SCIS 2004 The 2004 Symposium on
Cryptography and Information Security
Sendai, Japan, Jan.27-30, 2004
The Institute of Electronics,
Information and Communication Engineers

An Integration of PKI and IC cards for IPSec

Chung-Huang Yang[1] Long-Jian Lin[2] Kouichi Sakurai[3]

Abstract— As the Internet grows in scale almost every year, security measures are expected to become all the more important on the Internet. IPSec was introduced in 1995 to provide the capability for secure communication across IPv4 and IPv6 networks. Meanwhile, with substantial cost reductions and the ability to handle multiple applications on a single card, the IC cards are about to enter a period of rapid growth. An individual bearing a single IC card will be able to electronically and securely interact with several servers or service providers. In this research, we implemented IPSec with IC card acted as an integrated part within the system and is used as a portable token to manage cryptographic keys and certificates needed on the IPSec protocols. The open source software provided by the FreeS/WAN project is implemented and revised to be integrated with IC card USB reader on the Linux environment.

Keyword: IPSec, implementation, IKE, VPN, IC card, IPv6

1 Introduction

The security architecture for the Internet protocol, IPSec [1,2,3,4,5], gives the blueprint for doing security services on the Internet at the IP layer. IPSec is an option for the current version 4 of IP layer while is mandatory for the next generation Internet protocol, IPv6 [6,7,8]. IPSec consists of two types of extension headers a protocol to negotiate security setting. The AH (authentication header) [9] header and trailer provide data integrity and an optional replay protection for the ESP-encapsulated payload. The ESP (encapsulating security payload) [10] provides data confidentiality, authentication, and replay protection for the entire IP packet. The IKE (Internet key exchange) [11] protocol is used to negotiate IPSec security parameters for unicast communication.

Public-key infrastructures (PKI) [12,13,14,15] are comprised of supporting services that are needed for using public-key technologies on a large scale. A public-key certification system works by having a certification authority (CA) for the generation and management (application, storage, renewal, revocation, and inquiry) public-key certificates. Both CA and PKI are crucial parts of many secure network applications such as VPN, secure email, online stock trading, time-stamping, etc. PKI could have multiple CAs; each CA services a set of users and issues certificates for those users. Depending largely on how the trust relationship between CAs is arranged, the PKI provides traversing multiple CAs from the CA that's certifying other party's public-key to a root CA whose public-key has already been held in each PKI client, such as a system with IPSec. Each public-key certificate contains a public-key value and information about a particular person, agency, and other entity that holds the corresponding private-key. Certificates are digitally signed by the issuing CA, using CA's private-key.

IC cards [16,17] are much more difficult to duplicate than magnetic strip cards and cryptographic functions can be implemented inside these cards. With substantial cost reductions and the ability to handle multiple applications on a single card, the IC cards are about to enter a period of the rapid growth. An individual bearing a single IC card will be able to electronically and securely interact with several servers or service provides.

As a consequence, an entirely new type of commercial and educational landscape is being created. However, IC card itself has limited computing power and memory capacity. This makes it a difficult job to efficiently implement the cryptographic functions inside IC card.

In the following, we described our efforts in integrating IPSec with PKI and IC card, where IC card is used as a portable token to manage cryptographic keys and certificates needed on the IPSec protocols. The open source software provided by the FreeS/WAN project [18,19] is implemented on the Linux environment and

[1] Institute of Information and Computer Education, National Kaohsiung Normal University, 116, Ho Ping First Road, Kaohsiung 802, TAIWAN, http://crypto.nknu.edu.tw/, chyang@computer.org

[2] cello@icemail.nknu.edu.tw

[3] Theoretical Computer Science Group, Dept. of Computer Science and Communication Engineering, Kyushu University, Hakozaki, Fukuoka 812-81, JAPAN, http:// itslab.csce.kyushuu.ac.jp/, sakurai@csce.kyushu-u.ac.jp

integrated with IC cards. In FreeS/WAN, IKE authentication methods of pre-shard keys and RSA-signature are supported, but the cryptographic key and public-key certificates are stored in a file specified by the configuration file "ipsec.conf". To provide a better protection for the cryptographic keys, we choose to use IC card to secure store these keys and use the same IC card to carry public-key certificates issued by CA.

2 Implementation of IPSec with Free/SWAN

FreeS/WAN [18,19] is an open-source implementation of IPSec for Linux platforms. We installed and set up FreeS/SWAN software on two Red-Hat Linux machines so that they will act as security gateways and create a secure tunnel to protect all data communicated between them, as shown in Figure 1.

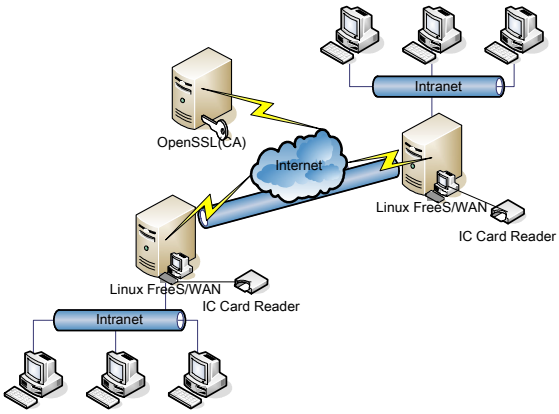

Figure 1: Security Architecture of PKI-based Security Gateways

We could issue an "ipsec look" command on the Linux machine with FreeS/WAN installed. Figure 2 shows the operations of a virtual tunnel between two security gateways. The default cryptographic algorithms used for tunnel security are the triple-DES and HMACMD5.

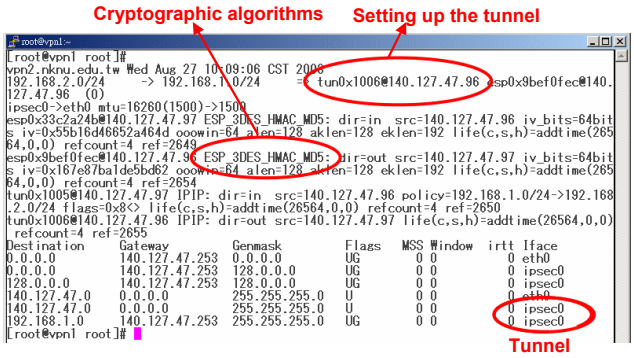

Figure 2: Operations of a FreeS/WAN VPN Tunnel

IPSec achieves security services with AH and ESP protocols, and through the use of IKE protocol. IKE [11,20,21] is used to negotiate and provide cryptographic key materials for IPSec peers, from which encryption and authentication keys are generated. It is operated in two ISAKMP [22] phases where two ISAKMP peers establish an ISAKMP security associations (SAs) during Phase 1 and then SA for other security services, such as AH or ESP, are established during Phase 2. For FreeS/WAN, a *Pluto* module is run as an IKE daemon on a network node. Pluto uses shared secrets or RSA signatures to authenticate peers with whom it is negotiating. This Pluto module is the software module, which we revised to incorporate IC card and PKI.

3 IPSec Integration with PKI and IC Cards

PKI is essential for large-scale secure network applications, such as IPSec. To safeguard pre-shared key and certificate of security gateway, our security gateway is equipped with an IC card with Omnikey's CardMan USB reader [23].

CA fundamentally performs the generation and management public-key certificates that are digitally signed by the CA's private key. We installed OpenSSL [24,25] open-source software on a Red-Hat Linux machine to act as a CA, which issues public-key certificates for IPSec peers.

```
[root@vpn1 root]# openssl x509 -req -days 3650 -sha1 \
>  -extfile /etc/ssl/openssl.cnf -extensions v3_req \
>  -CA /etc/ssl/certs/nknuca.crt.pem \
>  -CAkey /etc/ssl/private/nknuca.key.pem \
>  -CAserial /etc/ssl/nknuca.srl -CAcreateserial \
>  -in /tmp/leftsite.req.pem -out /etc/ssl/certs/leftsite.crt.pem
```

Figure 3: Setting Up OpenSSL as a CA

Then, we revised FreeS/WAN codes to let both security gateways communicated with each other using X.509 certificated issued by the CA.

```
ipsec_setup: Starting FreeS/WAN IPsec 2.02...
ipsec_setup: Using /lib/modules/2.4.20-8/kernel/net/ipsec/ipsec.o
[root@vpn1 log]# ipsec auto --verbose --up net-to-net
002 "net-to-net" #1: initiating Main Mode
104 "net-to-net" #1: STATE_MAIN_I1: initiate
106 "net-to-net" #1: STATE_MAIN_I2: sent MI2, expecting MR2
108 "net-to-net" #1: STATE_MAIN_I3: sent MI3, expecting MR3
002 "net-to-net" #1: Peer ID is ID_DER_ASN1_DN: 'C=TW, ST=Taiwan, L=kaoshiung,
 OU=ice, CN=vpn2, E=cello@icema.nknu.edu.tw'
002 "net-to-net" #1: ISAKMP SA established
004 "net-to-net" #1: STATE_MAIN_I4: ISAKMP SA established
002 "net-to-net" #2: initiating Quick Mode RSASIG+ENCRYPT+TUNNEL+PFS+UP
112 "net-to-net" #2: STATE_QUICK_I1: initiate
002 "net-to-net" #2: sent QI2, IPsec SA established
004 "net-to-net" #2: STATE_QUICK_I2: sent QI2, IPsec SA established
[root@vpn1 log]#
```

Figure 4: Operations of a Tunnel with X.509 Certificates

At present, we use IC card with the Infineon SLE 4418 [26] memory chip. This chip contains 1024 bytes of EEPROM memory and its contents are protected by 4 hexadecimal digits, the programmable security code (PSC).

4 Conclusions

The IP protocol is inherently insecure. IPSec can be used to protect any protocol that run on top of IP layer. IPSec runs over the current IP version (IPv4) and also the next generation of IP (IPv6). PKI is essential for large-scale network applications, including IPSec. In this research, we show our preliminary implementation

efforts in integrating PKI and IC cards with IPSec on Linux environment. We are currently in the process of applying our results on IPv6 environment.

Acknowledgement

Taiwan NICI IPv6 Steering Committee, R&D Division, supports the research. Under contract number R-0300.

References:

[1] IETF IP Security Protocol Working Group, http://www.ietf.org/html.charters/ipseccharter.html

[2] K. Tsukamot, et al., "An Experimental Study on IPSec," *IEICE Trans. Fundamentals*, Vol. E85-A,No. 1, Jan. 2002, pp. 175-180.

[3] C. Davis, *IPSec: Securing VPNs*, McGraw-Hill, 2001.

[4] N. Doraswamy and D. Harkins, *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*, 2nd edition, Prentice Hall PTR, 2003.

[5] E. Kaufman and A. Newman, *Implementing IPSec*, Wiley, 1999.

[6] IPv6 Promotion Council, http://www.v6pc.jp/

[7] S. Hagen, *IPv6 Essentials*, O'Reilly, 2002.

[8] IPv6 Forum, http://www.ipv6forum.org

[9] S. Kent and R. Atkinson, "IP Authentication Header," IETF RFC 2402, 1998.

[10] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," IETF RFC 2406, 1998.

[11] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," IETF RFC 2409, 1998.

[12] R. Hunt, "Technological infrastructure for PKI and digital certification," *Computer communications*, Vol. 24, No. 14, September 2001, pp.1460-1471.

[13] C. Adams and S. Lloyd, *Understanding Public Key Infrastructure*, Macmillan Technical Publishing,1999.

[14] A. Nash, W. Duan, C. Joseph, and D. Brink, *PKI: Implementing and Managing E-Security*, McGraw-Hill, 2001.

[15] A. Skarmeta, et al. "PKI Services for IPv6," *IEEE Internet Computing*, Vol. 7 No. 3, June 2003, pp.36-42.

[16] ISO 7816 Part 1 to 10: Identification Cards - Integrated Circuit(s) Cards with Contacts, 1987 to 2000.

[17] W. Rankl and W. Effing, *Smart Card Handbook*, 2nd edition, John Wiley & Sons, 2000.

[18] FreeS/WAN official Home Page, http://www.freeswan.org

[19] Unofficial FreeS/WAN support, http://www.freeswan.ca

[20] M. Borella, "Methods and Protocols for Secure Key Negotiation Using IKE," *IEEE Network*, Vol.14, No. 2, Jul/Aug. 2000, pp.18-29.

[21] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol," IETF Internet-Draft, Oct. 2003.

[22] D. Maughan et al., "Internet Security Association and Key Management Protocol (ISAKMP)," IETF RFC 2408, 1998.

[23] Omnikey CardMan Desktop USB2020, Omnikey AG, http://www.omnikey.com/en/produkt_details.php3?produkt=1&variante=3

[24] OpenSSL Project, http://www.openssl.org

[25] J. Viega, M. Messier, and P. Chandra, *Network Security with OpenSSL*, O'Reilly, 2002.

[26] Infineon Technologies AG, SLE 4428 Chip, http://www.infineon.com/cgi/ecrm.dll/ecrm/scripts/prod_ov.jsp?oid=15066&cat_oid=-9520