Journal of the Research Institute of Industrial Technology, Vol. 24, 2007

필수 서비스와 취약성을 이용한 생존성 분석 방법

이장세*

*한국해양대학교 IT공학부 조교수

Survivability Analysis Method Using Essential Service and Vulnerability

*J. S. Lee**

**Division of Information Technology Engineering, Korea Maritime University, Busan 606-791, Korea*

요 약 : 본 논문은 필수 서비스와 취약성을 이용하여 네트워크의 생존성을 정량적으로 분석하는 방법의 제안을 목적으로 한다. 생존성이란 외부의 공격 또는 사고 등에도 불구하고 자신이 제공해야 하는 필수적인 서비스를 지속적으로 제공할 수 있는 능력을 의미한다. 이와 같은 생존성 평가를 위하여 시뮬레이션 기반의 취약성 분석을 토대로 취약성 값을 구하고, 취약성과 서비스와의 관계를 이용하여 생존성을 분석할 수 있는 수식을 도출하여 적용한다. 이를 통하여 분석하고자 하는 노드 및 네트워크에 대한 생존성을 정량적으로 분석할 수 있다. 사례연구를 통하여 제안된 방법의 타당성을 검토한다.

핵심용어 : 생존성분석, 필수서비스, 취약성, 네트워크보안, 컴퓨터보안

ABSTRACT : *The objective of this paper is to propose a survivability analysis method using essential service and vulnerability. Survivability means an ability to provide essential services continuously in the presence of attacks or accidents . To do this, we propose an equation to analyse the survivability on a target network using the relation with vulnerabilities and services. To calculate vulnerability value used in the equation, we use the simulation based vulnerability analysis. The proposed method is able to analyze the survivability on target nodes and network quantitatively. Case study shows a validity of proposed method.*

KEY WORDS : survivability analysis, essential service, vulnerability, network security, computer security

* jslee@hhu.ac.kr

1. 서 론

최근의 세계적인 정보화와 인터넷의 확산을 통하여 조직 및 개인의 컴퓨팅 환경이 변화되고 있으며 이에 따라 정보통신 환경의 의존도가 급증하고 있다. 따라서 이와같은 환경하에서의 정보통신 기반구조에 대한 침해는 조직 및 개인은 물론 국가적, 경제적, 사회적으로 막대한 피해를 야기한다[1]. 이에 컴퓨터 및 네트워크 보안 분야에 있어서 시스템 자체의 버그, 부적절한 구성 설정, 개방형 인터넷 기반구조 등에 따른 취약성등을 탐지하고 분석하여 제거하려는 다양한 연구가 수행되고 있다. 특히, 최근에는 공격, 사고, 고장 등으로부터 컴퓨터 및 네트워크에 대한 지속적인 서비스 즉 필수 서비스를 보장할 수 있는 능력인 생존성 분석에 대한 연구의 필요성이 대두되고 있다[2]. 그러나 Aslam[3], Landwehr[4], Cohen[5] 등에 의한 기존의 취약성의 분석에 대한 연구는 취약성과 관련된 서비스와의 상관성을 분석하기 위하여 필수적인 반면, 생존성을 정량적으로 분석하기 위하여 취약성과 서비스와의 정량적인 관계를 표현하기에는 미흡하며, 시뮬레이션에 적용하기에 적합하지 못하다. 따라서 본 논문에서는 [6]에서 제안한 시뮬레이션 기반의 취약성 분석 방법론을 토대로 취약성을 분석하고 취약성과 관련된 필수 서비스를 정의하여 수식화함으로써 정량적인 생존성을 평가할 수 있는 방법을 제안한다. 사례연구를 통하여 제안한 방법의 타당성을 검토한다.

2. 관련연구

2.1 국내외 연구동향

생존성 분석에 대한 국내의 연구는 아직 많은 연구결과가 보고 되어 있지는 않으나, 한국정보보호진흥연구원, 국가보안기술연구소등에서 활발히 연구가 진행되고 있다. 특히, 한국정보보호진흥원에서는 기존의 침입예방기술, 탐지기술로는 대응할 수 없는 알려지지 않는 공격으로 인한 피해를 최소화시켜 서비스의 가용성과 신뢰성을 향상시키기 위한 침입감내 개념을 적용한 연구[7]와 생존성 평가를 위한 취약점의 모델링 방법에 대한 연구[8]등을 수행 중에 있다. 또한 국외의 경우, 미국의 CERT에서는 생존성 분석 연구를 수행하여 SNA(Survivable Network Analysis)라는 분석방법을 제안하고 있다[2,9]. 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 있으나 정량적인 분석에 대한 연구는 미흡한 실정이다.

2.2 시뮬레이션 기반 취약성 분석 방법

[6]에서는 시뮬레이션 기반의 취약성 분석 방법론을 제안하여 공격에 따른 네트워크에 대한 피해의 정도 및 공격의 성공 가능성 관점으로 노드, 링크, 네트워크 취약성 평가 척도를 정의하고 시뮬레이션 분석에 효과적으로 적용한 바 있다. Fig.1은 시뮬시뮬레이션을 적용한 정량적인 취약성 분석 방법론을 나타낸다. Phase I은 개념 명세화 단계로서, 분석의 목적, 요구사항, 제약조건 등을 고려하여 구조적 지식의 표현수단을 제공하는 SES(System Entity Structure)를 이용함으로써 정보통신기반 네트워크의 전반적인 구조를 명세화한다. Phase II에서는 SES에 의해 표현된 정보통신기반 네트워크 구조에 대하여 Pruning을 적용

하여 분석 대상이 되는 네트워크의 구조인 PES(Pruned Entity Structure)를 생성한다. 또, SES상의 단말 노드들에 해당하는 IDS, Firewall, Router 등과 같은 네트워크 구성원과 다양한 공격 시나리오를 갖는 공격자, 분석을 위한 다양한 분석 목록을 갖는 분석자에 대한 모델들은 DEVS 형식론(Discrete Event Sytem Specification)에 의하여 구축되어 MB(Model Base)에 저장된다. Phase III에서는 변환(Transformation Operation)을 적용하여 PES의 네트워크 구조와 MB의 동역학적 모델을 통합시킴으로써 사이버 공격 시뮬레이션을 위한 최종적인 시뮬레이션 모델이 생성된다. 생성된 시뮬레이션 모델에 EF(Experimental Frame) 개념을 적용하여 다양한 사이버 공격에 대한 시뮬레이션을 수행한다. 끝으로, Phase IV에서는 Phase III를 통하여 얻어진 시뮬레이션 궤적으로부터 사이버 공격에 따른 각 노드의 변화와 더불어 사이버 공격의 상세한 행위를 분석한다. 또한, 취약성 매트릭스를 시뮬레이션 결과에 적용함으로써 노드, 링크, 네트워크에 대한 취약성을 정량적으로 평가한다. 특히, [6]에서 제시한 노드 취약성은 네트워크 상의 구성원들이 갖는 취약성 항목들과 항목들의 피해정도인 영향력에 대한 종합적인 취약성 값을 의미한다. 여기서, 취약성 항목은 운영 체제 종류, 버전 등과 같은 시스템 요소에 의존적인 'Fixed Vulnerability'와 패스워드 구성 상태, 파일 접근 권한 등과 같은 시스템 구성 설정에 의존적인 'Changeable Vulnerability'로 분류되어 있다. 취약성 항목들의 값은 0에서 1사이의 값으로 시뮬레이션 평가를 통하여 얻을 수 있다. 본 논문에서는 이와 같은 취약성 항목들과 네트워크 구성원들이 제공하고자 하는 서비스와 관련성을 이용하며, 시뮬레이션 평가를 통하여 얻어지는 취약성 항목의 정량적인 값을 이용한다.

3. 생존성 분석 방법

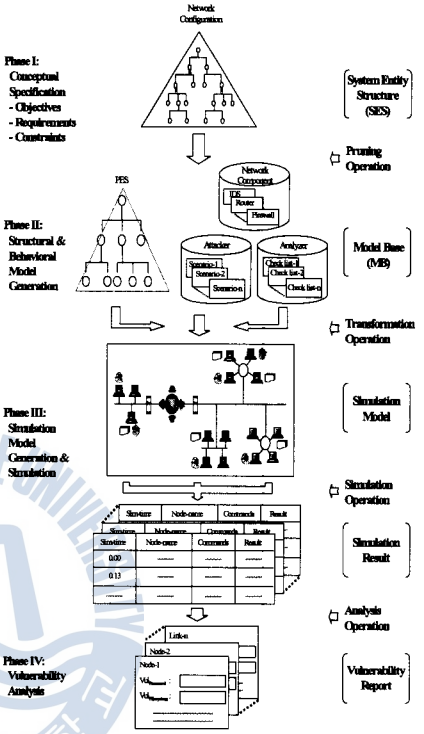

Fig. 1 Simulation-based approach for vulnerability analysis

네트워크 상의 구성원인 개별 노드에 대한 생존성과 노드들의 집합인 네트워크에 대한 생존성을 정량적으로 분석하는 방법을 제안한다.

3.1 노드 생존성

노드 생존성은 각각의 노드에 대한 생존성을 의미한다. 생존성이란 필수서비스에 대한 지속 능력을 의미하는 것으로서 해당 노드를 구성하는 필수 서비스와 해당 노드에 포함된 취약성과의 관계를 이용하여 생존성을 정의할 수 있다. 즉, 필수 서비스와 관련된 취약성 값

이 높을수록 필수 서비스의 제공 가능성이 낮아진다. 따라서 노드에 포함된 각각의 취약성 값과 이와 관련된 필수 서비스의 중요도에 대한 산술 평균을 구하고 최대 생존성 값인 1과의 차를 구함으로써 생존성을 구할 수 있다. 본 연구에서는 필수 서비스를 정의하기 위하여 노드에서 제공하는 다양한 서비스들에 대한 중요도를 0에서 1사이의 값으로 부여하고 기준값 0.5 이상의 중요도를 갖는 서비스를 필수 서비스로 정의하였다. 즉, 필수 서비스를 정의하기 위한 서비스의 중요도 및 기준값은 생존성을 분석하고자하는 조직의 상황에 따라서 달라질 수 있다. 또한 취약성 항목의 값은 2.2절에서 언급한 시뮬레이션 기반 취약성 분석을 통하여 정량적으로 계산하여 적용할 수 있다. 따라서 i번째 노드에 대한 생존성은 다음과 같이 정의한다.

$$NS_i = 1 - [\sum_{j=1}^{n} \sum_{k=1}^{m} vul\_val_j \times \{ES\_val_k \mid if\ vul_j\ \mathbb{R}\ ES_k\} / \sum_{k=1}^{m} ES\_val_k]$$

여기서, n은 해당 노드에 포함된 취약성 항목의 총 개수를 의미한다. vul_j는 j번째 취약성 항목을 의미하며 vul_val_j은 시뮬레이션으로 얻어진 취약성 항목의 값을 나타낸다. m은 해당 노드에서 제공하는 필수 서비스의 총 개수를 의미하며 ES_k는 k번째 필수 서비스 항목을 의미한다. ES_val_k은 필수 서비스 항목의 중요도를 의미한다. $\mathbb{R}$는 취약성 항목과 필수 서비스 항목과의 관련성을 의미하는 것으로 $\{ES_val_k \mid if\ vul_j\ \mathbb{R}\ ES_k\}$는 vul_j와 관련있는 ES_k의 중요도를 나타낸다.

3.2 네트워크 생존성

네트워크 생존성은 네트워크를 구성하는 구성원들의 개별 생존성을 기반으로 계산된 통합된 생존성을 의미한다. 따라서 네트워크 생존성은 각 노드의 중요도에 따라 가중치를 부여하고 앞 절에서 구해진 노드 생존성에 대한 산술 평균을 구함으로써 해당 네트워크의 전반적인 생존성을 얻을 수 있다. 즉, 다음과 같이 i번째 네트워크 생존성 $NetS_i$를 정의한다.

$$NetS_i = \sum_{j=1}^{n} (w_j \times NS_j) / \sum_{j=1}^{n} w_j$$

여기서, n은 해당 네트워크를 구성하는 구성원의 총 개수를 의미하며, w_j는 해당 네트워크를 구성하는 j번째 노드의 중요도를 나타낸다.

4. 사례연구

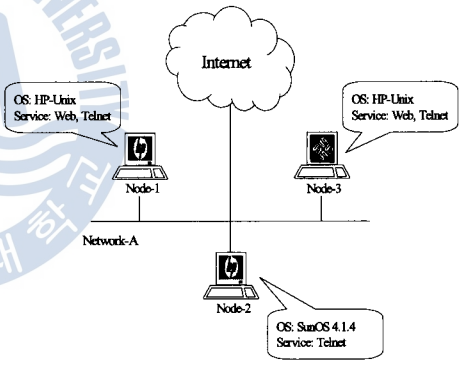

Fig. 2 Concept of sample network

앞서 제안한 생존성 분석방법의 타당성을 검토하기 위하여 Fig. 2와 같은 샘플 네트워크에 대하여 생존성 매트릭스를 적용해 보았다. Network-A는 3개의 노드로 구성되며 각각의 노드는 5개, 5개, 4개의 서비스로 구성된다. 예를 들어 Node1은 운영체제 서비스, Web서비스, Telnet 서비스, Ftp서비스, DB서비스를 제공한다. Table 1은 Node1에서 제공되는 서비스별 중요도와 해당 서비스와 관련된 취약성을 나타낸 것이다. 특히, OS, Telnet, Ftp는 중요도가 기준값 0.5 이상으로

서 필수 서비스를 의미한다.

Table 1 Definition of services on Node1

서비스항목(S_i)	중요도	취약성항목(V_i)
OS	1*	V_1
Web	0.4	V_2
Telnet	0.6*	V_1
Ftp	0.8*	V_2
DB	0.2	V_3
* 필수 서비스 (중요도 0.5 이상)		

Table 2 는 Node1에 존재하는 취약성의 값으로서 시뮬레이션에 의하여 구한다. 단, 본 사례연구에서는 생존성 분석이 목적이므로 값을 가정하여 사용하였다.

Table 2 Value of vulnerabilities analyzed by simulation on Node1*(assumed)*

취약성 항목(Vi)	취약성
V_1	0.2
V_2	0.5
V_3	1

Table 3, Table 4와 Table 5, Table 6은 각각 Node2와 Node3와 필수 서비스와 관련 취약성의 값을 나타낸다. 특히, 비교를 위하여 Node2에 포함된 취약성의 값은 Node1과 같도록 하고 필수 서비스만을 다르게 정의하였다. Node2의 필수 서비스는 OS, Telnet, Ftp, DB이며 Node3의 필수 서비스는 OS와 Ftp이다.

Table 3 Definition of services on Node2

서비스항목(S_i)	중요도	취약성항목(V_i)
OS	1*	V_1
Web	0.4	V_2
Telnet	0.6*	V_1
Ftp	0.8*	V_2
DB	0.7*	V_3
* 필수 서비스(중요도 0.5 이상)		

Table 4 Value of vulnerabilities analyzed by simulation on Node2*(assumed)*

취약성 항목(Vi)	취약성
V_1	0.2
V_2	0.5
V_3	1

Table 5 Definition of services on Node3

서비스항목(S_i)	중요도	취약성항목(V_i)
OS	1*	V_1
Telnet	0.3	V_1
Ftp	0.8*	V_2
DB	0.2	V_3
* 필수 서비스 (중요도 0.5 이상)		

Table 6 Value of vulnerabilities analyzed by simulation on Node3*(assumed)*

취약성 항목(Vi)	취약성
V_1	0.3
V_2	0.7
V_3	0.2

Table 7은 네트워크 생존성 분석을 위한 각 노드의 중요도를 나타내며 Table 8은 제안된 방법을 통하여 얻어진 각각의 노드 생존성 및 네트워크 생존성을 나타낸다. Node1, Node2, Node3의 노드 생존성 값은 각각 0.7, 0.55, 0.53임을 알 수 있다. Node1과 Node2의 경우 제공 서비스와 존재하는 취약성 값이 같으나 Node2에는 DB서비스가 추가적으로 필수 서비스로 지정되어 있고 그와 관련된 취약성이 존재함으로 인하여 생존성이 Node1에 비하여 낮음을 알 수 있다. 또한, Node1, Node2, Node3로 구성된 네트워크인 Network-A는 각 노드의 중요성이 반영되어 0.55정도의 네트워크 생존성을 나타냄을 알 수 있다. 이와 같이 필수 서비스와 그에 따른 취약성을 통하여 노드 생존성과 네트워크 생존성을 정량적으로 분석할 수 있다.

Table 7 Weight of each node

노드(Ni)	가중치(wi)
Node1	0.2
Node2	0.5
Node3	1

Table 8 Summary of each survivability

항목	값	비고
NS1	0.7	1-((0.2×1+0.2×0.6)+(0.5×0.8))/(1+0.6+0.8) = 1 - 0.3 = 0.7
NS2	0.55	1-((0.2×1+0.2×0.6)+(0.5×0.8)+(1×0.7)) /(1+0.6+0.8+0.7) = 1 - 0.45 = 0.55
NS3	0.53	1-((0.3×1)+(0.7×0.8))/(1+0.8) = 1 - 0.47 = 0.53
NetS	0.55	(0.2×0.7+0.5×0.55+1×0.53)/(0.2+0.5+1) = 0.55

5. 결 론

본 논문은 필수 서비스와 취약성을 이용하여 네트워크의 생존성을 정량적으로 분석하는 방법의 제안을 목적으로 하였다. 생존성이란 외부의 공격 또는 사고 등에도 불구하고 자신이 제공해야 하는 필수적인 서비스를 지속적으로 제공할 수 있는 능력을 의미한다. 이를 위하여 취약성과 서비스와의 관계를 이용하여 생존성을 분석할 수 있는 수식을 도출하고 기존에 제안된 시뮬레이션 기반의 취약성 분석으로부터 얻어진 정량적 취약성값을 적용하였다. 샘플 네트워크에 대한 사례연구를 통하여 제안된 방법의 타당성을 검토하였으며 제안된 방법을 통하여 분석하고자 하는 네트워크 및 구성 노드들에 대한 생존성을 정량적으로 분석할 수 있었다. 향후연구로는 서비스와 취약성에 대한 상세화가 필요하며 기존의 시뮬레이션 기반 취약성 분석 방법과의 연동을 통한 자동화에 대한 연구가 요구된다.

후 기

본 연구는 한국해양대학교 신진교수연구비 지원에 의한 것임.

참 고 문 헌

[1] T.A Longstaff, C.Chittister, R. Pethia, Y.Y. Haimes : "Are We Forgetting the Risks of Information Technology", IEEE Computer, 2000

[2] Robert J. Ellison, Richard C. Linger, Thomas Longstaff, and Nancy R. Mead : "Survivable Network System Analysis: a Case Study", IEEE Software, 1999

[3] T. Aslam : A Taxonomy of Security Faults in the Unix Operating System, M.S. thesis, Purdue University, 1995

[4] C.E. Landwehr, et. al. : "A Taxonomy of Computer Program Security Flaws", Computing Surveys, 26(3), 1994

[5] Fred Cohen : "simulating Cyber Attacks Defenses, and Consequences". 1999 IEEE Symposium on Security and Privacy Special 20th Anniversary Program, The Claremont Resort Berkeley, California

[6] 이장세 : 지능형 통합보안 관리 시스템을 위한 시뮬레이션 기반 취약성 분석 방법론, 박사학위논문

[7] 이태진, 김형종, 이강신 : "침입감내기술에서의 voting 및 그룹관리 신성 분석", 한국시뮬레이션학회 2004 춘계학술대회 논문집

[8] 김형종 : "생존성 평가를 위한 취약성 모델링 방법 연구", 2003 한국시뮬레이션 학회 추계학술 대회

[9] Cert Coordination Center, http://www.cert.org

원고접수일 : 2007년 1월 15일
원고채택일 : 2007년 1월 24일