유비쿼터스 환경에서의 국방 정보보호 발전 방안

김영화, 김정태
목원대학교

A Development Plan of Military Information Security in Ubiquitous Environment

Young-Hwa Kim, Jung-Tae Kim
Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

요 약

현재 우리나라는 유·무선의 통합, 광대역 통신기술 구현 및 디지털 컨버전스 등 첨단 기술이 실생활에 적용되고 있으며, 완전한 유비쿼터스 사회로의 진입을 위한 환경 구축이 정부 및 자치단체, 연구소, 관련 기업 등 여러 기관 및 단체별로 순차적으로 진행되고 있다. 국방 부분에서도 우리나라의 첨단 정보통신 기술을 바탕으로 과거부터 운영 중인 플랫폼 기반의 기존 전력을 재정비하여 첨단 선진군으로의 변화를 꾀하고 있다. 하지만 이와 더불어 해킹·바이러스 기술의 고도화를 통한 사이버테러 및 범죄 등의 침해 행위가 단순한 개인의 차원을 넘어서 국가적인 형태로 급진전되는 등 국방 분야 또한 이러한 위협으로부터의 정보보호가 더욱 중요한 이슈로 대두되고 있다. 이에 따라, 본 논문에서는 유비쿼터스 환경에서의 국방 정보보호기술의 발전 방안에 대하여 살펴보고 이러한 문제를 해결하기 위한 방법을 찾고자 한다.

Ⅰ. 서 론

정보기술의 발전에 따른 사회 전반에 걸친 정보화 추진과 정보체계 활용도 증가는 시/공간적 제약이 없는 정보의 자유로운 공유 및 유통을 보장하는 등 많은 긍정적인 발전을 가능하게 했으나, 해킹·컴퓨터 바이러스 등의 새로운 유형의 위협이 등장하는 기반을 제공하기도 하였다. 군도 국방정보화의 추진에 따라 다양한 정보통신 기술이 활용됨으로써, 새로운 위협 및 취약성이 증가하고 있다. 과거의 전쟁양상은 대량살상 및 파괴로 적의 저항을 무력화시키기 위한 것이며, 이는 대부분 전쟁에 사용된 무기체계에 의존한 것이다. 앞으로의 미래전 에서는 단일 무기체계에 의한 의존도는 점차 감소하며, 각종 정보수집 및 분석체계를 이용하여 적의 상황 및 전장상황을 한눈에 보고, 시·공간적으로 통합된 네트워크를 통하여 전 제대가 상황을 동시에 인지하며, 정밀타격/비 살상무기체계를 통하여 적의 핵심만을 무력화시켜 인명살상을 최소화시키는 방향으로 전개될 것이다. 이러한 변화는 비단 전장이라는 특수한 환경과 공간에서 뿐만 아니라 평시 인력, 군수 등 자원관리 분야와, 모병 및 병사 면회 등의 일상 군 생활에도 적용되어 일반사회의 정보화 환경과 크게 다르지 않으며, 오히려 군 이라는 특수성을 이용하여 일반 사회에서는 비용 투입의 제한으로 하기 어려운 신기술 적용 등의 시험 적용이 이루어 질 수 있다. 2006 국방백서의 국방정보화 추진은 크게 전장관리 정보화, 자원관리 정보화, 정보화 환경 조성의 3가지로 분류되어 언급 되어있으며, 이를 위하여 지휘통제체계와 전장관리의 자동화로 군사력의 질적 변환을 도모하고, 국방자원 관리의 디지털화와 전자거래를 기반으로 저비용·고효율의 국방관리와 운영을 실천하며, 이를 위해 정보화 기반을 확충하고, 국가정책과 연계된 국방정보화 정책을 추진하는 동시에 정보화 교육을 추진하고 있다[1]. 본 논문에서는 성공적인 국방 정보화 추진을 위하여 IT 환경변화에 따른 국방 환경의 변화와 유비쿼터스 환경에서의 국방 정보보호 기술 적용 및 발전에 관하여 살펴보고자 한다.

Ⅱ. IT 환경변화에 따른 국방 환경 변화

1) 유비쿼터스 사회로의 변화

현재 우리사회는 광대역 네트워크 인프라(BcN)를 기반으로 사람, 컴퓨터, 사물이 연결되는 유비쿼터스 환경으로 급격히 전환 중이다.

표 1. IT 환경 변화 특성[2]

구 분	전산화	정보화	유비쿼터스
시기	1980년대~1990년대 중반	1990년대 중반~2000년대 중반	2000년대 중반 이후
Keyword	자동화	온라인화	컨버전스(융합)
주요 구성	H/W, S/W	H/W, S/W, N/W	H/W, S/W, N/W, Sensing
서비스 특징	개별서비스	Seamless 서비스	자율서비스
정보의 유용성	정보축적	정보공유/확산	사물의 지능화
주 거래 방식	오프라인	온라인, 오프라인 병행	온라인-오프라인 연계

향후 5년간 네트워크에 연결되는 광의의 단말(Network Appliance)은 현재보다 100배, 10년 후에는 수만 배 규모로 증가하면서 총체적인 네트워크 연결시대(Network of All)로 변화할 것임. 사람과 사람(P to P) 간의 의사소통에 통신도구를 활용하던 것을, 사람과 기계(P to M), 사물과 사물(T to T)간에도 연결되어 통신이 이루어지는 유비쿼터스 환경으로 변화될 것임.

2) 최근 사이버위협의 특징

- **다기능 악성코드 출현 및 전파속도 고도화**

최근의 악성코드는 바이러스+자기복제+트로이목마+발신지제거 기능이 포함된 형태로 나타나며 기존 웜과 바이러스간의 경계가 파괴됨. 주로 TCP를 이용한 단일 프로토콜 이용 전파방식에서 다양한 전파방식(TCP, UDP, P2P, e-mail 등)을 사용하며, 취약점을 공격하여 유포하는 전파방식이 자동화됨. 단시간에 다수의 대상을 감염 시키기 위해 IP 주소 선택 알고리즘이 개선되었음.[3]

- **탐지를 회피하기 위한 웜·바이러스 출현**

탐지를 피하기 위해 잠복기를 갖거나 고의로 느리게 전파하는 웜도 출현하였으며, 정상 프로토콜이나 사용자 행위를 모사하여 탐지를 회피하는 기술을 보유하는등 날고 지능화 됨.

- **공격도구의 지능화**

개별적인 침입시도에서 자동화된 공격으로 전환되어 공격의 신속하여 졌으며, 침입차단 시스템의 기능을 무력화 하고 IDS를 우회하여 게시판을 공격 하는 등 날로 다양화, 지능화 됨.

- **시스템의 취약점을 이용한 공격 증가**

매년 2배 이상씩 증가되는 취약점을 이용하며, 0-day attackd이 증가됨

- **기간망에 대한 공격 증가**

과거 컴퓨터에 대한 공격에서 네트워크에 대한 공격으로 대상이 변경되고 있으며, 서비스 거부 공격, 웜 공격, DNS 공격, 라우터 공격이 주를 이룸.

- **해킹의 범죄화**

과거의 지적 호기심 충족과 도전정신의 실현을 위한 해킹에서 근래에는 중요 정보 절도, 개인정보 절도를 통한 금전전 이익 추구, 적국 또는 공격 대상에 대한 스파이 행위 및 테러에 악용되는 등 날로 그 심각성이 더해감.

3) 유비쿼터스 국방 정보보호 환경

- **네트워크를 통한 정보 공유**

네트워크 통합 및 연동이 증가하여 과거 국방 전용망, 체계별/목적별 통신망 이용 환경에서 seamless한 정보 유통을 보장하는 통신망 구조로 변경됨. 또한 정보의 생성, 소비, 유통의 수준 및 범위가 확장되어 유통 정보량이 급격히 증가하여 기반 네트워크 속도 및 대역폭 확장이 불가피함. 전장 환경변화에 따라 신속한 재구성/확장이 가능한 네트워크 구조의 동적인 변화/발전이 필요.

- **정보에 대한 통제 및 검증 제한**

정보통제 요구는 네트워크 수준에서 단위시스템/데이터 수준으로 확장되며, 정보 생산자/소비자의 사전 예측이 제한됨.

- **상용기술의 의존도, 활용도 심화**

기반 기술의 발전은 민간 영역에서 주도

- **지역적인 공격/침해가 전체로 쉽게 확산**

네트워크/시스템 연동이 확대되어 공격/침입 경로 또한 증가됨. 핵심 노드/연관체계 공격시 목표체계 마비/방해가 발생.

- **동적 네트워크 환경의 보안성 유지/관리 제한**

NCW(Network Centric Warfare : 네트워크 중심전) 작전 환경의 네트워크는 무선기술 활용이 확대되며, 무선 환경 정보보호기술의 미성숙으로 동적 네트워크 환경의 보안관리 기반 및 기술이 미비함.

- **불법적 체계 접근 및 활용 가능성 증가**

NCW 환경에서 통제 대상은 비약적으로 증가되며, 사용자의 사전 정의가 제한 됨. 한 네트워크/체계 중심 식별/인증 기술의 확대 적용이 제한됨.

III. U-환경에서 국방 정보보호 기술 적용/발전 방향

1) 침입대응 시스템

최근 바이러스 활동은 감소한 반면, 웜을 비롯한 각종 침입들은 새로운 형태를 취하며 점차 능동적으로 진화하고 있다. 새로운 악성 코드 및 공격들을 탐지하고 방지하기 위한 시스템은 침입 종류와 대응방식에 따라 크게 침입차단시스템(Firewall), 침입탐지시스템(IDS), 침입방지시스템(IPS)으로 분류할 수 있다.

- **침입차단시스템(Firewall)**

침입차단시스템은 라우터, 컴퓨터, 호스트 또는 호스트들의 집합이 될 수 있으며, 서브넷 밖의 호스트에서 남용될 수 있는 프로토콜과 서비스로부터 사이트나 서브넷을 특별히 보호하도록 구성된다. 개인 컴퓨터에서 사용가능한 형태로 만들어진 개인방화벽은 차후 그 사용이 널리 확산될 PDA나 스마트폰 등과 같은 모바일 기기를 위하여 필수적이며, 최근의 스마트 방화벽, 인텔리전트 방화벽, 능동형 방화벽은 단순 패킷 필터링 기술을 넘어서 상태 검사기법(Stateful Inspection)과 패킷 세부 검사기법(Deep Packet Inspection) 기법 등을 발전시켜 패킷 어플리케이션 콘텐츠에 대한 필터링도 제공하는 웹 방화벽의 적용이 필요하다.

- **침입탐지시스템(Intrusion Detection System)**

침입탐지시스템은 자원의 무결성(Integrity), 비밀성(Confidentiality), 가용성(Availability)을 저해하는 행위를 실시간 감지하는 것으로, 방화벽이 해킹되었을 경우는 물론 서브넷의 시스템 해킹시 이를 인지하도록 하며 해킹의 구체적인

내용을 관리자에게 알려주어 그에 따른 대응을 할 수 있도록 한다.

- **침입방지시스템(Intrusion Prevention System)**

침입방지시스템은 공격 시그니쳐를 찾아내 네트워크에 연결된 기기에서 수상한 활동이 이루어질 경우 자동으로 대응작업을 수행하여 행위를 중지시키는 시스템으로, 침입탐지시스템의 갈수록 복잡하고 지능화되는 보안침해 방법과 기술에 대처에 한계로 침입방지시스템으로 대체가 이루어지는 추세다.

표 2. IDS와 Firewall의 비교[4]

구 분	IDS	F/W
주요역할	탐지(Detection)	방어(Prevention)
물리적위치	내부에서 불법사용자 감시	외부와 내부 경계에서 외부출입자 방어
설계정책	명백하게 금지하는 것만 금지	명백하게 허용하는 것만 허용
시스템 장애시 네트워크 상태	네트워크가 오픈됨	네트워크 사용불능
네트워크 부하	적음	병목현상 발생

- **보안운영체제(Secure Operating System)**

보안운영체제란 컴퓨터 운영체제의 커널(Kernel)에 부가적인 보안 기능을 추가한 운영체제를 말하며, 서버의 보호, 시스템 접근 제한, 관리자에 의한 권한 남용 제한, 응용프로그램 버그를 이용한 공격으로부터의 보호 등 네트워크 중심 보안제품의 한계를 보완하는 것으로, 운영체제 수준의 보안성 보장과 실행 단계에서 권한을 안전하게 통제할 수 있는 보안운영체제의 사용이 요구된다.

2) 악성코드 대응

악성코드는 크게 바이러스, 웜, 트로이목마, 스파이웨어, 스팸 메일, 피싱으로 구분할 수 있으며 이에 대한 예방 시스템 운영이 요구된다.

- **바이러스 · 웜 · 트로이목마 탐지 및 예방**

바이러스, 웜, 트로이목마를 탐지하고 차단하는 방역체계의 사용 및 주기적인 업데이트가 필수적이다. 최근에는 PC 뿐만 아니라 모바일 기기를 대상으로 한 악성프로그램이 발견되고 있으며, 그 추세는 점점 증가할 전망이다. 복잡하고 고도화된 다양한 형태의 무선 단말기들이 네트워크상에서 다양한 파일 및 정보교환의 목적으로 사용될 것이 예상되며, 이에 대한 대응이 요구된다.

표 3. 바이러스, 웜, 트로이목마 특성 비교

구 분	바이러스	웜	트로이목마
자기복제	○	○	×
숙주 필요여부	○	×	×
전파방법	감염 파일의 실행 감염 디스크를 통한 부팅	감염대상을 자동 검색하여 전파	전파되지 않음
전파대상	파일 및 부트 섹터	네트워크 전체	전파되지 않음
악성행위	데이터 파괴 네트워크 마비	데이터 파괴 네트워크 마비	정보유출 검퓨터 제어

- **스파이웨어 탐지 및 예방**

스파이웨어는 웹서버나 개인 컴퓨터에 설치되어 정보들을 유출시키는 악성코드로, 사용자의 동의하에 또는 호스트의 취약점을 이용하여 설치된다. 스파이웨어는 차단 프로그램이나 통합 보안 시스템을 이용한다.

3) 인식 및 인증

PKI(Public Key Infrastructure)와 같은 인증서 기반의 전자서명과 SSO(Single Sign On)과 같은 다양한 인증 메커니즘을 단일 로그인 서비스하는 방식에서 AC(Attribute Certificate)를 이용한 사용자 권한 관리 기법인 PMI(Privilege Management Infrastructure)로의 전환이 예상된다. 유/무선의 다양한 네트워크 환경을 고려할 때 네트워크 연동시의 문제와 다양한 체계의 통합 인증, 소형 무선 환경에서 적합한 암호 관련 기술의 개발이 요구된다.

- **PKI(Public Key Infrastructure)**

PKI는 공개키 기반 구조로써, 네트워크 환경에서 보안 요구사항을 만족시키기 위해 공개키 인증서 사용을 가능하게 해준다. 메시지 암호화 시 사용되는 공개키와 개인키는 인증기관에 의해 같은 알고리즘을 사용하여 동시에 만들어지며 대부분 RSA(Rivest-Shamir-Adleman) 공개키 암호 방식을 사용한다. 암호화된 메시지 송신시는 수신자의 공개키를 사용하며, 암호화된 서명 송신 시에는 송신자의 개인키를 사용한다. 암호화된 메시지 해독 시에는 수신자의 개인키를 사용하여 복화하며, 암호화된 서명을 해독하고 송신자를 인증하기 위하여 송신자의 공개키를 사용한다.

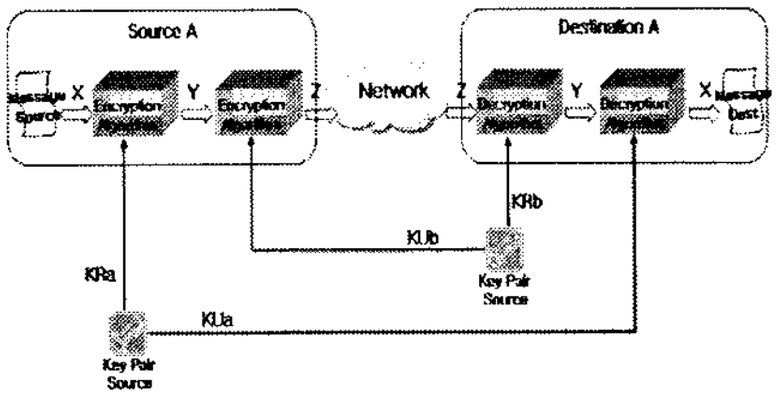

그림 1. 공개키 암호시스템(기밀과 인증)[5]

- **SSO(Single Sign On)**

SSO는 단 한번의 사용자 인증 및 권한 부여로 사용자가 가진 권한 범위 내에서 모든 컴퓨터와 시스템에 접근이 가능하도록 하는 메커니즘이다. 다양한 체계에 사용되는 로그인 정보를 별도로 관리할 필요가 없어 사용자의 개인 정보 유출 등의 문제를 효율적으로 개선할 수 있다.

- **PMI(Privilege Management Infrastructure)**

PMI는 다양한 응용 환경에서 특정 리소스에 접근할 수 있는 권한을 차등적으로 부여하여 보안 관리를 하는 메커니즘이다. 사용자 인증만으로 한정된 PKI와 달리 PMI는 인증뿐만 아니라 접근 권한까지 체계적으로 관리한다.

• **스마트카드**

스마트카드는 인증을 목적으로 사용되는 칩 기반 카드로 단말기와 직접적으로 통신하며, 자체전력을 가지고 있지 않고 단말기 등의 외부 장치로부터 전력을 공급받는다. 리더기 내에 삽입하여야 하는 특성 때문에 암호화 알고리즘을 수행하기에 적합한 접촉식 스카트카드와, 모든 비트에 대해 데이터 암호화 기술을 적용하는 비접촉식 스마트카드, 이를 결합한 하이브리드 스마트카드 등이 있다.

• **바이오인식 시스템**

사람마다 가지고 있는 고유한 생체정보는 보안성과 더불어 편리성을 제공한다. 접근제어 부문에서 여러 가지 활용이 가능하며, 체계설계 시는 특성을 고려하여 적합한 기술을 사용해야 한다. 특히 전장 환경을 고려하여 볼 때 신체의 일부분의 손상으로 인하여 사용이 불가할 경우 및 복제의 위험성을 줄이기 위하여 타 인증기술의 중복사용이 요구된다. 대표적인 활용 기술로는 음성, 지문, 망막, 홍채, 정맥인식 등이 있다.

• **일회용 패스워드(OTP : One Time Password)**

시스템이나 네트워크 접근에 대한 인증은 주로 기억된 비밀번호에 의존되어 노출시 악의적인 접근이 가능하다. OTP 인증은 비밀번호가 노출되더라도 다음 번 접근시는 다른 패스워드를 사용하는 일회용 암호 방식 인증으로 보다 안전하다.

4) 무선환경 보안

앞으로 일상생활은 물론이고 전장 환경을 고려하여 볼 때 무선 통신이 차지하는 비중은 점차 커질 것이 분명하다. 기존 통신망 운영의 이동상의 제한을 극복하여 뛰어난 성능과 편리성을 모두 갖춘 무선 네트워크를 활용하기 위해서는, 무선환경에 적합한 보안기술 개발이 요구된다.

• **RFID(Radio Frequency Identification)**

RFID는 소형 반도체 칩을 부착하여 무선주파수를 이용하여 사물을 식별하고 데이터를 주고받는 기술이다. 저렴한 가격 및 이용의 편의성으로 인하여 군수 물류 관리, 출입자 관리 등의 부분에서 주료 활용된다. 하지만, RFID 센서의 기능이 아주 단순하기 때문에 높은 보안기술을 접목시키기 어려운 단점이 있으며, 동시에 연산이나 저장 능력이 다른 매체에 비해 약하여 제한사항으로 작용한다. 정보보호에 활용할 수 있는 공간이 적으므로 기존의 표준 암호 알고리즘 대신 물리적인 보안 대책이 제안되고 있다.

표 3. RFID의 보안 위협[6]

종 류	내 용
물리적공격	태그를 획득하여 내용을 다른 태그로 복사하여 위장 공격
도청	RF통신 중 정보가 암호화되지 않은 채 전달되면 근거리에서 리더기로부터 정보 탈취 가능
스누핑	휴대용 리더기로 태그의 내용을 읽거나 위치 추적
스푸핑	태그의 내용을 변조하거나 정상 리더기로 위장 가능
서비스 거부 공격	강한 전파 송·수신을 통해 리더기와 RFID간 정상적인 통신 방해
세션 가로채기	인증된 세션을 가로채거나 프로토콜 일부를 다시 실행하여 세션을 얻음

• **USN(Ubiquitous Sensor Network)**

USN의 구조는 센서영역, 게이트웨이, 외부네트워크로 구분된다. 기본적으로 USN의 경우 센서들이 인증하는 절차가 필요하다. 이런 절차가 없을 시에는 인증되지 않은 침입자에 의해서 센서들이 제어되어 정보가 훼손되거나, 정보의 유출이 발생할 수 있다. 이와 같은 보안위협을 차단 및 대응할 수 있는 센서노드용 경량 보안 칩의 개발이 필요하다. 또한 보안 OS, 키 분배 및 관리, 경량 인증 메커니즘 등 USN 환경에 최적화된 센서 노드 보안 구조 기술 및 도청, 위·변조 등 인프라 공격을 능동적으로 모니터링, 탐지. 대응할 수 있는 USN 침입탐지 및 대응기술이 요구된다. RFID 서비스에 사용할 경우 태그와 리더간의 무선구간은 WEP, SSID, WPA와 같이 IEEE 802.11i의 보안기술을 적용할 수 있으며, 유선 네트워크 구간에서는 기존 유선구간과 유사하게 PKI, WPKI와 같은 보안 기술이 요구된다. 유선 네트워크와 정보 서버 구간 역시 인증알고리즘, SSL 서버인증과 같은 보안기술이 적용되어야 한다.

• **휴대인터넷(WiBro)**

휴대인터넷 서비스는 휴대형 단말기(휴대폰, PDA, 노트북 등)를 이용하여 정지 및 이동 중에도 빠른 전송속도를 제공한다. 휴대인터넷 구축 시 각 네트워크 간의 연동은 필수적이기 때문에 기존의 개별 네트워크를 넘어 연동되는 네트워크상세서의 인증, 키 교환 및 데이터 암호화 등을 가능하게 하는 연동 보안기술이 요구된다.

Ⅳ. 결 론

본 논문에서는 정보통신 기술의 발전에 기인한 유비쿼터스 환경에서의 국방 정보보호 발전에 관하여 언급하기 위하여 전장상황 이라는 특수성에 대하여는 언급하지 않았다. 다만 우리 사회의 유비쿼터스 사회로 진입하는 과정에서 나타나는 현상을 예상하여 볼 때 군대라는 영역에 적용시 일반적으로 취해야 할 정보보호에 관한 언급이므로, 실제 군 작전환경에 맞는 다양한 조건에서의 정보보호 요구사항이 이루어지도록 정책/제도 및 사이버전 역량 강화, 기발기술/체계의 고도화, 교육 등의 부분에서 다양한 환경 변화와 연계하여, 지속적인 변화와 발전을 위한 연구가 필요하다.

참고문헌

[1] 2006 DEFENSE WHITE PAPER, Ministry of National Defense
[2] 유비쿼터스 정보보호 기본전략 연구, KISA
[3] 박응기, "유비쿼터스 환경에서의 정보보호기술 발전추세", DISC 2007 논문지 pp.44-46
[4] 김종필, 박동섭, 이성중, "정보보호 핵심지식", 정일, pp. 324
[5] William Stallings, "Cryptography and Network Security" 3rd edition, Pearson Prentice Hall, pp. 296
[6] 2007 국가 정보보호 백서, National Information Security