S/W 시스템의 보안속성 모델링 사례연구

박범주[0] 김성수
아주대학교 정보통신전문대학원 정보통신공학과
bumjoo@samsung.com[0] sskim@ajou.ac.kr

A Study on Modeling Security Attributes of S/W System

BumJoo Park[0] Sungsoo Kim
Graduate School of Information and Communication, Ajou University

요 약

S/W 시스템의 보안속성에 대한 QoS 요구조건을 적용하기 위해서는 침입에 대한 객관적 모델 및 정량적 분석이 가능해야 한다. 즉, 특정 침입에 대응하는 보안기능의 존재여부를 중심으로 시스템의 성능을 평가하는 정성적 방식이 아닌 보안시스템의 분석적 모델에 의해 침입 형태별로 어떤 성능을 나타내는지를 수치적으로 제시할 필요가 있다. 본 논문에서는 Intrusion Tolerant System(이하 ITS라 함) 모델링에 대한 관련연구를 바탕으로 DoS 공격 등 침입양태별 모델링 사례를 시뮬레이션을 통해 분석하고 모델링의 방향을 제시하고자 한다.

1. 서론

일반적으로, S/W 시스템의 QoS(Quality-of-Service) 요구조건 중 신뢰도(Reliability), 가용도(Availability) 등은 군사, 항공, 전자상거래 등 다양한 응용분야에서 필수적인 요소로 이해되고 있다. 여기에, 인터넷 보급과 네트워크가 생활전반에 깊숙히 자리하고 디지탈 컨버전스 시대가 본격적으로 도래하면서 S/W 시스템이 다양한 보안침입에 노출됨에 따라 이에 대응하는 보안 관련 QoS 조건이 추가적으로 요구되고 있는 상황이다.

그런데, 기존 QoS 요구조건들을 특정 S/W 환경에 적용하기 위해서는 정량적인 평가가 선행되어야만 구체적인 반영이 가능했듯이, 보안요소에 대한 QoS 요구조건을 적용하기 위해서도 침입에 대한 객관적 모델 및 정량적 분석이 가능해야 한다. 따라서, 본 논문에서는 ITS에 대한 모델링 사례를 시뮬레이션을 통해 분석하고 모델링 방향을 제시하고자 한다.

2. 관련연구

[1]에서는 Privilege Graph를 이용한 UNIX 시스템의 취약성(Vulnerability)을 모델링하기 위해 시스템에 대한 침입시도가 성공할 확률을 지수분포로 가정하고 마르코프 체인으로 전환하는 방식으로 보안시스템의 성능분석 방법을 제안하고 있다. [2]에서는 ITS가 침입상황에서 갖추어야 할 동적인 이상거동을 상태 전이 모델로 나타내고 시스템이 가지는 취약성 및 위협요소를 어떻게 모델링할 수 있는가에 대한 기반연구를 진행하였다. 그러나 상태천이모델을 바탕으로 정량적 성능분석을 시도한 [3]의 연구에 따르면, 다양한 침입양태별로 실제 데이터에 기반한 성능분석의 어려움을 기술하고 있다. 즉, 제시한 모델링 방법의 타당성 검증이 선행되어야 하며, 모델 파라메타의 정확한 값을 정의하기 어려운 보안침입의 속성상 성능분석의 실효성을 담보하기 어려운 문제등이 남아있다.

3. 보안속성 성능분석을 위한 모델링

S/W시스템이 초기상태에서 보안침입에 노출되고 ITS가 가동되는 일련의 과정을 그림 1과 같이 9가지 상태(State)로 표현할 수 있다[2].

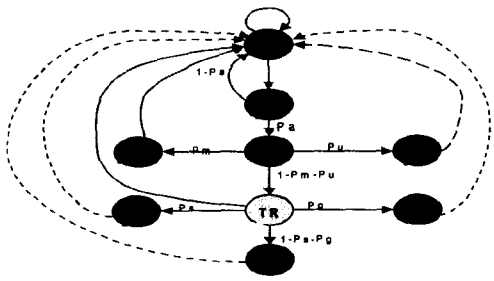

그림 1 ITS의 상태 전이 모델

여기서 침입자의 상태는 G(Good), V(Vulnerable), A(Attack)에 나타나고, 그에 따른 시스템의 대응은 MC(Masked Compromised), UC(Undetected Compromised), TR(Triage), FS(Fail Secure), GD(Graceful Degradation), F(Failed)에 포함되어 있다. 상기 모델을 바탕으로 성능평가 척도인 안정 상태의 가용도를 계산하기 위해 식 1의 확률과정을 정의할 수 있으며, 서비스 시간이 일반적인 분포인 M/G/1을 적용한 세미마르코프(Semi-Markov) 프로세스(이하 SMP라 함) 분석을 통해 보안요소 성능평가 모델링이 가능하다.

$$X(t): t>0, X_S = G, V, A, MC, UC, TR, FS, GD, F(1)$$

위 상태 전이 다이어그램은 모든 상태가 상호 도달 가능하므로 더 이상 줄일 수 없다(irreducible)고 할 수 있으며, 주기성을 갖지 않고 한정된 시간내에 특정상태로 회귀할 수 있으므로 erogodicity(aperiodic, recurrent, nonull) 특성을 만족하게 된다. 따라서, ITS 각 상태에 대한 SMP의 안정 상태 확률값이 존재하고 해당 SMP는 각 상태에서의 전이 확률(p_a,p_u,p_s,p_g,p_m)을 이용한 임베디드 이산마르코프체인에 의해 표현될 수 있다.

SMP의 각 상태에서의 평균 잔류시간을 h_i라 하고, 이산마르코프체인 안정 상태 확률을 ν_i라 할 때, SMP의 각 상태에 대한 안정 상태 확률 π_i는 식 2와 같이 나타낼 수 있다.[4]

$$\pi_i = \frac{\nu_i h_i}{\sum_j \nu_j h_j}, \quad i,j \in X_S \tag{2}$$

5. 침입 양태별 SMP 모델링 분석

침입 양태별 SMP 모델의 안정 상태 확률을 구하기 위해서는 상태 전이 다이어그램을 재정의해야 한다. 여기서는 DoS공격과 ASP 취약성의 경우에 상기 SMP 모델의 결과를 적용해 보고자 한다.

첫번째, SYN Flood 및 Smurfing와 같은 DoS 공격의 경우 DNS서버와 같은 특정서버에 악의적인 http 요청을 대량으로 보냄으로써 시스템의 리소스를 장악해 버리는 경우이므로, 그림 1의 A(attack) 상태에서 악의적 요청의 모든 경우를 감지하는 것은 불가능하다[2]. 따라서 DoS 공격시 ITS가 가동되는 TR상태로의 전이를 통해 시스템의 최소한의 기능을 담보해주는 GD상태를 거침으로써 가용도를 어느 정도 보장해주는 정책을 택하는 것이 적절한 방안이라 할 수 있다.

즉, DoS의 경우 시스템의 가용성 저하에 초점을 두는 공격이므로 TR상태에서 FS상태로의 천이를 통한 기밀성(Confidentiality) 보장은 의미가 없다고 할 수 있다.

따라서, 이 경우 그림 1에서 MS와 FS상태를 배제하여 축소 모델링 할 수 있으며, 식 2의 안정 상태 확률을 각 상태별로 구하면 식 3을 얻을 수 있다[4].

$$\pi_G = h_G/(h_G + h_V + p_a[h_A + p_u h_{UC} + (1-p_u)[h_{TR} + p_g h_{GD} + (1-p_g)h_F]])$$
$$\pi_V = h_V \pi_G/h_G,\ \pi_A = p_a h_A \pi_G/h_G,\ \pi_{UC} = p_a p_u h_{UC} \pi_G/h_G$$
$$\pi_{MC} = 0,\ \pi_{FS} = 0,\ \pi_{TR} = p_a(1-p_u)h_{TR}\pi_G/h_G$$
$$\pi_{GD} = p_a p_g (1-p_u) h_{GD} \pi_G/h_G$$
$$\pi_F = p_a(1-p_g)(1-p_u)h_F \pi_G/h_G \tag{3}$$

이 경우 DoS 공격에 대한 안정 상태 확률 A_{DOS}는 일반적인 경우와 달리 FS 상태가 존재하지 않으므로 다음과 같이 구할 수 있다.

$$A_{DOS} = 1 - (\pi_F + \pi_{UC})$$

두번째 ASP 취약성은 IIS(Internet Information Server)를 사용하는 사용자에게 해당서버의 텍스트 파일을 노출시키는 보안상의 취약성을 나타내는 것으로써 기밀성의 보장이 중요한 경우라 할 수 있다[2]. 이 경우는 그림 1의 TR상태에서 시스템의 가용도 뿐만 아니라 기밀성까지 동시에 고려해 주는 모델이 타당하므로 MS상태만을 배제한 모델링이 되어야 한다. DoS 공격과 같은 방법으로 안정 상태 확률을 구하면 식 4를 얻을 수 있다.

$$\pi_G = h_G/(h_G + h_V + p_a[h_A + p_u h_{UC} + (1-p_u)[h_{TR} + p_s h_{FS} + p_g h_{GD} + (1-p_g-p_s)h_F]])$$
$$\pi_V = h_V \pi_G/h_G,\ \pi_A = p_a h_A \pi_G/h_G,\ \pi_{UC} = p_a p_u h_{UC} \pi_G/h_G$$
$$\pi_{MC} = 0,\ \pi_{FS} = p_a p_s h_{FS}(1-p_u)\pi_G/h_G$$
$$\pi_{TR} = p_a(1-p_u)h_{TR}\pi_G/h_G,$$
$$\pi_{GD} = p_a p_g (1-p_u) h_{GD} \pi_G/h_G$$
$$\pi_F = p_a(1-p_s-p_g)(1-p_u)h_F \pi_G/h_G \tag{4}$$

한편, ASP 취약성은 DoS 공격의 경우와 달리 FS 상태가 존재하므로 안정 상태 확률은 다음과 같이 나타낼 수 있다.

$$A_{ASP} = 1 - (\pi_F + \pi_{FS} + \pi_{UC})$$

6. 시뮬레이션 및 분석

ITS의 SMP모델 분석 결과를 시뮬레이션하기 위해서는 전이 확률과 상태 전이 다이어그램내 각 상태에서의 평균잔류시간(Mean Sojourn Time)에 대한 파라메타 설정이 이루어져야 한다. 본 논문에서는 상기 일반적 모델링 결과 및 사례별 결과에 대한 수치적 검증을 실시하기 위해 두개 파라미터에 대해 표 1과 같이 수치를 정의하여 시뮬레이션을 수행하였다.

표 1 시뮬레이션 파라미터 설정

입력변수	파라미터 설정
평균잔류시간	$h_A = .25, h_V = 1/3, h_G = .5, h_{TR} = 1/6$ $h_{MC} = .25, h_{UC} = .5, h_{FS} = 1, h_F = 2, h_{GD} = 4$
Transition probability	p_a =.4, p_m=.3, p_u=.2, p_g=.6, p_s =.3

그림 2는 DoS공격과 ASP 취약성에 대해 시뮬레이션한 결과를 보여주고 있다.

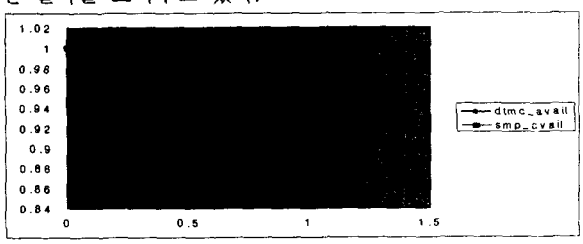

그림 2-a ASP vulnerability 경우(p_a 변화)

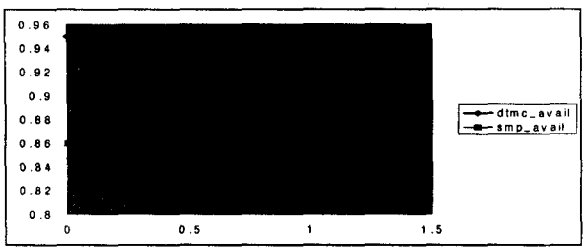

그림 2-b DoS 공격의 경우(p_u 변화)

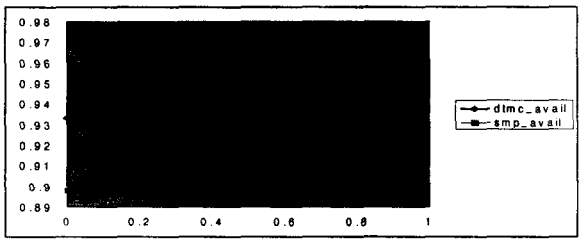

그림 2-c generic 경우(p_m 변화)

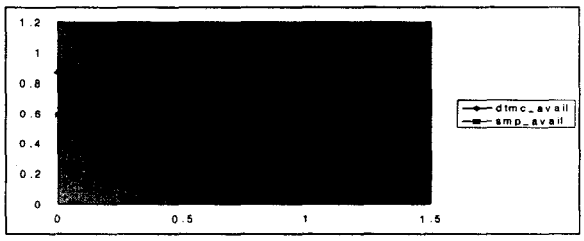

그림 2-d DoS 공격의 경우(p_g 변화)

몇가지 특징적인 부분을 살펴보면 다음과 같다.

첫째, 모든 경우에 대해 이산마르코프체인 안정 상태의 가용도가 SMP 안정 상태 가용도에 비해 높게 나타남을 알 수 있다. 이는, 이산마르코프체인의 경우 시스템의 각 상태에서의 평균 잔류시간을 고려하지 않은 경우에 대한 값이며, 일반적으로 평균 잔류시간을 고려한 SMP 모델의 경우가 실제 시스템의 상황을 더 잘 표현한다는 것을 나타낸다.

둘째, p_a(시스템이 V(Vulnerable)상태에서 공격상태로 천이할 확률)가 0에서 1까지 증가함에 따라 가용도는 1에서 점진적으로 낮아지게 된다. 그러나 공격 상태가 될 경우 시스템이 곧바로 마스킹(Masking) 가능한 상태나 ITS가 가동되므로 p_a가 1에 근접함에 따라 가용도도 특정값으로 수렴하게 된다.

세째, p_u(공격형태가 감지되지 못할 확률)값이 커지면 시스템내의 공격을 곧바로 마스킹할 수 있는 p_m 값이 상대적으로 작아지게 되고, 시스템 불안정성이 가중되므로 가용도는 점진적으로 감소하게 된다. 이때, 가용도의 수렴값이 존재하지는 않는다. 왜냐하면, UC상태는 시스템 재구성(Reconfiguration)을 통해서만 G상태로 갈 수 있으므로, p_u 값이 1이 될 경우 그때의 시스템 가용도가 어떤 값을 가지든 시스템은 즉시 재가동되기 때문이다.

네째, p_g, p_m 의 경우 1로 근접할수록 시스템의 안정상태 가용도 또한 1로 근접해 간다는 것을 알 수 있다. p_m은 외부 공격에 대해 즉시 마스킹할 수 있는 상태로 천이할 확률이므로 ITS를 가동할 필요 없이 시스템이 유지될 수 있는 상황이므로 가용도가 높아지게 된다. p_s는 시스템의 비밀성을 보장해주는 FS상태로의 천이이고, p_g는 DoS와 같이 시스템의 리소스를 마비시키는 형태의 공격으로부터 최소한의 기능만을 유지시켜서 가용도를 보장해주는 GD상태로의 천이이다. 따라서 FS 및 GD 모두 가용도는 기본적으로 보장되는 상태이므로 p_s 및 p_g 값이 증가함에 따라 F상태로 천이 확률인 $1-p_s-p_g$ 값이 감소하게 되어서 가용도가 증가하게 됨을 알 수 있다.

7. 결론

본 논문에서는 [3]에서 제시한 ITS에 대한 확률론적 모델링 기법을 보안공격 양태별 SMP 모델 분석 및 시뮬레이션을 통해 결과를 검증해 보았다. ITS의 각 상태를 9가지 상태로 정의한 후 각 상태에서의 전이 확률 및 평균 잔류시간을 통해 이산마르코프체인 안정 상태 확률 및 SMP 안정 상태 확률을 계산하여 시스템의 안정 상태 가용도를 정의하였으며, DoS 공격 및 ASP 취약성의 경우에 분석결과를 적용하여 그 결과를 시뮬레이션을 통해 검증해 보았다.

향후, 실제 ITS 프로토타입 시스템을 이용한 파라미터를 바탕으로 시뮬레이션을 실시할 경우 보다 정확한 검증결과를 얻을 수 있을 것으로 기대된다.

또한, 성능평가 척도로 안정 상태 가용도 뿐만 아니라 시스템의 MTTSF(Mean Time to Security Failure)를 정의하고 그에 대한 침입양태별 정량적 분석이 병행될 필요가 있을 것으로 판단된다.

[참고문헌]

[1] R. Ortalo, et. al., "Experiments with Quantitative Evaluation Tools for Monitoring Operational Securi -ty," IEEE Transaction Software Engineering, pp. 633-650, 1999.

[2] F. Goseva-Popstojanova, K. Trivedi, et. al., "Chara cterizing Intrusion Tolerant Systems using a State Transition Model," DARFA Information Survivabi-lity Conference and Exposition, pp. 211-221, 2001.

[3] B. Madan, Trivedi et. al., "Modeling and Quantifica tion of Security Attributes of Software Systems," International Conference on Dependable Systems and Networks, pp. 505-514, 2002.

[4] Leinard Kleinrock, Queueing Systems: Volume 1 Theory, John Wiley & Sons, 1974.