침입감내시스템의 생존성 모델

박 범 주[†] · 박 기 진[††] · 김 성 수[†††]

요 약

컴퓨터 시스템의 내/외부에 침입(attacks), 고장(failures)이 발생되더라도 적절한 방법으로 중요한 임무에(mission-critical) 해당한 역할을 수행하는 능력의 척도로 정의되는 생존성(survivability)에 대한 관심이 커지고 있다. 특히, 침입에 의해 시스템 일부가 손상(partially compromised) 되더라도, 최소한의 필수 서비스를 지속적으로 제공할 수 있게 해주는 침입감내시스템(intrusion tolerance system)의 설계시에 생존성 분석은 신뢰성(reliability), 가용도(availability)등과 같은 컴퓨터 시스템의 정량적 신인도(dependability) 분석과 함께 중요한 요소기술 중의 하나이다. 본 논문에서는 침입감내시스템의 방어능력을 평가하기 위해 자율컴퓨팅(autonomic computing)의 핵심 기술인 자가치유(self-healing) 메커니즘의 두 가지 요소(결함모델 및 시스템반응)를 활용하여, 주서버와 보조서버로 구성된 침입감내시스템의 상태천이(state transition)를 표현하였다. 또한, 침입감내시스템의 생존성, 가용도 및 다운타임 비용(downtime cost)을 정량적으로 정의한 후 시뮬레이션 실험 및 취약성(vulnerability) 공격에 대한 사례 연구를 수행하였다. 이를 통해 시스템의 신인도 향상 측면에서 초기상태에서의 침입감내능력 향상이 가장 중요한 요소임을 검증할 수 있었다.

키워드 : 생존성, 침입감내시스템, 취약성, 자가치유, 가용도

A Survivability Model of an Intrusion Tolerance System

Bumjoo Park[†] · Kiejin Park[††] · Sungsoo Kim[†††]

ABSTRACT

There have been large concerns about survivability defined as the capability of a system to perform a mission-critical role, in a timely manner, in the presence of attacks, failures. In particular, One of the most important core technologies required for the design of the ITS(Intrusion Tolerance System) that performs continuously minimal essential services even when the computer system is partially compromised because of intrusions is the survivability one of ITS included the dependability analysis of a reliability and availability etc. quantitative dependability analysis of the ITS. In this paper, we applied self-healing mechanism utilizing two factors of self-healing mechanism (fault model and system response), the core technology of autonomic computing to secure the protection power of the ITS and consisted of a state transition diagram of the ITS composed of a primary server and a backup server. We also defined the survivability, availability, and downtime cost of the ITS, and then performed studies on simulation experiments and two cases of vulnerability attack. Simulation results show that intrusion tolerance capability at the initial state is more important than coping capability at the attack state in terms of the dependability enhancement.

Key Words : Survivability, Intrusion Tolerance System, Vulnerability, Self-healing, Availability

1. 서 론

네트워크 기반 컴퓨터 시스템이 내/외부 침입에 의해 시스템 일부가 손상(partially compromised) 되더라도, 최소한의 필수 서비스를 지속적으로 제공할 수 있게 해주는 침입감내시스템(intrusion tolerance system)이 최근 관심을 끌고 있다. 이러한 현상은 방화벽, 백신 및 침입탐지(intrusion detection) 등의 다양한 보안 기술들이 이미 알려진 공격에 대해서는 탐지, 예방 및 치료가 가능하지만, 의도적이든 의도적이지 않던 아직까지 알려지지 않은 공격이나 결함에 대해서는 취약(vulnerable)하다는 단점에서 비롯되고 있다. 즉, 최근에 발견되는 공격 도구들이 은닉화(stealth), 분산화(distributed), 에이전트(agent)화 그리고 자동화(automation)의 특징을 가지고 있는 상황에서 이를 해결하기 위한 방법으로써, 예방 기술과 탐지 기술로 미처 발견하지 못한 네트워크 기반 컴퓨터 시스템 대상의 각종 공격이나 침입이 발생하는 경우에도 서비스의 정상적인 제공이 가능한 정보보호기술인 침입감내 기법이 활용되고 있는 것이다.

※ 이 논문은 아주대학교 2004년도 1학기 정착연구비 지원에 의하여 연구되었음. 본 연구는 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 정보통신부의 유비쿼터스컴퓨팅 및 네트워크 원천기반기술개발 사업의 지원에 의한 것임.
† 정 회 원 : 삼성전자 첨단기술연수소
†† 정 회 원 : 아주대학교 산업정보시스템공학부(교신저자)
††† 종신회원 : 아주대학교 정보통신전문대학원
논문접수 : 2005년 1월 8일, 심사완료 : 2005년 8월 18일

침입감내는 기존의 결함허용(fault-tolerant) 기술과 최근의 컴퓨터 보안기술(침입차단, 침입탐지 등)이 결합된 형태로 해당 시스템이 서비스 거부(DoS: Denial of Service) 공격과 같은 외부 침입이나 혹은 내부 침입에 의해 부분적으로 손상이 되더라도 중요한 임무에(mission-critical) 해당하는 서비스를 지속적으로 수행하는 개념이다[1]. 즉, 모든 악의적 공격을 반드시 실패하도록 보증하기보다는, 침입에 성공한 악의적인 몇몇 공격이 시스템 일부에 일정 부분의 손상을 가하더라도 신인도(dependability: reliability, availability, safety, survivability 등)를 갖는 침입 감내구조에 의해 서비스를 지속적으로 제공한다[2]. 이러한 침입 감내구조의 신인도를 향상시키기 위해서는 시스템이 제공하는 서비스의 품질 요구사항을 만족시키거나 서비스의 품질저하를 방지하면서 빠른 시간 안에 정상적인 서비스를 제공해야 하는데 이를 위해서는 예방(prevention), 탐지(detection)기술이 선행되고 최후에 중복 시스템(redundant system), 결함복구(fault recovery) 및 재활(rejuvenation)과 같은 감내(tolerance)기술이 적용되어야 한다.

특히, 신인도중에서 생존성(survivability)은 침임감내의 개념을 일관되게 반영하고 있는 척도(measure)이므로 침입감내시스템의 설계시 중요한 요소라 할 수 있다[3]. 그러나 네트워크 기반 컴퓨팅 환경에서 시스템의 생존성을 분석한 기존의 다양한 방법들을 살펴보면 생존성 정의에 활용된 성능척도가 20가지 이상으로써, 유일하게 적용될 수 있는 정의가 존재하지 않는다는 것을 알 수 있다[4]. 본 논문에서는 주서버와 보조서버로 구성된 Cold-Standby 침입감내시스템의 상태 천이 모델에 대해 기존의 가용도(availability) 개념이 응용된 생존성 척도를 도입함으로써, 시스템의 가용도와 생존성을 동시에 고려하는 신인도 향상 방안을 강구하였다.

한편, 침입감내시스템의 신인도 향상을 위해 자율컴퓨팅의 4가지 핵심 기술 중의 하나인 자가치유(self-healing) 메커니즘을 활용하는 접근 방법이 제시되고 있다[5]. 자가치유 기술은 결함허용 기법처럼 시스템의 신인도와 관련된 다양한 요소를 내포하고 있으나, 자가최적화(self-optimization), 자가구성(self-configure), 및 자가보호(self-protect) 등과 함께 시스템 내외부의 예상하지 못한 다양한 공격에 대해 적절히 대응할 수 있는 기술을 제공한다는 측면에서 기존의 결함허용 기법보다는 폭넓은 방식이라 할 수 있다[6]. 본 논문에서는 이러한 자가치유 메커니즘의 두 가지 요소(결함모델 및 시스템반응)를 침입감내시스템의 상태 천이 모델링에 활용함으로써, 자율컴퓨팅의 요소기술을 침입감내시스템에 접목할 수 있는 기반을 마련하였다. 그리고, 시뮬레이션 실험을 통해 침입감내시스템의 가용도, 다운타임 비용 및 공격상태에서의 평균잔류시간 비율의 데드라인을 고려한 생존성을 분석하고, 두 가지 경우의 취약성(vulnerability) 공격에 대한 사례 연구를 진행하였다.

2. 관련 연구

침입감내시스템 개발에 관한 연구중에서 Reynolds [7]의 HAQUIT(Hierarchical Adaptive Control of Quality of service for Intrusion Tolerance) 프로젝트의 경우, 오류 검출과 시스템 실패(failure)를 방지하기 위해 중복성과 다양성을 복합적으로 이용하며, 구조가 매우 간단하기 때문에 일반 COTS (Commercial Off-the-Shelf) 서버들로 비교적 쉽게 구현이 가능하다는 장점이 있는데 반해, 침입을 탐지하는 기능이 미약하고 확장하는데 한계가 있으며, 또한 사용자 요청이 응용 서버에 바로 전달되지 않기 때문에 시간적 추가 비용이 존재하는 문제점이 있다. 한편, 침입감내시스템의 결함허용 기능 강화를 위해 디자인 다양성(design diversity)을 채택하여, 주 서버와 보조서버가 각기 다른 운영체제와 웹서버 응용을 갖도록 구성하였으나, 두 서버가 Hot-standby 방식으로 연동되었기 때문에 외부 공격으로 인해 서버 모두 동시 손상될 수 있는 문제를 내포하고 있다.

Goseva-Popstojanova[8]에서는 침입 감내시스템이 외부공격 상황에서 갖추어야 할 동적인 이상거동을 상태천이도(state transition diagram)로 나타내고, 시스템이 가지는 취약성 및 위협 요소를 어떻게 모델링 할 수 있는가에 대한 침입감내 프레임워크에 관한 연구를 진행하였다. Wang[9]의 SITAR(Scalable Intrusion Tolerant Architecture)는 분산 서비스, 특히 COTS 서버를 위한 침입감내구조를 제시하고 있고, Wang [10]에서는 SITAR 시스템에 대해 다양한 상태천이도를 바탕으로 서비스 거부 공격 등 몇 가지 침입 유형별 정량적 성능 분석을 시도하였다. 그러나, SITAR 시스템의 경우 기존 COTS 서버의 변경없이 적용 가능하고 사용자에게도 투명하다는 장점이 있으나, 대량의 COTS 서버 공격에 대응 보장 한계와 COTS 서버 이외의 구성 요소들은 공격의 취약성을 갖고 있지 않아야 하는 조건이 있다. 또한, 침입 대응 과정을 담당하는 기능이 분산되어 있어서 과도한 지연 가능성 및 복잡한 구조로 인해 구현 비용 증가가 예상된다.

또한, Shelton[11]에서는 각각 분산 임베디드 시스템의 신인도 향상 및 시스템에 대한 비정상행위 탐지 문제를 해결하기 위해 자가치유 기술을 적용한 사례를 보여주고 있고, Knight[12]의 Willow 프로젝트는 침입감내시스템 개발의 사례로서 생존성을 지원해 주는 특징을 가지고 있다.

한편, 침입감내시스템의 성능분석을 위한 척도로써 생존성에 대한 정의 및 분석이 요구되고 있는데, Knight[13]에서는 생존성을 시스템이 갖추어야 하는 성능규격 이라는 관점에서 시스템에 활용될 환경적 요소를 고려한 엄격한 정의를 제안하고 있으며, 최근에는 기존의 신뢰성(reliability), 가용도 등의 신인도 척도를 복합적으로 고려하여 생존성을 분석하는 연구가 증가하고 있다. Liu[14]에서는 생존성 및 가용도를 향상하기 위해 가용도와 성능을 동시에 고려하는 프레임워크를 제안하고 있으며, Cowan[15]에서는 보안과 신뢰성을 함께 향상시키는 방법을 통해 생존성을 정의하고 있다. 본 논문에서는 침입감내시스템의 상태천이도 상에서 공격상태에서의 평균잔류시간 비율에 데드라인을 설정함으로써 기존의 가용도를 보다 엄격하게 적용하여 생존성을 산출하는 방법을 도입하였다.

3. 자가치유 메커니즘을 활용한 침입감내시스템

자가치유는 외부침입이나 시스템 내부문제에 의해 발생된 결함이나 오류를 자동적으로 감지(detect), 진단(diagnosis) 및 치유(repair) 함으로써 시스템의 오동작을 최소화하여 궁극적으로 시스템의 신인도를 향상시키는 자율컴퓨팅의 핵심 기술이다. 이러한 자가치유 기술이 시스템으로 완전하게 구현되기 위해서는 4가지 요소 - 결함 모델(fault model), 시스템 반응(system response), 시스템 완전성(system completeness) 및 디자인 문맥(design context) - 에 대한 정의가 필요하다[5].

결함모델은 시스템이 감내해야 하는 결함의 특성을 정의하는 것이며, 시스템 반응은 외부침입 등에 의한 결함의 감지, 결함에 대한 대응방법 및 복구전략에 대한 세부적인 정의에 해당한다. 예를 들면, SYN Flood 및 Smurfing과 같은 서비스 거부공격의 경우, DNS(Domain Name Server)같은 특정 서버에 악의적인 HTTP(Hypertext Transfer Protocol) 요청을 대량으로 발생시켜 시스템 리소스의 성능 저하를 야기하지만, 이러한 상황에서도 시스템의 필수 서비스 기능을 보장해 주는 점진적 기능 퇴화 개념이 시스템 반응의 요소에 포함될 필요가 있다. 한편, 시스템 완전성은 현실세계에서 시스템을 구현하는데 있어서 구조적인 불완전성을 극복하기 위해 갖추어야 할 요소에 대한 것이고, 디자인 문맥은 구현하고자 하는 시스템의 동질성(homogeneity) 및 선형성(linearity)을 확보하기 위한 자가치유 요소에 관한 것이다. 침입감내시스템이 자가치유적 기능을 갖게 하기 위해 위에서 기술한 4 가지 자가치유 구성요소 중에 결함 모델 및 시스템 반응에 관련된 세부 항목을 시스템의 상태천이도로 나타냈다.

결함모델의 경우, 서비스 거부 공격 및 다양한 취약성 노출이 초기 정상상태에 머물고 있는 시스템의 보안기능 저하를 야기시키고, 이로인해 궁극적으로 시스템이 다운되는 전과정에 적용하였다. 시스템 반응 측면에서는 외부공격에 대해 정상상태에서는 결함을 즉각적으로 감지하게 되고, 공격에 의해 시스템 성능이 저하되는 침입감내 상태에서는 재활을 통해 성능저하가 줄어들도록 하였으며, 고장상태에서는 여분의 서버로의 작업전이 및 즉각적인 복구를 통해 일정수준의 가용도 및 생존성이 보장되도록 구성하였다.

(그림 1)은 이러한 자가치유 구성 요소가 반영된 Cold-standby 침입감내시스템의 상태천이를 나타내고 있으며, 서비스 거부 공격에 대응하는 결함 모델의 세부요소와, 그에 상응하는 시스템 반응(결함감지(fault detection), 기능퇴화(degradation), 결함반응(fault response) 및 결함복구 등의 세부요소를 11가지 상태변화에 표현하였다. 침입감내시스템 모델링을 위해 적용한 가정은 다음과 같다.

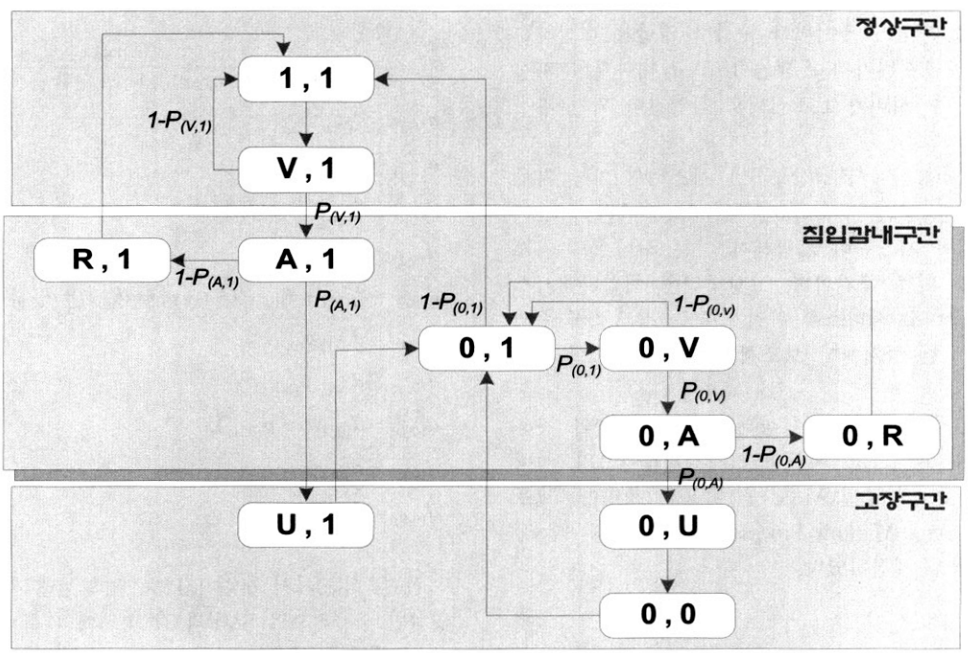
(1) 주-보조서버 사이의 작업전이 메커니즘은 Cold-standby 방식을 따른다.

(2) 침입감내시스템의 각 상태에 머무를 시간은 일반 분포를 따른다.

(3) 시스템은 초기상태에 정상 가동되며, 초기상태에 있을 때만 칩입이 가능하다.

(4) 주-보조서버 사이의 작업전이 이후 보조서버가 정상상태(0,1) 에서만 주서버로 작업전이 된다.

(1)의 의미는 동시에 두 대의 서버가 다운되는 것을 방지



상태 (주서버, 보조서버) , V : 취약상태, A : 공격상태, R : 재활상태

(그림 1) 침입감내시스템의 상태천이도

하기 위해 한 대가 다운되었을 경우 즉시 여분의 서버가 다운된 서버의 기능을 대신하게 되는 가정이고, (2)는 불확실한 외부공격에 대해 침입감내시스템의 특성상 각 상태에 머무는 시간을 지수분포와 같은 특정분포를 가정하는 것이 비현실적임을 반영하고 있다. (3)은 가장 보편적인 시스템 상태를 기준으로 모델링하기 위해 시스템이 정상 가동되는 상태에만 외부공격이 가능하도록 도입된 가정이다. 즉, 공격유형의 다양성은 크게 고려하지 않았다. (4)는 주서버의 작업전이 시기에 대한 가정으로써 주서버가 다운된 이후 보조서버의 6가지 상태가 존재하는데, 이때 주서버로의 작업전이는 보조서버가 정상상태에서 가능하다는 가정이다. 이는 일단 보조서버가 주서버의 역할을 수행하도록 하기위해 공격이 진행되는 동안에 주서버의 역할을 배제하고 침입감내 기능을 자체적으로 수행할 수 있도록 구성하기 위해서 도입되었다.

주서버와 보조서버가 모두 정상적으로 동작하는 상태 (1,1)에서 취약성이 노출되면, 침입 감내시스템은 (V,1)로 천이된다. 침입감지 모듈이 네트워크 트래픽 및 IP 주소 분석 등을 통해 모든 취약성 공격(attacks)을 방어하면 일정시간 이후 초기상태로 복원되지만, 그렇지 못할 경우 $P_{(V,1)}$의 확률로 주 서버가 공격 당하는 상태 (A,1)로 바뀐다. 주서버 공격 상태가 일정시간 지속되면 시스템 손상이 누적되며, 이때 침입 진단 모듈이 시스템의 CPU 부하 및 메모리 상태를 분석하여, 유의할 수준의 성능저하가 $1-P_{(A,1)}$의 확률로 감지될 경우 주서버를 재활상태 (R,1)로 전이시키지만, 성능저하를 감지하지 못할 경우 감지불능(undetected) 상태인 (U,1)로 전이되어 최종적으로 보조서버가 주서버 기능을 대신하도록 (0,1) 상태로 작업전이 된다. 외부 공격에 의해 주-보조서버가 동시에 다운되는 상태를 방지하기 위해 Cold-standby 구성을 채택하였으며, 이 경우 작업전이에 필요한 시간이 길어지게 된다. 보조서버가 주서버 역할을 대신하는 (0,1) 상태에서 보조서버가 다운되는 (0,0) 상태까지의 과정은 초기상태에서 주 서버가 보조서버로 작업전이 되는 과정과 동일하다.

전체적으로 (그림 1)에서 정상구간은 시스템의 기능 저하가 전혀 일어나지 않은 구간이고, 침입감내구간은 일정한 손상이 존재하지만 시스템이 제공해야 하는 서비스는 지속적으로 수행되고 있는 구간이며, 고장구간은 침입감내시스템 작동에도 불구하고 서비스를 하지 못하는 상태로써 주서버가 회복되지 못한 상태에서 보조서버까지 서비스 불가한 상태이다.

제안된 침입감내시스템의 평형상태(steady-state)의 가용도를 계산하기 위해 식(1)의 확률과정을 정의하였으며, 서비스 시간이 일반적인 분포인 M/G/1을 적용한 세미마르코프 프로세스(SMP: Semi-Markov Process) 분석을 통해 각 상태에 머무는 확률을 계산하였다.

$$X(t): \ t > 0 \tag{1}$$
$$X_S = \{ (1,1), (V,1), (A,1), (R,1), (U,1), (0,1), (0,V), (0,A), (0,R), (0,U), (0,0) \}$$

(그림 1)에 표시된 모든 상태는 상호 도달 가능하므로 더 이상 줄일 수 없으며, 주기성을 갖지 않고 한정된 시간 내에 특정 상태로 회귀할 수 있으므로 Erogodicity(aperiodic, recurrent, nonnull) 특성을 만족하게 된다. 따라서, 침입감내시스템 각 상태에 대한 SMP의 안정상태 확률이 존재하고 해당 SMP는 각 상태에서의 전이확률을 이용한 임베디드(embedded) 이산 마르코프 체인(DTMC: Discrete-time Markov Chain)에 의해 유도할 수 있다.

SMP의 각 상태에서의 평균 잔류시간(mean sojourn time)을 h_i라 하고, DTMC 평형상태 확률을 d_i라 할 때, SMP의 각 상태에 대한 평형상태 확률 π_i를 식(2)와 같이 나타낼 수 있다[16].

$$\pi_i = \frac{d_i h_i}{\sum_j d_j h_j}, \quad \text{i,j} \in X_S \tag{2}$$

이때, DTMC의 평형상태 확률 d_i들은 식(3)과 식(4)의 관계를 갖게 된다.

$$\vec{d} = \vec{d} \cdot P \tag{3}$$

$$\sum_i d_i = 1 \quad i \in X_S \tag{4}$$

여기서, $\vec{d} = [\, d_{(1,1)}\ d_{(V,1)}\ d_{(A,1)}\ d_{(R,1)}\ d_{(U,1)}\ d_{(0,1)}\ d_{(0,V)}\ d_{(0,A)}\ d_{(0,R)}\ d_{(0,U)}\ d_{(0,0)}\,]$이며, P는 (그림 1)의 X_S의 각 상태에서의 전이확률 $p_{(i,j)}$에 의해 표현되는 DTMC 전이확률 행렬(transition probability matrix)이다. 이들로부터 DTMC의 평형상태 확률을 구하면 식(5)와 같다.

$$\begin{aligned}
d_{(1,1)} &= \frac{1-p_{(0,1)}}{2(1+p_{(V,1)})(1-p_{(0,1)})+p_{(V,1)}p_{(A,1)}(1+p_{(0,1)}+2p_{(0,1)}p_{(0,V)}+p_{(0,1)}p_{(0,V)}p_{(0,A)})} \\
d_{(V,1)} &= d_{(1,1)} \\
d_{(A,1)} &= d_{(V,1)}p_{(V,1)} \\
d_{(R,1)} &= d_{(A,1)}(1-p_{(A,1)}) \\
d_{(U,1)} &= d_{(A,1)}p_{(A,1)} \\
d_{(0,1)} &= d_{(U,1)}+d_{(0,V)}(1-p_{(0,V)})+d_{(0,R)}+d_{(0,0)} \\
d_{(0,V)} &= d_{(0,1)}p_{(0,1)} \\
d_{(0,A)} &= d_{(0,V)}p_{(0,V)} \\
d_{(0,R)} &= d_{(0,A)}(1-p_{(0,A)}) \\
d_{(0,U)} &= d_{(0,A)}p_{(0,A)} \\
d_{(0,0)} &= d_{(0,U)}
\end{aligned} \tag{5}$$

한편, 식(5)에서 구한 DTMC 평형상태 확률을 식(2)에 대입하면 궁극적으로 SMP의 각 상태에 대한 평형상태 확률 π_i를 구할 수 있으며, 평형상태에서 시스템의 가용도는 상태천이도상의 X_S 각 상태에서 (U,1), (0,U) 및 (0,0) 상태에 있을 확률을 배제한 경우로 식(6)과 같이 정의된다.

$$Availability = 1-(\pi_{(U,1)}+\pi_{(0,U)}+\pi_{(0,0)}) \quad (6)$$

하지만 식(6)에서는 시스템의 성능이 전혀 고려되고 있지 못하며, 단지 시스템이 고장상태에 머무는 경우만을 비가용 상태로 간주하고 있다. 즉, (그림 1)의 상태천이도에서 시스템이 정상구간 및 침입감내구간내에 머물러 있다면 각 상태에 머무는 시간(잔류시간)에 관계없이 정상적인 서비스가 제공되는 구간으로 파악하게 된다. 그러나, 일반적으로 침입감내구간의 경우 시스템이 취약성에 노출되거나 외부공격에 의해 성능저하가 진행되고 있는 상태이므로, 공격상태가 일정시간 이상 지속되면 가용상태로 판단하기는 현실성이 떨어진다고 할 수 있다. 따라서, 공격상태에서의 잔류시간 비율이 일정수준(데드라인)을 넘어서는 경우, 비록 침입감내구간에 머물고 있다 할지라도 가용하다고 말하기는 어렵다. 즉, (A,1)과 (0,A) 상태에서는 진단모듈이 시스템의 성능저하를 제한된 시간내에 감지하지 못할 경우 고장구간으로 즉시 전이되므로 잔류시간의 정도가 시스템 가용성 및 생존성에 중요한 요소가 된다. 그러므로, 침입감내시스템의 상태천이도에서 각 상태에 머무는 잔류시간을 고려한 생존성 척도가 더욱 현실적인 시스템 성능의 판단 기준이라 할 수 있으며, 이러한 생존성 척도는 식(6)의 가용도 정의를 확장하여 아래와 같이 유도하였다.

주서버 및 보조서버 중 한 대가 공격상태에 놓인 경우((A,1),(0,A)) 시스템이 생존해 있다고 판단할 수 있는 평균 잔류시간 비율($d_i h_i$)의 데드라인을 D^*라 할 때 해당 상태에서의 시스템의 생존성 여부를 판정하기 위한 지시변수(indicator variable) Y_i(i = (A,1),(0,A))의 값을 다음 기준으로 결정한다.

$$d_i\ h_i \le D^* : Y_i = 0,\ d_i\ h_i > D^* : Y_i = 1$$

위에서 결정된 지시변수를 활용하여 침입감내시스템의 생존성 척도를 식(7)과 같이 정의하였다.

$$Survivability = Availability - (Y_{(A,1)} \times \pi_{(A,1)} + Y_{(0,A)} \times \pi_{(0,A)}) \quad (7)$$

침입감내시스템의 다운타임 비용은 가용도 및 생존성 관점의 비용을 전체 가동시간(T)과 서비스 불가능한 상태에서의 평형상태 확률에 의해 식(8)과 식(9)와 같이 나타낼 수 있다.

$$Cost\_Avail(T) = [C_\alpha \times \pi_{(U,1)} + C_\alpha \times \pi_{(0,U)} + C_\beta \times \pi_{(0,0)}] \times T \quad (8)$$

$$Cost\_Surv(T) = Cost\_Avail(T) + C_\gamma \times [Y_{(A,1)} \times \pi_{(A,1)} + Y_{(0,A)} \times \pi_{(0,A)}] \times T \quad (9)$$

여기서, C_α는 침입감내구간에서 고장구간으로 전이된 상태((U,1),(0,U))에서의 단위시간당 비용이고, C_β는 주서버와 보조서버가 모두 고장인 경우의 단위시간당 비용이며, C_γ는 침입감내구간 중 (A,1)과 (0,A) 상태에서 Y_i=1인 경우의 단위시간당 비용이다.

4. 성능 평가

4.1 기본 SMP 모델의 시뮬레이션 분석

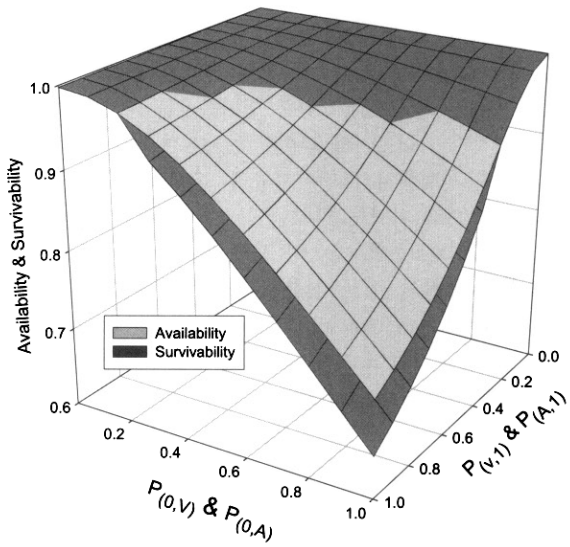
침입감내시스템의 SMP 모델을 분석하기 위해서는 전이확률과 각 상태에서의 평균 잔류시간, 생존성 분석과 관련된 데드라인 및 다운타임 비용 상수에 대한 파라미터 설정이 이루어져야 한다. 본 논문에서는 4가지 파라메타에 대해 <표 1>의 설정값을 기준으로 시뮬레이션을 수행하였다[17]. 각 상태에서의 평균 잔류시간은 일반분포를 따르므로 설정된 값은 상대적인 차이로서의 의미만 존재하며, 상태천이도에 나타난 5개 분기점에서의 전이확률이 침입감내시스템의 가용도에 독립적으로 미치는 영향을 분석하기 위해 0과 1사이의 값을 설정하였다. 한편, 생존성 분석을 위한 데드라인(D^*) 값은 공격상태에서의 평균 잔류시간 비율의 평균값(AMSTR: Average of Mean Sojourn Time Ratio)인 $(d_{(A,1)}\ h_{(A,1)} + d_{(0,A)}h_{(0,A)})/2$을 기준으로 설정하였다. 그리고 다운타임 비용 산출을 위해 가동시간을 1년으로 지정하였으며, C_α보다는 주서버와 보조서버가 모두 고장상태인 경우의 단위비용인 C_β를 10배 크게 설정하였으며, 생존성 척도 관점에서 비가용상태의 단위비용인 C_γ는 C_α와 동일한 수준에서 50배까지 변화해 가면서 시뮬레이션 분석을 수행하였다.

〈표 1〉 시뮬레이션 파라미터

입력변수	설정값
평균 잔류시간	$h_{(1,1)}$=50, $h_{(V,1)}$=30, $h_{(A,1)}$=25, $h_{(U,1)}$=50, $h_{(R,1)}$=20, $h_{(0,1)}$=50, $h_{(0,V)}$=30, $h_{(0,A)}$=25, $h_{(0,R)}$=20, $h_{(0,U)}$=50, $h_{(0,0)}$=50
전이확률	$0 < P_{(V,1)}, P_{(A,1)}, P_{(0,1)}, P_{(0,V)}, P_{(0,A)} < 1$
데드라인	평균잔류시간비율의 평균값 / 3 $< D^* <$ 평균잔류시간비율의 평균값
다운타임비용상수	C_α = 10 unit, C_β = 100 unit, 10 unit $< C_\gamma <$ 500 unit, T = 1 year

(그림 2)는 외부의 악의적인 공격상황에서 주서버와 보조서버가 각각 취약성을 감지 못하고 공격을 당하면서 시스템의 성능이 저하되는 과정에 따른 시스템의 가용도 및 생존성 변화 추이를 보여주고 있다. 주서버에 관한 전이확률인 $P_{(V,1)}$과$P_{(A,1)}$이 동시에 증가하거나 마찬가지로 보조서버에 관련된 $P_{(0,V)}$와 $P_{(0,A)}$가 증가하면서 가용도 및 생존성이 점진적으로 저하되는 현상을 보이고 있다. 전이확률이 0.2보다

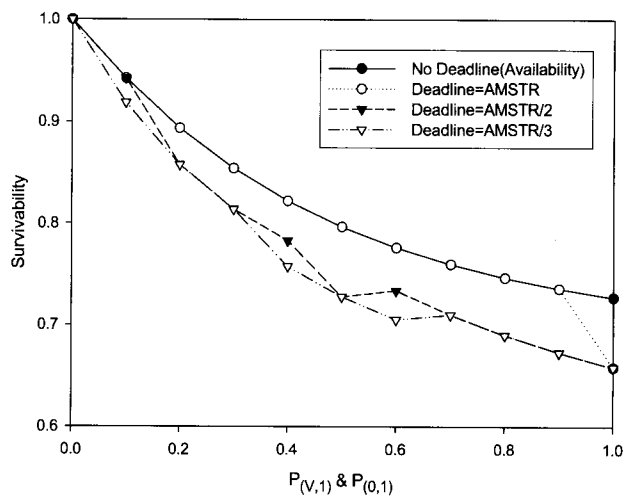
작은 구간에서는 가용도와 생존성의 차이가 미미하나, 0.2이상의 구간에서는 그 차이가 점진적으로 증가하게 되고 전이확률이 모두 1인 경우에 약 10%의 차이를 보이고 있다. 이러한 현상은 주서버와 보조서버가 공격에 노출된 상태에서의 잔류시간 비율이 증가하여 데드라인를 넘어서는 경우가 증가하면서 가용도에 비해 생존성 척도가 상대적으로 크게 감소하기 때문이다. 따라서, 생존성 감소를 방지하기 의해 외부공격이 진행되는 상황에서 (A,1)와 (0,A) 상태에서의 잔류시간 비율을 감소시킬 수 있는 침입감내시스템의 진단성능이 필요하다고 할 수 있다.



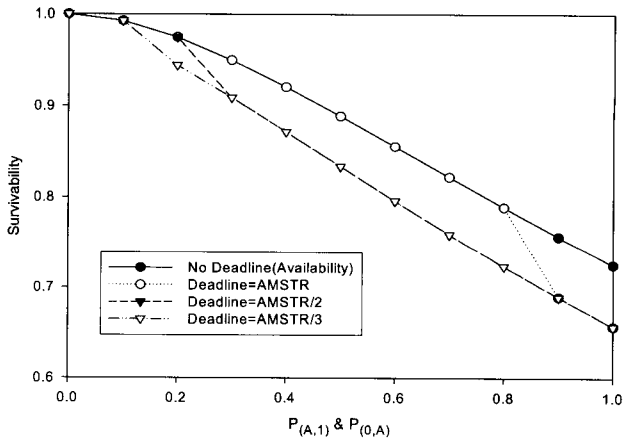
(그림 2) 주-보조서버의 전이확률 변화에 따른 가용도 및 생존성 분석

(그림 3)은 침입감내시스템의 초기대응 능력이 생존성 변화에 미치는 영향을 파악하기 위해 주서버와 보조서버가 취약성에 노출될 확률($P_{(V,1)}$,$P_{(0,1)}$)의 변화에 따른 시스템의 생존성 변동추이를 보여주고 있고, (그림 4)는 공격에 노출된 상황에서 시스템의 대응 능력을 판단하기 위해, 두 서버에 대한 공격 성공 확률($P_{(A,1)}$,$P_{(0,A)}$)의 변화에 따른 생존성 변화를 나타내고 있다. 잔류시간 비율의 데드라인이 없는 경우는 생존성이 가용도와 동일한 값을 갖게되고, 데드라인이 보다 엄격하게 적용될수록 생존성 척도가 저하되는 경향이 나타나고 있다.

(그림 3)과 (그림 4)를 통해 제안된 Cold-standby 침입감내시스템을 구성하면 주-보조서버가 각각 공격상황 및 취약한 상황에 노출된 초기단계에서 시스템의 이상거동을 감지할수록 생존성이 극대화된다는 것을 알 수 있다. 한편, $P_{(A,1)}$과 $P_{(0,A)}$가 0에 가까운 값일 경우 생존성이 저하되는 경향이 둔화되는 현상을 보이고, $P_{(V,1)}$과 $P_{(0,1)}$의 경우 초기에는 급격한 감소를 보이지만 1에 근사할수록 생존성 감소가 둔화되는 경향을 보이고 있다. 그 이유는 시스템이 초기에 취약한 상황에 쉽게 노출되었다 하더라도 주-보조서버가 공격상황에 노출된 상태인 (A,1)과 (0,A)에서 침입감내시스템의 진단기능을 통해 유의할 만한 성능저하를 즉각적으로 감지할 수 있다면, 재활모드로의 전환을 통해 초기상태로 복귀시킴으로써 생존성을 보장할 수 있기 때문이라 판단된다. 그리고, $P_{(A,1)}$과 $P_{(0,A)}$가 1일 경우의 생존성이 $P_{(V,1)}$ 과 $P_{(0,1)}$이 시스템에 가장 불리한 값을 가진 경우의 생존성 값과 거의 근사한 결과를 보이고 있는데 이는 초기상태에서 이상거동을 감지하지 못하더라도 단일시스템에 비해 Cold-standby 침입감내시스템의 구조가 외부의 악의적 공격 상황에서도 작업전이, 복구 등의 다양한 감내 기능에 의해 시스템이 서비스 불가하거나 다운되는 상태에 놓일 확률을 최대한 줄여줌으로써 생존성 저하를 방지해 주기 때문이라 할 수 있다.



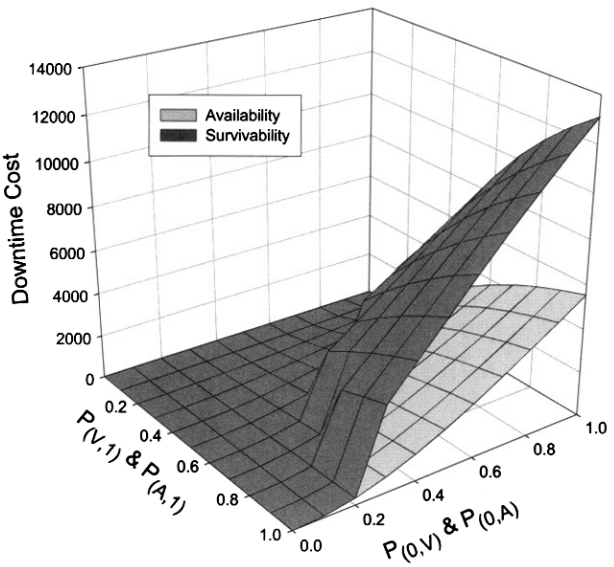
(그림 3) 초기대응능력 및 데드라인 변화에 따른 생존성 분석



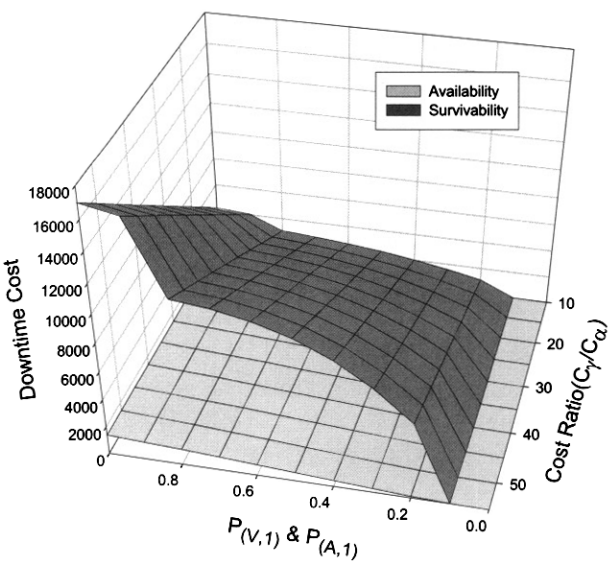
(그림 4) 공격대응능력 및 데드라인 변화에 따른 생존성 분석

(그림 5)는 주서버에 관한 전이확률인 $P_{(V,1)}$과 $P_{(A,1)}$, 그리고 보조서버에 관련된 $P_{(0,V)}$와 $P_{(0,A)}$의 변화에 따른 시스템의 다운타임 비용을 가용도 및 생존성 척도 두가지 경우에 대해 보여주고 있다. 전이확률의 크기가 1에 근접할수록 다운타임 비용이 급속하게 증가하게 되며, 생존성에 대한 다운타임 비용은 가용도에 대한 경우보다 Cost Ratio(C_γ/C_α)에 따라 증가하게 된다. 이는 침입감내구간내의 공격상태에서 잔류시간 비율이 데드라인을 넘어서는 경우에 생존성이 감소하게 되고, 다운타임 비용은 그 감소량에 대해 C_γ값에 비례하여 증가되기 때문이다.

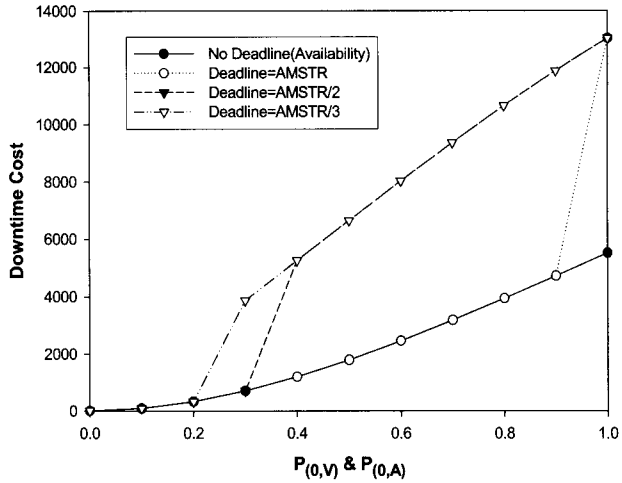
(그림 6)은 주서버가 취약성과 공격에 노출된 상황에서 Cost Ratio의 증가함에 따라 다운타임 비용이 어떻게 변화하는지를 가용도와 생존성 척도의 경우를 비교하여 보여주고 있다. Cost Ratio가 증가하더라도 시스템이 초기상태에서 취약성 공격에 즉시 대응하거나 본격적인 외부 공격에 노출된 상황에서도 재활모드에 의해 초기상태로 즉시 전환할 수 있다면, 다운타임 비용 증가는 미미한 경향을 보임을 알 수 있다. 그러나 $P_{(V,1)}$과$P_{(A,1)}$이 커지면 Cost Ratio에 따라 다운타임 비용이 급격하게 증가하게 된다. 따라서, 다운타임 비용 증가를 방지하게 위해서는 침임감내시스템의 초기대응능력을 향상시키거나, 생존성 척도 관점에서 비가용상태의 단위비용인 C_γ를 줄일 수 있는 시스템 구조설계가 중요한 요소라 할 수 있다.



(그림 5) 주-보조서버의 전이확률 변화에 따른 다운타임 비용 분석



(그림 6) $P_{(V,1)}$,$P_{(A,1)}$ 및 Cost Ratio 변화에 따른 다운타임 비용 분석



(그림 7) $P_{(0,V)}$,$P_{(0,A)}$ 및 데드라인 변화에 따른 다운타임 비용 분석

(그림 7)은 보조서버에 관한 전이확률인 $P_{(0,V)}$와 $P_{(0,A)}$가 증가할때의 다운타임 비용의 변동추이를 데드라인 변화에 따라 비교한 결과이다. 전이확률이 0.2보다 작은 경우, 잔류시간 비율의 데드라인 유무에 관련없이 다운타임 비용의 증가가 동일한 경향을 보이고 있으나, 0.2보다 커지면 데드라인의 적용이 엄격해 지면서 다운타임 비용은 단계적으로 증가함을 알 수 있다. 따라서, 시스템의 안정성 확보를 위해 데드라인을 엄격하게 가져가야 한다면, 외부공격에 대한 시스템의 초기대응 능력을 높이는 것이 필요하다.

침입감내시스템의 생존성 및 다운타임 비용 분석을 종합해 보면, 초기상태의 침입감내 능력이 공격상태에서의 대응능력에 비해 가용도, 생존성 증가 및 다운타임 비용 감소측면에서 상대적으로 더 중요함을 알 수 있다. 한편, 주서버가 공격에 노출되어 고장상태에 이르더라도 작업전이를 통해 보조서버가 즉각적인 초기대응을 하게 된다면, 주서버 고장으로 인한 생존성 및 다운타임 비용 손실정도를 어느 정도 상쇄시킬 수 있다. 특히, 시스템의 안정정 확보를 위한 잔류시간 비율의 데드라인을 엄격하게 설정하는 것이 중요하다고 할 때, 취약성 공격에 대한 주-보조서버의 초기 대응능력이 무엇보다 중요함을 알 수 있다.

4.2 취약성 공격 사례별 분석

침입감내시스템의 기본 SMP모델을 실제 공격 사례에 적용하기 위해Goseva-Popstojanova[8]에서 제시한 두 가지 공격 유형인 Active Server Page(ASP) 취약성 및 Common Gateway Interface(CGI) 취약성을 채택하여 분석을 수행하였다.

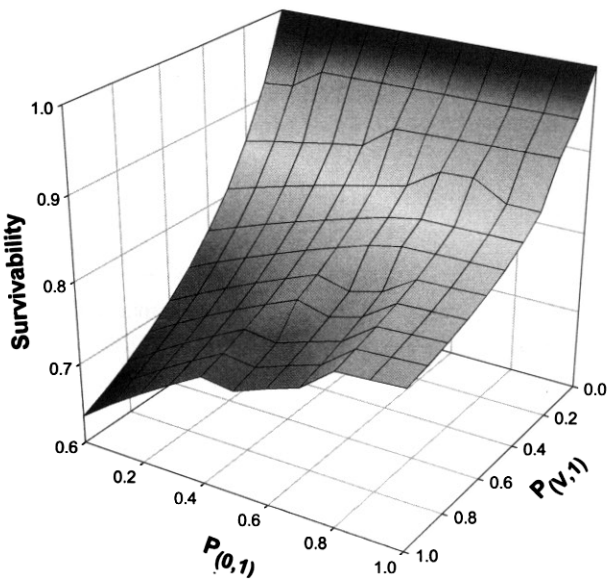
첫번째 사례로써 ASP 취약성은 Internet Information Server (IIS)의 파일 중에서 showcode.asp가 악의적인 공격자에게 노출되는 경우 발생되는 취약성 공격 유형이다. 즉, 공격자가 특정 URL(http://target/msadc/samples/SELECTOR/showcode.asp?source=/path/file)을 활용하여 웹서버의 소스파일을 임의대로 볼 수 있게 됨으로써 기밀성(confidentiality)에 심각한 손상을 야기시키게 된다. 이 경우 주-보조서버가 각각 공격상태에서 진단모듈에 의해 침입을 능동적으로 감지하기

어렵기 때문에 재활상태로 진입할 수 없게 되므로 $P_{(A,1)}$과 $P_{(0,A)}$가 1인 특수한 사례에 해당한다.

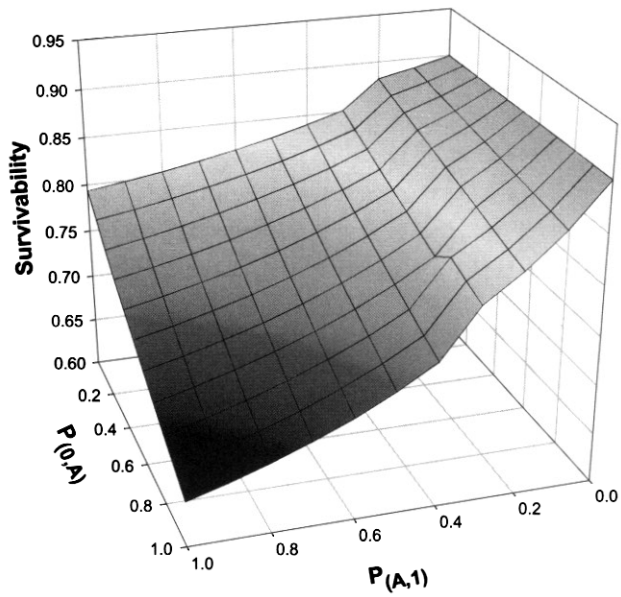
(그림 8)은 이러한 ASP 취약성 경우에 대해 SMP 모델 적용 결과를 분석하기 위해 $P_{(A,1)}$ 과 $P_{(0,A)}$를 1로 고정시킨 후 $P_{(V,1)}$과 $P_{(0,1)}$의 값을 변화시켜 가면서 시스템의 생존성 변화를 분석한 결과를 보여주고 있다. 이 경우 (그림 2)의 결과와 마찬가지로 주-보조서버가 각각 공격상황 및 취약한 상황에 노출되기 전의 초기상태에서 시스템의 이상거동을 감지할수록 생존성이 극대화된다는 것을 알 수 있다. 그러나, (그림 8)에서 생존성의 최소값은 기본 SMP모델의 경우에 비하여 $P_{(V,1)}$=1과 $P_{(0,1)}$=0일 때 약 10% 정도 더 작아지게 된다. 그 이유는 주-보조서버가 각각 (R,1) 상태 및 (0,R) 상태를 통한 침입감내 기능을 활용하지 못한 것으로 인해 야기되는 생존성 척도의 손실치라 판단된다. 한편, (그림 8)의 3차원 곡면상에 불연속면이 발생되는 것은 잔류시간 비율의 데드라인이 침입감내구간내의 공격상태에 적용되는 과정에서 나타나는 현상이다.

두번째 사례로써 CGI 취약성은 윈도우즈 NT 계열의 프락시 서버가 CGI 스크립트로 도스 방식의 파일을 사용함으로써 야기된 취약성이며, 네트웍상의 원격 공격자가 특정 URL을 이용하여 배치 파일을 도용함으로써 시스템 파일이나 사용자 계정등의 중요파일을 수정할 수 있게 되기 때문에 기밀성 및 무결성(integrity)에 심각한 문제를 야기시키게 된다. 그런데, 이 경우 시스템이 공격상태에 진입하기 전에 URL 필터링과 같은 취약성 감지 기능을 활용하기 어렵기 때문에 주-보조서버가 각각 (V,1) 및 (0,V) 상태에서 초기상태로 회복하지 못하고 바로 (A,1)과 (0,A)로 진행된다 ($P_{(V,1)}$=$P_{(0,V)}$=1).

(그림 9)은 CGI 취약성에 대한 생존성 분석 결과를 보여주고 있다. $P_{(A,1)}$과 $P_{(0,A)}$가 커지면서 생존성은 점진적으로



(그림 8) ASP 취약성에 대한 생존성 분석



(그림 9) CGI 취약성에 대한 생존성 분석

저하되게 되고, $P_{(A,1)}$=$P_{(0,A)}$=1 일 경우 가용도가 가장 작은 값을 갖게 되는데 기본 SMP 모델의 경우에 비하여 약 13% 정도 줄어든 결과를 보여주고 있다. 이러한 현상은 주-보조서버가 각각 (V,1) 상태 및 (0,V) 상태에서의 침입감내 기능을 활용하지 못함으로 인해 야기된 생존성 저하가 극대화된 것이라 할 수 있으며, 두 가지 취약성 공격 사례적용 결과를 비교해 볼 때 초기상태의 침입감내 능력이 공격상태에서의 대응능력에 비해 생존성 측면에서 상대적으로 더 중요함을 알 수 있다.

5. 결론 및 향후 연구방향

본 논문에서는 침입 감내시스템의 가용도, 생존성 및 다운타임 비용을 분석하기 위해 자율컴퓨팅의 핵심 기술인 자가치유 메커니즘을 접목시키는 방안을 제시하였다. 주서버와 보조서버가 각 1대인 Cold-standby 방식의 침입감내시스템을 11가지 상태로 정의한 후 각 상태에서의 전이 확률 및 평균 잔류시간을 통해 Discrete-Time Markov Chain 평형상태 확률 및 Semi-Markov Process 평형 상태 확률을 계산하여 일반적인 시스템의 가용도를 정의하였고, 이를 바탕으로 평균잔류시간 비율의 평균값에 데드라인을 적용한 시스템의 생존성을 계산하여 기본 Semi-Markov Process 모델에 대한 시뮬레이션 및 두 가지 취약성 공격 사례(active server page vulnerability, common gateway interface vulnerability) 분석을 통해 생존성 향상과 다운타임 감소 방안을 기술하였다. 향후, 본 논문에서 고려한 자가치유 메커니즘의 두 가지 요소 이외에 시스템 완전성 및 디자인 문맥 등을 함께 고려한 모델링을 통해 침입감내시스템의 신인도를 향상시킬 수 있는 방안을 연구할 예정이다. 아울러, 침입

감내시스템의 생존성 분석를 위해 가용도 이외에 시스템의 고유특성을 보다 폭넓게 반영하는 척도를 개발하여 적용할 계획이다.

참 고 문 헌

[1] F. Wang, R. Uppalli, and C. Killian, "Analysis of Techniques for Building Intrusion Tolerant Server Systems," Pro- ceedings of Military Communications Conference, pp.729- 734, Oct., 2003.

[2] A. Avizienis, J. Laprie, and B. Randell, "Fundamental concepts of dependability," 3rd Information Survivability Workshop, pp.7-12, Oct., 2000.

[3] R. Ellison, et al., "Survivable Network Systems: An Emerging Discipline," Proceedings of the 11th Canadian Information Technology Security Sysposium, May, 1999.

[4] V. Westmark, "A Definition for Information System Survivability," Proceedings of the 37th Annual Hawaii International Conferences on System Sciences, Vol.9, No.9, pp.90303a, Jan., 2004.

[5] P. Koopman, "Elements of the Self-Healing System Problem Space," Workshop on Architecting Dependable Systems, pp.31-36, May, 2003.

[6] D. Chess, C. Palmer, and S. White, "Security in an Autonomic Computing Environment," IBM Systems Journal, Vol.42, No.1, pp.107-118, 2003.

[7] J. Reynolds, et al., "On-line Intrusion Detection Attack Prevention Using Diversity Generate-and-Test, and Generali- zation," Proceedings of the 36th Annual Hawaii International Conferences on System Sciences, pp.335-342, Jan., 2003.

[8] K. Goseva-Popstojanova, et al., "Characterizing Intrusion Tolerant Systems using a State Transition Model," DARFA Information Survivability Conference and exhibition, Vol.2, pp.211-221, June, 2001.

[9] F. Wang, et al., "SITAR: A Scalable Intrusion-Tolerant Architecture for Distributed Services," Proceedings of the Foundations of Intrusion Tolerant Systems, pp.359-367, 2003.

[10] D. Wang, B. Madan, and K. Trivedi, "Security Analysis of SITAR Intrusion Tolerance System," Proceedings of the ACM Workshop on Survivable and Self-Regenerative Systems, pp.23-32, Oct., 2003.

[11] C. Shelton, P. Koopman, and W. Nace, "A Framework for Scalable Analysis and Design of System-Wide Graceful degradation in distributed Embedded Systems," Eighth IEEE International Workshop on Object-oriented Real-time Dependable Systems, pp.156-163, Jan., 2003.

[12] J. Knight, et al, "The Willow Architecture: Comprehensive Survivability for Large-Scale Distributed Applications," submitted to: The International Conference on Dependable Systems and Networks, June, 2002.

[13] J. Knight, K. Strunk, and K. Sullivan, "Towards a Rigorous Definition of Information System Survivability," Pro- ceedings of the DARPA Information Conference and Exposition, pp.78-89, April, 2003.

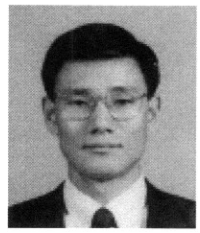
[14] Y. Liu and K. Trivedi, "A general Framework for Network Survivability Quantification," Proceedings of the 12th GI/ITG Conference on Measuring, Modelling and Evaluation of Computer and Communication Systems, pp.369-378, Sep., 2004.

[15] C. Cowan and Immunix Inc., "Survivability: Synergizing Security and Reliability," Sep., 2003.

[16] K. Trivedi, "Probability and Statistics with Reliability Queueing and Computer Science Applications," John Wiley & Sons, Inc., pp.472, 2002.

[17] B. Madan, et al., "Modeling and Quantification of Security Attributes of Software Systems," International Conference on Dependable Systems and Networks, pp.505-514, June, 2002.

박 범 주

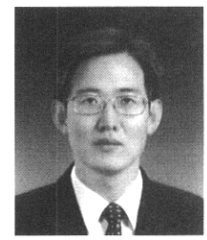


e-mail : bumjoo@samsung.com
1989년 서울대학교 조선공학과(공학사)
1992년 포항공과대학교 산업공학과 (공학석사)
1992년~1995년 삼성종합기술원 그룹CAE센타 주임연구원
1995년~1998년 삼성전자 소그룹 전략기획총괄 첨단기술센타 과장
1998년~현재 삼성전자(주) 첨단기술연수소 차장
2002년~현재 아주대학교 공과대학 정보통신전문대학원 박사과정
관심분야 : 결함허용, 성능분석, 클러스터컴퓨팅, 소프트웨어재활, 침입감내시스템

박 기 진

e-mail : kiejin@ajou.ac.kr
1989년 한양대학교 산업공학과(공학사)
1991년 POSTECH 산업공학과(공학석사)
1991년~1997년 삼성전자 선임연구원
1997년~2001년 아주대학교 컴퓨터공학과(공학박사)
2001년~2002년 한국전자통신연구원 선임연구원
2002년~2004년 안양대학교 컴퓨터학과 전임강사
2004년~현재 아주대학교 산업정보시스템공학부 조교수
관심분야 : Dependable Embedded Computing, Intrusion Tolerance Systems, Cluster Computing

김 성 수



e-mail : sskim@ajou.ac.kr
1982년 서강대학교 전자공학과(공학사)
1984년 서강대학교 전자공학과(공학석사)
1995년 Texas A&M University 전산학과 (공학박사)
1983년~1996년 삼성전자 수석연구원
2002년~2003년 Texas A&M University 교환교수
1996년~현재 아주대학교 정교수
관심분야 : Dependable System & Network, Autonomic Computing, Ubiquitous Computing & Network