DMKB를 이용한 IT 기반구조의 생존성 평가 시스템

(Survivability Assessment using DMKB for IT infrastructure)

최 은 정 † 김 명 주 ††
(Choi Eun-Jung) (Kim Myuhng-Joo)

요 약 초고속 네트워크의 보편화와 하드웨어 및 서버 기술의 발달로 인해 대규모 고성능 분산 네트워크 중심의 IT 기반구조 구축이 사회 전반에 걸쳐 확대되고 있다. 이러한 IT 기반 구조에 대한 평가 척도는 매우 다양하게 제시될 수 있지만, 기반 구조라는 특성 상 생존성 평가는 매우 중요한 척도로 간주된다. 주어진 IT 기반 구조에 대하여 어느 정도의 생존성을 가지고 있는지 평가하는 것은, 무수한 IT 기반 구조들에 대한 보편적인 평가 척도를 제시하는 것일 뿐만 아니라 해당 평가결과를 토대로 한 추가 개선 작업을 통하여 더욱 생존성이 강화된 IT 기반 구조로의 발전을 보장해준다. 본 논문에서는 현재의 IT 기반 구조를 구성하고 있는 개별 구성요소들에 대하여 이미 구축해 놓은 방어메커니즘 데이타베이스(DMKB)를 토대로 하여, 전체 IT 기반 구조의 생존성을 평가하는 시스템을 제시한다.

키워드 : 정보통신 기반구조, 생존성 평가, 시스템 및 네트워크 보안, 방어메커니즘

Abstract The popularization of high-speed networks and the innovation of high-performance hardware/servers have enlarged the role of large-scale, highly distributed IT infrastructure. Though many criteria on the assessment of IT infrastructure can be considered, the survivability assessment is treated as the most important one due to the essential role as an infrastructure. While assessing the survivability of some given IT infrastructures, we can not only choose the best one among them but also improve their survivability by modifying their structure and security policies. In this paper, we propose a DMKB-based assessment system on the survivability of IT infrastructures, where DMKB is a kind of database which provides the known vulnerabilities and defense mechanism for many system components.

Key words : IT infrastructure, Survivability Assessment, System & Network Security, DMKB

1. 서 론

현재의 IT 인프라는 고속 네트워크와 고성능 하드웨어 개발로 인해 대규모 분산 네트워크로 발전하게 되었다. 네트워크 시스템의 발전은 컴퓨터 시스템을 기반으로 하는 서버 개체 중심의 관리체계를 벗어나 서버, 네트워크, 기타 네트워크 장비를 포함하는 네트워크 인프라 스트럭처의 전체 시스템을 하나의 단위로 관리하게 되었고 고성능 분산 네트워크 구조를 확립하였다[1]. 현재 사회의 대표적인 특징으로 경계가 없는 네트워크에서 동작하는 인터넷과 같은 고속 분산 정보시스템의 증가를 들 수 있다. 경계가 없는 네트워크는 지역네트워크의 경계 내에서 중앙의 단일 관리자에 의해 제어되는 것과 달리 분산되어 관리된다는 특징이 있고, 전체 네트워크에 대한 완벽한 정보를 유지할 수 없다[2]. 이러한 환경에서의 정보보호의 방식도 변화하고 있다.

DARPA에서는 다음과 같이 보안의 3세대를 정의하고 있다[3]. 보안의 첫번째 세대는 초기 단계로 신뢰할 수 있는 컴퓨팅 환경을 기본으로, 접근 제어, 암호화, 방화벽, 그리고 다른 경계 제어와 같은 방지 단계로 명명할 수 있다. 이런 형태의 대응은 시스템 운영에 부하을 초래하여 복잡한 내부적 연결과 정보 공유가 요구된다. 두번째 세대는 시그니처, 이형태, 그리고 형태적 연관

· 본 연구는 2006년도 서울여자대학교 학술연구비 지원에 의해 수행되었음
† 정 회 원 : 서울여자대학교 정보통신교육원 교수
chej@swu.ac.kr
†† 종신회원 : 서울여자대학교 정보보호학 전공 교수
mjkim@swu.ac.kr
논문접수 : 2006년 5월 24일
심사완료 : 2006년 8월 17일

기술과 같은 사례에 대한 탐지를 목표로 하지만, 100%의 성공적 탐지와 0%의 오류를 만들어 내는 이상적인 탐지로는 여전히 불가능 하다. 마지막으로 세 번째 세대는 IA&S(Information Assurance and Survivability) 프로그램으로 첫번째와 두 번째 세대의 기술을 포함하며, OASIS를 통해 연구가 진행되고 있다. 이와 같은 보안 시스템 구축에 대한 최근의 연구는 공격의 발생 이후의 대응에 주 목적을 두어 감내를 위한 생존성과 회복성를 주요 이슈로 한다. 특히, 생존성은 보안, 오류 감내, 안정성, 신뢰성, 재사용, 성능, 인증, 평가와 연관된 연구 분야와 새로운 개념과 기준을 설명해 주는 최신 동향으로 경계가 없는 네트워크 구조에서 생존성의 개념을 적용하여 보안 대책을 제시하는 다양한 연구가 이루어지고 있다[2].

본 논문에서는 최근의 보안 잇슈인 생존성에 대해 알아보고 이를 기준으로 주어진 IT 기반 구조를 대상으로 생존성을 평가 시스템을 설계한다. 이를 위해 DMKB (Defense Mechanism Knowledge Base)[4]를 이용하여 개별 요소에 대한 평가가 이루어지고 전체 IT 기반 구조의 생존성 여부를 판단하게 된다. 이를 통해 IT 기반구조의 생존성 평가와 함께 생존성 향상을 위한 지표를 제공하게 된다.

2. 생존성(Survivability)

고성능 분산 네트워크 환경의 확장과 함께, 인터넷과 같은 경계가 없는 네트워크 인프라에서 정보보호는 보호와 공격탐지의 정도로는 한계를 가질 수밖에 없다. 최근 정보보호의 흐름이 생존성에 대한 연구에 관심을 두는 이유도 이와 같다. 생존성은 유효 시간 내에 공격, 실패, 또는 사고가 발생할지라도 원래 목적대로 서비스할 수 있는지에 대한 능력으로 정의된다[5]. 공격이나 사고, 혹은 오류가 발생하더라도 사용자에게 필요한 서비스를 지속적으로 제공한다[6]. 따라서 사용자 측면에서는 만족할만한 서비스를 제공 받을 수 있고, 이러한 상황에서 시스템은 피해시스템의 복구와 정상화를 위한 시간을 확보할 수 있기 때문에 서버와 클라이언트 모두에게 효과적인 정책으로 적용될 수 있다. 이를 위해 서비스 제공자는 새로운 수준의 보안 대책을 마련해야 하며, 이전에 행해져 왔던 데이타 보안, 침입탐지, 접근제어 등의 방식은 한계를 가질 수밖에 없다.

생존성의 조건은 필수 서비스 진행 과정에 대응되고 사용자 요구로부터 도출되고, 독립적인 시스템 개체의 안에서 생존성 속성들을 요구에 맞춘 필수 서비스의 흐름을 정의해야 한다[7]. 이를 위해 특정시스템의 필수 서비스에 대한 정의가 필요하며 이에 대한 안정성을 보장해 주어야 한다. 따라서 안전한 시스템에 대한 광범위한 보안보다는 시스템의 목적, 사용자의 요구에 대해 지속적인 서비스를 통해 최적의 환경을 제공하는 것이 생존성의 목표이다.

2.1 관련 연구

정보전 대응에 필요한 정보보증 및 생존성 기술 개발을 위한 연구인 DARPA의 IA&S와 OASIS(Organically Assured and Survivable Information System Program)가 대표적인 연구이다. IA&S 프로젝트에서는 ITS(Intrusion Tolerance System)과 FTN(Fault Tolerance Networks)를 통해 생존성 문제를 다루고 있으며 침입을 감내하며 결함을 허용하는 시스템 설계와 구축에 관한 전반적인 기술을 모색한다[8]. OASIS 프로젝트는 생존성 시스템의 정의를 공격이나 침입에 대해 특정 서비스의 지속적인 제공하는 것으로 정의하고 이를 위해 다중 계층의 방어 개념을 제공하고 있다[9].

2.2 생존성 평가 기술

CERT에서는 생존성과 관련된 연구를 중심으로 생존성이 강화된 시스템 구현을 위한 방법을 제시하고 있다. 먼저, 시스템에 필수 서비스를 제공하고 공격에 대해서도 무결성, 비밀성, 성능 보장과 같은 중요 속성을 유지하도록 하며, 공격이 이루어진 경계 없는 네트워크 시스템의 보증에 대한 생존성 방법 제안과 함께, 생존성 실행의 현재 상태, 생존성 요구의 조건, 생존성 확보를 위한 기준, 그리고 생존성 분석을 위한 기술과 흐름을 위한 통합 프레임워크 제안하였다[10]. 이를 기반으로 구현된 생존성 평가 시스템은 필수 서비스를 정의하고 사용자요구로부터 도출된 시스템 자원으로의 독립성과 필요한 생존성의 속성을 정의하여 발생 가능한 공격 패턴으로 유추된 침입 시나리오 등을 통해 대응(resistance), 감지(recognition), 복구(recovery)가 가능한 생존성 시스템을 설계하였다[11]. 이러한 생존성 강화 시스템은 전체 정보통신 인프라에 적용되어야 하며 다양한 침입 패턴 및 시나리오를 구현이 필요하기 때문에 운영 중인 정보통신 인프라에 바로 적용하기에는 어려움이 있다. 따라서 효율적인 생존성 평가를 위해 현재 운영 중인 정보통신 인프라에 적용할 수 있어야 한다.

본 논문에서는 정보통신 인프라를 평가하고 그에 대한 생존성 평가해주는 방법으로 취약점 정보를 이용하고자 한다.

취약점은 정보보호 침해사고의 원인으로 작용하며, 정보통신 인프라 시스템에 내제되어 있는 보안 문제점이다[12]. 이러한 취약점은 공격자들이 침해사고를 일으키는 대부분의 원인으로 작용한다. 생존성은 공격의 발생에 대한 생존 여부를 의미한다. 따라서 특정 시스템에 취약점이 많이 존재하면 생존성은 보장받기 어려워지게 된다. 그러나 취약점이 존재한다고 하더라도 해당 취약

점에 대한 적절한 대책이 적용되어 있다면 생존성을 보장 받을 수 있게 된다.

본 논문에서는 수집된 취약점 정보와 이에 대한 대응 정보를 이용하여 생존성 평가에 활용할 수 있게 한다.

3. 생존성 평가를 위한 프레임

생존성 평가를 위해서는 먼저, 평가 대상이 되는 범위를 한정하고 이를 기반으로 주요한 요소들과 함께 평가를 위한 구조를 정의한다. 생존성 평가를 위한 기반 환경은 가장 일반적인 정보통신 인프라를 모델로 하여 공격, 오류가 일어날 수 있는 네트워크 시스템을 대상으로 한다. 생존성 평가를 위한 프레임은 다음의 그림 1과 같이 대상이 되는 IT 기반구조를 대상으로 하고 이에 다한 평가 결과로 평가 점수를 제공하게 된다.

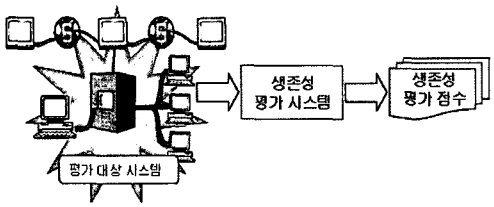

그림 1 생존성 평가 프레임

생존성 평가 시스템은 두 단계를 통해 결과를 제공하게 된다. 먼저, DMKB를 이용하여 개별적 요소에 대한 생존성을 평가하고 그 결과를 바탕으로 전체 IT 기반구조의 목적에 맞춘 생존성을 판단하게 된다. 각각의 과정에서는 평가 매트릭스와 판단 매트릭스를 이용하게 되며, 결과는 점수로 제공되게 된다.

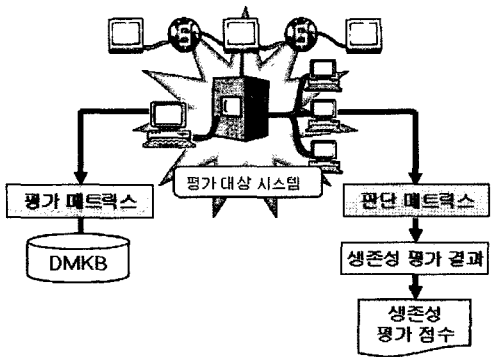

그림 2 생존성 평가 시스템

3.1 DMKB

DMKB(Defense Mechanism Knowledge- Base)는 정보보호 침해사고와 공격, 이에 대한 원인인 취약점, 대응 방법에 대한 방어 메커니즘을 제공하고 있다[4]. 방어메커니즘은 침해사고의 조건에 해당하는 시스템 사양 및 종류, 원인에 해당하는 취약점, 이를 통해 이루어지는 공격 입력을 중심으로 하는 Condition DB와 이에 대한 대응을 위해 취약점을 제거하거나 시스템 보안을 위한 시스템 입력을 관리하고 각종 보안 정책 및 해결책을 적용하는 정보인 Action DB로 구성되어 있다. DMKB는 다음의 그림 3과 같이 시스템 사양, 취약점, 공격 정보를 중심으로 하는 Condition DB와 취약점 제거, 시스템 설정 관리, 보안정책 적용 등의 대응책을 제시하는 Action DB의 관계를 통해 구성되어 있다.

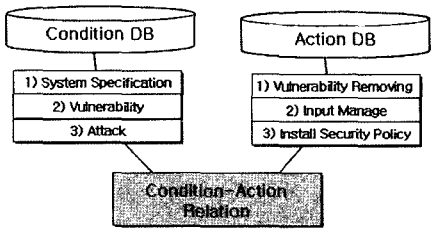

그림 3 DMKB Schema

DMKB에 저장된 방어 메커니즘은 총 325개이며, 분석데이타는 CVE 29개, 공격 1개, CERT 사고노트 13건이다. 구현 시스템은 Pentium IV 700MHZ, 이고 OS는 LINUX Redhat 7.3, 웹서버는 apache 1.3.7, DBMS는 Oracle 9.0.1, 웹 인터페이스는 PHP 4 Zend이다. 다음의 그림 4는 DMKB를 통해 제공되는 방어메커니즘 지식이다.

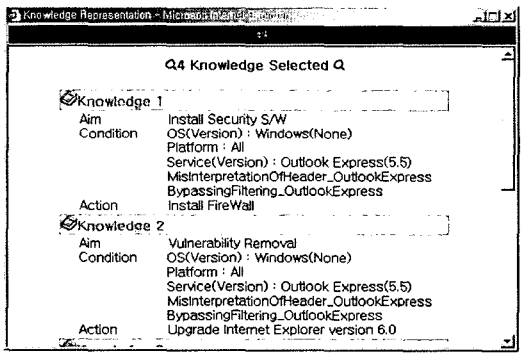

그림 4 knowledge of DMKB

3.2 평가 매트릭스(Assessment matrix)

서버, 클라이언트를 비롯한 정보통신 인프라 개체를 평가하기 위한 기준으로 DMKB를 참고하여 생성된다. 1차 기준은 해당 시스템의 지원 가능한 서비스 목록을 System Specification에 작성한다. 해당 시스템에서 제

공하는 다양한 서비스에 대한 목록을 Service 항목에 작성하고 이에 대해 condition과 action을 추출하고 방어 메커니즘이 적용되었는지 여부를 판단한다. 이를 통해 주요한 시스템 사양과 이름을 기준으로 하여 해당 서버에서 제공하는 서비스들에 대해 취약 항목과 방어 항목을 체크한다. 따라서 각각의 개별 서비스에 대한 방어 비율을 기준으로 생존성 정도를 백분율로 산출하게 된다.

표 1 평가 매트릭스

System Specification (Alias name)	Condition	Action	Y/N	Rate (%)
Service1				
.....				
Servicen				
Result	Sum of Y/Total	Average (%)		

3.3 판단 매트릭스(Decision matrix)

최종적인 생존성 여부 평가 단계로 이전 단계에서 작성된 데이타의 서비스 별 결과 항목을 가져오게 된다. 평가 매트릭스가 개별적인 시스템을 중심으로 작성되었기 때문에, 이 단계에서는 서비스를 기준으로 개별적 시스템에서 평가한 생존성 값을 나열하고 최종적인 생존성 여부를 판단하게 된다.

판단 매트릭스는 다음의 표 2와 같이 구성된다. 주어진 IT 인프라에서 제공하는 서비스들의 목록을 Service list 항목에 정리하고 각각의 서비스에 대해 제공했던 개별적 시스템들을 System 항목에 기록하고 각각의 시스템들 간의 관계를 Relation 항목에 명시하고 이를 기반으로 선택되는 생존성 값을 Rate Choice에서 선택하게 된다. 부가적으로 필수 서비스 항목을 Essential Service에 한 번 더 체크하게 된다. 판단 매트릭스는 제공되는 서비스와 IT 인프라의 시스템 개체 수에 따라 확장시켜 작성할 수 있다. 작성된 판단 매트릭스 값을 기준으로 최종적인 IT 인프라의 생존성을 Survivability Decision에서 판단하게 된다.

이 단계에서는 사용되는 관계와 서비스의 단순 나열이 아니 개별적인 시스템 간의 관계에 대한 정보를 포함하게 되어 있다. 서비스의 경우는 필수 서비스의 개념을 두어 IT 기반구조에서 제공하는 서비스들의 우선순위의 개념이 적용하도록 한다. 특히, 관계의 경우는 IT 기반구조를 운영하는 조직의 특성과 상황에 따라 운영되는 기준을 의미하는 것으로써 특정 서버에 대한 백업(backup)이나 서비스에 대한 미러링(mirroring), 임시로 운영하는 템퍼러리(temporary) 등의 역할을 정의할 수 있다. 백업과 미러링의 경우는 연관된 서버 혹은 서비스 개체와의 연결 관계로 다루어지기 때문에 생존성 판단 단계에서 대체 가능한 서버 혹은 서비스로 판단된다. 관계는 최종적 생존성 판단에 중요한 영향을 미치게 되므로 네트워크 구성 상황에 따라 다양하게 표시 될 수 있다. 각각의 개체에 대한 관계는 서버의 구성형태에 따라 다음과 같이 정의되고 이를 기준으로 해당 서비스의 방어 비율을 표 3과 같이 결정하게 된다.

표 3 판단 기준

Relation	Meaning	Decision of System Rate
AND	Essential service	Average rate
OR	Non-essential service	Small rate
OPT	Optional service	Priority rate
ALONE	Alone service	

AND 관계는 필수 서비스를 위한 관계로 주어진 정보통신 인프라에서 반드시 유지되어야 하는 것으로 우선적인 고려가 필요하기 때문에 각각의 시스템 방어 비율의 평균값을 구하게 된다. OR는 필수 서비스가 아닌 경우로 서비스 제공 실패에 대한 부담이 상대적으로 덜한 경우이다. 이 경우에는 해당 서비스에 대한 보장여부의 중요성이 낮기 때문에 최종적으로 낮은 값의 방어 비율 선택하게 된다. OPT는 부가적인 서비스로, 각각의 항목의 중요도에 따라 방어 비율 값을 선택하게 된다. ALONE은 독자적인 서비스를 의미하며 주어진 값을 그대로 선택하게 된다.

4. 생존성 평가 사례

IT 인프라를 제시하고 이에 대한 생존성 평가 과정을 보인다. 본 사례의 IT 인프라는 세 개의 서버로 구성되어 있으며, 제공되는 서비스들에 대해서는 IIS를 통한 웹 서비스를 필수 서비스로 정의한다. IT 인프라 구조

표 2 판단 매트릭스

Service list	System *1*	Relation	.....	System *n*	Relation	Rate Choice (%)	Essential Services
Service *1*							
.....							
Servicen							
Result			Survivability Decision				

에 대한 개체간의 관계를 표현하기 위해서 복합 시스템 사례를 제시하고 각각의 시스템의 역할을 정의하였다. 두 대의 서버로, Windows 2000과 Solaris 7을 운영하는 경우를 제시하고 각각의 시스템 상태에 대해서는 임의의 값을 적용하였다.

4.1 복합 시스템(Complicated system)

본 사례는 세대의 서버를 포함하고 있는 다중 시스템의 네트워크 인프라이다. 시스템의 주요 사양은 Windows 2000, Windows NT, Solaris 7이다. 본 네트워크 인프라에서 각각의 서버는 개별적으로 동작하지만 Windows 2000 서버가 주 서버이고 Windows NT 서버는 주 서버가 제대로 작동 할 수 없을 때를 대비한 미러링 서버로 설정되어 있다. Solaris 7 서버는 이용은 하지만 특별한 필수 서비스를 제공하고 있지는 않다. 본 사례에서도 대상 인프라의 필수서비스는 IIS를 통해 제공하는 웹서비스이다.

4.2 평가 매트릭스

평가 대상이 되는 세 개의 시스템에 대해 적용하기 위해 동일한 운영체제를 사용하는 두 개의 Windows 2000 서버를 평가한다. 각각의 시스템은 동일한 운영체제를 사용하지만 시스템의 보안 상태는 다르게 평가되고 있다. 또 다른 하나인 Solaris 7 시스템의 경우는 인트라넷 지원을 위해 운영 중인 시스템이다. 각각의 시스템의 주요한 웹 서비스로는 Apache, SSH를 중심으로 평가하였다.

첫 번째 사례의 경우는 웹서비스와 관련된 IIS, ISAPI, IE의 생존성 여부를 측정한다. 이를 기반으로 각각의 서비스 항목의 생존성에 대해 평균값을 산출해 낸다.

두 번째 사례의 경우는 윈도우 2000 서버로 웹서비스와 관련된 IIS, ISAPI, IE의 생존성을 측정하고 평균값을 산출한다.

세 번째 사례는 솔라리스 서버로 IIS를 이용한 서비

표 4 평가 매트릭스 사례 - 1

Windows 2000 (Web service)

Window2000 (Web-main)	Condition	Action	Y/N	Rate (%)
IIS	NoCheckParameterCondition EnabledGainFileInfo_IIS	Patch MS_q269862	Y	33.3
	CGIFilenameIsDecodedTwice ExecuteArbitraryCode_IIS	Patch MS_29787	N	
	CGIFilenameIsDecodedTwice ExecuteArbitraryCode_IIS	Patch MS_29764	N	
ISAPI	StackOverflow RootShellCreated_idq.dll	Install MS_30833	Y	50.0
	StackOverflow RootShellCreated_idq.dll	Upgrade Windows XP	N	
	StackOverflow RootShellCreated_idq.dll	Install based on OEM	Y	
	StackOverflow RootShellCreated_idq.dll	Patch MS01-033	Y	
	StackOverflow RootShellCreated_idq.dll	Restore OS (patch set)	N	
	StackOverflow RootShellCreated_idq.dll	Install MS_30800	N	
IE	UnauthorizedCodeInjectionInCache_IE GainInfo-Path_IE ExecuteArbitraryCode_IE	Patch MS_q286045	Y	100.0
Result	5/10	Average (%) 61.1		

표 5 평가 매트릭스 사례 - 2

Windows 2000 (Mirroring of Web Service)

Window2000 (Web-mirror)	Condition	Action	Y/N	Rate (%)
IIS	NoCheckParameterCondition EnabledGainFileInfo_IIS	Patch MS_q269862	Y	66.6
	CGIFilenameIsDecodedTwice ExecuteArbitraryCode_IIS	Patch MS_29787	Y	
	CGIFilenameIsDecodedTwice ExecuteArbitraryCode_IIS	Patch MS_29764	N	
ISAPI	StackOverflow RootShellCreated_idq.dll	Install MS_30833	Y	33.3
	StackOverflow RootShellCreated_idq.dll	Upgrade Windows XP	N	
	StackOverflow RootShellCreated_idq.dll	Install based on OEM	N	
	StackOverflow RootShellCreated_idq.dll	Patch MS01-033	Y	
	StackOverflow RootShellCreated_idq.dll	Restore OS (patch set)	N	
	StackOverflow RootShellCreated_idq.dll	Install MS_30800	N	
IE	UnauthorizedCodeInjectionInCache_IE GainInfo-Path_IE ExecuteArbitraryCode_IE	Patch MS_q286045	N	0.0
Result	4/10	Average (%)		33.3

표 6 평가 매트릭스 사례 - 3

Solaris 7 (Intranet)

Solaris 7 (Intra-net)	Condition	Action	Y/N	Rate (%)
Apache	GainInfo_HTTPDVersion	Set httpd.conf : ServerTokens Prod[uctOnly]	Y	50.0
	RootShellCreated_snmpXdmid StackOverflow	patch sun patch	N	
	StackOverflow RootShellCreated_lpd	Patch Sun_107115-08	Y	
	StackOverflow RootShellCreated_lpd	Patch Sun_109321-04	N	
Apache SSH	StackOverflow RootShellCreated_lpd	Patch Sun_109320-04	Y	100
	EncryptedPasswdComparisonError_ssh ExecuteArbitraryCode_wu-ftpd StackOverflow RootShellCreated_lpd	Upgrade SSH Secure Shell 3.0.1	Y	
Result	4/6	Average (%)		70

표 7 판단 매트릭스 2

Service list	Win2K (Main)	Rel.	Win2K (Mirror)	Rel.	Solaris7	Rel.	Decision of Rate(%)	Essential Services
IIS	33.3	AND	66.6	AND	N/A		66.6	O
ISAPI	50.0	OR	33.3	OR	N/A		33.3	
IE	100.0	OR	0.0	OPT	N/A		100.0	
Apache	N/A		N/A		50.0	OR	50.0	
Apache/SSH	N/A		N/A		100.0	OR	100.0	
Result		**Survivable Decision (%)**					**66.6**	

스는 제공하지 않으며 apache를 이용한 인트라넷 서비스를 제공하고 있다. 따라서 제공하는 서비스에 대한 생존성을 판단하고 이에 대한 평균을 산출한다.

4.3 판단 매트릭스

이전 단계에서 구해진 평가 매트릭스의 값을 이용하여 최종적인 생존성 여부를 평가한다. 다수개의 서버, 동일한 서비스들이 제공되고 있기 때문에 생존가능성을 판단하기 위해서 각 서버간의 관계를 고려하여 최종적인 방어 비율 값을 결정한다.

예를 들어 IIS 서비스의 경우 주요 웹 서버의 방어 비율 33.3에 그치지만 동일한 서비스가 가능한 다른 시스템에서 66.6의 방어 비율을 보이고 있고 각각의 서비스가 AND 관계로 우선순위를 갖기 때문에 비율 값 중에서 가장 높은 값을 선정할 수 있어 66.6의 비율 값을 결정하게 된다. ISAPI의 경우는 제공되는 각각의 서비스의 비율이 50.0, 33.0을 나타내지만 두 개 서비스 간의 관계가 OR로 시스템 오류 발생 시에 우선순위를 가질 수가 없기 때문에, 작은 값만큼만 보장을 받게 되어 33.3이 선택된다. 생존가능성 선택에 의해서는 필수 서비스로 지정된 IIS 서비스를 기준으로 66.6이 선택된다.

5. 결 론

본 논문에서는 DMKB를 활용하여 IT 인프라의 생존성을 평가하는 시스템을 제시하였다. IT 기반구조의 생존성 평가를 위하여 우선 프레임을 정의하고 평가과정에서 필요한 평가 매트릭스와 판단 매트릭스를 정의하였다. 평가 매트릭스 단계에서는 주어진 시스템에 대한 방어메커니즘을 선택 적용 여부를 판단하였고 이를 통해 특정 시스템의 서비스에 대한 방어 비율을 판단할 수 있다. 판단 매트릭스에서는 서비스 항목과 방어 비율을 기반으로 주어진 네트워크의 구조, 관계에 맞추어 방어 비율을 선택하고 필수 서비스에 대응되는 값을 선택하여 생존가능 판단 값을 얻게 된다.

향후 생존성 평가 프레임을 생존성 개선시스템으로 확장할 것이다. 다음의 그림 5와 같이 생존성 평가를 통한 결과를 통해 개선 조치를 유도하게 되어 평가 대상 시스템에 적용 주어진 시스템의 생존성 향상을 기대할 수 있게 된다.

아울러 판단매트릭스의 평가 요소에 대한 다양성을 부여하는 연구도 진행할 필요가 있다. 현재로는 서비스

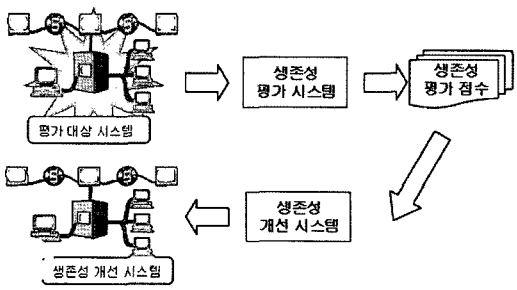

그림 5 생존성 개선 시스템

를 제공하는 서버들 간의 관계만 고려되고 있지만 취약성의 연관성, 보안 정책의 적용 여부에 따른 정량적 표현이 추가되면 더 실무적인 평가 시스템으로 발전할 것이다.

참 고 문 헌

[1] D. A. Fisher and H.F. Lipson, "Emergent Algorithms – A New Method for Enhancing Survivability in Unbounded Systems," Proceedings of the 32nd Annual Hawaii International Conference on System Sciences, Maui, Hawaii, January 5~8, 1999 (HICSS-32), IEEE Computer Society, 1999.

[2] R. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, and N. Mead, "Survivable network systems: An emerging discipline," Technical Report CMU/SEI-97-153, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213, November 1997.

[3] J. H. Lala, "Introduction," Proceeding of the Foundation of Intrusion Tolerant System (OASIS'03), IEEE Computer Society, 2003.

[4] Eun-Jung Choi, Hyung-Jong Kim, Myuhng-Joo Kim, "DMKB : A Defense Mechanism Knowledge Base," International Conference ICCSA, May 2004, Assisi Italy, LNCS 3043 2004.

[5] H. F. Lipson, D. A. Fisher, "Survivability - A New Technical and Business Perspective on Security," Proceedings of the 1999 New Security Paradigms Workshop. Caledon Hill, ON, September 21-24, 1999. New York, NY: Association for Computer Machinery, 2000.

[6] S. Jha and J. M. Wing., "Survivability Analysis of Networked Systems," Proceedings of the 23rd International Conference on Software Engineering (ICSE2000), pages 307-317, 2001.

[7] R. C. Linger, A. P. Moore, "Foundations for Survivable System Development: Service Traces, Intrusion Traces, and Evaluation Models," Technical Report CMU/SEI-20001-TR-029, Carnegie Mellon University, Pittsburgh, PA 15213,October 2001.

[8] Jaynarayan H. Lala, "Information Assurance and Survivability," International Conference on Dependable Systems and Networks, NY, USA, June 25-28, 2000.

[9] Dale M. Johnson and Ph.D.Doug Williams, Ph.D., "Organically Assured and Survivable Information Systems (OASIS)," MITRE Technology Symposium, Washington, June 2002.

[10] R. J. Ellison and D. A. Fisher and R. C. Linger and H. F. Lipson and T. Longstaff and N. R. Mead, "Survivable Network Systems: An Emerging Discipline," CERT, November 1997 Revised: May 1999, CMU/SEI-97-TR-013.

[11] Richard C. Linger and Andrew P. Moore, "Foundations for Survivable System Development: Service Traces, Intrusion Traces, and Evaluation Models," CERT, CMU/SEI-2001-TR-029, October 2001.

[12] M. Bishop: Vulnerabilities Analysis. Proceedings of the Recent Advances in Intrusion Detection, (1999).

최 은 정

1997년 서울여자대학교 전산과학과학과(이학사). 2000년 서울여자대학교 대학원 컴퓨터학(이학석사). 2005년 서울여자대학교 대학원 컴퓨터학과(이학박사). 2006년~현재 서울여자대학교 정보통신교육원 전임강사

김 명 주

1986년 서울대학교 컴퓨터공학과(공학사) 1988년 서울대학교 컴퓨터공학과(공학석사). 1993년 서울대학교 컴퓨터공학과(공학박사). 1993년~1995년 컴퓨터신기술공동연구소 특별연구원. 2003년~2004년 미국 펜실바니아대학교(UPen) 객원 연구원. 1995년~현재 서울여자대학교 정보미디어대학 정보보호학 전공 교수