워게임 시뮬레이션 시스템을 위한 보안시스템 설계 및 구현

송 종 석[†] · 김 진 수[††] · 신 문 선[†††] · 류 근 호[††††]

요 약

워게임 시뮬레이션 시스템은 군사작전을 가상으로 실시하는 시스템으로서 운용되는 자료들은 대부분 군사적으로 보호되어야할 자료들이다. 그러나 워게임 시뮬레이션 시스템 개발시 이러한 군사기밀정보 및 네트워크 트래픽에 대한 보안을 고려하지 않아 이에 대한 정보유출의 위험성을 내재하고 있는 상황이다. 이 논문에서는 워게임 시뮬레이션 시스템의 보안 취약점을 분석하여 보안정책을 수립하고 워게임 시뮬레이션 시스템에 적합한 보안시스템을 설계 및 구현하였다. 구현된 보안시스템은 인증시스템, 암호화시스템, 네트워크보안시스템으로 구분하여 설계하였다. 구현된 보안시스템을 워게임 시뮬레이션시스템에 적용하여 시험한 결과 워게임시뮬레이션시스템 성능을 저하 시키지 않고 신뢰성있는 보안 기능을 수행한다.

키워드 : 워게임 시뮬레이션 시스템, 보안시스템, 인증, 암호화, 네트워크 보안

Design and Implementation of Security System for Wargame Simulation System

Jong Seok Song[†] · Jin Soo Kim[††] · Moon Sun Shin[†††] · Keun Ho Ryu[††††]

ABSTRACT

War simulation system is a virtual space that army tactical simulation exercise is held. The data used in this system are considered sensitive and needs to be protected. But security vulnerabilities and possible security loopholes were not considered when designing the war game simulation system. So currently the systemis highly vulnerable against hackers and data leakages. This paper proposed a security system for war game simulation system based on considering the currently vulunerabilities and possible security leakages. The proposed security system supports security patches. In this paper, we analyze vulunerabilities of the running environment of current system and we design and implement the security system that is consisted of three components : Authentication System, Encryption System and Network Security System. The security patches are safe and there are no negative effects on the system's performance. The patches are proved to be effective and very reliable towards solving the security vulnerabilities.

Key Words : Wargame Simulation System, Security System, Authentication, Encryption, Network Security

1. 서 론

워게임 시뮬레이션 시스템은 군사작전을 가상으로 시뮬레이션하도록 개발된 시스템이다[1].

많은 국가들이 경제적이고 과학적인 군사훈련 수단으로 워게임 시뮬레이션 시스템을 개발하여 발전시키고 있다. 한국군 역시 지난 70년대 말부터 미군의 M&S 그룹 지원하에 워게임 시뮬레이션 시스템을 사용하기 시작하였다. 그러나 사용모델들은 미군교리나 장비위주로 개발하고 운영됨으로 인해 한국적 특성(교리,장비,지형등)을 반영한 훈련에는 많은 불편함과 제한사항이 존재하였다. 이에따라 1990년대에 한국형 독자 훈련모델을 개발하기 위한 시도가 이루어졌으며 1999년 비로소 사·여단급 훈련용 모델인 "창조21"모델[2]을 개발 성공하였다. 이러한 개발경험을 바탕으로 2002년에는 후방 사단급 훈련용인"화랑21"모델[3], 연대급 훈련용인"전투21"모델[3]이 연이어 개발에 성공함으로서 한국군의 위상을 한껏 드높였다[1, 2, 3].

이러한 워게임 시뮬레이션 시스템은 군사지도 자료, 군관련 자료가 포함된 시나리오 파일등의 군사 기밀자료를 이용하여 시뮬레이션을 한다. 그러나 워게임 시뮬레이션 시스템 개발시 이러한 군사기밀정보 및 네트워크 트래픽에 대한 보안을 고려하지 않아 워게임에 참여하는 사용자들이나 비인가된 사용자들에 의해 정보유출의 위험성을 내재하고 있는 상황이다[3].

따라서 이 논문에서는 이와같은 문제점을 해결하고 워게임 시뮬레이션 시스템의 운용환경 및 취약성 분석을 통해 안전

† 준 회 원 : 육군본부 지휘통신참모부
†† 정 회 원 : 육군교육사 체계분석실
††† 정 회 원 : 충북대학교 전자계산학과 이학박사
†††† 종신회원 : 충북대학교 전기전자및컴퓨터공학부 교수
논문접수 : 2004년 12월 31일, 심사완료 : 2005년 3월 22일

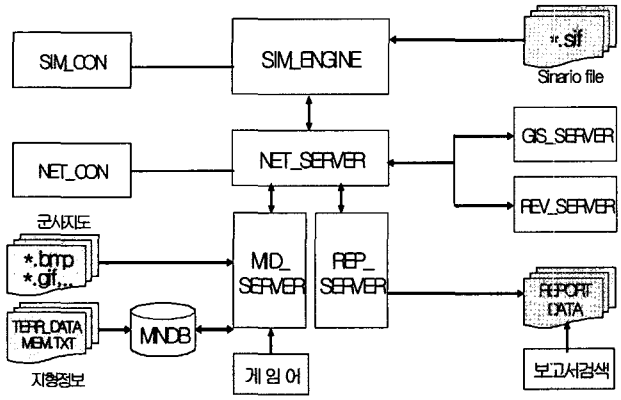
한 워게임 시뮬레이션 시스템 운영환경을 구축하기 위한 보안시스템을 제안한다. 제안한 보안시스템은 군사기밀자료에 대한 접근제어를 위해 사용자 인증시스템과 중요데이타에 대한 무결성과 기밀성을 제공하기 위한 데이터 암호화시스템, 각 시스템구성요소인 서버와 클라이언트 상호간 암호화 통신 시스템 등으로 구성한다.

이 논문의 구성은 2장에서는 워게임 시뮬레이션 시스템을 분석하고 3장에서는 이 시스템의 보안정책을 수립한다. 4장에서는 워게임 시뮬레이션 보안 시스템을 설계 및 구현하고 5장에서는 실험 결과를 분석하며 마지막으로 6장에서는 결론 및 향후 연구를 제시한다.

2. 워게임 시뮬레이션 시스템 분석

2.1 워게임 시뮬레이션시스템 운용환경

워게임 시뮬레이션시스템의 위협요소를 분석하여 보안정책을 수립하고 보안시스템을 설계하기 위한 시스템의 각구성요소는 (그림 1)과 같으며 각 구성요소 상호간의 동작은 다음과 같다.



(그림 1) 워게임 시뮬레이션시스템의 각 구성요소

모의엔진(SIM_ENGINE)은 워게임을 시뮬레이션하는 서버로서 시나리오 파일을 읽어들여 실시간으로 워게임을 실행하며, 네트워크서버(NET_SERVER)는 모의엔진과 중계서버(MID_SERVER)의 네트워크 연결을 중계한다. 중계서버(MID_SERVER)는 군사지도 파일과 지형정보 파일을 관리하며, 클라이언트(게임어)와 모의엔진 사이의 시뮬레이션 진행을 중계한다. 워게임을 시작하면, 게임어들은 클라이언트를 이용해 사용자 인증을 수행하며, 각 클라이언트들은 모의엔진에 명령어를 전송하며, 이를 수신한 모의엔진은 시뮬레이션을 진행한다. 모의엔진은 시뮬레이션의 진행경과를 중계서버에 전달하고, 이는 클라이언트에 전달되어 화면에 반영된다. 이러한 반복을 통해 워게임을 계속적으로 진행한다. 또한 모의엔진 제어기(SIM_CON), 네트워크제어기(NET_CON)는 모의엔진과 네트워크 서버를 통제하며 워게임 시뮬레이션의 결과는 보고서의 형태로 생성되어, 보고서 서버(REP_SERVER)와 사후검토 서버(REV_SERVER)에 저장되며, 상황도서버(GIS_SERVER)를 통해 지도상에 입체적으로 도시한다.

2.2. 워게임 시뮬레이션 데이터

워게임 시뮬레이션 시스템은 군사지도 데이터, 군부대 정보를 포함하는 시나리오 파일과 같은 군사기밀 정보를 이용하여 군사작전을 가상으로 시뮬레이션하는 것으로 이와 같은 정보는 반드시 보호해야 할 대상이다. 이 시스템에서 사용하는 중요 정보는 크게 지형정보, 시나리오 파일, 군사지도 파일이다. 이 가운데 시나리오 파일은 각 부대정보, 보급품, 군수품 정보 등과 같은 기밀을 포함하고 있다. 이와 같은 정보는 기본적으로 오라클 데이터베이스에 저장 관리되며, 이를 편집 관리하는 통합관리 툴이 제공된다. 또한 부대정보를 편집하는 시스템, 지형정보를 편집하는 툴 등이 다수 존재한다.

3. 워게임 시뮬레이션시스템의 보안 정책

3.1 보안 취약성 분석

보안 기본요소를 적용하여 워게임 시뮬레이션 시스템의 취약성을 분석해 보고자 한다. 보안 기본 요소는 정보의 송·수신자 또는 정보시스템 이용자의 신원을 식별·확인하기 위한 인증/식별(authentication)과, 비인가자가 시스템에 부정한 방법으로 접근하여 사용하는 것을 방지하기 위한 접근통제(access control)가 있으며, 전송 또는 보관중인 정보를 비인가자가 부정한 방법으로 입수하더라도 그 내용을 알 수 없도록 보호하는 기밀성(confidentiality)과 전송 또는 보관중인 정보를 인가되지 않은 방법으로 위조 또는 변조할 수 없도록 보호하는 무결성(integrity)이 있다. 또한 사용자가 정보통신 시스템을 통하여 정보를 송·수신하거나 처리한 사실을 부인하는 것을 방지하는 부인방지(non-repudiation)와 데이터의 전송 또는 컴퓨터 처리시스템이 허가된 사용자의 사용을 보장하는 가용성(availability)이 있다[4, 6].

현재 운용되는 워게임 시뮬레이션 시스템의 취약점 분석을 통해 도출된 워게임 시뮬레이션 운영 환경에 대한 보안 위험요소는 다음과 같다.

첫째, 우선 사용자(지휘관)들이 게임을 하기 위해 사용하는 클라이언트 및 시뮬레이션을 모니터링하는 통제관 시스템 등은 사용자 인증없이 쉽게 접근하여 사용하는 것이 가능한 상태이다.

둘째, 군사기밀 정보(지도데이터, 군부대 정보가 포함된 시나리오 파일)가 보안장치 없이 ASCII 파일 및 데이터베이스를 이용해 관리되어 유출에 대한 위험성을 가지고 있다.

셋째, 군사기밀 정보가 워게임 시뮬레이션 시스템의 각 구성요소 상호간 TCP/IP 네크워크 통신을 통해 전송되기 때문에 네크워크 패킷에 대한 도청 및 변조 등에 대한 위협을 내재하고 있다.

넷째, 모의엔진 서버, 네크워크 서버, 중계서버 등과 같은 시스템 구성요소가 네트워크에 직접 연결되어 있기 때문에 이에 대한 공격 및 비인가 접근 등과 같은 위협이 내재하고 있으며 시스템 상호 연동시 시스템 상호간 인증이 불가능하다.

이러한 운용 환경에서 분석된 사용자 인증/접근통제, 네트워크 패킷에 대한 도청/변조, 네트워크 보안에 대한 취약성을 해결하기 위한 보안 정책을 수립한다.

3.2 보안 정책 수립

워게임 시뮬레이션 시스템의 보안정책은 인증, 접근통제, 기밀성/무결성, 부인방지, 가용성 측면에서 기술적 보안 정책 수립이 요구된다[7, 8, 9]. 앞 절에서의 보안 위협요소 분석결과를 해결하기위한 기술적 보안 대책은 다음과 같다.

첫째 통제관 시스템의 사용자 인증 문제 해결을 위해서 사용자 인증시스템을 도입한다. 사용자 인증 메커니즘은 ID/PASSWORD 방식, ONE-TIME PASSWORD 방식, 공개키 인증서 이용방식 등이 있다. 워게임 시뮬레이션 시스템의 모든 사용자는 아이디와 패스워드를 가지고 사용자 인증을 거친후 인증서를 기반으로 한 SSL에 의해 보안유지를 한다. 이는 단순 아이디/패스워드 방식과 인증서방식을 통합함으로써 보다 강화된 사용자 인증을 제공할 수있기 때문이다.

둘째 워게임 클라이언트 및 서버 시스템에 대한 접근제어를 위해서는 서버시스템의 경우는 SSH과 SSL을 이용하며 클라이언트의 접근제어는 사용자 인증메커니즘과 결합 운용하며 권한별 접근제어를 구축한다.

셋째 워게임 시뮬레이션 시스템의 데이터에 대한 무결성과 기밀성에 대한 취약성을 보완하기위해서 소프트웨어 암호 라이브러리를 사용한다. 소프트웨어 암호 라이브러리는 클라이언트에 암호모듈을 탑재하여 사용자 인증후에 복호화하여 실행하도록 한다.그러나 공개키를 사용하게 됨으로 키관리에 대한 어려움이 내재한다.

넷째 워게임 시뮬레이션시스템의 각 구성요소 상호 간 네트워크를 통해 군사기밀정보가 전송되어 네트워크 패킷에 대한 도청 및 변조의 위협이 있으므로 이를 암호화 통신 프로토콜을 구현하여 해결한다. TCP 계층 위에서 구현되는 SSL을 이용하면 안정성에 대한 신뢰도가 높고 실제 워게임 운용에 성능 저하를 초래하지 않는 범위에서 네트워크 보안을 구축할 수 있다.

다섯째 침입 차단시스템과 침임 탐지 시스템을 도입하여 해커의 침입이나 DOS공격등을 탐지할 수 있도록 하는 보안대책이 필요하다.

위와 같은 보안 정책을 구현하기 위하여 워게임 시뮬레이션 시스템의 보안성 평가기준을 <표 1>과 같은 보안 등급으로 정의하였다[17].

이와 같은 기준으로 구현된 워게임 시뮬레이션 보안시스템에서는 보안등급 Level 1에서는 세부등급 1-1과 1-3, 1-4를 구현하고, Level 2에서는 2-1, 2-2, 2-3을 구현하고 Level 3에서는 3-1, 3-2를 구현하고자 한다.

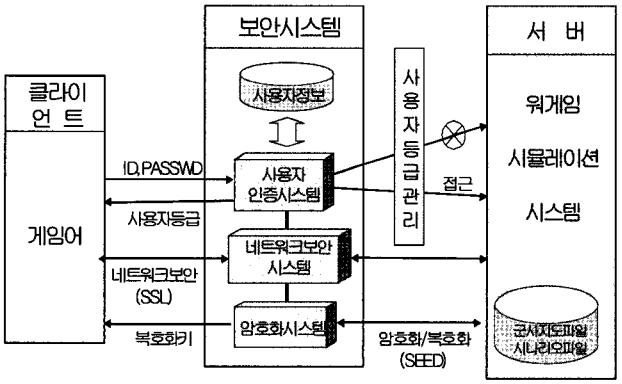
위와 같은 보안등급으로 정의된 워게임 시뮬레이션 보안시스템을 설계하고 구현한다. 워게임 시뮬레이션 시스템의 특성상 보안시스템으로 인해 성능저하를 초래하게 되면 워게임시뮬레이션의 본래의 목적을 달성할 수 없으므로 성능 저하에 미치는 영향에 대한 평가가 있어야한다[1].

〈표 1〉 워게임 시뮬레이션시스템의 보안등급

등급	Level 1 사용자인증	Level 2 접근제어	Level 3 로그 및 감사	Level 4 보안레이블/ 정책설정
세부등급	1-1 ID/PASWORD 방식	2-1 사용자별 데이타 접근권한 설정	3-1 사용자별 로그기록	4-1 보안 레이블을 통한 사용권한 설정
	1-2 ONE-TIME PASSWORD 방식	2-2 서버 데이터 접근권한 설정	3-2 각 시스템별 로그 기록	4-2 보안 정책 설정을 통한 통합 보안 관리
	1-3 PKI기반 사용자인증	2-3 각 시스템간 인증을 통한 네트워크 접근 제어	3-3 로그분석을 통한 감사추적	없음
	1-4 IC카드/USB 토큰연동	2-4 데이터베이스 접근제어	없음	없음

4. 워게임 시뮬레이션 보안시스템 구조

이 장에서는 3 장에서 수립한 워게임 시뮬레이션 시스템의 보안정책을 바탕으로 다양한 워게임 시뮬레이션 응용플랫폼에서 독립적으로 보안서비스를 제공할 수 있도록 워게임 시뮬레이션 보안시스템을 설계하고 구현한다. 워게임 시뮬레이션 보안시스템은 (그림 2)와 같이 사용자 인증시스템, 암호화 시스템, 네트워크 보안시스템의 세 부분으로 구성된다.



(그림 2) 워게임 시뮬레이션 보안시스템 구성

인증시스템은 사용자의 ID와 PASSWORD에 의해 사용자별 접근을 통제하고, 암호시스템은 워게임시스템내에서 군사지도파일과 시나리오파일등 군사기밀 정보에 대한 암호화/복호화를 제공한다. 또한 네트워크 보안시스템은 서버간 및 서버와 클라이언트간에 전달되는 구성요소간에 암호화 통신을 제공한다.

4.1 사용자 인증시스템

사용자 인증시스템은 사용자의 접근제어 및 접근권한을 통제하기 위한 기능을 제공한다. 기존'ID / PASSWORD 관리

시스템'은 UNIX 로그인 방식을 의미하며, 사용자 ID와 PASSWORD를 등록하여 이용하는 방법으로 구현이 용이하지만 ID와 PASSWORD가 노출될 위험이 존재한다[10].

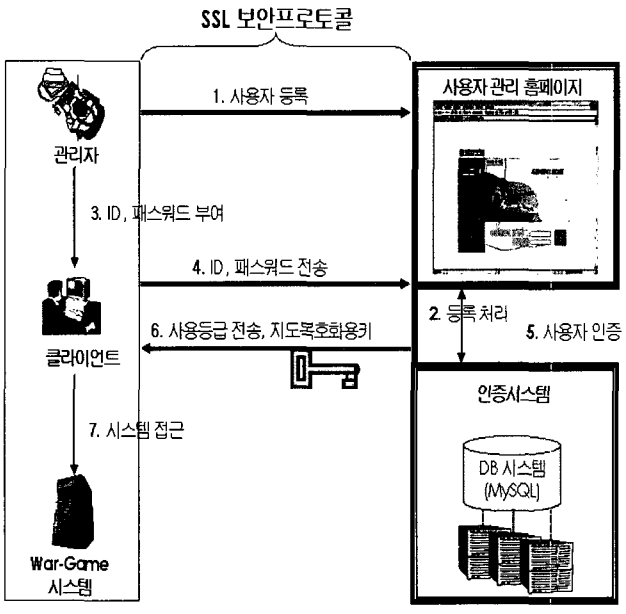
'ONE-TIME PASSWORD 관리시스템'은'ID/PASSWORD 관리시스템'을 개선한 것으로 PASSWORD 노출에 대한 위협을 해결하기 위해 매번 로그인할때마다 PASSWORD를 달리 사용하는 방식이다. 이방식은 보다 강화된 인증방식을 제공하지만 매번 바뀌는 패스워드를 사용하고 관리하기 어려운 문제가 있다.

또한 'Digital ID 시스템'은 X.509 공개키 인증서를 활용하여 사용자 인증용으로 사용하는 방식으로 디지털 아이디의 소유자가 맞는지를 검증하는 메카니즘을 포함하여 강화된 사용자 인증메커니즘을 제공한다. 이방식은 강화된 인증방식을 제공하고 암호화통신과 접목할수 있는 장점이 있지만 CA구축등 부가시스템이 필요한 문제가 있다[4].

'IC카드/USB 보안토큰 시스템'은 H/W를 이용하여 안전하게 인증정보를 관리하기 위한 방식이며 매우 강력한 인증방식을 제공하는 반면 CA등 부가시스템 및 인증정보관리 H/W를 추가로 구입해야하는 문제가 있다[11, 12].

이논문에서는 패스워드관리가 용이한 'ID/PASSWORD 관리시스템'과 암호화통신과 접목할수 있는 강화된 인증방식을 제공하는 'Digital ID 시스템'을 통합하여 사용자 인증시스템을 설계하였다. 즉, 각 사용자 ID와 PASSWORD를 통해 사용자 인증시스템으로부터 인증받고 이때 전송되는 ID와 PASSWORD는 인증서를 기반으로한 SSL에 의해 보호받게 된다. 또한 워게임시뮬레이션 시스템에 접근하는 모든 사용자에 대한 로그를 생성하고 관리하여 정보감사에 활용될수 있도록 하였다.

사용자 인증시스템의 구성은 (그림 3)과 같으며 이 시스템의 각 시스템 구성요소 상호간의 동작은 다음과 같다.



(그림 3) 사용자 인증시스템

관리자는 사용자를 사용자관리 홈페이지를 통해 등록하며 사용자관리 홈페이지는 사용자를 등록하고 데이터베이스에 저장한다. 관리자는 사용자에게 ID와 PASSWORD를 부여하고 사용자는 클라이언트쪽 인터페이스에서 ID와 PASSWORD를 입력한다. 클라이언트는 입력된 ID와 PASSWORD를 사용자 인증시스템에 전송하고 사용자인증시스템은 사용자 인증을 수행한다. 사용자인증시스템은 사용자 인증결과로 사용등급과 지도복호화용 키를 전송하며 사용자는 워게임 시뮬레이션시스템에 접근토록 하였으며 암호화시스템과 통합하여 구현한다.

(그림 4)의 authentication 함수는 사용자로부터 ID와 Password를 입력받아 사용자 인증을 처리하고, 인증 성공시 암호화/복호화용 키를 생성한다.

authentication(char* ID, char*passwd, int authType, int algId)	
입력파라미터	**출력파라미터**
char* ID : 사용자의 ID	없음
char*passwd : 사용자의 비밀번호	**리턴값**
int authType : 인증방식	
AUTH_ID_PASS(1) : ID와 비밀번호 단순비교(N/A)	사용자
AUTH_OTP(2) : 원타임 패스워드 비교(N/A)	인증결과에
AUTH_DIGITAL_ID_ICC(3) : IC카드에 저장된 디지털 ID를 이용한 인증	따라
AUTH_DIGITAL_ID_FILE(4): 파일에 저장된 디지털 ID를 이용한 인증	AUTH_SUCCESS(1) OR
int algId : 알고리즘	
ALG_SEED(100) : SEED	
ALG_DES(101) : DES	AUTH_FAILURE(0)
ALG_3DES(102) : 3DES	

(그림 4) 사용자 인증 함수

crypt.dll을 사용하기 위해서는 먼저 사용자 인증이 반드시 이루어져야하다. 사용자 인증이 이루어진 후에는 파일이나 binary데이타에 대해서 암호화/복호화를 수행할수 있는 상태가된다.

4.2 암호화 시스템

기존의 워게임 시뮬레이션 시스템은 군사기밀 정보(지도데이타, 군부대정보가 포함된 시나리오파일)가 보안장치없이 ASCII파일로 관리되어 유출에 대한 위험성을 가지고 있다. 이러한 정보는 반드시 암호화하여 저장/관리되어야하며 데이터 기밀성 제공을 위해 블록알고리즘을 사용한다. 블록 암호알고리즘(Block Ciphers)은 대부분은 Feistel 구조로 설계되며 Feistel 구조는 각 t비트인 L_0, R_0 블록으로 이루러진 2t비트 평문블록(L_0, R_0)이 r 라운드($r \geq 1$) 을거쳐 암호문 (L_r, R_r) 으로 변환되는 반복구조를 말한다. 즉 평문 블록이 여러 라운드를 거쳐 암호화되는 과정을 말한다. DES는 공표된 이래로 암호강도에 비해 키 길이가 너무 작다는 단점이 있다. 이러한

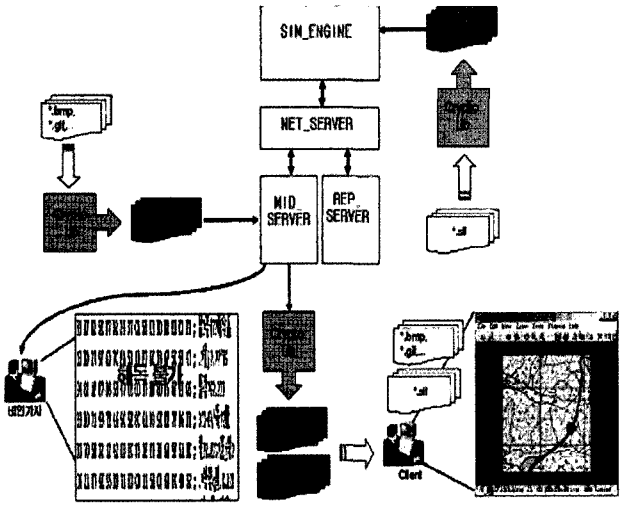
DES를 안전하게 사용하기 위해서는 키 길이와 키 선택이 중요하며 키 전수 탐색방법(Brute-force)이나 차분해독법(Differential Cryptanalysis), 선형해독법(Linear Cryptanalysis) 등의 공격으로부터 안전하려면 키 길이를 112비트 이상 늘려야한다[13].

암호시스템중 S/W암호라이브러리'방식은 클라이언트에 암호모듈을 탑재하여 사용자 인증후에 실행되도록 하는 방식으로 공개키 암호를 사용하지 않을 경우 키 관리에 대한 어려움이 내재하지만 클라이언트 사용자들이 사용하기 간편한 장점이 있다[14].

S/W모듈과 동일한 기능을 수행하지만 스마트카드 혹은 USB모듈을 사용하는 'H/W 연동라이브러리'방식이 있다. 이 방식은 클라이언트 사용자들을 강력하게 통제할수 있지만 H/W를 구입해야하는 어려움이 있다[14].

이논문에서는 데이터 기밀성 제공을 위해 블록암호알고리즘을 사용하며 128비트 이상의 키 길이를 사용하는 국내 표준알고리즘인 SEED을 사용하여 클라이언트 사용이 간편한 'S/W 암호라이브러리'방식으로 설계 및 구현한다.

(그림 5)는 암호라이브러리로 암호화되는 데이터 보안 처리 절차를 보여준다. 각 클라이언트 사용자들은 이 데이터를 복호화한 후 사용하게 되는데 인가되지 않은 사용자는 암호화된 데이터를 복호화할수 있는 키가 없으므로 데이터를 얻는다 해도 내용을 볼 수 없게 된다.



(그림 5) 데이타보안 처리절차

Crypto-lib API는 워게임 시뮬레이션 시스템의 보안 기능을 구현하는데 사용되는 암호화 라이브러리이다. 여기에 포함된 기능은 사용자 식별을 위한 IC 기반 사용자 인증 모듈, 데이터기밀성을 제공하기 위한 암호화/복호화 모듈, 데이터 무결성을 위한 MAC(Message Authentication Code)등을 포함하고 있다.

4.2.1 파일 암호화/복호화

encryptFile은 파일을 암호화하는 함수이며 전제조건으로

int encryptFile(char* inFileName, char* outFileName)	
입력파라미터	**출력파라미터**
char* inFileName : 암호화할 파일이름 char* outFileName : 암호화해서 저장할 파일이름 NULL일 경우 inFileName에 확장자 .sac를 붙인다	없음 **리턴값** 암호화 결과에 따라 정의된 값을 리턴한다

(그림 6) 파일암호화 함수

int decryptFile(char* inFileName, char* outFileName)	
입력파라미터	**출력파라미터**
char* inFileName : 복호화할 파일이름 char* outFileName : 복호화해서 저장할 파일이름 NULL일 경우 inFileName에 확장자 .bmp를 붙인다	없음 **리턴값** 암호화 결과에 따라 정의된 값에따라 리턴한다

(그림 7) 파일복호화 함수

key는 사용자 인증후 생성되어 글로벌 메모리에 저장되며 함수는 (그림 6)과 같다.

decryptFile은 encryptFile 함수로 암화된 파일을 복호화하는 함수이며 전제조건으로 key는 사용자 인증후 생성되어 글로벌메모리에 저장되며 함수는 (그림 7)과 같다.

encryptFile, decryptFile 각각에 암호화할 파일이름과 암호화될 파일이름, 암호화된 파일이름과 복호화될 파일이름을 입력하여 쉽게 사용할 수 있다.

4.2.2 Binary 데이터 암호화/복호화

encryptData은 Binary 데이터를 암호화하는 함수로서 전제조건으로 key는 사용자 인증후 생성되어 글로벌메로리에 저장되며 함수는 (그림 8)과 같다.

decryptData는 encryptData 함수로 암호화된 binary 데이터를 복호화하며 전제조건으로 Key는 사용자 인증후 글로벌메모리에 저장되며 함수는 (그림 9)와 같다.

Binary 데이터를 암호화/복호화하기 위해서는 encryptData와 decryptData라는 두 함수를 이용해야하며 이 두 함수의 인수가 포인터이므로 사용하는데 있어서 주의가 필요하다. 암

int encryptData (BYTE* in, long inLength, BYTE** out, long* outLength)	
입력파라미터	**출력파라미터**
BYTE* in : 암호화할 데이타 long inLength : 암호화할 데이터의 길이 int algID : 암호화알고리즘	BYTE** out : 암호화된 데이터 long* outLength : 암호화된 데이터의 길이
	리턴값
	암호화 결과에 따라 정의된 값을 리턴한다

(그림 8) Binary 데이터 암호화 함수

int decryptData (BYTE* in, long inLength, BYTE** out, long* outLength)	
입력파라미터	**출력파라미터**
BYTE* in : 복호화할 데이타 long inLength : 복호화할 데이터의 길이 int algID : 복호화알고리즘	BYTE** out : 복호화된 데이터 long* outLength : 복호화된 데이터의 길이
	리턴값
	복호화 결과에 따라 정의된 값을 리턴한다

(그림 9) Binary 데이터 복호화 함수

호화/복호화 절차는 (그림 10)과 같다.encrytData를 사용하기 위해서는 암호화할 binary 데이터가 필요하며 비주얼베이직의 배열형태로 선언한후 데이터를 집어 넣는다. 또한 binary 데이터에 대한 길이가 필요한데, 이는 Long형으로 선언한후 길이를 집어넣는다(라인 1~4).

encryptData가 수행된 후 암호화된 결과를 가리키는 포인터가 필요한데 비주얼베이직에서는 포인터 형을 지원하지 않으므로 포인터 값을 충분히 담을수 있는 Long형으로 포인터를 선언한다(라인 5~7).

이함수의 첫 번째 인수는 암호화할 binary 데이터에 대한 포인터이다. 앞에서 선언한 byte 배열에 대한 포인터를 비주얼베이직에서 제공하는 VarPtr이란 함수를 통해서 얻는다(라인 8,9). 함수를 호출할 때 인수를 넘기는 순서는 암호화 할 binary데이타에 대한 포인터(inData_ptr), 암호화할 Binary 데이터에 대한 길이(inLength), 암호화된 binary를 받을 포인터(outData_ptr), 암호화된 binary 데이터에 대한 길이(outLength)이다(라인 10).

```
1: Dim inData(256) As Byte
2: indata(0) = &H1; indata(1) = &H2; indata(2) = &H3;
   indata(3) = &H4; indata(4) = &H5;
3: Dim inLength As Long
4: inLength = 5
5: Dim outData_ptr As Long
6: Dim outLength As Long
7: Dim ret As Integer
8: Dim inData_ptr As Long
9: inData_ptr =Varptr(indata(0))
10: ret = encryptData(inData_ptr, inLength, outData_ptr, outLength)
11: Dim outData(256) As Byte
12: call memcpy_from_ptr_to_byte_array(outData_ptr, outData, outLength)
13: Dim decData(256) As Byte
14: Dim decLength As Long
15: Dim decData_ptr As Long
16: ret = decryptData(outData_ptr, outLength, decData_ptr, decLength)
17: call memcpy_from_ptr_to_byte_array(decData_ptr, decData, decLength)
18: public sub memcpy_from_ptr_to_byte_array(ptr As Long, byteArray() As
    Byte, Length As Long)
19: call CopyMemory(ByVal VarPtr(byteArray(0)), ByVal ptr,Length)
20: end sub
```

(그림 10) Binary데이터 암호화/복호화 절차

비주얼베이직은 포인터를 지원하지 않기 때문에 함수를 호출한후 얻은 outData_ptr을 그대로 사용할수 없다. 따라서 아래 정의한 memcpy_from_ptr_to_byte_array 함수(라인 18~20)를 사용하며 포인터의 내용을 byte 배열로 복사해주는 함수다. 호출할 때 넘기는 인수는 복사할 포인터(outData_ptr), 복사될 내용을 담을 byte 배열(outData), 복사할 내용의 길이(outLength)의 순서로 넘긴다. 함수 memcpy_from_ptr_to_byte_array를 소스에 반드시 포함하도록 한다(라인 11, 12).

4.3 네트워크 보안시스템

네트워크 보안시스템은 모의엔진 서버와 네트워크 서버, 중계서버, 클라이언트 사이에 대한 암호화 통신을 제공한다. 암호화통신 보안 프로토콜은 별도 보안 프로토콜을 설계하여 구현할 수 있다. 이 프로토콜로 설계하는 것은 성능에 최적화된 프로토콜을 적용 가능하나 구현이 복잡하고 안정성에 대한 신뢰도가 낮다[14].

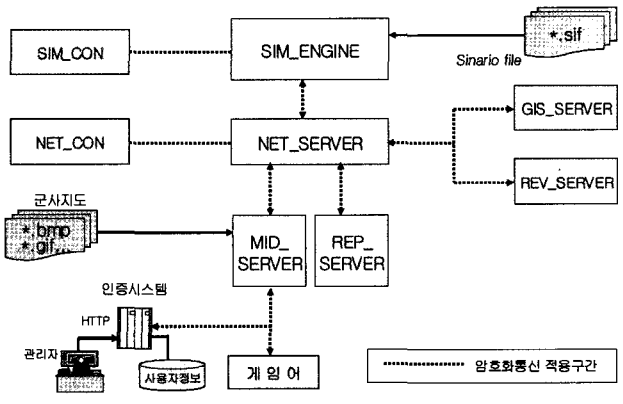
다음은 기존에 널리 사용되는 프로토콜을 활용할수 있다. 인터넷에서 검증되어 널리 사용되고 있는 보안 프로토콜로는 TCP 계층위에서 구현되며, 인증, 무결성, 기밀성을 제공하는 SSL이 있다. 이 프로토콜은 안정성에 대한 신뢰도가 높다[15,

16].

다음은 IP계층에서 구현되는 보안 프로토콜로 IPSec를 활용하는 방식이 있다. 이 프로토콜은 운영체제에 탑재된 IPSec을 활용할수 있지만 IPSec 운용이 어렵고 성능저하가 큰 단점이 있다[5].

이 논문에서는 시스템의 특성상 안정성에 대한 신뢰도가 높고, 실제 테스트결과 성능저하가 미미한 SSL를 활용하여 구현되었다. SSL은 클라이언트, 서버 두 통신 응용프로그램간에 프라이버시를 지원하고 상대방을 인증하기 위해 설계된 프로토콜로서 SSL프로토콜은 데이터를 주고받기 위해, TCP와 같은 트랜스포트 프로토콜을 이용한다. SSL의 특징은 응용프로토콜과 독립되어 있는 것으로, HTTP, FTP, TELNET과 같은 상위계층 응용 프로토콜은 SSL프로토콜 위에서 투명하게 동작할 수 있다. SSL프로토콜을 이용하면 암호화 알고리즘과 세션키를 협상할수 있고, 응용프로토콜이 데이터를 보내거나 받기전에 공개키 기법과 같은 비대칭적 암호방법을 이용해 상대방의 인증을 수행할수 있다. 또한 비밀키를 정하기 위한 간단한 통신 이후에는 모든 메시지를 암호화하여 전송하여 메시지의 기밀성을 보장하고 MAC(Message Authentication Code)을 통해 메시지의 무결성을 제공한다.

SSL은 레코드 프로토콜과 핸드쉐이크 프로토콜로 구성되어 있다. SSL레코드 프로토콜은 SSL 핸드쉐이크 프로토콜을 포함한 다양한 상위 레벨의 프로토콜을 캡슐화하는데 사용되고, SSL핸드쉐이크 프로토콜은 응용프로토콜이 데이터를 주고 받기전에 클라이언트와 서버가 서로를 인증하고, 암호화알고리즘과 암호화키를 협상하는데 이용된다. 워게임 시뮬레이션시스템을 구성하는 서버와 서버,서버와 클라이언트사이에 이루어지는 TCP/IP연결에 대해서 SSL을 통한 보안통신을 (그림 11)과 같은 구간에서 적용한다.



(그림 11) 암호화 통신

워게임 시뮬레이션 통신 암호화라이브러리에 포함되는 모듈은 크게 서버용 모듈과 클라이언트용 모듈로 나눌수 있다. 이 두 모듈은 연결, 데이터전송, 연결종료에 대해서 보안 통신을 수행하기 위한 함수를 공통으로 가지고 있다. 이 외에 워게임 시뮬레이션 시스템과 통신 암호화 라이브러리가 상호작용할 수 있도록 지원하는 함수들도 포함하고 있다.

5. 실험 및 결과분석

워게임 시뮬레이션 시스템은 적의 동시다발적인 적의 공격에 대해 신속한 상황조치를 하여 대응하여야 하기 때문에 보안 시스템으로 인해 시스템 전체의 성능저하를 초래하게 되면 실제 상황을 시뮬레이션 하는데 큰 지장을 초래하므로 보안 시스템으로서 가치를 상실하게 된다.

〈표 2〉 시험 환경

시스템 명		운용 체제	시스템명		운용 체제
SIM_ENGINE	모의엔진	Linux 7.2	MID_SERVER	중계서버	Linux 7.2
SIM_CON	모의엔진 제어기	Win 2000	REP_SERVER	보고서 서버	Linux 7.2
NET_SERVER	네트워크 서버	Linux 7.2	GIS_SERVER	상황도 서버	Linux 7.2
NET_CON	네트워크 제어기	Win 2000	REV_SERVER	사후검토 서버	Linux 7.2

따라서 워게임 시뮬레이션 시스템에 보안 시스템을 적용하여 과거에 훈련한 명령 및 데이터를 활용, 성능평가를 실시하였다. 성능평가는 워게임 환경이 구축된 상황에서 보안시스템을 적용시켰을 경우와 적용시키지 않았을 경우로 나누어 그 측정 결과를 비교하였다. 실험 환경은 <표 2>와 같은 성능의 다중 서버가 설치된 (그림 1)과 같은 구성도를 가진 실제 워게임환경이며, 과거에 훈련한 명령 및 데이터를 그대로 활용하여 재 실행하였으므로 실제 훈련시와 동일한 다수의 클라이언트들이 연결된 환경이다.

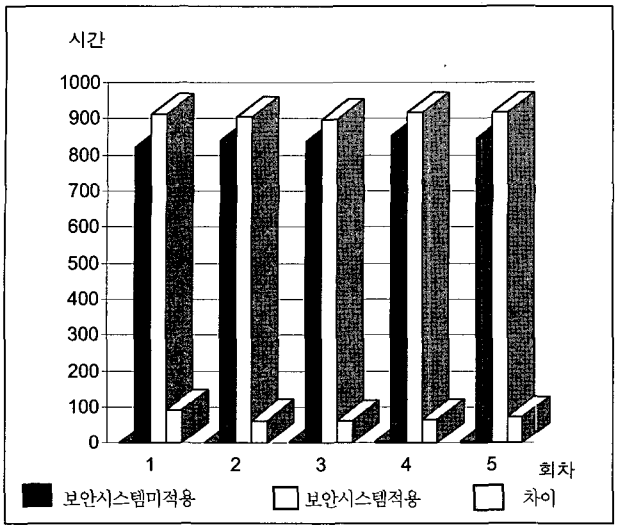
5.1 네트워크 보안시스템 성능평가

5.1.1 시험방법/데이타

성능평가방법	명령건수	전송데이타	단위시간
재현(Replay) 명령수행	20,220 건	89,726 kbyte	초(second)

성능평가를 위해 실행한 명령은 과거에 실제 워게임을 실시할 때 실행되었던 명령(Replay 명령)을 다시 실행하였으며 명령건수는 20,220건(89.726kbyte) 의 다양한 종류의 명령어이며 워게임 시뮬레이션 시스템에 제안한 보안시스템을 연동한 상태와 연동하지 않은 기본시스템 환경하에서 총 5회에 걸쳐 반복시험을 실시하였다.

5.1.2 시험결과



회차	보안시스템 미적용	보안시스템 적용	차이
1	821	912	91
2	841	904	63
3	836	897	61
4	852	917	65
5	843	915	72
평균	838.6	909	70.4

(그림 12) 네트워크 보안시스템 성능평가 실험 결과

성능을 평가한 결과 (그림 12)와 같이 보안시스템을 적용하기전에는 명령어를 실행한 결과 평균 838.6초가 소요되었으나 보안시스템을 적용하였을때는 평균 909초가 소요되어 보안시스템 적용후 평균 70.4초라는 짧은시간 지연이 발생한 것을 볼때 성능저하가 거의 발생하지 않은것을 알 수 있다. 따라서 개발된 체계가 워게임 시뮬레이션 보안시스템으로 가용하다는 것을 알 수 있다.

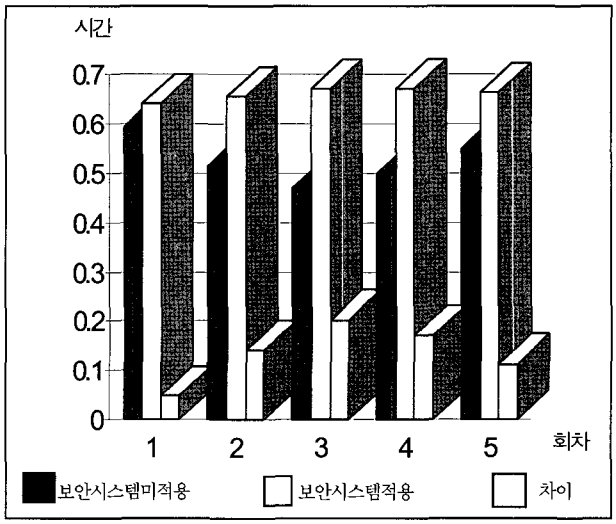
5.2 암호화 시스템 성능평가

5.2.1 시험방법/데이타

성능평가방법	이미지수량	이미지데이타	단위시간
암호화된 이미지 파일 화면출력	1:5만 20개 1:10만 20개	1:5만지도(184 kbyte) 1:10만지도(134 kbyte)	초(second)

성능평가를 위해 암호화된 이미지파일인 1:5만지도(184kbyte) 20개를 검색했을때 소요되는 시간을 시험하였으며, 또한 1:10만 지도(134kbyte) 20개를 검색했을때 소요되는 시간을 시험하였다. 워게임 시뮬레이션 시스템에 제안한 보안시스템을 연동한 상태와 연동하지 않은 기본시스템 환경하에서 총 5회에 걸쳐 반복시험을 실시하였다.

5.2.2 시험결과

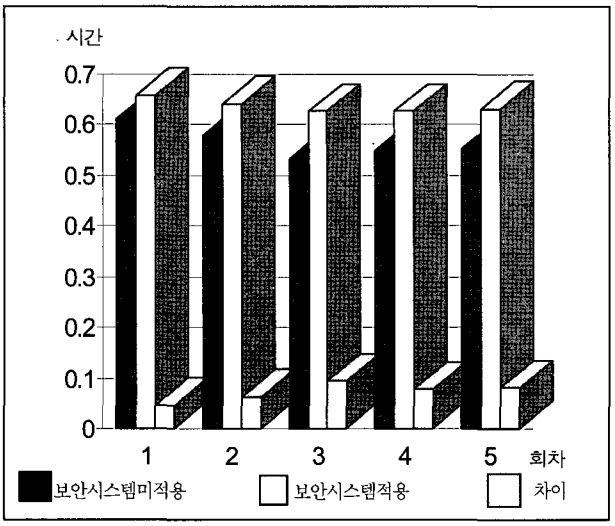


회차	보안시스템 미적용	보안시스템 적용	차 이
1	0.593750	0.640625	0.046875
2	0.515625	0.656250	0.140625
3	0.468750	0.671875	0.203125
4	0.500000	0.671875	0.171875
5	0.550000	0.663375	0.113375
평균	0.550000	0.663375	0.113375

(그림 13) 암호화시스템 성능평가(1:5만 지도)

성능을 평가한 결과 (그림 13)과 같이 보안시스템을 적용하기전에는 명령어를 실행한 결과 평균 0.55 초가 소요되었으나 보안시스템을 적용하였을때는 평균 0.66초가 소요되어 보안시스템 적용후 평균 0.11초라는 짧은시간 지연이 발생한 것을 볼때 보안시스템을 설치하여 암호화를 한 파일도 신속하게 검색되므로 워게임 시뮬레이션시스템으로 가용하는 것을 알 수 있다.

성능을 평가한 결과 (그림 14)와 같이 보안시스템을 적용하기전에는 명령어를 실행한 결과 평균 0.55 초가 소요되었으나 보안시스템을 적용하였을때는 평균 0.63초가 소요되어 보안시스템 적용후 평균 0.08초라는 짧은시간 지연이 발생한 것을 볼때 보안시스템을 설치하여 암호화를 한 파일도 신속하게 검색되므로 워게임 시뮬레이션시스템으로 가용하는 것을 알 수 있다.



회차	보안시스템 미적용	보안시스템 적용	차 이
1	0.609375	0.656250	0.046875
2	0.578125	0.640625	0.062500
3	0.531250	0.625000	0.093750
4	0.546875	0.625000	0.078125
5	0.550000	0.631250	0.081250
평균	0.550000	0.631250	0.081250

(그림 14) 암호화시스템 성능평가(1:10만 지도)

6. 결 론

워게임 시뮬레이션 시스템은 군사작전을 가상으로 실시하는 시스템으로서 운용되는 자료들이 대부분 보안성이 요구되는 자료들이다. 특히 워게임 시뮬레이션 시스템 개발시 지도데이타, 부대정보등과 같은 군사기밀 정보 및 네트워크에 대한 보안 실험을 고려하지 않아 이에 대한 정보 유출의 위험성을 내재하고 있다. 따라서 이러한 군사관련정보의 유출을 방지하기 위한 보안대책이 강구되어야 하며 보안시스템 개발이 필요하였다.

이 논문에서는 워게임 시뮬레이션 시스템을 위한 보안시스템 개발을 위해서 먼저 운용환경 및 보안 취약성 분석을 통해 워게임 시뮬레이션 시스템에서 필요로하는 보안 정책을 수립하고 이를 수행하기 위한 보안시스템을 설계 및 구현하였다. 워게임 시뮬레이션 시스템을 지원하는 보안 시스템의 구성 요소는 사용자 인증 시스템, 암호화시스템, 네트워크보안 시스템이다.

구현된 보안시스템을 워게임 시뮬레이션시스템에 적용하여 실험한 결과 암호화시스템,네트워크 보안시스템 모두 적용전과 비교하여 성능을 저하시키지 않고 신뢰성있는 보안기능을 수행할수 있어 워게임 시뮬레이션시스템의 보안성 향상에 기여할수 있음을 확인하였다.

향후 연구과제로는 구현된 보안시스템에 통합인증시스템, Secure OS, 침입차단시스템, 침입탐지시스템등의 보안기능을 통합 및 확장하여 적용하고 군에 추진하고 있는 C4I체계에 적용하기 위한 연구가 필요하다.

참 고 문 헌

[1] DoD, USD(A&T), "DoD Modeling and Simulation Master Plan", October, 1995.

[2] 김진수, "워게임 시뮬레이션 시스템을 위한 점진적 형성 뷰 관리모델",박사학위논문, 2004.

[3] 최상영(국방대학교), "국방모델과 시뮬레이션에 대한 고찰", 안보연 연구보고서, 1997.

[4] Matt Bishop, "Computer Security : Art and Science", Pearson Education, 2003.

[5] Ben Galbraith, et. al., "Professional Web Services Security", Wrox, 2002.

[6] Charles P. pfleeger and Shari Lawrence Pfleeger, "Security in Computing", 3rd ed. pearson Education, 2003.

[7] 이재승, 김상춘, "대규모 네트워크 환경에서의 보안관리를 위한 보안평가 시스템 설계", 한국정보처리학회, 2003.

[8] 이상대, 이일수, 김성수, "포항종합제철(주)의 정보보안시스템 적용사례", 한국정보처리학회, 1997.

[9] 김수형, 장철수, 노명찬, 김성훈, 김중배, "응용서버를 위한 보안프레임워크 설계 및 구현", 한국정보처리학회, 2003.

[10] Simson Garfinkel & Gene Spafford, "Practical UNIX & Internet Security", O'REILLY, Second Edition, April, 1996.

[11] Zhiqun Chen, "Java Card Technology for Smart Cards", Addison-Weslely, 2000.

[12] Uwe Hansmann, Marin S. Nicklous, Thomas S Nicklous, Frank Seliger, "Smart Card Application Development Using Java", Springer, 1999.

[13] 홍성룡, 조성호, "SDR System 적용을 위한 한국형 암호알고리즘(SEED)구현 및 성능분석", 한국정보과학회, 2002.

[14] William Stallings, "Cryptography and Network Security-Principles and Practices", Prentice Hall, 2003.

[15] Alan O. Freier, Phillip Karlton, Paul C. Kocker, "The SSL Protocol version 3.0", Netscape, 1996.

[16] 조은애, 김영갑, 문창주, 박대하, 백두권, "SSL 컴포넌트의 설계 및 구현", 한국정보과학회, 2002.

[17] KISA, http://www.kisa.or.kr/sysevaluation/menu1/sub2/tcsec.html

송 종 석

e-mail : compsong@empal.com
1986년 금오공과대학교 전산학과(학사)
1989년 국방대학교 전산학과(이학석사)
1996년 충북대학교 전산학과 박사과정 수료
2003년~현재 육군본부 지휘통신참모부 근무
관심분야 : 시공간 데이터베이스, 데이타마이닝

신 문 선

e-mail : msshin@dblab.chungbuk.ac.kr
1988년 충북대학교 전산통계학과 학사
1997년 충북대학교 전자계산교육 석사
2004년 충북대학교 전자계산학과 이학박사
관심분야 : 시공간 데이터베이스, 데이터 마이닝, 데이터베이스 보안, 침입탐지 시스템

김 진 수

e-mail : kjs9990@yahoo.co.kr
1981년 계명대학교 수학과(학사)
1987년 국방대학교 전산학과(이학석사)
1998년 충북대학교 전산학과 박사과정 이수
2002년~현재 육군교육사 체계분석실 근무
관심분야 : 실시간 객체, 분산컴퓨팅, 시공간 데이터베이스

류 근 호

e-mail : khryu@dblab.chungbuk.ac.kr
1976년 숭실대학교 전산학과 이학사
1980년 연세대학교 공학대학원 전산전공 공학석사
1988년 연세대학교 대학원 전산전공 공학박사
1976년~1986년 육군군수 지원사 전산실(ROTC장교), 한국전자통신 연구원(연구원), 한국방송통신대 전산학과(조교수)
1989년~1991년 Univ. of Arizona Research Staff (TempIS 연구원, Temporal DB)
1986년~현재 충북대학교 전기전자및컴퓨터공학부 교수
관심분야 : 시간 데이터베이스, 시공간 데이터베이스, Temporal GIS, 객체 및 지식기반 시스템, 지식기반 정보검색 시스템, 데이터마이닝, 데이터베이스 보안 및 Bio-Informatics