Zero-day 공격 대응을 위한 네트워크 보안의 지능화 기술

정일안 | 김익균 | 오진태 | 장종수
한국전자통신연구원

요 약

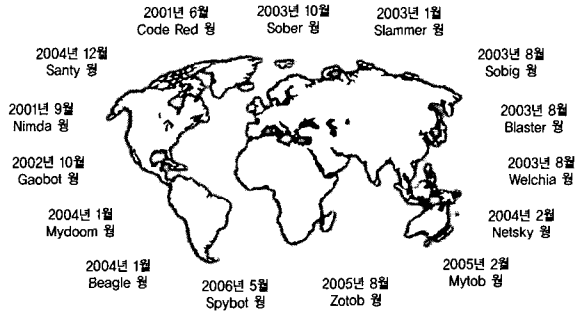
최근 네트워크 공격 기술이 날로 발전함에 따라 각 시스템에서 노출된 취약성이 패치되기 전에 네트워크 환경을 위협하는 zero-day 공격이 최대 이슈로 등장하고 있다. 본 고에서는 zero-day 위협에 대응하기 위해서, 활발하게 진행되고 있는 탐지 시그니처 자동 생성 기술에 대한 최근 연구 동향에 대해 소개하고, 이러한 기존 연구 및 기술들의 단점을 보완하기 위해 개발되고 있는 하드웨어 기반 고성능, 시그니처 자동 생성 시스템을 포괄하는 네트워크 보안 지능화 기술을 소개한다. 그리고 생성된 탐지 시그니처를 타 보안 솔루션들과 공유하기 위한 운영 프레임워크를 제안하고, 생성된 시그니처를 공유하기 위해 사용하는 시그니처 생성 교환 프로토콜과 메시지 교환 형식을 정의한다. 이러한 지능화 대응 기술을 활용함으로써 zero-day 공격에 대해 초기에 탐지하고 신속하게 대응하여 네트워크 인프라를 보호하는 효과를 기대할 수 있다. 또한, 체계적인 보안 정책 관리를 통하여 향후 발생할 네트워크 위협 공격들에 대해서도 빠르게 대응할 수 있도록 하여 국가적인 차원에서의 효과적인 방어 체계를 구축하는데 기여할 것이다.

1. 서 론

통신 및 네트워크 기술의 발달과 함께 스팸(spam), 바이러스(virus), 서비스 거부 공격(Denial of Service), 웜(worm) 등 네트워크를 통한 사이버 공격은 다양한 기법이 사용되고 있고, 전파속도가 단축되면서 더욱 치명적인 형태로 진화하고 있다.

2003년에 발생한 1.25 대란으로 잘 알려진 Slammer 웜의 경우, 발생 10분 내에 전 세계 90%의 취약성을 가진 호스트를 감염시켰으며, 발생 후 5일간의 생산성 피해가 10억 달러에 이르는 것으로 추정하고 있다. 2001년 기준 Nimda와 Code-Red의 경우, 각각 6억 3천만 달러와 26억 달러, Blaster의 경우는 약 20억 달러의 경제적 손실을 초래한 것으로 추정하고 있고, 국내의 경우에는 높은 PC 보급률과 함께 세계적인 수준의 인터넷 인프라를 구축하고 있어 공격에 대한 피해 역시 전체의 10% 이상을 차지하고 있다.

최근의 네트워크 환경을 위협하는 공격들은 메신저, e-mail 등을 이용하는 것과 같이 형태가 매우 다양해지고 있으며, (그림 1)과 같이 Blaster, Welchia, Sasser 등과 같은 신종 웜의 출현이 계속적으로 보고되고 있다[1].



(그림 1) 전 세계 네트워크 보안사고 현황

Symantec 보고에 의하면, 2006년 상반기 Win32 계열의 웜/바이러스 악성 변종이 8,258개가 되고, 상위 50위 악성코드들 중에서 웜 은 52%, 봇(bot)은 14%를 차지하며, 사용자의 중요한 개인 정보를 유출할 목적으로 제작되어 퍼지고 있다. 또한, Code-Red 웜의 경우와 같이, 과거에는 한 두 차례에 지나지 않았던 변종 웜이 출현하기도 하고(Code-Red II), Bagle, MyTob, Sober 같은 웜들은 다양한 형태로 지속적으로 출현하고 있으며, 점차 MS의 WMF, 오피스 취약점, J2ME, 모바일 디바이스용 악성코드도 출현하고 있는 추세이다[2].

현재 이러한 공격들에 대한 침입 탐지 및 방지 시스템(IDS/IPS)에서 사용하고 있는 비정상 트래픽 탐지를 이용하는 방법은 공격에 사용되는 특성에 관계없이 공격이 유발하는 트래픽의 특성을 분석하여 탐지하는 방식이다. 이 방법은 전반적인 네트워크 공격에 광범위하게 적용 가능하지만, 오탐율이 높은 편이여서 현재 대부분의 상용 제품에서는 비정상행위 탐지 기능을 비활성화하거나 제한적인 상황에서만 활용하고 있는 수준이다. 한편, 알려진 공격이 가지는 고유패턴을 탐지하는 방법은 현재 대부분의 통합형 방화벽과 침입 탐지 및 방지 시스템에서 널리 사용되며, 네트워크상의 패킷을 공격 패킷으로부터 추출한 시그니처와 비교하여 탐지함으로써, 신속하고 정확하게 공격을 탐지하거나 차단할 수 있다. 그러나 탐지에 사용되는 패턴(signature)의 생성이 수작업으로 이루어지고 있는 실정이다. 이러한 공격 시그니처의 생성 지연으로 인하여 변종 웜과 알려지지 않은 공격에 대응하기 위한 효과적인 방어 체계가 수립되어 있지 않다. 즉, 취약성을 공격하는 Exploit 코드 발생 시간에 비해 해당 취약성 공격에 대한 탐지 시그니처 배포 및 적용 시간이 길어짐으로 인해 zero-day 공격 위협에 노출될 가능성이 점점 높아지고 있다.

IDC 보고에 의하면 세계 보안 시장에서 방화벽 관련 시장은 2007년까지 소폭 성장을 보이다가 이후 감소할 것으로 예상되나, 네트워크 기반 IDS/IPS 시장은 연평균 30%대의 커다란 성장을 보이며 2008년 8억 달러 시장규모를 생성할 것으로 보이고 있다. 특히, 단일 플랫폼에서 방화벽, 바이러스 탐지/차단, IDS/IPS 기능 등을 제공하는 Unified Threats Management (UTM) 분야가 기존의 방화벽과 같은 단일 보안제품을 빠르게 대처해 나가면서 2006년 8억에서 2008년 20억 달러의 시장을 형성할 것으로 보인다. 국내 보안 시장의 경우에도 세계 시장과 비슷한 경향을 보일 것으로 보이나, IDS/IPS분야가 2009년 까지 완만한 성장세를 보이며, UTM의 규모가 2008년 42%로 늘어날 전망이다. 그러나, 기존의 IDS/IPS뿐만 아니라 UTM에서도 알려지지 않은 공격을 탐지하고 대응하기 위해 비정상행위 탐지 기능을 사용하였으나, 비정상행위 탐지의 오탐(false alarm)으로 인하여 대부분 기능을 비활성화 하여 사용하고 있는 실정이다. 네트워크 공격 시그니처 자동 생성 기술 시장은 기존 보안 제품뿐만 아니라, 차세대 핵심제품인 UTM관련 제품의 핵심기술로 대두될 것이다. 시그니처 생성 및 자동 검증 기술이 적용된 정보보호 제품의 점유율은 2007년 10%에서 2009년 이후에는 70% 이상일 것으로 예상되고, 이 기술의 부가가치는 전체 정보보호 장비의 10%정도를 차지할 것으로 전망된다[3,4].

기존 보안 기술들의 한계와 국내외 차세대 보안 대응 기술에 대한 보안시장의 요구와 함께 지속적으로 출현하는 변종 또는 다형성 (polymorphic) 웜, 알려지지 않은 공격(unknown attack) 등의 보안패치나 시그니처가 패치되기 전에 발생하는 공격(zero-day attack)에 대하여 실시간으로 대응하기 위한 기술들의 개발이 진행되고 있다. 세계적으로 네트워크 환경에서의 공격 시그니처 자동생성 기술은 초기 단계의 연구 주제로서, 최근 미국을 중심으로 시그니처 추출에 국한된 연구가 활발히 진행되고 있다. 특히, 미국의 과학재단, 국토안전국, 국방부 등과 같은 정부 관련 기관의 지속적인 지원 속에서 CMU (Carnegie Mellon Univ.), UCSD(Univ. California at San Diego), UC-Davis, Penn State Univ. 등의 대학에서 시그니처 추출에 관한 연구가 진행 중이다. 산업체에서는 Intel이 CMU와 공동연구를 진행 중이며 Cisco는 UCSD로부터 관련기술을 매입하였다. 국내에서는 KISA에서 CMU와의 공동연구를 통해 시그니처 추출과 관련된 유사한 연구를 수행하고 있다.

이러한 공격들의 특징을 자동으로 추출하는 기술에 의해 생성된 시그니처들을 다른 보안 솔루션에 제공하고 공유하여 네트워크를 위협하는 공격에 효과적이고 신속하게 대응할 수 있어야 한다. 또한, 이러한 공격들과 기존 공격들과의 연관 관계를 분석하기 위해 공격 시그니처들의 데이터베이스를 구축하는 것도 필요하다. 그리고 새로 생성되는 시그

니처들을 상호 공유하여 다른 보안 솔루션들의 서비스에 활용하기 위한 시그니처 교환 프로토콜 개발과 공통된 시그니처 메시지 형식의 정의가 필요하고, 여러 시그니처 자동생성 시스템들로부터 생성된 시그니처들을 수집하고 통합 및 관리하여 다른 보안 솔루션으로 안전하게 분배하거나 교환함으로써 안전한 네트워크 인프라를 제공할 수 있는 체계도 필요하다. 현재 네트워크 공격에 대한 시그니처를 생성하는 연구와 관련한 표준화가 진행되고 있지 않고 있다. 따라서, 보안 문제에 대한 해결책이 복잡하고, 다양하게 제시되고 있어, 현재의 대응 기술뿐만 아니라 향후에 제시될 다양한 방향에 대한 기술검증과 더불어 국내외의 표준화도 필요하다.

본고에서는 네트워크 환경이 발전함에 따라 점차 지능화되고 다양한 형태와 방법 및 경로로 퍼지고 있는 zero-day 공격에 대해 효과적으로 빠르게 대응할 수 있는 신뢰도 높은 시그니처를 자동으로 생성하여 대응하는 기술에 대해 설명한다. 또한, 생성된 시그니처를 다른 보안 솔루션으로 분배하거나 교환하여 상호 공유할 수 있는 교환 프로토콜과 공통된 시그니처 메시지 형식을 정의하고, 이러한 시그니처들을 통합 및 관리하여 안전한 네트워크 인프라를 위해 체계적으로 운영하기 위한 방법에 대해 설명한다.

II. 본 론

2.1 시그니처 생성 및 검증 기술

2.1.1 기존 공격 시그니처 생성 기술

Intel-CMU는 2004년과 2005년 Autograph와 Polygraph라는 공격 시그니처 자동생성 기술을 발표하였다[5,6]. 그러나 공격으로 의심되는 세션을 비정상 행위로 탐지하고, 탐지된 세션의 모든 패이로드(payload)를 저장하고 조합하여 시그니처를 생성함으로써 전체 시스템의 과부하(overhead)가 높아질 수 있다. 현재 공개된 버전의 Autograph는 P4-3GHz 시스템을 사용하여 T3급(45Mbps) 링크를 모니터링 하는데 사용되는 수준으로 고속 네트워크 환경에는 부적합하다. 단순한 기능의 비정상 트래픽 탐지 기술을 사용하면 오탐의 원인이 되며, 네트워크 내의 모든 패킷에 대한 탐지가 이루어지지 않는다. 전체 시스템의 과부하를 줄이기 위하여 패킷 내의 특정 값(Anchor) 만을 샘플링하고 이 값들에 의하여 시그니처를 생성하게 되면, 생성되는 시그니처의 분포가 고르지 않을 수 있고, 이로 인하여 탐지를 실패(false negative)하는 경우가 발생할 수 있다. 생성된 시그니처의 검증 절차가 없어, 생성된 시그니처의 신뢰도는 보장되지 않는다. 또한, 생성된 시그니처와 웜과의 상관도 분석 기능이 없어 대응 효과에 대하여 검증된 바가 없다.

USCD는 2004년 Earlybird라는 공격 시그니처 자동생성 기술을 발표하였다(현재 Cisco가 특허권을 가짐)[7]. 시그니처의 신뢰도가 낮고, 생성된 시그니처가 공격의 특성을 정확하게 추출하지 못하고 있어 화이트 리스트(white list) 등을 이용하여 문제를 해결하고자 하고 있다. 그러나, 화이트 리스트 관리는 시스템 성능에 심각한 성능 저하를 초래할 수 있고, 방대한 양의 수작업을 요구함으로써 시그니처의 실시간 적용에 중요한 장애요소가 된다. 전체 시스템의 과부하를 줄이기 위하여 네트워크에서 발생하는 패킷의 패이로드를 랜덤하게 샘플링하고 (1/64의 확률로 샘플링) 이 값들에 의하여 시그니처를 생성하게 되면, 생성되는 시그니처의 분포가 고르지 않을 수 있으며, 이로 인하여 탐지에 실패(false negative)하는 경우가 발생할 수 있다.

Penn. State Univ.는 2005년 EMIST (Evaluation Method for Internet Security Technology) 프로젝트의 세부과제로 시그니처를 생성하는 기술을 연구 중에 있다[8]. IP Cluster를 기반으로 하는 웜 공격 탐지기술을 개발했으며, 현재 이를 시그니처 생성에 접목하고 있지만 아직 초기단계의 연구로 알려져 있다.

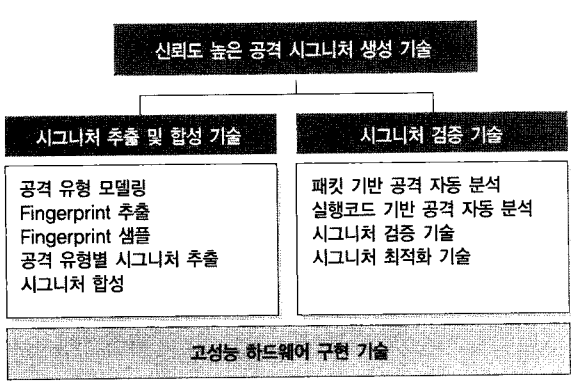
UC-Davis에서는 호스트를 기반으로 하는 웜의 시그니처를 탐지하는 기술을 개발하고 있다[9]. 호스트에서 네트워크를 통해 수신한 패킷 내용을 시뮬레이션 할 수 있는 가상의 환경을 구성하고 이를 바탕으로 공격패킷이 호스트의 시스템 제어를 빼앗는 코드를 탐지하여 시그니처 생성에 이용하고 있다. 정확도 측면에서는 앞의 연구보다 높을 수 있으나, 동일 네트워크 내의 다른 공격에 대한 탐지가 불가능하고, 탐지된 시그니처가 네트워크 전체의 보호에 사용되기 위하여 해당 네트워크로 다시 분배할 필요가 있으며, 이러한 과정으로 인하여 공격을 차단하는데 상당한 지연이 발생할 수 있다.

국내 산업체에서는 기존의 바이러스 차단 제품을 판매하는 보안 업체(안철수연구소, 시만텍 등)에서는 기존 바이러스 및 웜으로부터 시그니처를 추출하는 기술을 보유하고 있지만, 보안 전문가가 직접 해당 공격 프로그램을 분석하고 이로부터 공격 시그니처를 추출하는 것이다.

공격 시그니처의 자동생성 기술은 크게 네트워크상의 트래픽을 분석하여 시그니처를 생성하는 기술과 호스트 기반에서의 인터넷 웜의 동작 상태를 분석하여 시그니처를 생성하는 두 기술이 중점 연구되고 있다. 현재 가장 널리 연구되고 있는 주제는 다양한 정보로부터 공격 시그니처를 어떻게 생성할 것인가에 초점이 맞추어져 있다. 그러나, 향후 중요한 대응 기술이 될 것으로 예상되는 생성된 공격 시그니처의 정확도 및 신뢰성을 어떻게 향상시켜 실제 네트워크 환경에서 사용할 수 있도록 할 것인가에 대한 시그니처 검증 기술이 더욱 필요하고, 이 기술 구현을 통해 향후에는 기존 보안 장비 및 소프트웨어의 핵심 기술로 활용될 것이다.

2.1.2 신뢰도 높은 공격 시그니처 생성 기술

기존 연구들의 단점을 보완하고 네트워크 공격에 대하여 신뢰도 높은 시그니처를 생성하여 실시간으로 대응하기 위해서, 본고에서 개발중인 (그림 2)와 같은 고성능 하드웨어 기반의 시그니처 추출 및 합성 기술과 시그니처 검증 기술이 필요하다.



(그림 2) 신뢰도 높은 공격 시그니처 생성 기술

(1) 시그니처 추출 및 합성 기술

의심되는 유해 트래픽(suspicious flow)의 결정을 위해 네트워크 공격 유형별 모델링이 필요하다. 시그니처 생성에 사용되는 패킷 페이로드 샘플링을 보다 효율적으로 하기 위한 알고리즘들을 비교하고 분석하여 새로운 알고리즘을 개발하고 샘플링으로 인하여 발생할 수 있는 오탐을 최소화해야 한다. 시그니처 생성의 기본 단계인 핑거프린트(fingerprint) 추출은 핑거프린트 샘플링에 있어서 샘플링 되는 대상의 분포가 편중되지 않고, 샘플링 되는 패이로드의 간격을 안정적으로 하기 위한 기술이 필요하다. 그리고 핑거프린트의 연관성 분석을 통하여 공격 유형별로 신뢰도 높은 공격 시그니처를 추출 할 수 있어야 하고, 의심되는 유해 트래픽으로부터 얻어진 다양한 시그니처에 대한 유기적인 합성과정이 필요하다.

(2) 시그니처 검증 기술

Earlybird, Autograph, Polygrph와 같은 기존 시그니처 생성 기술들의 경우에는 생성된 시그니처가 공격 패킷과 P2P 패킷, 그리고 일정한 기간 동안 인터넷 상에서 관심도가 높아 빈번이 발생하는 패킷(flash cloud)과는 서로 구별하지 못하여 오탐율이 높은 편이다. 오탐을 줄이는 방안으로 화이트 리스트를 주로 사용하고 있으나, 고속네트워크에서 화이트 리스트의 사용은 시스템에 성능 저하를 유발하게 된다. 따라서, 화이트 리스트를 최소화하기 위한 기술이 필요하다. 이러한 오탐을 줄이는 방안으로 시그니처의 조합을 사용하는 방안이 최근 연구되고 있다.

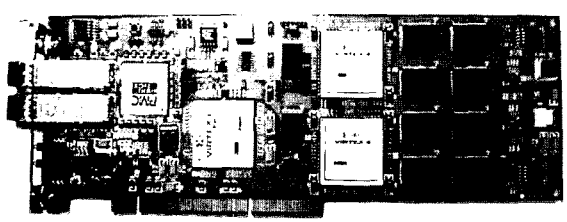
효과적인 조합과 시그니처 시퀀스(sequence)를 찾는 기술은 탐지된 시그니처 조합 또는 시그니처 시퀀스가 공격 패킷이 가지는 행동 특성을 파악하여 공격성을 판별하는 것이다. 또한, 시그니처를 효율적으로 적용하기 위하여 생성되는 시그니처 조합 또는 시퀀스의 고유성을 판별하는 기술도 필요하다. 여러 형태의 공격 시그니처를 효율적으로 관리하기 위한 데이터베이스 기술은 생성된 시그니처와 기존 공격 시그니처 데이터베이스와 비교 검증하는 것으로, 생성된 시그니처와 정상 트래픽과의 비교 검증을 통해 신뢰도가 낮은 시그니처의 생성을 최소화하는 것이다.

(3) 고성능 하드웨어 구현 기술

기가(Gbps)급의 네트워크 트래픽을 실시간으로 감시하여 조기에 공격을 탐지하고 공격에 사용된 포트와 패킷에 포함

된 패턴을 찾아내는 하드웨어 기술이 필요하다. 앞서 설명한 시그니처 생성 및 검증기술은 기존의 보안시스템에 적용된 시그니처 기반 탐지기술 등을 포함한 일반적인 보안기술보다 그 복잡도가 높다. 이러한 기술을 구현하기 위한 방안으로 네트워크 프로세서(Network Processor)를 이용한 방식과 FPGA(Field Programmable Gate Logic)를 이용한 하드웨어 기반의 방식이 있다. 네트워크 프로세서 기반의 방식은 하드웨어 기반의 방식보다 구현은 쉬우나, 시스템 처리속도가 구현 알고리즘의 복잡도와 사용되는 데이터의 크기에 따라 가변적이다. 따라서, 높은 복잡도의 작업을 초고속 네트워크에서 링크 속도(line speed)로 수행하기 위해서는 고도의 하드웨어 및 시스템 구현 기술이 필요하다.

(그림 3)은 현재 본 고에서 개발중인 FPGA 기반의 고성능 시그니처 자동생성(ETRI-ZASMIN) 보드 시제품이다[10].



(그림 3) 하드웨어 기반 ETRI-ZASMIN 보드 시제품

이 시제품은 의심되는 유해 트래픽에서 고성능의 하드웨어 기반으로 신뢰도가 높은 시그니처를 자동으로 생성하는 보드이다. 다양한 트래픽 특성을 고려하고 패킷의 공격 연관성을 분석하여 자동으로 시그니처를 생성하고 검증한다. 그리고 분산 지점에서 생성된 시그니처들의 연관성을 분석하고 화이트 리스트의 최소화로 생성된 시그니처를 최적화시킨다.

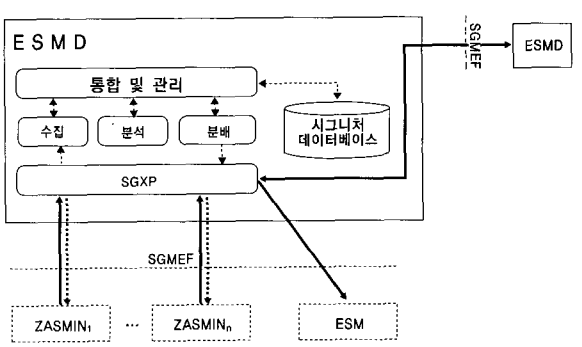
2.2 시그니처 관리 및 분배 기술

2.2.1 통합 시그니처 관리 및 분배 프레임워크

신뢰도 높은 시그니처를 생성하는 기술과 더불어 생성된 여러 시그니처를 통합하여 관리하고 다른 보안 솔루션으로 분배하거나 교환하여 상호 공유하기 위한 운영 기술도 필요하다. 본고에서 제안하는 통합 시그니처 관리 및 분배 프레임워크(ESMD; Enterprise Signature Management and Distribution)의 주요 역할은 다음과 같다.

(1) 네트워크 위협 공격에 대한 시그니처 자동생성 시스템에서 생성되는 시그니처들을 수집하고 통합 및 관리하는 역할
(2) 시그니처 생성 및 분배 시스템들을 포함한 타 보안 솔루션들과 연동하고 시그니처를 공유하는 역할
(3) 수집된 시그니처들을 대상으로 고수준 시그니처로 가공하거나 통합하는 역할
(4) 시그니처 생성 메시지 교환 형식으로 변환하여 전송하는 역할
(5) 시그니처 생성 교환 프로토콜을 통해 안전하게 시그니처를 분배하거나 교환하는 역할

(그림 4)는 본고에서 제안하는 통합 시그니처 관리 및 분배 프레임워크의 주요 구성 요소들과 타 보안 시스템들과의 관계를 표현한 것이다.



(그림 4) 통합 시그니처 관리 및 분배 프레임워크

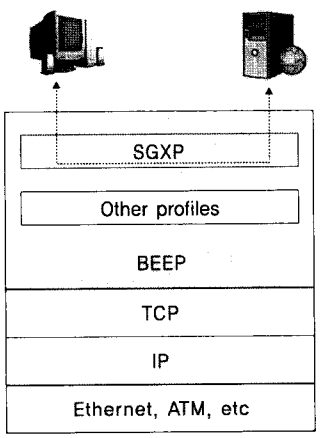
생성된 시그니처를 수집하고 통합하여 관리하고 분배하거나 교환하는 역할을 하는 프레임워크의 주요 구성 요소로는 ZASMIN(Zero-day Attack Signature Management INfrastructure) 시스템들로부터 생성되는 시그니처를 수집하거나 다른 보안 솔루션에게 시그니처를 분배 또는 교환하기 위해 사용하는 시그니처 생성 교환 프로토콜인 SGXP(Signature Generation eXchange Protocol)와 시그니처 생성 메시지 교환 형식인 SGMEF(Signature Generation Message Exchange Format), 이 프로토콜과 메시지 형식을

통해 다수의 ZASMIN 시스템들로부터 생성되는 시그니처를 수집하는 수집 기능 요소, 수집된 시그니처를 다양한 방법으로 분석하여 고수준의 시그니처로 가공하기 위한 분석 기능 요소, 이러한 시그니처들을 통합하여 관리하기 위한 통합 및 관리 기능 요소, 수집하거나 가공된 시그니처 정보를 저장하기 위한 시그니처 데이터베이스, 다른 보안 솔루션으로 분배하거나 교환하기 위한 분배 기능 요소가 있다. 기본적으로 ESMD는 ZASMIN로부터 생성된 시그니처를 수집하고, 공유하기 위한 시그니처를 내부 네트워크에 있는 ESM(Enterprise Security Management)이나 ZASMIN에 분배하거나 외부 네트워크에 있는 다른 ESMD와 서로 교환한다.

2.2.2 시그니처 생성 교환 프로토콜 및 메시지 교환 형식

각 연구 기관이나 보안 솔루션 업체들에서 생성한 시그니처들은 자체 관리되고 있으며, 네트워크를 통한 공유 역시 제한적인 상황이다. 시그니처들의 공유 제한 문제는 네트워크 공격에 대한 빠른 대응을 저해하는 요소이다. 이러한 공유 문제를 해결하고 시그니처를 빠르게 교환하기 위해서 시그니처 생성 메시지 교환 형식과 높은 보안성을 제공하는 프로토콜이 필요하다. 우선, 시그니처 메시지 교환 형식 표준은 시그니처 공유에 있어서 보안 시스템간의 호환성을 제공하기 때문에 필수적이다. 그리고 높은 보안성은 시그니처 데이터 공유로 인해 발생할 수 있는 해킹으로부터 데이터를 보호하여 시그니처를 우회하는 새로운 형태의 네트워크 공격을 사전에 차단한다. 본 절에서는 지속적으로 발생하는 알려지지 않은 네트워크 공격들을 검출하여 새롭게 생성한 시그니처들을 서로 공유하고, 각 보안 솔루션에 적용하여 빠르게 대응하기 위한 공통된 시그니처 메시지 교환 형식과 안전한 교환 프로토콜을 정의한다.

본고에서 제안하는 시그니처 생성 교환 프로토콜(SGXP)은 시그니처 생성 시스템들과 보안 솔루션들간의 시그니처 정보를 교환하기 위한 BEEP 프레임워크 기반의 응용 레벨의 프로토콜이다(일종의 BEEP 프레임워크 기반의 프로파일)[11]. 이 프로토콜은 BEEP(Block Extensible Exchange Protocol) 세션을 설정하고 그 세션상에서 데이터 교환을 위한 SGXP 채널(channel)을 설정하는 절차 및 데이터 형태를 XML 스키마(schema)로 정의한다. 이 프로토콜의 동작은 크게 세션 연결, 상호 협상 및 인증, 시그니처 메시지 교환 과정으로 이루어진다. 또한, 이 프로토콜은 시그니처 전송을 위한 연결 설정 과정 부분에서는 BEEP에 기반하는 SGXP를 정의하고, 시그니처 메시지 교환 형식으로는 XML 기반의 SGMEF에 대해 정의하고 있다.



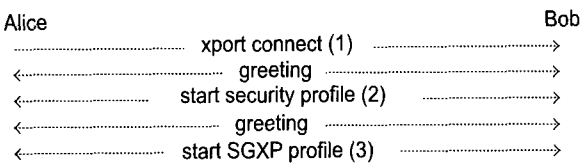
(그림 5) BEEP 프레임워크 기반 SGXP

IETF에서 표준화된 블록 확장 교환 프로토콜인 BEEP는 연결성, 비동기성 (asynchronous) 통신을 지원하기 위한 일반적인 응용 프로토콜로 TCP 계층에서 동작하는 모든 프로토콜을 블록화하여 프로파일 형태로 제공하도록 준비된 프레임워크이다. BEEP 프레임워크에서는 시그니처 교환에 필요한 많은 프로파일들을 제공하고 있으며 본고에서 제안하는 프로토콜에서는 아래와 같은 프로파일(profile)들을 포함한다.

- The TUNNEL Profile
- The Simple Authentication and Security Layer (SASL) Family of Profiles
- The TLS Profile

SGXP는 BEEP 프레임워크 내에 정의된 프로파일들을 이용하여 상호 인증, 무결성, 기밀성 같은 보안 특성을 제공받는다. 이러한 보안 특성은 TLS, SASL 프로파일들과 같은 조절용(tuning) 프로파일을 통해서 제공된다. (그림 5)는 BEEP 프레임워크 상에서 SGXP를 이용하여 통신하는 것을 나타낸 것이다.

SGXP의 흐름은 크게 세션 연결, 상호 협상 및 인증, 시그니처 메시지 교환 과정으로 분류할 수 있고 전체 흐름은 (그림 6)과 같다.

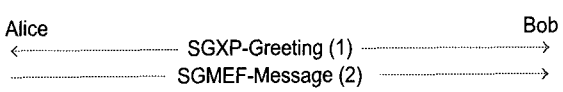


(그림 6) SGXP 전체 동작 흐름

(1) 'Alice'는 BEEP Greeting 메시지를 교환하기 위해서 'Bob'에게 전송 연결(transport connection)을 요청한다.
(2) 각 단(peer)은 BEEP Security Profile을 통해 상호 협상 및 인증을 수행한다. 상호 인증 과정은 BEEP 프레임워크의 해당 프로파일(SASL, TLS 등)의 정의와 동작에 따라 이루어진다.
(3) 각 단은 SGXP Profile을 통해 시그니처 메시지를 교환한다.

SGXP에서는 위의 세 가지 외에 각 과정의 흐름을 이어주기 위해 "greeting" 메시지를 사용한다. 즉,"greeting" 메시지는 각 과정의 사이에서 교환되며, 개별적인 규격을 갖는 세션 연결, 상호 협상 및 인증, 메시지 교환의 과정은 "greeting" 메시지에 의해 이어지게 된다. 또한, "greeting" 메시지는 이전 과정에 대한 성공/실패 메시지를 포함하며, 동시에 다음 과정을 위한 프로파일 교환을 수행한다.

시그니처 메시지 교환은 SGXP Profile에 의해 이루어진다. SGXP Profile은 SGMEF-Greeting 메시지와 SGMEF 메시지의 전송 절차에 관해 정의한다. SGXP Profile의 흐름은 (그림 7)과 같다.



(그림 7) SGXP Profile 동작 흐름

(1) 'Alice'와 'Bob'은 SGMEF-Message를 전송하기 전에 SGXP 채널을 설정하기 위해 서로 SGXP-Greeting을 교환한다.
(2) 'Alice'는 'Bob'에게 SGMEF-Message를 전송한다(단, 여기서 'Alice'가 Client의 역할이라고 가정했을 때이고, 만약 'Bob'이 Client일 경우에는 (2)의 화살표는 반대 방향이 된다).

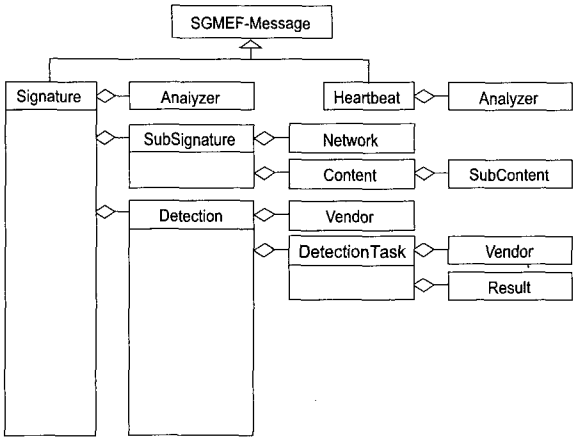
시그니처 메시지의 교환을 마치고 해당 채널의 연결 설정을 해제하려면 BEEP 프레임워크의 "close" 메시지 전송 과정을 통해 이루어진다.

시그니처 생성 메시지 교환 형식(SGMEF)은 네트워크 환경을 위협하는 공격에 대해 생성된 시그니처 정보를 표현하기 위해 본고에서 제안하는 데이터 형식이다. 이 데이터 형식은 상업용, 오픈 소스, 연구용 시스템에서 생성된 시그니처 정보들을 공통된 형식으로 표현하고, 사용자, 기업, 기관 등 여러 조직에서 상호 교환하여 활용 가능한 공통의 데이터 교환 형식이다. SGMEF 형식을 체계적으로 정의하기 위하여 데이터 모델과 이에 따른 실제 구현 방법을 정의한다. 객체 지향 방법론 설계 언어인 UML(Unified Modeling Language)의 클래스 다이어그램을 사용하여 시그니처 정보의 데이터 모델을 정의한다. UML의 클래스 다이어그램을 사용함으로써 확장성과 융통성을 보장할 수 있고, 시그니처 정보의 표준 표현을 제공하여 복잡한 정보들간의 관계를 묘사하는데 효율적이다. 그리고 이 모델의 구현 방법은 XML(eXtensible Markup Language)의 스키마(Schema)로 정의하여 구현 수준에서의 확장성과 융통성을 보장하도록 한다. 여기서, XML의 데이터 모델을 표현하는 언어로는 DTD(Document Type Definition)와 스키마(schema) 가 있으나, DTD는 자체적으로 Namespace 기능을 지원하지 못하고 상속의 개념이 없다. 또한, DTD는 XML과 상이한 문법을 사용하여 XML과 DTD 파서가 모두 필요하다는 단점을 갖고 있다. 따라서, 본고에서 정의한 SGXP와 SGMEF는 BEEP 프레임워크에 따라 XML을 사용하여 메시지를 생성하고 XML의 데이터 모델을 표현하기 위해 스키마를 사용한다.

시그니처 생성 교환 메시지 형식에서 가장 상위 클래스는 SGMEF-Message로 모든 종류의 시그니처 생성 교환 메시지를 총칭한다. 본고에서 제안하는 SGMEF 데이터 모델은 시

그니처를 어떻게 생성하고 검증할 것인가를 정의하지는 않는다. 즉, 단지 어떻게 시그니처가 형식화되고 구성될 수 있는지에 관한 내용만 정의한다.

(그림 8)은 전체 SGMEF 데이터 모델의 개관이고, 본고에서는 주요 클래스에 대한 정의만을 소개한다. SGMEF-Message 클래스는 시그니처 생성 메시지 교환 형식에서 최상위에 위치하고 전송하고자 하는 메시지를 하위 클래스로 포함한다. SGMEF-Message는 하위 두 가지 클래스들 중 반드시 하나로만 구성되어야 한다.



(그림 8) SGMEF 전체 클래스 다이어그램

Signature 클래스는 네트워크 위협 공격들에 대해 시그니처 생성 시스템에서 탐지 과정을 거쳐 생성된 시그니처의 정보들을 표현한 상위 클래스이다. Signature 클래스는 하위 요소로 Analyzer 클래스, SubSignature 클래스, Detection 클래스를 포함한다. Heartbeat 클래스는 관리자에게 활성화 상태를 점검하기 위해 단말(node)의 기본적인 정보들을 표현한 것으로, 하위 요소로 Analyzer 클래스를 포함한다. Heartbeat 메시지는 지정된 시간이나 일정 간격 시간에 메시지를 전송한다. 모든 단말은 Heartbeat 메시지를 받는 기능을 지원해야 하지만, 단말이 그 메시지를 사용하는 것은 선택적이다.

Analyzer 클래스는 시그니처를 생성한 단말의 정보들을 표현한 것으로, 이 정보에서는 단말의 위치 정보나 단말간의 관계 정보는 포함하지 않는다. SubSignature 클래스는 공격에 대해 유해 트래픽을 분석하여 생성한 시그니처 정보들을 표현한 것으로, 하위 요소로 Network 클래스와 Content 클래스를 포함한다. Network 클래스는 시그니처를 생성하는데 사용된 패킷들의 IP 주소 및 포트 정보 등의 네트워크 트래픽 정보들을 포함한다. Content 클래스는 생성된 시그니처의 상세 정보를 표현하기 위한 상위 클래스로, 하위 요소로 SubContent 클래스는 시그니처 데이터의 표현 형식, 길이 및 내용을 포함한다. Detection 클래스는 유해 트래픽을 분석하여 시그니처를 생성시키는데 사용된 다양한 탐지 태스크(task) 정보를 표현한 것으로, 하위 요소로 Vender 클래스와 DetectionTask 클래스를 포함한다. Vendor 클래스는 해당 모듈들을 개발한 벤더 (vendor)의 정보들을 포함한다. DetectionTask 클래스는 시그니처 생성을 위해 사용된 탐지 태스크 정보들을 표현한 것으로, Vendor 클래스와 Result 클래스를 포함한다. Result 클래스는 시그니처를 생성하는데 사용된 탐지 태스크의 결과 정보를 표현하기 위한 것이다. (그림 9)는 본고에서 개발중인 공격 시그니처 자동생성 시스템에서 Win32/Blaster 웜에 대해 생성한 시그니처 정보를 SGMEF로 표현한 예이다.

```
<?xml version="1.0" ?>
- <sgmef:SGMEF-Message version="1.0" xmlns:sgmef="http://signature.etri.re.kr/sgmef">
  - <sgmef:Signature messageId="70625001">
      <sgmef:generationTime>2007-06-25 20:12:59</sgmef:generationTime>
    - <sgmef:Analyzer analyzerId="ZASMIN-02">
        <sgmef:name>zasmin</sgmef:name>
        <sgmef:manufacturer>ETRI-SGS</sgmef:manufacturer>
        <sgmef:version>alpha</sgmef:version>
        <sgmef:ostype>CentOS</sgmef:ostype>
        <sgmef:osversion>4.4</sgmef:osversion>
      </sgmef:Analyzer>
    - <sgmef:SubSignature signatureId="70625001">
        <sgmef:createTime>2007-06-25 20:09.57</sgmef:createTime>
      - <sgmef:Network>
          <sgmef:protocol>6</sgmef:protocol>
          <sgmef:srcAddress>192.168.107.110</sgmef:srcAddress>
          <sgmef:srcPort>1050</sgmef:srcPort>
          <sgmef:dstAddress>115.184.48.111</sgmef:dstAddress>
          <sgmef:dstPort>135</sgmef:dstPort>
        </sgmef:Network>
      - <sgmef:Content>
        - <sgmef:SubContent category="hexa">
            <sgmef:length>7</sgmef:length>
          - <sgmef:sigcontent>
              <![CDATA[ 05 00 00 03 10 00 00 ]]>
            </sgmef:sigcontent>
          </sgmef:SubContent>
        + <sgmef:SubContent category="hexa">
        + <sgmef:SubContent category="hexa">
        + <sgmef:SubContent category="hexa">
        + <sgmef:SubContent category="hexa">
        - <sgmef:information>
            <![CDATA[ 00 00 ]]>
          </sgmef:information>
        </sgmef:Content>
      </sgmef:SubSignature>
    + <sgmef:Detection category="NetworkBased">
    + <sgmef:Detection category="NetworkBased">
      <sgmef:assessment>4.8</sgmef:assessment>
    </sgmef:Signature>
</sgmef:SGMEF-Message>
```

(그림 9) Win32/Blaster 웜에 대한 SGMEF 예

2.3 국내외 시그니처 관련 표준화 현황

공격 시그니처 자동생성은 초기 단계의 연구로 현재까지 보고된 표준화 관련 활동이 없다. 그러나, 시그니처 차원이 아니라, 시그니처를 포함하는 정책(Policy) 차원에서의 표준 포맷에 대한 표준화는 IETF의 NWG(Network Working Group)를 중심으로 정의하고 있다(RFC 3460 등)[12]. 또한, 시그니처를 통해 탐지된 정보를 공유하기 위하여 필요한 프로토콜과 데이터 포맷을 IETF IDWG(Intrusion Detection Working Group)를 중심으로 정의하고 있다(RFC 4765, RFC 4767)[13,14].

향후 시그니처 모델링과 분배 및 교환에 관한 기술에 대하여 국내외 표준화가 필요한 실정이다. 현재, 국내 한국정보통신기술협회(TTA)에서는 네트워크 위협 공격에 대한 시그니처 관리 및 분배에 관한 프레임워크와 시그니처 교환 프로토콜 및 메시지 교환 형식에 관한 주제로 표준화가 진행되고 있고, 2007년 9월에 스위스에서 개최된 ITU-T SG17 Q6회의에서 Security Information Sharing Framework 에 관한 주제로 국제 표준화가 추진되고 있다.

2.4 시그니처 관리 및 분배의 기본적인 운영 모델

네트워크 환경을 위협하는 공격들에 대해 그 피해를 최소화하고 신속하게 대응하기 위해서, 관리 네트워크 내의 여러 시그니처 생성 시스템들로부터 생성된 시그니처들을 최상위의 ESMD에서 수집하고 통합 및 관리하여 관리 네트워크 내외의 타 보안 솔루션으로 안전하게 분배하거나 교환하기 위한 운영 방법에 대해 설명한다. 본고에서 제시하는 시그니처 관리 및 분배의 기본적인 운영 모델은 (그림 10)과 같고, 이 운영 모델을 구성하는 요소들의 설명과 그 역할은 다음과 같다.

(1) ZASMIN: 네트워크 환경의 위협 공격들에 대한 시그니처를 자동으로 생성하는 시스템을 말한다. 생성된 시그니처는 이 시스템의 관리자에 의해 직접 IDS/IPS 또는 FW로 분배하거나 ESMD로 전송하는 역할을 한다.

(2) ESMD: 생성된 시그니처를 수집, 분석, 통합 및 관리, 분배하는 기능을 갖는 시스템을 말한다. 수집된 시그니처는 통합하여 관리하고, ESM 또는 ZASMIN에게 분배하거나 외부 네트워크에 있는 다른 ESMD와 상호 교환하는 역할을 한다. 여기서, ESMD가 분배 또는 교환하는 대상 보안 솔루션은 ZASMIN, ESM, ESMD로 한정한다. 본고에서 '분배'와 '교환'의 의미는 같고, '교환'은 ESMD들간의 상호 전송으로 정의하고, '분배'는 ESMD와 기존 보안 솔루션들간의 전송으로 정의한다.

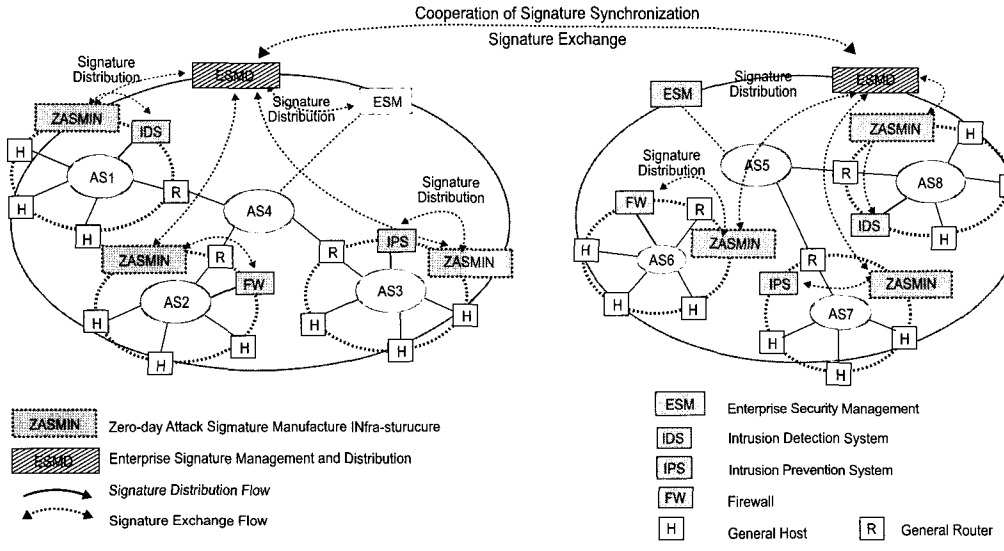
(3) ESM: 기존 보안 솔루션들에서 생성되는 경보들을 수집하고 분석하거나 내부 네트워크 내의 보안 시스템들을 관리하는 시스템들을 말한다. ESMD에서 분배되는 시그니처를 전송 받아 내부 네트워크의 기존 보안 솔루션들에게 시그니처를 분배하는 역할을 한다. 여기서, 시그니처 분배 대상 솔루션들 중에서 ZASMIN, ESMD는 제외한다.

(4) IDS/IPS: 침입 탐지 및 방지 시스템으로 알려진 공격들에 대한 탐지를 수행하거나 적극적으로 대응하는 시스템들을 말한다. ZASMIN 또는 ESM에서 분배된 시그니처를 적용하여 유해 트래픽에 대해 탐지 및 대응을 하는 역할을 한다.

(5) FW: 방화벽 시스템으로 정책 설정에 의한 네트워크 흐름을 허용하거나 불허하는 역할을 하는 시스템들을 말한다. ZASMIN 또는 ESM에서 분배된 시그니처를 적용하여 네트워크 흐름을 허용 또는 차단하는 역할을 한다.

(6) H 또는 R: 일반적인 사용자 호스트 시스템이나 라우팅 기능을 하는 네트워크 시스템들을 말한다.

이 운영 모델은 기존 보안 솔루션들로 구성된 네트워크 환경에서 공격 시그니처를 생성하기 위한 ZASMIN 시스템과 수집, 분석, 통합 및 관리하여 타 보안 솔루션으로 분배 및 교환하기 위한 ESMD 시스템을 추가한 형태이다. 이 운영 모델은 기존 보안 솔루션들로 구성된 네트워크 환경을 변경할 필요 없이 운영 가능하다는 장점이 있다. 이 모델의 기본적인 운영은 먼저, 네트워크 환경의 위협 공격들에 대해 ZASMIN들이 각 공격들의 시그니처를 생성한다. ZASMIN에서 생성된 시그니처는 기존 보안 솔루션(FW, IDS/IPS)에 바로 적용하여 대응하거나, SGMEF 메시지 형식으로 SGXP를 통해 ESMD 시스템으로 시그니처 정보를 전송한다. 수집한 시그니처 정보들을 통합 및 관리하는 ESMD는 내부 네트워크의 ESM이나 다른 ZASMIN에게 분배하여 시그니처 정보



(그림 10) 시그니처 관리 및 분배의 기본적인 운영 모델

를 공유할 수 있다. 또한, 이러한 ESMD들은 각 업체 및 기관별로 설치되어 운영될 수 있으며, 통합하여 관리하는 시그니처를 SGXP와 SGMEF 메시지 형식으로 상호 교환하여 서로 다른 네트워크에서도 공유할 수 있다.

III. 결 론

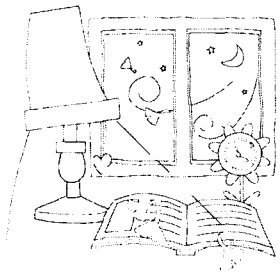
노출된 취약성을 해결할 패치가 발표되기 전에 취약성을 공격하는 zero-day 공격에 대해 초기에 탐지 및 대응함으로써 네트워크 인프라를 보호하는 네트워크 정보보호 제품 및 관련 서비스 산업에 대한 관심과 수요가 지속적으로 증대되고 있다. 기존의 IDS/IPS 제품이 비정상 행위 탐지 기능의 오탐으로 인하여 비활성화되고 있는 정보보호 제품군의 지속적인 성장을 위해서는 실시간으로 네트워크 위협 공격에 대한 시그니처를 자동 생성하여 적용하는 기술이 필수적이다.

본고에서는 기존 시그니처를 생성하는 연구 및 기술들의 단점을 보완하기 하기 위해 고성능의 하드웨어 기반으로 생성된 시그니처를 검증하여 신뢰도가 높은 시그니처를 생성시키는 연구를 소개했다. 이와 같이 생성된 시그니처를 다른 보안 솔루션으로 분배하거나 교환하여 상호 공유하기 위한 통합 시그니처 관리 및 분배 프레임워크를 제안하고, 이 프레임워크의 구성 요소들과 기본적인 운영 모델에 대해 설명하였다. 또한, 이 프레임워크에서 사용할 시그니처 생성 교환 프로토콜 및 메시지 교환 형식을 정의하고, 이 프로토콜의 동작과 Win32/ Blaster 웜에 대해 생성된 시그니처를 메시지 교환 형식으로 표현하였다.

이러한 시그니처 생성, 검증, 관리 및 분배 기술들은 국내외 네트워크 환경의 위협 공격의 시그니처 생성 및 교환을 위한 관리체계를 구축하는데 발생할 수 있는 혼란을 최소화하고 체계적인 시그니처 교환 및 관리의 활성화에 기여할 것이다. 또한, 이러한 체계적인 관리를 통하여 네트워크의 위협 공격에 대해 빠르게 대응할 수 있도록 하여 국가적인 차원에서의 효과적인 방어 체계를 구축하는데 기여할 것이다.

[1] Inside the Slammer, in IEEE Security and Privacy 2003.
[2] Symantec ISTR VXI, 2007.
[3] IDC, Worldwide IT Security Software, Hardware, and

Services 2004-2008 Forecast : The Big Picture
[4] IDC, Korea Security Appliances 2004-2008 Forecast and Analysis, 2005.
[5] H.-A., Kim and Karp, B. "Autograph: Toward Automated, Distributed Worm Signature Detection," Proc. of the 13th Usenix Security Symposium, 2004.
[6] Newsome, J., Karp, B., and Song, D., "Polygraph: Automatically Generating Signatures for Polymorphic Worms," Proc. of the IEEE Symposium on Security and Privacy, 2005.
[7] Singh S., Estan C., Varghese G., and Savage S., "Automated worm fingerprinting, "Proc. of 6th Symposium on Operating System Design and Implementation, 2004.
[8] EMIST project, http://emist.ist.psu.edu
[9] Levitt K.N., Rowe J. and Schooler E. M., "A Distributed Host-based Worm Detection System," the Special Interest Group on Data Communication, 2006.
[10] ETRI-ZASMIN, http://www.etri.re.kr
[11] IETF RFC 3080, The Blocks Extensible Exchange Protocol Core (BEEP), 2001.
[12] IETF RFC 3460, Policy Core Information Model (PCIM) Extensions, 2003.
[13] IETF RFC 4765, The Intrusion Detection Message Exchange Format (IDMEF), 2007.
[14] IETF RFC 4767, The Intrusion Detection Exchange Protocol (IDXP), 2007.



약 력

정 일 안

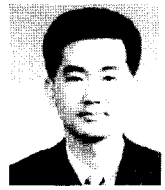
1999년 전남대학교 정밀화학공학 학사 졸업
2002년 전남대학교 전산학과 석사 졸업
2004년 전남대학교 박사졸업
2004년 ~ 현재 한국전자통신연구원 연구원
관심분야 : 시스템 및 네트워크 보안, 표준화

김 익 균

1994년 경북대학교 컴퓨터공학과 학사 졸업
1996년 경북대학교 컴퓨터공학과 석사 졸업
1996년 ~ 1999년 한국전자통신 연구원
2000년 ~ 2001년 (주) 팍스콤 선임연구원
2004년 ~ 2005년 Purdue University 객원연구원
2001년 ~ 현재 한국 전자통신 연구원 선임연구원
관심분야 : 네트워크보안, 컴퓨터네트워크

오 진 태

1990년 경북대학교 전자공학과 학사 졸업
1992년 경북대학교 전자공학과 석사 졸업
1992년 ~ 1998년 한국전자통신연구원 선임연구원
2003년 ~ 현재 한국전자통신연구원 보안게이트웨이 연구팀 팀장/선임 연구원
관심분야 : 네트워크보안, 비정상행위 탐지기술



장 종 수

1984년 경북대학교 전자공학과 학사 졸업
1986년 경북대학교 전자공학과 석사 졸업
2000년 충북대학교 박사 졸업
1989년 ~ 현재 한국전자통신연구원 보안응용 그룹 그룹장/책임연구원
관심분야 : 네트워크보안, 정책기반 보안관리기술