Journal of the Korean Nuclear Society
Volume 36, Number 4, pp.346~356, August, 2004

《Technical Note》

Vulnerability Analysis on a VPN for a Remote Monitoring System

Jung Soo Kim, Jong Soo Kim, Il Jin Park, Kyung Sik Min, and Young Myung Choi
Korea Atomic Energy Research Institute
150, Deokjin-dong, Yuseong-gu, Daejeon, 305-353, Korea
kjs@kaeri.re.kr

(Received November 7, 2003)

Abstract

14 Pressurized Water Reactors (PWR) in Korea use a remote monitoring system (RMS), which have been used in Korea since 1998. A Memorandum of Understanding on Remote Monitoring, based on Enhanced Cooperation on PWRs, was signed at the 10th Safeguards Review Meeting in October 2001 between the International Atomic Energy Agency (IAEA) and Ministry Of Science and Technology (MOST). Thereafter, all PWR power plants applied for remote monitoring systems. However, the existing method is high cost (involving expensive telephone costs). So, it was eventually applied to an Internet system for Remote Monitoring. According to the Internet-based Virtual Private Network (VPN) applied to Remote Monitoring, the Korea Atomic Energy Research Institute (KAERI) came to an agreement with the IAEA, using a Member State Support Program (MSSP). Phase I is a Lab test. Phase II is to apply it to a target power plant. Phase III is to apply it to all the power plants. This paper reports on the penetration testing of Phase I. Phase I involved both domestic testing and international testing. The target of the testing consisted of a Surveillance Digital Integrated System (SDIS) Server, IAEA Server and TCNC (Technology Center for Nuclear Control) Server. In each system, Virtual Private Network (VPN) system hardware was installed. The penetration of the three systems and the three VPNs was tested. The domestic test involved two hacking scenarios: hacking from the outside and hacking from the inside. The international test involved one scenario from the outside. The results of tests demonstrated that the VPN hardware provided a good defense against hacking. We verified that there was no invasion of the system (SDIS Server and VPN; TCNC Server and VPN; and IAEA Server and VPN) via penetration testing.

Key Words : remote monitoring, vulnerability analysis, penetration testing, virtual private network, safeguard.

1. Introduction

A remote monitoring system can provide technical advantages, such as reductions in inspections and exposure to radiation. In addition, it is less intrusive to facility operators. However,

an RMS also has drawbacks, such as the possible loss of information surety, a heavy initial investment, and transmission cost. In Korea, remote monitoring systems have been in operation as a part of an enhanced cooperation with the IAEA to reduce the safeguards efforts in PWRs, following the recommendations of a working group from the IAEA and Korea, since August 2000. Before August 2000, under the responsibility of the Korean support program, one reactor was using remote monitoring. At the moment, fourteen reactors are operating with remote monitoring systems. At the moment, the IAEA operates 57 cameras, 20 Facilities, 8 countries, 4 continents and 238 MB of downloaded data per day [1]. Roughly 40 % of the IAEA surveillance cameras installed worldwide are in Korea. Korea launched an extensive program to use remote monitoring systems in PWRs, following both the recommendations of the working group between Korea and the IAEA for enhanced cooperation of integrated safeguards and a task of the Member State Support Program (MSSP). All PWRs were equipped with digital surveillances and seals as a part of the digitization of the C/S, which assists the RMS inspection regime. Since the installation of a remote monitoring system at Younggwang #3 in October 1998, fourteen reactors have acquired operating remote monitoring systems.

TCNC established the Central Monitoring Station (CMS) for the evaluation, reception, and relay of remote data. It houses a hub station that was supplied by the IAEA. Remote data from the surveillance devices and the seals in the reactors are transmitted to the hub station via telephone and to the IAEA via a frame relay from the hub station. Three PWRs were selected for rehearsal and are being evaluated for a nationwide application. If the rehearsal for three reactors is successful, remote monitoring will be expanded to all the PWRs in Korea [2]. Figure 1 shows the configuration of the CMS for the transfer of image data to the IAEA. In this figure, the frame relay link is used to the IAEA from Korea. The advantage of a frame relay is that it is a reliable and permanent link; however, it is very expensive.

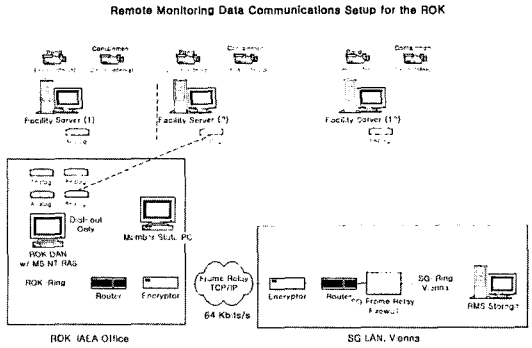

Fig. 1. The Configuration of CMS for Transferring Image Data to the IAEA

Figure 1 shows that the facility server' s image data is transferred to the server at the Central Monitoring Station (CMS). The communication is made through the public switched telephone network (PSTN) via a 56 Kbps modem. There is some limitation for a full communication speed of the modem within an analog communication. Figure 2 shows the remote monitoring system at

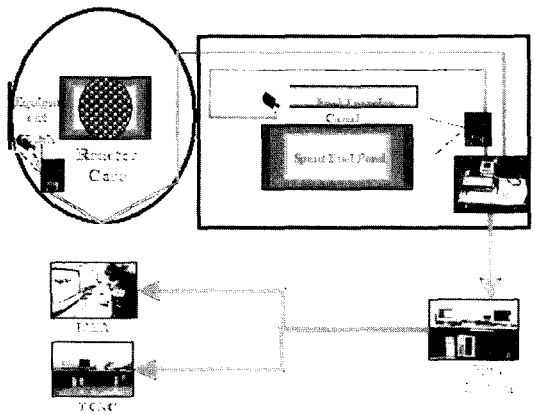

Fig. 2. Remote Monitoring System at Kori-2

Kori-2.

With the existing system, the communication cost using telephone lines were estimated at about $66,000 per year. Due to the high communication fee, the IAEA and Korea wanted to replace the current telephone line with an Internet line. The IAEA and KAERI are carrying out the Member State Support Program (MSSP) "Implementation of Virtual Private Networking (VPN) for Remote Monitoring" to apply the VPN to the existing remote monitoring systems. The program is progressing in three phases: Phase I is a Lab test; phase II is to apply the VPN to a target power plant; and Phase III is to apply the VPN to all the power plants. This paper reports on the penetration testing of Phase I. Phase I involved both domestic testing and international testing. The target of the testing consisted of a SDIS Server, IAEA Server and TCNC Server. In each system, VPN system hardware was installed, and the penetration of the three systems and the three VPNs was tested. The domestic test involved two hacking scenarios: hacking from the outside and hacking from the inside. The international test involved one scenario from the outside. Figure 3 shows the configuration of the Phase 1 Lab tests.

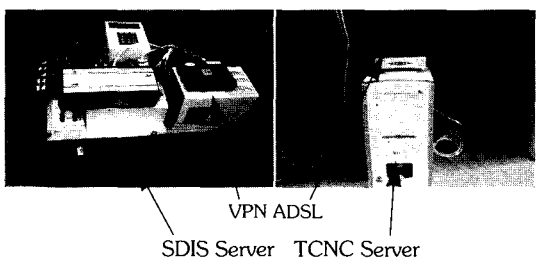

Fig. 3. The Configuration of the Phase 1 Lab Tests

In this paper, section 2 of this paper describes the Virtual Private Network and the Internet Protocol Security (IP Sec) communication. Section 3 describes the communication configuration between the IAEA and the TCNC for the test. Section 4 describes the penetration analysis of the tests of the three systems and the VPN, including the hacking scenarios and hacking test results. Section 5 presents our conclusions.

2. Virtual Private Network and IPSec Communication

Virtual Private Network is the concept of constructing a Private Network using the Internet or a public network. The technology for the VPN used IP security or IPSec and Non-IPSec for constructing the VPN[3-6].

2.1. IPSec Communication

IPSec defines the packet layer security protocol that is performed to ensure privacy, integrity, and authenticity of communication within the Internet. Using IPSec, it is possible to construct an independent security network. IPSec is supported from the Authentication Header and Encapsulating Security Payload. To communicate with IPSec, it is necessary to exchange identification information (Internet Key Exchange [IKE]: Key exchange protocol) between systems before communication. IKE communication is compared or negotiated with some mediation parameters in the authentication method, encryption algorithm etc, at two hosts. The IKE communication method is called the Security Association (SA). For the identification and encryption data in an IKE communication, IKE processes Phase 1 and Phase 2. At Phase 1, it negotiates the SA and then finishes the SA. In Phase 2, it communicates the encrypted data. There are two modes for negotiating the SA during Phase 1: a main mode and an aggressive mode. The vulnerable identification of the security at the Phase 1 step is that hackers try the "Brute Force Attack" of Hash value exchanged with the

ID/Password or Public Key at intervals between two points of time. As shown in Fig 4, a cracking attack of the public key is performed between "③" and "④".

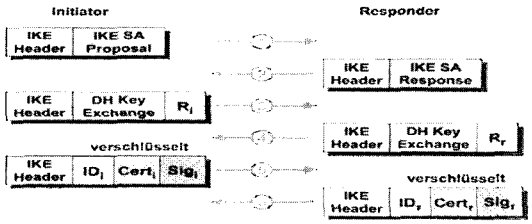

Fig. 4. Processing the Negotiation of SA in IKE

2.2. Contents for the Fitness of Security of a Section on VPN

A hacker is checking for the key crack by packet sniffing at the IKE' s process of the VPN + firewall device. The hacker gives a hacker' s mind to the possibility of the crack of the encrypted data and the fitness of the security of the encrypted data using the forged IKE packet.

3. The Communication Configuration for the Test Between the IAEA and the TCNC

The VPN device used in the NS5XP was made by Netscreen Co. The hardware version of the VPN is 3010 and the OS version is 4.0 or 6.0. NS5XP is composed of both untrusted and trusted Internet Protocols (IP) used for the Network Address Translation (NAT). In the case of the Untrusted, IP used for the Public IP (Asymmetric Digital Subscribed Line(ADSL) IP). Otherwise, in the case of the Trusted, IP used for the Private IP (10.x.x.x). The communication method likes this. In the case of the IAEA and SDIS Server, the IAEA Server requested at every hour was taken from the SDIS Server' s image data that took a picture every minute in the DCM-14. In the case of the TCNC and SDIS Server, the TCNC server was taken from the SDIS Server' s image data at the designated hour per every day. The configuration of the VPN device consisted of the window display of the NS5XP. The important configuration likes the IPSec Phase 1 configuration, IPSec Phase 2 Configuration, Policy Configuration and so on. Fig. 5 shows the initial display of the NS5XP.

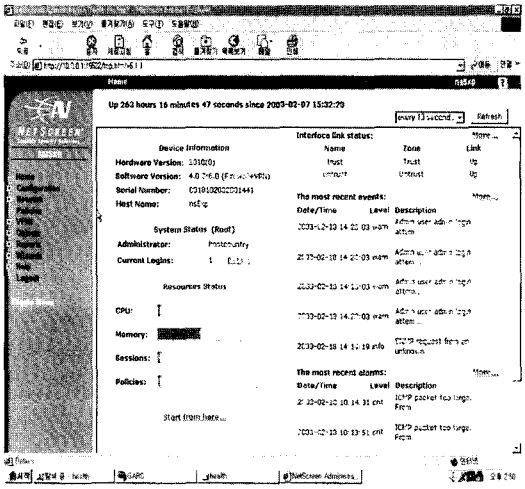

Fig. 5. The Initial Display of NS5XP

From Fig. 5, the NS5XP driven by the pull down menu is shown on the left side. The configuration of the VPN needs IP information for the two systems, and the encryption algorithm for the IPSec. From Sec. 2, IPSec supported the IKE. IKE makes the process for Phase 1 and Phase 2. Fig. 6 shows the configuration of the Phase 1 parameters. From Fig.6, the authentication method is Pre-shared, encryption is 3DES, Hash algorithm is SHA-1 and the Diffie-Hellman algorithm is 1024 bit. The result of Phase 1 consists of the IKE tunneling. Fig. 7 represents Phase 2 of the IPSec. Phase 2 of the IPSec exchanges the mediation parameters using IKE tunneling. That is, it exchanges the ESP

(Encryption Security Protocol) through the Policy and exchanges it for the new key value generated by the 3DES and MD5 algorithm.

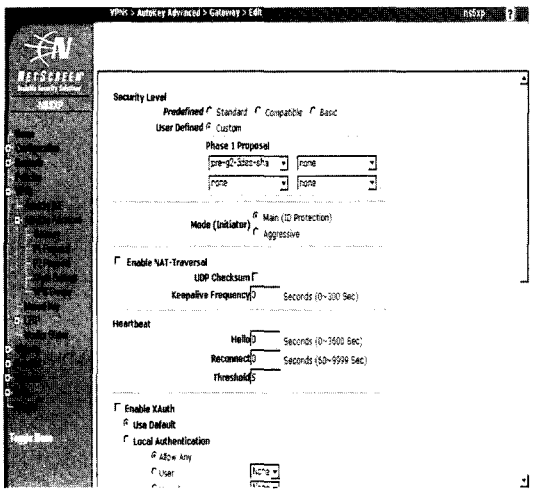

Fig. 6. The Configuration Display of IPSec Phase 1

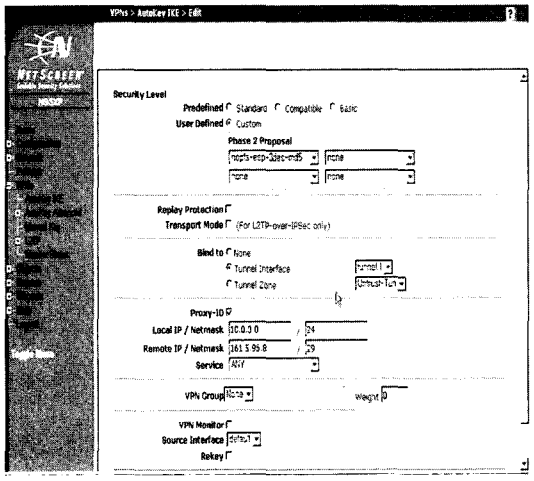

Fig. 7. The Configuration Display of IPSec Phase 2

At last, the configuration of the Policy is considered. The Policy of the VPN consisted of the configuration between the server and the client. For example, if we configured it to deny the ping command or Internet, then the VPN does not respond while the ping command reaches the client from the external. Fig. 8 shows the configuration of the policy of the VPN. Fig. 9 shows the status of the communication data at the VPN captured by the Network Sniffer that used the network monitoring software. In this figure, the hidden part means the encrypted data. After tunneling, it exchanges the encrypted data using the VPN. The normal data shows the ASCII type, but the encrypted data is the hidden type.

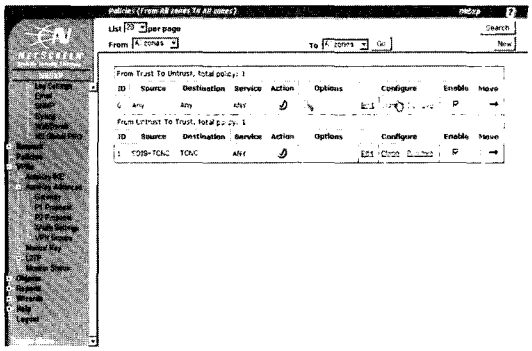

Fig. 8. The Configuration of the Policy of VPN

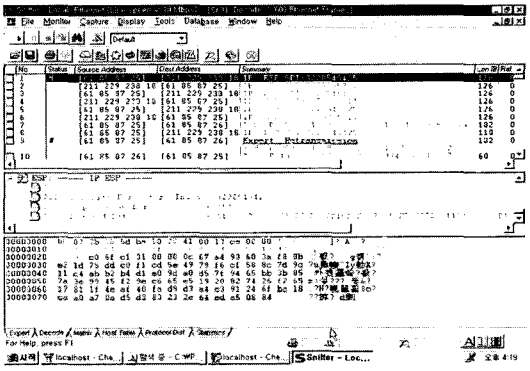

Fig. 9. The Encrypted Data Using VPN

Fig. 10 shows an example of the image data (decrypted data) from the SDIS Server to the TCNC Server. From Fig 9, the image of SDIS server communicates with the encrypted data to TCNC server. When the communication process finished, then the communication data decrypted.

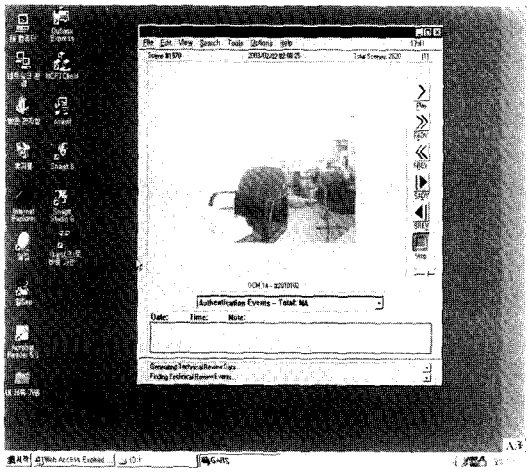

Fig. 10. The Image Data from the SDIS Server

4. Hacking Test for Vulnerability

The hacking method of the VPN was not used for the general TCP/IP hacking tool due to the IPSec' s encrypted communication of the IP security protocol. It should be noted that, because the scanning of the open ports of the target system is not known as a typical hacking method, due to the packet-filtering policy of the VPN + Firewall, the method of hacking was very limited. We decided to perform the penetration test for the vulnerable parts of the IPSec protocol, where the Inter Key Exchanged occurred in the communication process between Phase 1 (Main/Aggressive Mode) and Phase 2 mode (Quick mode).

4.1. Domestic Hacking Test

4.1.1. External Hacking

Assuming that a hacker is only recognized at the IP information stage of the target system (VPN+Firewall), Unauthorized External Hacking is to check out the port scanning of the target server and to scan for the vulnerable identification. In the case that the high risks existed from the vulnerable identification, a hacker tries to get the administrator' s authority using hacking tools. When the hacker did not get the administrator' s authority, the penetration test came to an end. The hacker' s computer was connected to the external network and scanned by the VPN + firewall device. The hacker tried to attack by using a forged IPSec/IKE packet, and communicated with the target system using the forged IPSec communication. Through this process, the hacker made a judgment on the acquired possibility of actual data and of the encryption key using IPSec packet sniffing. Figure 11 shows the routing path for the attack of an external network.

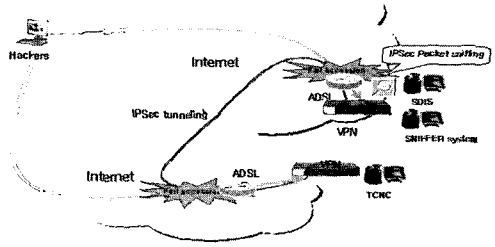

Fig.11. The Routing Path for Attack in an External Network

4.1.2. Internal Hacking

The hacker' s computer is directly connected to the trusted network and tries to attack by using a forged IPSec/IKE packet and packet sniffing at the VPN + firewall gateway or at the remote Server/VPN + firewall device. Figure 12 shows the routing path for the attack of an internal network

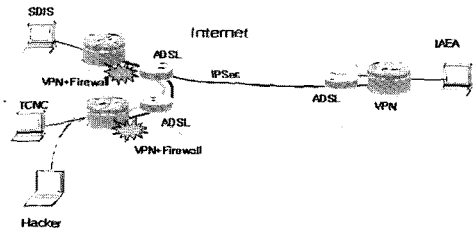

Fig.12. The Routing Path for Attack in an Internal Network

4.1.3. Results from Hacking of the Target System

Table 1 shows the results of the hacking test.

Table 1. Results from Hacking Test of the Target System

Type of scenario	Target (server/ VPN device)	IP address	Result
External Hacking	SDIS Server	211.x.x.x	Fail
	TCNC Server	61.x.x.x.	Fail
	SDIS VPN+Firewall	211.x.x.x.	Fail
	TCNC VPN+Firewall	61.x.x.x	Fail
Internal Hacking	SDIS Server	10.x.x.x	Fail
	TCNC Server	10.x.x.x	Fail
	SDIS VPN+Firewall	10.x.x.x	Fail
	TCNC VPN+Firewall	10.x.x.x	Fail

4.1.4. Information Profiling of External Hacking Test

To gather the gateway device' s information connected to the SDIS/TCNC server, the hacker used "nmap"(port scanning tool), based on Linux. Port scanning was performed to consider the User Datagram Protocol (UDP) and TCP ports. The scanning result of the UDP port was that multiple ports of the UDP opened at the SDIS VPN + firewall (211.229.238.129) device. Figure 13 shows the open port information of the UDP using the "nmap" tool.

The result of the TCP port scanning was that it opened at the 8888 port of the TCP

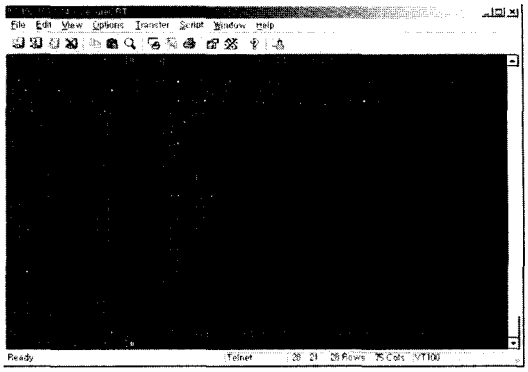

Fig.13. UDP Port Scanning for a SDIS VPN +Firewall

(Transmission Control Protocol), while the other ports of the TCP were inaccessible.

And the other method for the external Hacking used to traceroute using User Datagram Protocol (UDP) and traceroute using Internet Control Message Protocol(ICMP). Fig. 14 shows that the Hacker used the "traceroute" command in the UNIX and searched for the routing path. However, due to the isolated UDP protocol at the VPN + firewall gateway, the hacker failed to determine the network structure. In Fig. 14, "*" indicates that the packet filtering was isolated and that it was impossible to search for the routing path.

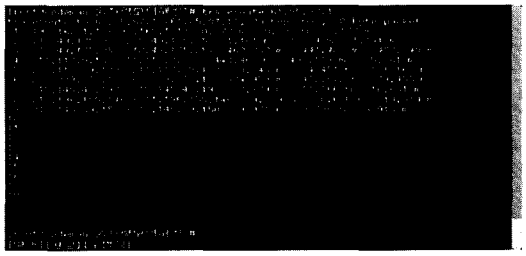

Fig. 14. UDP Traceroute of a TCNC'

As an isolating UDP Protocol, the hacker used the "tracert" command in the Windows Operating System (ICMP protocol) and searched for the routing path. Figure 15 shows that the hacker found the routing path using the tracert command.

The result was that it was impossible to search for the routing path.

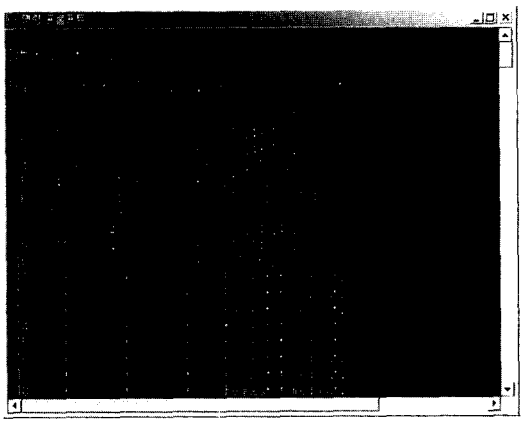

Fig. 15. ICMP Traceroute of a SDIS VPN +Firewall Device

4.1.5. Information Profiling for IPSec Protocol at VPN + Firewall

Before IPSec tunneling of the VPN, the VPN + firewall was exchanged for the identification using the "Backoff" function (VPN client was already sent to the server (IKE Security Association Request packet) but the server responded to the responding packet and the client had no response at the server packet. When the hacker sent the requested packet identified by the VPN + firewall device, the device did not respond to either the requesting packet or the generated timeout message. The hacker failed to identify the VPN device. In Fig. 16, the packet was normal for ten numbers of the responding packet from the VPN + firewall at the SDIS Server, but a few of the responding packets were received, which indicates an identification failure.

Fig. 16. Forged IKE Scanning in a SDIS VPN +Firewall

Figure 17 shows how the hacker tried to scan the forged IKE packet at the IKE phase 1 step (main mode) in the TCNC VPN + firewall. The hacker scanning failed, due to the unanswerable message from the VPN + firewall gateway

Figure 18 shows that the hacker sent the forged Initiator IKE Request packet in an aggressive mode of an IKE Phase 1 and then waited for the response of the VPN + firewall gateway. The unanswerable message from the VPN + firewall gateway prevented the hacker from scanning.

Fig. 17. Forged IKE Scanning in a TCNC VPN+Firewall Device

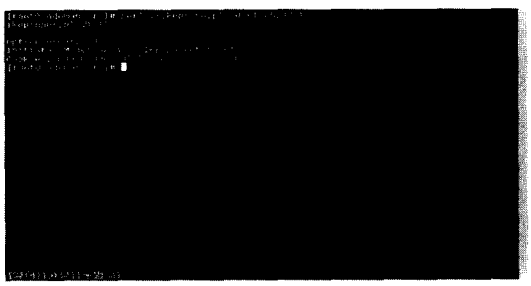

Fig. 18. Scanning the Forged Packet in an IKE Aggressive Mode

4.1.6. Internal Hacking

From 2.2, the hacker analyzed the possibility of

key extraction in the IKE's authenticated exchange protocol. The result was that the hacker was shown the cookie value between the VPN client (Initiator) and the VPN gateway (Responder). The cookie value was randomly produced, and the attack using forged identification failed. Key sniffing also failed. Figure 19 shows that the packet contents for exchanging the cookie before the two hosts were communicated to the IPSec.

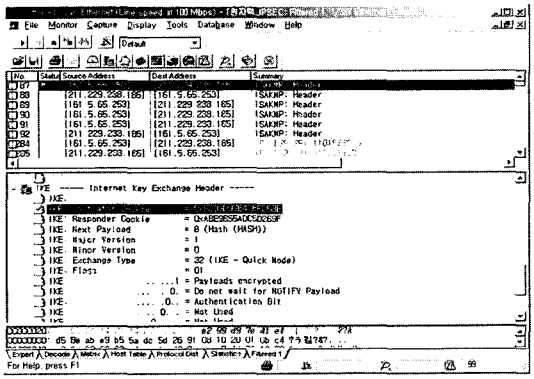

Fig.19. Capture of IKE (ISKMAP) Packet

4.1.7. Internal Hacking Test

To gather the gateway device's information in a trusted network (internal), the hacker used the "Nmap" (port scanning tool) based on Microsoft Windows. The scanning result failed to access the packet.

The result of port scanning at the trusted network in the TCNC VPN + firewall was that the TCP 15522 port existed in the Web administrator mode of the VPN device. The hacker tried to connect, but the authentication window of the user was displayed. The hacker tried to attack the user ID and password using a brute force program, but failed to get the password or to authenticate the administrator (refer to Figs. 20 and 21).

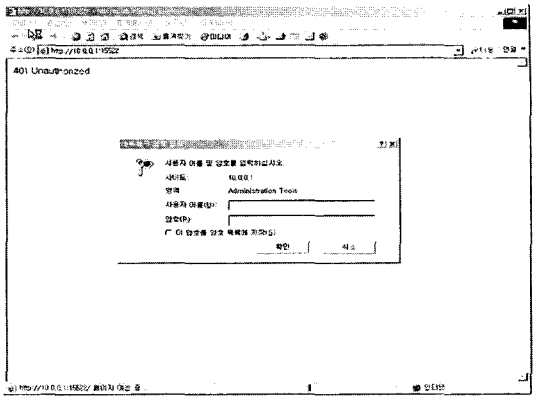

Fig. 20. Administrator Authentication of Netscreen-5xp (VPN device)

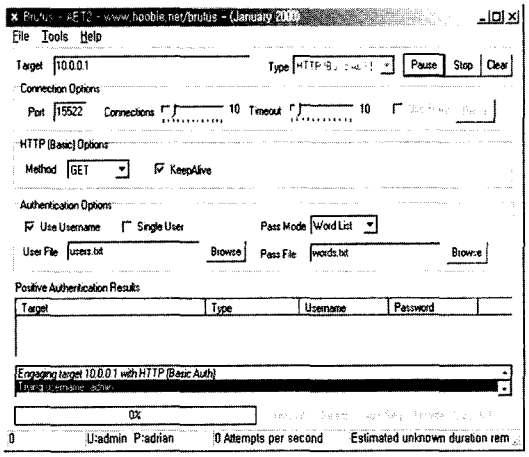

Fig. 21. Brute-force-attack for the WEB Administrator ID/Password

Finally, the hacker tried a denial of service(DoS). DoS(Denial of Service) was attempted for the attack of the Tursted and Untrusted network. At the trusted network in the TCNC server, the hacker tried to put in garbage data (DoS) at the TCNC VPN + firewall device. As a result, the CPU load of the VPN + firewall device was high, and the speed of this device became very slow. The low of speed represented the vulnerability identification of the device (refer to Figs. 22 and 23).

Fig. 22. DoS Attack on the Trusted Network in the TCNC VPN +Firewall Device

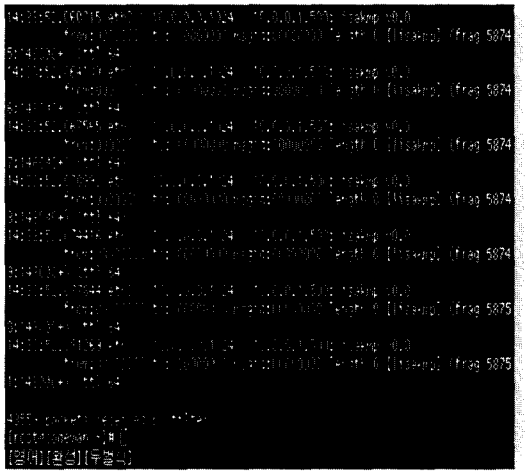

Fig.23. Packet Dump Against DoS in the IKE (UDP 500 port)

4.2. International Hacking Test for Penetration

4.2.1. Hacking Method and Result

An international hacking test was performed for fours days. During the first two days, the hacker attacked the IAEA server and for the remaining two days, the hacker attacked the SDIS server.

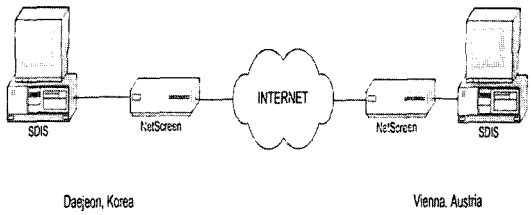

Fig. 24. The Configuration of Target System for International Hacking

Figure 24 shows the attacking system.

The international hacker's initial probes and tests of the VPN environment at each location did not return any adverse findings. The devices tested appeared to be completely filtered and did not respond to the Internet Control Message Protocol (ICMP) "pings" or other network probes.

Since these probes and scans with nmap yielded no findings, a manual validation was performed to ensure accurate results. These manual testing attempts also yielded no responses and validated the results from the nmap probes. Penetration attempts were unsuccessful.

The assessment also involved saturation attempts on the DSL links to determine if the configuration is susceptible to denial-of-service attacks. During this testing, the links in Daejeon and Vienna were saturated with traffic during two separate periods, each for approximately one hour in duration. When the attacker halted the network flooding, services were quickly restored. Since the links do not carry time sensitive data, the objectives would not be affected by denial-of-service attacks.

5. Conclusions

This paper has reported on the penetration testing for a VPN applied to an existing RMS. The existing remote monitoring system's communication cost was estimated to be about $66,000 per year. Owing to these high

communication fees, IAEA is now conducting a study on using the Internet to replace the telephone line that is currently used for communications. The use of the Internet, however, entails data security concerns. IAEA and Korea want to replace the current telephone line with the Internet line using VPN. The IAEA and KAERI are carrying out the Member State Support Program (MSSP) "Implementation of Virtual Private Networking (VPN) for Remote Monitoring" to apply the VPN to the existing remote monitoring systems. The program is progressing in three phases: Phase I is a Lab test; phase II is to apply the VPN to a target power plant; and Phase III is to apply the VPN to all the power plants.

The composition of phase I consisted of the SDIS Server, IAEA Server and TCNC Server. In each system, VPN system hardware was installed, and the penetration of the three systems and the three VPNs was tested. The domestic test involved two hacking scenarios: hacking from the outside and hacking from the inside. The international test involved one scenario from the outside.

The hacking from the outside involved a hacker' s computer connected to an external network that scanned the VPN + firewall. The hacker tried to attack by using a forged IPSec/IKE packet, and communicated with the target system using the forged IPSec communication. Through this process, the hacker made a judgment on the acquiring possibility of the actual data and of the encryption key, using IPSec packet sniffing. However, the hacking attempt failed, due to the security policy of VPN.

The hacking test from the inside involved a hacker' s computer directly connected to the trusted network. The hacker tried to attack using a forged IPSec/IKE packet and packet sniffing at the VPN + firewall gateway and the remote server/VPN + firewall. These attacks also failed. However, during an internal DoS attack and ping flooding, the test showed that the CPU load increased more than 60 % and that the VPN' s performance obviously diminished. Therefore, it will be necessary to compensate for the VPN' s weak points.

If we replace the existing RMS with the VPN (Internet), it will reduce the cost by 1/5 and the communication speed will be increased.

Acknowledgement

This work has been carried out under the Nuclear Research and Development program supported by MOST.

Reference

1. Jim S. Regula, "Communications Technologies Appropriate for Remote Monitoring", IAEA, (2001).
2. W.K.Yoon, et al., "Remote Monitoring for Enhanced Cooperation",' 01 ESARDA, (2001).
3. H. Smart, S. Caskey, R. Martinez, "Secure Transfer of Surveillance Data Over Internet Using Virtual Private Network Technology", STUK-YTO-TR174, (2001).
4. H. Smart, et.al, "Application of a Virtual Private Network to the Finnish Remote Environmental Monitoring System", 41st INMM, New Ore. (2000). .
5. J.S.Kim, et.al, " The current status of developing the VPN technologies and application for Remote Monitoring" , KAERI/GP-189/2002, VPN workshop for Remote Monitoring, Daejeon, (2002).
6. Susan Caskey and Don Glidewell, Virtual Private Networks, KAERI/GP-189/2002,VPN workshop for Remote Monitoring, Daejeon. (2002).