정보전 대비 실시간 침입자 감지 및 경보 네트워크 구축방안

한국전자통신연구원 서동일 · 윤이중 · 조현숙

1. 서 론

20세기 전쟁 양상의 대표적인 특징은 대량파괴·살상에 의해 전쟁의 자원을 소모시키므로써 전쟁 당사국의 전쟁 수행능력을 박탈하였다는 점이다. 그러나, 21세기에 접어 들면서 이러한 대량파괴 및 살상에 의한 전쟁보다는 전쟁이 발발하기 전에 상대국의 전쟁 수행능력 자체를 무력화시키므로써 승리를 획득할 수 있는 정보전의 개념이 발달하게 되었다. 이러한 미래전의 핵심은 정보전(Information Warfare)에 있을 것이며, 특히 사이버상에 존재하는 주요 전략적 정보 시스템을 파괴·마비 시키므로써 전쟁 수행능력을 무력화 시키는 사이버 전쟁(Cyber Warfare)이 그 주축이 될 것이다.

정보전의 정의는 매우 다양하며, 1995년 Emmet Paige는 "우리의 정보와 시스템을 막는 동안에 적의 정보와 정보 시스템에 영향을 주어 국가적 군사 전략을 지지하여 정보 우월성을 성취하기 위해 취해진 행위들"이라고 말하였다. 또 다른 정의인 U.S. Air Force에 의하면 "적을 부인, 착취, 부패 또는 파괴시키는 어떤 행위"로서 그러한 행위들에 대해 우리 자신을 보호하는 것이다. 즉, 정보전은 정보를 파괴하고 정보 흐름과 정보 내용의 신뢰도를 감소시키고 서비스로의 접근을 부인하는 것이다. 또한, 보안 전문가인 Winn Schwartau는 다음과 같이 정의하였다[3]. "정보전은 기업들, 정치적 세력 범위, 광범위한 경제력, 또는 전 국가들과 싸우는 것이다. 기술에 대한 기술의 사용이다. 즉, 이것은 보안과 보안의 절도에 관한 것이다. 소유자에 대해 정보를 바꾸는 것이다. 기술과 정보를 사용할 수 있는 능력을 가진 적을 부인하는 것이다".

이와 같이 정보전은 전쟁 수행을 하기 위해 필요로 하는 각종 자원들에 대해 그 능력을 무력화 시키는 것을 말하며, 다음과 같은 여러 가지 형태로 실재하게 된다.

- Command and Control Warfare(명령과 통제전) : 군사 세계에서는 명령과 통제전이 가장 중요한 정보전의 한 축이 될 것이다.
- Intelligence based Warfare(지능기반 전쟁) : 지능 기반 전쟁은 정보전의 전통적인 구성요소이지만 정보전의 광대한 범위를 반영하기 위한 노력이 필요하다.
- Electronic Warfare(전자전) : 전자전은 군사 운영을 특성화한 정보전에서 고기술 요소이고, 전통적으로 전자기 스펙트럼(분포범위)에 대한 억제와 관련된다. 전자전은 전쟁의 다른 형태와 좀더 밀접하게 통합될 필요가 있다.
- Psychological Operations(심리전) : 심리적 작전(행동)은 정보전의 인간적인 면을 포함한다.
- Hacker Warfare(해커전) : 컴퓨터 해커들에 의해 자국의 정보를 보호함과 동시에 상대국의 정보 시스템 및 네트워크를 무력화 시키기 위한, 정보전의 대표적인 한 부분이다.
- Economic Information Warfare(경제정보전) : 경제적 정보전은 주식시장을 마비시키고 은행 계정을 공격하는 등의 사항을 포함한다.
- Cyber Warfare(사이버전) : 사이버전은 현재 현실적이거나 그렇지 않은 정보전의 요소를 모두 표현하며, 정보전의 핵심 부분이다. 넓은 의미의 사이버전에는 위에 언급하였던 각종 형태들

이 모두 포함된다고 볼 수 있다.

본 기고문에서는 위와 같이 다양한 형태로 전개될 수 있는 정보전에서 특히 해커전, 경제정보전, 사이버전에서 주로 활용할 수 있는 정보전 기술과 네트워크 침입자의 실시간 감지 및 경보 네트워크 구축에 관하여 제언하고자 한다.

제1장의 서론에 이어 제2장에서는 사이버 전쟁을 위한 기술 및 국내외의 동향을 알아보고, 제3장에서는 정보전을 대비하기 위한 국내의 실시간 침입자 감지 및 경보 네트워크 구축 방안을 제시하고, 제4장에서 결론 및 향후 연구방향을 이야기하고자 한다.

2. 정보전을 위한 기술 및 국내외 동향

이전의 전쟁에 비교해 볼 때, 정보전의 무기는 전투기, 탱크, 잠수함, 핵폭탄 등만으로 이루어진 것이 아니다. 새로운 전쟁의 형태와 함께 새로운 무기가 생겨나고 있으며, 여기에는 적의 전략적 시스템과 네트워크를 파괴·마비하기 위한 해킹 기술, 바이러스 기술, 해킹툴 이용 기술 등이 포함된다. 이러한 정보전을 위한 각종 기술 및 침입자 탐지 관련 국내외 동향을 알아보도록 한다.

2.1 해킹기술

적의 전략적 정보 시스템을 해킹하는 방법에는 매우 다양한 수법들이 존재하고 있으며, 여기에서는 대표적인 몇가지 수법에 대해서 간략히 알아보도록 한다. 이러한 방법들은 인터넷과 같은 민수용 네트워크를 사용하게 되는 미래 국방 네트워크에서 적용될 수 있다[7].

o 시스템의 환경 설정 변수를 이용 : 일반적으로 사용되고 있는 컴퓨터 시스템은 매우 다양한 운용체제를 가지고 있으며, 또한 다양한 사용자의 요구를 만족시키기 위하여 각 시스템 별로 환경 변수(environment variable)들을 이용하고 있다. 해커들은 바로 이러한 환경 설정 변수들이 잘못 설정되어 있는 경우 이를 이용하여 관리자의 권한을 획득하게 된다.

o 사용자 도용 : 웹 사이트 혹은 메일 서버와 같이 다수의 이용자가 존재하는 경우, 각각의 사용자들은 기본적으로 패스워드 방식을 통해 해당 시스템을 이용하게 된다. 이때 일부 사용자들은 패스워드를 손쉽게 기억하기 위하여 매우 단순한 방식으로 만드는 경우가 많으며, 해커들은 바로 이러한 사용자들의 아이디(ID)를 도용하여 해당 시스템을 해킹할 수 있게 된다.

o 경쟁조건(race condition)을 이용 : 유닉스 시스템에서는 한정된 자원을 여러 개의 프로세스들이 - 여러명의 사용자들이 공유하게 된다. 이렇게 한정된 자원들을 여러 객체들이 공유하여 사용하게 되므로 하나의 자원을 사용하려고 서로 경쟁하는 모양을 갖추게 되며, 이러한 현상을 이용하여 일반 사용자가 시스템의 관리자 권한을 획득할 수 있게 된다.

o 버퍼 오버플로우 취약점 이용 : Buff Overflow 공격이란 지정된 버퍼의 크기보다 더 많은 데이터를 입력하여 프로그램이 비정상적으로 동작하도록 만드는 것을 말한다. 이를 이용하여 해커는 공격하고자 하는 시스템을 파괴할 수도 있으며, 관리자의 권한을 획득하여 정보의 변조나 유출등을 시도할 수 있게 된다. 특히 이 기술은 1997년 Phrack 49호에 발표된 이후 해커들이 매우 자주 사용하는 공격 수법의 하나가 되고 있다.

o 네트워크 프로토콜의 취약점 이용 : 인터넷 통신 방식의 근간을 이루는 것은 TCP/IP 프로토콜이며, 인터넷의 최초 구성 이유가 정보의 공유에서 출발 되었듯이 본 프로토콜 또한 이러한 특성에 맞게 개방적인 구조를 이루고 있다. 따라서, 이러한 개방적인 구조를 이용하여 해킹하는 방법은 매우 다양하며, 대표적으로 IP Spoofing 공격, SYN Flooding 공격, 스니퍼링 공격, 서비스거부(DOS) 공격 등이 있다.

- 암호 스니퍼링(password sniffering) 공격 : 스니핑은 네트워크상에서 흘러다니는 정보를 가지고 사용자의 패스워드 등을 알아내는 공격 방법을 말한다. 이러한 공격 방법을 사용할 때에는 매우 다양한 해킹 툴들이 존재하므로 해커들은 손쉽게 공격 대상 컴퓨터의 사용자 아이디와 패스워드들을 획득할 수 있게 된다.

- IP Spoofing 공격 : 해커가 IP 주소를 도용하여 임의로 인터넷 프레임을 만들어 공격 대상 컴퓨터에 전송시키면, 목적지 컴퓨터는 해당 인터넷 프레임이 잘못 만들어진 것인지 아닌지를 판단할 수 없게 된다. 이를 이용한 공격 방법이 IP Spoofing 공격이다.

- SYN Flooding 공격 : 인터넷의 주요 프로토콜 중 하나인 TCP(Transmission Control Protocol) 프로토콜은 연결 지향 전송을 제공하므로, 연결 설정 과정을 3-way handshaking이라는 방법을 사용하여 두 컴퓨터 시스템을 연결하게 된다. SYN Flooding 공격은 이러한 연결 방식의 취약점을 이용하는 것이다.

- ICMP(Internet Control Message Protocol) 이용 : 인터넷 프로토콜은 비신뢰성, 비연결 지향 전송을 제공하는 통신 규약이다. 이러한 통신 방식에 있어서는 전송되고 있는 패킷이 어떤 사유로 인해 목적지에 도착할 수 없는 경우 해당 패킷을 전송하는 시스템에서는 이를 알아 낼 수가 없다. 이러한 단점을 어느 정도 해소 시켜 주기 위해 인터넷에서는 에러 정보를 상호 교환해 주는 ICMP 프로토콜을 사용하는데 이를 이용한 공격법이 ICMP Echo Reply 공격 등이 있다.

- 라우팅 프로토콜 이용 : 인터넷에서는 전송하고자 하는 패킷의 경로를 알기 위해 여러가지 라우팅 프로토콜을 사용하고 있으며, 이때 거짓된 라우팅 정보를 전달하여 해커가 의도하는 컴퓨터로 중요한 정보 등을 전송하게 만들 수 있다.

- DOS(Denial of Service) 공격 : 유닉스 시스템과 같은 다중 작업을 지원하는 운영체제에서는 하나의 프로세스가 시스템의 자원을 독점하거나 모두 사용해 버린다면, 다른 프로세스들이 정상적인 서비스를 수행하지 못하게 된다. 바로 이러한 점을 악용하는 것이 서비스거부 공격이다. 서비스거부 공격은 관리자의 권한을 획득하거나 혹은 데이터를 파괴, 절취하기 위한 공격이 아니며, 해커가 공격하고자 하는 시스템이 정상적인 서비스를 수행하지 못하도록 방해하는 공격 방법이다. 이러한 공격법은 최근 급격히 증가하고 있는 전자상거래를 직접적으로 위협하는 것이며, 매우 다양한 공격 방법들이 가능하기 때문에 공격의 원인이나 공격자를 추적하기가 매우 힘들고 또한 공격을 당하고 있는 것을 감지 하더래도 이를 해결하기가 어렵다는 특징을 가진다.

o 응용 S/W의 보안 오류 이용 : 인터넷에서 누구나 손쉽게 설치하여 사용할 수 있는 FTP,Telnet, SendMail, Web 프로그램과 같은 각종 응용 프로그램들의 버그(bug)를 이용하여 공격하는 방법이다.

2.2 바이러스 기술

정보전을 위한 공격기술의 큰 축을 형성하고 있는 바이러스 유포에 의한 컴퓨터 시스템의 파괴, 데이터의 위변조 등도 매우 다양한 수법들이 존재하고 있다 [7].

이들은 감염 방법에 따라 원래의 프로그램을 파괴하지 않고 프로그램의 앞이나 뒤에 바이러스 프로그램이 추가되는 기생형(대부분의 바이러스 유형임), 원래의 프로그램이 있는 곳에 바이러스 프로그램이 겹쳐져서 위치하는 겹쳐쓰기형(Leprosy Virus, Lehigh Virus 등), EXE 파일에 직접 감염되지 않고 같은 이름의 COM 파일을 만들어 여기에 바이러스 프로그램을 넣어두는 산란형(AIDS II Virus 등), 프로그램에 직접 감염되는 것이 아니라 디렉토리 영역에 프로그램 시작 위치를 바이러스 프로그램의 시작 위치로 바꾸어 줌으로써 컴퓨터 바이러스로서의 동작을 수행하게 하는 연결형(DIR-II Virus, Byway Virus 등), 윈도우 상에서 사용되는 마이크로소프트 제품의 매크로 기능을 이용하는 매크로형 등으로 구분할 수 있다.

운용체계에 따라서 분류하면 대부분의 바이러스가 속해있는 도스 바이러스, Win95/CIH, Anxiety_Poppy, Win3.1 Virus, Win32 Virus와 같이 윈도우 시스템에서 동작되는 바이러스, 애플리케이션에 내장된 매크로 혹은 스크립트 언어를 사용하여 제작된 바이러스로서 운용체제와 상관없이 해당 응용 프로그램을 플랫폼으로 하여 동작되는 애플리케이션 파생 바이러스, Linux/Bliss 등과 같은 리눅스 바이러스, Java 언어를 기반으로 하여 동작되는 자바 바이러스 등으로 구분할 수도 있다.

감염 부위에 따라 분류하면 Brain, Monkey 등과 같이 부트 섹터에 자리잡는 부트 바이러스(Boot Virus), 예루살렘, Sunday, Crow, Win 95/CIH 바이러스와 같이 실행 가능한 프로그램에 감염되는 파일 바이러스(File Virus), Invader, Euthanasia, Ebola 바이러스 처럼 부트 섹터와 파일에 모두 감염되는 부트/파일 바이러스(Multipartite Virus), 감염대상이 실행 파일이 아니라 마이크로 소프트사의 액셀과 워드 프

로그램에서 사용하는 문서 파일에 감염되는 매크로 바이러스(Macro Virus) 등으로 구분 가능하다.

최근에는 네트워크와 연결된 컴퓨터의 주소록을 이용하여 순식간에 전세계에 E-mail을 통하여 감염시키는 웜 바이러스나 시스템 내부에 잠복해 있다가 특정한 요일 혹은 특정한 조건하에서 동작하는 트로이 목마와 같은 지능형 바이러스가 점차적으로 증대되고 있다.

2.3 해킹툴(Hacking Tools)

보안강화도구(해킹툴)란 원래 시스템의 관리자들에게 시스템의 보안 수준을 높여줄 수 있는 편리한 도구로써 제공되어지던 것이였으나, 해커들에 의해 이러한 도구들이 악용되므로써 해킹의 주요 수단으로 발전되고 있는 추세이다. 또한, 이러한 툴들은 인터넷을 통하여 매우 손쉽게 구할 수 있는 것이며, 이로 인해 초보 해커들이 양성되는 문제점을 가지게 된다. 여기에서는 이러한 해킹툴 중에서도 대표적인 몇가지 도구들을 살펴보도록 한다[5].

o 내부 점검 도구

- COPS(Computer Oracle and Password System) : COPS는 유닉스 보안과 관련된 여러가지 프로그램들을 수집하여 하나의 패키지 형태로 제공하는 보안 점검 도구이다. 해커들은 이를 이용하여 시스템의 각종 파일 및 디렉토리들의 권한, 예측 가능한 패스워드, 관리자의 권한으로 수행 가능한 파일, 몇가지 시스템 설정의 문제점 등을 알아낼 수가 있으며, 이를 이용하여 다음 단계의 해킹 작업을 수행하게 된다.

- Tiger : COPS 도구와 유사한 형태의 보안 점검 도구이며, 메일 스풀(mail spool) 디렉토리 검사, 시스템 파일의 권한 조사, 몇가지 시스템 설정 조사, 관리자의 권한으로 수행 가능한 파일 등을 조사하여 알려주는 도구이다.

- Tripwire : 본 도구는 시스템에 존재하는 파일들의 정보를 데이터베이스화하며 이를 바탕으로 하여 파일의 내용이 변경되었을 때 시스템 관리자가 알 수 있도록 도와 주는 도구이다. 그러나, 해커들은 이러한 특징을 이용하여 자신이 해킹한 시스템에서 본인을 은닉화시키기 위한 도구로써 사용하고 있다.

o 패스워드 점검 도구

- 패스워드 점검 도구에는 사용자들의 패스워드를 여러가지 규칙과 많은 단어를 포함하고 있는 사전을 조합하여 알아내 주는 crack 프로그램, John 프로그램, L0phtCrack 프로그램 등이 있다. 원래 이러한 패스워드 점검 도구도 시스템 관리자들에게 관리하고 있는 사용자들의 패스워드를 좀더 강화시키도록 권고할 수 있도록 하기 위해 제공되었으나 이를 악용하여 해킹에 사용하고 있는 것이다.

o 보안 취약점 스캐너 도구

- ISS(Internet Security Scanner) : 한 시스템에 대해 지금까지 알려진 여러가지 보안상의 취약점을 점검해 주고 이를 수정할 수 있는 방법을 관리자에게 알려주는 도구이며, 해커들은 이를 이용하여 공격하고자 하는 시스템의 취약점을 손쉽게 알아 낼 수가 있게 된다.

- SAINT(Security Administrators Integrated Network Tool) : ISS와 마찬가지로 여러가지 알려진 보안 취약점들을 점검하여 위험의 정도를 관리자에게 상세히 알려주는 도구이다. 특히, 본 도구는 원격지에 있는 시스템의 finger, NFS, NIS, ftp, tftp, statd 등의 서비스를 검사하여 잠재적인 문제점들을 보고해 주기 때문에 관리자에게 매우 유용하게 사용될 수 있는 도구이다.

- SATAN(System Administrator Tool for Analyzing Network) : 이 프로그램도 ISS와 마찬가지로 각종 시스템의 취약점을 분석하여 보고해 주는 도구로써 원격지 시스템도 검사할 수 있다.

- Nmap and Xnmap : 원격지에서 목표 시스템이 제공하고 있는 서비스 포트들이 무엇인지를 알려주는 도구이다. 현재 가장 많이 사용되고 있는 스캐닝 도구의 하나이다.

- Sscan and mscan : 리눅스에서 동작되는 네트워크 보안 취약점 점검 도구이다. 특히, sscan은 mscan의 후속 버전으로 분석할 수 있는 취약점의 수가 매우 많아 nmap과 함께 가장 많은 사용자층을 가지고 있는 해킹툴이다.

- Shadow Scan : 그래픽 사용자 인터페이스를 갖고 있는 매우 뛰어난 윈도우 기반의 스캐닝 도구이다. 이를 통해 ping, port scanner, site

information, network port scanner, proxy scanner, tracerouter, telnet, nslookup, DNS information, netstat , finger, echo 등의 일반적인 유닉스 명령어들을 사용하여 다양한 목표 시스템의 정보들을 획득 할 수 있게 되어 있다.

o 모니터링 도구

- Tcpdump : 네트워크 인터페이스 상에 있는 패킷 중에서 목표로 하는 패킷만을 추출하여 해당 패킷의 헤더 정보를 보여주는 도구이다.

- Sniffit : 해킹 기술중 스니퍼링 공격시 사용할 수 있는 도구로써, 패킷이 가지고 있는 데이터의 내용을 보여주는 도구이다.

- Snoop : tcpdump와 같이 이더넷에 현재 전송되고 있는 각종 패킷들을 분석하여 보여주는 도구이다.

2.4 인터넷 보안그룹 활동 현황

인터넷에 관한 표준을 정하는 조직인 IETF (Internet Engineering Task Force)에서는 인터넷 보안 분야에 관하여 2000년 10월 현재 다음과 같은 20개 워킹그룹을 결성하여 각종 표준을 제정하고 있다[6]. 이는 인터넷이 최초 탄생시 개방 지향적이였기 때문에 가지고 있는 기본적인 보안 취약성이 크므로 이를 보완하기 위한 것이다[10].

• An Open Specification for Pretty Good Privacy(openpgp) : PGP 알고리즘 연구

• Authenticated Firewall Traversal(aft) : 방화벽 연구

• Common Authentication Technology (cat) : 공통 인증 기술

• IP Security Policy(ipsp) : 정책기반 보안기술

• IP Security Protocol(ipsec) : IP 보안 알고리즘

• IP Security Remote Access(ipsra) : IP 원격접속 연구

• Intrusion Detection Exchange Format (idwg) : 서로다른 침입탐지 시스템들 사이의 정보교환을 위한 교환절차 및 Data 규격을 제정하기 위한 연구

• Kerberized Internet Negotiation of Keys (kink) : 키관리 기술

• Kerberos WG(krb-wg) : Kerberos 알고리즘

• One Time Password Authentication(otp) : 일회용 패스워드 인증

• Public-Key Infrastructure (X.509)(pkix) : 공개키기반 인증

• S/MIME Mail Security(smime) : 안전한 e-mail 전송

• Secure Network Time Protocol(stime) : 안전한 네트워크 타임 프로토콜

• Secure Shell(secsh) : 안전한 쉘 프로그램

• Securely Available Credentials(sacred) :

• Security Issues in Network Event Logging(syslog) : 안전한 로깅기술

• Simple Public Key Infrastructure(spki) : 간단한 공개키기반 인증

• Transport Layer Security(tls) : 안전한 전송계층

• Web Transaction Security(wts) : 웹보안

• XML Digital Signatures(xmldsig) : 디지털 서명기술

2.5 미국의 대응 현황

미국은 연방정부 차원에서 주요 컴퓨터 시스템을 정보전(사이버 공격)으로부터 보호하기 위한 업무를 추진하고 있으며, 1998년 PCCIP(President's Commission on Critical Infrastructure Protection)와 CIAO(Critical Infrastructure Assurance Office)를 중심으로 중요 정보통신 기반구조 보호를 위한 연구 개발 계획을 발표하여 실행하고 있다. 이를 위해 2000년 1월 국가 주요 기반구조 보호(CIP : Critical Infrastructure Protection)를 위한 국가 차원의 계획(National Plan)을 발표하였으며, DARPA (Defense Advanced Research Project Agency)에서는 정보보증 및 생존(Information Assurance & Survivability : IA&S) 프로그램을 진행하고 있다.

미국은 CIP를 위해 달성하여야 할 목표를 3가지로 나타내고 있으며, 이를 위한 구체적인 10개의 프로그램을 제시하고 있다. 첫번째 목표는 준비 및 예방(Prepare and Prevent)으로서 프로그램 1(보호 대상과 상호 의존성 파악 및 취약성

평가)을 통해 미국의 주요 정보 네트워크에 대한 명백한 공격 가능성을 최소화하고, 공격을 당하더라도 지속적으로 운영될 수 있는 기반구조를 구축하는 것이다. 두번째 목표는 탐지 및 대응(Detect and Respond)으로서 프로그램 2~5(공격 및 침입 탐지, 첩보/법적 대응 능력 확보, 경보 및 정보공유, 대응/재구성 및 복구능력 확보)를 통해 미국의 주요 기반구조에 대한 공격을 즉각적으로 식별하고 평가하는 데 필요한 수단을 개발하는 것이며, 피해 복구와 피해 시스템을 재구축하는 것이다. 세번째 목표는 강력한 기반을 구축(Build Strong Foundations)하는 것으로서 프로그램 6~10(연구개발, 전문가 확보, 홍보, 법률적 지원, 개인의 권리와 사생활 보호)을 통해 미국의 주요 정보 네트워크에 대한 공격에 대비하기 위한 준비 및 예방, 탐지 및 대응을 수행하는데 기반이 되는 국가적 차원의 활동을 수행하는 것이다[8].

또한, 군사적으로는 2000년 10월 우주 사령부에 "사이버전쟁" 담당 부서를 신설하여 유사시 미국의 컴퓨터 시스템과 네트워크를 보호하고, 적국의 컴퓨터망을 공격하는 작전을 담당하도록 하였다. 기술개발에 있어서는 전략적 사이버 방어를 위해 IA&S 프로그램을 통해 6가지 영역에 걸친 총 8가지 연구개발 프로그램을 2003년 완료 예정으로 실행하고 있다. 6가지 영역에는 정보보증 과학 및 공학(Information Assurance Science & Engineering), 사이버 센서 및 이용(Cyber Sensors & Exploitation), 사이버 상황인지(Cyber Situation Awareness), 사이버 지휘 통제(Cyber Command & Control), 방어 메커니즘(Defensive Mechanisms), 사이버 방어 전략(Cyber Defense Strategy)이 있으며, 8가지 연구개발 프로그램은 전략적 침입 평가 (Strategic Intrusion Assessment), 침입 감내 시스템(Intrusion Tolerant Systems), 고장 감내 네트워크(Fault Tolerant Networks), 동적 연립(Dynamic Coalitions), 정보보증(Information Assurance), 정보보증 과학 및 공학 툴 (Information Assurance Science and Engineering Tools), 자율적 정보보증(Autonomic Information Assurance), 사이버 지휘 통제(Cyber Command and Control)를 말한다[9].

특히, 미국은 사이버 공격에 대한 감시기능을 갖는 연방차원의 FIDnet(Federal Intrusion Detection Network)을 구축하고 있으며, 이는 기존의 전쟁 형태에서 이용되었던 조기경보체계와 비슷하게 주요 정보통신망에 침입자를 감지할 수 있는 수단을 제공하기 위한 것이다. 동시에 군사적인 목적으로 사용하기 위해 주요 국방 네트워크를 모니터링하고 침입 또는 공격을 당한 이후에 원래의 기능을 복원하기 위한 JTF-CND (DoD Joint Task Force - Computer Network Defense) 네트워크를 구축하여 운영하고 있다.

2.6 국내의 대응 현황

국내에서는 미래 정보전에 대비하기 위한 기술개발을 추진하기 위해 국방부에서 전략적 추진체계를 형상화하고 있는 단계이며, 그 실적은 아직은 매우 미미한 수준이다. 그러나, 정보전에 이용될 수 있는 정보화역기능 방지기술 개발은 2000년 7월부터 한국전자통신연구원(ETRI) 및 한국정보보호센터(KISA)를 중심으로 2002년 12월 완료 예정으로 일부 시행되고 있다.

특히, 국내의 보안 산업은 침입차단시스템(Firewall)과 항바이러스(Anti-Virus)를 중심으로 발전하고 있으며, 몇몇 산업체에 의해 동남아시아를 중심으로 해외 수출도 이루어지고 있다. 또한, 올해 들어 PKI(Public Key Infrastructure)와 침입탐지시스템(Intrusion Detection System)쪽의 개발이 활발하게 이루어지고 있다.

그러나, 미래 정보전에 대비하기 위한 기본적인 기반시설인 실시간 침입자 탐지 및 경보 네트워크 구축은 아직까지 이루어지지 않고 있으며, 이는 사이버전쟁 발발시 즉각적인 탐지 및 경보의 미비로 인한 대규모 피해가 발생될 우려가 높은 현실이다.

3. 실시간 침입자 감지 및 경보 네트워크 구축

미래 정보전(사이버전쟁)을 위해 국가적인 관점에서 기본적으로 진행하여야 하는 첫번째 사업은 침입자를 실시간으로 감지하고 이를 관련 기관에 신속히 경보할 수 있는 '실시간 침입자 감지 및 경보 네트워크'를 구축하는 것이다. 본 장

에서는 침입감지시스템 및 경보시스템이란 무엇이며, 어떠한 기능을 담당하여야 하고 어떻게 구축되어야 할 지를 알아보도록 한다.

3.1 침입탐지시스템 및 경보 네트워크

침입감지 혹은 탐지 시스템이란 대상 시스템에 대한 비인가된 행위 혹은 비정상적인 행동을 탐지하고 구별하며 이에 대응하는 기능을 가진 시스템이라고 정의할 수 있다. 즉, 컴퓨터 시스템의 비정상적인 사용이나 오용, 남용 등을 탐지하는 시스템이다.

이러한 침입탐지 시스템은 침입차단시스템(FireWall, 방화벽) 만으로는 내부 사용자의 불법적인 행위와 외부 해킹에 대해 근본적인 대처가 불가능하기 때문에 이를 보완하기 위해 사용된다. 또한, 해커들의 침입패턴에 대해 이를 차단하고 역으로 이들을 추적하기 위해서도 필요한 시스템이다.

IDS(Intrusion Detection System)는 일반적으로 모니터링의 대상에 따라 네트워크 기반 IDS, 호스트기반 IDS로 나뉘어지며 최근에는 이 두 가지 방식을 혼합한 하이브리드 방식의 IDS가 연구 개발되고 있다. 또한, 침입자의 탐지 방법에 따라 비정상탐지(Anomaly Based Detection) IDS, 오용탐지(Misuse Based Detection) IDS 로도 나뉘어 진다. 이러한 분류 방법들에 의한 기술개발은 점차적으로 어느 한 가지 분야에 의한 독자적인 동작 보다는 여러 가지 방법들을 통합하여 실행되는 방법으로 변화되고 있는 추세이다.

이러한 침입탐지시스템의 장점으로는 다음과 같은 것들이 있다.

- 해킹 패턴을 미리 데이터베이스화 한 후 이를 기반으로 해커의 침입을 탐지하므로 해킹 신기술의 적용이 빠르다.
- 외부로 부터의 사이버 공격뿐만 아니라 내부자에 의한 해킹도 어느 정도 차단할 수 있다.
- 침입차단시스템(FireWall)과는 달리 해킹 패턴에 따른 즉각적인 대응이 가능하다.
- 침입자의 탐지뿐만이 아니라 해커를 역추적할 수도 있으므로, 수동적인 침입차단시스템과는 달리 적극적인 대응이 가능하다.
- 기존의 침입차단시스템이 인증된 IP 주소를 갖고 침입하는 경우 이를 차단할 수 없었으나, IDS는 접속하는 IP에 상관없이 모든 패킷에 대해 검사를 수행하므로 인증된 IP 주소를 갖는 공격자에 대해서는 안전하게 방어할 수 있다.

근거리통신망(LAN)과 같은 소규모 네트워크에서는 한 두개의 침입탐지시스템으로 충분히 그 역할을 수행할 수 있으나, 국가적인 대규모 네트워크나 이들을 통합한 주요정보통신 기반망에 대한 침입탐지는 한 두 개의 침입탐지시스템이 동작되고 있다고 해서 사이버공격에 대해 탐지할 수 있는 게 아니다. 따라서, 국방 네트워크와 같이 대규모적인 네트워크에서는 수백여대의 침입탐지 모니터링 시스템을 구축하고 이들을 상호 연관시켜 통합적으로 관리할 수 있는 시스템 구축이 절실히 필요하게 된다.

또한, 이러한 침입탐지시스템의 통합관리와 함께 침입 정보를 정확히 필요로 하는 기관 및 알려주어야 할 기관에 이를 통보하기 위한 경보 네트워크 또한 구축되어야 한다.

3.2 기관별 네트워크 구축 방안

국가적인 침입탐지시스템 및 경보 네트워크를 구축하기 위해서는 먼저 각각의 소규모 네트워크를 구축 운영하고 있는 각각의 기관별 침입탐지 네트워크가 구축되어야 한다.

각 기관별 네트워크에는 다음과 같은 기능이 운용되어야 하며, 운용된 결과를 중앙 분석 시스템으로 통보할 수 있는 적절한 경보 네트워크 또한 구축되어야 한다.

- 인가된 사용자의 접근 및 행동규칙과 인가된 사용자의 비정상적인 행동을 식별할 수 있는 능력이 구비되어야 한다.
- 침입차단시스템(방화벽)과 함께 설치되어 운용되어야 한다.
- 네트워크에 연결되어 있는 시스템을 식별할 수 있고, 그 시스템이 어떠한 일을 하고 있는지 판단할 수 있으며, 접근 및 행동 규칙을 파악할 수 있고, 보안등급을 조절할 수 있는 능력을 갖춘 기관 차원의 관리 프로그램이 동작되고 있어야 한다.
- 악성 코드를 식별, 분석할 수 있는 기능이 있어야 한다.

위와 같은 기능을 포함하여 소규모 네트워크에

대한 침입탐지시스템 및 경보 네트워크를 구축한 후, 이를 통해 의심스러운 행위 및 동작 등에 대한 감시 및 모니터링을 실시하게 된다. 또한, 수집된 정보들은 실시간으로 중앙분석시스템으로 전송하게 되며 여기에서는 국가적인 차원의 침입자 감지 및 경보 기능이 수행되어야 할 것이다.

3.3 국가적인 네트워크 구축 방안

각 기관차원의 소규모 침입자 감지 및 경보 네트워크의 구축이 완료되면, 이를 통해 수집된 정보들을 분석하고 대응하기 위한 국가적인 차원의 침입자 감지 및 경보 네트워크의 구축이 실시되어야 한다.

즉, 기관 차원의 침입탐지시스템에서 수집된 정보들이 NIDC(National Intrusion Detection Center)와 같은 중앙 부서에 통합 수집되어 이들을 실시간으로 분석하도록 한다. 이를 통해 각 기관에 대한 사이버 공격과 인가되지 않은 침입을 탐지하고 분석하며, 이들 기관들 사이의 공격 경보 및 관련 정보를 공유하게 되고, 이러한 공격에 대한 대응을 통합적으로 수행하게 된다. 또한, 침입자에 대한 역추적이 기관 차원의 소규모 네트워크를 통해서는 불가능하게 되나, 중앙 집중화된 NIDC에서는 분석된 정보를 기반으로 하여 공격자를 역추적할 수 있게 된다.

미래 정보전을 위해서는 국가기반통신망과 같은 대규모 네트워크를 위한 침입자탐지 시스템 구축과 동시에 분석된 침입패턴 정보 및 역추적 결과등을 실시간으로 필요 기관에 분배할 수 있는 경보 네트워크 또한 국가적인 차원에서 구축되어야 한다. 이를 위해서는 실시간 침입탐지 및 역추적을 위한 NIDC와 같은 중앙 기관 이외에, ISAC(Information Sharing and Analysis Center)과 같은 정보 공유 및 분석, 분배 기관이 필요할 것이다.

4. 결론 및 향후 연구방향

미래 전쟁의 형태는 대량 파괴·살상에서 전쟁 수행능력의 무력화를 시도하는 정보전 형태로 발전하게 될 것으로 분석되고 있다. 이러한 정보전은 다양한 형태로 발생할 수 있으며, 특히 사이버상에서 상대국의 주요 정보통신기반망의 무력화를 시도하는 해킹 공격이나 바이러스 유포 공격등은 공격에 따른 영향력이 매우 크기 때문에 이에 대한 올바른 대처가 절실히 필요로 할 것이다. 따라서, 이와 같은 사이버전쟁시 침입자를 실시간으로 탐지하고 이를 관련된 기관에 경보할 수 있는 네트워크의 구축은 매우 절실히 요구되는 사항이라 할 것이다.

본 기고문에서는 현 단계의 사이버 전쟁에서 이용할 수 있는 각종 해킹 기술, 바이러스 기술, 해킹툴 이용기술들을 알아 보았으며, 미래 정보전을 위한 국내외 기술개발 현황에 대해 간략히 분석하여 보았다. 이를 기반으로 하여 현재 국가적으로 미래 정보전을 대비하여 반드시 구축하여야 할 '실시간 침입자 감지 및 경보 네트워크' 구축 방안을 제언하였다.

그러나, 현재 국내에서는 미래 정보전에 대한 심도있는 연구가 진행되지 않아 국외 선진국들에 비해 기술 수준이 현저히 낮으며 대응 체계도 갖추어져 있지 않다. 이는 국가의 존속에 많은 영향을 미칠 수 있기 때문에 국내에서도 정보전에 대한 체계적인 전략 수립과 함께 다음과 같은 추가적인 연구개발이 절실히 요구된다 할 것이다.

- 미래 정보전 대비 기술의 개발 전략 수립
- 국방망의 정보전 대비 상호 의존성 분석
- 사이버 데프콘 발령 및 모델링 기술
- 시스템 및 네트워크의 신뢰성 및 생존성 보장기술
- 실시간 침입자 탐지, 감시, 역추적 및 경보 네트워크 구축
- 정보전을 위한 전술형 사이버 공격기술 및 도구 개발
- 전장정보 가시화를 위한 지능형 센서 네트워크 기술
- 국방망의 통합 및 분산 관리 시스템
- 정보전을 위한 법적 제도적 지원
- 정보전을 위한 인력 양성 및 교육, 홍보

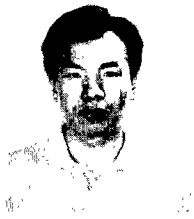
참고문헌

[1] Peter Sommer, "Intrusion detection systems as evidence", Computer Networks 31 (1999), pp 2477 - 2487.

[2] Robert Graham, "FAQ: Network Intrusion Detection Systems", http://www.

robertgraham.com/pubs/network-intrusion-detection.html, Version 0.8.3, 2000. 3. 21.
[3] Winn Schwartau, Information Warfare, 2nd Edition, Thunder's Mouth Press, 1996.
[4] James Adams, The Next World War : Computers Are the Weapons and the Front Line is Everywhere, Simon & Schuster, 1998.
[5] 포항공대 유닉스 보안연구회, Security PLUS for UNIX, Youngjin.com, 2000.
[6] http://www.ietf.org/html.charters/wg-dir.html#Security_Area.
[7] 서동일, 윤이중, 조현숙, "사이버테러 기술 및 대응방안의 현황분석", Telecommunications Review, 제10권5호, 2000년 10월.
[8] CIAO, National Plan for Information Systems Protection, Version 1.0 : An Invitation to a Dialogue, 2000.1.
[9] http://www.darpa.mil/
[10] 서동일, 강훈, "인터넷 보안기술 동향 분석", 주간기술동향, 96-34호, 1996년 9월 4일.

서 동 일



1989. 2 경북대학교 전자공학과(학사)
1994. 2 포항공과대학교 정보통신학과(석사)
2000 충북대학교 전산학과(박사과정)
1989. 1~1992. 2 삼성전자 종합연구소
1994. 3~현재 한국전자통신연구원 사이버테러기술분석팀장
관심분야:Network Security, Hacking, 인터넷정보보호
E-mail:bluesea@etri.re.kr

윤 이 중

1988. 2 인하대학교 전산학과(학사)
1990. 2 인하대학교 전산학과(석사)
1997. 3~현재 충남대학교 컴퓨터과학과(박사과정)
1990. 2~현재 한국전자통신연구원 정보보호시스템연구부장
관심분야:유무선 PKI, Secure OS, 인터넷정보보호
E-mail:yej@etri.re.kr

조 현 숙

1979. 2 전남대학교 수학과졸업(학사)
1991. 2 충북대학교 전산학과 졸업(석사)
2000 충북대학교 전산학과(박사과정 수료)
1982. 3~현재 한국전자통신연구원 책임연구원 정보보호기술연구본부장
관심분야:Network Security, Conditional Access System
E-mail:hscho@etri.re.kr