파일 암호화와 키 생성을 이용한 통신보안 연구

이재현* · 박대우*

*호서대학교 벤처전문대학원 IT응용기술학과

A Study of Communications Security by Using Key Generation and File Encryption

*jae-hyun Lee · *Dea-Woo Park

*Dept. of IT Application Technology, Hoseo Graduate School of Venture

E-mail : *leejh9708@paran.com · *prof1@paran.com

요 약

파일 보안의 일반적 방법은 암호화를 이용한 보호이다. 인터넷과 같은 네트워크 환경의 발전에 따른 시스템들 간의 정보의 공유가 일반화 되고, 사용자에게 편리함을 제공하는 반면, 개개인 혹은 조직의 중요한 기밀 정보들에 대한 접근이 용이하여 해킹으로 발생한 시스템 침입이 빠르게 증가하는 추세이다. 본 논문은 최근 발생하고 있는 해킹으로 발생한 파일시스템 침입 즉 Sniffing에 대한 사용자의 파일 암호화와 키 생성을 이용한 Sniffing Tool 패킷분석을 통해 IP 및 데이터를 살펴본다.

본 연구를 통해 개인정보보호의 중요성을 각인시켜 해킹사고에 사전예방과 사용자들의 보안수준 의식을 높이는 것에 기여할 것이다.

ABSTRACT

File security is typically protected by encryption methods. The development of a network environment, such as the Internet according to the sharing of information between systems become commonplace, while providing convenience to users, individuals or organizations that facilitate access to sensitive information caused by hacking the system to attack the rapidly growing is a trend. This paper is the latest generation file system caused by the hacking attacks on the Sniffing for users using file encryption and key generation, Packet Sniffing Tool IP and data through the analysis are discussed. Through this study, the importance of protecting personal information by imprinting Proactive in the hacking incident, and what users will contribute to increase the level of security awareness.

키워드

Encryption, Hacking, Sniffing, Sniffing Tool, File Security

Ⅰ. 서 론

개인은 신원도용의 대상이 되고 취약점 악용으로 프라이버시, 전자적 거래 등의 개인정보 침해 사고사례가 그림 1처럼 증가하고 있다[1][2].

2010년 2월 1일 국회 의원회관 소회의실에서 열린 “패킷감청” 시연회에선 MSN Messenger로 나눈 대화 내용이 실시간으로 드러났다. Sniffing Tool(Wireshark)을 통해 인터넷 회선에 접속한 결과 메신저 대화 내용뿐만 아니라 Web-mail의 발신 수신 메일 내용과 로그인 ID, Password까지 드러났다[3][4].

그림 1. 개인정보 침해건수

인터넷 정보화 사회의 발달로 E-mail은 정보의 전달수단으로 보편화되고 있고 메신저는 사생활

의 내용까지도 문자와 화상을 통해 비용을 들이지 않고 통화가 가능하다[5][6].

따라서 네트워크 환경으로부터 개인신상 정보를 보호하기 위해 암호화를 이용한 정보보호가 실생활 되어야 한다[7][8].

본 논문에서는 Sniffing Tool을 이용한 메신저(NateOn, MSN), E-mail(Paran, Naver)을 이용하여 개인사생활 정보를 주고받았을 때 암호화 된 내용과 그렇지 않았을 때 암호화 패킷 분석에 대해 연구한다.

Ⅱ. 관련연구

2.1. Sniffing 기법

Sniffing기법은 Sniffer라는 프로그램에 의해 사용된다.

Sniffer는 "컴퓨터 네트워크상에 흐르는 트래픽을 엿듣는 도청장치"라고 말할 수 있다. 이러한 Sniffing 공격은 메신저, E-mail 등과 같이 여러 사용자가 네트워크를 공유하는 환경에서 매우 위협적인 공격이다[9].

2.2. 패킷분석

Sniffer 프로그램은 전기신호 형태로 흐르는 패킷을 수집한다. 이 방법으로 사용자의 메신저 대화 내용, 이메일 작성화면 등 정보를 볼 수 있다. 그림 2와 같이 패킷을 수집한다[10].

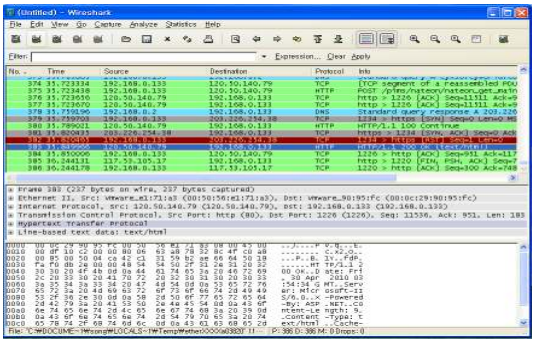

그림 2. Wireshark 패킷 수집

2.3. 암호화 GPG

암호화(Encryption) 및 키 생성/관리(Key Manager)는 GPG프로그램을 이용하여 데이터를 암호화 한다.

이러한 기법을 적용하면, 데이터에 접근할 때 수동으로 파일을 암호화하고 복호화 하는 과정을 명시해야 한다. 다양한 사용자 응용이 각각 다른 인터페이스와 키 관리, 암호화 알고리즘을 적용하기 때문에 다양한 안전성을 보장해줄 수 있다. 하지만, 이 기법은 많은 사용자 간섭이 필요하고 인증과 키 관리에 대한 어려움 때문에 여러 응용간에 일관성을 유지하기 힘들다. 그림 3은 암호화 방식의 구조이다.

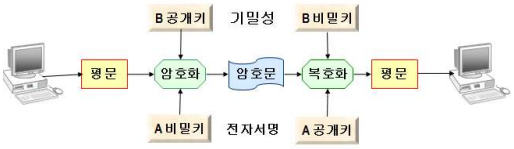

그림 3. 암호화 방식의 구조

Ⅲ. Sniffing에 의한 패킷분석

3.1. 실험환경

그림 4와 같이 네트워크 환경이 구성되어 있다.

■ 시스템

- CPU : Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz
- OS : Microsoft Windows XP Professional
- RAM : 512MB
- HDD : 40GB
- 가상 OS software : VMware
- 네트워크 환경 : NAT(Network Address Translation) 기반의 가상 네트워크

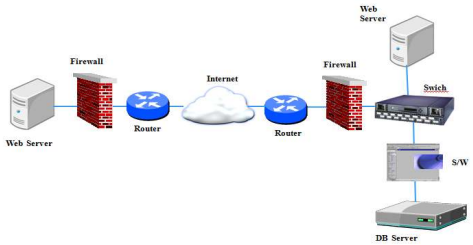

그림 4. 네트워크 환경

■ Sniffing Tool

- MSN Messenger 2009(14.0): MSN Sniffer2
- NateOn 4.0 : NateOnSniffer
- Naver : HttpAnalyzerstdV5
- Paran : HttpAnalyzerstdV5

■ 실험내용 : MSN Messenger, NateOn을 통한 “메시지 전송중입니다” 란 데이터를 전송하여 실험을 한다.

3.2. Sniffing 실시

트래픽을 수집하기 위해 공개 소프트웨어 Sniffing Tool을 사용 한다. 비정상으로 과도한 트래픽이 확인되는 구간의 패킷 내용(packet payload)을 분석하여 암호화의 여부를 확인한다.

3.2.1 메신저통신

MSN Sniffer2을 이용하여 패킷을 분석한 결과 그림 5와 같이 MSN Messenger는 암호화 되지

않은 평문이 드러났다. 반면에 NateOnSniffer로 Sniffing하여 실험한 NateOn은 평문이 암호화되어 내용이 드러나지 않았다. 그림 6은 NateOn Sniffing 화면이다.

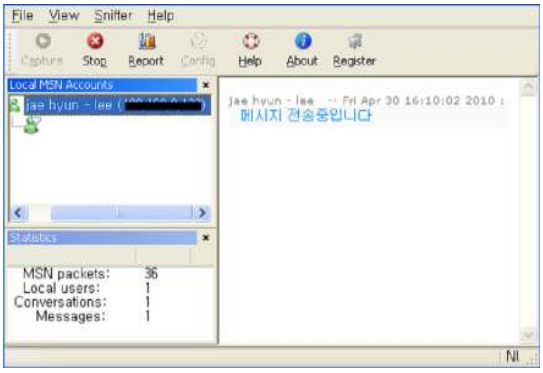

그림 5. MSN 메신저 Sniffing

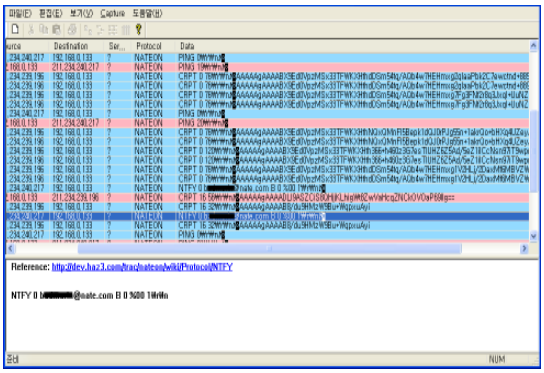

그림 6. NateOn 메신저 Sniffing

3.2.2. E-mail통신

그림 7, 8과 같이 Naver E-mail, Paran E-mail 패킷분석 실험에서 수신 된 이메일 확인 시, HttpAnalyzer을 실행하여 패킷 수집을 한다. Naver의 경우 평문이 암호화 되있는 것을 확인했다. Paran은 평문이 그대로 드러났다.

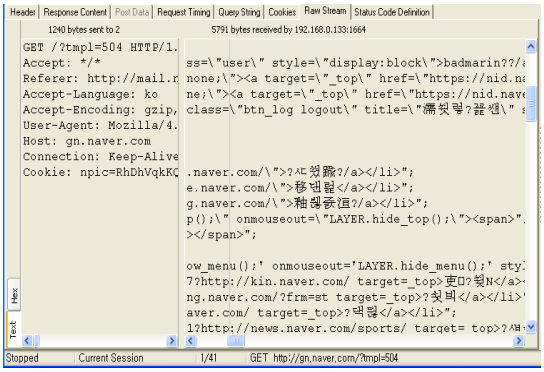

그림 7. naver E-mail 전송 Sniffing

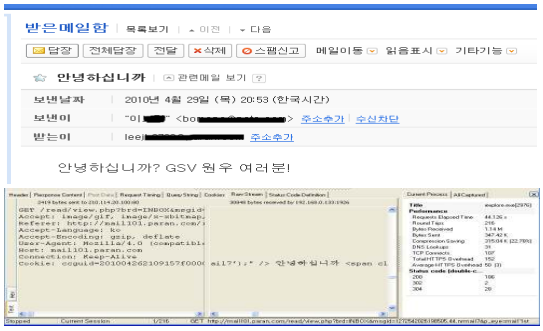

그림 8. Paran E-mail 전송 Sniffing

IV. 키 생성 후 암호화전송 분석

4.1. 키 생성

키를 만들고 관리하는 것은 암호화 프로세스에서 중요한 부분이다. 공개 키는 모든 사람에게 공개될 수 있는 반면, 개인 키는 공개키를 사용하여 암호화된 데이터를 해독할 사람만 알고 있어야 한다.

4.1.1. 공개키/비밀키 생성

사용자 인증을 위해 비밀번호를 입력하는 방법을 대체하는 공개키 사용자 인증을 한다. 즉 비밀키를 소유함으로써 사용자는 자신을 인증할 수 있다. 사용자는 이름, 메일주소, 비밀번호를 입력하여 그림 9와 같이 key를 생성할 수 있다.

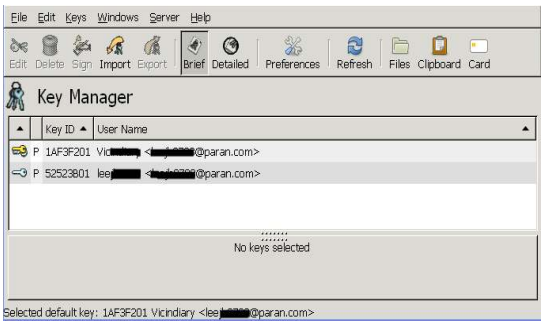

그림 9. 공개키/비밀키 생성

4.2. 전송내용 암호화

상대방의 공개키가 등록되고 clipboard를 이용해 전달할 내용을 작성한다.

그림 10. 전송 내용 암호화

Encrypt 버튼을 눌러 그림 10과 같이 암호화한다. 이때 받는 사람의 공개키로 암호화한다.

4.3. 암호화전송 통신보안 분석

데이터암호화를 통해서 데이터의 기밀성을 유지하며 또한 기본적인 암호화 구조 이외에 의미론적 안정성을 제공한다. 그림 11은 암호문 패킷을 분석 화면이다.

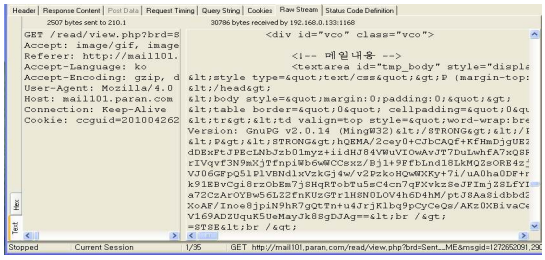

그림 11. 암호문 패킷 분석

4.3.1. 평문, 암호문 통신 분석(메신저, E-mail)

실험을 통해 평문과 암호문을 비교한 결과 표 1과 같이 평문 전송은 보안에 취약하다는 것을 밝혔다.

표 1. 메신저 E-mail Sniffing

암호화	대상	평문	암호문
메신저	NateOn	해독불가능	해독불가능
	MSN	해독가능	해독불가능
E-mail	Naver	해독불가능	해독불가능
	Paran	해독가능	해독불가능

따라서 메신저, E-mail 전송 시 프로그램 자체에 보안설정이나 암호화 프로그램을 설치하여 자신의 개인정보를 보호하는 것이 중요하다.

V. 결 론

우리의 개인정보는 해커에게 해킹 프로그램으로부터 정보를 지키지 위해서는 보안시스템의 보안성과 정책의 지원도 중요하지만 개개인의 정보보호에 적절한 관리와 지침으로 데이터의 기밀성 및 안정성을 유지하는 것이 중요하다. 따라서 암호화 기능의 투명화를 통해 사용의 편리성보안에 취약한 점들을 완벽하게 예방할 수 없지만 가능한 한 줄일 수 있다. 따라서 암호화 방법을 사용하여 경제적 손익과 개인정보침해에 대비한 사전 대응이 필요하다.

향후 연구에서는 네트워크 메신저 환경에서의 실시간 Sniffing 및 해킹을 당하였을 경우 IP 역추적 실시에 대한 기술과 포렌식 방법론에 대한 연구에 기여할 것이다.

참고문헌

[1] 김기수, “유비쿼터스 네트워크에서 안전한 개인정보보호를 위한 프라이버시 보호 방안”, 한국정보과학회, 제 34권 제 2호, pp.132-135, 2007. 10.

[2] 김우한, 최중섭, 홍관희, “정보통신 인프라 침해사고현황 및 대응체계”, 한국통신학회지, 제 21권 제 9호, pp.38-47, 2004. 9.

[3] 이민영, “직장내 전자우편의 감청에 대한 규율 방안”, 정보통신정책, 제 15권 제 23호, pp.19-39, 2003. 12.

[4] 이정애, 박종식, “메신저 메일 비밀번호 낱낱이 기술로도 ‘못막는 무제한 감청’”, 한겨레 http://www.hani.co.kr/arti/society/society_general/402316.html

[5] 신동휘, 최윤성, 박상준, 김승주, 원동호, " 네이트온 메신저의 사용자 인증 메커니즘에 대한 취약점 분석“, 정보보호학회논문지 제 17권, 제 1호, pp.67-80, 2007. 2.

[6] 천우성, 박대우, “WiBro 네트워크에서 메신저, VoIP 도청 및 포렌식 연구”, 한국컴퓨터정보학회, 제 14권 제 5호, pp.149-156, 2008. 9.

[7] 남기효, 박상중, 강형석, 남기환, 김성인, “개인정보보호기술의 최신 동향과 향후 전망”, 정보보호학회지, 제 18권 제 6호, pp.11-19, 2008. 12.

[8] 임재덕, 은성경, 김정녀, "데이터 보호를 위한 암호화 파일시스템의 분석“, 전자통신동향분석, 제 16권 제 4호, pp.54-66, 2001. 8.

[9] 박대우, “VoIP 서비스의 도청 공격과 보안에 관한 연구”, 한국컴퓨터정보학회논문지, 제 11권 제 2호, pp.155-164, 2006. 9.

[10] 정성모, 송재구, 김석수, 박길철, “패킷 스니핑을 활용한 효율적인 모니터링 시스템에 관한 연구”, 한국정보기술학회 논문집, pp.587-590, 2009. 6.