모델링 및 시뮬레이션 기술의 정보보안 분야에의 활용

김 형 종*

Abstract

최근 정보화 사회의 정착으로 인해 개인의 정보통신 인프라에 대한 의존도가 높아졌고, 정보통신 인프라에 대한 사이버테러의 위협이 증가되었다. 이로 인해 정보통신 기술 영역의 화두로 등장하고 있는 요소 기술 중 하나가 정보보안 기술이다. 해킹기술과 정보보안기술은 창과 방패의 관계를 갖으며, 다양한 해킹기술의 등장과 함께 나날이 새로운 정보보안 기술이 등장하고 있다. 특히, 공격자의 행동 특성에 대한 연구와 네트워크와 시스템의 특성 연구는 이들 중 중요한 연구 주제이다.

본 논문은 이러한 정보보안기술 영역에서 시뮬레이션 기술이 활용되고 있는 영역에 대해서 소개하고자 한다. 특히, 본 영역에서 두각을 나타내고 있는 몇 가지 연구 결과를 소개하여 국내 시뮬레이션 관련 기술 연구자들이 정보보안 분야에 기여할 수 있는 방향을 고려해 고자 한다.

1. 개요

최근 정보통신 인프라에 대한 사회 기반 시설들의 의존도가 증가하고 있다. 이러한 사회 기반 시설들의 올바른 운용을 위해서는 정보통신 인프라의 신뢰성 확보가 선행되어야한다. 정보통신 인프라는 다양한 운영체제의 시스템들과 이들의 연결을 위한 네트워크 장비들로 구성된다. 이렇게 구성된 네트워크는 사회기반 시설 또는 각 개인에게 특정 서비스를 제공하기 위한 응용 프로그램을 탑재하고 있다. 이러한 정보통신 인프라는 외부의 악의적인 공격, 내부적인 오류나 불의의 사고가 있더라도 사회 기반 시설들의 필수적인 서비스들을 지연 없이 제공할 수 있도록 설계 및 구현되어야 한다.

이러한 목표를 달성하기 위해서 국내·외적으로 연구 개발 노력이 이루어지고 있다. 특히, 인가되지 않은 사용자의 네트워크 접근을 제어하기 위한 접근제어시스템, 접근제어를 우회하여 들어온 공격자의 행위적 특성에 근거에 이를 탐지하는 침입탐지시스템, 그리고 침입탐지시스템을 우회한 공격에 대한 네트워크의 침입 감내 기능들이 활발히 연구되고 있다. 또한, 최근에는 이러한 보안 시스템들을 효율적으로 관리하기 위한 전사적인 보안관리 시스템이 개발되고 있다. 특히, 보안 관리와 관련된 연구에 있어서 현재 해당 정보통신기반의 자산(Asset)에 대한 정의와 이를 보호하기 위해 가용한 예산의 수준이 고려되어 적정 수준의 보안 시스템을 구매 및 배치가 이루어져야한다.

시뮬레이션 기술은 현재 수집 가능한 정보에 근거해서 시뮬레이션 모델을 만들고, 이 모델의 실행을 통해 정보를 수집하여 모델링 대상이 되었던 시스템의 특성을 파악하는데 활용 될 수 있다. 이러한 시뮬레이션 기술이 정보보안 분야에 활용되기 시작한 것은 그리 오래된 것이 아니지만, 최근 몇몇 괄목할 만한 연구가 국외에서 진행되고 있다. 특히, 정보보안 영역에서 예측이 어려운 상황을 위한 연구와 보안 관리자들의 교육을 위한 연구개발이 진행되고 있다.

본 논문에서는 시뮬레이션 기술이 이러한 보안 기술 분야에 어떻게 활용되고 있는지에 대해서 살펴보고자 한다. 특히, 국외의 연구 동향을 통해 현재 수행되고 있는 정보보안 분야의 시뮬레이션 기술 연구를 간략히 살펴보고자 한다.

* 한국정보보호진흥원 기술단 선임연구원

또한, 한국정보보호진흥원(KISA)에서 수행하고 있는 "정보통신기반 모델링 및 시뮬레이션" 과제에 대해서 소개하고, 보안 분야 시뮬레이션 기술에 대한 소개를 마무리하고자 한다.

2. 정보보안 분야의 시뮬레이션 활용 예

본 장에서는 국외에서 진행되고 있는 정보보안분야의 모델링 및 시뮬레이션 연구의 각 분야를 간략히 소개하고자한다. 다음은 [1]에서 소개하고 있는 정보보안 영역에서의 시뮬레이션의 형태이다.

가. Canned Attack/Defend : 주로 게임형태의 학습용 시뮬레이션 도구에 해당하는 예이다. 공격과 방어 기법을 사전 정의하고 이를 의사 결정 트리를 사용 시뮬레이션을 수행하도록 하는 것이 일반적이다. 이러한 시스템은 구축하는 데에 오랜 시간과 많은 비용이 들지만, 한번 구축되면 배포가 매우 쉽다는 장점이 있다. 이러한 시뮬레이션의 예로는 InfoChess, CyberProtect, Information Security War gaming System 등이 있다.

나. Sniffer + Network Design Tool : 기존의 네트워크 모델링 시뮬레이션 패키지를 보안 분야에 활용하는 예이다. 이 예에서는 네트워크의 설계와 함께 보안 요소를 같이 고려할 수 있으며 현재는 주로 네트워크의 패킷 흐름에 관련한 보안 취약성의 시뮬레이션이 가능하다. 특히, 최근 Sniffer와 같은 네트워크의 패킷 흐름을 분석하는 도구와 연동하여 시뮬레이션을 수행하는 기술들이 등장하였다.

다. Security Management Simulation : 과제 관리자로 하여금 시스템 구성요소들 사이의 관계를 잘 파악할 수 있도록 하는 데에 활용되는 시뮬레이터로서, 보안 분야의 주 관심대상인 악의적인 공격에 대한 관리 대상 전반에 미치는 영향을 분석하는데 활용된다.

라. Packet War : 공격 대상 네트워크에 대해 실재 공격을 가하는 형태로 수행하는 시뮬레이션으로, 공격자들로 하여금 공격 대상 네트워크에 대한 다양한 공격을 시도하는 것을 허용한다. 이러한 시뮬레이션의 예로는 매년 SANS에서 주관하는 ID'ed Net, DEFCON에서 매년 열리는 해킹 시합과 Toorcon에서 개최하는 Rootwars 등이 있으며, 국내에도 해커스랩의 FHZ(Free Hacking Zone)과 KISA의 정보보호훈련장 등이 있다. 이러한 시스템의 단점은 구축비용이 많이 든다는 것과 새로운 사용자에게 초기 상태의 네트워크 상태를 유지하고 제공해야한다는 점이다.

마. Role Playing : 컴퓨터를 기반으로 한 시뮬레이션을 수행하는 대신, 사람들이 대면한 가운데 시나리오를 수행해보는 형태로 진행된다. 특히, 규모가 큰 국가 차원에서 대비해야하는 공격들에 대해서 각 개인이나 기관의 역할을 시나리오화 하여 이를 수행해 본다. 이러한 형태의 시뮬레이션의 장점은 인적 변수를 다룰 수 있다는 것으로, 정보보안 = 사람 + 프로세스 + 기술의 등식에서 인적 변수에 강조점을 두게 된다. 본 논문에서는 시뮬레이션 소프트웨어로 구성되는 Canned Attack/Defend, Flexible Network Design, 그리고 Security Management Simulation에 대해서 자세히 살펴보겠다.

3. Canned Attack/Defend Scenario

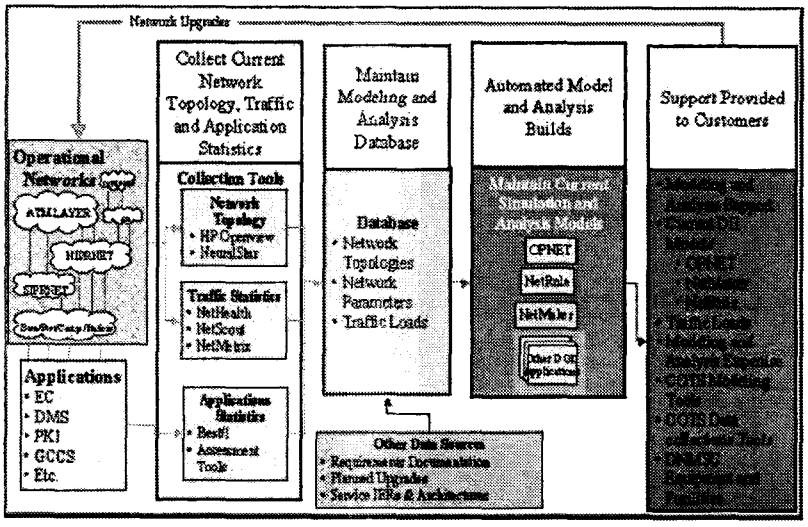
주로 IT 분야 종사자들의 보안 교육에 활용되는 시뮬레이션 도구에로 멀티미디어 형태로 제작된다. 이러한 도구의 제작을 위해서는 많은 인력의 투입이 요구되며, 공격 경로가 일반적으로 고정되어 있는 것이 특징이다. 또한, 생성되는 공격이나 방어 시나리오가 고정되어 있으며, 난수성을 고려하더라도 한정된 시나리오에서 선택 시에 고려하는 정도이다. 또한, 교육 도구이기 때문에 교육 대상자로 하여금 의사결정 트리를 지나면서 의사결정을 하도록 하고 이의 결과를 제시하는 형태로 이루어진다. 이러한 형태의 시뮬레이션 도구로는 InfoChess, CyberProtect,

F. Cohen의 원인결과 모델, Information Security War gaming System이 있다.

InfoChess[3]는 군사 정보 운영(Military Information Operation)에 초점을 맞춘 보드 게임이며, 이에 특화된 규칙들을 체스 게임에 삽입하여 정보운영에 관련된 특성을 학습 할 수 있게 하였다. 정보 운영이라 함은 "자신의 정보와 정보시스템을 보호하면서, 적의 정보와 정보 시스템에 영향을 미치는 행위들"을 말한다[2]. InfoChess는 미군의 정보전 그룹들에 의해서 많이 활용되고 있다.

CyberProtect는 미 국방성 산하의 DISA (Defense Information Systems Agency)에 의해 개발된 교육용도구이다. 주로 LAN에서의 보안 시스템의 역할을 학습할 수 있도록 해준다. 시뮬레이션 수행은 고정된 LAN에 다양한 보안 시스템을 배치함으로써, 외부의 공격에 대한 네트워크의 보안성을 평가받게 된다. 보안 시스템의 배치를 위해서 CyberProtect에서는 4번의 배치 기회를 주며, 각각 40, 20, 20, 20 포인트의 구매를 위한 자원을 할당해 준다. 시뮬레이션 수행자는 주어진 자원을 활용하여, 보안 시스템을 구매 및 배치하고 외부의 공격을 받게 된다. 4번째 배치 기회까지 90점을 넘게 되면 테스트를 통과한 것으로 본다.

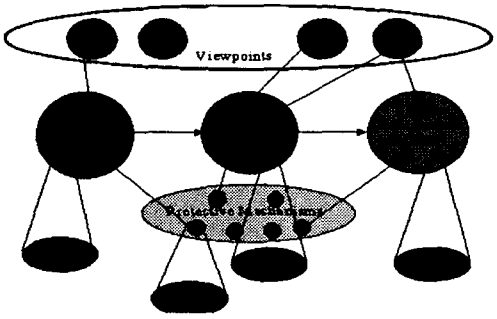
F. Cohen [4]의 사이버 공격, 방어 모델링에서는 원인-영향 고리(cause-effect chain)의 집합을 생성하여 공격과 방어의 절차를 시뮬레이션 하고자 하였다. 시뮬레이션 수행을 위해 위협, 공격 그리고 방어 정보를 수집하고 이들을 상호 참조 관계로 연결하여 큰 정보베이스를 구축하였다. 이러한 정보베이스는 원인-영향 고리의 집합을 형성하고, 이러한 정보에 시간의 개념을 집어넣어 시뮬레이션을 수행하도록 하였다. Cohen의 연구에서 원인-효과 모델은 정보보호 영역에서 일어날 수 있는 모든 사건에 대한 연관 관계를 원인과 효과의 관계로 모델링 한 결과물로써 일종의 취약성 데이터베이스와 같은 역할을 하는 정보 집합이다. 원인-효과 모델은 시뮬레이션의 모든 이벤트의 근본이 되는 정보를 가지고 있다. Cohen이 지적한 정보보호 영역에서의 모델링 및 시뮬레이션이 어려운 큰 이유 중 하나인 신뢰성 있는 정보의 부족의 문제를 Cohen은 이 모델을 통해서 해결하고자 하였다. 이 모델의 구성을 살펴보면 37개의 위협(threat) 클래스, 94개의 공격 메커니즘 클래스 그리고 140개의 방어 메커니즘 클래스가 존재한다. 여기서 위협은 공격과 상호 연결성을 가지고 있으며 공격은 방어와 상호 연결성을 가지고 있다. [그림 1]은 원인 결과 모델을 도식화 한 그림이다.



[그림 1] DISA의 네트워크 모델링 및 시뮬레이션 방법론

4. Sniffer + Network Design Tool

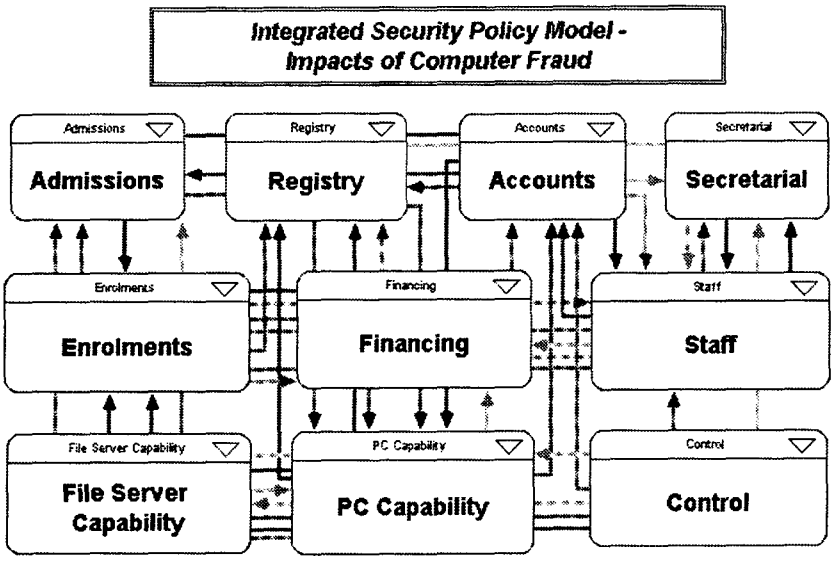
전문적인 시스템 관리자나 응용 프로그램 개발자들은 네트워크의 구조나 사용 프로토콜에 따른 특성을 분석하기 위한 모델을 요구해 왔다. 이러한 요구의 산물이 기존의 네트워크 시뮬레이션 도구들이다. 이러한 네트워크 시뮬레이션 도구들 보안 분야에 활용하기 위한 노력들이 있다. 특히, 네트워크의 패킷 흐름을 분석하기 위한 Sniffer와 같은 도구를 사용하여 수집된 정보를 네트워크 시뮬레이션 도구의 실행 정보로 활용할 때 네트워크가 가지고 있는 네트워크 프로토콜 상의 취약점을 예측할 수 있다. 특히, 이러한 도구들이 광범위한 네트워크의 모델링 및 시뮬레이션이 가능하게 해주기 때문에 이를 잘 활용할 경우 많은 성과를 가져올 수 있다. DISA에서는 [그림 2]와 같은 네트워크 모델링 및 시뮬레이션 절차를 제시하였다. 그림의 첫 절차는 작동중인 네트워크에서 네트워크 토폴로지와 네트워크의 트래픽 및 응용 프로그램의 통계를 수집하는 작업이다. 이러한 작업을 통해서 나온 정보들은 두 번째 절차인 모델링 및 분석을 위한 자료로 사용된다. 또한, 이 자료는 자동화된 모델 구현과 분석을 수행하는 데에 활용된다. 모델 구현과 분석 수행결과는 결국 최종 사용자에게 네트워크 관리에 관련한 다양한 정보를 제공해주고, 이것은 현재 운영중인 네트워크를 보완하는 데에 기초자료로 활용된다. 이러한 기술은 주로 이상 네트워크 트래픽에 의한 공격인 서비스 거부공격의 시뮬레이션에 활용될 수 있다.



[그림 3] Fred Cohen의 원인 결과 모델

5. Security Management Simulation

보안 관리 영역에 시뮬레이션 기술을 활용한 예를 보여준다. [그림 3]은 통합 보안 정책 모델의 예를 보여주고 있다. 이러한 시뮬레이션에서는 과제 관리자나 프로그램 진행자가 외부의 악의적인 공격이 시스템의 각 구성요소 및 시스템



[그림 2] 통합 보안 관리 시뮬레이터

전체에 미치는 영향을 분석 할 수 있도록 해준다. 시스템의 구성요소로는 사람, 장비, 자본 등으로, 분석 가능한 모든 사항을 최대한 고려하는 것을 목적으로 한다. 이렇게 다양한 구성요소들을 하나의 모델에 통합하는 것을 통해서 악의적인 공격의 직접 혹은 간접적인 영향을 분석할 수 있게 된다. 이러한 분석은 보안 분야의 문제가 시스템 혹은 전체 환경에 미치는 영향을 분석하게 함으로써 보안 관리자뿐 아니라 아닌 최종 의사결정권자들에게 보안 요소를 어떻게 봐야할 것인가에 대한 전반적인 관점을 갖게 한다는 장점이 있다.

예를 들어, 특정 회사의 서버 시스템이 기능이 외부 공격에 의해 정지한 경우 이로 인해 서버 시스템의 특정 데이터가 손실될 수 있으며, 이것은 고객의 신뢰를 잃게 만드는 원인이 되어 회사의 고객이 줄어들고, 이것은 회사의 직원을 줄여야하는 결과를 초래하고, 회사가 문을 닫는 결과를 낳을 수도 있다. 이러한 시뮬레이션 모델에서 시도할 수 있는 것은 정보기술예산 중 보안에 사용할 예산의 비율을 다르게 해서 시뮬레이션을 수행하는 것이다. 이러한 과정을 통해서 회사가 투입할 수 있는 적정 수준의 정보보안 예산을 산정 하는 데에 필요한 데이터를 얻을 수 있다. 이러한 시뮬레이션 도구는 위험 분석 및 관리에 활용되게 된다.

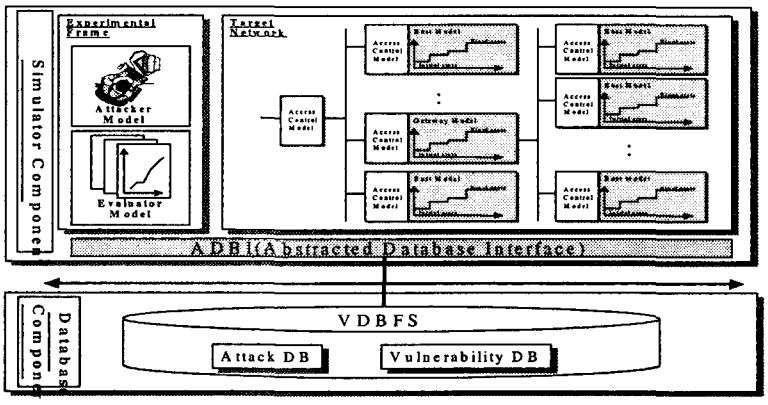
최근에 카네기 멜론 대학의 소프트웨어 공학연구소(CMU/SEI)에서는 EASEL(Emergent Algorithm Simulation Environment Language)을 개발하였다[5].

EASEL은 emergent 알고리즘 기반의 범용성 있는 시뮬레이션 언어로써 불확실하게 보이는 영역의 행위적 특성을 예측하기 위한 목적으로 만들어 졌다. EASEL의 연구에서는 특히 unbounded system-인터넷, 전력분야, 전화 시스템, 생물학 시스템, 증권 시장, 소프트웨어 구성-의 특성을 파악하기 위해 emergent algorithm을 소개하고 이를 통한 정보보안 영역의 모델링 가능성을 제시하였다. 이 밖에 CMU/SEI에서는 공격자 모델링에 대한 방법론[6]을 개발하였으며, 공격에 대한 필수 서비스의 생존성(Survivability)을 평가하기 위한 시뮬레이션 기술을 연구하고 있다[7].

6. KISA의 정보통신기반 모델링 및 시뮬레이션

한국정보보호진흥원(KISA)에서는 정보보안 분야에 시뮬레이션 기술을 도입하기 위한 목적으로 2000년부터 "정보통신기반 모델링 및 시뮬레이션" 과제를 수행해 왔다. 특히, 2001년부터는 정보통신기반의 보안 취약성 진단을 위한 시뮬레이션 도구개발을 위해 연구를 수행하고 있으며, 이를 위한 국외 기술동향 분석 및 과제 연구를 수행 중 이다. 또한, DEVS(Discrete EVent System Specification) 방법론 [9] 을 보안 분야에 적용하기 위한 노력을 진행중이다.

[그림 4]는 KISA에서 개발 중인 취약성 진단



[그림 4] 취약성 평가를 위한 통합 시뮬레이션 환경

시뮬레이션 시스템의 구조도 이다. [그림 4]의 통합 시뮬레이션 환경은 시뮬레이션 컴포넌트와 데이터베이스 컴포넌트로 구성된다. 시뮬레이션 컴포넌트는 취약성 평가 환경에 해당하는 실험 프레임(Experimental Frame), 평가 대상이 되는 네트워크(Target Network)와 데이터베이스 컴포넌트와 인터페이스를 위한 추상 데이터베이스 인터페이스(ADBI : Abstracted Database Interface)로 구성된다. 데이터베이스 컴포넌트는 시뮬레이션을 위한 기반 데이터를 제공해 주기 위한 자료의 저장 장소로 VDBFS(Vulnerability Database For Simulator)라는 시뮬레이터를 위한 취약성 데이터베이스가 존재한다. VDBFS는 대상 네트워크의 취약성 정보를 제공해주는 취약성 DB(Vulnerability DB)와 공격자 모델(Attacker Model)에 공격정보를 제공해 주기 위한 공격 DB(Attack DB)로 구성된다. 이러한 시뮬레이션 시스템의 구성을 위해서 본 연구에서는 다음과 같은 연구가 진행되었다.

가. 취약성 분석 및 시뮬레이션을 위한 취약성 정보 데이터베이스 구축 : 현존하는 다양한 취약성 분석 기법을 조사 및 정리하고 이를 시뮬레이션에 사용하기에 적절한 데이터형태로 구축하기 위한 절차 정립 및 형태적, 의미적 대표성을 갖는 자료의 수집.

나. 평가 대상 네트워크의 취약성 기반의 모델 구축 : 평가 대상 네트워크의 플랫폼, 운영체제, 제공 서비스에 따른 취약점의 모델링 방법론 정립.

다. 실험 프레임웍(Experimental Frame) 설계 및 구현 : 평가 대상 네트워크 모델의 취약성 진단을 위한 공격자 모델과 대상 네트워크의 반응을 취합하고 분석하기 위한 평가 모델 설계 및 구현.

라. 보안 정책 표현을 위한 접근제어 모델링 : 실험 프레임웍의 생성 공격에 대한 접근제어 규칙의 지식 기반 시뮬레이션 방법론 기반의 접근제어 모델링.

7. 결 론

본 논문은 정보보안 분야에 국외의 시뮬레이션 기술을 활용 예를 살펴보고, 국내의 연구로서 KISA의 "정보통신기반 모델링 및 시뮬레이션" 기술 개발을 소개하였다. 정보보안 분야의 파악이 어려운 다양한 상황들을 시뮬레이션을 통해 파악하고자 하는 노력과 이를 교육 도구로 활용하는 노력은 설명된 바와 같이 다각도로 진행되고 있다. 실제 보안 전문가들이 피부로 느끼는 어려움도 대상 네트워크에 대한 전체적인 관점을 갖기가 어렵고, 이로 인해 전사적 보안 대책의 마련이 어렵다는 것이다. 이러한 문제에 대한 답을 제시해 줄 수 있는 기술이 모델링 및 시뮬레이션 기술이다. 필수 서비스를 지속적으로 제공해야하는 정보통신기반 네트워크의 경우 모델이 구축되어 지속적인 관리를 통해 가장 적절한 보안 정책의 표현 및 자원의 관리가 요구된다. 또한, 지속적인 보안 전문가들과의 의견교환을 통해 요구사항을 지속적으로 얻어내고 필요한 기술을 제안하는 것이 필요하다. 국내의 현실이 아직 시뮬레이션에 예산을 투자하는 것에 대해 부담을 갖거나, 시뮬레이션보다는 실제 환경에서의 작업을 선호하는 경향이 있다. 아직 시뮬레이션 마인드가 부족한 국내의 현실을 뛰어 넘기 위해 시뮬레이션 기술 연구자들의 지속적인 해당 분야의 요구분석과 연구 제안이 요구된다.

참고문헌

1) John H. Saunders, *"The Case for Modeling and Simulation of Information Security"*, Computer Security Institute's 28th Annual Conference, October. 2001.

2) Waag, Gary L. et al. *"Modeling and Simulation for Information Assurance : State-of-the-Art-Report", IATAC, Defense Technical Information Center, Ft Belvoir,*

VA, 2001.

3) InfoChess Home Page, Aegis Research Coo peration. 2001, http://www.aegisresearch.co m/info_chess1.htm
4) F. Cohen, *"Simulating Cyber Attacks, Defences, and Consequences"*, Computer & Security, Vol.18, pp. 479-518, 1999
5) D. Fisher, "Design and Implementation of EASEL-A Language for Simulating Highly Distributed Systems," Proceedings of MacHack 14, the 14th Annual Conference for Leading Edge Developers. Deerborn, MI, June 24-26, 1999
6) A. P. Moore, R. J. Ellison and R. C. Linger, *"Attack Modeling for Information Security and Survivability"*, Technical Report No. CMU/SEI-2001-TR-001, Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, March, 2001.
7) S. D. Moitra and S. L. Konda, *"A Simulation Model for Managing Survivability of Networked Information System"*, Technical Report No. CMU/SEI-2000-TR-020, Pittsburgh, PA:Software Engineering Institute, Carnegie Mellon University, December, 2000.
8) Nong Ye, Joseph Giordano, *"CACA - A Process Control Approach to Cyber Attack Detection"*, Communications of the ACM
9) B. Zeigler, H. Praehofer and T. Kim, "The Theory of Modeling and Simulation - Second Edition," Academic Press, 2000