침입감내기술 기반의 보안시스템 설계 및 구현 : 워게임체계를 중심으로

이강택* · 이동휘** · 김귀남**

요 약

오늘날 디지털혁명을 기반으로 한 세계화속에서 우리나라는 1990년대 후반부터 'IT 강국'으로 급부상하였으나, 이러한 정보화에 따른 역기능으로 해킹, 바이러스유포, 스팸릴레이, 피싱 등의 보안 침해사고가 매년 증가하여 정보사회 구현에 큰 걸림돌로 작용하고 있다. 이처럼 정보화의 역기능은 우리군의 국방체계에 대한 침해로 자연스레 연결되고 있으며, 이에 군은 국방체계에 대한 정보보호를 위해 다양한 노력을 기울이고 있으나, 점차 자동화, 지능화, 대중화, 분산화, 대규모화되고 있는 해킹수법들과 알려지지 않은 취약점이나 새로운 공격기법에 대해 효율적으로 대응하는데 한계가 있다. 따라서 국가안위와 직접적으로 연관될 수 있는 현 국방체계의 주요 운용 자원들(Resources)에 대한 가용성(Availability), 신뢰성(Reliability), 무결성(Integrity) 및 기밀성(Confidentiality) 등의 보장뿐만 아니라, 운용 시스템에 대한 예상치 못한 공격이나 침입행위가 발생하거나 또는 시스템 결함이 발생할 경우에도 무중단 시스템 운영을 보장하기 위한 체계 안정성(Safety)과 지속성(Maintainability)을 충족시켜주는 '의존성'(Dependability)에 대한 보장이 절실히 요구된다 하겠다. 본 연구는 국방체계의 의존성 보장을 통해 보안 및 무중단운영 요구를 충족시키고자 침입감내기술을 기반으로 하는 보안구조 설계 완성을 목표로 하였다. 이를 위해 침입감내시스템 구축에 요구되는 핵심기능들을 관련연구로 식별하였으며, 국방체계들중 구현대상체계로 선정한 워게임체계의 구조분석을 통해 보안상의 문제점을 식별하여 단계별·계층별 보안 메커니즘 제시하고 식별된 핵심 요구기능들을 구현하여 침입감내기술 기반의 국방체계 보안구조 설계를 완성하였다.

Design and Implementation of Security System Based on Intrusion Tolerance Technology : Focus on Wargame System

Gang Tack Lee* · Dong Hwi Lee** · Kuinam J Kim**

ABSTRACT

Objective of this study is to design and implement security system based on intrusion tolerance technology for the improvement of dependability in defense system. In order to do so, I identify and extract core technologies through the research and analysis into characteristics, structures, main functions, and technologies of intrusion tolerance architecture. And I accomplish a design of security system through the redundant system based on these core technologies. To implement and verify intrusion tolerance system, I chose "wargame system" as a subjected system, and accomplished 'Wargame Intrusion Tolerance System' and verified security required functions through a performance test. By applying showed security system into the development of application software based on intrusion tolerance, systematic and efficient system could be developed. Also applying "WITDS" can solve the current security problems, and this will be basic model for design of security architecture in the federation system after.

Key words : Intrusion Tolerance Technology, wargame

* 공군대학 워게임학과

** 경기대학교 정보보호학과

1. 서 론

최근 정보화의 역기능은 우리군의 국방체계에 대한 침해로 자연스레 연결되고 있는데, 이는 군의 IT 환경이 1990년대 중반 이후에 Client-Server 환경으로 전환하였을 뿐만 아니라 2000년부터는 웹(Web)체계를 도입하여 운용중에 있으며, 또한 보유하고 있는 정보가 쉽게 접하기 어렵다는 측면에서 무엇보다 매력적일 뿐만 아니라 가치 또한 크기 때문일 것이다. 국방체계에 대한 대표적인 침해 사례로서 2004년 7월에 있었던 "국방연구소, 공군대학 등 정부의 보안기관들에 대한 해킹 사건"[5]을 들 수 있으며, 이 시기에 북한이 김정일 위원장의 지시로 해킹부대를 운영하면서 남한의 정보를 수집하고 있음.

이 국군 기무사령부에 의해서 처음으로 공식 발표된 사실에 근거해 볼 때 국방체계에 대한 보안대책이 절실하다 하겠다.

본 연구는 각 국방체계에 대한 의존성을 보장함으로써 운용 자원들을 보호할 뿐만 아니라 시스템의 무중단 운영을 지원하기 위한 보안 구조설계 개발을 위한 발로로서 시작되었으며, 그 결과 침입감내기술[1](Intrusion Tolerance Technology)의 응용이 하나의 솔루션이 될 수 있음에 귀착되었다.

따라서, 본 연구는 국방체계에 대한 의존성 보장을 위해 결함허용기술과 정보보호기술이 결합된 형태인 '침입감내기술 기반의 국방체계 보안구조 설계'를 목적으로 하고 있다.

본 연구를 통해 새롭게 제시되는 보안구조 설계 방법은 워게임체계를 대상체계로 하여 다음과 같은 과정으로 이루어진다.

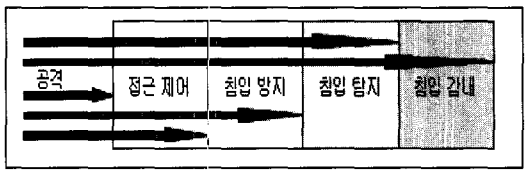
첫째, 침입감내기술의 이해 및 요구기능 식별
둘째, 워게임체계의 이해 및 보안구조 설계
셋째, 침입감내 워게임시스템 설계 및 구현
넷째, 종합적 워게임체계 보안구조 설계에 대한 성능평가 및 검증

이상의 보안구조 설계 작업은 단계별로 순차적으로 진행하였으며, 연구 대상 연습체계는 '합동연습체계'를 대상으로, 보안구조에 대한 성능평가 및 검증작업은 M&D(주)의 협조를 얻어 해당업체에서 개발한 'RS-J(합동전·모델)'를 이용하여 실시되었다.

2. 관련 연구

2.1 침입감내기술

침입감내기술(Intrusion Tolerance Technology)은 기존의 침입차단이나 탐지기술에 의하여 해결될 수 없었던 알려지지 않은 보안 취약점을 이용한 공격으로 발생되는 시스템의 피해를 방지하기 위한 기술이며, 중요 서비스의 품질 요구사항과 지속성 요구사항 만족을 통해 정상적인 서비스를 제공할 수 있도록 하는 기술이다[2].



(그림 1) 계층적 정보보호의 개념

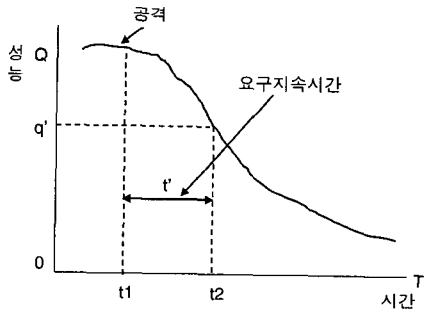
(그림 1)은 계층적 정보보호의 개념을 설명한 것으로 정보통신기반 보호를 위하여 정보보호기술들이 어떻게 적용되는가를 보여준다.

워게임과 같은 중요한 서비스가 정상적으로 유지되기 위한 필수조건으로서 가용성, 신뢰성, 무결성, 기밀성이 유지되어야 하는데, 이러한 특성을 의존성(Dependability) 특성이라고 한다[4].

의존성 특성이 충족되지 않는다면 해당 시스템은 신뢰할 수 없는 상태이며, 의존성 특성을 해치는 기본적인 원인은 시스템의 손상이다. 시스템의 손상은 일반적으로 '결함'으로부터 시작되며, 이러

한 결함은 우발적 또는 의도적으로 발생할 수 있고 발생 요인 또한 내부적 결함 또는 외부환경에 의한 결함, 설계의 결함 등 다양한 원인으로부터 발생할 수 있다.

따라서, 침입감내는 워게임체계와 같은 중요한 서비스를 제공하는 국방체계를 대상으로 악의적 공격이 발생하였을 경우에도 품질요구수준 범위 내에서 서비스를 일정한 시간동안 지속적으로 제공하여 주기 위한 기법이다[4]. 침입감내를 위한 요구사항은 서비스의 '품질수준 요구사항' Q(Quality) 와 '지속시간 요구사항' T(Time)로 표현된다. 아래 (그림 2)는 침입감내시스템에 요구되는 '품질수준 요구사항' q'와 '지속시간 요구사항' t의 상관관계를 설명해 주고 있다.

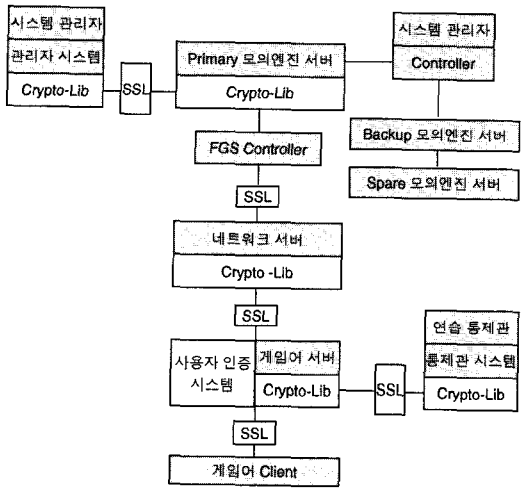


(그림 2) 침입감내 요구사항

결함허용기술이 시스템과 소프트웨어의 우발적인 결함에 대하여 관심을 가진다면 침입감내기술은 이와 같은 범주의 결함 이외에 악의적인 행위에 의하여 발생하는 결함, 즉 불법적 접근, 침투, 바이러스, 웜 등과 같은 악성코드 유포에 대하여 관심을 가진다는 것이 다른 점이다.

3. 워게임체계 보안구조(WSA) 설계

WSA(Wargame Security Architecture)란 현 워게임연습체계의 보안 구조적 측면에서 요구사항을 충족시킬 수 있는 보안 메커니즘을 지니며, 그 실행 구조에 있어서는 예상치 못한 새로운 공격 기술로 인한 시스템 오류 또는 고장으로 연습이 중단되는 것을 방지하는데 목표를 두고 새롭게 설계된 계층별 보안 구조이다.



(그림 3) WSA 프레임워크

(그림 3)의 WSA 프레임워크는 WSA를 구축하기위한 보안 구조와 기능에 대한 기본 골격과 체계이며, 기존의 보안구조에 대한 보완적 개념의 구조적 요구사항과 침입감내기술을 결합하여 완성하였다.

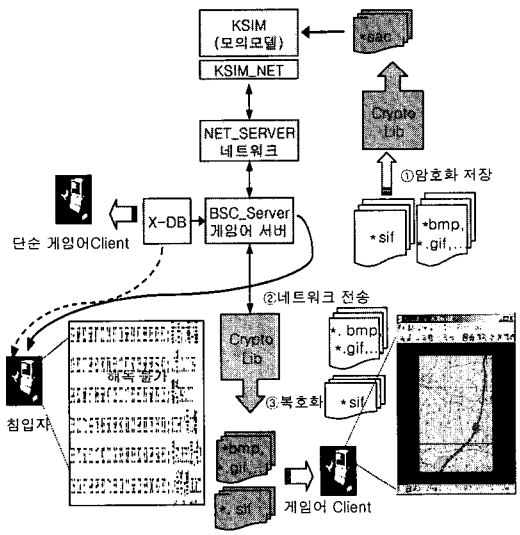
3.1 인증시스템(1계층) 모듈

네트워크 보안 라이브러리(SSL : Secure Socket Layer)에 ID/Password 방식을 적용한 구조도를 설명한 것으로 기존의 SSL의 암호화 방식에서 키 교환의 문제 해결이 가능하고, 기존 공개키 인증서 발급을 위한 별도의 CA시스템 대신 연습 홈페이지 운영을 통해 사용자를 인증토록 함으로써 시스템 성능보장 및 연습참가자의 편리성을 보장하였다. 또한 상위등급의 연습참가자에게만 데이터 복호화용키를 전송함으로써 군사자료에 대한 불

필요한 접근을 사전 차단하여 정보보호의 기능이 발휘되도록 하고 있다.

3.2 데이터 암호화 모듈(2계층)

데이터 암호화는 2계층으로서 (그림 4)는 연습 시나리오를 기초로 하는 각종 정보보호가 요구되는 데이터들에 대한 암호화를 통해 직접적인 데이터 보안이 보장되도록 구현한 구조도이다. 이를 위해 한국정보보호진흥원(KISA)에서 개발한 128비트 블록암호 알고리즘 'SEED' 소스코드를 배포받아 시험 적용하였다.



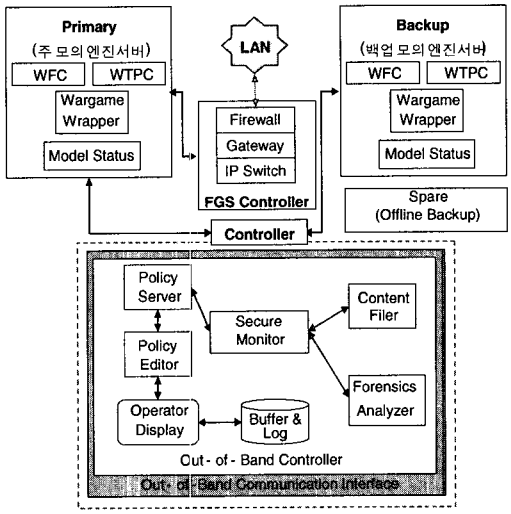
(그림 4) 데이터베이스 이원화/암호화 구조

3.3 네트워크 보안 모듈(3계층)

네트워크 보안은 3계층으로서 외부로부터 정보보호를 위해 가장 선결되고 보장되어야 하는 것으로 네트워크 서버에 MS Window2000의 IIS(Internet Information Server)에 의해 제공되는 SSL 3.0 프로토콜을 인스톨하여 게임어(Cleint)와 서버를 확인하고 특정 통신 세션중 보안이 이루어지도록 구축하였다.

3.4 침입감내 시스템(ITWS : Intrusion Tolerance Wargame System)(4계층)

본 연구의 핵심인 WSA의 마지막 계층으로 (그림 5)와 같이 COTS 서버의 중복을 통하여 침입감내 기술을 구현하였다.



(그림 5) ITWS 구조

Controller는 Out-of-band 네트워크로 구성되어 일반사용자의 접근이 금지된 보안 관리자에 의해서만 운영되는 침입감내 시스템의 주 장치로서 핵심적 역할 모듈인 Secure Monitor에 의해 시스템의 가용성 보장을 위한 Backup으로의 전환 또는 Failover 할 것인가에 대한 결심과정 등을 통제하고, 요청에 대한 응답 검사와 침입자 IP 차단 및 Game checkpoint, restores, rollback에 대한 결심 및 통제 기능 등을 제공한다. 또한 서비스회복에 대한 방법 등 전반적인 보안 정책을 수립하

여 시행한다. 이러한 기능들을 수행하기 위해서 Policy Server & Editor, GUI 환경의 Operator Display, Buffer & Log, Content Filter and Forensics Analyzer 등의 모듈들이 작동한다.

4. WSA 성능 평가 및 분석

WSA의 성능테스트는 3단계로 진행되었다. 첫 번째로 방역효과에 대한 평가, 두 번째로 침입감내에 대한 평가, 그리고 마지막으로 이벤트(명령문) 처리와 연관된 시스템성능 평가순으로 진행되었다.

4.1 가정 사항

다음과 같은 가정 하에 성능평가 작업을 수행한다.

첫째, WSA에서 제시된 각 자원(보안모듈)이외 WSA 성능평가를 위해 구축된 시스템과 일반시스템은 모두 동일한 환경이다.

둘째, WSA 성능평가를 위해 구성된 각 팀들간 작업은 평가목표에 부합하도록 평가자의 명령된 작업만 수행한다.

셋째, 성능평가시 워게임모델의 게임 스피드는 3.5배속으로 진행하며, 배속증가는 평가에 아무런 영향을 미치지 않는다.

4.2 작업 환경

실제 워게임연습체계를 기반으로 성능평가를 하기에는 현실적인 문제점이 발생하여 실제 연습체계를 축소한 테스트용 시스템을 구축, 다음과 같은 자원을 기반으로 두개의 팀을 구성하였다.

첫째, 인트라넷 시스템내 접속 자원 규모

- 서버 : SUN Fire V880 1대, SUN Blade 2000 2대 * OS는 Unix, DBMS는 Oracle과 SQL
- 클라이언트 : Workstation급 PC 8대
- 네트워크 : 로컬망만 이용하며, 외부망은 단절됨

둘째, 명령문 규모 - 성능평가 결과에 대한 신뢰도를 높이기 위해 실제 연습시 처리되는 명령문 규모를 채택하였다.

- 명령 건수 : 2,000건
- 측정 횟수 : 총5회 반복
- 전송데이터 : 총 9,026Kbyte
- 모델내 유닛 수 : 3000유닛

셋째, 팀 구성

- Red Team(3명) : 인가되지 않은 게임어로 바이러스 유포, 불법적 접근 및 Sniffing 시도
- Blue Team(5명) : 인가된 게임어로 정상적인 명령문 입력 및 게임 실행

4.3 목표 설정

침입차단 부분에서는 측정 기간 중의 FGS Control 시스템의 성능을 검증할 수 있다. 침입탐지 부분에서는 Primary 서버에 내장된 각종 보안모듈에 대한 성능을 검증할 수 있으며, Controller와 연관되어 침입감내 및 서비스 복구 성능 평가 및 절차를 setup 시킬 수 있다. 마지막으로 WSA 구조개선에 따른 부작용(Side Effect)이다. 부작용이란 WSA 구조로 인하여 바람직하지 못한 현상이 발생되는 것을 의미하며, 워게임의 Performance 지연이 바로 그것이다. Performance 지연은 명령문 처리 시간 측정을 통해 평가토록 한다.

4.4 평가 시스템 구성

WSA의 성능평가를 위한 평가시스템은. 각 단계별 보안기능 매커니즘을 형성하며, 게임어 인증시스템, 데이터 암호화, 네트워크 보안 단계를 그친 후 FGS Controller를 통과하여 RS-J 모의엔진이 장착된 Primary와 Backup 서버와 접속하게 되는 구조를 보여준다.

4.5 평가 결과 및 분석

4.5.1 침입 차단

먼저, WSA에서 1, 2, 3계층으로서 구현된 인증 시스템, 데이터보안, 네트워크보안에 대한 성능평가에 대한 결과는 다음 <표 1>과 같다.

〈표 1〉 1~3계층 성능평가 결과

구 분	평가 항목	평가 결과
인증시스템	등급별 사용자 인증	단순/선임계임어로 구분 ID/PW 정상적 수신
데이터보안	군사지도파일 암호화	선임계임어만 복호화 키 수신 및 군사지도 판독함
네트워크보안	SSL 프로토콜 성능	"hello"전송을 통한 SSL 프로토콜 성능확인

다음은 본연구의 핵심인 침입감내시스템에 대한 성능평가이다. 아래 <표 2>는 Red Time에 소속된 침입자들이 각기 다른 종류의 웜 바이러스를 유포하여 측정된 결과를 보여주고 있다. Welchia 웜은 시스템 성능을 저하시키고, Mydoom.A는 백도어를 설치하여 데이터의 유출 및 위·변조가 가능하도록 하기 때문에 평가도구로서 선정하였다.

〈표 2〉 웜 바이러스 종류 및 결과

Welchia	Mydoom.A

주요증상으로는 시스템 성능저하 및 백도어 설치 WSA구조시 100% 차단 및 CPU 사용률 50% 미만 일반구조에서는 차단 실패.

결론적으로 WSA의 침입차단에 대한 성능평가는 만족스러운 결과를 획득하였다.

4.5.2 침입 탐지

Red Time에 소속된 3명의 침입자가 각각 sniffing 공격도구를 활용하여 침입을 시도한 결과를 <표 3>에서 보여주고 있다.

〈표 3〉 공격도구 종류 및 평가결과

도구	ARP Redirect	ARP Spoofing	ICMP Redirect
공격 횟수	총 15회	총15회	총15회
탐지 결과	15건	15건	15건
레포팅	15건	15건	15건

위 표에서 보는 바와 같이 WFC와 WTPC에 의해 침입탐지가 정상적으로 이루어져 보안관리자에게 레포팅이 이루어짐을 알 수 있다.

4.5.3 침입 감내

침입 감내 성능에 대한 평가를 위한 객관적인 방법을 채택하기는 매우 어려움이 따른다. 왜냐하면 침입감내기술에 대한 연구들이 시작된 지 얼마 되지 않았으며, 미국과 영국에서 진행되었거나 진행중인 연구프로젝트들은 Target System을 가지고 있다. 따라서 침입감내기술을 적용한 시스템에 대한 성능평가는 시스템의 특성이 고려된 다소 주관적 요소가 평가 기준이 될 수밖에 없으며, 따라서 워게임연습체계에 적용한 침입감내 시스템의 성능평가는 <표 4>의 평가 기준에 의거한다.

〈표 4〉 평가 기준

구 분	기 준	측정방법
시스템 요구 성능	70%이상	게임 스피드 변화율(3.5배속→2.5배속까지 허용)
시스템 지속 시간	2시간	복구까지 소요시간(Backup→Primary로 재전환)

아래 <표 5>에서 보는바와 같이 시스템전환은 Backup으로 모두 성공적으로 이루어졌으며, 전환에까지 소요된 시간은 평균 6초로 양호하였고 게임어들은 시스템 전환을 인지하지 못하였다. 또한 Primary 시스템의 복구시간은 평균 50분이 소요되어 평가기준인 2시간 이내를 충족하였다.

〈표 5〉 침임감내 기능 측정 결과

횟수	시스템 전환	전환소요 시간(초)	Primary 복구시간(분)	결과
1회	Backup	7	57	충족
2회	Backup	5	93	충족
3회	Backup	7	17	충족
4회	Backup	6	50	충족
5회	Backup	5	33	충족
평균		6	50	

4.5.4 게임 성능

워게임연습체계의 성능으로 제시되는 기준은 이벤트(명령문)처리와 연관된 게임스피드이다. WSA는 워게임연습체계의 보안을 위해 제시된 계층별·단계별 상이한 메커니즘 보안구조로서 각각의 계층별 보안 모듈이 게임속도의 지연으로 그 영향을 미친다면 가치는 전무하다 할 수 있다. 따라서 WSA 채택전·후 워게임연습체계의 이벤트(명령문) 처리시간을 비교하여 WSA 구조 개선 전후 성능 변화에 대한 비교가 가능하다. 측정 결과는 다음과 같다.

〈표 6〉 게임성능 측정 결과

구분	WSA 적용 유·무	명령문처리 시간(초)	차이	게임 스피드 (3.5배속 기준)
1회	미적용	83	6	3.5
	적 용	89		3.5
2회	미적용	82	8	3.5
	적 용	90		3.5
3회	미적용	83	5	3.5
	적 용	88		3.5
4회	미적용	81	6	3.5
	적 용	87		3.5
5회	미적용	82	4	3.5
	적 용	86		3.5
평균			5.8	3.5

<표 6>에서 보듯이 WSA에 설치된 보안 모듈들이 명령문 처리 기능 지연에 큰 영향을 미치지 않음을 알 수 있다.

4.6 결과 종합 분석

이상에서 나타난 결과들을 종합하여 볼 때 WSA 구조가 워게임 성능에는 영향을 미치지 않으면서 효과적인 보안기능을 수행하고 있음을 도출할 수 있다.

5. 결론 및 향후 과제

본 연구는 국방체계의 의존성 보장을 통해 보안 및 무중단운영 요구를 충족시키고자 침입감내기술기반의 보안구조 설계 완성을 목표로 하였다. 이를 위해 침입감내시스템 구축에 요구되는 핵심 기능들을 관련연구를 통해 식별하였으며, 국방체계들중 구현대상체계로 선정한 워게임체계의 구조분석을 통한 보안상의 문제점을 식별하여 단계별·계층별 보안 메커니즘 제시하고 식별된 요구기능들을 구현하였다. 'WSA'는 침입감내 워게임 시스템인 'ITWS'를 중심으로 인증시스템, 데이터 보안, 그리고 네트워크보안 등의 보안기능을 포함하는 종합적인 보안구조 설계이며, 구현된 WSA에 대해 제한된 성능검증으로 침입감내기술의 성공적인 적용가능성을 확인하였다.

본 연구의 핵심 성과물이라 할 수 있는 'ITWS'는 침입감내기술을 적용하고자 하는 국방체계에 대한 표준모델로서, 4단계로 구분된 침입차단, 침입탐지, 침입감내, 침입복구 등의 각 단계별 요구기능들이 타 국방체계 뿐만 아니라 일반체계에 대해서도 적용될 수 있음을 의미한다. 즉, 침입감내 시스템을 구축하고자하는 대상체계는 'ITWS'를 표준모델로 하여 체계특성에 맞도록 각 단계별 요구기능들을 구현함으로써 완성된다.

아울러, 워게임체계의 보안 인프라 구조의 발전

적 개선책으로 제시된 침입차단기술, 탐지기술, 결함허용기술 등의 정보보호기술들이 결합된 침입감내기술을 적용한 종합적 보안구조인 WSA가 워게임체계 뿐만 아니라 향후 각 군 모델간 페더레이션 구축에 적용할 보안표준프로세스 개발에 대한 보안구조설계의 기본 모델이 될 수 있을 것으로 기대된다.

향후 과제로서, 침입감내시스템의 지속적인 연구를 통해 요구기능에 대한 성능을 향상시킬 수 있도록 응용 소프트웨어를 보다 체계적·효과적으로 개발하기 위한 개발방법론에 대한 연구가 지속되어야 할 것이다. 또한 다양한 국방체계를 대상으로 침입감내시스템 알고리즘 설계 및 구현과 이를 통해 보다 확장된 운용을 실험하는 것이다.

참 고 문 헌

[1] 조은숙, 이강신, "침입감내 소프트웨어 모델링을 위한 요구사항 추출 및 명세", 한국시뮬레이션학회 논문지, 제13권, 제1호, Mar 2004.

[2] 최중섭 외, "침입감내기술 연구 동향", 정보보호학회지, 제13권, 제1호, Feb 2003.

[3] J. E. Just, and J. C. Reynolds, "HACQIT (Hierarchical Adaptive Control of QoS for Intrusion Tolerance", In 17th Annual Computer Security Applications Conference, 2002.

[4] J. C. Laprie, "Dependability : Basic Concepts and Terminology in English, French, German, Italian and Japanese", ISBM 3-211 -82296-8, Springer-Verlag, 1992. p. 265,

[5] "국가차원 사이버戰 가능성", 조선일보 2004년 7월 13일자.

[6] 국가기밀 논란 與 "비공개 당연", 서울신문 2004년 10월 9일자.

[7] 美, 對이라크전 예행연습서 참패<가디언>, 연합뉴스 2002년 9월 6일자

이 강 택

1988년 공군사관학교
전자계산학(이학사)
2002년 포항공과대학교
정보통신학과(공학석사)
2005년 현재 경기대학교
정보보호학과(공학박사)
현재 공군대학 교수보

이 동 휘

2000년 경기대학교 전자계산학과(이학사)
2003년 경기대학교 정보보호기술공학과(공학석사)
2004년~현재 경기대학교 정보보호학과 박사과정

김 귀 남

미국 캔자스대학 수학과
(응용수학사)
미국 콜로라도주립대학 통계학과
(통계학석사)
미국 콜로라도주립대학 기계·산업공학과(기계·산업공학박사)
현재 경기대학교 정보보호기술공학과 주임교수