# 사이버 국방 보안에 대한 연구
# A Study for National Cyber Security and Defense

이문구(김포대학교)

**차 례**

1. 서론
2. APT 공격의 특징과 공격사례
3. 사이버국방 보안을 위한 APT공격 대응방안
4. 결론

## 1. 서론

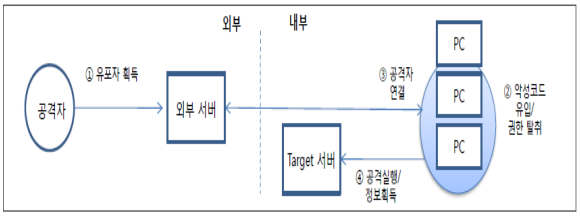
인터넷 서비스기술과 통신 기술의 발전으로 정보화의 순기능에 의한 정보화 사회의 실현은 급속도로 이루어졌으며, 우리의 실생활은 신속하고 다양한 정보의 공유로 많은 도움을 받고 있다. 그러나 그 이면에 정보화의 역기능으로 인한 보안상의 위협 역시 매우 다양하고, 지능적인 방법으로 우리 사회를 위협하고 있다. 정보화의 역기능현상 중에 사이버 범죄(Cyber Crime)는 해킹, 컴퓨터 바이러스와 같은 유형의 사이버 테러형 범죄와 사이버 명예훼손과 전자상거래 사기, 개인 정보침해, 불법사이트 개설, 디지털 저작권 침해 등과 같은 일반 사이버 범죄가 있다. 또한 1998년부터 정보전을 준비해온 북한은 사이버 테러 능력을 갖춘 사이버 공격조직을 2002년 북한이 인민무력부 정찰총국 산하에 1000명의 규모로 구축하여 갖추고 있다. 이러한 북한의 사이버공격조직의 범죄는 중국의 IP를 이용 혹은 경유하여 원격의 좀비 PC를 조종하여 정부기관 및 포털 사이트에 접근하여 해킹 등으로 사이버 테러를 가하고 네티즌을 가장한 유언비어 유포 활동을 하고 있으며 그 사례가 2004년 이후 무려 5만건에 이르고 있다[1].

최근 북한의 소행으로 알려진 2009년 7.7 디도스(DDoS : 분산 서비스 거부)공격, 2011년 4월 농협 전산망 마비 사고, 그리고 2011년 7월 SK커뮤니케이션즈 고객 정보 유출 사고, 2013년 3월 금융 및 방송망 마비 사고[2] 등이 있다. 최근의 이러한 공격들은 단순한 호기심 충족이나 기술의 과시, 서비스 거부 공격으로 끝나는 것이 아니라 특정 조직의 경제적, 정치적 목적 달성을 위해 공격자가 해당 목표에 맞는 제로데이 취약점, 사회공학 기법 등 다양한 기법을 조합하여, 오랜 기간 지속적으로 탐지 및 대응을 회피하며 지능형 지속 위협(Advanced Persistent Threat)공격을 진행하고 있다는 것이다. 이에 본 연구에서는 APT 공격의 개념을 이해하고 공격 사례[8]를 기반으로 사이버 국방 보안에 대하여 우리가 고려해야 할 대응방안을 제시하고자 한다.

## 2. APT 공격의 특징과 공격사례

### 2.1 APT 공격의 주기와 특징

APT 공격은 특정 대상의 주요 정보 획득의 목적을 갖고 지속적으로 공격하는 해킹이다.




▶▶ 그림 1. APT 공격 시나리오

APT 공격의 주기는 그림 1의 공격 시나리오처럼 공격 목표에 대해 공격 목표의 홈페이지, 외부 공개자료, 조직도, 주요 임직원 정보, 협력업체, 정보시스템 유형 및 버전, 애플리케이션의 종류 및 버전 등 공격목표에 대해 전방위적으로 정보를 수집하고 공격에 활용할 수 있는 취약점을 식별하는 공격 준비 과정으로 사전조사 단계를 갖는다. 사전 조사된 정보를 바탕으로 정보시스템, 웹 어플리케이션 등의 알려지지 않은 취약점 및 보안시스템에

서 탐지되지 않는 악성코드 등을 이메일, SNS, App 등을 통해 공격 대상을 감염 시킨다.

해당 취약점에 의해 악성코드에 감염된 PC는 동일한 취약점을 보유하고 있는 PC를 스캔하여 다시 감염시킨 후 정상적인 이용자로 가장하여 시스템 접속정보 등에 대한 정보수집과 서비스 이용패턴, 방법 등에 대한 모니터링을 수행하는 것으로, 관리자 계정의 확보를 시도하여 관리자 권한으로 상승 후 수집 가능한 모든 정보를 수집한다.

이처럼 시스템 관리자로서의 권한상승을 통해 목표로 하는 정보를 획득한 이후 공격대상의 내부 서버에 암호화하여 저장하거나 압축파일로 저장하여 비정기적으로 공격자의 단말기로 유출하는 등 공격이 탐지되지 않도록 하는 활동과 공격이 탐지되었는지를 지속적으로 모니터링 하는 활동이 이루어진다. 만약 공격이 탐지된 경우 대응을 하는 활동이 이루어지고, 이후 공격자는 핵심정보를 지속적으로 유출하기 위하여 백도어 프로그램을 설치한 후 표적이 되는 대상에게 지속적으로 접근을 한다.

## 2.2 APT 공격 사례

### 2.2.1 해외 사례

APT 공격의 해외 피해사례는 표 1에 정리된 바와 같다[2]. 1999년에는 미국 국방부와 항공우주국(NASA) 해킹사고가 발생하였으며 이로 인해 핵무기 정보와 군사시설정보 등 국가기밀이 유출되었다. 미 국방부와 NASA는 해당 사실을 1999년에 인지했으나 공격자는 1998년부터 이미 1년 동안 내부의 컴퓨터에 잠입해 정보를 유출한 것이었다. 2010년 6월에는 이란의 원자력 발전소 일부가 마비되는 사고가 세상에 알려졌다. 실제로 이란 대통령이 핵발전 원심분리기가 출처불명의 악성코드에 의해 작동이 정지되었다고 시인했다. 피해를 입은 것은 가동 중인 우라늄 원심분리기 약 1,000여대(전체의 10%)이었으며, 공격자의 악의적 조작에 의해 작동불능 상태에 빠진 것으로 밝혀졌다. 공격은 내부의 업무프로세스와 사용되는 컴퓨터 운영체제 버전, 그리고 산업제어시스템(SCADA)의 구조 등의 정보를 면밀히 파악하고 이들의 취약점을 이용한 공격이었다.

최초의 감염은 USB를 통해 시작되었고, 내부 전이를 위해서는 4개의 제로데이 취약점(Zero Day Vulnerability)을 이용하는 등 복합적이고 지능적인 방법을 사용하였다. 뿐만 아니라 내부의 백신정보를 스캔하고 자신을 은닉하거나 스스로 삭제하는 등의 지능화된 안전장치도 있었다.

미국의 IT전문매체인 인포월드(infoworld)의 조사에 의하면 이 공격에 이용된 악성코드의 첫 번째 등장은 피해가 밝혀졌던 2010년 6월의 1년 전인 2009년 6월부터이며, 전문개발팀이 5명에서 30명 사이의 규모로, 6개월의 준비기간이 걸렸을 것으로 추정된다고 한다[3-5].

피해의 대상은 국방과 국가 주요기관만이 아니었다. 핵심 산업기밀 정보를 보유한 조직에도 APT공격은 발생했는데 2011년 3월 미국 RSA사의 OTP제품(One-Time Password)인 'SecureID'의 기술정보 해킹사고가 그 예이다. OTP는 일회성으로 사용되는 비밀번호를 의미하며, 높은 수준의 보안성을 보장하며 안전한 사용자 인증기술로 알려져 있는데 이의 핵심정보인 비밀번호 생성 알고리즘이 유출된 것이다. 공격과정에서

**표 1. 해외 APT 주요 공격 사례**

| 피해 기관(시설)명 | 내용(피해규모) | 상세 내 용 |
|---|---|---|
| 소니해킹<br>(2011년 4월) | 고객정보 유출<br>(1억여건) | - 룰즈섹 해커그룹, 2011년 4월 이후부터 16차례 이상 해킹<br>- 소니 가입자 개인정보 유출건수 1억 여건 |
| EMC/RSA해킹<br>(2011년 3월) | 보안인증 기술<br>(OTP) 유출 | - SNS로 공격대상 정보수집, 사회공학적 기법으로 악성코드 감염<br>- 이후 범용SW의 제로데이 취약점을 이용 정보유출 |
| 모건 스탠리 해킹<br>(2010년 1월) | 산업기밀 유출 | - 구글과 모건스탠리를 해킹, 내부 중요정보를 탈취<br>- 2009년 6월에 시작하여 6개월간 지속된 것으로 확인됨 |
| 글로벌 에너지 기업 해킹<br>(2011년) | 제조/ 영업 관련 기밀자료 유출 | - 취약한 웹서버에 SQL인젝션 공격으로 악성파일 업로드<br>- 스피어-피싱을 통해 접속을 위한 계정정보 획득, 내부PC감염<br>- 획득한계정정보로 계정 추가수집 및 시스템 접속<br>- 표적대상서버 서서히 접근, 자료 외부 유출(2009년부터 2년간) |
| 이란원자력발전소마비<br>(2010년 7월) | 핵 발전시설<br>시스템 마비 | - 독일 지멘스사의 산업자동화시스템, SCADA 임의 제어<br>- 원심분리기 1,000여대 작동 불능 상태로 만듦<br>- USB로 내부망 최초 침투, MS 4개 제로데이 취약점 이용 확산<br>- 인터넷 연결된 일반PC 감염, 내부 정보를 스캔, 자신 은닉 |
| 100여 개국 대사관 및 정부기관 해킹<br>(2009년) | 국가기밀 유출 | - 전 세계 103개국 대사관, 정부기관 잠입 국가기밀정보 유출<br>- 2007년 5월부터 데이터 수집 시작, 2009년 3월까지 지속<br>- 감염된 호스트 평균 활동시간 145일, 가장 긴 시간 660일 |
| 미국 국방부, 항공우주국 해킹<br>(1999년) | 국가기밀 유출<br>(핵무기 정보, 군사 시설 지도, 병력 구성 등) | - 1998년부터 1년 동안 지속되었음.<br>- 미 국방부는 침입자 경로 역추적, 구소련 해커의 소행임을 주장, 러시아는 확인을 거부. |

**표 2. 국내 APT 공격 주요 사고 사례**

| 피해 기관(시설)명 | 내 용 | 상세 내 용 |
|---|---|---|
| 3.20 전산대란<br>(2013년 4월) | 주요 방송국 · 금융사<br>전산망 마비 | - 목표 조직의 내부PC 악성코드로 감염, 자산관리서버의 로그인 인증 관련 취약점 악용 접근, HDD 파괴 악성코드 배포<br>- 2012년 6월경부터 무려 1,590회나 국내 금융사 전산망에 침입<br>- 총 4만8천여 대의 PC, 서버가 피해를 입음 |
| 넥슨 메이플스토리 해킹<br>(2011년 11월) | 고객정보 유출<br>(1,320만 건) | - 내부 직원 PC에 악성코드 설치, 서버 운영관리팀장 PC 침투<br>- 정보 수집 통해 백업시스템 접근 계정 획득, 개인정보 유출 |
| SK 커뮤니케이션즈 해킹<br>(2011년 7월) | 고객정보 유출<br>(3,500만 건) | - 네이트의 DB에 저장된 가입자 3,500만 명의 아이디, 비밀번호, 이름, 주민등록번호, 연락처 등의 개인정보 유출<br>- 웹서버 취약점, 내부 임직원 비인가 SW사용 악용하여 악성코드 유포, 이를 통해 중요서버의 접근계정 획득, 정보 유출 |
| 농협해킹<br>(2011년 4월) | 서비스 마비<br>(18일) | - 외주업체 직원의 서버관리용 노트북 외부 반출입, 악성코드 감염<br>- 이를 통해 내부 확산점령. 중요 서버 계정/비밀번호 등 정보수집<br>- 4월 12일에 서버들은 서로를 공격하여 30분 만에 절반 파괴 |
| 현대 캐피탈<br>(2011년 4월) | 고객정보 유출<br>(175만 건) | - 퇴직한 직원의 계정을 습득한 뒤, 메일서버 및 업무서버에서 화면 캡처와 문서 다운로드를 통해 고객정보 해킹 |
| 옥션 해킹<br>(2008년 2월) | 고객정보 유출<br>(1,081만 건) | - 이메일을 통해 내부직원 PC에 침투<br>- 서버관리자 PC에 키로거 프로그램 설치, 서버 접근계정 탈취, 이를 통해 고객정보를 유출함. |

도 사회공학적인 기법을 이용하는 APT의 특성이 나타났다. 공격자는 2011년 3월 RSA의 특정 직원들에게 “2011 채용공고”라는 제목의 피싱 메일을 전송하였다. 여기에는 Adobe Flash의 제로 데이 취약점을 이용하는 악성코드가 심어진 엑셀 파일이 포함되어 있었다. 메일 제목에 흥미를 지닌 특정 직원들은 불필요한 업무메일임에도 불구하고 해당 파일을 실행하였으며, 그와 동시에 백도어가 PC에 설치되어 공격자가 원격에서 제어할 수 있게 되었다. 이 사건의 2차 피해로 RSA의 고객사인 군수업체 록히드 마틴(Lockheed Martin)과 L-3 커뮤니케이션즈(L-3 Communications)의 전산망이 해킹 공격을 받았고 이로 인해 2011년 6월 RSA사는 SecureID 4천만 개를 전면 리콜 조치하였다.

#### 2.2.2 국내 사례

국내의 APT 피해사례는 표 2에서 정리된 바와 같다. SK커뮤니케이션즈의 회원정보 3,500만 건이 유출되는 사고가 2011년 7월에 발생했다. 개인정보 유출건수로 가장 큰 규모의 피해가 발생했던 사고이다. 내부의 PC가 공격자의 매개체로 사용되었는데, 공격자는 내부 인력들이 사용하는 비인가 SW를 조사하여, 해당 소프트웨어의 업데이트서버 취약점을 이용함으로써 내부에 진입했다. 공격자는 내부에서도 지속적인 관찰조사를 통해 DB관리자PC와 개발자PC를 장악했다. 이를 통해 개인정보 DB에 접근하여 정보를 수집하고 외부로 유출하였다. 2011년 4월에 발생한 농협해킹사고는 기술적 보안 뿐 아니라 관리적보안도 중요한 과제임을 보여준 사례이다. 농협은 외주직원관리, 서버 작업용 PC(노트북)관리, 서버의 비밀번호 변경관리 등이 미흡했으며, 관리적 허점들이 공격자에게 악용되면서 대국민 금융서비스를 18일 동안 제공할 수 없었다.

공격자는 웹하드 사이트의 업데이트 프로그램으로 위장된 악성코드를 배포하던 중, 농협 시스템 관리자 PC가 감염된 것을 알게 되었고, 7개월간 노트북을 모니터링해서 공격을 감행했다. 이로 인해 내부 서버 550여대의 하드디스크가 손상을 입었으며 재해복구용 서버도 파괴되었다. 최소 80억원 이상의 피해가 발생했다고 알려져 있다. 2013년 3월 20일, 국내 주요방송 3사와 은행 3사의 전산망이 일시에 마비되는 사건이 발생했다.

공격자는 2012년 6월경부터 10개월간 국내 금융사 전산망에 1,560회나 침입하는 등 장기간에 걸쳐 치밀한 준비를 하여 공격을 하였다. APT공격의 특징과 피해사례를 보면, 이는 이전까지의 공격 패러다임과 크게 다르다는 것을 알 수 있다.

APT공격은 자동화된 공격 툴에 의존하지 않고 정형화되지 않으며, APT 공격이 장기간에 걸쳐 진행되며, 대부분 그 피해가 가시화되기 전까지 인지하지 못한다는 것이다. 심지어 피해가 발생한 이후에도 계속 알지 못하는 경우도 있다.

## 3. 사이버 국방 보안을 위한 APT공격 대응방안

### 3.1 사이버 공격 대응방안

#### 3.1.1 제로데이 공격의 대응방안

최근 APT 공격은 제로데이 취약점을 이용하여 그 공격이 더욱 치밀해졌다. 제로데이 공격(Zeroday Attack)

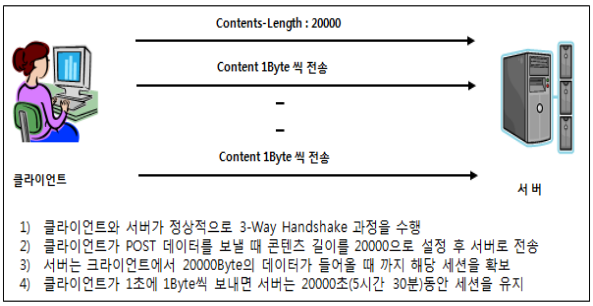
이란 취약점 발견 후 패치 등 가용한 대응수단이 마련되기 전 해당 취약점을 이용하여 행해지는 공격이며, 피해 범위가 클 경우 대응책이 없으므로 운영자 및 사용자들이 혼란상황에 빠질 수 있다. 그러므로 국가적인 차원에서 블랙홀(Black Hole), 싱크홀(Sink Hole) 그리고 통합관제센터 운영과 국가 차원의 강력한 CERT (Computer Emergency Response Team : 컴퓨터 침해 사고 대응반) 운영이 필요하다. 일반적인 블랙홀공격은 라우팅기능에 대한 공격으로, 라우팅 정보값을 추가하거나 변경하여 패킷이 올바르게 전달되지 못하게 할 목적으로 시도된다. 일반적인 형태의 블랙홀 공격은 라우팅정보를 변경하여 모든 전송노드들이 패킷을 블랙홀 노드로 전송하게 하고, 블랙홀 노드는 여러 노드들로부터 수신한 패킷들을 폐기하여 정보전송이더 이상 이루어지지 않게 한다[6].

### 3.1.2 DDos 공격의 대응 방안

디도스 공격은 사이버 공격의 대표적인 해킹방법이고 ISP 및 조직만으로 대응이 어려우므로 차후에는 국가적 차원의 대응체계 마련 및 고도화 할 필요가 있다. 디도스 대응체계의 고도화를 위한 공격 기술 개발로는 PDoS(Permanent DOS), VoIP 단말감염 등 에 대응할 수 있는 기술 개발이 필요하다. 보안 소프트웨어 유지보수효율의 현실화와 보안소프트웨어 산업 활성화를 위해 보안전문인력의 양성의 강화와 특수 전문기관의 활성화가 필요하다.

### 3.1.3 Slow Read DDoS Attack 개념과 대응 방안

슬로우 리드 디도스 공격(Slow Read DDoS Attack)의 개념을 그림 2에서 도식화 하였다. 먼저 클라이언트와 서버가 정상적으로 3-Way Handshake 과정을 거친 후 클라이언트가 POST 데이터를 보낼 때 콘텐츠 길이를 20000으로 설정후 서버로 전송한다. 서버는 크라이언트에서 20000Byte의 데이터가 들어올 때 까지 해당 세션을 확보한다. 클라이언트가 1초에 1Byte씩 보내면 서버는 20000초(5시간 30분)동안 세션을 유지하게 된다. 이때 여러 클라이언트들이 좀비가 되어 공격하면, 좀비 수만큼의 세션이 장시간 유지되고 결국 대상 웹 서버의 모든 세션이 점유 당하고, 신규 서비스 불가 상태가 되면서 장애가 발생하게 된다. 이러한 슬로우 리드 디도스 공격에 대한 대응방안을 정리하면 표 3과 같다.




▶▶ 그림 2. Slow Read DDoS Attack의 개념

### 3.1.4 APT 공격의 대응방안

실질적으로 APT 공격을 방어하기 위해서는 단일 솔루션이나 자동화된 툴에 의존하지 않아야 하며, 정보와 사람 중심의 대응전략이 마련되어야 한다. 가장먼저 보호대상을 명백히 하고, 접근통제와 보안관제를 강화하며 서버보안과 내부인력 및 정보 사용자에 대하여 보안관리가 주기적으로 이루어지도록 하고 APT 대응을 위한 전담 조직 팀이 구성되어 전략적으로 대응을 하여야 한다.

표 3. Slow Read DDoS Attack 대응방안

| 대응방안 | 설명 |
|---|---|
| 데이터 크기의 하한 설정 | 비정상적으로 작은 데이터의 접속을 거부 한다. |
| 요청 시간 제한 | 개인이 요청할 수 있는 시간을 제한하도록 설정한다. |
| POST 폼 메시지 크기의 제한 | POST 폼에 메시지 크기를 제한한다. |
| TCP 상태의 모니터링 | 상시 모니터링을 통해 회선설립(Established) 및 대기시간(Time Wait) 값이 많은지를 확인한다. |
| 최저 전송속도의 제한 | 공격자의 임계치 조작 및 접속자 속도의 다양성, HTTP 등에 의한 속도저하 등 다양한 변수로 실제 적용에 어려움을 감안하여 설정한다. |

일반적으로 APT 공격은 악성코드를 통해 내부망 PC를 감염 시켜서 1차 침입에 성공한 후 지속적으로 해킹 전략에 의해 공격하므로 기존의 백신 프로그램으로는 바이러스 감염된 PC를 보호하지 못한다. 왜냐하면 기존 백신 프로그램들은 블랙리스트방식의 시그니처 기반 진단 기능을 제공하므로 새로운 공격에 대한 백신프로그램이 개발되기까지 공백기간의 취약점을 이용한 제로데이 공격을 이용하기 때문이다. 그러므로 화이트리스트 방식으로 신규 파일 및 데이터에 대하여 실시간으로 파일을 탐지, 분석, 차단, 접근허용 등이 이루어질 수 있는 탐지기법이 종단 시스템에 설치되도록 하여 좀비 PC가 되지 않도록 앤드포인트(End-point)의 보안강화가 더욱 강조된다[7]. 이러한 APT 공격의 대응방안을 표 4에 정리하였다.

표 4. APT 공격의 대응방안

| 구분 | 대응방안 | 설명 |
|---|---|---|
| 관리적 | CERT 공조 | 조직적 공격을 예방하고 대응하기 위한 국가간 CERT 공조 |
| | 보안 거버넌스 | 인력, 조직, 정책, 예산 등 전사적 보안 대응 체계 마련 |
| 기술적 | 침투 테스트 (Penetration Test) | 보안지침, 매뉴얼 기반의 주기적 모의 훈련 및 침투 Test 수행 |
| | 실시간 보안 관제 | UTM 체계를 통한 실시간 보안 모니터링 및 대응 |
| | 백업 체계 구축 | 피해를 최소화하기 위한 계층적 백업 체계 구축 |
| | 백신 등 단말 보안 | Client 및 서버 악성코드 제거 |
| | 접근 통제 | 관리자 권한 최소화, 계정 관리, 중앙 접근 관리 |
| 물리적 | 작업 공간분리 | 작업에 따른 공간, 네트워크를 외부와 분리 |

## 4. 결론

인터넷과 통신 기술이 발달하면서 우리 국방은 사이버 공격에 대한 방어체계가 더욱 강조되는 시점이다. 2004년 이후 북한의 소행으로 드러난 사이버 공격 사례가 무려 5만 건에 이르고 최근 2009년, 2011년 대표적인 디도스(DDoS) 공격과 그 피해로 인한 자산의 손실, 악성 거짓정보로 우리 국민을 혼란시키는 사이버 범죄의 피해가 급증하고 있다. 이러한 피해사례를 기반으로 분석한 결과 최근의 사이버 공격은 APT(지능형 지속 위협)에 의한 공격방식으로 진화되고 있다. 이에 본 연구에서는 장기간에 걸쳐 진행되고, 대부분 그 피해가 가시화되기 전까지 인지하지 못하고  심지어 피해가 발생한 이후에도 계속 알지 못하는 경우도 있는 APT 공격의 국내와 해외 사례를 정리하였으며, APT 공격에 이용되는 제로데이 취약점 공격, 디도스(DDoS) 공격, 느린 진행속도와 작은 임계치의 은밀한 행위로 이루어지는 슬로우 리드 디도스 공격 등에 대한 대응책을 제시하였다. 이러한 보안 대응책을 기반으로 사이버 국방보안에 대한 노력에 도움이 되고자 한다.

## 참고문헌

[1] 안유성, 사이버공격에 대비한 국방체계 발전방안 연구, 정보보호학회지 제 23권 제 2호, 2013. 04.
[2] 장영준, APT 공격의 현재와 미래 그리고 대응 방안 P9-10, 2012
[3] Strategies for Dealing With Advanced Targeted Threats, GARTNER Aug. 2011.
[4] http://isis.kisa.or.kr/ 2011. 2012, 2013.
[5] Blue Coat Labs Report: Advanced Persistent Threats, BlueCoat, BlueCoat, 2011.
[6] 김영동, “블랙홀 공격이 있는 MANET에서 패킷 취합에 따른 음성 트래픽 전송 성능”, 한국전자통신학회 춘계학술지 제6권 제1호, 2012.6, 368-371 (4 pages)
[7] 박세균, “Endpoint Level의 효과적인 APT공격 대응방안 연구” 2013년 한국정보과학회, 한국정보과학회 학술발표논문집 , 2013.6, 732-734 (3 pages)
[8] 이문구, 배춘석, “APT 공격의 주요사례에 대한 연구“ 대한전자공학회, 2013 추계학술대회논문, CFP-026.

## 저자소개

● 이 문 구 (Moon-Goo Lee)

▪ 1984년 2월 숭실대학교 전자계산학과 (공학사)
▪ 1993년 8월 이화여자대 대학원 전산교육학과 (석사)
▪ 2000년 2월 숭실대학교 대학원 컴퓨터과 (공학박사)
▪ 2000년 3월~현재 김포대학 모바일환경공학부 인터넷정보과 정교수
<관심분야> : 인터넷 보안, 암호화 알고리즘, 전자상거래 보안, 멀티미디어 콘텐츠 보안