情 報 保 護 學 會 誌
第18卷 第1號, 2008. 2

제로-데이 웜 공격 대응을 위한 ZASMIN 시스템 구조

오 진 태*, 김 익 균*, 장 종 수*, 전 용 희**

요 약

현재의 정보보호시스템은 시그니처가 알려지지 않은 공격에 대하여 효과적인 대응 기법을 제공하지 못하고 있다. 그러나 앞으로 알려지지 않은 취약성을 이용하는 제로-데이 웜이 실제적으로 큰 위협이 될 전망이다. 그러므로 비록 알려지지 않은 공격에 대하여도 탐지하고 차단할 수 있는 능력을 가진 시스템이 요구된다. 본 논문에서는 제로-데이 웜 공격에 대응할 수 있는 ZASMIN 시스템의 구조를 제안하고, 주요 기능 및 요구사항, 시그니처 분배 프레임워크에 대하여 기술하고자 한다.

Ⅰ. 서 론

현재의 침입탐지시스템(IDS: Intrusion Detection System)이나 침입방지시스템(IPS: Intrusion Prevention System)은 시그니처가 알려지지 않은 공격에 대하여 효과적으로 방어할 수 있는 수단을 제공하지 못하고 있다. 이로 인하여 고속으로 전파되는 슈퍼 웜 형태의 공격이 발생하는 경우, 그 피해가 크게 확산 될 수 있다. 따라서 비록 알려지지 않은 공격이라도 이를 탐지하고 차단할 수 있는 시그니처를 실시간으로 생성하여 해당 공격에 의한 피해를 최소화할 수 있는 시스템이 요구된다. 이를 위하여 본 논문에서는 제로-데이 웜 공격에 대응할 수 있는 ZASMIN(Zero-day Attack Signature Manufacture INfrastructure) 시스템의 구조, 주요 기능 및 요구사항에 대하여 제시하고자 한다[1,2].

제로-데이 공격에 대한 하나의 정의는 "보안 취약성이 일반적으로 알려진 바로 그날에 보안 취약성을 이용하는 것"이다[3]. 또 다른 정의에 의하면 "패치나 다른 구제책이 컴퓨터에 설치되기 전에 행해지는 공격"이다. 이 정의는 방어 수단이 있기 전에 공격이 먼저 발생한다는 것이 정의의 핵심임을 나타내고 있다. 따라서 제로-데이 공격은 알려지지 않은 공격으로 볼 수 있다. 이런 알려지지 않은 공격은 해당 공격의 특징이 알려지지 않았거나, 알려지지 않은 취약점을 이용하여 시도하는 공격이다. 즉 일반적인 침입 탐지나 차단 시스템에서 해당 공격을 탐지할 수 있는 시그니처를 보유하지 않은 공격을 의미한다.

이러한 알려지지 않은 공격으로부터 네트워크 인프라를 보호하기 위하여, 네트워크 공격을 조기에 탐지하고 공격 패킷들만이 가지는 시그니처를 공격 초기에 생성하여 공격에 대응할 수 있는 하드웨어 기반의 실시간 시그니처 생성 및 관리 시스템의 개발이 필요하다. 본 논문에서 제안하는 ZASMIN 시스템은 알려지지 않은 네트워크 공격을 조기에 탐지하여 해당 공격에 속하는 공격 패킷들만이 가지는 시그니처를 생성하며, 이렇게 추출되는 시그니처는 Snort과 유사한 Semantic을 만족시키는 형태의 시그니처이다.

본 논문의 구성은 다음과 같다. 2장에서는 ZASMIN 시스템의 구조를 제안하고 서브시스템 구조에 대하여 기술한다. 3장에서는 시스템의 주요 기능 요구사항에 대하여 기술한다. 4장에서는 시스템의 동작 시나리오에 대하여 기술하고, 5장에서는 시그니처 분배 프레임워크를 제시하고, 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 구조

2.1. 시스템 구조

* 한국전자통신연구원 정보보호연구단 보안응용그룹(showme@etri.re.kr, ikkm21@etri.re.kr, jsjang@etri.re.kr)
** 대구가톨릭대학교 컴퓨터정보통신공학부(yhjeon@cu.ac.kr)(교신저자)

본 시스템은 크게 다음과 같이 3개의 서브시스템으로 구성된다.

· 시그니처 추출 서브시스템(SES: Signature Extraction Sub-system): 시그니처 추출 기능 수행

· 시그니처 검증 서브시스템(SVS: Signature Validation Sub-system): 추출된 시그니처 검증 기능 수행

· 시그니처 관리 서브시스템(SMS: Signature Management Sub-system): 생성된 시그니처 관리 분배 기능 수행

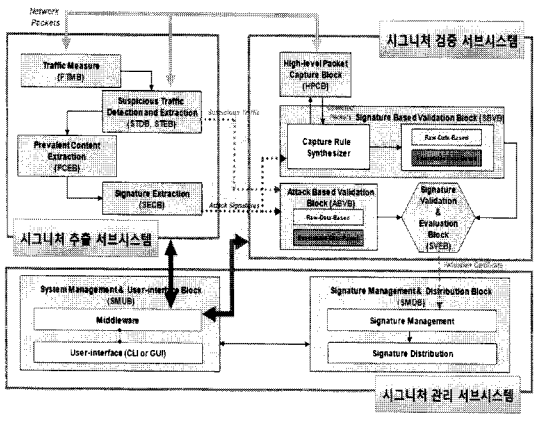
SES는 공격 패킷으로 예상되는 네트워크상의 패킷으로부터 해당 네트워크 패킷들을 차단할 수 있는 시그니처를 추출한다. SVS는 시그니처를 추출하는데 사용되거나 관련된 네트워크 패킷들과 추출된 시그니처를 이용하여 해당 시그니처의 정당성 및 신뢰성을 검증한다. SMS는 생성된 시그니처를 관리하고 원격 시스템으로 분배하여 적용한다. [그림 1]은 시스템 블록구조를 보여준다.

본 시스템은 네트워크상의 에지에서 시그니처 추출 및 검증 기능을 수행하며, 기가-비트 인터페이스를 포함하며 별도의 관리 네트워크 인터페이스를 포함한다.

2.2. 서브시스템 구조

2.2.1. 시그니처 추출 서브시스템(SES)

SES 시스템의 블록들은 다음과 같이 구성되며 기능을 간략하게 기술한다.



〔그림 1〕 ZASMIN 시스템 블록 구조

· FTMB(Flow-based Traffic Measuring Block): 네트워크에 유입되는 트래픽을 모니터하여 비정상 트래픽 분석에 사용될 기초 정보를 생성한다.

이 블록에 의하여 분석된 정보는 트래픽 용량별 정보, 세션 관련 정보, 목적지 주소별 정보 등을 포함한다. 분석되는 흐름(flow)단위로는 최소 단위 흐름(Primitive Flow) 및 집합 흐름(Aggregation Flow)이 사용된다. 기가 망을 통과하는 네트워크 트래픽을 모니터링하여 플로우 기반으로 Address Dispersion, 세션 성공률, Stealth Scan Count 등의 정보를 하드웨어 기반으로 측정하여 전달한다. 이 정보를 바탕으로 의심스러운 트래픽에 대한 결정을 하여 추출할 패킷 정보를 알려주게 된다.

· STDB(Suspicious Traffic Decision Block): FTMB에서 생성된 트래픽 정보를 분석하여 비정상 트래픽을 탐지하는 기능을 수행한다. 공격 트래픽 탐지를 위해서 관리되는 각 트래픽 정보에 대하여 프로토콜, 포트 기반, 각 프로토콜, 포트 별 트래픽 정보 기반으로 공격 소스를 산출하고 이를 기반으로 공격 여부를 판단한다.

· STEB(Suspicious Traffic Extraction Block): STDB로부터 의심스러운 트래픽 추출에 대한 정책을 전달받아 내부 알고리즘에 적용하고, 이를 토대로 전체 유입 패킷에서 의심스러운 트래픽만을 추출하는 기능을 수행한다. 비정상 트래픽 추출 기능은 3-tuple(프로토콜, 소스 IP, 목적지 IP)을 기반으로 수행되며, 추출된 트래픽은 플로우 별로 저장 및 관리하고 이를 시그니처 검증 서브시스템(SVS)으로부터의 요구에 따라 전달하는 기능을 수행한다.

· PCEB(Prevalent Content Extraction Block): STEB로부터 전달받은 패킷의 페이로드 정보를 분석하여 페이로드의 유형과 특성을 관리하고, 내부 알고리즘 및 정책을 통하여 이상 분포를 가지는 페이로드 스트링을 탐지한다. 이는 해쉬 기반의 단순 매칭으로 수행되며, 전체 페이로드에 대한 분석은 일정 크기의 서브 스트링 단위로 이루어진다. 또한 이상 분포의 페이로드 스트링에 대한 빈도를 관리하고, 내부 알고리즘 및 정책을 통하여 시그니처 생성에 필요한 페이로드 스트링을 정확히 탐지한다.

· SECB(Signature Extraction Control Block): PCEB로부터 생성된 분자열들을 분석 · 조합 · 정제하고 이를 표준 시그니처 형태로 변환하여 시그니처 검증 서브시스템으로 전달한다.

2.2.2. 시그니처 검증 서브시스템(SVS)

SVS 시스템의 블록들은 다음과 같이 구성되며 기능을 간략하게 기술한다.

· HPCB(High-level Packet Capture Block): SBVB에 의하여 생성된 패킷 수집 규칙을 수신하여 해당 규칙을 이용하여 네트워크로부터 패킷들을 수집하고, 수집된 패킷을 SBVB로 전달하여 시그니처를 검증한다.

· SBVB(Signature-Based Validation Block): SES로부터 수신한 시그니처를 수정·보완하여 패킷 수집규칙을 재생성하고 이를 HPCB로 전달하며 공격 여부를 판단한다.

· ABVB(Attack-Based Validation Block): SES로부터 수신한 네트워크 패킷들과 시그니처를 이용하여 해당 패킷들이 공격인지 여부를 판단한다. 이를 위하여 패킷 내의 콘텐츠를 이용하여 검증하는 패킷 콘텐츠 분석 기능과 이진 데이터 분석 기능을 가진다.

· SVEB(Signature Validation Evaluator Block): ABVB와 SBVB에서 수행한 검증 결과를 토대로 각 검증 방법에 가중치를 부여하여 해당 검증 결과를 산출하며, 산출된 검증 결과를 인증서 형태로 구성하여 시그니처 관리 서브시스템으로 전달한다.

2.2.3. 시그니처 관리 서브시스템(SMS)

SMS 시스템의 블록들은 다음과 같이 구성되며 기능을 간략하게 기술한다.

· SMUB(System Management & User-Interface Block): 각 블록들의 상태를 관리하고, CLI(Command Line Interface) 혹은 GUI(Graphic User Interface)를 통하여 전체 시스템을 제어하고 모니터링 한다.

· SMDB(Signature Management & Distribution Block): SVEB로부터 시그니처에 관련된 정보를 받아서 원격 시스템에 적합한 형태로 시그니처를 가공하며, ZASMIN 시스템에서 최종적으로 생성된 시그니처를 원격 시스템으로 전달하기 위한 분배 프로토콜을 제공한다.

Ⅲ. 기능 요구사항

3.1. 시그니처 추출 서브시스템(SES)

SES 시스템의 주요 기능은 다음 세 가지와 같다.

· 비정상 트래픽 추출 기능: 네트워크 트래픽을 분석하여 비정상 트래픽 및 그 특성을 모니터링 하는 기능을 제공한다. 탐지된 비정상 트래픽의 특성에 따라서, prevalent content 추출에 사용되는 트래픽의 양을 조절하는 기능을 제공한다. 시그니처 생성에 사용된 최종 패킷이 속하는 세션의 네트워크 패킷 정보들을 시그니처 검증 서브시스템(SVS)에 전달한다.

· Prevalent Content 추출 기능: 탐지된 비정상 트래픽에 대하여 해당 패킷이 가지는 바이트 분포를 실시간으로 분석하는 기능을 제공한다. 입력 패킷으로부터 일정 크기의 문자열(substring)들을 추출하고, 추출된 문자열의 분포 분석을 통하여 비정상적인 분포를 보이는 문자열들을 추출하는 기능을 가진다. 비정상 트래픽으로 분류되어 입력된 패킷들의 페이로드를 바이트 단위로 이동하면서 일정 크기의 문자열 단위로 해쉬값을 구하고, 이를 바탕으로 단위 문자열들에 대한 시간별 빈도 분포를 관리한다.

· 시그니처 생성 기능: 추출된 비정상 문자열을 조합하여 공격 시그니처를 추출하는 기능을 제공한다. 추출된 시그니처를 분석하여 일반적으로 네트워크에 많이 사용되는 비공격 문자열들만으로 구성된 시그니처를 제거하는 기능을 제공한다. 최종적으로 생성된 시그니처는 Snort과 유사한 형태를 가지며 시그니처 생성에 사용된 최종 패킷과 함께 시그니처 검증 서브시스템(SVS)에 전달하게 된다.

3.2. 시그니처 검증 서브시스템(SVS)

SVS의 주요 기능 요구사항은 아래와 같이 분류된다.

· 일반 기능: SVS는 시그니처 생성 서브시스템에서 생성한 공격 시그니처에 대한 검증 기능을 수행하며, 시그니처 생성 간 사용된 네트워크 패킷 또는 해당 패킷과 관련된 패킷을 이용한 검증과정을 수행한다. 또한 생성된 시그니처를 기반으로 수집된 네트워크 패킷에 대한 공격 패킷 여부 검증 과정을 수행한다. SVS는 수집된 네트워크 패킷이 공격 패킷일지를 판단할 때, 시그니처 생성 간 활용된 네트워크 패킷을 이용한 검증결과와 생성된 시그니처를 기반으로 수집된 네트워크 패킷을 이용한 검증 결과를 통합 분석하여 해당 시그니처의 신뢰도를 추출한다. 시그니처 검증 결과에 따른 신뢰도를 표현하는 인증서(Certificate)를 작성 배포하는 기능을 제공한다.

· 공격 검증 기능: SVS는 시그니처 추출에 활용되거나 시그니처 추출에 활용된 패킷과 동일 세션에 포함되는 네트워크 패킷을 이용하여 해당 패킷이 공격 패킷인지를 검증하는 기능을 제공한다. 해당 패킷이 공격 패킷인지를 검증하는 과정에서 해당 패킷의 다양한 특징을 이용하여 해당 네트워크 패킷이 공격 패킷인지 여부를 판단하는 기능을 제공한다.

· 시그니처 검증 기능: SVS는 추출된 시그니처를 기반으로 수집한 네트워크 패킷을 이용하여 해당 패킷이 공격 패킷인지를 검증하는 기능을 제공한다. 수집된 네트워크 패킷이 공격 패킷인지를 검증하는 과정에서 해당 패킷의 다양한 특징을 이용하여 해당 네트워크 패킷이 공격 패킷인지 여부를 판단하는 기능을 가지고 있다. 또한 시그니처를 기반으로 작성된 수집 필터링(Capture Filtering) 규칙을 기반으로 네트워크 패킷에 전달되는 모든 트래픽에 대해 이 규칙을 적용하여 해당 규칙에 적용되는 네트워크 패킷을 수집하는 기능을 가진다.

· 검증결과 평가 기능: 공격 및 시그니처 검증 기능을 통해 수행된 검증 결과를 수집하여 해당 시그니처에 대한 통합적인 검증 결과를 도출하는 기능을 제공하며, 검증 결과를 확인할 수 있는 검증 결과를 포함하는 인증서를 생성한다.

3.3. 시그니처 관리 서브시스템(SMS)

· 일반 기능: SMS 서브시스템은 ZASMIN 시스템에서 생성된 시그니처의 관리 및 전달에 관한 기능을 제공하며, 사용자 정합을 위한 기능을 제공한다.

· 관리 기능: 각 서브시스템의 블록 별 상태를 관리하는 기능을 가지며, 사용자 인터페이스로서 CLI (Command Line Interface) 또는 GUI(Graphic User Interface)를 제공한다.

· 시그니처 분배 기능: ZASMIN 시스템에서 최종적으로 생성된 시그니처를 원격 시스템으로 전달하기 위한 분배 프로토콜을 제공한다.

Ⅳ. 시스템 동작

본 장에서는 ZASMIN 시스템을 통하여 구현 및 제공되는 서비스의 동작을 나타낸다.

· SES는 네트워크상에서 송수신되는 네트워크 패킷을 지속적으로 수집한다.

· 수집된 네트워크 패킷을 ZASMIN의 분석 기능을 통하여 공격으로 의심되는 패킷을 탐지한다.

· 해당 공격에 공통적으로 출현하는 정보를 이용하여 해당 패킷을 탐지 · 차단 할 수 있는 시그니처를 생성한다.

· 생성된 시그니처와 해당 시그니처를 생성하는데 활용된 네트워크 패킷 및 그와 관련된 네트워크 패킷 및 기타 상태 정보들이 SMS로 전달된다.

· SMS는 수신된 상태정보를 이용하여 ZASMIN 시스템의 상태를 표현한다.

· SMS는 수신된 네트워크 패킷과 시그니처를 SVS로 전달한다.

· SVS는 수신된 네트워크 패킷을 이용하여 공격 여부 판단을 위한 검증을 수행한다.

· SVS는 SES로부터 수신한 시그니처를 기반으로 패킷 수집 규칙을 작성하고 이를 기반으로 네트워크 패킷을 수집한다.

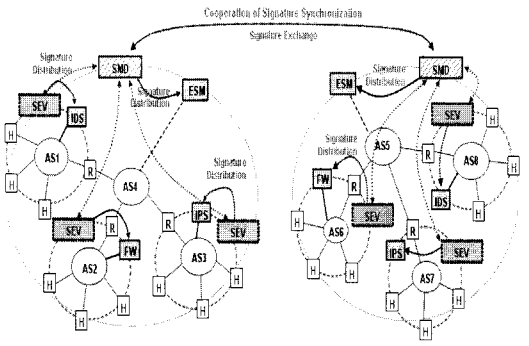
· SVS는 수집된 네트워크 패킷들을 이용하여 해당 네트워크 패킷들이 공격인지를 판단하는 검증과정을 수행한다.

· SVS는 전달받은 검증 결과들을 종합하여 해당 시그니처의 최종 신뢰도를 추출하고, 이를 인증서 형태로 구성한다.

· SVS는 구성된 인증서를 SMS로 전달한다. 인증서를 전달받은 SMS는 해당 인증서를 분배한다.

배포된 시그니처는 해당 보안장비를 운영하는 관리자에 의해 적용되어 발생중인 공격을 신속하게 차단하게 된다.

Ⅴ. 시그너처 분배 기술



[그림 2] 시그너처 분배 프레임워크

[그림 2]는 위험정보 공유를 위한 시그니처 분배 프레임워크를 보여준다.

이 그림은 새로 발생되는 취약성 및 사이버 공격 정보 등을 안전하게 상호 공유하기 위한 프레임워크로서, 위험 정보 공유 프레임워크에 관한 요구사항과 기능 규격을 정의하고 기술한다. 제안된 '보안 정보 공유 프레임워크'는 시스템의 취약점, 공격, 악의적인 행위 정보 등에 관한 '위험 정보 공유 기술'로 향후 기술 상용화시 상호 호환성을 보장하기 위한 프레임워크로 현재 사이버보안 정보공유를 위한 보안 분야에서 논의되기 시작한 최신기술로 판단된다.

Ⅵ. 결 론

본 논문에서는 현재 정보통신 환경에서 발생하고 있는 제로-데이 웜 공격에 대응하기 위하여 탐지 시그니처를 자동으로 생성 및 분배하는 기능을 수행하는 고성능 자동 시그니처 생성 시스템인 ZASMIN의 설계 및 구현을 위한 시스템 구조와 기능, 시그니처 분배 프레임워크에 대하여 기술하였다. 특히 본 논문에서는 ZASMIN 시스템 구현에 필요한 설계 이념에 대하여 제시하고자 하였다. 본 논문에서 제시한 시그니처 분배 기술은 2007년 9월에 ITU-T에 제안되어 국제 표준 과제로 채택된바 있다. 현재 ITU-T에서는 위험 정보 공유 기술의 표준을 추진하기 위해 보안 관련 정보와 업데이트를 위한 벤더 중립의 프레임워크에 관한 초안이 작성되고 있다. ITU-T SG17 산하 Cybersecurity 그룹(Q.6/17)에서 관련 국제표준 개발 작업이 추진되고 있으며, 한국, 일본 등이 참여하여 관련 국제표준 개발 작업을 주도하고 있다. 제안된 보안 정보 공유 기술은 국내 최초로 위험 정보 공유 기술 분야에서 국제표준과제로 채택되었으며. 향후 국제 표준으로 채택될 전망이다.

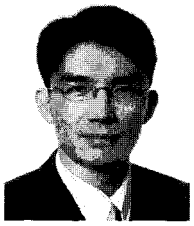
참고문헌

[1] 한국전자통신연구원 정보보호연구단, *ZASMIN 시스템 요구사항 정의서(V 1.0)*, 15면, Sep. 2006.

[2] 한국전자통신연구원 정보보호연구단, *고성능 자동 Signature 생성 시스템 설계서(V 1.1)*, 22면, Oct. 2006.

[3] Bryce Porter, Approaching Zero: A Study in Zero-Day Exploits- Origins, Cases, and Trends, 28pages, Norwich University, 2005.

〈著者紹介〉

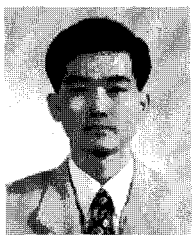


오 진 태(Jintae Oh)

1990. 2 : 경북대학교 전자공학과 공학사
1992. 2 : 경북대학교 전자공학과 석사
1992. 2 ~ 1998. 2 : 한국전자통신연구원 선임연구원
1998. 3 ~ 1999. 1 : 미국 MinMax Tech. 연구원
1999. 2 ~ 2001.10 : 미국 Engedi Networks. Director
2001. 10 ~ 2003. 1 : 미국 Winnow Tech. Co-founder, CTO 부사장
2003. 3 ~ 현재 : 한국전자통신연구원 선임연구원, 보안게이트웨이 연구팀 팀장
관심분야 : 네트워크보안, 비정상 행위탐지기술, 공격 시그니처 자동생성기술, 보안하드웨어기술

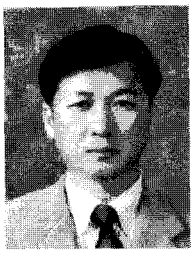
김 익 균(Ikkyun Kim)

1994년 : 경북대학교 컴퓨터공학과 공학사 .
1996년 : 경북대학교 컴퓨터공학과 석사
1996년 ~ 1999년 : 한국전자통신연구원
2000년 ~ 2001년 : (주) 팍스콤 선임연구원
2004년 ~ 2005년 : 미국 Purdue University 객원연구원
2001년 ~ 현재 : 한국 전자통신연구원 선임연구원
관심분야 : 네트워크보안, 컴퓨터 네트워크



장 종 수(Jong-Soo Jang)

1984년 : 경북대학교 전자공학과 학사,
1986년 : 경북대학교 대학원 전자공학과 석사,
2000년 : 충북대학교 대학원 컴퓨터공학과 박사,
1989년 7월 ~ 현재 : 한국전자통신연구원 정보보호연구단 보안응용그룹 그룹장/책임연구원
관심분야 : Network Security, 정책기반보안관리, 비정상트래픽탐지, 유해정보차단



전 용 희 (Yong-Hee Jeon)

1971. 3 ~ 1978. 2 : 고려대학교 전기전자전파공학부
1985. 8 ~ 1987. 8 : 미국 플로리다공대 대학원 컴퓨터공학과
1987. 8 ~ 1992. 12 : 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 석사, 박사
1978. 1 ~ 1978. 11 : 삼성중공업(주)
1978. 11 ~ 1985. 7 : 한국전력기술(주)
1979. 6 ~ 1980. 6 : 벨기에 벨가톰사 연수
1989. 1 ~ 1989. 6 : 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989. 7 ~ 1992. 9 : 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA
1992. 10 ~ 1994. 2 : 한국전자통신연구원 광대역통신망연구부 선임연구원
1994. 3 ~ 현재 : 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2001. 3 ~ 2003. 2 : 대구가톨릭대학교 공과대학장 역임
2004. 2 ~ 2005. 2 : 한국전자통신연구원 정보보호연구단 초빙연구원
2007. 1 ~ 2007. 12 : 한국정보보호학회 학회지 편집위원장
2008. 1 ~ 현재 : 한국정보보호학회 부회장
관심분야 : 네트워크 보안, 웜 모델링 및 대응 기술, 통신망 성능분석