

E-mail encryption methods and lawful interception methods of it

Young Sic Jeong^{*}, Shin Gak Kang^{**}

^{*} SRC(Standard Research Center), ETRI(Electronics and Telecommunications Research Institute), Korea

^{**} ETRI(Electronics and Telecommunications Research Institute), Korea

jys@etri.re.kr, sgkang@etri.re.kr

Abstract—This paper presents e-mail encryption methods and lawful interception method of it. We deal with OpenPGP, S/MIME, SSL and TLS methods for e-mail encryption. Gmail encryption scheme is analyzed briefly. We also present lawful interception schemes for e-mail encryption methods. We want to explain e-mail encryption general terms.

Keywords— e-mail, encryption, lawful interception

I. INTRODUCTION

This paper presents e-mail encryption methods and lawful interception method of it. We deal with openPGP(Open Pretty Good Privacy), S/MIME(Secure Multipurpose Internet Mail), SSL(Secure Socket Layer) and TLS(Transport Layer Security) methods for e-mail encryption. Gmail encryption scheme is analysed briefly. We also present lawful interception schemes for e-mail encryption methods. We want to explain e-mail encryption general terms.

We want to explain various e-mail encryption methods. We also show g-mail encryption scheme. Finally, we introduce lawful interception scheme of e-mail according to the e-mail encryption methods.

A test was done by professor in Korea. That test is kinds of hacking on e-mail system such as daum, nate, paran, yahoo and google. The purpose of that test is identify how strong web-mail about hacking. The result is shocking one. Every e-mail data was hacked by a program which is downed from internet. By hacking, we easily can see the content of e-mail except g-mail. Because that g-mail is encrypted, we cannot see the contents of g-mail although we hacked g-mail data. Related this test, main portals such as daum, naver and nate announced e-mail encryption plan. Yahoo announced e-mail encryption plan by using SSL in second quarter of 2012.

Therefore, the government have to know how encrypt e-mail and how law enforcing agency can make lawful interception on encrypted e-mail.

We analysis various e-mail encryption scheme and present several schemes for lawful interception in this paper.

II. E-MAIL ENCRYPTION SCHEMES

Various methods exist for encryption of e-mail. We present encryption schemes for e-mail and deal with related problems. OpenPGP, S/MIME, SSL, TLS and IBS will be analysed in this chapter.

A. OpenPGP(Open Pretty Good Privacy)

OpenPGP is a standard what encrypts e-mail by using public key. It encrypts e-mail body and attached files. E-mail encryption scheme is same as following Figure 1.

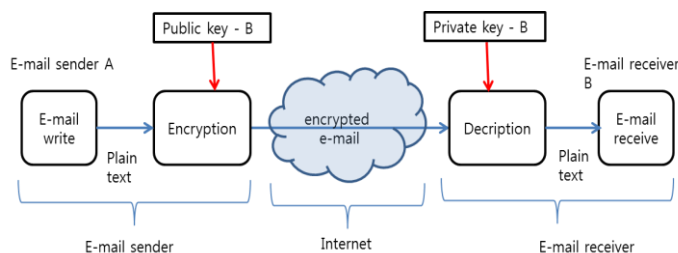


Figure 1. E-mail Encryption system by using OpenPGP

The e-mail sender A write a e-mail and encrypt it by using public key of e-mail receiver B and send that e-mail through the internet to e-mail receiver B. The e-mail receiver decrypts the received e-mail by using private key of B firstly and read decrypted e-mail that has plain text form. Although everyone easily know public key of B but no one decipher encrypted e-mail without private key of B. OpenPGP uses public key infrastructure to encrypt and decrypt of e-mail.

In this system, Lawful interception of e-mail by capturing the e-mail packet in the internet is extremely difficult because encrypted e-mail flows through the internet. Encrypted e-mail only can be read after decryption by using private key of receiver. This e-mail encryption scheme is standardized as IETF rfc 4880. This scheme is not related e-mail server. E-mail encryption of OpenPGP can be done between sender and receiver regardless of e-mail server.

Eavesdropping of e-mail encrypted by OpenPGP is extremely difficult but it has some defect. That is possibility of spreading of malware when using OpenPGP.

In case that sender sends e-mail which is contained malware in body or attached file of mail(Figure 2.), If that e-mail is not encrypted, vaccine program of receiver can protect the malware, because the pattern of malware is exposed to the vaccine program.

In case that sender sends e-mail which is contained malware in body or attached file of mail(Figure 3.), If that e-mail is encrypted, vaccine program of receiver cannot protect the malware, because that the pattern of malware is encrypted also, so it is not exposed to the vaccine program.

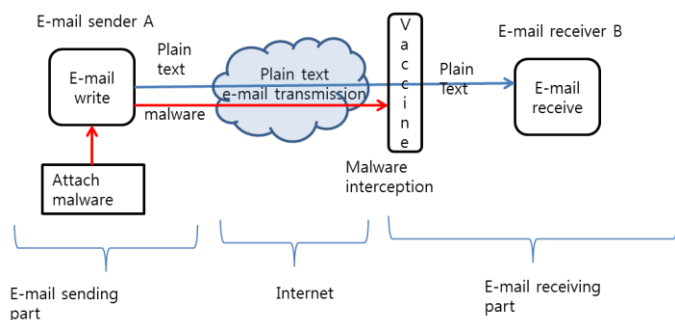


Figure 2. Protection of malware in case of no encryption

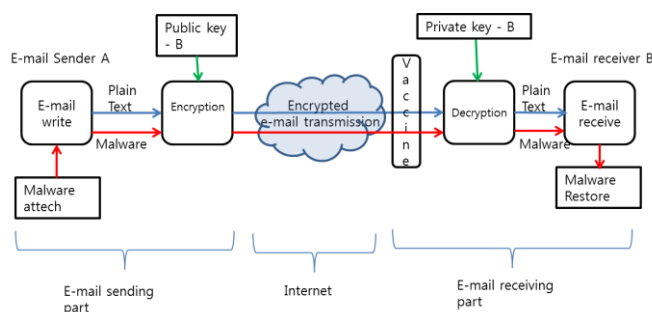


Figure 3. Malware spreading in case of encryption

B. S/MIME(Secure Multipurpose internet Mail)

S/MIME is a standard based on encryption of MIME by public key. S/MIME provide cryptographic secure service such as authentication of electronic message, integrity of message, non-repudiation of sender, privacy and security of data. S/MIME was standardized as IETF rfc 3369, 3370, 3850 and 3851. It is not widely used because it is not appropriate to client of web mail. S/MIME has been implemented at Outlook express of Macrosoft. We can use S/MIME only in case that e-mail server supports it.

Figure 4. Concept of QoR

C. SSL(Secure Socket layer)

SSL located at between TCP/IP and application layer as encryption program based on public key. SSL provide cryptographic security, interoperability and extendibility. SSL provide cross authentication, electronic signature for integrity and encryption for confidentiality so that it provide secure communication between client and server. SSL protect e-mail by making to flow of e-mail which includes its body and attachment file through session encrypted by SSL. Because that SSL encrypt communication between mail server and client, we can use it only in case that mail server and client support SSL. SSL has no possibility of spreading of malware because it encrypts session itself. It has two disadvantages. First one is SSL increase loading of server and client because encryption should be processed by server and client. Second one is server should manage public keys.

Processing procedure is same as following when we send e-mail by SSL encryption. :

- SSL encryption block of sender A encrypt it by using public key of server after generate an arbitrary random number to make security session between server and client.
- E-mail server extracts random number which is sent by sender A by decrypts the data which is sent by sender A by using private key of server and use it as session key of SSL security session.
- A SSL security session is established between e-mail client and server by using encryption which utilize session key.
- a e-mail sent by sender A goes to the e-mail server through SSL security session and decrypted e-mail which was undergone SSL decryption process is saved to e-mail server.
- E-mail receiver get the e-mail by using SSL session between server and client and can read it after SSL decryption.

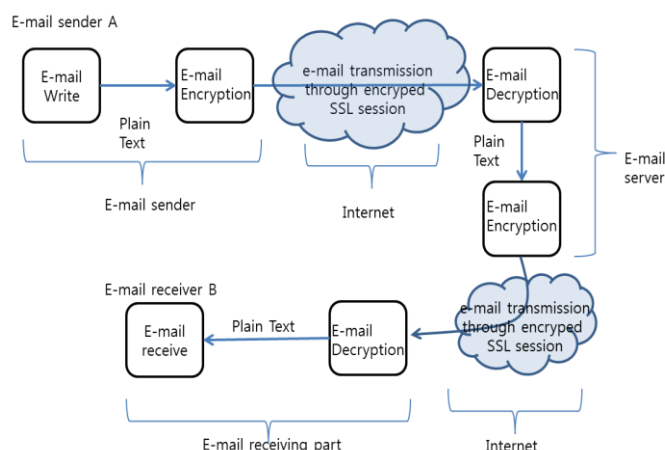


Figure 5. E-mail encryption by using SSL

D. TLS(Transport Layer Security)

TLS provide security service by encapsulation HTTP, FTP and SMTP. Because TLS encrypts communication between server and client, e-mail server and client should support TLS. Its latest version is 1.2 and standardized IETF rfc 5246. TLS used to encrypt SMTP(Simple Mail Transfer Protocol). TLS is a standard method to encrypts SIP(Session Initiation protocol) signalling.

E. IBE(Identity Based Encryption)

IBE generate public key based on specific text such as e-mail or subscribe ID. IBE has advantage to identification of sender because it generate public key based on text.

III. GMAIL ENCRYPTION

In this chapter, we present gmail encryption system. Gmail uses encryption scheme based on SSL.

Processing procedure is same as following when we send gmail by SSL encryption. :

- SSL encryption block of sender A encrypt it by using public key of server after generate an arbitrary random number to make security session between server and client.
- Gmail server extracts random number which is sent by sender A by decrypts the data which is sent by sender A by using private key of server and use it as key of SSL security session.
- A SSL security session is established between gmail client and server by using encryption which utilize session key.
- a gmail sent by sender A goes to the gmail server through SSL security session and decrypted gmail which was undergone SSL decryption process is saved to gmail server.
- Gmail receiver get the gmail by using SSL session between server and client and can read it after SSL decryption.

By using two layers gmail authentication which use ID, password, mobile phone short message and voice call, gmail server certificate user of gmail.

Plain text mail saved to gmail server and when gmail user read the mail, SSL security session is established between client and gmail server. Gmail is transmitted through encrypted SSL secure session to user of gmail. Gmail user can read the content of gmail by SSL decryption. Therefore, content of gmail is protected when it is transmitted through internet but email in the server is not secure because plain text email is saved to server.

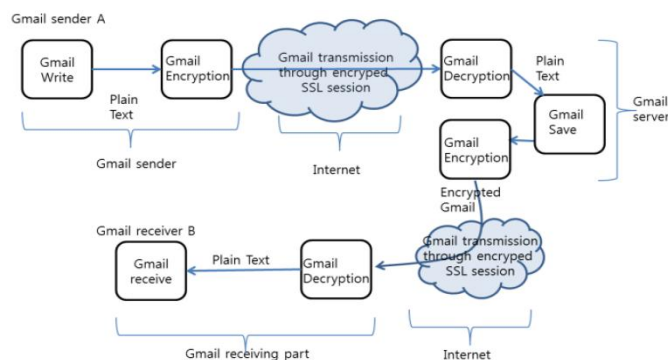


Figure 6. Gmail Encryption by using SSL

IV. ENCRYPTION OF EMAIL AND LAWFUL INTERCEPTION(LI)

A. LI of e-mail which is encrypted by OpenPGP, IBE or S/MIME

Encrypted e-mail is transmitted through internet and encrypted e-mail is saved to e-mail server because e-mail is encrypted before transmission between e-mail sender and receiver.

For lawful interception of e-mail which is encrypted by OpenPGP, IBE or S/MIME, it is needed private key of mail receiver. Without private key of e-mail receiver, decryption of e-mail is almost impossible.

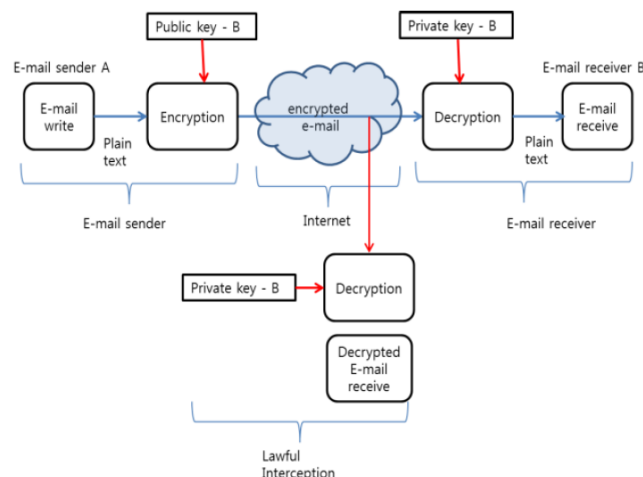


Figure 7. Additional service system for mobile IPTV

B. LI scheme in case that e-mail is transmitted through encrypted secure channel such as SSL or TLS

Encrypted e-mail is transmitted and decrypted plain text e-mail is saved to e-mail server because that e-mail is transmitted through encrypted secure session.

For lawful interception, it is needed to extract decrypted e-mail from e-mail server. Lawful interception of e-mail which is transmitting through secure channel is extremely difficult because secure channel is encrypted by SSL or TLS.

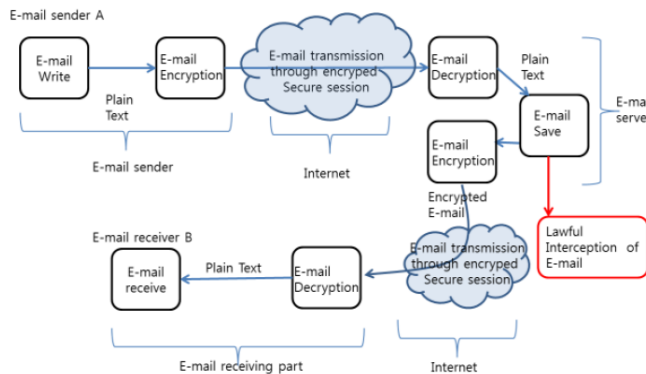


Figure 8. LI of e-mail encrypted by OpenPGP, IBE or S/MIME

ACKNOWLEDGEMENTS

This research was supported by the ICT Standardization program of MKE (The Ministry of Knowledge Economy) / KCC(Korea Communications Commission)

REFERENCES

- [1] IETF rfc 4880, "OpenPGP Message format", 5-6, 2007
- [2] IETF rfc 3369, "Cryptographic message syntax", 2002
- [3] IETF rfc 3850 "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling", 2004
- [4] ETSI TS 133.108 v8.6.1 "Handover interface for Lawful Interception(LI)", 2009.4 Recommendations (Draft), Q.769.1, "SS7
- [5] ANSI/J-STD-025-B, "Lawfully Authorized Electronic Surveillance", 2006.7
- [6] ITU-T Recommendations, Q.701 ~ Q.708, "MTP Specifications of SS7", 1993.
- [7] ITU-T Recommendations, Q.711 ~ Q.716, "SCCP Specifications of SS7", 1993.
- [8] ITU-T Recommendations, Q.761 ~ Q.764, "ISUP Specifications of SS7", 1993.
- [9] ITU-T Recommendations, Q.1200 series, "INAP Specifications of SS7", 1993.
- [10] ITU-T Recommendation, Q.699, "Interworking between ISDN Access and Non-ISDN Access over ISUP", 1997.
- [11] ITU-T Recommendation, Q.730, "ISDN User Part Supplementary Services", 1999.
- [12] ITU-T Recommendation, Q.850, "Use of cause and location in the digital subscriber Signaling System No.1 and Signaling System No.7 ISDN user part". 1998.
- [13] ITU-T Recommendation, Q.1600, "Interaction between ISUP and INAP".

- 1997.
- [14] ANSI T1, Baseline Working Documents for Switching and Signaling", T1S1.6/98-001, 1998.1.6.
- [15] TIA/EIA, IS-41D, "Cellular Radio telecommunications Intersystem Operations", 1997. 12.
- [16] TIA/EIA, IS-95A, "Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Systems", 1995,5
- [17] TIA/EIA, IS-95B, "Mobile Station-Base Station Compatibility Standard for Dual-Mode Spread Spectrum Systems", 1998, 12
- [18] TIA/EIA, IS-771, "Wireless Intelligent Network", 1999.7.
- [19] 3G TS 22.066: "Support of Mobile Number Portability (MNP); Service description. Stage 1".
- [20] 3GPP TS 23.060 Technical Specification Group Services and System Aspects, "GPRS (General Packet Radio Service) Service Description", Release 1999.
- [21] 3GPP TS 33.106 Technical Specification Group Services and System Aspects, "Lawful Interception Requirements", Release 1999.
- [22] 3GPP TS 33.107 Technical Specification Group Services and System Aspects, "Lawful Interception Architecture and Functions", Release 1999.
- [23] ETSI ETR 331 Security Techniques Advisory Group, "Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies", December 1996.
- [24] ETSI ES 201 158 Telecommunications security, "Lawful Interception (LI); Requirements for network functions", 1998.