情 報 保 護 學 會 誌
第 12 券 第 6 號, 2002. 12

정보전 기술과 개발 현황

서 동 일*, 손 승 원*, 조 현 숙*, 이 상 호**

요 약

21세기를 흔히 지식정보화 사회라고 한다. 이는 20세기 산업사회가 자본과 노동력을 기반으로 발전된 것에 비해, 21세기에는 지식과 정보가 주요한 생산요소로 작용하고 있음을 의미한다. 따라서 전쟁의 주요도구들도 농경사회의 창과 칼, 산업사회의 탱크, 비행기, 총포등에서 이제는 정보지식과 기술이 사용되기 시작하였다. 또한, 정보지식 사회로 발전할수록 정보 인프라 의존도는 급격히 늘어나기 때문에 컴퓨터나 네트워크와 같은 정보통신 기반체계에 대한 공격은 국가 사회의 존립을 좌우할 수 있는 매우 중차대한 문제로 부상하고 있다. 본 기고문에서는 이러한 혁신적인 정보지식 사회의 전쟁 패러다임의 변화를 수용하기 위한 여러 가지 공격기술과 방어기술에 대한 최근의 경향과 함께 국내외 기술 개발 현황에 대해서 알아보고자 한다.

Ⅰ. 서 론

21세기 지식 정보화 사회의 기반이 되는 인터넷은 정보전을 위한 가장 기본적인 공격대상이 되고 있으며, 정보전 기술 개발의 핵심 축을 이루고 있다 해도 과언이 아닐 것이다.

특히, 21세기 들어 오면서 기존의 모든 네트워크 환경은 "인터넷(Internet)"으로 통합되어 상호 연동이 가능하게 되었으며, 이를 통해 실 생활에서 발생할 수 있는 각종 업무들을 수행할 수 있게 되었다. 또한, 지난 20세기 후반에 나타난 "가상사회"라는 개념은 "보다 안전한 가상사회" 라는 개념으로 발전하고 있다. 이는 기존의 인터넷 환경에서 공.사적인 업무를 볼 수 있게 되고, 개인 혹은 공적인 주요 정보들이 인터넷을 통해 전달되면서 이들을 보다 안전하게 사용할 수 있는 환경을 요구하게 되었기 때문이다.

사이버 공간에서의 사이버테러(혹은 정보전)을 유발시키는 일반적인 특징으로는 첫째, 인터넷이 비대면성을 가진다는 점이다. 사이버 공간은 컴퓨터를 이용하여 형성되는 생활 공간으로서 불가시적이므로 현실세계와는 달리 행위자들이 자신의 얼굴을 드러내지 않고 행동 할 수 있다는 특징을 갖고 있다. 이러한 비대면성으로 인하여 피해자는 행위자를 거의 알 수 없어 범인파악이 어렵게 되고 피해의식이나 공포감이 훨씬 커지게 되는 취약성을 가지게 된다. 또한, 이러한 특징에 의해 실제 전장에서의 행위보다도 매우 손쉽게 사이버 공간에서의 정보전이 이루어질 수 있는 것이다. 두번째 특징으로는 첫번째 특징과 연관되어 사이버 공간에서의 익명성 보장에 있다. 즉, 사이버 공간에서는 자신의 신분을 노출 시키지 않은 채 활동하는 것이 가능하다는 점이다. 이처럼 자신을 숨길 수 있는 익명성이 보장되므로 사이버 공간에서는 여러가지 범죄에의 유혹에 쉽게 빠져들 수 있게 되며, 또한 수사기관이 범죄자를 적발해 내는데 많은 어려움을 겪게 되는 주 원인이 되는 것이다. 세번째로는 사이버테러를 유발시키는 범죄자들은 매우 높은 전문성과 기술성을 보유하고 있는 경우가 대부분이라는 점이다. 네번째 특징으로는 사이버 공간이 시간적 공간적으로 제한을 받지 않는 시공초월성을 갖는다는 점이다. 따라서, 누구든지 마음만 먹으면 인터넷을 24시간 내내 이용할 수 있으며, 별다른 어려움 없이 세계 어느 곳과도 접속할 수 있게 되는 것이다. 마지막으로 사이버 공간에서는 시간과 장소의 제약을 뛰어 넘어 모든 정보들이 매우 빠르게 집약되고 전파되며, 그 피해 역시 추산하기 어려울 정도로 매우 광범위하게 미치게 된다는 점이다. 이는 인터넷 환경이 개방성을 기반으로 설

* 한국전자통신연구원 ({bluesea, swsohn, hscho}@etri.re.kr)

계되어 있어 전문적인 사이버테러를 위한 기술 정보에 매우 손쉽게 접근할 수 있기 때문이다. 이처럼 인터넷은 사이버테러(혹은 정보전)가 발생될 수 있는 소지가 매우 큰 취약한 네트워크이지만, 21세기 지식정보화 사회의 근간이 될 정도로 매우 광범위하게 사용되고 있으므로, 이를 보호할 수 있는 정보보호 기술의 연구는 매우 중요한 일이라 할 것이다.

본 기고문에서는 이처럼 중요항목으로 부각된 정보보호 기술에 대한 현황과 발전 경향에 대해 검토해 보고자 한다. 특히, 정보보호 기술 중에서 인터넷에 대한 정보전 공격 기술과 방어기술의 개발현황을 분석하고자 한다. 제2장에서 정보전의 일반적인 개념에 대해 알아보고, 제3장에서 정보전 공격기술로 활용 가능한 기존의 사이버테러 기술 (특히, 해킹/바이러스 기술을 중심으로)을 알아본다. 제4장에서 정보전 방어기술로 활용 가능한 기존의 정보보호 기술의 현황과 차세대 정보보호 모델을 제시하고, 마지막으로 결론과 함께 추가적인 연구 항목에 대해 언급한다.

Ⅱ. 정보전의 일반 개념

정보전에 대한 일반적인 정의는 자신의 모든 중요 정보 자원 및 시스템은 적으로부터 보호하는 반면, 적의 중요 정보 자원 및 시스템은 파괴하거나 손해를 입히고, 정보의 획득과 유지에 있어서 비교 우위를 차지하기 위한 모든 행위를 의미한다[1]. 또한, 차세대 정보전은 현대에 들어와서 방어적인 정보보안의 개념에서 좀 더 공격적인 개념을 도입하고 있는 상태이다[2].

일반적인 정보전의 특징은 첫째 사이버 공간에서의 전쟁이므로, 공공과 개인의 구분이라든지 전쟁과 범죄의 구분이 없다는 점을 들 수 있다. 두 번째는 앞서 사이버 공간의 특징에서도 살펴본 바와 같이 시간적,지리적 제약이 없다는 점이다. 즉, 시공 초월성 특징을 가지고 있다. 세 번째는 공격자와 피해자, 공격 준비자등의 구분이 모호하다는 점이다. 이는 곧 전쟁 주체자가 익명성을 가지게 된다는 것이다. 네번째는 선전포고가 별도로 필요치 않은 전쟁이며, 마지막으로 적은 비용으로도 매우 높은 효과를 유발할 수 있는 차세대 전쟁 패러다임의 한 주축이라는 특징을 가지고 있다.

또 다른 미래의 정보전 개념에 있어서 유비쿼터스 공간(제3공간)에서의 전쟁은 기존의 물리공간(제1공간)이나 현재까지 이루어지고 있는 전자공간(제2공간)이 아닌 제3의 전쟁 공간위에서 이루어질 것으로 예측하고 있다. 그러나, 이는 현재의 제2공간에서 이루어지는 정보전 보다도 더 미래의 전쟁이므로 본 기고문에서는 다루지 않을 것이지만, 기초연구는 시작되어야 할 것이다.

Ⅲ. 정보전 공격기술과 개발현황

1. 인터넷 보안의 문제점[3,4]

인터넷은 해커(혹은 침입자/공격자)들에게 있어서 매우 침입하기 용이한 여러 가지 상황들을 제공하고 있다. 이러한 이유는 다음과 같은 여러 가지 이유들로 인해 인터넷 보안이 매우 취약하기 때문이다. (해커 및 크래커에 대한 용어는 사용자에 따라 그 의미가 약간씩 다르게 사용되고 있으나, 본 기고문에서는 일반적으로 통용되고 있는 불법적인 사이버테러의 행위자를 의미하고 있음.)

- ○ UNIX 운영체제 및 TCP/IP 프로토콜의 source 공개
- ○ 인터넷 접속의 다양성 존재 및 접속 자체가 매우 쉬움
- ○ 해킹 방법에 관한 정보 접근의 용이성
- ○ 인터넷의 개방 지향적 사고방식
- ○ 각종 응용 프로그램들의 버그 존재
- ○ 시스템 및 망관리자의 보안 의식/능력 부족
- ○ 정보 전달과 관련된 인터넷 프로토콜의 근본적인 취약점 존재

위와 같은 취약성을 이용하여 단순한 호기심에 의해서든 아니면 고의적이던지 인터넷을 통한 허가 받지 않은 불법적인 침입은 그 자체만으로도 21세기 지식 정보화 사회에 있어서 매우 위협적인 요소가 되고 있는 것이다. 또한, 이러한 취약점을 활용하여 좀 더 공격적인 정보전에의 활용이 손쉽게 이루어지고 있는 실정이다.

2. 기존의 해킹 기술[4,5,6]

정보전은 기본적으로 인터넷과 같은 정보통신 인프라를 주요 대상으로 하기 때문에 기존의 해킹 기술은 매우 유용한 정보전 공격기술이라 할 수 있다.

컴퓨터 시스템을 해킹하는 방법에는 매우 다양한 수법들이 존재하고 있으며, 여기에서는 대표적인 몇가지 수법에 대해서 간략히 알아보도록 한다.

먼저, 기본적인 시스템의 환경 설정 변수를 이용하는 방법이 있다. 인터넷에 연결되어 사용되는 컴퓨터 시스템은 매우 다양한 운용체제를 가지고 있으며, 또한 다양한 사용자의 요구를 만족시키기 위하여 각 시스템 별로 환경 변수 (environment variable)들을 설정하도록 하고 있다. 해커들은 바로 이러한 환경 설정 변수들이 잘못 설정되어 있는 경우 이를 이용하여 관리자의 권한을 획득하게 된다. 또 다른 기본적인 해킹 기법에는 정상적인 시스템 사용자의 ID를 도용하는 방법이 있다. 인터넷의 각종 웹 사이트나 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.

두 번째는 경쟁조건(race condition)을 이용하는 해킹기법이 있다. 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.

세 번째는 버퍼 오버플로우 취약점을 이용하는 것이며, 현재 가장 많이 사용되고 있는 해킹 기법이다. Buffer 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.

네 번째는 인터넷 네트워크 프로토콜의 취약점을 이용하는 방법으로서 서비스거부공격시 가장 많이 활용되고 있는 방법이다. 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) 공격등이 있다. 암호 스니퍼링 (password sniffering) 공격이란 네트워크상에서 흘러다니는 정보를 가지고 사용자의 패스워드등을 알아내는 공격 방법을 말한다. IP Spoofing 공격이란 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 공격이란 TCP(Transmission Control Protocol) 프로토콜의 특징을 이용한 것이다. 인터넷의 주요 프로토콜중 하나인 TCP 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.

최근 Root DNS 서버 공격시 사용되었던 방법이 ICMP(Internet Control Message Protocol) 프로토콜의 취약점을 이용한 것이다. 인터넷 프로토콜은 비신뢰성, 비연결지향 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 해소시켜 주기 위해 인터넷에서는 에러 정보를 상호 교환해 주는 ICMP 프로토콜을 사용하는데 이를 이용한 공격법이 ICMP Echo Reply 공격등이 있다. 또다른 공격법으로서 라우팅 프로토콜을 이용하는 방법이 있다. 인터넷에서는 전송하고자 하는 패킷의 경로를 알기 위해 여러가지 라우팅 프로토콜을 사용하고 있으며, 이때 거짓된 라우팅 정보를 전달하여 해커가 의도하는 컴퓨터로 중요한 정보등을 전송하게 만들 수 있다.

인터넷 네트워크 프로토콜의 취약점을 이용하는 마지막 방법이 서비스 거부 (DOS : Denial of Service) 공격 방법이다. 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 시스

템이 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 매우 어렵다는 특징을 가진다. 2002년 1월에는 DDoS (Distributed DoS)의 해커입장에서의 취약점을 해결한 DRDoS (Distributed Reflection DoS) 공격기법이 나타났으며, 이는 방어하기가 더욱더 어려운 고난이도의 공격기술이다.

다섯 번째로는 응용 S/W의 보안 오류를 이용하는 방법이다. 인터넷에서 누구나 손쉽게 설치하여 사용할 수 있는 FTP, Telnet, SendMail, Web 프로그램과 같은 각종 응용 프로그램들의 버그(bug)를 이용하여 공격하는 방법이다.

이외에도 2000년 하반기부터 나타나기 시작한 포맷스트링 해킹기법이라든지, 보안강화 도구를 이용한 해킹기법, 해킹을 하기 위한 전용툴인 해킹툴을 이용하는 방법등이 있다.

3. 바이러스 기술

정보전에 의해 적의 주요 정보통신 인프라 및 자원을 파괴하거나 위변조 하는 방법에는 바이러스 기술을 활용할 수 있다. 이러한 바이러스 유포에 의한 정보통신 인프라의 파괴, 정보의 위변조등은 사이버 테러의 또 다른 큰 축을 형성하고 있으며, 매우 다양한 수법들이 존재하고 있다.

최근에는 네트워크와 연결된 컴퓨터의 주소록을 이용하여 순식간에 전세계에 E-mail 을 통하여 감염시키는 웜 바이러스나 시스템 내부에 잠복해 있다가 특정한 요일 혹은 특정한 조건하에서 동작하는 트로이 목마와 같은 지능형 바이러스가 점차적으로 증대되고 있다[7].

4. 보안강화 도구 및 해킹 툴

보안강화도구(해킹툴)란 원래 시스템의 관리자들에게 시스템의 보안 수준을 높여줄 수 있는 편리한 도구로써 제공되어지던 것 이였으나, 해커들에 의해 이러한 도구들이 악용 되므로써 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[4,5]. 이러한 해킹툴 중에서도 대표적인 몇가지 도구들은 아래와 같다.

- 내부 보안 취약점 점검 도구 : COPS (Computer Oracle and Password System), Tiger, Tripwire
- 원격 보안 취약점 점검 도구: ISS (Internet Security Scanner), SAINT (Security Administrator's Integrated Network Tool), SATAN (System Administrator Tool for Analyzing Network), Nmap and Xnmap, Sscan and mscan, Shadow Scan
- 모니터링 도구 : Tcpdump, Sniffit, Snoop, Ethereal
- 패스워드 점검 도구 : password crack 프로그램, John 프로그램, L0phtCrack 프로그램
- 기타 : Back Oriffice, Subseven, School Bus, Peekabooty, Camera/Shy, etc

5. 최근 사이버테러 기술의 특징

일반적인 사이버테러의 특징은 간단한 조작, 속임수로 광범위한 피해를 유발할 수 있으며, 사이버테러의 자동성과 반복에 의한 연속성, 국제성과 광역성, 추적과 증거의 어려움, 컴퓨터 전문가에 의한 사이버테러 발생, 범죄의식의 희박성등을 들 수 있다. 이러한 특징은 그대로 정보전의 일부 특징으로 나타나고 있다.

또한, 과거에는 해킹 기술과 바이러스 기술이 별개로 구분되었으나, 1999년 이후로는 해킹 기술과 바이러스 기술이 통합되어 더욱 복잡한 형태의 사이버 테러 방식으로 발전하고 있으며, 웜(Worm), DDoS(Distributed Denial of Service), DRDoS(Distributed Reflection DoS)와 같이 전체 네트워크에 악영향을 미치는 방향으로 진보하는 추세이다. 또한, 기존의 특정 서비스나 호스트를 겨냥하던 해킹의 대상이 인프라 자체에 대한 위협으로 변화하고 있으며, 무선 인터넷의 일반화와 더불어 무선에서의 해킹도 등장하고 있다.

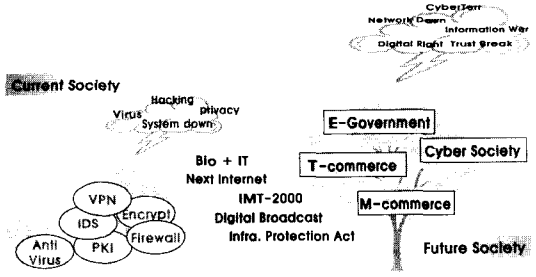
즉, Hacktivism의 확장으로 사이버 테러는 개인적인 지적 호기심 만족을 위한 특정 시스템을 침

입 및 파괴하던 기존의 형태에서, 개인적 목적이 아닌 정치/사회, 군사/산업적 목적으로 악용되어 네트워크 또는 특정 서비스의 기능을 마비 및 파괴시키는 침입 형태로 변화하고 있다. 더불어, 해킹 및 바이러스 기술은 날로 자동화, 지능화, 대중화, 분산화, 대규모화, 은닉화되는 경향을 띄고 있으며, 이의 대표적인 경우가 최근 발생된 DRDoS 공격 기술, 피카부티(peekabooty), Camera/Shy 프로그램 등이 있다.

Ⅳ. 정보전 방어기술과 개발 현황

1. 최근의 정보보호 기술 현황 및 경향

현재의 정보보호 시장은 정보통신 환경 변화에 따른 새로운 정보보호 제품군이 출현하고 있다. 즉, 통신분야에서 정보보호가 일종의 부가 기능에서 핵심요소 기능으로 부각되면서, 보안 기능별 제품에서 다기능이 하나로 합쳐진 통합보안 형태의 제품이 등장하고 있다. 또한, 네트워크 차원의 정보보호 중요성이 날로 증가함에 따라, 기존의 수동적인 정보보호 제품에서 능동적이고 적극적인 정보보호 제품으로 발전하고 있으며, BT-IT 융합기술 발전에 따라 생체인식 시장이 급성장하는 추세이다. 따라서, 전체적인 정보보호 제품은 성능을 고려한 하드웨어화, 보안 기능의 지능화 및 복합화, 보안 기능간의 연계를 위한 통합화, 네트워크 기능으로의 접목화 등의 방향으로 진화할 것이다.



〔그림 1〕 정보보호 서비스의 변화 추세

현재 사용가능한 해킹 및 바이러스 대응기술은 〔표 1〕과 같이 침입 차단, 침입 탐지, 가상사설망(VPN), 항바이러스, 공개키기반(PKI) 및 각종 암호 기술과 같은 보안 요소 기술들이 있다. 그러나, 〔그림 1〕에서 볼 수 있듯이, 미래의 지식 정보화 사회에서는 사이버 테러, 네트워크 파괴, 신용 파괴, 저작권 침해, 정보전과 같은 기존보다 고도화되고 훨씬 치명적인 위협들이 있을 수 있으며, 이와 같은 위협들이 전자정보, T-commerce, M-commerce, 가상 사회의 활성화를 방해하고 있다. 따라서, 보안 기능을 강화한 차세대 인터넷 기술 및 IMT-2000 기술, 생체 인식 등과 같은 Bio 기술과 IT 기술의 통합, 그리고 안전한 통신에 대한 법적 대응 등을 통해서 새로운 네트워크 위협들을 해결해 나가야 할 것이다.

〔표 1〕 해킹 및 바이러스 대응기술

기술	내용
방화벽	- 외부 연결 및 트래픽 제어 - 패킷 필터링을 이용한 보안정책 강화 - 각종 공격/정책 위반 차단 및 보고
침입탐지시스템	- 이상 및 오용 탐지 - 침입 탐지 시 대응 - 방화벽과의 연동 대응
취약점 분석도구	- 취약점의 검색 - 취약점 대책 제시 - 새로운 취약점의 자동 update
항 바이러스	- 각종 바이러스 탐지 및 차단 - 바이러스 피해 복구
VPN	- 안전한 가상 사설망 제공 - 암호화 기능
인증/인가 시스템	- PKI (Public Key Infrastructure), PMI 환경 제공 - 생체인식 기능
ESM	- 각 정보보호 제품 통합 제어 - 로그 기록의 통합 분석 - 침입 탐지/대응/복구 연동

2. 차세대 정보보호 개념 모델

미래 지식정보화 사회를 위한 정보보호 기술은 다음과 같은 네가지 측면에서의 검토가 필요하다. 먼저, 네트워크 측면에서 보면, 네트워크 기술이 발달함에 따라 보다 많은 양의 데이터를 보다 빠르게 주고 받을 수 있게 되었고, 정보보호기술 또한 고속화, 대용량화를 추구하게 되었다. 또한 기존의 네트워크 장비와 별도로 관리하는 부담을 줄이기 위해 표준 인터페이스를 이용한 네트워크 장비와의 통합 및 연동에 대한 요구사항이 대두되고 있으며, 분산되어 설치된 네트워크 장비를 중앙에서 관리자가 관리하는 것과 같이 네트워크상에 설치된 보안 장비를 중

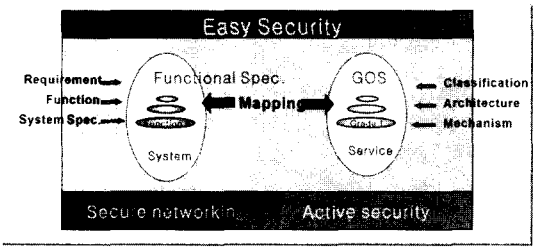
앙에서 관리하기 위해 정책기반관리기법 도입에 대한 요구사항도 나타나고 있다.

서비스측면에서 보면, 기존의 보안 장비는 보안전문지식이 있는 사용자만이 다룰 수 있기 때문에 보안지식이 없는 사용자의 경우 효율적으로 장비를 설정하여 사용하는데 어려움이 많았다. 따라서 개별적으로 보안장비를 구입하여 사용하기 보다 보안 지식이 없는 사용자라도 합리적인 비용으로 원하는 보안서비스를 선택하여 받을 수 있도록 사용자의 요구사항이 반영된, 차등화된 보안 서비스의 제공에 대한 요구사항이 나타나고 있다.

사이버테러 측면에서 보면, 네트워크를 이용한 다양한 해킹기술이 발달함에 따라 피해 범위가 점차 확산되고, 피해정도 또한 심화되고 있으므로 수동적인 모니터링이 아닌 적극적인 대응방안에 대한 필요성이 대두되고 있다. 과거에는 시스템 위주의 공격이 대부분이었으나, 점차 네트워크 공격으로 발전하고 있으며, 개인적 목적의 해킹에서 정치/사회/군사적 목적의 해킹으로 발전하고 있다. 따라서 이러한 추세에 부응하는 다양한 해킹탐지기법에 대한 요구사항과 네트워크 공격에 대응하기 위한 다양한 보안서비스의 연동에 대한 요구사항이 나타나고 있다.

마지막으로 정보보호 측면에서 보면, 기존의 단일 보안기술을 통합함으로써 다양한 보안 제품들을 관리하는데 드는 비용을 줄이고, 다양한 보안 서비스간의 연동을 통해 새로운 보안서비스를 제공하는 기술로 변화하고 있다.

위에서 살펴본 바와 같이 네 가지 측면에서 새로운 정보보호 요구사항이 대두되고 있으며, 이러한 요구사항을 반영한 차세대 정보보호 서비스를 예측해 볼 수 있다. 즉, 차세대 정보보호 서비스는 기존의 정보보호 제품에서 제공하는 보안 기능을 제공할 뿐만 아니라 정보통신 기반기술의 발전에 따른 새로운 정보보호 요구사항을 만족 하여야 하며, 차세대 네트워크 기술 진화를 수용할 수 있어야 한다.



〔그림 2〕 차세대 정보보호 개념모델

따라서, 위의 요구사항을 반영한 차세대 정보보호 모델은 〔그림 2〕와 같이 크게 Easy, Active Security, Secure Networking의 세 가지 요소를 모두 수용하여야 하며, 이의 특징을 요약하면 다음과 같다.

첫째, Easy 란 사용자의 이용 및 접근이 용이한 통합 보안 기술을 의미하는 것으로써, 사용자가 손쉽게 이용할 수 있도록 다양한 보안 서비스 등급을 정의하여 사용자의 요구사항에 맞는 등급별 보안 서비스를 제공한다. 둘째, Active Security란 다양한 침해에 대하여 능동적으로 대응하는 보안기술을 의미한다. 통합 모니터링 분석 기능을 이용한 동적인 보안기능의 설정 및 해제를 통해 보안 서비스의 유연성을 제공한다. 셋째, Secure Networking이란 사용자 선택에 의한 등급별 보안서비스를 제공하기 위한 네트워크 수준의 상호 연동성 보장 기술을 의미한다. 이러한 보안 노드간의 연동을 통해 사용자가 원하는 보안 수준을 유지할 수 있다.

결론적으로, 위와 같은 차세대 정보보호 개념 모델을 수용하기 위해서는 기존의 암호화기술, 침입자 차단 및 탐지기술, 생체인식 기술, 침입자 역추적 기술등과 함께, Self Secure Network, Active Network, Sensor Network과 같은 차세대 정보전 기술들이 연구되어야 할 것이다.

3. 주요 정보전 대응 기술 현황

주요 정보전 대응기술에는 정보통신 인프라 및 시스템을 보호하기 위한 암호기술, 침입차단기술, 인증/인가 기술, 생체 인식 기술, ESM (Enterprise Security Management) 기술과 침입자를 탐지하기 위한 침입자탐지 기술, 자원 오용분석 기술, 바이러스 탐지기술등이 있으며, 공격 탐지 이후 대응과 복구를 위한 기술, 마지막으로 역공격을 위한 바이러스 유포기술, 침입자 유인기술, 침입자 역추적 기술등이 있다.

침입자 역추적 기술이란 사이버 범죄를 시도하는 공격자의 네트워크 상의 실제 위치를 자동화된 기법을 이용하여 추적하는 기술을 의미하며, 이를 이용하여 시스템 혹은 네트워크 침입자를 찾아내는 서비스를 역추적 서비스 기술이라 한다.

현재까지 해커의 실제 위치를 추적하기 위해 사용하는 방법은 오프라인에서 전문가에 의해 직접 해킹당한 시스템의 로그 기록들을 분석하여, 공격을 위해 사용된 바로 이전 단계의 시스템을 찾아내는 방

법을 사용하고 있다. 그러나, 이러한 방법은 시간적, 공간적 제약에 의해 실제 해커의 위치를 찾아가는데 너무 많은 시간이 소요되는 약점이 있다. 또한, 공격자가 실제 존재하고 있는 곳까지의 connection chain 상의 시스템들 중 어느 한군데의 로그 기록이 삭제 혹은 위조된 경우에는 connection chain 상의 이전 단계의 시스템을 찾을 수 없게 되어 실제 해커의 위치를 역추적 할 수 없게 된다. 위와 같은 기술을 TCP connection traceback 이라 말하며, 여기에는 Host-based traceback 기술 및 Network-based traceback 기술로 나뉘어 연구가 진행되고 있다.

TCP Connection 역추적 기술은 1995년경부터 많은 관심을 가지고 연구되어 왔으나, 아직까지 실제 인터넷 환경에 적용하여 사용할 수 있을 만한 시스템은 개발되지 않았었다. 이는 역추적을 위해 공통적으로 포함하여야 하는 모듈들이 모든 호스트에 설치되어야 하는 host-based 역추적 시스템들이었기 때문이다. 그러나, 근래에 들어 네트워크 단에서 송수신 패킷을 확인하여 connection들을 확인하고 이를 이용하여 connection chain을 구성할 수 있는 알고리즘이 개발되기 시작하면서, 실제 인터넷 환경에 적용할 수 있는 가능성이 제기되고 있다.

Host-based Traceback 기술이란 역추적을 수행하기 위한 모듈이 호스트에 설치되어 역추적을 진행하는 형태로, 일반적으로 인터넷 상의 모든 호스트에 역추적 모듈이 설치되어야만 실제 역추적이 가능하다. 따라서 현재의 인터넷 환경에 적용하는 것은 사실상 불가능하다고 할 수 있다. 대표적인 기술로는 CIS(Caller Identification system)[22], AIAA (Autonomous Intrusion Analysis Agent) 시스템[26] 등이 있다.

Network-based Traceback 기술이란 역추적 모듈을 송수신되는 패킷을 확인할 수 있는 위치, 즉 라우터나 스위치가 설치되는 위치에 설치하여 송수신되는 패킷을 확인하고 확인되는 패킷들로부터 특정한 정보를 추출하여 역추적에 활용하는 형태의 역추적 시스템을 의미한다. 이러한 Network-based 역추적 기술은 일반적으로 침입에 사용되는 연결(Connection)로 부터 해당 연결의 특징을 추출하고, 이와 동일한 특징을 가지고 있는 연결을 검색함으로써 이전 단계의 공격 시스템을 찾아내는 방식을 이용한다. 현재 개발되고 있는 제품으로는, 국외의 경우에 미국에서 iTREX 프로젝트에 의해 상용화 제품을 개발하고 있으며, 국내의 경우에는 한국전자통신연구원에서 IDIP(Intruder Detection and Isolation Protocol), SWT (Sleepy Watermark Tracing)[27] 기법을 활용한 역추적 기술이 개발되고 있는 상태이다.

또한, 각각의 연결로부터 어떤 정보를 이용하여 다른 연결들과 비교할 것인가에 대한 연구는 매우 활발히 진행되고 있다. 대표적으로 세가지 방법이 있다. 먼저, Stuart Staniford-Chen에 의해 1995년에 발표된 것으로, 송수신 패킷의 내용(Contents)를 비교하여 같은 Connection Chain에 속하는지를 판단하는 방법이 있으며[23], 두번째 방법으로는 송수신 되는 패킷의 암호화 여부와는 상관없이 Sequence Number의 증가 정도는 유사할 것이라는 가정하에 K. Yoda에 의해 개발된 방법이 있다[24]. 세번째 방법으로는, 네트워크 상에 송신되는 데이터가 존재하는지 여부를 이용하여 ON-OFF Period를 결정하고 이를 비교함으로써 같은 Connection Chain에 속하는지를 판단하는 방법이 있다[25].

이 외에도 우회공격자의 위치를 역추적하기 위한 방법으로서 미국에서는 IDIP 프로토콜을 활용한 CITRA(Cooperative Intrusion Traceback and Response Architecture)[28] 프로젝트와 능동네트워크를 활용하는 방법등이 제안 연구되고 있다. 국내에서는 웹사이트를 활용하는 침입의 경우에 이를 역추적할 수 있는 기술이 상용화되어 판매되고 있는 상태이다.

침입자 역추적 기술중 IP Packet Traceback이란 임의 시스템에 수신된 패킷의 실제 송신위치를 추적하는 기법을 말한다. 일반적으로 어떤 시스템에 도착하는 패킷들은 IP 헤더에 패킷을 송신한 호스트의 IP 주소가 포함되어 있어 직관적으로 패킷의 송신지를 확인할 수 있으나, IP 주소가 변경된 패킷의 경우에는 해당 패킷의 실제 송신지 위치를 파악 할 수 없게 된다. IP 패킷의 주소를 변경하는 기법은 주로DoS (서비스 거부 공격) 공격에 사용되고 있다. 이는 IP 주소가 변경된 패킷을 사용하는 경우에는 시스템 간의 connection을 지속적으로 유지할 수 없기 때문이다. 이와 같은 이유 때문에 현재 IP Packet Traceback에서는 IP가 변경된 패킷을 송신하는 서비스 거부 공격의 실제 공격 위치를 파악하기 위해 연구가 진행되고 있다.

ESM 기술은 기존의 다양한 정보보호 제품들을 독자적으로 관리 운용하는 것이 매우 비효율적이라

는 데에서부터 시작된 기술이다. 예를 들어, 방화벽, 침입탐지시스템, 항바이러스 제품, 각 개별 시스템의 로그 기록등을 취합한 다음, 각각의 로그 기록을 통합적으로 분석 하므로써 일정 수준 이상의 좀더 정제된 정보를 가공 제공할 수 있는 기술인 것이다. 이러한 분야는 국외의 경우에는 NMS (Network Management System)의 정보보호 기능과 연계되어 활발히 개발이 진행되고 있는 상태이며, 국내에서는 각 개별 정보보호 제품을 통합관리하기 위한 방법으로 ESM 제품이 출시되어 판매되고 있는 상태이다.

국내의 경우에 사이버테러대응 기술 및 정보전 대응기술 개발은 한국전자통신연구원(ETRI)의 정보보호연구본부 및 국가보안기술연구소, 한국정보보호진흥원(KISA)에서 주로 이루어져 왔으며, 최근 수년동안에는 민간 업체에 의한 주요 인터넷 정보보호 제품들이 상용화되어 판매되고 있는 상태이다.

V. 결 론

지금까지 정보전의 개념에 대해 알아본 후, 정보전의 가장 큰 대상중의 하나인 인터넷을 공격할 수 있는 정보전 공격기술과 이를 방어하기 위한 정보보호 기술의 개발 현황에 대해서 분석해 보았다.

정보기술의 급격한 발전과 함께 대부분의 컴퓨터들이 네트워크에 연결되고, 사이버 스페이스의 주요 특징인 익명성, 비대면성, 시공초월성등과 함께, 부주의와 소프트웨어에 기본적으로 내재될 수 밖에 없는 버그 및 각종 취약점 등으로 인해 사이버테러로부터 정보 시스템을 보호하는 것은 점점 더 어려워지고 있다. 게다가 사이버테러 기술의 악의적, 군사적 활용도가 높아지면서 사이버테러는 더욱 기승을 부리고 있고 앞으로도 계속적으로 증가할 것으로 예측되고 있다. 특히, 21세기 들어 정보시스템에 대한 의존성이 심화되고 인터넷을 통하여 주요 정보들이 유통되기 시작하면서, 이들에 대한 공격이 급격히 높아지고 있는 추세이다. 최근 걸프전과 유고전의 정보전쟁 사례를 보더래도 재래식 전쟁에 비해 훨씬 더 적은 비용으로 매우 높은 효과를 얻을 수 있는 정보전에 대한 연구는 전세계적으로 매우 활발히 진행되고 있는 상황이다.

본 기고문에서는 현재 개발되고 있는 각종 정보보호 기술의 현황과 향후 발전 방향에 대해 분석하였다. 또한, 정보전 방어에 적용 가능한 차세대 정보보호 모델을 구축하기 위해 네가지 측면의 요구사항을 알아보았으며, 이를 통해 Easy, Active Security, Secure Networking이라는 세가지 요소를 포함한 차세대 정보보호 모델을 제시하였다. 앞으로는 이러한 분석하에 실제적인 사이버테러 행위자들의 행동을 추적 감시할 수 있는 대응체계에 대한 연구와 함께, 해커의 침입을 발견하고 차단하는 기술뿐만이 아니라 침입자의 행위를 감시하고 이들을 역으로 추적할 수 있는 대규모 통합 감시 네트워크가 구축되어야 할 것이다.

또한, 기존의 암호화기술, 침입자 차단 및 탐지기술, 생체인식 기술, 역추적기술, ESM 기술등과 함께, Self Secure Network, Active Network, Sensor Network, 유비쿼터스 군사 및 전술공간 기술과 같은 차세대 정보전 기술들이 연구되어야 할 것이다.

참 고 문 헌

[1] Reto E. Haeni, "Information Warfare: an Introduction," Information Warfare Conference, 1995

[2] Winkler J.R., Oshea C.J. and Stokrp M.C., "Information Warfare, INFOSEC and Dynamic Information Defense," Proceedings of NISSC, 1996 December

[3] 서동일, 강훈, "인터넷 보안기술 동향 분석", ETRI 주간기술동향, 1996. 9. 4 (96-34)

[4] 서동일, 윤이중, 조현숙, "사이버테러 기술 및 대응방안의 현황 분석", Telecommunications Review, Vol.10, No.5, 2000 October

[5] POSTECH, Security PLUS for UNIX, Youngjin.com, 2000

[6] Joel Scambray, Stuart McClure and George Kurtz, Hacking Exposed : Network Security Secrets & Solutions - 2nd Edition, McClure-Hill, 2001

[7] 안철수연구소, http://www.ahnlab.com

[8] David S. Alberts, John J. Garstka, Richard E. Hayes, David A. Signori, "Understanding Information Age Warfare", CCRA Publcation, 2001 August

[9] 최양서, 최병철, 강동호, 서동일, "Network 기반 실시간 역추적 시스템의 설계", 12th

JCCI, 2002 April
[10] 서동일, 최병철, 손승원, 이상호, "해킹 기법을 이용한 내부망 보안 평가 방법", KIPS Journal, Vol 9-C, No.3, 2002 June
[11] 강동호, 최양서, 서동일, 이상호, "방화벽 우회 방지 기술 분석", 7th COMSW, 2002 July
[12] Y.S. Choi, Dong-il SEO and Sung Won Sohn, "A New Buffer Overflow Hacking Defense Technique with Memory Address Confirmation", LNCS 2288, 2002 April
[13] S.W. Han, D.H. Kang, Dong-il SEO and Sang Ho Lee, "Design of Network-based Real-Time Traceback System", AMS 2002
[14] CERT, http://www.cert.org
[15] DARPA, http://www.darpa.mil
[16] CIAO, National Plan for Information Systems Protection, Version 1.0 : An Invitation to a Dialogue, 2000.1
[17] IETF, http://www.ietf.org
[18] http://www.infowar.com
[19] 장희진, 박보석, 김상욱, "차세대 공격형 정보 보안 기술," 정보처리 제7권 제2호, 2000. 3
[20] Byeong-Cheol Choi, Dong-il Seo, Sung-Won Sohn, Sang-Ho Lee and Chaeho Lim, "Adaptive Rule Estimation (ARE) Algorithm against Eluding NIDS", FIRST 2002, 2002 June
[21] KISA, http://www.kisa.or.kr
[22] Hyn Tae Jung, H.L. Kim, Y.M. Seo, G. Choe, S.L. Min, C.S. Kim, "Caller Identification System in the Internet Environment", Proceedings of the 4th USENIX Security Symposium, 1993
[23] Stuart Staniford-Chen and L. Todd Heberlein, "Holding Intruders Accountable on the Internet", Proceedings of the 1995 IEEE Symposium on Security and Privacy, May 1995
[24] K.Yoda and H. Etoh, "Finding a Connection Chain for Tracing Intruders", In F. Guppens, Y.Deswarte, D.Gollarnann, and M. Waidner, editors, 6th ESORICS 2000, LNCS-1985, Toulouse, France, 2000 Oct.
[25] Y. Zhang and V. Paxson, "Detecting Stepping Stones", Proceedings of 9th USENIX Security Symposium, August 2000
[26] 임채호, 원유헌, "인터넷 해킹 피해시스템 자동분석에이전트(AIAA) 및 침입자 역추적 지원 도구 구현", 정보처리학회 논문지, 1999. 11
[27] X. Wang, D. Reeves, S.F. Wu, and J. Yuill, "Sleepy Watermark Tracing: An Active Network-Based Intrusion Response Framework", Proceedings of IFIP Conference on Security, 2001 Mar.
[28] D. Schnackenberg, K. Djahandari, and D. Strene, Harley Holiday, Randall Smith, "Cooperative Intrusion Traceback and Response Architecture (CITRA)", Proceedings of the 2nd DARPA DISCEXII, June 2001.
[29] http://www.terrorism.com
[30] 이준엽, 이승형, 양훈기, 고재영, 강철오, 정주영, "IP 역추적을 위한 새로운 접근 : 패킷 손실 기반의 논리적 전송 경로 추정", 정보보호학회 논문지, 제12권 제3호, 2002. 6
[31] 정연서, 류걸우, 장종수, "네트워크 보안을 위한 ESM 기술 동향", ETRI 주간기술동향, 01-48호, 2001. 12
[32] T. Baba and S. Matsuda, "Tracing network attacks to their sources", IEEE Internet Computing, Vol.6 Issue 2, 2002 March-April
[33] Drew Dean, Matt Franklin, Adam Stubblefield, "An algebraic approach to IP traceback", ACM Transactions on Information and System Security, Vol.5 No.2, 2002 May
[34] R.F. Erbacher, K.L. Walker, D.A. Frincke, "Intrusion and Misuse Detection in Large-scale Systems", IEEE Computer Graphics and Applications, Vol.22 Issue 1, 2002 Jan.-Feb.
[35] Vern Paxson, "An analysis of using reflectors for distributed denial-of-

service attacks", ACM Computer Comm. Review, 2001 July
[36] Anthony Ruocco, Nathan Buchheit, and Daniel Ragsdale, "A Combined Offensive/Defensive Network Model", Proceedings of IEEE Workshop on Information Assurance and Security, 2000 June
[37] A.R. Chaturvedi, M.Gupta, S.R. Meehta, and Wei T. Yue, "Agent-Based Simulation Approach to Information Warfare in the SEAS Environment", Proceedings of 33rd Hawaii International Conference on System Sciences, 2000
[38] J.Schumacher and D.Welch, "Preparing to Defend Against Cyberattack", Proceedings of IEEE Workshop on Information Assurance and Security, 2000 June

〈著 者 紹 介〉

서 동 일 (Seo, Dong-il)
정회원

1989년 : 경북대학교 전자공학과 졸업
1994년 : 포항공과대학교 정보통신공학과 석사
2002년~현재 : 충북대학교 전자계산학과 박사과정
1994년~현재 : 한국전자통신연구원 선임연구원(팀장)
관심분야 : 인터넷 정보보호, 컴퓨터 통신, 네트워크

손 승 원 (Sohn, Sung-Won)
정회원

1984년 : 경북대학교 전자공학과 졸업
1994년 : 연세대학교 컴퓨터공학과 석사
1999년 : 충북대학교 컴퓨터공학과 박사
1991년~현재 : 한국전자통신연구원 책임연구원(부장)
관심분야 : 이동인터넷보안, 정보보호, 네트워크보안

조 현 숙 (Cho, Hyun-Sook)
종신회원

1979년 : 전남대학교 수학과 졸업
1991년 : 충북대학교 전자계산학과 석사
2001년 : 충북대학교 전자계산학과 박사
1982년~현재 : 한국전자통신연구원 책임연구원
관심분야 : 네트워크보안, 이동인터넷보안, CAS

이 상 호 (Lee, Sang-Ho)
종신회원

1976년 : 숭실대학교 전자계산학과 졸업
1981년 : 숭실대학교 전자계산학과 석사
1989년 : 숭실대학교 전자계산학과 박사
1981년~현재 : 충북대학교 컴퓨터과학과 교수
관심분야 : 네트워크 보안, 망관리, 프로토콜