Design and Implementation of the Ipsec-based Security System

Ji-Hoon JEONG, Geon-Woo KIM, So-Hee PARK and Sung-Won SOHN
Internet Security Research Team,
Electronics & Telecommunications Research Institute (ETRI),
161 Kajong-Dong, Yusong-Gu, Taejon, 305-350,
KOREA

Abstract: - Ipsec is a standard protocol to offer Internet information security service. Recently Ipsec is implemented through out the world on the base of various operating systems. Through the inter-operability test among multiple independent implemented devices, it is now the mandatory function of Internet equipment. Ipsec adds two headers (i.e.,AH & ESP) and protocol to the legacy IP packet so therefore, Ipsec offers not only internet security service such as internet secure communication, and authentication service but also the safe key exchange and anti-replay attack mechanism. In this paper, we propose the design and implementation of C-ISCAP, which is Ipsec based Internet information security system and also we will show the data of performance measurement.

Key-Words: - Ipsec, AH, ESP, Security Association, Security Policy, Security Management & Evaluation

1 Introduction

The traditional approaching methodology of offering information security service in the network is finding the independent solution which do not influence the application program on the upper layer of the protocol stack. To add to this, from the view of the network protocol designers, it is most effective to offer the security service from the network layer. You can see the initial attempt in the projects such as SDNS(secure Data Network system) of the NIST[1], and network layer security protocol of the ISO[2].

In November 1992, the members of the IETF started to design the IP layer security protocol, which is suitable for the large scaled Internet environment. As a result of this, swIPe[3] was born and the design concept of the first stage was proven that the security service from the IP layer is possible. A few years later from the development of swIPe, the specification of the IP layer security start to be written by the IETF Ipsec WG. During the 34th IETF Meeting in Dallas(December 1995), the inter-operability test of Ipsec system was performed for the first time. The system, which is wholly based on the Ipsec documents, implemented by the Internet device manufacturers and researchers independently. The Ipv6 WG adopted Ipsec, and now it is mandatory requirement of the next generation Internet. After this, Ipsec security architecture, transform algorithms, AH(Authentication Header), ESP(Encapsulating Security Payload) were confirmed as a RFC. Up to date, new RFCs and Internet drafts related to Ipsec are made. [4, 5, 6, 7, 8, 9]

The characteristics of the Ipsec summarized as below. First, Ipsec provides a transparent information security services to the Internet users owing that it is offered by the IP layer and is needless to modify the application programs of the upper layer. Second, the consistent security service is possible in the system owing that Ipsec provides the same information security service to the application layer and the transport layer. Third, Ipsec has an open architecture therefore, it does not depend on the specific algorithm or authentication mechanism and it easily can adopt the existing technology or a new technology.

Ipsec is used broadly though all systems especially in VPN(Virtual Private Network) equipment. Ipsec is understand to be the only Internet security protocol to solve scalability and compatibility in VPN when adapt to the large scaled network. In this paper, we propose the design and implementation of C-ISCAP, which is Ipsec based Internet information security system and also we will show the data of performance measurement.

2 Our Implementation of C-ISCAP

2.1 C-ISCAP Architecture

C-ISCAP is composed of secure host/gateway system containing Ipsec engine and IKE, security management system, security policy system, and security evaluation system. Figure 1 shows the C-ISCAP architecture.

2.2 Ipsec Engine

Ipsec engine divides into two different functions as secure host and gateway. The two functions are similar in some ways but have much differentiation in the system role and position. Secure host function is ported generally on the user terminal with single network

interface, however secure gateway function is ported on the system with multiple network interfaces such as router, firewalls, and VPN server.

Secure host/gateway establishes secure connection between hosts, gateways, and host and gateway by observing policy of SPD. Also Ipsec engine must observe SAD including SA, which is made by IKE negotiation.

After the creation of SA and SP, user packet process is as below. In outbound packet process, Ipsec engine decides whether to Ipsec application, packet bypass, packet discard using the information of SPD selector(Source and Destination IP Address, Source and Destination Port). In case of applying Ipsec policy, Ipsec engine searches SAD entry by SA selector(destination IP address, Ipsec protocol, and SPI(Security Parameter Index) of packet header) and process the Ipsec by SA. Inbound packet process is performed in reversed order of the outbound.

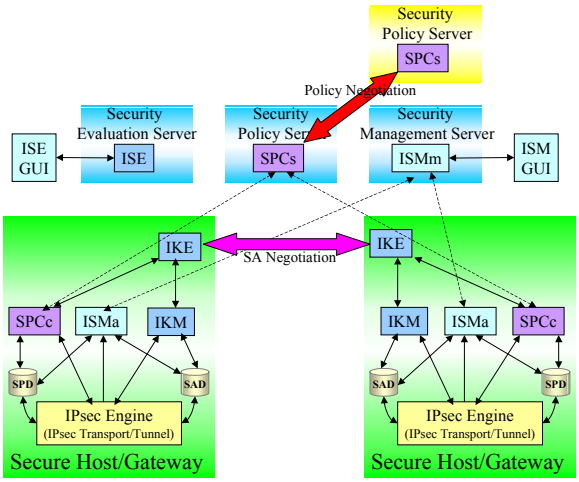


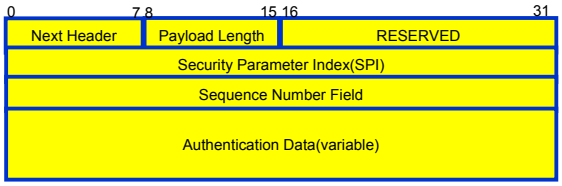
Fig.1 C-ISCAP Architecture

2.2.1 AH/ESP Header

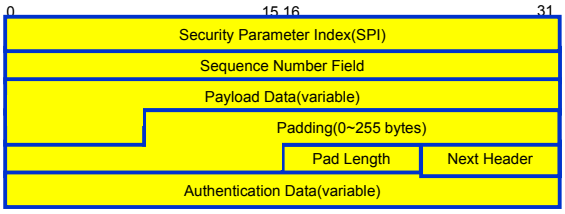
Ipsec Engine handles AH and ESP header defined by the IETF Ipsec WG. AH offers Integrity of IP packet and authentication of packet origin. ESP header is used to encrypt the upper layer information of packet payload. Figure 2 shows the AH and ESP header formats.

AH is formed of SPI(Security Parameter Index), SN(Sequence Number) and ICV(Integrity Check Value). ICV is the MAC(Message Authentication Code) value, which is calculated by the unidirectional hash function such as MD-5 or SHA-1. Only the user who knows the key of hash function can find out the hash value and check the forgery that can occur during the procedure. SN is used to check whether if one packet is received twice for the sake of anti-replay attack. SPI is used as parameter to indicate specific Ipsec process such as destination address, SN, AND ICV. All of these information are stored in SAD(Security Association Database). AH is an extension header and when AH is used as a tunnel mode, outer header is attached in front of AH so as to hide both of the original header and payload information of IP packet. When AH is used as a transport mode, AH is placed in between the original IP packet header and payload so as to hide only the original header of IP packet.

ESP locates data to encrypt in the payload field. SPI and SN is used in the same way as the AH. In transport mode, the data part of the payload is the upper layer data. But in tunnel mode, it is the original IP packet and payload. The symmetric key block cipher is used for an encryption and the plane text is padded to fill the block. The mandatory algorithm is DES-CBC(RFC 1892) and Null Encryption(RFC 2410). ICV is the MAC value, which is calculated from the values of ESP header, payload, and ESP trailer.



(a) AH Header Format



(b) ESP Header Format

Fig.2 AH and ESP Header Format

2.2.2 SAD

- **Destination IP Address**
- **Security Parameter Index(SPI)**
- **IPsec Protocol**

- Name : user ID & system name
- Data Sensitivity Level
- Source IP Address
- Transport Layer Protocol
- Source and Destination Ports
- Sequence number counter
- Sequence counter overflow
- Anti-replay window
- AH authentication algorithm & key
- ESP encryption algorithm & key
- ESP authentication algorithm & key
- Lifetime of SA
- IPsec protocol mode
- Path MTU

… … …

Before the Ipsec processing such as data encryption and ICV calculation, SA must be negotiated between the two systems. SA factors are hash function, encryption algorithm, keys and lifetime of keys. Those are fixed by the communicating system when the SA negotiation is performed. For the full duplex connection two SAs are necessary, which are inbound and outbound SA because SA has only one-way packet forwarding information. These SAs are stored in SAD and SAD has the fields

described above.

SAD is selected from destination IP address, SPI, and Ipsec Protocol. And Ipsec engine references the SAD during the AH or ESP process and that enables security service to the specific connection. SA can assign transport layer protocol or port of upper layer so it makes it possible to control the granularity of SA.

2.2.3 SPD

The security manager can set up encryption algorithm, key size and tunnel in single domain. Also those can be set up by negotiation between SPSs. Ipsec engine must reference SPD on the procedure of outbound packet process as well as inbound. In outbound process, Ipsec engine decides whether to apply Ipsec or how to apply it from SPD. In inbound process, Ipsec engine verifies if the security service is correctly adopted from SPD. SPD has the following fields.

- Source IP Address
- Destination IP Address
- Source Port Number
- Destination Port Number

- IPsec Header Type(AH/ESP)
- IPsec Mode(tunnel/transport)
- Security Paramter Index(SPI)
- IPsec Action
-
- **Authentication Algorithm**
- **Encryption Algorithm**
- **Key Length of Algorithm**
- **The Number of Rounds in Encryption**
- **Lifetime of Keys**
- **Exchange Mode of IKE**
- **Diffie-Hellman Group**
- **Tunneling Points**

  … … …

SPD divides into two parts, which are parameters for Ipsec process by Ipsec engine, and parameters for SA negotiation by IKE. SPD entry is identified by source/destination IP address and port number. The parameters of SPD are mostly for SA negotiation of IKE than the Ipsec engine. The SPD parameters for SA negotiation of IKE are authentication algorithm, encryption algorithm, key length of algorithm, the number of rounds in encryption algorithm, lifetime of keys, exchange mode of IKE(main, aggressive, quick, new-group), Diffie-Hellman group and tunneling points. The SPD parameters for Ipsec processing of Ipsec engine are Ipsec header type(AH, ESP), Ipsec mode(tunnel/transport), Ipsec action(bypass, drop, applying Ipsec) and SPI.

2.3 IKE

IKE offers automated key negotiation, and it is a mixed type of protocols ISAKMP, Oakley and SKEME. ISAKMP protocol provides two phases of processing and the functions are the authentication and key exchange. Oakley provides definition of key exchange mode and SKEME provides key sharing and re-keying mechanism. IKE is designed to defense DoS(denial of Service) and Man-in-the-middle attack, and also satisfy the PFS[10].

SPS invokes IKE and SA negotiation creates key, which is stored in SADB. To accomplish this, IKE processing divides into two phases. In phase 1, ISAKMP SA negotiation and key material creation is performed for protection of ISAKMP messages. In phase 2, Ipsec negotiation and key creation is performed for security service of IP packet. IKE has 4 exchange modes, which are main, aggressive, quick, and new group. The ISAKMP SA created from phase 1, and Ipsec SA created from phase 2 are stored in ISAKMP SADB and Ipsec SADB, respectively.

The negotiated SA and keys are managed by the key management system. The key management system stores and deletes SA. Also, when the lifetime of SA is expired, the key management system requests IKE to renegotiate SA. Another function of the key management system is to store and manage the certificate from CA and to provide API of crytpo-library. Figure 3 shows the interaction between CA and IKE, SA negotiation between IKEs, management of SA, and crypto-library.

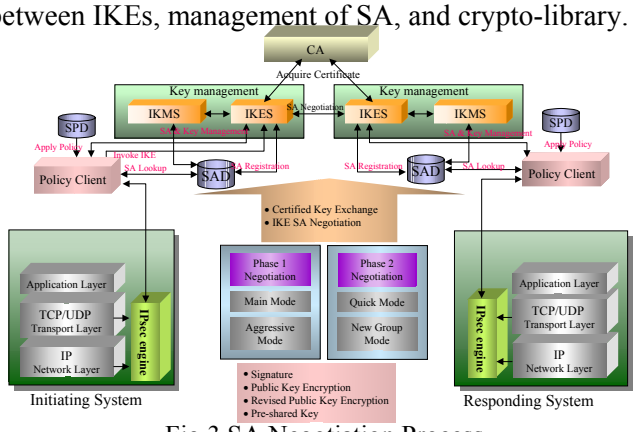


Fig.3 SA Negotiation Process

2.4 SPS

Security policy system decides hash or encrypt algorithm, the size of the key, a term of validity, and connection type of the domains or the systems and also manages them.[11,12] The security policy is set up manually by the security manager or set up automatically by the policy negotiation between SPSs,

SPS is composed of PS(Policy Server), PC(Policy Client), Master Files, SPS Databases, and SPP(Security policy protocol) handler. Master File has local policy and information about secure domain. SPS Database has local and remote policies. When PC or another PS requests for a policy information PS provides it to them.

When secure host/gateway establishes secure connection between systems, Ipsec engine requests the policy to PC. Then, PC searches local SPD if there is an appropriate policy, and if so, it response to Ipsec engine. Otherwise, PC requests PS for the policy. Then, PS searches SPS Database if there is an appropriate policy, and if so, PS response to Ipsec engine through PC.

Otherwise, PS and peer PS negotiate security policy by using SPP[13] to make a new policy between them. Figure 4 shows the security policy negotiation process between the PS of two different domains.

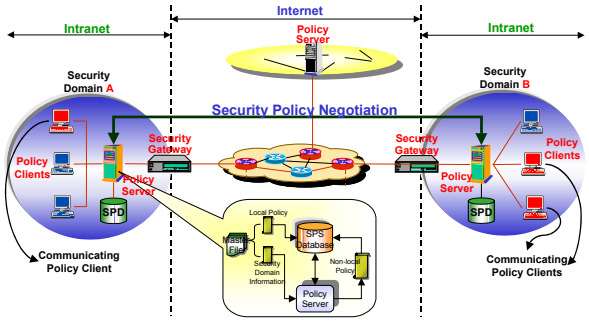


Fig.4 Policy Negotiation Process

2.5 SMS and SES

Security Management System(SMS) offers control mechanism to security manager. The functions of the security management system are observation of security service status, collection of audit information. To manage as above, the definition of MIB(Management Information Base) is necessary. MIB is not standardized yet and IETF is working on it. MIB at present are Ipsec monitoring MIB[14], IKE monitoring MIB[15], ISAKMP DOI-Independent MIB[16], and Ipsec DOI textural conventions MIB[17]. Figure 5 shows SMS security management mechanism.

Security Evaluation System(SES) estimates the system safety and finds the threat factor before the threat occurs. The function of SES is collecting network information using sniffer, searching evaluation rule database(ERD) to evaluate specific system, analyzing the result, and reporting the result to the security manager. ERD has evaluation method and attack technique of how to evaluate and attack the security of the system.

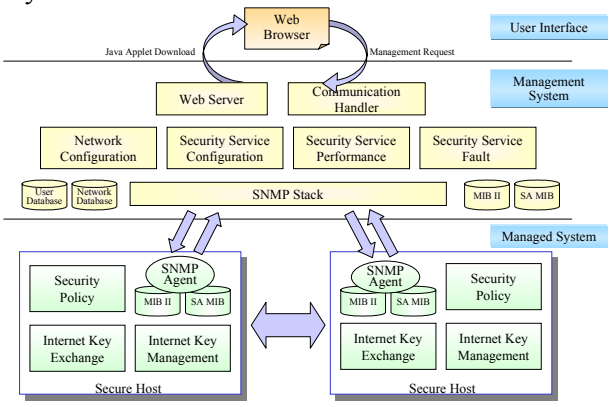


Fig.5 Security Management Mechanism

3 Ipsec Performance Measurement

Ipsec Performance parameters of interest include latency and throughput. We measured latency using **ping**. The measurement configuration consists of two machines running our C-ISCAP software. Two machines were 800MHz Pentium equipped with 100Mbps Ethernet card. We did the test for different packet size(512, 1024, 2048 and 4096 bytes of payload) and different Ipsec transforms, ping between each other. The results can be seen in Figure 6. The graph shows that the cost of authenticating packets does not downgrade response time, but that encryption(especially triple-DES) is major bottleneck. The second test, we transferred 20MB of Image data from Pentium PC to SUN Enterprise 450 with 100Mbps Ethernet card. We used **ttcp** to measure throughput, with TCP as the transport protocol. Figure 7 shows the results.

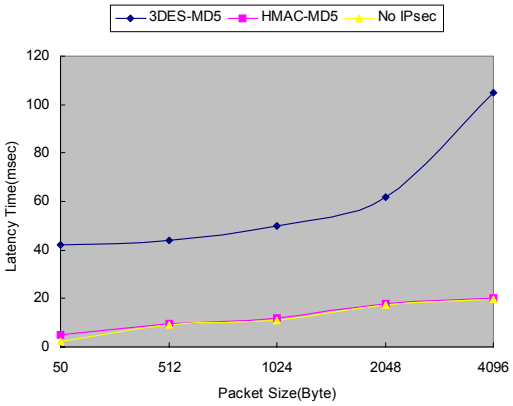


Fig.6 Ping Performance of IPsec

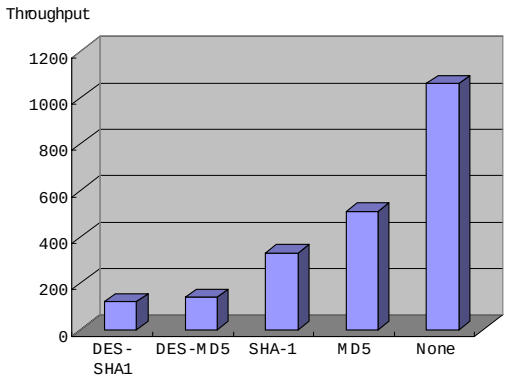


Fig.7 Throughput of TCP Transfer

4 Conclusion and Future Works

In this paper, we have mentioned about the architecture and implementation of C-ISCAP, Internet security system, based on Ipsec. Ipsec is considered as a successful Internet standard protocol with IKE. We can see it from the fact that in spite of VPN equipment manufacturers have their own security protocol, such as L2TP and PPTP, they adopt Ipsec as a VPN security standard. However, to deploy Ipsec and IKE, the supply of PKI (Public key Infrastructure) must be advanced. Also for the performance enhancement of Ipsec engine of massive packet processing in large-scaled network, hardware-based encryption algorithm is necessary.

The future works must be focused on Ipsec and IKE adaptation in remote and Mobile IP environment, which are already discussed in IETF ipsra WG. Also the works of kink and secred WG must be performed in parallel with the IETF ipsra WG. The kink WG researches the simple key exchange method, which substitutes heavy IKE. The secred WG researches downloading credentials from server without carrying the user authentication information.

References:

[1] NISTIR 90-4250: Secure Data Network Systems(SDNS) Network, Transport and Message Security Protocol, National Institute of Standards and Technology, February 1990.

[2] ISO-IEC DIS 11577 - Information Technology - Telecommunications and Information Exchange Between Systems - Network Layer Security Protocol, ISO/IEC JTC1/SC6, November 1992.

[3] J. Ioannidis and M. Blaze, "The Architecture and Implementation of Network-Layer Security Under Unix", Forth USENIX Security Symposium Proceedings, October 1993.

[4] RFC2401: Security Architecture for the Internet Protocol, S. Kent and R. Atkinson, November 1998.

[5] RFC2402: IP Authentication Header, S. Kent and R. Atkinson, November 1998.

[6] RFC2404: The Used of HMAC-SHA-1 within ESP and AH, C. Madson and R. Glenn, November 1998.

[7] RFC2405: The ESP DES-CBC Cipher Algorithm with Explicit IV, C. Madson and N. Dorawamy, November 1998.

[8] RFC2406: IP Encapsulating Security Payload, S. Kent and R. Atkinson, November 1998.

[9] RFC2409: Internet Key Exchange, D. Harkins, D.Carrel, November 1998.

[10] M. Blaze, A. Keromytis, M. Richardson, L. Sanchez, "IPSP Requirements", Internet draft, July, 2000.

[11] M. Blaze, A. Keromytis, M. Richardson, L. Sanchez, "Ipsec Policy Architecture", Internet draft, July, 2000.

[12] L. Sanchez, M. Condell, "Security Policy Protocol", Internet draft, July, 2000.

[13] T. Jenkins, J. Shriver, "Ipsec Monitoring MIB", Internet draft, July, 2000.

[14] T. Jenkins, J. Shriver, "IKE Monitoring MIB", Internet draft, July, 2000.

[15] T. Jenkins, J. Shriver, "ISAKMP DOI-Independent Monitoring MIB", Internet draft, July, 2000.

[16] J. Shriver, "Ipsec DOI Textal Conventions MIB", Internet draft, June, 2000.