情報保護學會論文誌
第17卷 第6號, 2007. 12

DDoS 공격에 대한 방화벽 로그 기록 취약점 분석*

천 준 호†, 신 동 규‡, 장 근 원, 전 문 석
숭실대학교 컴퓨터학과

Analysis of Security Vulnerability on Firewall Logging Mechanism against DDoS Attack

Junho Choun†, Dong-Gyu Shin‡, Kun-Won Jang, Moon-Seog Jun
Department of Computing, Soongsil University

요 약

DDoS 공격과 같이 전송량이 폭주하는 상황에서는 방화벽이 정상적으로 로그를 기록하지 못하는 취약점이 발생한다. 이와 같은 로그의 누수 현상은 방화벽이 패킷을 정상적으로 필터링 했는지 여부를 알 수 없게하며, 침해사고 대응의 가장 기초적인 자료가 되는 방화벽 로그에 대한 신뢰성을 심각하게 위협한다. 또한 통신망의 속도가 높아질수록 이와 같은 현상이 보다 잦은 빈도와 대량으로 발생한다. 따라서 단순히 방화벽 시스템의 하드웨어를 강화하여 해결하는 방법은 방화벽의 대중화와 상충되므로 바람직하지 않다. 본 논문에서는 국내 대부분의 방화벽의 모태가 되는 iptable의 로그 누수현상을 실험을 통해 입증함으로서 기존의 방화벽 로그 처리 방식에 개선이 필요함을 보인다.

ABSTRACT

In the context of mass traffic, firewall system cannot record normal log files against DDoS attack. The loss of log record causes that a firewall system does not know whether a packet is normally filtered or not, and firewall log, which is an essential data for the counter measure of violation accident, cannot be verified as trusted. As a network speed increases, these problems happen more frequently and largely. Accordingly, the method to use simply additional hardware devices is not recommended for the popularization of firewall.

This paper is devoted to verify the loss of iptable log that is the mother's womb of most domestic firewall systems and show that the log handling methods for conventional firewall systems are needed to improve.

Keywords : DDoS, Firewall, Network Security

Ⅰ. 서 론

방화벽은 네트워크의 구성에 필수적인 요소가 되었으며 인터넷의 발달과 맞물려 처리용량이 증가되었다. 과거에는 대규모 네트워크에만 제한적으로 사용됐으나, 임베디드 기술과의 접목으로 기존의 유닉스 시스템 기반의 방화벽에 비해 가격대비 효율이 향상됨에 따라 현재는 스위칭 허브나 IP 공유기와 같은 기본적인 네트워크 장비에도 설치된다. 또한 네트워크를 따라 점파되는 웜(Worm)을 차단하기 위해서나 인터넷 뱅킹과 온라인 게임 등과 같이 개인정보보호가 필요한 분야가 증가했기 때문에 개인용 컴퓨터에도 필수적으로 설치된다[1].

접수일: 2007년 4월 27일; 채택일: 2007년 10월 16일
*본 연구는 숭실대학교 교내연구비 지원으로 이루어졌음
† 주저자, opendr@ssu.ac.kr
‡ 교신저자, dgstyle@ssu.ac.kr

한편 방화벽 로그는 침해사고 발생시 침입자를 파악하고 침입 방법을 알아내는 중요한 단서가 되기 때문에 로그를 일정 기간 동안 보관하고 분석할 것을 정부 차원에서 권고하고 있다[1,2]. 또한 1.25 인터넷 대란과 같이 DoS/DDoS 공격이 원인이 되는 경우 로그 분석을 통해 공격의 징후를 파악하는 등의 대책을 강구할 수 있다[3].

고속화된 통신망 때문에 처리해야할 패킷의 수가 기하급수적으로 증가했으며, 로그를 저장하는 방법은 내부 메모리 보다 수천배 이상 속도가 느린 디스크 입출력을 사용하므로, 방화벽이 로그를 모두 정확히 기록 못하는 경우가 발생한다. 정확히 기록되지 못한 로그는 [그림 1]과 같이 비정상적인 형태로 저장된다.

이러한 로그를 통해서는 방화벽이 정상적으로 패킷을 필터링 했는지 여부를 알 수 없으며 정확한 로그 분석을 방해한다. 또한 전송량이 증가함에 따라 이러한 부정확한 로그의 발생 빈도가 증가하기 때문에, DoS/DDoS와 같이 고의적으로 전송량을 폭주시키는 공격 유형에 대응하기 위해서 반드시 해결해야하는 문제점이다. 일부 제조사에 따라서는 시간 이외에 내용이 동일하면서 매우 짧은 시간 차이의 로그는 횟수만을 기재하고 전송량을 합산하여 하나의 로그로 저장하는 등의 기법이 존재하지만, IP Table을 기반으로 만들어진 대부분의 방화벽은 위와 같은 취약점을 공통적으로 갖는다. 본 논문에서는 이와 같은 현상을 분석함으로서 침해사고 대응의 기초자료가 되는 방화벽 로그의 신뢰도를 재고하고자 한다.

```
time="2006-11-10 03:00:02" src=172.16.24.4 dst=224.0.0.10
time="2006-11-10 03:00:02" src=172.16.24.6 dst=224.0.0.18
time="1970-01-01 00:00:00" src=172.16.24.2 dst=224.0.0.10
time="1970-01-01 00:00:00" src=172.16.24.2 dst=224.0.0.10
time="1970-01-01 00:00:00" src=172.16.24.6 dst=224.0.0.18
time="1970-01-01 00:00:00" src=172.16.24.252 dst=224.0.0.1
time="1970-01-01 00:00:00" src=172.16.24.5 dst=224.0.0.10
time="1970-01-01 00:00:00" src=172.16.24.6 dst=224.0.0.18
time="1970-01-01 00:00:00" src=172.16.24.252 dst=224.0.0.1
time="1970-01-01 00:00:00" src=172.16.24.5 dst=224.0.0.10
time="1970-01-01 00:00:00" src=172.16.24.3 dst=224.0.0.10
time="1970-01-01 00:00:00" src=172.16.24.253 dst=224.0.0.1
time="1970-01-01 00:00:00" src=172.16.24.1 dst=224.0.0.10
```

〔그림 1〕 방화벽 로그의 누수현상

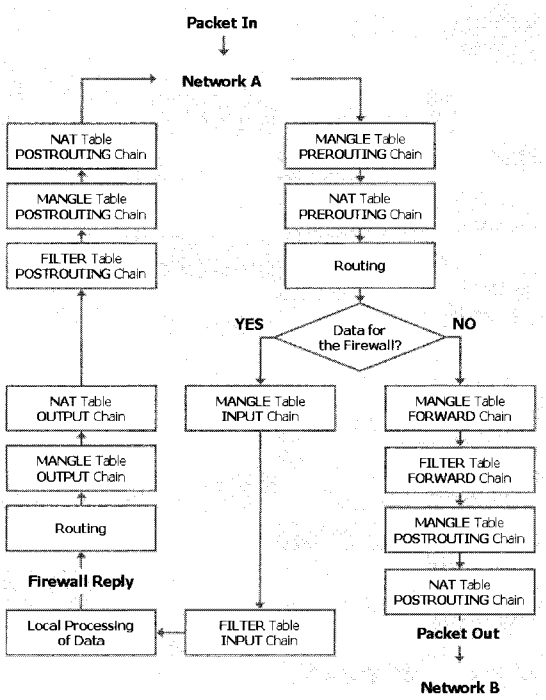
Ⅱ. 관련연구

2.1. Packet Filter

IP Table은 GNU 라이센스에 기반한 공개 소프트웨어로서 대부분의 유닉스/리눅스 시스템에 기본적으로 설치 및 운용되고 있는 방화벽 소프트웨어이다. 현재 국내의 대부분의 방화벽은 IP Table을 기본으로 구현되었다[4].

IP Table은 기본적으로 Output/Input/Forward Chain에 설정된 규칙대로 패킷 필터링을 하며, 이외에도 NAT(Network Address Transition)과 Masqurade 기능 등을 탑재하고 있다[10].

패킷 필터가 로그를 기록하는 시점은 [그림 2]의 최종 단계인 Packet Out 상태가 지난 후, 다음 패킷을 기다리는 사이에 발생하는 유휴시간이다.[5] 즉 패킷 하나당 한 번의 디스크 I/O를 수행하므로 내부 메모리에서만 수행되는 패킷 필터링 속도에 비해 로그 기록에 소요되는 시간이 상대적으로 길다. 이러한 수행 시간의 차이가 로그 기록의 누수를 발생시키는 원인이 된다.



〔그림 2〕 Packet Filter의 순서도

2.2. 로그 처리

전송망의 속도 향상과 맞물려 방화벽이 처리하는 패킷의 수도 급격히 증가했기 때문에 방화벽 로그를 실시간으로 분석하는 것은 사실상 불가능하다. 일반적으로 하루 분량의 로그를 백업하여 네트워크 전송량이 비교적 적은 유휴시간에 별도의 로그 분석기를 사용해서 1일 1회 이상 비실시간으로 분석하여 통계를 산출하는 것이 일반적이다[9].

로그 기록에 널리 쓰이고 있는 Syslogd는 DBMS의 경우 보다는 적은 I/O 시간을 필요로 하지만 로그의 모든 내용을 텍스트 방식으로 저장하기 때문에 하루 분량의 로그 용량이 수 Giga-byte를 넘는 경우가 많다. 최소 6개월 분량의 로그를 백업하는 실정에 적용하기에는 저장 공간에 대한 문제와 함께, 분석에 많은 시간이 소요되므로 방화벽 로그에 적합하지 않다.

가장 현실적이며 현재 널리 쓰는 방식은 [그림 3]과 같이 바이너리 파일 형태로 저장하는 방식이다. 메모리/하드디스크 시간별 사용현황, 보안 감사 등의 부가적인 로그를 남기기도 하지만 기본적으로 사용하는 로그는 [그림 4]와 같이 admitted/denied 로그 두 종류이며 전송 속도에 따라서 Little/Big Edian을 혼용한다. 방화벽의 로그는 이외에도 여러 종류가 있지만, 전송량과 직접적인 연관이 없는 로그는 양이 많지 않으므로 로그의 누수 현상은 발생하지 않는다. 또한 방화벽 시스템의 하드웨어적 사양을 고려하여 admitted/denied 로그를 분석하면 계산 할 수 있는 정보이다. 그러나 속도면에서 가장 월등하다고 할 수 있는 아래의 방법도 로그의 누수 현상이 발생하며 본 논문이 분석하고자 하는 대상 역시 이와 같은 바이너리 파일을 사용한 비실시간 로그 분석이다[7,8].

한편, 체크포인트사의 스마트 디펜스와 같이 선제적 방어를 목적으로 하는 통합보안관리 도구는 DDoS 공격과 같이 비정상적으로 전송량과 그에 따른 로그가 폭주하는 경우, 로그의 가장 많은 비중을 차지하는 admitted 로그의 저장을 중단하고, 나머지 보안기능에서 나오는 로그들을 Correlation 알고리즘이라는 상호 연관관계에 의거 분석되어, 각각의 솔루션에서 미처 발견되지

```
00000020h: 43 72 39 20 43 72 39 20 00 00 00 0D 00 00
00000030h: 00 00 00 00 05 58 45 03
```

[그림 3] Denied 로그의 Binary 형식

Number of byte RCVD							
Number of byte SENT							
SRC IP				DST IP			
Number of packet RCVD				Number of packet SENT			
Start Time				End Time			
Rule ID				SRC Port		DST Port	
Rule Number		FW Number		Priority	Protocol	SRC IF	RCVD
SRC IP				DST IP			
Rule ID				Time			
SRC Port		DST Port		RSVD			
Flag	Dir	Protocol	Priority	Action	RSVD		

[그림 4] 로그 포맷
(a) admitted log, (b) denied log

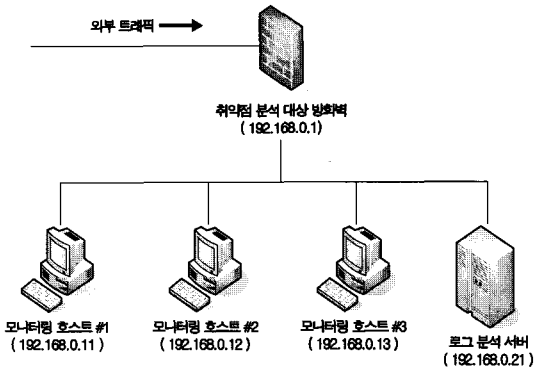
못한 부분을 감지한다. 즉 스마트 디펜스에서 사용되는 Correlation 알고리즘은 메모리 사용량, CPU 사용량 등의 자원 사용량에 대한 로그와 보안 감사 로그와 이벤트 로그 등을 종합하여 네트워크의 상황을 판단하는 것이다. 이러한 기능이 없는 방화벽의 경우, DDoS가 발생하여 네트워크 효율이 감소하거나 로그의 소실이 누적되어 모니터링이 불가능해지는 시점에서야 DDoS의 발생을 감지하지만, 스마트 디펜스의 선제적 방어를 위한 Correlation 알고리즘을 사용 할 경우, 보다 빠른 감지 및 대응이 가능하다는 장점을 갖는다.

그러나 DDoS로 인한 시스템 자원의 고갈을 방지하기 위해 전송량과 전송자에 대한 정보가 담겨있는 admitted/denied 로그 저장을 중단시키므로 DDoS의 정확한 발생 원인과 발신지에 대한 정보를 수집하는데 어려움이 따른다.

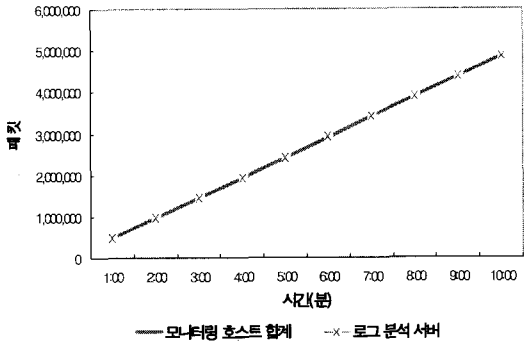
Ⅲ. 전송량에 따른 로그 처리 취약성 분석

3.1. 네트워크 및 로그 분석 설계

본 논문에서 분석하고자 하는 로그의 누수 현상을 보이기 위해 [그림 5]와 같이 네트워크를 설계한다. 분석 대상이 되는 방화벽을 통해 유입된 트래픽은 모니터링 호스트 세 대에 분산시킨 후, inbound로 Sync Flooding 공격을 시도하며[6] 실험에 사용된 시스템의 사양은 [표 1]과 같다.



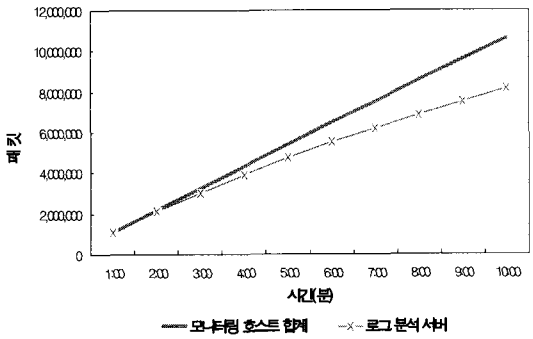
〔그림 5〕 로그 누수 현상 탐지를 위한 네트워크 설계



〔그림 6〕 DDoS 발생 이전의 admitted 로그 분석 결과

〔표 1〕 실험에 사용된 시스템 사양

시스템명	사양 (CPU / RAM / HDD)
취약점 분석 대상 방화벽	PPC750FX 800MHz / 512 RAM / 5400 RPM
모니터링 호스트 #1	펜티엄4 2.66GHz / 512 RAM / 7200 RPM
모니터링 호스트 #2	펜티엄4 2.66GHz / 512 RAM / 7200 RPM
모니터링 호스트 #3	펜티엄4 2.66GHz / 512 RAM / 7200 RPM
로그 분석 서버	펜티엄 듀얼 코어 3.40GHz (64-bit) / 2G RAM / 7200 RPM



〔그림 7〕 DDoS 발생 이후의 admitted 로그 분석 결과

방화벽을 통과한 트래픽은 세 대의 모니터링 호스트에 유입되고 각각의 호스트는 트래픽 양을 계산한다. 일정 시간이 경과한 후 방화벽의 로그가 바이너리 형태로 저장되면 로그 분석 서버로 전송하고 로그 분석 서버에서 계산된 결과를 모니터링 호스트에서 계산한 트래픽 양의 합과 비교하여 로그의 누수가 있었는지 여부를 분석한다.

로그의 부정확한 기록이 방화벽이 보장하는 전송량 범위 이내에서 발생함을 보이기 위해, 실험을 위해 인위적으로 발생시킨 트래픽의 양은 모든 실험에서 분석 대상이 되는 방화벽의 한계 전송량 이내로 조절하였다.

3.2. 전송량에 따른 로그 분석

방화벽의 필터링 규칙에 위배되지 않도록 패킷을 생성시켜 admitted 로그를 남기도록 의도하였다. DDoS를 발생시키지 않은 상태의 트래픽을 유지하면서 모니터링 한 결과 모니터링 호스트에 수신된 로그 보다 방화벽이 남긴 정상적인 로그의 수는 $1/10^{-6}$% 적었다. 시간에 다른 로그의 축적을 그래프로 나타내면 [그림 6]과 같다.

DDoS 공격이 발생한 이후의 admitted 로그를 분석한 결과는 [그림 7]과 같다. 실험이 진행되는 시간 동안 세 대의 모니터링 호스트가 받은 전송량의 합과 방화벽 로그를 분석한 결과의 합 차이는 23.10%였다. 이 차이 만큼의 로그는 시간이나 IP 주소 등이 손상되어 [그림 8]와 같이 정상적으로 기록하지 못하였다. 방화벽이 정상적으로 패킷을 필터링 하였으나 로그를 정확히 기록하지 못한 결과이다. 시간이 지남에 따라 로그 누수가 증가하는 이유는, 방화벽이 로그 기록에 필요한 충분한 메모리를 확보하지 못하기 때문에 최초의 누수가 발생하고 로그를 디스크에 옮기기 위한 작업이 수행되는 동안 발생하는 로그가 버려지거나 훼손되기 때문으로 분석된다.

[그림 8]의 경우 로그의 수가 10^7 건이며 각 로그의 크기가 56byte이므로 총 560Mbyte 크기의 저장 공간을

```
time="2006-11-11 12:00:02" src=192.168.0.2 dst=192.168.0.11
time="2006-11-11 12:00:02" src=192.168.0.2 dst=192.168.0.11
time="1970-01-01 00:00:00" src=192.168.0.2 dst=192.168.0.11
time="1970-01-01 00:00:00" src=192.168.0.2 dst=192.168.0.11
time="1970-01-01 00:00:00" src=192.168.0.2 dst=192.168.0.12
time="1970-01-01 00:00:00" src=192.168.0.4 dst=192.168.0.11
time="1970-01-01 00:00:00" src=192.168.0.5 dst=192.168.0.13
time="1970-01-01 00:00:00" src=192.168.0.2 dst=192.168.0.13
time="1970-01-01 00:00:00" src=192.168.0.4 dst=192.168.0.11
time="1970-01-01 00:00:00" src=192.168.0.5 dst=192.168.0.11
time="1970-01-01 00:00:00" src=192.168.0.3 dst=192.168.0.12
time="1970-01-01 00:00:00" src=192.168.0.2 dst=192.168.0.13
time="1970-01-01 00:00:00" src=192.168.0.2 dst=192.168.0.11
```

(a)

```
time="2006-11-11 12:00:02" src=192.168.0.2 dst=192.168.0.11
time="2006-11-11 12:00:02" src=192.168.0.2 dst=192.168.0.11
time="1970-01-01 00:00:00" src=192.168.0.2 dst=192.168.0.11
time="1970-01-01 00:00:00" src=192.168.0.2 dst=112.168.0.11
time="1970-01-01 00:00:00" src=192.168.0.2 dst=112.168.0.12
time="1970-01-01 00:00:00" src=192.168.0.4 dst=112.168.0.11
time="1970-01-01 00:00:00" src=192.168.0.5 dst=112.168.0.13
time="1970-01-01 00:00:00" src=192.168.0.2 dst=112.168.0.13
time="1970-01-01 00:00:00" src=192.168.0.4 dst=112.168.0.11
time="1970-01-01 00:00:00" src=192.168.0.5 dst=112.168.0.11
time="1970-01-01 00:00:00" src=192.168.0.3 dst=0.168.0.12
time="1970-01-01 00:00:00" src=192.168.0.2 dst=0.168.0.13
time="1970-01-01 00:00:00" src=192.168.0.2 dst=0.168.0.11
```

(b)

〔그림 8〕 방화벽의 비정상적 로그 처리
(a) 시간 기록의 오류, (b) IP 주소 오류

확보해야 한다. 그러나 실험에 사용한 취약점 분석 대상 방화벽의 메모리가 이 보다 작으므로, 불가피하게 디스크 접근이 발생했으며, 메모리에 비해 상대적으로 속도가 낮은 저장방식 때문에 로그가 유실된 것이다.

즉, 전체 메모리에서 로그 기록에 사용할 수 있는 최대치를 초과할 때 발생하는 디스크 접근이, 로그 유실을 발생시키는 주원인으로 분석된다.

Ⅳ. 결 론

본 논문에서는 방화벽의 로그가 비정상적으로 저장되어 침해사고에 대한 자료로서의 가치가 저하되는 현상을 실험을 통해 입증함으로서 방화벽의 성능과 기능적인 요소 외에도 고려해야할 사항이 있음을 보였다. 또한 이러한 현상은 방화벽 제품이 보장하는 한계 전송량 범위 이내에서도 발생한다. 따라서 DDoS/DoS 공격과 같이 전송량이 폭주하는 경우에 더욱 잦은 빈도로 발생하므로 로그 분석의 필요성이 더욱 요구되는 상황에서 실질적인 가치가 더욱 감소한다. 충분한 크기의 메모리를 확보하는 것은 통신망의 고속화 추세에 맞지 않으므로 보다 원천적인 해결책이 필요하다. 본 논문의 후속 연구로는 패킷 필터링에서 부터 로그 기록에 대한 고려가 포함된 재설계를 하고자한다. 즉 패킷에 대한 비교를 최소화하고 각 비교 단계에서 로그를 부분적으로 기록하는 방식에 대한 연구를 수행하고자한다.

참고문헌

[1] 행정자치부, 전자정부전문위원회, "정보시스템 구축 운영 기술 가이드라인 2.0", 2005. 10.

[2] 법제처, "정보통신망 이용촉진 및 정보보호 등에 관한 법률", 제 48조의 4항, 법률 제8289호, 2007. 01. 개정.

[3] S. Gibson "The Strange Tale of the Denial of Service Attacks Against GRC.COM," http://grc.com/dos/grcdos.htm, 2002.

[4] Open Source IDS Snort, http://www.snort.org

[5] L. Feinstein, Dan Schnackenberg, "Statistical Approaches to DDoS Attack Detection and Response," Information Survivability Conference and Exposition, 2003.

[6] David K, Y. Yau, "Defending Against Distributed Denial-of-Service Attacks With Max-Min Fair Server-Centric Router Throttles," IEEE/ACM TRANSACTIONS ON NET-WORKING, Vol.13 No.1, Feb., 2005.

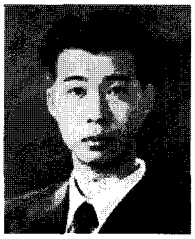
[7] C. Hare, K. Siyan, "Internet Firewalls and Network Security," 2nd BK&CD edition, New Riders Publishing, Aug., 1996.

[8] G. Class, "Unix for Programmers and Users Complete Guide," McGraw-Hill, Aug., 1994.

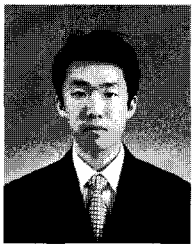
[9] 이상훈, 국경완, "실시간 파일시스템 접근 로그 감시를 통한 리눅스 보안강화에 관한 연구", 한국전자통신연구원, Jul., 2001.

[10] Jeffery C. Mogul, Richard F. Rashid and Michael J. Accetta, "The Packet Filter : An Efficient Mechanism for User-level Network Code," In Processings of the 11th ACM Symposium on Operating System Principles, pp. 39-51, ACM Press, Nov., 1987.

〈著者紹介〉

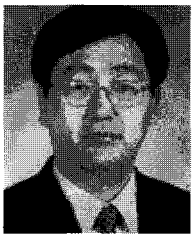


천 준 호 (Junho Choun) 정회원
2003년 2월 : 숭실대학교 컴퓨터학과 졸업
2005년 2월 : 숭실대학교 컴퓨터학과 석사
2005년 3월~현재 : 숭실대학교 컴퓨터학과 박사과정
<관심분야> 정보보호, 암호학, 정수론, u-City



신 동 규 (Dong-Gyu Shin) 정회원
2004년 2월 : 천안대학교 컴퓨터학과, 정보처리학과 졸업
2006년 2월 : 숭실대학교 컴퓨터학과 석사
2006년 3월~현재 : 숭실대학교 컴퓨터학과 박사과정
<관심분야> 정보보호, 멀티미디어 보안, Sensor Network, RFID

장 근 원 (Kun-Won Jang) 정회원
1998년 2월 : 고려대학교 영어영문학과 졸업
2003년 2월 : 숭실대학교 정보과학대학원 정보통신학과 석사
2007년 2월 : 숭실대학교 컴퓨터학과 박사
<관심분야> 정보보호, Sensor Network, DRM, Steganography



전 문 석 (Moon-Seog Jun) 정회원
1981년 2월 : 숭실대학교 전자계산학과 졸업
1986년 2월 : University of Maryland Computer Science 석사
1989년 2월 : University of Maryland Computer Science 박사
1986년 9월~1989년 12월 : University of Maryland 강사
1989년 3월~7월 : Morgan State University 조교수
1989년 9월~1991년 2월 : New Mexico State University Physical Science Lab. 책임연구원
1991년 3월~현재 : 숭실대학교 정교수
<관심분야> 정보보호, 전자여권, 전자상거래