한국게임학회 논문지
제5권 제1호 2005년 3월

시뮬레이션 환경하에서 인터넷 게임 사고 대응시스템모델 연구

*신승중, **최운호
한세대학교 IT학부
expersin@hansei.ac.kr

A Study on the Emergency Response System for internet game event with simulation circumstance.

*Seung-Jung Shin, **Woon-Ho Choi
Dept. of IT Hansei university

요약

본 논문에서는 인터넷환경에서 증가하는 인터넷게임의 바이러스/웜의 공격에 의한 침해사고 발생 시 정의되어야 할 정보와 이를 활용한 대량 트래픽을 발생시키는 탐지하는 방안을 제안하였다. 이에 따라 인터넷 게임 사고대응시스템에서의 자동화된 역추적 방안에 대한 설계와 기능에 대한 개념을 제시한다.

Abstract

This paper is model can be useful and capable of automatically collecting and classifying the various information about a wide range of security incidents such as hackings, worms, spyware, cyber-terror, network espionage and information warfare from firewall, IDS, VPN and so on. According to them Internet game and an automated/integrated computer emergency response system can perform an attack assessment and an early warning for any incidents based on Enterprise Security Management environment.

Key Words: CIP, EWIS, connection trace-back

1. 서론

인터넷의 발달로 악의를 가지고 침입하여 개인정보와 인터넷게임에 사용되는 공인인증체계의 정보 등 금융신용정보가 유통되는 시스템의 정보를 획득한 후 불법적인 일에 사용하는 경우가 자주 발생하고 있으며 컴퓨터 바이러스나 웜 등을 확산시켜 정보를 파괴하거나, 중요서비스를 마비시켜 정보통신기반보호법에 규정된 중요시설 에 대한 사이버 테러나 해킹 등 사이버 범죄를 일으키고 있다.

종래에 이러한 해킹 등의 침해 사고를 처리하기 위해서는 피해자가 일일이 해당 시스템에 대한 피해 정도나 관리자, 블랙리스트(IP주소와 같은), 사고 발생 시점까지의 해당 시스템에 대한 로그/패치 정보, 이력 관리 그리고 백업 등에 관한 정보 등을 침해사고대응팀 (CERT : Computer Emergency Response Team; 이하 "CERT"라 한다)) 등의 정보보호 전문 기관에 전화나 이메일로 상담하며, 해당 전문기관에서는 각각의 상담 내용을 자신의 시스템으로 수동 입력하고 이를 근거로 침해 사고 내용을 분석하여 판단하고 있다.

또한, 각 조직의 정보보호 담당자가 자신이 보유한 시스템의 취약성 및 이력을 상세히 파악하여, 새로 나오는 취약점을 매일 패치하고, 이를 연계하여 침입탐지시스템에서 알려주는 공격 정보에 효과적으로 대응하기는 더더욱 어려우며, 수시로 발생하는 악성 바이러스 및 웜에 실시간 대응도

못하는데 현실적인 문제점이다. 이렇듯, 개인의 중요 정보 시스템 및 전산센터/전산시스템 그리고 금융, 통신 등 정보통신기반보호법(법률 6383호) 상에 정의된 주요 정보통신 기반시설 (CIP : Critical Infrastructure Protection)과 같은 여러 중요한 시스템을 해킹이나 사이버테러로부터 보호해야 할 필요가 대두되고 있음에도 그에 대한 효율적이고 일괄적인 방법이 제시되지 못하고 있는 실정이다.

본 논문에서는 게임관련 정보의 안전한 공유시스템 및 네트웍 제공, 각 침해사고에 대한 공격평가와 조기 경보가 가능하며, 새로운 침해사고에 대한 테스트(시뮬레이션)를 수행하고, 조기경보시스템 (EWIS(Early Warning Information System)) 설계와 기능에 대한 개념을 논의하고 시뮬레이션 환경하에서 게임 등 각종 발생할 수 있는 사고에 대한 대응 시스템을 연구하고자 한다.

2. 본론

역추적이란 사이버 범죄를 시도하는 공격자의 네트워크 상의 실제 위치를 탐색하는 기술이다. 추적 기술은 일반적으로 크게 2가지 분야로 분류되는데, 이는 해커가 우회공격을 시도하는 경우, 해커의 실제 위치를 추적하는 기술과, IP 주소가 변경된 패킷의 실제 송신지를 추적하는 기술이다. 이때, 우회 공격을 시도하는 해커의 실제 위치를 추적하는 기술을 TCP 연결 역추적(TCP connection traceback) 혹은 연결 역추적(connection traceback)이라 하고, IP 주소가 변경된 패킷의 실제 송신지를 추적하는 기술을 IP 패킷 역추적(IP packet traceback) 혹은 패킷 역추적(packet traceback)이라 한다.

기존의 역추적 기술은 시스템 로그 분석, Logging, Ingress Filtering, Link Testing, ICMP Traceback등과 IP역추적 시스템은 라우터 기능을 이용한 형태, 로그데이타를 이용하는 구조 혹은 링크를 테스트하는 방식이며, 다양한 방법이 논의되고 있다. 크게 로그를 이용한 역추적기술과 TCP 연결 역추적기술로 분류할 수 있는데 역추적을 위해서는 기본적으로 시스템 로그를 활용하며, 로그와 이상 파일을 바탕으로 시스템에 침입이 있었는가를 밝히고, 침입이 있었다면 언제 어느 사용자가 어디에서 접근하여 이루어졌는가를 밝힌 후 침입자가 접근한 시스템에 접근하여 그 시스템에서 로그를 검색하여 그 사용자의 원래의 출발지를 연속적으로 찾아가는 방식으로 침입자의 출발지를 추적하는 시스템이다. TCP 연결 역추적 기술은 크게 호스트 기반 연결 역추적 기술과 네트워크 기반 연결 역추적 기술로 분류 할 수 있다. 호스트기반 연결 역추적 기술은 역추적을 위한 모듈이 인터넷 상의 호스트들에 설치되는 역추적 기법으로 호스트에서 발생하는 로그 기록 등의 다양한 정보를 바탕으로 역추적을 진행하는 기술이다. 그러나 이러한 방법을 이용하여 역추적을 수행하기 위해서는 인터넷 상의 모든 호스트에 역추적 모듈이 설치되어야 하고, 역추적 경로 상의 단 1개의 시스템에서라도 어떤 문제에 의해서 역추적 정보를 얻을 수 없게 되는 경우가 발생하면 역추적이 불가능하게 되는 단점을 가지고 있다. 네트워크 기반 연결 역추적 기술은 네트워크 상에 송수신 되는 패킷들로부터 역추적을 수행할 수 있는 정보를 추출하여 역추적을 수행하는 것으로 역추적 모듈이네트워크 상에 송수신되는 패킷을 확인할 수 있는 위치에 설치되어야하고, 다만 네트워크 상에서 얻을 수 있는 패킷으로부터 어떤 정보를 활용해야 공격 연결과 같은 연결에 속하는가를 판단할 수 있을지에 대한 알고리즘만이 제기되고 있는 상황이다. 이는 네트워크 상의 패킷들로부터 얻게 되는 각종 연결 정보들을 네트워크 상에 존재하는 역추적 시스템들과 공유하는데 있어서, 생성되는 정보의 순서관계 및 동기화가 매우 어렵고, 네트워크상에서 발생하는 모든 연결에 대한 정보를 지속적으로 보유하고 있어야 하는 문제가 발생할 수 있기 때문이다. 또 다른 네트워크 기반 연결 역추적 기술로는 액세스 네트워크상에서 동작하는 기술들이 있다. 그러나 액세스 네트워크를 기본으로 하기 때문에 현재의 인터넷 환경에 적용하는 데 많은 어려움이 있는 것이 사실이다. 이런 상황에서 각종 침해사고에 대한 대응은 적극적이지 않은 상황이다.

2.1. 침해사고사례

침해사고사례에는 여러 가지 유형이 있는데 패스워드 파일 획득후에 패스워드를 크랙하여 불법으로 접속하는 방법과 네트워크 및 시스템 취약점 탐지를 위한 스캔공격, 침입 후 다음 침입을 위해 백도어(Backdoor)를 설치하는 방법, Denial of Service 등이 있다. 이들 불법침해유형도시간이 지날수록 변화하고 있는 실정이다.

2.2. 침해탐지 단계

(1) 망라우터의 NMS

게임운영시 전체 ISP망 관리 시스템(NMS)상 에서의 트래픽의 추이 및 PPS (packets per second)를 감시하여 갑자기 트래픽이 폭증하거나 트래픽의 변화가 없어도 CodeRed 처럼 작은사이즈의 패켓이 다량 발생하여 PPS의 급속한 증가가 있는지를 탐지한다.

(2) IDS(Intrusion and Detection System)의 이용

국제Gateway및 주요 백본망 point에 IDS장비를 설치하여 항시 망을 감시하고 있으며 일상적인 트랙픽이 아닌것에 대해서는 그 원인을 분석하여 조치하고 있으며 패켓추이를 항상 감시하고 있다. 특히 불법적인 비인증 접속자의 감시나 이에 따른 망관리 및 관제측면의 감시에 위험요소를 탐지하는 기능을 보유하고 있다.

3. 통합관제시스템(ESM)

이러한 현상에 대응할 목적으로 ESM(기업 통합 정보보호 관리시스템 ; Enterprise Security Management; 이하 ESM이라 한다.)이 개발되어 사용되고 있다. 이러한 ESM은 초기 1단계 제품에서는 네트워크나 시스템 리소스들의 각종 위험 요소들을 분석하고 모니터링하는 일종의 "관리 도구"로서 침입 차단 시스템(F/W), 침입 탐지 시스템(IDS), 안티 바이러스 제품 등 기존의 다양한 회사에서 생산된(Multi-Vendor) 정보보호 솔루션들을 통합하여, 하나의 화면에서 모니터링하는 방법을 다음과 같이 제공하고 있다.

현재, 일반적으로 정부/공공분야, 대기업, 금융기관, 대학 등에 설치된, 여러 분야의 정보보호제품(F/W, IDS, VPN, SeOS 등)을 ESM에 접속하여 전체적인 정보를 보여주며, 필요시, ESM등 이들 제품이 집중적으로 설치된 센터를 보호하고, 출입자의 접근관리를 위한 물리적인 장치들이 설치되고, 이러한 대형 관제센터를 자체적으로 보호하기위한 F/W, IDS등이 별도로 설치되기도 한다.

그러나, 이러한 ESM에 의하는 경우에도, 너무 많은 이벤트가 발생하므로 이벤트를 일정한 방법으로 필터링하여도 관리자가 연관관계나 사고대응 등의 업무를 처리하기에는 원시적이고 불편하였으며 ESM을 효율적으로 운영하기 위해서는 많은 정보보호 전문인력이 투입되어 분석하여야 하

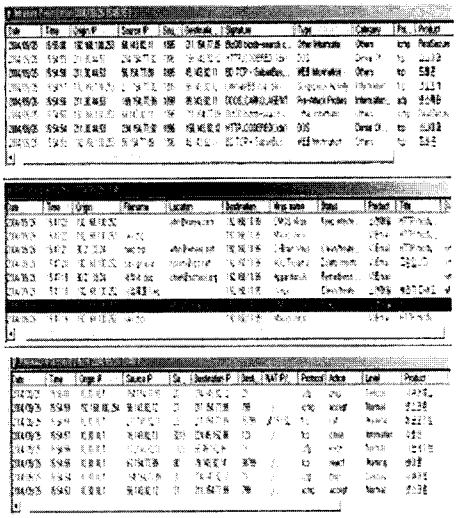


그림1-1. ESM 모니터링

나 대부분의 회사나 조직이 인원 부족이 부족한 실정이며, 이러한 ESM을 1단계 ESM이라 하고, ESM은 다음과 같은 구조를 가진다.

2단계의 ESM에서는 이러한 데이터의 대규모 발생으로 분석이 불가능했던 1단계 ESM에서 보다 발전하여, 보안정보(이벤트)간 연계분석, 상관관계 분석, 분석결과의 전파와 대응을 수행하고 있지만, 역시 아직은 많은 양의 데이타와 분석 근거 부족으로 즉각적인 침해사고 대응, 공격 평가, 조기 예/경보 등 대응은 신경쓰지 못하고 있다.

3단계에서는 아직 제품은 출시되지 않고 있지만 데이타 마이닝(Data Mining) 등을 통한 정보 상관분석, 침해사고 분석 시스템 구축, 사고 예방기능 강화, 블랙리스트에 기반한 공격 대응 등을 목표로 하고, 필요시 시스템적인 조기 경보와 대형 관제센타간에 실시간 정보공유가 필요한 조기경보네트웍(Early Warning Contact Network)이 구축되어 제공되어야 한다.

호스트별로 법적인 문제가 되는 침해사고로 판명되었거나 그러한 의심이 가는 정보의 증거 확보 및 관리를 수행하며 구체적인 필드로는 침해사고 발생 일시, 발견자 이름, 침해사고로 인한 피해결과, 예상되는 피해결과 등이 있을 수 있으며, 구체적인 증거로서 침입방지시스템(Firewall) 또는 침입탐지 시스템(IDS System)의 로그, 파일 또는 메일에 첨부된 바이러스 파일 등이 함께 저장될 수 있다. 자동화된 침해사고 대응시스템에서의 디지털 증거 수집을 위한 시스템 구성은 아래그림과 같다.

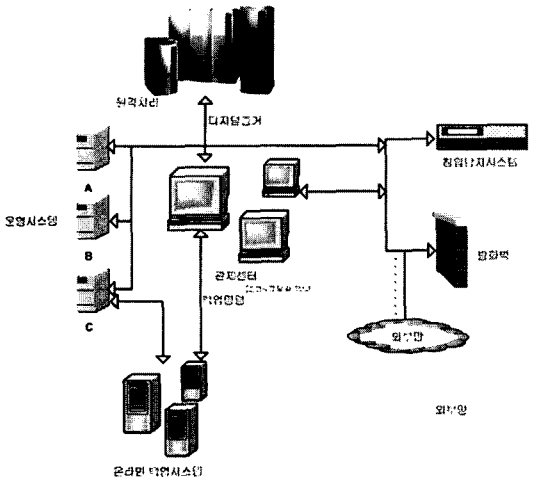


그림1-2. 백업 디지털 증거 수집 시스템

4. 결론

게임운영 및 각종서버를 이용하여 사업모델을 진행하는 환경에서 종합 침해사고 대응 시스템을 이용한 침해사고 대응방법은 1) 정보 수집/관리부가 소정의 통신망을 통하여 침해사고 및 취약성 정보와 같은 보안정보를 수집하는 정보 수집단계와 2) 정보 가공/관리부가 수집된 보안정보를 데이터베이스화하고 소정의 분석 알고리즘을 이용하여 분석하는 정보 가공/분석 단계와; 3) 가공/분석된 보안정보를 공유할 수 있도록 관리하고, 외부의 요청시 검색제공하는 정보 공유/검색/전파단계와; 4) 침해사고 및 취약성 정보 중 경보가 필요한 경우 소정의 조기 경보 정보를 하나 이상의 내/외부 시스템으로 전송하는 경보 단계로 이루어질 수 있다.

또한, 게임의 이용범위가 광범위하게 만들어지고, 소정의 시스템 자체 정보보호부를 이용하여 구축된 종합 침해사고 대응시스템의 자체 정보보호를 수행하는 단계(자체 정보보호 단계)와, 종합 침해사고 대응시스템이 발생한 정보 중 타기관과 공유하여야 하는 정보를 관리하고, 필요한 타기관 시스템으로 전송하는 타기관 공유 단계도 추가로 포함할 수 있다.

참고문헌

[1] 박상서, 박춘식, "정보전 개념과 주요 동향", 정보처리학회지 제10권 2호 pp. 47-57, 2003년 3월.

[2] 국가사이버안전센터. '2003년도 국내 전산망 침해사고 사례분석', 2004

[3] 정관진, 이희조, "인터넷 웜과 바이러스의 진화와 전망," 정보처리학회지 제10권 2호 pp. 27-37, 2003년 3월.

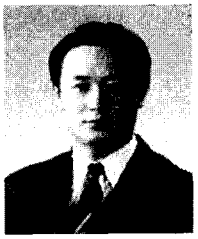
[4] Rik Rarrow, "Correlating Log File Entries", The Ohio State University Incident Response Team, The Magazine of Usenix & Sage, pp. 38-44, November, 2000.

[5] GAO, 'CRITICAL INFRASTRUCTURE PROTECTION, Establishing Effective Information Sharing with Infrastructure Sectors', 2004

[6] 이득춘, "ESM 동향 및 추세", 한국정보보호진흥원

신승중

1988년 8월 세종대학교 경영학과 석사
1994년 2월 건국대학교 전자계산학 석사
2000년 8월 국민대학교 정보관리학박사
1995년 3월 ~ 2003년 2월 중부대학교 정보보호학과 부교수
2003년 3월 ~ 한세대학교 IT학부 부교수
관심분야 : 정보보호, 이동통신, 게임공학, 네트워크보안, 유비쿼터스보안



최운호

1990년 광운대학교 학사
1995년 광운대학교 대학원 전자계산학과 이학석사
2001년 광운대학교 대학원 박사과정 수료
2005년 한세대학교 대학원 정보보호공학과 공학박사
1989 ~ 1996 한국전산원 선임연구원
1996 ~ 2001 한국정보보호진흥원 팀장
2001 ~ 2005. 8 금융결제원 금융ISAC실 팀장
관심분야 : 정보보호, 통신공학, 네트워크보안