생존성 평가를 위한 취약성 모델링 방법 연구

김형종*

A Study of Vulnerability Modeling Method for Survivability Analysis

Kim, Hyung Jong

Abstract

2003년 1월 25일의 인터넷 침해사고는 정보통신망의 중요성을 실감하게 해준 사건이다. 이 사건의 원인을 여러 가지로 말할 수 있지만, 가장 근본적인 원인은 소프트웨어의 취약점에 대한 관리가 부재한 것이었다. 소프트웨어가 특정 취약점을 갖게되는 데에는 다양한 원인이 존재하며 이에 대한 연구는 폭넓게 진행되어 왔다. 본 논문은 이러한 연구들을 기반으로 취약성을 모델링하는 방법에 대해서 다루고자 한다. 특히, 단위 취약점 개념을 사용한 취약성의 시스템적인 분석 방법을 설명하고, 이러한 개념이 생존성 평가에 어떻게 활용될 수 있는지를 다루고자 한다. 본 논문의 연구 결과는 기존의 취약성 분석 기법을 좀더 정형화 해주는 역할을 할 뿐만 아니라, 정보보호 영역에 시뮬레이션 기술을 어떻게 활용할 수 있는지에 대한 하나의 방법으로 활용될 수 있다.

Key Words: 네트워크 생존성 평가, 취약성 분석, 모델링 및 시뮬레이션

1. 서론

모델링 및 시뮬레이션은 미래의 예측하기 힘든 상황을 예측하거나 현재의 이해하기 어려운 복잡도가 높은 시스템을 이해하는 도구로 이미 널리 사용되는 도구라고 할 수 있다. 컴퓨터 네트워크의 정보보호에 있어서도, 모델링 및 시뮬레이션 기술을 활용할 경우 이익을 얻을 수 있는 많은 요소들이 있다. 이는 현재의 컴퓨터 네트워크의 구조 및 사용 프로토콜의 복잡도가 높아지고, 이로 인해 가까운 미래를 예측하는 것이 어려워질 뿐 아니라, 현재의 상태조차도 이해하기 어려워지는 현실 때문에 더욱 그러하다. 지난 2003년의 1.25 인터넷 침해사고에서 네트워크의 마비현상의 원인을 규명

* 한국정보보호진흥원, 기반시설보호단

하는 데에 많은 시간이 사용된 것은, 네트워크의 구조 및 프로토콜의 복잡도로 인한 이해의 부족이 어떠한지를 잘 보여준 예라고 할 수 있다.

생존성이라는 개념은 컴퓨터 네트워크가 외부의 공격이나 내부적인 오류 혹은 불의의 사고가 있더라도 자신이 제공해야하는 필수적인 기능을 끊김 없이 제공할 수 있는 성질을 말한다. 이러한 생존성의 개념은 기존의 보안성의 개념보다 많은 시스템의 속성들이 고려되는 개념으로서 주요정보통신기반시설이 꼭 가져야만 하는 특성으로 사용되는 개념이다. 생존성의 확보를 위해서 반드시 고려되어야하는 3가지 요소가 있는데 이는 첫째, 외부의 악의적 공격 및 불의의 사고, 둘째, 네트워크가 가지고 있는 취약점 그리고 셋째, 네트워크에 적용되는 정보보호 기술이다. 이 3가지 요소가 어떤 조합으로 되어 있느냐에 따라서 네트워크의 생존능력은 달라지게 된다.

이러한 생존성을 평가하기 위한 가장 직접적인 방법은 네트워크에 직접적인 공격을 실행하여 이의 생존 능력을 평가하는 방법이 있다. 그러나, 이러한 방법을 사용할 경우 네트워크에 심각한 문제를 일으켜서, 네트워크가 필수적으로 제공해야하는 서비스를 제공하지 못하는 현상이 발생할 가능성이 있다. 또한, 평가대상이 되는 네트워크가 현재 존재하지 않고 가까운 미래에 구축 되어야하는 경우에는 이를 평가할 수 있는 방법이 없다. 상기한 평가의 위험성 또는 부재로 인한 평가의 불가능을 해결할 수 있는 가장 현실적인 방법이 바로 모델링 및 시뮬레이션이다.

본 논문은 네트워크의 생존성을 평가하기 위한 기술적인 접근 중 하나로 시뮬레이션을 활용하여 평가하는 방법에 대한 연구의 일부를 담고 있다. 특히, 본 논문의 초점은 네트워크가 가지고 있는 특성 중 생존성 평가의 직접적인 원인 제공이 되는 취약점의 모델링 방법에 있다. 본 논문의 구성은 제 2장에서 본 연구의 배경이 되는 몇 가지 기존 연구를 살펴보고, 제 3장에서 생존성평가 시뮬레이션시스템의 구조 및 환경을 제시하고, 제 4장에서는 취약성 모델링 방법을 제시한다. 마지막으로, 제 5장을 통해 본 논문의 결론을 제시한다.

2. 배경 지식

2.1 DEVS 형식론

DEVS(Discrete Event System Specification) 형식론은 계층적이고 모듈화된 이산 사건 모델을 위해 정의된 이론이다[5]. 일반적으로 시스템은 시간의 흐름에 따라 입력, 상태, 출력, 상태 전이 함수들을 갖는다. DEVS 형식론은 시스템이 일반적으로 갖는 특성들을 정의하여 시스템을 모델링 할 수 있는 기반을 제공하였다. DEVS 형식론에서는 두 가지 종류의 모델을 정의하였다. 하나는 basic 모델이고, 다른 하나는 coupled 모델이다.

Basic 모델의 구성은 다음과 같다.

$M = < X, S, Y, \delta_{int}, \delta_{ext}, \lambda, ta >$

단,

X : 입력 사건의 집합.

S : 순차적 상태의 집합.

Y : 출력 사건의 집합.

$\delta_{int} : S \rightarrow S$: 내부 전이 함수

$\delta_{ext} : Q \times X \rightarrow S$: 외부 전이 함수

$\lambda : S \rightarrow Y$: 출력 함수

$ta : S \rightarrow R^{+}_{0} \rightarrow \infty$: 시간 진행 함수

단, $Q = \{(s,e) \mid s \in S, 0 \le e \le ta(s)\}$

e : 최근의 상태 전이 이후로 흐른 시간.

Coupled 모델의 구성은 다음과 같다.

$DN = < D, \{M_i\}, \{I_i\}, \{Z_{i,j}\}, select >$

단,

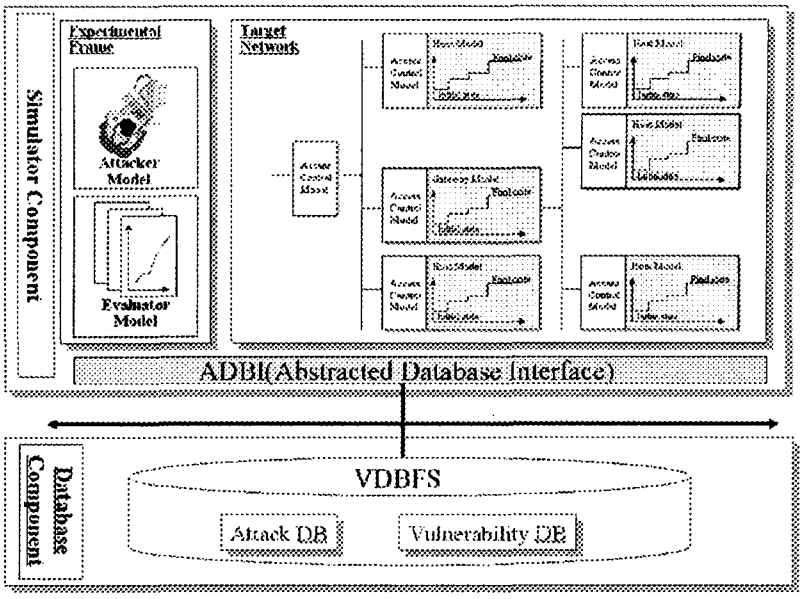
D : coupled 모델의 구성요소 모델 i에 대한 이름의 집합.

M_i : 구성요소가 되는 basic 모델.

I_i : 모델 i의 영향을 받는 모델들의 집합.

$Z_{i,j}$: I_i의 원소 각 j에 대해서 i에서 j로의 출력 번역 함수.

Select : 타이 브레이킹 함수.



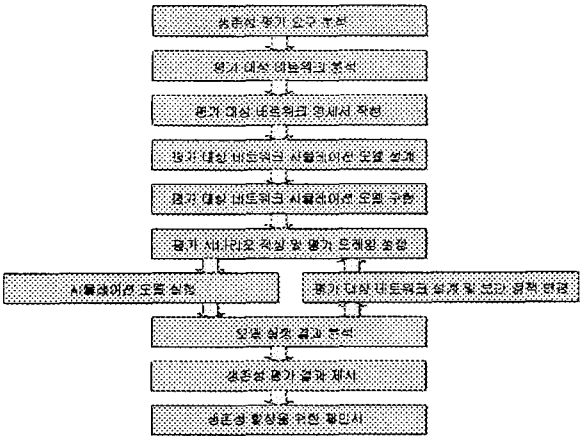
[그림 1] 생존성 평가를 위한 시뮬레이션 환경

2.2 정보보호 분야의 시뮬레이션 연구

정보보호 분야의 시뮬레이션 기술연구에 대해서는 [1]에 정리되어 있다. 그중 본 연구와 직접적인 연관이 있는 연구로는 F. Cohen[2] 연구와 미국 CERT의 생존성분석 연구[3]가 있다. F. Cohen은 사이버 공격 및 방어 사이의 관계를 원인-영향 고리(cause-effect chain)의 집합을 통해 표현하고, 공격과 방어의 절차를 시뮬레이션 하고자 하였다. 시뮬레이션 수행을 위해 위협, 공격 그리고 방어 정보를 수집하고 이들을 상호 참조 관계로 연결하여 큰 정보베이스를 구축하였다. 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 추상화 수준이 높은 이 모델을 통해서 해결하고자 하였다. 미국 CERT의 생존성 분석 연구에서는 SNA(Survivable Network Analysis)라는 분석방법을 제안하고 있다. SNA에서는 네트워크가 가지고 있는 공격 경로의 분석과 네트워크의 필수 서비스 제공경로를 분석하여, 이 두 경로 중 겹쳐지는 부분을 찾고 이를 취약지점(Soft Spot)이라고 명명하였다. 그리고, 취약지점에 대한 정보보호 대책을 제시하는 것을 생존성 분석의 결과물로 제시하고 있다.

3. 생존성 분석 환경 구조

[그림 1]은 생존성평가 시뮬레이션 시스템의 구조도 이다. 시뮬레이션 환경은 시뮬레이션 컴포넌트와 데이터베이스 컴포넌트로 구성된다. 시뮬레이션 컴포넌트는 생존성 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 시뮬레이션



[그림 2] 생존성 평가 절차

을 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.

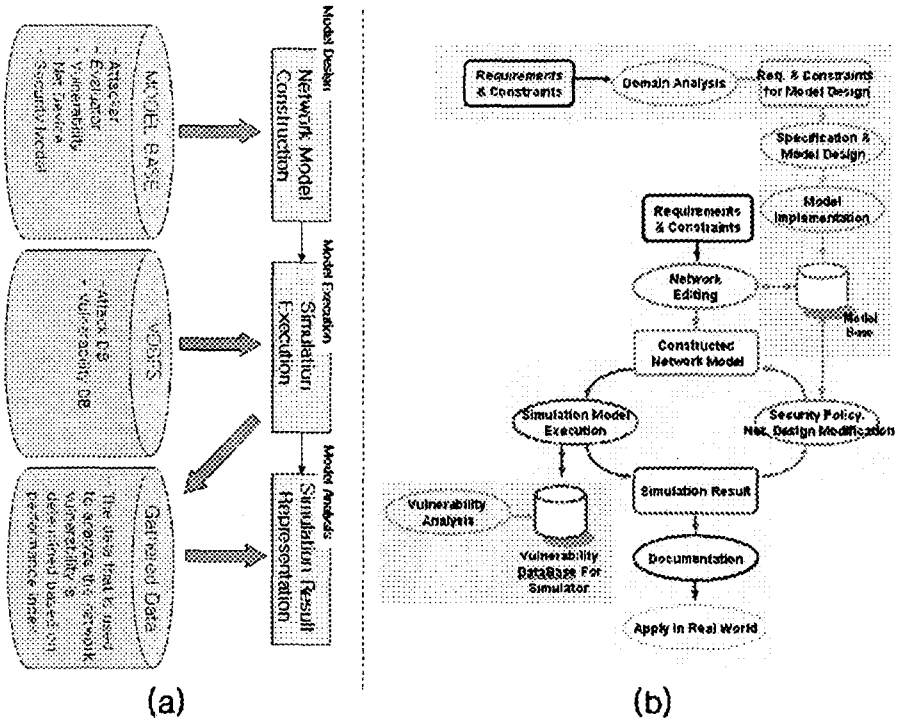
생존성 평가 지표와 그것을 얻어내기 위한 평가 절차의 연구는 현존하는 네트워크, 시스템, 서비스의 정상적인 운용을 위한 다양한 방어 메커니즘의 적용 예와 이의 신뢰성 있는 평가의 수행을 위한 절차를 마련한다. 생존성 평가절차(그림 4)은 다음과 같다.

- 생존성 평가 요구 분석 : 네트워크 관리자나 보안 담당자로부터 해당 네트워크의 주요 평가 대상 시스템 및 서비스에 대한 정보를 수집하고, 해당 시스템들에 대해서 이슈가 되는 평가 요소를 얻어내는 일을 수행
- 평가대상 네트워크 분석 : 생존성 평가 대상이 되는 네트워크의 토폴로지, 네트워크 대역폭, 주요 제공 서비스, 구성 호스트 정보 등을 수집
- 평가대상 네트워크 명세서 작성 : 수집과 분석의 결과를 평가대상 네트워크의 명세서 형태로 도출
- 평가 대상 네트워크 시뮬레이션 모델 설계 : 작성된 명세서에 작성된 네트워크가 갖는 특성 정보들을 근거로 해서 네트워크 시뮬레이션 모델 설계
- 평가 대상 네트워크 시뮬레이션 모델 구현 : 모델 설계 결과물을 활용하여 생존성 평가를 위한 모델을 구현하고 구현된 모델은 생존성 평가 요구분석에 근거한 생존성 평가 대상 네트워크 모델 구현물임
- 평가 시나리오작성 및 평가 프레임 설정 : 추출하기를 원하는 평가 지표를 찾아내기 위한 시나리오를 작성하고, 시나리오는 구체적인 설정 값으로 변환되어 평가 프레임의 입력정보로 활용됨
- 시뮬레이션 모델 실행 : 평가대상 네트워크 모델에 입력을 제공하고 그 반응을 수집함. 이러한 평가 프레임과 대상 네트워크사이의 연동은 시뮬레이션 모델이 실행된 후 시뮬레이션 관측 시간동안 지속적으로 이루어짐
- 모델 실행 결과 분석 : 실행 결과는 평가 프레임 내부의 분석모델에 의해서 분석되고 그 결과가 다양한 방법으로 제시됨
- 평가대상 네트워크 설계 및 보안정책 변경 : 제시된 결과를 바탕으로 평가대상 네트워크 모델의 디자인 변경 및 새로운 보안 정책의 적용에 활용
- 생존성 평가 결과 제시 및 제안서 : 시뮬레이션 결과는 실 시스템의 설계 변화나 보안 설정 변경에 활용되어지도록 생존성 향상 제안서(Suggestion for Enhancing Survivability)를 제시하도록 함

4. 취약성모델링 방법 연구

4.1 생존성 평가에서의 취약성 모델링

[그림 3]은 시뮬레이션의 전반적인 프로세스를 보여주고 있다. (a)는 시뮬레이션의 일반적인 프로세스인 모델 디자인, 모델 실행, 결과 분석의 3단계를 보여주고 있다. 모델 디자인의



[그림 3] 시뮬레이션 프로세스

경우 본 연구에서의 내용은 네트워크 모델을 편집하는 것으로서, 네트워크를 구성하는 구성요소들을 그래픽 사용자 인터페이스를 통해 편집하고, 각 구성요소들의 설정 값을 입력하는 과정을 말한다. 모델의 실행에 있어서 참조되는 정보는 네트워크 모델에 입력되는 공격정보들과 해당 공격에 대한 반응을 위한 정보에 해당하는 취약점 정보가 필요하다. 이러한 정보들은 모두 VDBFS에 저장되어 있으며, 시뮬레이션의 실행 중에 해당 정보들이 참조되어 모델의 동적 특성이 나타나게된다. 모델이 실행중에 생성되는 정보는 곧 시뮬레이션 결과로 저장되며, 저장된 값은 시뮬레이션 결과를 사용자가 원하는 형태로 표현하게된다.

[그림 3]의 (b)는 (a)의 경우를 다른 관점으로 표현한 것으로 중앙의 십자 모양의 프로세스가 네트워크 모델편집, 모델실행, 결과 분석에 해당하는 것이고 그 나머지 부분은 해당 프로세스를 수행할 수 있도록 하는 준비 단계에 해당하는 프로세스들이다. 첫째는, 모델베이스를 구축하는 과정이라고 할 수 있고, 둘째는 VDBFS를 구축하는 과정이라고 할 수 있다. 모델베이스를 만드는 과정에서는 일반적인 요구사항 및 제약조건(Requirements and Constraints)에 근거해 문제 영역을 분석(Domain Analysis)하고, 모델디자인을 위한 요구사항과 제약조건에 근거해서 모델 디자인을 수행한다. 모델디자인이 완료되면 이에 근거해서 모델을 구현하고, 구현된 모델은 모델베이스에 저장된다. 앞에서 언급한 바와 같이 시뮬레이션 모델의 실행을 위해서는 실행 지식에 해당하는 VDBFS 정보가 존재해야한다.

이러한 정보를 얻기 위해서 본 연구에서는 AV-CV(Atomic Vulnerability and Compound Vulnerability) 기반의 취약성 분석을 수행하고, 이 결과로 VDBFS를 구축하였다.

4.2 취약성 모델링 방법

AV-CV 기반의 취약성 분석에 있어서 DEVS 형식론을 기반으로 CV 및 AV를 정의하였다.

CV는 다음과 같이 정의되며,

CV = {Icv, Qcv, cv, WSX, VX}

단,

Icv = {Icv1, Icv2, ·, Icvn}

Qcv= {Normal, Intermediate, Warning, Consequence}

cv : Icv × Qcv → Qcv

WSX : warning state vulnerability expression

VX : vulnerability expression

AV는 다음과 같이 정의된다.

AV = {Iav, Qav, av, Type, Category}

단,

Iav = {Iav1, Iav2, ·, Iavn}

Qav = Q(initial state) ú Q(final state)

av : Iav × Q(initial state) → Q(final state)

Type : {Fact, NonProb, Prob}

Category : {Generic, Application-Specific, System-Specific}

이러한 AV-CV의 정의를 기반으로 취약점 정보가 분석되고, 이렇게 분석된 정보는 VDBFS에 저장되어 시뮬레이션 실행 시간에 외부 공격정보를 기반으로 시스템의 상태전이를 일으키게된다.

5. 결론

본 논문은 생존성 평가를 위한 취약점의 모델링 방법에 대해 설명하고 있다. 특히, AV-CV기반으로 취약성 분석을 수행하고 이러한 취약점 정보의 데이터베이스를 통해서 외부의 공격에 대해서 적절히 반응하고 상태변화를 일으키는 모델의 설계를 다루고 있다. 본 연구의 결과물은 Modsim III와 Oracle DBMS를 통해서 구축되었고 현재 약 300여 개의 대표적 취약점을 분석 및 저장하였다. 향후, 본 연구를 통해서 고려된 내용들은 생존성 평가 지표 및 평가 방법론에 활용되어 네트워크의 생존성의 평가에 사용될 것이다.

참고문헌

[1] 김형종, "모델링 및 시뮬레이션기술의 정보보호 분야에의 활용" 2002 한국시뮬레이션학회 춘계 학술대회,2002년 5월

[2] F. Cohen, "Simulating Cyber Attacks, Defences, and Consequences," Computer & Security, Vol.18, pp. 479-518, 1999

[3] Nancy R.Mead et. al., "Survivable Network Analysis Method", CMU/SEI-2000-TR-013, Sep. 2000

[4] M. Bishop, "Vulnerabilities Analysis", Proceedings of the Recent Advances in Intrusion Detection, September, pp. 125-136, 1999.

[5] B. P. Zeigler, H. Praehofer and T. Kim, "Theory of Modeling and Simulation, Second Edition", Academic Press, 2000