특집 10

미래 사이버전 및 대비방안

목 차

김승권 · 김상국 · 최종화
(안보경영연구원)

1. 서 론

21세기 정보통신 기술 및 유비쿼터스 기술의 발전은 국가·사회의 경쟁력 강화 및 발전에 기반이 되고 있다. 하지만 정보화 추진의 역기능으로 발생하는 다양한 보안문제는 국가·사회의 안정을 해치는 현실적인 위협으로 대두되고 있으며, 이러한 위협은 미래 유비쿼터스 사회로 발전함에 따라 더욱 심화될 것으로 예측된다.

유비쿼터스 사회에서는 이렇게 네트워크, 인프라망 차원에서 광대역화, 융합화를 특징으로 하는 진화된 네트워크를 통해 지능화 서비스 제공이 가능하게 될 것이다. 유비쿼터스 환경의 도래로 네트워크가 이동공간뿐 아니라 RFID, 스마트카드 등이 내재된 사물로까지 확장되면서 사회 전반에 역기능이 발생할 폭도 넓어졌다. 따라서 미래사회에는 Malware, 스파이웨어, 봇넷을 이용한 공격, 모바일 스팸 등 신종 유비쿼터스 범죄가 등장할 것으로 우려되고 있다.

따라서 본 연구는 사이버공격(해킹)의 최근 동향과 기법들을 알아보고, 최근의 사이버 침해 및 위협에 따른 국·내외의 정보보호를 위한 노력들을 살펴보며, 유비쿼터스 기술을 기반으로 한 사이버공격의 환경적 변화에 대처하기 위하여 향후 사이버전의 위협요소와 그에 따른 대비방안을 도출하고자 한다.

2. 사이버공격(해킹)의 최근 동향 및 기법

2.1 사이버전의 정의

사이버(Cyber)라는 말은 조정, 통제, 통치의 의미를 가진 그리스어에서 유래한 것이나, 정보통신 기술의 혁신적인 발달이 진행되고 있는 오늘날은 '현실'과 배치되는 개념으로서 컴퓨터나 통신 네트워크를 공간으로 한 '가상'이라는 의미로 통용된다[6].

사이버전 역시 정보를 다루는 유무형의 자산이 전쟁수행의 핵심적인 도구로 부상하게 된 근래에 생성된 용어로, 보는 관점에 따라 다양한 견해가 있다. 이에 대한 명확한 정의는 내려지지 않은 상황이고 사이버전에 대한 정의는 정보전과 관련하여 협의의 개념, 광의의 개념 그리고 정보전과 분리된 개념으로 보는 세 가지 관점에서 이루지고 있다.

〈표 1〉 Libiki의 사이버전 분류

종 류	의 미
정보테러리즘 (Information Terrorism)	일종의 개인에 대한 사이버테러로서 주된 컴퓨터 해킹을 통해 개인을 공격
시뮬라 전 (Simula-warfare)	컴퓨터 시뮬레이션 결과를 실제전투로 대신
깁슨전 (Gibson-warfare)	사이버 공간에서 대리자(에이전트)간의 전쟁으로 실제 전투 대신
시멘틱 공격 (Sementic attacks)	시스템의 외적인 변화 없이 시스템의 내부적인 요소에 영향을 미침
해커전 (Hacker warfare)	시스템의 외적 상태에 영향을 미침 (예, 시스템의 정지)

첫째, 협의의 개념으로서 사이버전을 정보전(Information Warfare)의 한 유형으로 인식하는 개념이다. 리비키(Martin C. Libichi)는 사이버전(Cyber Warfare)을 지휘 및 통제전(Command and Control Warfare), 군사정보전(Intelligence-based Warfare), 전자전(Electronic Warfare), 심리전(Psychological Warfare), 해커전(Hacker Warfare), 경제정보전(Economic Information Warfare) 등과 함께 정보전의 7가지 유형 중 하나로 분류하여 제시하고 있다. 이와 유사한 정의로 사이버전을 정보전의 한 형태로 구분하고 또 사이버전을 컴퓨터와 네트워크시스템에서 이루어지는 전쟁으로서 정보전의 한 유형으로 분류하였다[10].

둘째, 사이버전을 광의의 개념으로 보는 입장에서는 정보기술의 발달이 가상공간에서의 전쟁을 기존의 육, 해, 공, 우주에 이르는 4차원의 전장공간에 추가하여 제5의 새로운 전장 공간으로 인식함은 물론, 나아가 군사조직, 전략, 작전 등 제반 군사분야에 근본적인 변혁을 유발하는 것으로까지 확대하여 인식하는 개념이다[1]. 광의의 사이버전은 전략적 정보전(Strategic information warfare) 및 네트전(Net warfare)과 유사한 개념으로 파악되고 있으며, '군사혁신(RMA)'의 구현 형태와도 밀접한 상관성이 있는 것으로 인식할 수 있을 것이다.

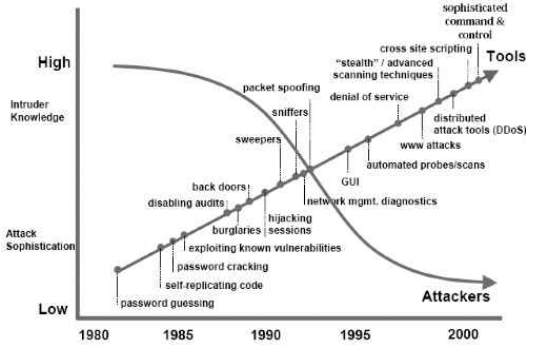
셋째, 협의 또는 광의의 개념과 달리 분리된 개념으로 인식하는 입장이다. 정보전은 군사부문을 대상으로 하지만 사이버전은 군사부문과 민간부문을 포함하는 개념이라는 점에서 서로 비교할 수 있는 어떤 한 연속선장에 놓여 있지 않기 때문에 상호간의 관계를 정의하는 것은 부적절하다는 것이다[3].

본 연구는 기존의 정의를 바탕으로 컴퓨터와 관련된 기반 장비를 토대로 한 네트워크상의 공간(사이버 공간)과 실제 공간에서 다양한 사이버 공격수단을 사용하여 상대의 군사부문과 민간부문의 정보체계를 마비시키기 위해 취해지는 유·무형적인 공격적 행동과 자국의 군사·민간부문의 정보체계를 보호하기 위한 방어적 행동으로 정의한다.

2.2 사이버 공격의 최근 동향

시간의 변화에 따라, 해커들이 사용하는 방법(method), 도구(tool) 및 기법(technique)들을 포함한 컴퓨터 보안에 대한 공격 기법들도 점차 진화하고 있다. 1980년대의 공격자들은 공격대상 시스템에 불법적인 접근권한을 얻기 위해 암호나 알려진 취약성을 주로 공격하였다. 이후에 공격자들은 프로토콜의 문제점(flaw)으로 이동하였고, 새로운 보안 결함들을 조사하고, 네트워크에 sniffer 프로그램을 설치하고, 추가적인 공격 대상을 식별하기 위해 폭넓은 자동화된 스캐닝을 하였다. 이러한 진화의 단계를 거치면서, 많은 지식을 습득하게 된 공격자들은 최근 기술들을 활용하여 사용하기 쉬운 스크립트(script)나 전문화된 도구들을 만들어서 새로운 신참 공격자들에게 자신들의 전문성을 전수하였다.

(그림 1)은 시간이 지남에 따라 공격자들에 요구되는 전문적인 지식이 점차 줄어들지만 공격이나 공격 도구들의 전문성이 늘어나는 것을 보여주고 있다. 이는 전문적인 지식이 없어도 손쉽게 해커가 될 수 있음을 보여주고 있다. 즉, 사



(그림 1) 공격기법과 침입자의 지식(CERT/CC 2002)

이버 공격에 대한 특별한 지식이 없어도 단지 몇 번 마우스만을 클릭해서 전문적인 사이버 공격을 수행할 수 있다는 것을 보여주고 있다.

1988년 이후 사이버 공격의 동향을 분석한 CERT Coordination Center의 2001년 사이버 공격 동향 분석 보고서(CERT/CC(2), 2002)는 사이버 공격 동향을 6가지로 제시하고 있다.

첫째 자동화(Automation), 공격 도구들의 속도 향상: 공격 도구의 자동화 수준은 계속해서 발전하고 있다.

둘째 공격 도구의 능력 향상: 개발자들은 이전에 비해 고도의 기술을 사용하고 있다. 이에 따라, 예전에 비해 분석을 통해 공격 도구의 흔적을 발견하기가 더 어려워졌으며, 백신 소프트웨어나 침입탐지시스템과 같이 공격 흔적을 기반으로 하는 시스템을 탐지하기도 어려운 실정이다. 정교한 공격 도구들의 한 예로서, 많은 수의 도구들이 침입자와 침투된 시스템간의 자료 및 명령의 전송을 위해 IRC나 HTTP 프로토콜을 사용한다. 결과적으로 공격시도와 정상적이고 합법적인 네트워크 트래픽을 구분하기가 어려워 졌다.

셋째, 취약성의 신속한 발견 : 최근 보고되는 새로운 취약성의 수는 매년 두 배 이상씩 증가하고 있다. 이에 따라 시스템 관리자들이 패치를 적용하기도 어려운 실정이다. 게다가 매년 새로운 종류의 취약성들이 발견되고 있다. 새로운 취약성을 확인하기 위하여 현존하는 코드를 검토하기 위해서는 수백 개의 소프트웨어 제품에 취약성이 존재하는지 반복적으로 확인하여야 한다. 반면 공격자들은 취약성 사례를 개발자(또는 제작자)보다 먼저 발견하고 있다. 공격자들이 기술적으로 새로운 취약성을 신속히 발견하고 있기 때문에 "패치 시간"은 점점 작아지고 있다.

넷째, 방화벽 침투 증가: 방화벽은 침입자로부터 시스템을 보호하기 위한 초보적인 보호 수단으로 인식되고 있다. 현존하는 방화벽의 문제점은 우선 전형적으로 구성된 방화벽을 통과하도록 설계된 기술이 존재한다는 것이다.

다섯째, 비대칭적 위협 증가: 인터넷에서의 보안은 그 특성상 서로 연관관계가 깊다. 인터넷에 연결된 한 시스템이 공격에 노출되면 전 세계 인터넷에 연결된 나머지 시스템의 보안 상태도 영향을 받는다. 공격기술이 발전함에 따라 한 명의 공격자는 하나의 희생자를 효과적으로 공격하기 위하여 수많은 분산 시스템을 쉽게 이용할 수 있다. 공격 도구 배치의 자동화와 공격 도구 관리의 정교화에 따라 위협의 비대칭성은 계속 증가할 것이다.

여섯째, 기반 공격의 위협 증가: 또 다른 주요 경향 중 하나가 DNS와 라우터 등과 같은 정보통신기반에 대한 공격이 증가한다는 것이다. 또한 기술적인 특성을 요약하면, 사이버공격의 에이전트화, 분산화, 자동화, 그리고 은닉화를 들 수 있다.

2.3 해킹 기법

해커들을 시스템이나 네트워크의 취약성을 이용하여 해킹을 시도한다. 이들은 시스템의 정상적인 동작을 방해하여 시스템이 사용자가 요구하는 서비스를 처리하지 못하도록 하는 서비스 거부공격을 감행하거나 Back Orifice를 이용하여 Windows를 공격 하기도하고, 주로 Unix 계

열 운영체제의 런 타임 스택이 갖는 특성을 이용하여 버퍼 오퍼플로우 공격을 하거나 CGI 취약점을 이용하여 웹 서버나 홈페이지를 공격하는 등 다양한 기법과 도구를 이용한다. 여기에는 대표적인 방법[2,5]을 간략하게 살펴보자.

기본적인 시스템의 환경 설정 변수를 이용하는 해킹 방법이 있다. 인터넷에 연결된 컴퓨터 시스템은 매우 다양한 운용체계를 가지고 있으며, 또한 다양한 사용자의 요구를 만족시키기 위하여 각 시스템별로 환경변수들을 설정하도록 하고 있다. 해커들은 바로 이러한 환경설정 변수들이 잘못 설정되어 있는 경우 이를 이용하여 관리자의 권한을 획득하거나 정상적인 시스템의 사용자의 ID를 도용하는 방법이 있다.

두 번째는 경쟁조건(race condition)을 이용하는 해킹기법이 있다. 유닉스시스템에서는 한정된 자원을 여러 개의 프로세스 혹은 여러 명의 사용자들이 공유하게 된다. 이렇게 한정된 자원을 여러 프로세스 혹은 객체들이 공유하여 사용하게 되므로 하나의 자원을 상용하려고 서로 경쟁하는 모양을 갖추게 되며, 이러한 현상을 이용하여 일반 사용자가 시스템의 관리자 권한을 획득할 수 있게 된다.

세 번째는 버퍼 오버플로우 기능을 이용하는 것이며, 현재 가장 많이 사용되고 있는 해킹 기법이다. Buffer Overflow 공격(손태식,2001) 이란 지정된 버퍼의 크기보다 많은 데이터를 입력하여 프로그램이 비정상적으로 동작하도록 만드는 것을 말한다. 이를 이용하여 해커는 공격하고자하는 시스템을 파괴할 수 도 있으며, 관리자의 권한을 획득하여 정보의 변조나 유출 등을 시도할 수 있게 된다.

네 번째는 인터넷 프로토콜 취약점을 이용하는 방법으로 서비스 거부 공격을 수행할 때 가장 많이 활용되는 방법이다. 인터넷이 기반으로 하고 TCP/IP 프로토콜이며, 인터넷의 정보의 공유라는 가치를 실현하기 위해 TCP/IP 프로토콜도 개방형 구조를 가지고 있다. 따라서 이러한 개방적인 구조를 이용하여 해킹하는 방법은 다양하며, 대표적인 기법으로 Sniffing Spoofing 공격, SYN Flooding 공격, 스니퍼링 공격, 서비스 거부(Denial of Service: DoS) 공격 등이 있다.

다섯 번째 컴퓨터 바이러스는 '70년대 미 국방성 Alpha Net에서 처음 발견된 이래, 최근 들어 급속히 들어나고 있다. 바이러스들은 인터넷의 영향으로 인해 점차 그 확산속도가 빨라지고 있다. 주로 실행파일에 부착되는 악성프로그램으로 세 가지 유형이 존재한다. 컴퓨터가 부팅될 때 운영체제가 로드되는 부분에 상재하는 바이러스인 부트섹터 바이러스, 실행파일에 기생하는 바이러스로써 특정한 조건을 만족하면 하드디스크를 삭제하는 등의 악의적인 행위를 수행하는 프로그램 바이러스, 마지막으로 매크로 바이러스가 존재한다. 최근에는 네트워크와 연결된 컴퓨터의 주소록을 이용하여 순식간에 전 세계에 E-mail을 통하여 감염시키는 웜 바이러스나 시스템 내부에 잠복해 있다가 특정한 조건하에서 작동하는 트로이 목마와 같은 지능형 바이러스가 증대되고 있다.

여섯 번째는 웜(worm)의 진화이다. 웜은 스스로 전파되는 악성 코드로서, 전파를 위하여 사람이 개입하여야 하는 바이러스와 달리 스스로 전파될 수 있다. 88년 11월 2일 최초로 발견되었을 때, 웜은 컴퓨터, 네트워크, 및 사용자에 대한 정보를 입수한 뒤, 다른 시스템의 소프트웨어적 취약점을 이용하여 해당 시스템에 침투하고, 자신의 복사본을 만들어 또 다른 시스템으로 옮기는 방법으로 수천대의 컴퓨터들의 정상적인 동작을 방해하였으며, 인터넷을 며칠간 마비시켰다. 최근 들어, 웜은 고수준으로 자동화되어 있을 뿐 아니라 그들이 이용하는 취약성이 상대적으로 과다하기 때문에 몇 시간 만에 수많은 시스템을 감염 시킬 수 있다. 실제로 Code Red는 2001년 7월 19일 단지 9시간 만에 25만대 이상의 시스템

을 감염시켰다. 또한 서비스거부 공격을 위한 페이로드(payload)를 내장하고 있고, sadmind/IIS와 code Red는 웹사이트 페이로드를 가지고 있을 뿐 아니라 W32/Leavers와 같은 웜은 동적으로 변형되는 능력을 보유하고 있기도 하다.

마지막으로 전자우편폭탄/스팸 메일을 활용하는 방법이다. 적대국에 악의적 또는 별 의미 없는 내용을 담은 전자우편을 대량으로 발송하여 컴퓨터나 네트워크를 마비시킬 수 있다. 유고 전에는 발신처가 벨그라드인 메일이 해군 항공기지에 200통이 전달된 사례가 있으며 하루에 2000통씩의 메일이 계속적으로 나토와 미 국방성 관련 사이트에 발송된 사례도 있다.

2.4 최근 사이버전 사례

최근의 사이버공격은 이전의 시스템 침입이나 웜·바이러스에 의한 파일 변조, 자료 유출 등 개별시스템과 개인에 대한 공격에서 원격 조정이 가능한 해킹도구를 사용한 정교한 타겟 공격이나, 웜·바이러스 등을 통해 대량의 트래픽을 발생시킴으로써 인터넷 망 기반구조를 공격하는 형태로 변화되고 있다.

최근 정부를 대상으로 이루어지는 해커들의 공격으로 인해 각국 정부 당국들이 대응책 마련에 부심하고 있다. 미 국방부와 국무부가 해커들에 공격을 받아 뚫리는가 하면, 영국, 독일, 프랑스의 정부 및 주요기간 전산망들을 해커들이 휘젓고 다니고 있어 이들 국가들의 보안상태가 취약한 것으로 드러나고 있다.

사이버전이라는 이름으로 가시화된 최초의 사이버전은 에스토니아에 대한 사이버공격과 중국의 미국이나 유럽에 대한 해킹 공격이다. 특히 2007년 4월 27일부터 2007년 5월 11일까지 2주간에 걸쳐 러시아에 의해 수행된 것으로 의심받고 있는 에스토니아에 대한 분산 서비스 거부공격(DDoS; Distributed Denial of service)은 에스토니아의 정부, 뉴스 그리고 은행과 같은 주요 전산망을 대상으로 집중적으로 수행되었다. 에스토니아에 대한 사이버 공격은 호기심이나 개인의 경제적 이익을 위해 수행되었던 기존의 해킹과 규모나 대상 측면에서 전혀 다른 양상을 보이고 있다.

〈표 2〉 에스토니아 사이버공격 일지

날자	주요 내용
2007.04.28	러시아의 첫 번째 공격
2007.04.30	두 대의 봇넷(botnets)을 통한 DDoS 공격
2007.05.01	ISP 라우터 공격
2007.05.04	Storm Worm-botnet의 첫 번째 공격
2007.05.05	첫 번째 스팸 e-mail 공격
2007.05.06	두 번째 스팸 e-mail 공격
2007.0509	타 CERT팀에 의한 스팸 e-mail 공격/Elion 라우터 공격 www.valitsus.ee(에스토인아 정부) 사이트 Akamai로 이전
2007.05.10	TERENA[1]의 TF-CSIRT에 의한 에스토니아 지원(rescue)을 발표
2007.05.11	세번째 스팸(abuse) e-mail 공격 네번째 스팸 e-mail 공격
2007.05.12	다섯번째 스팸 e-mail 공격
2007.05.13	여섯번째 스팸 e-mail 공격
2007.05.13	닷 ee 사이트에 대한 DDoS 공격
2007.05.24	ENISA 에스토니아에 대한 대량 공격사실을 언론에 공표함.

〈표 3〉에스토니아 사이버공격 형태분석

공격횟수	목표	Address or owner
35	195.80.105.107/32	pol.ee
7	195.80.106.72/32	www.riigikogu.ee
36	195.80.105.158/32	www.riik.ee, www.peaminister.ee, www.valitsus.ee
2	195.80.124.53/32	m53.envir.ee
2	213.184.149.171/32	www.sm.ee
6	213.184.49.194/32	www.agri.ee
4	213.184.50.6/32	
35	213.184.50.69/32	www.fin.ee (Ministry of Finance)
1	62.65.192.24/32	

에스토니아 사이버공격에 대한 분석 보고서에 따르면[8], 총 128회의 DDoS 공격이 수행되었다. 이중에서 115회는 ICMP flood 공격, 4회가

1) Trans-European Research and Education Networking Association

TCP SYN flood, 그리고 9회는 일반적인 트래픽 flood 공격이었다. 사이버 공격의 직접적인 원인은 소련군 전몰자 추모 동상 철거를 시도하는 에스토니아 경찰과 러시아계 이민자들과 충돌한 사건에서 시작된 사이버전은 표면적으로 정부의 개입을 입증하지 못했지만 정부의 도움 없이 이루어질 수 없는 다각적인 공격이었으며 정부, 언론, 방송, 은행과 같은 국가 핵심전산망이 주 표적이었다는 점과 사이버 공격의 강도가 일반적인 해커나 특수집단의 능력을 훨씬 뛰어넘기 때문에 국가의 지원을 받는 사이버 공격으로 여겨지고 있다. 특히 봇넷을 통한 공격은 전형적인 정보전의 유형을 보여주고 있다. 이 공격을 위해 당시 100만대 이상의 컴퓨터가 사용된 것으로 알려졌고, 이는 해커들 사이의 해킹이 아닌 국가 전체를 공격한 전면전 양상을 보였기 때문에 비상한 관심을 끌고 있다. 또한 중국이 주도한 것으로 의심받고 있는 영국과 프랑스에 대한 해킹과 독일총리실에 '트로이 목마'를 침투시킨 사건으로 인해 진정한 의미의 사이버전이 시작되었다고 얘기하고 있다.

3. 국·내외 정보보호 추진 방향

3.1 국내 정보화 추진동향

90년대 중반이후 인터넷의 폭발적인 보급 및 활용이 확대됨에 따라 해킹, 바이러스, 침해 등과 사이버 침해의 위협은 점차 증가하였다. 이에 정부, 차원에서 2001년 사이버 침해행위로부터 국가와 국민생활 인전을 보장하기 위해 '정보통신기반보호법'을 제정하여 시행하고 있다.

하지만 2003년 발생한 1.25 인터넷 대란은 국가·사회의 안정에 있어 국가 IT 인프라에 대한 체계적인 보호의 중요성을 상기하는 계기가 되었으며, 개인 또는 단위 조직 차원에서의 정보보호 및 사이버 침해 대응을 넘어서서 국가적 차원의 종합적인 대책을 요구하게 된다.

이러한 문제를 해결하기 위해 국가위기관리차원에서 국가안전보장회의 사무처 중심으로 사이버위협 대응 시스템을 구축하였다. 하지만 2004년 상반기에 발생한 주요 국가기관 해킹사고 처리과정에서 유관 기관간 유기적인 협조체계가 다소 원활하지 못한 문제점이 제기되었으며, 이러한 운용상의 문제를 해결하기 위해 정부 부처간 협의 하에 범정부적 사이버안전관리체계를 구축하였다.

이 협의에 따라 대통령훈령으로 국가사이버안전관리규정을 제정하기로 하고, 동 규정에는 국가사이버안전관리센터와 사이버안전 관리 담당 전무기관 간 각종 사이버위협 정보의 공유·협력을 의무화하고 국가기관·지자체·공공기관은 기관별 사이버안전대책을 수립하며 국가정보원이 그 이행여부 및 안전성을 확인하여 시정조치를 권고할 수 있게 하였다. 또한 사이버공격 발생 시 해당기관은 국가 사이버 안전센터에 신고를 의무화하고 국가사이버안전센터는 피해확산 방지를 위한 조취를 취하고 관련된 사고조사를 실시할 수 있게 하였다.

3.2 미국

9.11사태 이후 미국은 2002년에 국토안보 총괄을 위해 주요기반보장국(CIAO), 비밀정보기관(Secret Service) 등의 22개 기관을 통합하여 국토안보부(DHS)를 신설하는 등 정보보호 정책을 강화한 바 있다. 2005년에는 제2스테이지 리뷰를 통해 DHS 조직을 개편하는 등 정보보호 조직체계를 한층 강화하였다. 이 새로운 체제는 정보보호 분야와 관련된 조직을 준비국(Directorate for Preparedness)과 과학기술국(Science and Technology Directorate)의 2개 국(局)으로 통합하는 것을 골자로 하며, 이와 함께 자문위원회를 설립하여 DHS 장관 및 대통령에게 국토안전보장에 대해 제안하도록 하였다[9].

한편, 연구개발 측면과 관련하여 2006년에는

"연방정부 정보보호 및 보증 연구개발 계획(Federal Plan for Cyber Security and Information Assurance Research and Development)"을 발표했다. 이 계획은 연방정부 차원으로는 첫 번째 정보보호 연구개발 기본계획으로 현재 개발이 추진되고 있는 보안기술에 대한 현황 분석, 정보보호 연구개발 촉진을 위한 10개의 권고안을 담고 있다[9].

3.3 일본

일본은 2010년까지 세계적인 IT 선도국가가 되는 것을 목표로 u-Japan 정책과 IT신개혁전략을 추진하고 있으며, 내각관방을 중심으로 총무성, 경제산업성이 양대 축이 되어 정보보호 대책을 추진하고 있다. 또한, 내각관방 산하에 국가정보보호센터를 설립하여 국가 주요 정보보호 정책을 결정하고 지원하는 등 u-네트워크 보급에 따른 불안해소에 힘쓰고 있다[11].

3.4 EU

EU의 경우 2010년까지 미국을 추월하겠다는 "리스본 전략"과 IT를 동력으로 지속적인 성장을 추구한다는 "i2010"의 성공을 위한 기반으로서 정보보호 정책을 추진하고 있다. 구체적으로는, EU 집행위의 정보보호 전략과 ENISA의 행동계획을 발표하였고, '정보보호 문화 실현'을 위한 관련 정책을 강화하고 있다. 연구개발의 측면에서도 2007년부터 2013년까지 추진될 제7차 Framework Programme에서 90억 유로를 투자할 계획을 세우는 등, IT 및 정보보호 경쟁력 확보를 위해 과감한 정보보호연구개발 투자를 아끼지 않고 있다[9].

3.5 해외 정보보호 동향의 시사점

해외 주요국 정보보호 정책 동향을 살펴보면 다음과 같은 공통점을 발견할 수 있다. 주요국의 정보보호와 관련된 예산이 지속적으로 확대되고 있음을 알 수 있다. 특히 미국의 정보보호 예산이 주요국 중에 가장 많았다. 이는 공공부문의 연방정보보호관리법(FISMA) 등 정보보호 투자를 촉진할 수 있는 법체계와 관련 인프라들이 잘 갖추어져 있기 때문이다.

주요국의 정보보호 정책의 또 다른 특징으로는 민·관 협력모델 구축이 강조되는 것을 발견할 수 있었다. 이러한 경향은 EU쪽에서 두드러지게 나나탄고 있는데, 그 이유는 유럽이 정보보호 위협과 모범사례에 대한 정보공유체계가 잘 작동하고 있지 않기 때문이다. 마지막으로, 법제도 측면에서는 정보보호 전반에 관한 법규, 개인정보보호 관련 법규, 사이버범죄 관련 법규 등이 광범위하게 정비되고 있었으며, 미국의 정보보호 법규수준을 다른 국가들이 벤치마킹하며 따라가고 있다고 볼 수 있다.

4. 미래의 사이버전 대비 발전방향

4.1 미래전 사이버전 위협과 취약점 분석

기존의 전장환경은 유선 네트워크 기반의 정보전달방식으로 전장상황 정보를 획득하고 공유하는데에 많은 시간이 소요되었으며 각 군가의 실시간 전장정보공유는 지휘통제본부에 국한되어 이루어져있다. 그러나 미래전에서는 전군이 네트워크로 연결됨으로서 전장에서 요구되는 전장상황 정보가 실시간으로 공유될 것이며, 또한 정찰감시체계에서 정밀타격 체계까지 네트워킹을 통해 실시간 연동이 가능해질 것이다. 이러한 네트워크 중심전(NCW)환경에서의 정보보호 위협 및 취약요소는 다음처럼 구분할 수 있다.

• 네트워크 중심전(NCW) 환경에서의 전장 인프라는 기존 전장 환경과는 달리 다양한 형태의 유무선 네트워크가 융합될 것으로 예상되며 기존의 전장 환경에서는 대부분 유선 네트워크 환경이었던 것과는 달리 NCW 환경에서는 다양한 형태의 무선 네트워크가 등장할 것으로 예상

된다. 따라서 전투에 참가하는 객체간의 네트워킹을 위한 무선 센서 네트워크, Ad-hoc 네트워크 등의 다양한 무선 네트워크가 도입됨으로써 전투원이 침입하기 힘든 지역을 센서 및 무인로봇을 이용하여 전장 상황 정보를 수집하는 환경이 될 것으로 예상된다. 전장 인프라에 적용되는 기술들은 RFID, USN 등이 있으며, 여기서 나타나는 정보보호 위협 요소들은 다음과 같이 살펴볼 수 있다.

- USN에서 이동단말, 센서 등은 CPU와 배터리의 용량이 적기 때문에 보유자원을 집중적으로 소모시키는 공격을 받을 경우, 해당 서비스의 중단이 예상된다.
- USN은 보안 기능이 취약한 Ad-hoc 네트워크 구조로 이동단말기기에 대한 통제가 어려워 사이버 공격에 취약하다.
- RFID EPC(Electronic Product Code) 네트워크에서는 DB취약성으로 인한 정보유출 가능성이 증대된다.
- RFID ODS(Object Directory System)의 분산 구성으로 어느 한 정보의 위·변조로 연쇄적인 위험을 초래할 수 있다.

• 기존의 전장환경에서는 대부분 음성 위주의 전장 데이터인 반면 NCW 환경에서는 음성뿐만 아니라 영상 등 다양한 멀티미디어 데이터가 융합된 환경이 도래할 것으로 예상된다. 따라서 기존의 음성위주의 데이터를 전송하기 위한 통신장비 및 통신환경은 대용량의 멀티미디어 데이터를 전송할 수 있도록 IPv6 기반하의 광대역통합망으로 진화될 것이며, 이에 대한 새로운 보안 취약점이 대두될 것으로 예상된다. 이에 대한 정보보호 위협 요소들은 다음과 같이 살펴볼 수 있다.

- BcN은 기존 통신망과 프로토콜, 서비스가 상이하며 기존의 정보보호 기술로는 사이버 공격에 대응하기가 곤란하다.
- 개방형 망구조로 인해 통신망에 접근이 용이해 악성코드 및 사이버공격이 용이하다.
- IPv6의 취약점을 이용한 새로운 양상의 공격이 가능하다.
- 인터넷망에서 발생된 위협이 BcN을 통해 통신망 및 USN까지 확산가능하다.
- USN에서 송수신되는 정보 유출로 인한 위험이 확대가능하다.
- VoIP 기술을 이용하여 기존의 회선 교환망에서 인터넷망으로 전환되는 경우, 음성통신도 웜바이러스 등 인터넷침해사고에 노출될 수 있다.
- IPv6망으로의 전환 과도기에 IPv4와 IPv6의 병행사용이 요구되어 End-to-End 네트워크 보안이 어렵다.
- IPv6환경에서는 DNS에 의한 의존도 증가로 주소 위·변조 공격 가능성이 높아져, 피싱과 같은 공격에 악용될 위험성이 증가된다.

• 기존에는 각 군이 관리하고 있는 시스템, 통신망에 대하여 개별적으로 보안관제를 수행하고 있었으나, NCW 환경에서는 전군의 시스템 및 통신망이 연동되므로 전군통합보안체계 구축이 필연적이다.

4.2 사이버전을 대비한 주변국들의 정보보호 동향

미국의 경우에 범세계 통신망에 대한 공격과 방어작전을 위한 정책, 기술지원 및 실행과 국방CERT 운영담당인 JTF-GNO(Joint Task Force-Global Network Operations), 컴퓨터네트워크 방어/공격 임무를 총괄하는 조직인 USSTRATCOM(United States Strategic Command), 전 세계에 대한 사이버공격 및 방어를 주 임무로 하는 JFCC-NW(Joint Functional Component Command for Network Warfare) 등이 있다. 특히 JFCC-NW는 적의 민·군의 주요정보통신기반시설에 침투해 정보통신체계를 마비시키거나 원격제어까지 가능한 능력을 보유하고 있다.

중국군은 국가차원에서 사이버전 교리·체

계·조직·훈련을 강화하고 있다. 90년대 중반부터 사이버 전사 및 전문가를 집중 육성해 유사시 미국과 대만의 군사령부와 통제시스템의 컴퓨터망을 교란시키기 위한 컴퓨터 바이러스 부대를 창설하여 운영하고 있다. 이후 적의 군사 및 민간 사이버 공간에 출몰, 전자 공황 상태를 초래하고 시스템을 마비/파괴시키는 것 등이 포함된 역대 최대 규모의 인터넷 공간상 전쟁훈련을 시행하고 있다.[2] 인민해방군은 현재, 7대 군구 중 4개 군구에 사이버 부대를 운용하고 있는 것으로 추측되며, 현재 정보전을 대비한 각종 무기와 전술을 개발해 미국과 비등한 최강의 정보전 능력을 갖췄다는 평가를 받고 있다.

일본은 정보보호에 대한 국가전반의 요구에 따라 종합적인 정책수립을 추진하기 위해 2004년 내각관방의 IT전략본부에 '정보보호 기본문제 위원회'를, 2005년에는 국가정보보호센터(NISC)를 설치하였으며, 그해 5월 정보보안정책 기본전략 책정, 기본전략에 기반한 정보보안정책의 사전평가 실시, 사후평가와 그 결과 공표, 정보보안대책에 관한 표준화된 안전기준, 안전기준에 기초한 평가결과를 근거로 각성청의 정보보안대책 보고, 긴급사태 대응책 마련 및 실시를 주요 임무로 하는 정보보안안정책회의를 설치하였다. 사이버전 관련하여 일본 방위청은 2000년 바이러스 제작과 사이버공격 기술을 독자적으로 개발하고, 육·해·공군 자위대가 통합 운영하는 사이버전 부대를 창설하는 방침을 발표하였으며, 현재까지 공식적인 발표는 없으나 이미 사이버전 부대가 창설되어 운영되고 있는 것으로 추측된다. 그리고 방위청 전략연구실과 국가방위연구소에서 사이버전 교리개발 및 관련기술, 정책에 대한 연구를 통해 사이버전 부대를 지원하고 있는 것으로 추정된다.

4.3 미래 사이버전 대비방안

유비쿼터스(Ubiquitous) 환경이 도래함에 따라 네트워크의 통합화, 정보통신 서비스의 융합화 등을 통하여 정보보호의 환경이 변화하고 있다. 에너지·금융·전력·교통 등의 기반구조는 정보통신 네트워크로 연결되고 광대역통신망(BcN), u-센서네트워크(USN) 등의 구축에 따라 산재한 컴퓨터를 자유롭게 이용하는 공간 지능화 환경이 초래한 반면에, 사이버 공격으로 인한 개별망의 피해가 유·무선 통합망으로 확대되고 나아가 방송망, USN까지 확산될 수 있는 환경이 되었다. 따라서 성능 중심의 e-정보보호에서 사용자 중심의 u- 정보보호로 정보보호의 개념이 변화되고 있다. 정보보호 패러다임의 변화는 해킹 대응중심의 정보보호에서 사용자의 권익, 행복 및 사생활 보호로 변화되고, 개별서비스 정보보호에서 IT서비스의 융복합화로 융복합 서비스 정보보호로 변화하며, 시스템 및 네트워크 유선 중심의 정보보호에서 유비쿼터스 환경의 무선 및 모바일 중심의 정보보호로 변화되고 있다.

이와 같은 패러다임의 변화는 오늘날 변화하고 있는 사이버 위협 양상에 대한 정보보호 대책을 중심으로 나타나고 있으며, 국내외 주요국들도 이러한 최근의 사이버 위협 특징들을 중심으로 보안대책을 수립하고 있다. 이러한 시사점을 바탕으로 본 연구에서는 u-IT기술의 진화로 사이버 위협요소가 개별망에서 유·무선 통합망으로 확산됨에 따라 BcN, RFID, VoIP, Wibro의 개별적인 정보보호 위협요소와 정보보호 대비방안을 분석하였다.

4.3.1 BcN

광대역통합망(BcN)은 유·무선 통신망, 인터넷망, 방송망간의 연동을 구현하고 최종적으로는 센서 네트워크를 ALL-IP망에 통합하는 통합망으로 이기종망간 접속은 IPv6체계를 이용한다.

2) 1999년 10월, 인민해방군 기관지 해방군보(解放軍報)

가. BcN의 계층별 위협요소

1) 응용계층

사용자의 개인정보 유출, 다양한 콘텐츠에 대한 침해, 개방형 API제공으로 인한 비인증 장비 접속 취약점이 존재한다.

2) 제어계층

QoS 및 보안관리제어 정보의 도청/위변조 위협과 이기종망 연동에 사용자 세션 하이잭킹 위협 그리고 망간 연동관련 장비에 대한 공격의 위협이 존재한다.

3) 전달계층

서비스 품질보장 저해 위협, DDoS/Dos 공격으로 인한 서비스 지연 및 장애, 타망으로의 피해 확산 위협, 접근인증 및 권한문제(불법관리자, 시스템)의 취약점이 존재한다.

4) 접속계층

다양한 단말로부터 과다 트래픽 유발을 통한 DDoS 공격, 이동성 보장에 따른 공격 위치 다양화로 인한 역추적 어려움이 존재하며, 도청 및 비인가 사용자의 접속 취약점이 존재한다.

나. 정보보호 대비방안

안전한 서비스 제공을 위해서 다양한 이기종망들이 통합되는 BcN환경의 구축단계에서부터 운영 및 활성화 단계에 이르기까지 발생 가능한 보안위협을 식별하고 이에 대한 대응책을 마련해야 한다.

1) 종단망 연동시 정보보호 대비책

응용서비스 사용자 등록 메시지 위·변조 위협은 발생 시 사용자 피해의 정도는 크다고 할 수 있으나, 응용서비스 및 공격기법에 대한 고도의 지식과 공격기술을 필요로 하기 때문에 공격 발생 가능성은 낮다. 그러나 공격에 대한 대응을 위해서 사용자 등록세션의 암호화가 요구된다. 서비스 제공자는 응용서비스를 처리하는 서버와 가입자 관리서버가 독립적으로 운영되도록 구성해야 한다.

2) 망간 연동시 정보보호 대비책

망간 대량의 트래픽은 정상 사용 혹은 특정 도메인 내에 발생한 침해사고에 기인한 트래픽 급증으로 타 사업자에 전파될 수 있다. 어느 한 망 도메인에서 보안이 강화된 대책을 운영하더라도, 종단간 서비스의 경우에서는 연동하는 타 망 관리자의 보안 수준이 취약할 경우 발생하는 침해사고로 인해 의도하는 보안 서비스를 제공할 수 없다. 따라서 침해의 원인이 발생한 위치를 확인하는 것 등의 요구사항이 있다.

3) 시스템 보호를 위한 정보보호 요구사항

IP주소, Port 필터링 등을 통해 서비스 시스템에 대한 비인가된 IP주소, 포트 등의 접근을 차단해야 하고 서비스 시스템에 접속시 기기인증 또는 사용자 인증을 수행하여 정상적인 기기 또는 사용자만 접속을 허용한다. 외부에서 메시지 처리시스템에 직접 접근할 수 없도록 하거나, 접근을 제어할 수 있는 네트워크 구조로 운영하여야 한다.

4.3.2 RFID

가. RFID의 정보보호 위협요소

RFID는 비접촉식 기술의 특성과 무선의 취약성, 제3자의 리더기를 통한 정보수집 가능성 등 여러 가지 정보보호 취약성을 가지고 있다. 이는 RFID 시스템이 RFID의 독자적인 기술이 아니라 이전의 기술과의 융합된 신기술이기 때문이다. 따라서 RFID 위험요인은 이전의 기술들의 위험요인들까지도 같은 위험요인으로 인식되어야 한다.

1) 도청

인가되지 않은 리더로 적절한 접근제어 기능이 없는 태그의 정보를 읽는 적극적인 공격과 리

더와 태그간의 무선주파수(RF)를 수신하는 수동적인 공격이 있다.

2) 트래픽 분석

특정 지역에서 태그와 리더가의 트래픽을 통계경계분석(Statistical Threshold Analysis) 또는 패턴 매칭(Pattern Matching)으로 실시간 또는 일괄처리 분석하여 정보를 유추하는 공격기술이다.

3) 스니핑(Sniffing), 스캐닝(Scanning), 스푸핑(Spoofing)

- 스니핑(Sniffing) : 네트워크상에서 다른 목적지로 향하는 다른 모든 패킷을 감시
- 스캐닝(Scanning) : 네트워크에 접속된 서버들의 유형, 운영체제의 버전과 데몬들의 정보를 알아내는 것
- 스푸핑(Spoofing) : IP를 변조하거나 응답을 변조하여 서버를 속이는 것

4) 서비스거부(DOS, Denial of Service) 공격

여러대의 장비 또는 시스템을 이용하여 RFID 서버가 처리하지 못할 엄청난 데이터를 집중적으로 전송함으로써 서버의 정상적 기능을 방해하는 것

5) 세션 가로채기(Hijacking), 재생(Reply), 중간자 공격(Man in Middle Attack)

RFID 리더와 태그 사이의 상호인증을 위한 인증 프로토콜 수행시 발생할 수 있는 공격들로 인증된 세션을 가로채거나 프로토콜 일부를 다시 실행시키는 재생공격, 인증 프로토콜 수행 중간에 정보를 삽입하는 공격등이 있다.

6) 위조

태그 또는 리더를 위조하여 정보를 변조하는 위협행위

나. RFID 정보보호 대비방안

RFID 시스템은 기존의 정보시스템의 보호기술을 그대로 적용하기에는 RFID 자체의 환경적·기술적 차이가 많다. 따라서 기존 정보시스템의 정보보호 기술을 분석하여 적용 가능한 정보보호 기술을 도입하여 효과적으로 시스템을 구성하는 것이 필요하다. 대부분 RFID 시스템을 공격하는 경우, 앞서 설명한 정보보호 위협요소를 1개 또는 2개 이상 조합하여 RFID 시스템을 공격한다. 일반적으로 예상할 수 있는 공격유형은 악의적인 공격자가 태그의 정보를 얻고자 시도하는 경우, 정상적인 리더와 태그 사이의 데이터를 공격자가 엿듣는 경우, 공격자가 정상적인 데이터를 위조하여 리더 또는 태그를 혼란시키는 공격, 태그와 관련된 데이터를 입수하기 위해 서버에 불법적으로 접근(해킹)하는 경우, 그리고 인증되지 않은 DoS 트래픽으로 공격하는 경우로 분류될 수 있다. RFID/USN 환경에서는 개인이 소유한 모든 물체 단위까지 침해 범위가 확대되고 태그·센서 정보의 무단 유출 및 위·변조, 오동작, 개인추적정보의 불법 수집·유통 등과 같은 새로운 보안 위협 초래된다. 따라서 RFID/USN 서비스를 안전하게 제공하기 위한 초경량 객체정보 기술개발이 요구된다.

4.3.3 VoIP

VoIP 정보보호 위협요소로는 음성패킷을 불법으로 수집 및 조합해 통화내용을 재생하는 도청을 비롯하여 서비스 관련 시스템 자원 고갈 및 비정상 패킷의 다량 발송을 통한 회선 마비 등의 서비스거부(DoS)공격이 있다. 사용자의 등록정보를 조작하거나 추가해 서비스를 이용하는 서비스 오용공격, 사용자 등록 과정에 개입해 사용자의 세션 제어권한 등을 획득하는 세션 가로채기, 인터넷 회선을 공유해 녹음기 등을 통해 발송하는 VoIP 스팸도 있을 수 있다.

VoIP 기술도입시 사전에 고려해야 할 정보보호 요구사항은 VoIP 프로토콜의 보안특성과 IP 기반 환경에서 현재 알려진 취약점 및 잠재적인 보안위협 유형을 이해하여 서비스 제공에 앞서

고려해야 하는 정보보호 목표라고 할 수 있다. 안전한 망 설계 방안과 장비 및 트래픽 보호, IP 보안 위협에 대한 대책, 방화벽/NAT 통과 해결, 관리적 대책 등이 세부 내용이다.

실시간 멀티미디어 서비스에 적합한 암호화 기술개발과 긴급통화서비스 제공 방안, 안전한 VoIP 응용서비스 제공방안, 보안 기술간 상호운용성 확보 방안 및 QoS 상충문제 해결, 합법적 감청지원 방안 등이 요구된다.

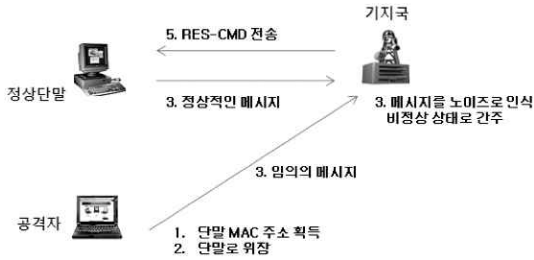
세션가로채기는 프로토콜에 대한 MitM 방법으로 공격자는 Proxy 서버에 스푸핑 등의 방법으로 가장하여 사용자의 INVITE 메시지를 가로채 통신제어 권한을 획득하고 통화를 가로채는 공격이다. 세션가로채기로 통화정보 및 음성통화내용을 도청할 수 있고 통화를 강제 종료시키거나 사용자 위장 공격을 할 수 있다. VoIP 스팸 공격에 대응은 상대적으로 상당히 어려움이 존재한다. 전화서비스의 특성상 불특정 다수로부터 수신되는 호를 사전에 필터링하기가 어렵고 VoIP 스팸이 P2P방식으로 발송될 경우에는 사업자의 스팸차단 정책을 우회할 수 있기 때문이다. E-mail 스팸처럼 발신자의 신분조작이 용이하여 접속의 다양성으로 인해 스패머의 위치추적에 어려움이 있다.

4.3.4 Wibro

Wibro(Wireless Broadband)는 무선광대역 인터넷의 의미를 내포하고 있다. 와이브로는 이동전화단말기처럼 정지/이동 중일때 언제 어디서나 인터넷을 사용할 수 있다는 점에서 무선랜이나 초고속인터넷, 모바일 인터넷 서비스와 다르다.

가. Wibro 정보보호 위협요소

와이브로 서비스 환경은 기존 인터넷에서 발생하는 보안취약성이 그대로 나타날 수 있을 뿐만 아니라, 와이브로 자체의 특징에 의한 새로운 보안위협이 존재한다. 와이브로 환경에서 발생 가능한 위협은 정상단말로 위장하여 서비스거부



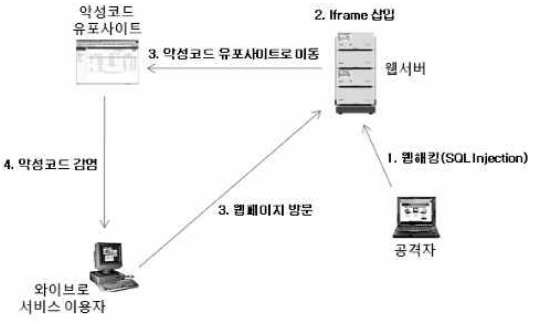
(그림 2) 정상단말로 위장하여 서비스공격 유도

(그림 3) EAP 메시지를 이용한 서비스거부공격 유도

공격을 유도하거나, EAP 메시지를 이용한 서비스거부공격을 유도할 수 있다. 기존인터넷 환경에서 발생했던 위협은 홈페이지 해킹을 통한 개인정보 유출과 사회 공학적 방법에 의한 악성코드를 유포하는 행위이다.

(그림 2)은 와이브로 환경에서 RES-CMS라는 메시지를 이용하여 서비스공격이 발생하는 동작절차를 나타내는 것으로, 위와 같은 위협에 대비하기 위해서는 각 단말의 메시지 트래픽에 대한 모니터링을 통해 비정상적인 동작을 하는 단말을 탐지하고 지속적으로 이상 징후를 보일 경우에 이에 대처할 수 있는 관리적 방안이 필요하다.

(그림 3)는 EAP Start 메시지에 의한 서비스거부공격의 동작절차를 나타내는 것으로, 와이브로 단말은 EAP 기반 인증을 받기위해, 우선 인증 요청메시지를 기지국에 보낸다. 이 메시지를 받은 기지국은 EAP 기반 인증과정이 시작됨을 인지하고, 단말에게 Identity를 요구하며 인증을 시작한다. 일단 인증이 시작되면 기지국은 같



(그림 4) 홈페이지 해킹을 통한 개인정보 유출

은 단말로부터 수신한 인증요청 메시지를 무시하게 된다. EAP Start 메시지에 의한 공격방식은 이러한 취약성을 이용한다. 공격자는 정상단말로 위장한 뒤 정상단말이 EAP 인증요청을 하기 전에, 기지국에 EAP 인증요청 메시지를 지속적으로 보낸다. 이때 정상단말이 전송하는 EAP Start 메시지는 기지국이 수신하지 못하기 때문에, 정상단말은 망에 접속할 수 없다. 이 공격이 지속적으로 이루어질 경우, 서비스거부공격으로 나타낼 수 있다. 이러한 보안위협에 대응하기 위해서는 EAP-Start 등의 메시지에 대해서 와이브로 시스템에서만 보낼 수 있도록 설정하거나, 각 단말들의 와이브로망 접속 성공, 실패 등의 통계자료를 통해 비정상적인 동작을 하는 단말을 탐지하고 대응할 수 있는 방안이 필요하다.

홈페이지 해킹을 통한 개인정보 유출은 기존 인터넷 환경에서 발생했던 보안 취약성이지만, 와이브로 서비스 환경에서도 그대로 발생할 수 있다. (그림 4)는 홈페이지 해킹을 통한 개인정보 유출 과정을 보여준다. 이 그림은 와이브로 서비스 환경에서 일반 사용자가 웹사이트 접속 시, ID, Password 등 개인정보가 공격자에게 유출될 수도 있는 보안위협을 보여준다. 이러한 위협을 예방하기 위해서는 보안패치 및 백신 바이러스 프로그램을 설치가 필요하다. 또한 사회공학적 방법에 의한 악성코드 전파도 중요한 위협이 된다. 사용자의 부주의로 인한 악성코드 감염 사례가 증가할 수도 있기 때문이다.

나. Wibro 정보보호 대비방안

1) 단말에서의 정보보호 대비방안

사용자가 단말을 분실할 경우를 대비하여 이를 신고할 수 있는 신고센터와 분실된 단말은 이용할 수 없도록 하는 시스템이 있어야 한다. EAP 인증시스템 또는 공개키 기반 인증(무선 PKI)등과 같이 단말과 기지국간 상호인증기술이 적용되어야 한다. 단말과 기지국에서 무선주파수를 이용하여 전송되는 데이터가 노출될 수 있다. 데이터 암호화방식으로 128bit AES기반 암호방식 등 강력한 방식을 적용해야 한다. 단말과 기지국에서 전송되는 데이터의 무결성 보장을 위해 CRC와 CheckSum등과 데이터 오류 검사기능과 데이터에 대한 해쉬값을 암호화하여 전송하는 등과 같은 위변조 방지기법이 필요하다. 단말과 기지국과의 통신을 위해 사용하는 무선주파수 대역을 지속적으로 감시하고, 변동사항을 주시할 수 있는 기술기법을 기지국에 탑재하여 이에 대한 위협을 조기에 탐지하거나 단말 및 관제 센터에 통보할 수 있는 시스템의 구축이 필요하다. 기지국 및 단말에서 지속적으로 연결을 요청하는 단말 및 기지국을 식별할 수 있는 기술이 있어야 한다. 또한 기지국 및 단말에서 지속적인 연결메시지를 거부하거나 차단할 수 있는 기술이 있어야 한다. 단말이 기지국에 연결을 요청하는 과정에서 전송되는 메시지의 위변조 및 메시지를 전송한 주체에 검증과정이 필요하다. 단말이 기지국과 인증을 수행하는 과정에서 인증결과를 보내는 메시지에 대해 위변조 및 전송주체에 대한 검증과정이 필요하다. 단말(기지국)이 기지국(단말)에 연결을 종료하기 위해 전송되는 메시지에 대한 위변조 및 메시지 전송주체에 대한 검증과정이 필요하다. 단말이 기지국에 재인증을 요청하는 메시지에 대한 위변조 및 메시지 전송 주체에 대한 검증과정이 필요하다.

2) 기지국에서의 정보보호 대비방안

기지국에 접근하여 사용하는 내부자에 대한 관리감독이 필요하다. 기지국을 사용하는 경우 ID, Password와 같은 인증과정을 거친 후 사용하도록 한다. 외부에서 네트워크를 통해 접근하여 기지국을 이용할 수 없도록 하거나 기지국에 접근할 수 있는 IP주소 및 사용자를 제한해야 한다. 기지국에 접속하려는 단말은 단말 인증뿐 아니라 항상 EAP 인증 시스템(EAP-AKA) 또는 공개키 기반인증(무선 PKI) 등과 같은 인증과정이 필요하다. 기지국에 설정된 기본적인 ID, Password를 삭제하거나, 기본적인 ID/Password를 통해 기지국의 중요정보에 접근하지 못하도록 접근제한을 둔다. 또한 각 사용자별로 접근할 수 있는 데이터 항목을 구분하여 설정할 수 있도록 하는 기술을 적용한다. 기지국과 장치 및 서버사이에 전송되는 데이터를 생성한 주체 검증하는 과정이 필요하다. 또한, 전송된 데이터가 변조 되었는지를 판단할 수 있는 검증과정이 있어야 한다. 기지국과 장치 및 서버와 전송되는 데이터에 대해 암호화 기능을 적요하여 데이터가 유출되지 않도록 해야 한다. 기지국(사용자 단말)에서 사용자 단말(기지국)과의 접속을 종료하는 경우, 접속종료를 요청하는 메시지 및 메시지를 보낸 주체에 대한 검증과정이 필요하다. 기지국은 일정시간이 지나면 재인증을 요청한다. 일정시간이 지나지 않은 상황에서 공격자가 정상적인 사용자 단말로 위장하여 재인증 메시지를 전송할 때, 전송되는 메시지를 보내 주체 및 메시지 변조여부를 검증해야 한다. 사용자 단말이 다른지역으로 이동하는 경우, 기존 기지국과의 연결을 종료하기 위해 핸드오프 메시지를 전송한다. 기지국에 전송되는 메시지를 보낸 주체 및 메시지 변조 여부를 검증해야 한다.

3) 제어부에서의 정보보호 대비방안

제어국에 접근하여 사용하는 내부자에 대한 관리감독이 필요하다. 제어국을 사용하는 경우 ID, Password와 같은 인증과정이 필요하다. 외부에서 네트워크를 통해 제어국을 이용할 수 없도록 하거나, 제어국에 접근할 수 있는 IP주소 및 사용자를 제한해야 한다. 제어국의 서비스를 이용하려는 서버 및 장치는 항상 공개키 기반인증(유선 PKI)등과 같은 인증과정을 거치도록 한다. 제어국으로 장치 및 서버사이에 데이터를 전송하는 경우 데이터를 생성한 주체에 대한 인증 및 데이터 위변조 여부를 검증할 수 있어야 한다. 기지국과 장치 및 서버와 전송되는 데이터에 대해 암호화기능을 적용하여 중요 정보가 유출되지 않도록 해야 한다. 제어국에 속한 기지국 및 사용자 단말에 대용량의 데이터를 전송하는 경우 제어국에 미리 전송할 데이터의 양을 통보하는 메커니즘을 도입하여 제어국의 용량에 맞게 처리할 수 있도록 해야 한다.

5. 결 론

유비쿼터스와 컨버전스 환경을 기반으로 제공되는 미래의 정보통신 서비스는 개인의 사적·공적 정보가 혼재되어 사용될 것이다. 이러한 정보들이 악의적인 의도를 가지고 활용될 경우 그 파급효과는 개인은 물론 국가적인 차원의 재앙으로 발전할 수 있는 소지가 있다. 따라서 향후에 새로운 IT를 통해 제공되는 서비스들이 신뢰할 수 있는 수준에서 제공될 수 있도록 정보보호 기반구조를 튼튼하게 만들도록 노력해야 할 것이다. 또한 사용자 중심의 u-정보보호로 정보보호의 패러다임의 변화가 사이버 위협의 형태 또한 변화하도록 하는 이런 시점에서 사이버 위협 양상에 대한 정보보호 대책을 해외의 주요국들이 최근에 보안 대책을 수립하고 있는 만큼, 우리 또한 정보보호를 위한 체계개발과 전략 및 보호를 위한 요구기술들을 하루빨리 확보해야 하는 중요한 시점이라는 사실을 인식하여야 할 필요가 있다. 국가안보와 직결되는 국방정보보호

를 위한 대책으로는 정보보호위험관리체계, 전장관리체계에 대한 통합보안관체체계, 사이버전 수행지원을 위한 사이버전 모의훈련체계와 같은 정보보호체계를 구축해야 하며, 또한 정보보호 기술을 위해서는 네트워크 중심전(NCW) 인프라 보호를 위한 기술과 네트워크 중심전(NCW) 실시간 전장 데이터 보호에 필요한 보호기술, 그리고 네트워크 중심전(NCW) 보안상황 인지 및 대응에 필요한 기술이 요구될 것이다.

참고문헌

[1] 노훈-이재훈, "사이버전의 출현과 영향, 그리고 대응방안", 국방정책연구(가을)(서울: 한국국방연구원, 2001), p 180

[2] 박상서, 박춘식, "정보전 위협과 사례", 정보보호학회지, 제12권 6호, 2002.12.

[3] 배달형, "정보작전의 이해", 국방전문연구시리즈 08-10(서울: 국방연구원, 2003) pp71-76

[4] 손태식, 서정택, 은유진, 이철원, 장준교, 김동규, "Heap과 Stack 영역에서의 경계 체크를 통한 Buffer Overflow 공격 방지 기법에 대한 연구", 정보보호학회지, 제11권 6호, 2001

[5] 서동일, 손승원, 조현숙, 이상호, "정보전 기술과 개발현황", 정보보호학회지, 제12권 6호, 2002.12.

[6] CERT/CC, 「Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues」, 2002

[7] CERT/CC(2), 「overview of attack trends」, may 2002.

[8] http://www.cert.hu/dmdocuments/Estonia_attack2.pdf

[9] http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD. pdf

[10] Martin C.Libiki, What is information warefare, 1995

[11] NIA, 「주요국 정보보호 동향조사」 2006. 12.

저자약력

김 승 권

1995년 한국외대 체코어(학사)
1998년 한국외대 경영학(MIS) (석사)
2007년 고려대학교 경영학(MIS) (박사)
2006년~현재 안보경영연구원 책임연구원
관심분야 : 소프트웨어 평가, CMMI, 정보보호 및 정보보안
이 메 일 : sgkim@smikorea.org

김 상 국

1998년 한양대학교 산업공학(학사)
2000년 서울대학교 산업공학(석사)
2007년 Ph.D in Mathematical Science, Florida Insitute of Technology
2008년 4월~현재 안보경영연구원 책임연구원
관심분야 : Queueing, Stochastic Control, Fuzzy in SCM, 데이터 암호화 기법
이 메 일 : sanggook_kim@smikorea.org

최 종 화

2001년 세종대학교 컴퓨터공학과 (학사)
2005년 세종대학교 컴퓨터공학과 (석사)
2008년 세종대학교 컴퓨터공학과 (박사)
2007년 12월~현재 안보경영연구원 책임연구원
관심분야 : 지능형 홈 서비스 로봇, 게임물리엔진, HCI, 국방 M&S
이 메 일 : jhchoi@smikorea.org