive applications may require that a new password not be the same as any of the previous two, three, …., N passwords.

Passwords that are created or selected by a user should be checked by the automated password system as meeting all of the criteria of the password system. The password created by user should contain both upper and lower case characters, numbers and punctuation characters. Passwords that do not meet all the criteria should be rejected by the automated password system.

This is to ensure that user created a strong password or passphrase that are not easily guessed. This is to mitigate current issue 1 from happening.

5. System do not request user to change password periodically.

Passwords should be changed on a periodic basic and must be changed whenever their compromise is suspected or confirmed.

When the same password had been used for too long. The attacker is able to be sniffing, interception and eavesdropping to sniff out the hash value of the password and with the current technology attacker is able to crack it soon or later. These allow the attacker to logon and the audit logs will only show authorize logon.

6. System does not provide limit logon attempts, when wrong password is entry more than three times (normal requirement) the system do not locked the account.

Limit Login Attempts - A threshold can be set to allow only a certain number of unsuccessful login attempts. After the threshold is met, the user's account can be locked for a period of time or indefinitely. The administrator should be the only one who can enable the account manually for the user following these events. However, there should be a maximum number of trials allowed for a password to be entered correctly. A maximum of three attempts is considered adequate for users and a security record should be maintained of the fact that incorrect passwords were entered.

7. Account harvesting when using Checkpoint VPN-1 Secure Remote

Checkpoint's VPN-1 secure remote software for VPN connection provides different error messages if a user tries to log in with an invalid username vs. a valid username but invalid password. Based on the error message generated, an attacker can determine whether or not he/she has guessed a valid username to attempt another type of attack. Combining point 1 and 6 weakness the attacker is able to make numerous wrong password entries without locked user account.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Tools/ Technique attackers can use

Port Scanner

In the Internet there are a lot of tools that a hacker can use. One of the tools is Nmap; it is a popular tool for scanning of open ports. The result of the Nmap is show below:

```
# nmap (V. 3.00) scan initiated Mon Apr 14 15:44:42 2003 as: nmap -sU -P0 -R -O -T 3
-oN Filename.log xxx.xxx.xxx.xxx (ip address)
Warning:  OS detection will be MUCH less reliable because we did not find at least 1
open and 1 closed TCP port
Interesting ports on xxx.xxx.xxx.xxx (ip address)
(The 1463 ports scanned but not shown below are in state: closed)
Port       State       Service
135/udp    open        loc-srv
137/udp    open        netbios-ns
138/udp    open        netbios-dgm
259/udp    open        firewall1-rdp
500/udp    open        isakmp
```

This tool is used to scan one of the workstation at remote site. The result show that UDP Port 259 RDP is open, UDP Port 500 is open.

From the open ports the hacker can assume that this workstation is installed with Checkpoint Secure Remote software and is using IKE for the negotiation protocol. Since Checkpoint Secure Remote software use UDP Port 259 RDP encryption to manage the encrypted session and UDP Port 500 is used for ISAKMP (IKE) key exchange between firewalls or between a firewall and a host running secure remote or secure client.

Sniffing Attacker

The attacker next step is to confirm where the host is connecting. With the use of sniffer the attack can capture the host VPN server destination IP address. IPSec provides two modes of operation, transport and tunnel modes.

In transport mode only the IP payload is encrypted, and the original IP headers are left unchanged. It allows devices on the public network to see the final source and destination of the packet.

In tunnel mode, an attacker can only determine the tunnel endpoints which is the VPN gateway IP address and not the true source and destination of the tunneled packets. In most cases, when deploy IPSec tunnel model will be used.

Upon capture of the destination IP address the attacker can use other tools to identify and confirmation on the IPSec VPN server been used. One of the tool that attacker can use is NTA Monitor VPN Discovery and Fingerprinting Technique

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

NTA Monitor VPN Discovery and Fingerprinting Technique

NTA Monitor VPN discovery and fingerprinting technique allows organizations to test their own networks to see what information a hacker could discover and close any holes before they can be exploited. When been use by an attacker it is a great tool for discovering and confirmation of an IPSec VPN server, fingerprint which implementation of an IPSec VPN server is being used.

Below show the result when using the NTA IKE-SCAN, it successfully show the correct type of firewall the company is using. (The live IP address is replaced with xxx for security reason)

```
C:\ikeScan>ike-scan xxx.xxx.xxx.xxx
Starting ike-scan 1.2 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx) Notify message 9101 [Checkpoint Firewall-1 4.x or
NG Base]

Ending ike-scan 1.2: 1 hosts scanned.  0 returned handshake; 1 returned notify

See http://www.nta-monitor.com/ike-scan/ for details.
See http://www.nta-monitor.com/ike-scan/whitepaper.pdf for the white paper.
```

Upon confirmation that Checkpoint firewall is being used an attacker can easily download Checkpoint Secure Remote install program and install into any PC.
After that an attacker can start to use account harvesting to find out a list of user ID.

Account Harvesting

Attackers can often discover valid usernames for a particular applications using technique called account harvesting.

Account harvesting is a good example of a technique that has been applied to all kinds of systems and applications. Using this technique, an attacker can determine legitimate userIDs and even passwords of a vulnerable system or application. Account harvesting is a very simple concept, targeting the authentication process when a system or application is using the single-factor authentication of using userID/password combinations to prove identity. Systems or applications that generate different error messages for wrong user logon ID and wrong password are vulnerable to this type of attack. Based on the type of error message, an attacker can customize an attack that first determines a valid user logon ID and then uses other forms of password cracking techniques to get the password.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

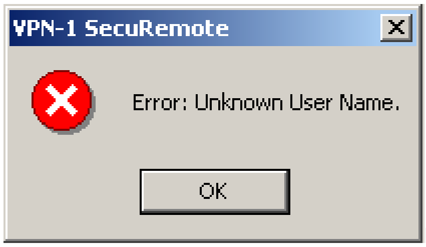
Possible Login States

State #1 Valid Username Valid Password	***State #2*** Valid Username Invalid Password
State #3 Invalid Username Invalid Password	***State #4 (Impossible)*** Invalid Username Valid Password

Figure 1

Source from: SANS Security Essentials with CISSP CBK Version 2.1 Volume One, SANS Press

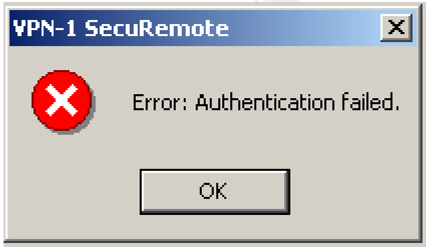
As an attacker of getting to State #1: a valid username and password combination is almost impossible unless the attacker is very lucky star on that day or a sticky note can be found with user ID and password. An attacker will start by first trying to compile a list of valid login names, and only spend his time guessing passwords to those accounts that is valid. That's where account harvesting comes in; it's a method of compiling this list.



Error: Unknown User Name.

Figure 2

An account harvester will start by trying some obviously bogus login names and some junk passwords, trying to get to State #3 (Figure 2). If an attacker is really exceptionally lucky star on that day, there's an possible that the bogus login names and "junk password" could be valid and he could end up in State #1 with a successful login, but it's more likely that it ended up in State #2 (Figure3). He would have guessed a valid user ID, which is exactly what an attacker is looking for when harvesting accounts.



Error: Authentication failed.

Figure 3

Once an attacker determines a list of valid user logon ID he can use other forms of password cracking techniques to get the password. If the target system or application doesn't lock out user account due to a given number of invalid password attempts, the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

attacker can write a script with the user ID previous harvested and try password guessing of using trial-and-error, dictionary attacks, brute force attacks and social engineering.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Mitigating Current Issues and Risks (during snapshot)

After identify the current issues and risks by using password base authentication, an in-depth review of using two-factor authentication was conducted.

Two-Factor Authentication

Two-factor authentication is much stronger than passwords based authentication. It unique in its strength because it does not rely exclusively on something a user know, with addition of something that a users have to present two forms of identification before gaining access to protected resources. The combination proves that users are who they say they are. This devices or things that a user has are sometimes referred to as smart cards or smart tokens. The smart cards or smart tokens are unique and not easily replicable.

Something you have: This factor includes keys, cards, tokens and so on. These things can also be stolen or lost.

Something you know: Passwords and PINs are examples of this factor. It is important to note that this knowledge can be lost, shared or guessed by others.

Two-factor authentication comes in many options and each type has benefits, disadvantage and costs. Common methods include:

Digital Certificates

Digital Certificates help identify users by requiring access to digital credentials that should only be used by the rightful owner. Digital certificates are issued to users from a trusted party. Digital certificates provide the most secure and scalable way to implement a VPN by giving companies the power to control user access, provide strong authentication and non-repudiation. The certificate management support for certificate life cycle through the use of Certificate Revocation Lists (CRLs)

Smart Cards and Smart Tokens using Digital Certificates

There are two major types of smart cards and smart tokens, those that use digital certificates and those that use a proprietary algorithm. Using smart cards or smart tokens with digital certificates is one of the strongest levels of authentication service. Accessing to the smart card is protected with two-factor authentication, key pairs can also generated and stored on the smart card. The private key never leaves the card or token, so it can never be accessed by unauthorized users or copied to another location.

Smart cards look like a credit card with a small-embedded computer chip, and require the use of a smart card reader. Smart tokens are technologically same as smart cards with the exception of their interface. Smart tokens are small in size like a house key and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

can be plugged directly into the Universal Standard Bus (USB) ports found in most computer or notebook nowadays.

Password generation tokens

A password generation token creates a unique password each time it is used. The password is generated from a secure algorithm that is based on both a unique user ID and the current time. A PIN is needed to activate the password generation token and assure that it becomes useless if it is lost or stolen.

Recommendation

My recommendation to migrate the current issues and risks is to use smart token with using of digital certificates.

The reasons for using smart token over smart card are:

1) Smart tokens are small in size, are similar to a house key, can easily fit on a key chain.
2) Smart tokens can simply plug into USB ports commonly found on most modern computers/notebooks.
3) No additional device is needed to read the data, unlike smart card need a smart cards reader.
4) Most Operating Systems have USB drivers built-in that utilize plug-and-play techniques to load the required smart token drivers.
5) Data transfer speed is much faster for USB port compare to traditional parallel or communication port connection for smart card reader.
6) Most notebook has limited number of communication port and parallel port, sometime this port are needed for other usage and leaving no port for the smart card reader.

Using Smart Token with Digital Certificates

Using of digital certificates is more secure than using a password but the security of certificates and keys is still at risk when they are stored on PC, laptop and floppy disk, and transmitted across a network. This is being the certificate and keys can be duplicated via copy easily. Therefore many certificate management systems support the use of tamper-resistant cryptographic hardware, such as smart card or smart token.

Certificates and keys are store securely on the smart token, allowing for portability of security credentials between computers, while protecting the user’s private key. When a certificate is issued, it is saved with its keys directly onto the smart token. To use it most smart token require the user plug the smart token directly into the USB port and enter the smart token password. After successfully authenticated the smart token password, the certificate or private key store on the smart token is used for authentication to the requested remote site Certificate Authority (CA).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

There are different brand of smart token that can be found in the market and mostly are using the two-factor concept with different feature.

One of the smart token brands that can be found in the market is Aladdin Knowledge Systems (Nasdaq: **ALDN**). This company is a leader in digital security, providing organizations with award-winning solutions for software commerce and Internet security. One of the Internet Security Products they are selling is smart token that they name it eToken (Trademark). The solution I recommended is based on Aladdin eToken feature.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Enhanced Security (after snapshot)

The recommendations in the previous section do not eliminate the risks totally but should be able to reduce the current issues and risks that remote access via VPN connection that are facing to an acceptable level.

With the use of two-factor authentication it greatly improves the assurance of the authentication. The administrator can assurance that it is the right person is who is accessing the corporate network via VPN. Attacker cannot access the corporate network via VPN without the token. Should user loss the token and without the personal token password the attacker also cannot access the corporate network via VPN unless user write down the password and stick it on the token.

Administrator can issue the token to regional office staffs and assigns the token with a password. The use of token is a compensate control for the administrator who create and know the password. Once the user received the token he or she cannot deny of his or her action. For Aladdin eToken they provide a password quality tool for validating of a new password user had entry that meet all criteria in accordance with the organization password quality policy.

Most certificates also have a validity periods of one year, define by issuer, after that a new certificate will be issued to the user. Therefore users do not need to periodically change the password. With a 1024-bit key been used it take an attacker a projected time of 3 million years to break according to RSA press, PKI Implementing and Managing E-Security. When users suspect any compromise of the certificate issued to him or her, the certificate can be revoked.

The eToken will be deactivated should token password is entry wrongly that hit the threshold set by the administrator. When this happen the user certificate will not be able to be used for authentication until an administrator reset the eToken.

There is no way an attacker can do an account harvesting of userID because two-factor authentication requires the eToken itself that had already identify the user, together with the eToken password.

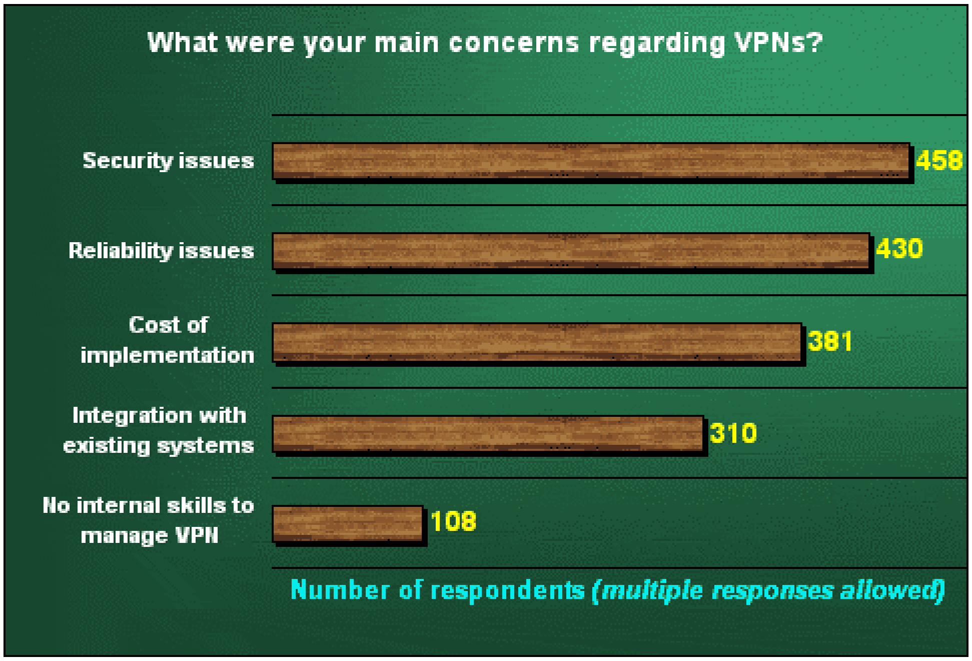
Conclusion

VPN is equal to user inside the company. When an hacker is able to get hold any VPN account (user ID and password) it is the same as the hacker had break through your physical security in the company and the hacker can start study resources in the company and planning another stage of attack.

Hacker is the same as robbery who want to rob a bank. The robbery will not rob a bank without planning. He will study when the bank will have a lot of money, how many security guard is inside the bank, how to break the save code, how soon he much get out of the bank, how far and how soon the local police will reach the bank upon alarm bell activated, the route to escape from the bank. There are more items the robbery will think of when planning to rob the bank.

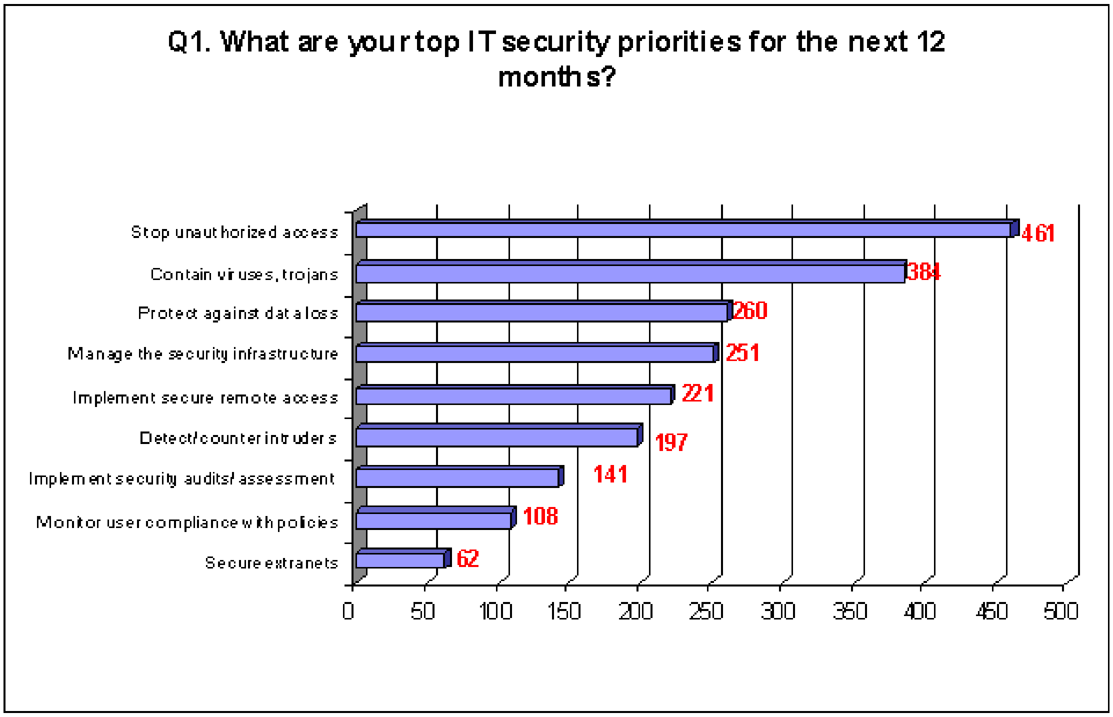
Strong authentication must be implemented to a VPN, but we cannot depend on strong authentication along. Do not forget of having a security-in-depth or layers security to have complete defenses of your assets.

Appendix A



Source: CMP VPN Survey 2002 - An Executive Report

The main concerns that most respondents had with regards to VPNs were security - especially in the form of external intrusions, and viruses - and reliability. This result is not surprising, given the fact that VPNs utilize the Internet as the primary network data carrier.

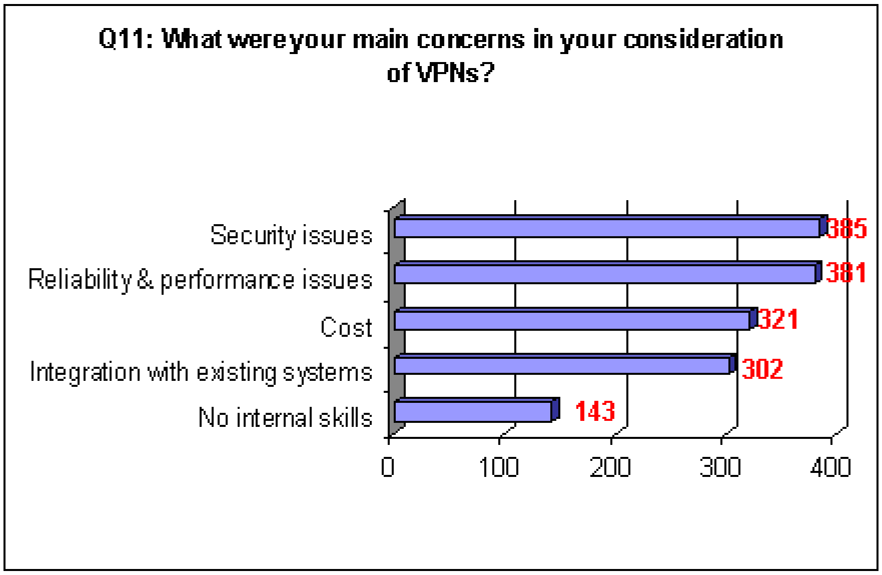


Source: CMP Net. Asia VPN Knowledge Centre Security Survey April 2003
- An Executive Report

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix A

According to our respondents, the top two priorities for 2003 were to prevent unauthorized access and intrusion into their corporate network, and to contain viruses, Trojans and other malicious code from entering and proliferating in their organization. Interestingly enough, the increasing importance of protecting against data loss shows that organizations are beginning to see the need for business continuity solutions, given the current climate. Finally, organizations are also gearing themselves to cope with an increasingly complex security infrastructure that has resulted from the implementation (over time) of multiple point products from various vendors



Source: CMP Net. Asia VPN Knowledge Centre Security Survey April 2003
- An Executive Report

The main concerns that most respondents had with regards to VPNs were security - especially in the form of external intrusions, and viruses - and reliability. This result is not surprising, given the fact that VPNs utilize the Internet as the primary network data carrier.

References

Harold F. Tipton Micki Krause, Volume 3 “Information Security Management Handbook” 4th Edition, Auerbach Publications

Shon Harris, All In One CISSP Certification Exam Guide, McGraw Hill

Stuart MCClure, Joel Scambray, George Kurtz, “Hacking Exposed Network Security Secrets & Solutions” Third Edition, Osborne/McGraw Hill

Richard E. Smith, Authentication From Passwords to Public Keys, Addison – Wesley

Andrew Nash, William Duaned, Celia Joseph, Derek Brink, PKI: Implementing and Managing E-Security, RSA Press

Carlton R.Davis, IPSec Securing VPNs, RSA Press

Federal Information Processing Standards Publication 112, Announcing the Standard for PASSWORD USAGE. URL
http://www.itl.nist.gov/fipspubs/fip112.htm

CMP Net.Asia VPN Survey 2002 - An Executive Report. 2002. URL
http://www.cmpnetasia.com/tech_guide/vpn/vpn_survey.cfm
http://www.cmpnetasia.com/tech_guide/vpn/vpn_concern.htm

CMP Net.Asia VPN Knowledge Centre Security Survey April 2003
- An Executive Report. URL
http://www.cmpnetasia.com/tech_guide/vpn/security_survey_result.cfm
http://www.cmpnetasia.com/tech_guide/vpn/q1.htm
http://www.cmpnetasia.com/tech_guide/vpn/q11a.htm

NTA Monitor calls on Industry to help users address personal IT Security URL :
http://www.nta-monitor.com/Password-survey-press-release_trade_final.doc

Password Survey/ 64 Percent Write Passwords Down Compromising Corporate Data URL:
http://www.hostingtech.com/news/2003/4/29/Print/St_Nitf_Password_Survey_64_Percent_Wri_p0428003.5rw.html

Well Known Port Numbers (last updated 2003-06-18) URL:
http://www.iana.org/assignments/port-numbers

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checkpoint Known Ports URL:
http://storm.myhome.homeip.net/CP_port_number.html
http://www.phoneboy.com/fom-serve/cache/405.html

The SANS Windows Security Digest
A Resource for Computer and Network Security Professionals, Volume 4, Number 11, November 30, 2001 URL:
http://www.security.unicamp.br/docs/informativos/2001/11/b17.txt

Cisco – IPSec
White Paper IPSec Executive Summary URL:
www.cisco.com/warp/public/cc/so/ neso/sqso/eqso/ipsec_wp.htm

Two-Factor Authentication – Making Sense of all the Options URL:
http://www.itsecurity.com/papers/rainbow2.htm

Product Brief, iKey^{tm} 1000 Series – Smart Devices for Two-Factor Authentication URL: http://www.rainbow.msk.ru/ua/iKey1000_pb.pdf

Gaining Access Using Application and Operating System Attacks – Part I, Edward Skoudis, URL: http://www.chi-publishing.com/portal/backissues/pdfs/ISB_2001/ISB0608/ISB0608ES.pdf

VPN Discovery and Fingerprinting Technique Executive Overview URL:
http://www.nta-monitor.com/ike-scan/
http://www.nta-monitor.com/ike-scan/whitepaper.pdf

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.