제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

워게임 연습체계에서의 효율적 정보보호 방안 연구

이 강 택* 이 동 휘* 김 귀 남*
* 경기대학교 정보보호기술공학과

요 약

미국이 대 이라크전 연장선에서 북한 핵문제를 봄에 따라, 한반도의 긴장은 날로 증가하고 있으나, 국내 여건의 변화에 따른 국방 가용재원의 감소, 대규모 야외군사훈련을 수행하기 위한 공간 확보의 어려움 및 안전과 환경문제 등으로 인해 한국군의 야외훈련 여건은 날로 열악해져 가고 있는 실정이다.

이에 따라, 야외훈련의 대체방안으로서 보다 경제적이고 과학적인 워게임 모델에 의한 CPX(Command Post Exercise: 지휘소연습) 즉, 워게임 연습이 최적의 대안으로 주목받고 있으며, 이를 통한 단독, 합동 및 연합연습이 수행되고 있다.

그러나, 현 워게임 연습체계는 정보보호라는 관점에서 볼 때 많은 문제점을 안고 있다. 국방전용망의 경우 그 구성이 인터넷과의 단절을 전제로 네트워크 레벨에서의 암호화만을 통해 데이터를 보호하고 있는 실정이고, 워게임 연습체계 내에서의 공격이나 신뢰하고 있는 네트워크를 통한 공격에 대해선 무방비 상태에 놓여져 있으며, 시스템 레벨에서의 보안 또한 부실한 실정에 있다.

따라서, 본 연구에서는 워게임 연습체계의 효율적이며 안전한 정보보호 방안 제시를 위해 네트워크 레벨에서의 정보보호 체계 및 시스템 관점에 초점을 두고 연구가 수행되었으며, 결론적으로 현 워게임 연습체계에서의 최적의 정보보호 방안을 제시하고자 한다.

A Study on the Efficient Information Security Methodology under a Korea War-Game Exercise System

Kang Taek Lee* Dong Hwi Lee* Kuinam J Kim*

ABSTRACT

There is increasing tension in the Korean Peninsula from the US' putting the NK's nuclear issue along the line of war in Iraq. However, there is worsening in ROK's field exercise condition from decresing defense financial supports, being difficlut to obtain enough space for volumable exercises, and securities and circumstances issues.

With acknowleging those problems, CPX(Command Post Exercise), namely war game exercise which is more economical and scientific exercise has earned its attention as the best alternative measure of field exercise war game exercise has already been applyied to independent, joint, and combined exercises.

However, the current war game system contains lots of problems in terms of security. Defense network uses dedicated line isolated with internet and secure data through network level encoding. It is vulerable to get attack during war game exercise or from credited network. Sytem security is also subject to reinforced.

This research is performed focusing on network and system level securities, and through it, the author will show the effective and optimized security solution for war game system.

I. 서 론

9. 11 참사에 대한 보복의 일환으로 '미국의 대 테러와의 전쟁선언'과 함께 시작된 이라크전이 종전된 지도 벌써 1년이 지났으나, 부시 행정부의 실정과 약한 전쟁의 명분으로 인해 반미감정이 날로 격해짐에 따라, 친미국가를 대상으로 하는 보복테러로 인해 국제정세는 이전보다 더욱 혼란스러울 뿐만 아니라 북한 핵문제와 관련하여 한반도의 긴장도 날로 증대되고 있다. 또한, 국내 사회여건의 변화에 따른 국방 가용재원의 감소, 대규모 야외군사훈련을 수행하기 위한 공간확보의 어려움 및 안전과 환경문제 등으로 인해 한국군의 야외군사훈련 여건은 날로 어려워져 가고 있는 실정이다. 이에 따라, 보다 경제적이고 과학적인 훈련방안의 도입이 절실히 요구되고 있는데 첨단IT기술의 급속한 발전에 힘입어, 현재 워게임모델에 의한 CPX(Command Post Exercise: 지휘소연습)연습 즉, 워게임 연습이 최적의 대안으로 각광받고 있다.

그러나, 현 워게임 연습체계는 국방전용망을 기반으로 합동참모본부를 중심으로 하는 각 군 작전사별 분산 연습체계를 구축·운영하고, 각 사이트 링크마다 보안장비를 설치하여 연습이 수행되어지고 있다. 하지만, 독립된 전용 네트워크 및 보안장비의 설치에 대하여 보안적 관점에서 볼 때, 단순한 물리적 보안에 치중하는 형태로 구성되어 있는 현 워게임 연습체계는 많은 문제점을 내재하고 있다. 왜냐하면, 실제 네트워크 상에서 발생하는 정보 유출의 대부분은 물리적 보안 측면보다는 추상적 측면에 더 빈번히 발생하고 있기 때문이다. 추상적 측면이란 데이터의 무결성, 가용성, 비밀성 보장 등이 이에 속한다.

상용 인터넷의 경우 정보보호를 위한 방안으로 각각의 기능에 맞는 정보보호 장비를 채택하여 사용하고 있다. 하지만, 현재 국방전용망의 경우 그 구성이 인터넷과의 단절을 전제로 네트워크 레벨에서의 암호화만을 통해 데이터를 보호하고 있는 실정이다. 따라서, 워게임 연습체계 내에서의 공격이나 신뢰하고 있는 네트워크를 통한 공격에 대해선 무방비 상태에 놓여있다.

본 연구에서는 워게임 연습체계의 효율적이며 안전한 네트워크 구성을 위한 방안을 제시함으로써 보호되어야 할 워게임 모델내의 객체들이 가지고 있는 속성 값들에 대한 자료 유출, 변조 및 파괴 등의 위험을 최소화하여 워게임 연습체계내의 무결성, 가용성, 비밀성 보장의 목표를 달성하고자 한다.

이를 위해, 네트워크 레벨에서의 정보보호 체계 및 시스템 관점에 초점을 두고 연구가 수행되었으며 이것을 통해 워게임 연습체계의 보안 요구사항을 만족하는 종합적인 정보보호 대책을 수립할 수 방안에 대해 알아보고자 한다.

II. 한국군 워게임 연습체계 및 문제점

1. 워게임 연습의 개요

가. 워게임 연습의 정의

워게임 연습의 일반적 정의는 지휘소연습(CPX), 즉 "가상적으로 연출된 전쟁 상황하에서 지휘관 및 참모요원으로 하여금 현행 교리, 전역계획, 작전계획, 예규, 규정, 교범 및 절차 등을 적용하고 이를 평가하여 개선, 보완할 목적으로 실시하는 통제형 전쟁 연습"[1]을 수행함에 있어 워게임모델을 그 수단으로 활용하는 연습 방법을 말한다. 한국군의 대표적인 워게임 연습으로 함참주관의 압록강연습과 연합사 주관의 을지포크스렌즈연습이 있으나, 본 연구에서는 한국군 단독연습인 압록강연습을 주 대상으로 하였다.

■ 모델(Model) : 현실체계의 특성들 간의

1) 합동참모본부, "연합 및 합동훈련 규정", 2002

관계를 구현한 소프트웨어

■ 시뮬레이션(Simulation)

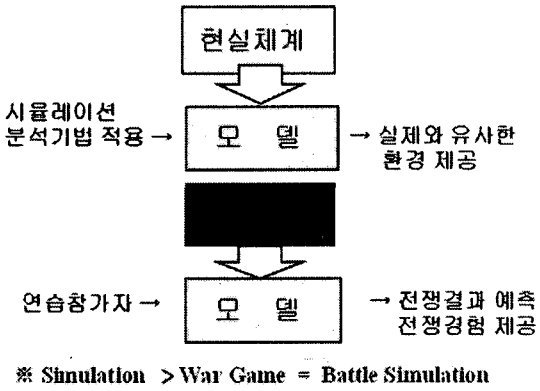


그림 <2-1> 워게임 모델

■ 워게임(Wargame)

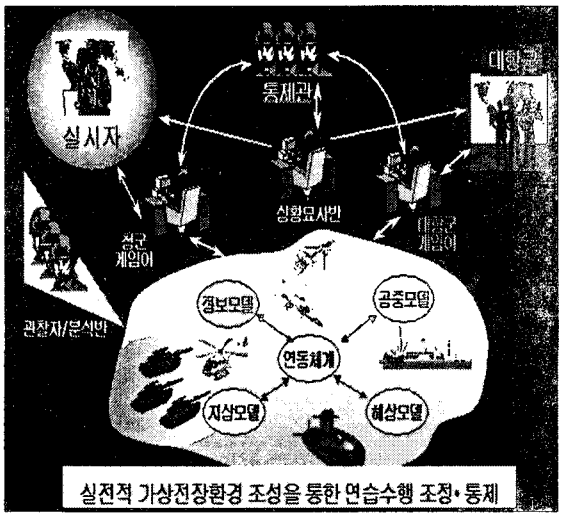


그림 <2-2> 워게임 연습의 정의 및 형태

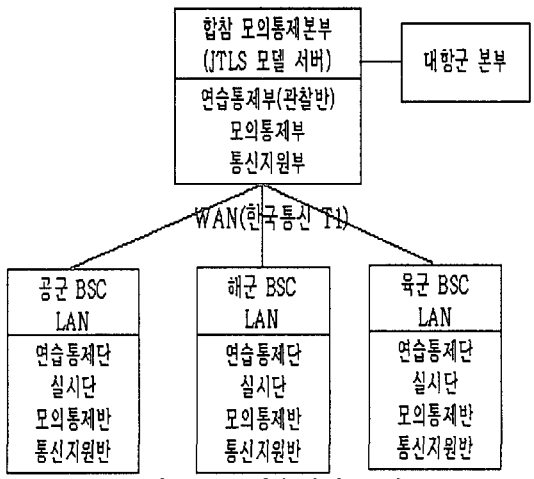
나. 워게임 연습체계 및 구성

한국군의 합동 워게임 연습체계는 연습수행체계, 워게임운영체계, 통신지원체계로 구분할 수 있다.

연습수행체계는 연습을 계획, 진행 및 통제하고 사후강평을 통해 연습의 성과를 평가하며 연습간 임무수행을 위해 연습통제단, 실시단, 대항군, 관찰반 등을 구성하여 운용한다.

워게임운영체계는 연습의 주요수단인 JTLS(Joint Theater Level Simulation: 합동전 모델)의 연습개시제원을 포함하는 데이터베이스 등을 연습목적에 맞게 사전 구축하고, 분산 BSC(Battle Simulation Center: 전투모의센터)간 운영모델 및 시스템을 지원하며, 이를 위해 모의통제반을 구성하여 운영한다.

통신지원체계는 연습수행을 위한 별도의 국방전용망 및 통신체계를 구축하여 운용·지원하며, 이를 위해 각 BSC별 통신지원반을 구성하여 운용한다.



<그림 2-3> 연습체계 구성도

2. 워게임 연습체계의 문제점

가. 운용적 측면 문제점

국방정보통신망은 각 목적에 맞는 군 전용망을 토대로 발전하여왔다. 또한, 군 보안 정책이 기밀성에만 치우친 네트워크 정책으로 운용되고 있어 시스템과 네트워크를 분리하여 관리하는 정책이 부재한 실정이다. 현재 워게임 연습체계에서는 독립된 전용망 및 암호화 장비를 제외한 보안 장비는 부재한 상태에 있다.

특히 워게임 연습에 있어서 적·아간의 전력과 관련한 비밀자료 및 전투결과 데이터 등에 대한 무결성, 비밀성 및 가용성 등의 보장은 매우 중요함에도 불구하고 이들에 대한 정보보호 대책이 매우 부실한 상태에 있으며, 네트워크를 통해 적이나 내부자에 의한 데이터의 유출, 삭제 및 위/변조 등이 되었는지 여부를 파악조차 할 수 없는 실정에 놓여있다.

나. 구성적 측면 문제점

현재 워게임 연습체계의 구성은 국방전용망(한국통신 TI급)을 통한 각각의 BSC(전투모의센터)가 동일한 암호화 장비(ED-90X)를 사용함에 따른 상호 신뢰구조이다.

즉, 데이터 암호화에 의존하여 정보를 보호하는 기법만을 적용하고 있다. 그러나, 실시간 고속의 다수 명령문처리가 요구되는 워게임 연습체계의 특성상 각 링크 단위로 암호화 장비를 통한 암호화를 함에 따라, 데이터 전송속도의 성능 저하로 연습의 효율성을 감소시키고 있으며, 네트워크 단위의 암호화만을 적용하여 사용하고 있기 때문에 인트라넷(LAN) 상의 공격에 대한 대비방법이 부재한 실정이다. 해킹 사고의 대부분이 내부 자나 기 침입한 불법침입자에 의한 것임을 감안했을 때 반드시 보완되어야할 사항이라 할 것이다.

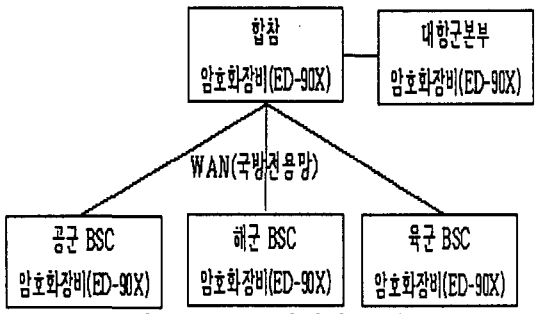


그림 <2-4> 보안체계 구성도

Ⅲ. 워게임 연습체계의 보안 필수 요소

1. 네트워크 레벨 정보보호

네트워크 레벨에서 보안적 측면으로 고려되어야 할 사항은 스니핑을 막는 것과 쉘 코드가 담긴 패킷들을 차단하고, 승인되지 않은 IP로부터의 진입을 막는 것 등과 같은 조치를 취함으로써 기본적으로 달성 가능하다.

가. 침입탐지시스템

침입탐지시스템을 논하기 전에 먼저 침입의 정의에 대해 살펴보면, 침입은 컴퓨터가 소유하는 자원의 무결성(integrity), 비밀성(confidentiality), 가용성(availability)을 저해하는 일련의 행위들의 집합을 의미하며, 컴퓨터 시스템의 보안정책을 파괴하는 행위를 의미한다[2].

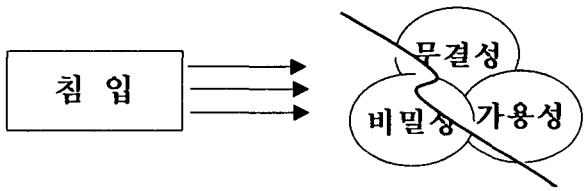


그림 <3-1> 침입의 정의

앞의 정의로부터 현재는 침입을 네트워크의 범위로 확장하여 적용하고 있다.

침입탐지시스템은 사용자 및 외부 침입자가 컴퓨터시스템 또는 네트워크의 자원을 정당한 권한 없이 불법적으로 사용하기 위한 시도 또는 내부 사용자가 자신의 권한을 오용하여 권한이 외의 자원을 사용하기 위한 시도를 사전에 탐지하여 그 피해를 예방하는 시스템을 말하며, 워게임 연습체계에서 필수적인 요소라 하겠다.

나. 침입차단시스템(방화벽)

2) S.kumar, "Classification and Detection of Computer Intrusions", Purdue University, Aug., 1995

워게임 연습체계의 정보보호를 위한 침입차단 시스템은 기본 요구사항이다. 침입차단시스템, 일명 방화벽은 두 네트워크간을 흐르는 패킷들을 미리 정해놓은 규칙에 따라 차단하거나 보내주는 패킷 필터링을 하는 장비를 말하며, 이 또한 워게임 연습체계에서 필수적으로 설치되어야 하겠다.

다. 암호화 장비

암호 기술은 평문을 해독 불가능한 형태로 변형하거나 또는 생성된 암호문으로부터 해독 가능한 형태로 변환하기 위한 원리, 수단, 방법 등을 취급하는 기술로 국방전용망에서의 불법적인 도청을 방지하기 위하여 사용 되어야하며, 암호화 장비설치를 통해 워게임 연습체계간 데이터를 암호화할 수 있다.

2. 시스템 레벨 해킹 방어대책

침입자에 의해서나 정상적인 권한을 가진 사용자가 시스템 내에 접속하여 불법적 접근시도를 방어할 수 있는 조치방안으로 보안운영체제 및 인증 시스템 도입이 요구된다.

가. 보안 운영체제

컴퓨터 운영체제의 보안상 결함으로 인하여 발생 가능한 각종 해킹으로부터 시스템을 보호하기 위하여 기존의 운영체제 내에 보안 커널을 추가로 이식한 보안 운영체제가 설치되어야 한다.

나. 인증 시스템

워게임 연습 참가자들로부터 시스템 내의 중요 정보와 자원을 보호하기 위해서는 시스템에 접근하는 사용자를 확인하는 과정은 필수적이다.

이와 같이 시스템 사용자의 접근 가능성 여부를 통제하고 확인하는 사용자 인증시스템이 설치되어야 한다.

Ⅳ. 역할기반 복합 암호화 체계의 제안

역할기반 복합 암호화 장비의 채택이 위에서 살펴본 보안 필수 요소들 중 다수를 현 워게임 연습체계의 큰 변동 없이 가장 효과적으로 만족시킬 수 있는 방안이라 판단된다.

가. 역할기반 체계

각 군의 단위 구성별 BSC 및 워게임 전장환경에서 사용이 허가된 사용자를 세분화 하여 각 모듈별 또는 보안이 필요한 민감한 정보만을 선택적으로 암호화하여 시스템의 피해를 최소화 할수있는 체계이다.

첫째, 모듈별 단위를 선택적 암호화로 성능저하를 최소화 하면서 보안성을 확보하는 인증키 및 접근제어 한다.

둘째, 각 BSC와 DB에 대한 강력한 접근 제어를 통해 인가된 내부 사용자의 데이터 남용 및 위변조를 방지하고 최고 권한을 이용하여도 유출되는 사고로부터 데이터를 보호 할수 있다.

셋째, 합참 모의통제 본부에 통합보안센터를 설치하여 전체 보안을 관리하며, 워게임 통합 훈련의 특성상 인증키는 역할에 따른 휘발성 1회용으로 제작 배포한다. 그리고 보안체계 수립, 보안사고 및 예방에 대한 활동을 한다.

나. 복합적 형태의 암호화 장비

외부로 전송되는 데이터의 암/복호화 기능 및 시스템 사용가능 접근제어 기능의 병행 수행이 가능한 암호화 장비를 말하며, 이는 네트워크 전체에 대해 동작할 수도 있고, 단순한 시스템 하나만을 위해 동작될 수도 있다.

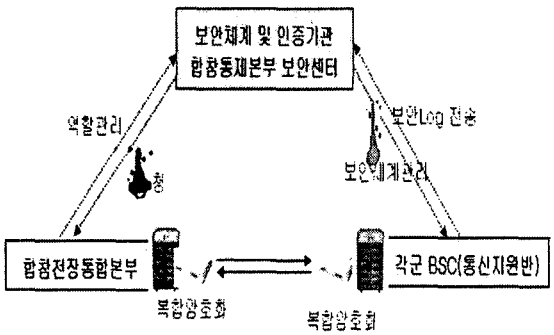
복합 암호화 장비의 주된 목적은 단일 시스템에 대한 인증, 암/복호화, 접근 통제를 동일한 정책과 관리를 통해 구현하고자 하는 것이므로, 단일화된 시스템 사용을 기반으로 하는 워게임 연습체계에 적용함은 당연한 것이다.

또한, 단순한 암호화 기능뿐만 아니라 내부에

Embaded-OS를 탑재시켜 다양한 종류의 서비스와 인증 등을 수행하게 할 수도 있다.

복합 암호화 장비의 동작을 위해서는 암호화 장비간에 키를 인증할 수 있는 인증기관이 필요하며, 암호화 장비 자체의 해킹을 막기 위해 Embaded-OS를 보안 운영체제로 구성하여 암호화 장비를 통한 해킹 방지가 가능하다.

그림<4-1>역할기반 복합 암호화 체계 흐름



다. 역할기반 복합 암호화 장비 적용시 이점

복합 암호화 장비를 워게임 연습체계에 적용할 시 얻을 수 있는 이점들은 다음과 같다.

- 개인용 방화벽 모듈을 암호화 장비에 구축이 가능
- 사용자에게 보안여부에 관한 투명성 보장
- 암호화에 따른 시스템 부하의 최소화
- 암호화 모듈 업그레이드시 합참을 통한 중앙 집중식 업그레이드가 가능하므로 암호화 장비의 관리가 용이
- 보안이 요구되는 시스템 사용자의 인증서/키 등을 내부(통신지원반)에서 관리
- 암호화 기능 및 정보보호 정책까지 적용 가능
- 별도의 운영체제를 탑재한 Embaded-System 이용 가능
- 외부로부터의 사용시스템에 대한 정보 은폐를 통한 시스템의 직접적 해킹 위험성의 최소화

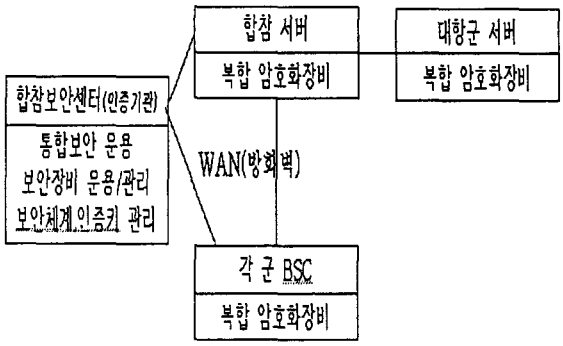


그림 <4-2> 복합 암호화 장비를 사용한 워게임 연습체계

복합 암호화 장비들은 인증센터로부터 각각의 역할기반의 인증서를 부여받고 복합 암호화 장비를 구동하고 있는 시스템들끼리 암호화 통신을 함으로써 기밀성과 인증을 보장할 수 있다.

또한, 외부 망에 있는 사용자이거나 내부망 사용자이거나 모두 역할기반 및 접근통제 기법과 탐지, 보안 운영체제의 통합을 운용함으로써 보다 안전한 네트워크의 구성이 가능하다.

V. 결론

현 워게임 연습체계는 국방전용망(WAN)과 단순 암호화 장비만으로 보안체계를 형성하고 있기 때문에 내.외부의 침입에 대해 극히 미약한 방비 상태에 놓여있다는 것을 알아보았다. 본 연구를 통해 현재의 워게임 연습체계 구성에 큰 변화를 주지 않으면서 효과적인 정보보호체계를 구축하는 방안을 제시하였다.

합참의 보안센터와 각군의 통신지원반을 통한 역할분담 및 인증센터 운영 그리고 각 보안장비를 통합하여 설치/운용의 임무를 부여하고, 각각의 연습 사이트에 복합 암호화 장비를 설치하여 효율적으로 운영한다면 워게임 연습시 중요한

군사자료 및 데이터의 무결성, 비밀성 및 가용성을 보장 해 주리라 확신한다.

참고문헌

[01] 국방대학원 석사학위 논문, □□정보전에 대비한 군 정보통신망 정보보호 대책 연구□□, 1999.12, 김 유 재

[02] 공군작전사령부, "을지포커스렌즈 워게임" 2001

[03] 합동참모본부, "연합 및 합동훈련 규정" 2002

[04] 합동참모본부, "JTLS 장비운용 지침서" 2004

[05] 합동참모본부, "JTLS 공군 지침서" 2004

[06] 정보보호 방식 연구, 연세대학교

[07] 정보보호 총서, 한국 정보보호 센터

[08] S.kumar, □□Classification and Detection of Computer Intrusions□□, Purdue University, Aug., 1995

[09] 역할 속성을 이용한 역할기반 접근통제 메커니즘 한국정보보호학회 김기현 외 5명 1998

이 강 택

1988년 공군사관학교 전산학(이학사)

2002년 포항공과대학교 정보통신학과 (공학석사)

2004년 경기대학교 정보보호기술공학과 박사과정

현재 공군 작전사령부 모의운영과장

이 동 휘

2000년 경기대학교 전자계산학과 (이학사)

2003년 경기대학교 정보보호기술공학과 (공학석사)

2004년 경기대학교 정보보호기술공학과 박사과정

현재 (주)피에스엠코리아 선임연구원

김 귀 남

미국 캔자스대학 수학과(응용수학사)

미국 콜로라도주립대학 통계학과(통계학석사)

미국 콜로라도주립대학 기계산업공학과(기계·산업공학박사)

현재 경기대학교 정보보호기술공학과 주임교수