유비쿼터스 컴퓨팅의 신뢰성 모델링을 위한 정량적 분석법

°
최창열 김성수
아주대학교 정보통신전문대학원
{clchoi, sskim}@ajou.ac.kr

A Quantitative Analysis Method for Reliability Modeling of Ubiquitous Computing

°
Changyeol Choi◊ Sungsoo Kim◊
Graduate School of Information and Communication, Ajou University

요 약

유비쿼터스 컴퓨팅은 네트워크로 상호연결된 프로세서로 구성되며, 하나 이상의 컴퓨터로 이뤄진다. 하지만 기존 보안 솔루션은 존속성에 대한 명확한 정의가 결여되어 있어 본 논문에서는 유비쿼터스 컴퓨팅 시스템을 위한 존속성을 기반으로 하여 시스템의 보안 정도를 정량적으로 측정할 수 있는 기법을 제안한다. 존속성을 모델링하기 위한 논리적 첫 단계가 요구사항 도출이므로 먼저 공격 유형 모델을 도출하고 실제 공격 사례 중 Code-Red 웜 공격을 공격 유형 모델과 존속성 모델을 통해 분석하였다.

1. 서 론

IT 기술 진화에 따라 다소 원리적이던 이론들이 실제 구현이 가능할 수 있는 기반구조가 형성되고 있는데, 대표적인 예가 유비쿼터스 컴퓨팅이다. 유비쿼터스 컴퓨팅이란 언제, 어디서나 사용자가 신뢰성 높은 서비스를 지속적으로 받을 수 있는 환경이다[1]. 따라서 악의적인 공격에 효율적으로 대응하여 신뢰성 높은 유비쿼터스 컴퓨팅 시스템을 제공해야만 실현이 가능해진다. 그런데 전통적인 시스템 보안 유지 기법 및 정책[2,3]은 대부분 기밀성 유지를 위한 암호화 기법에 집중된 연구 결과나 특정 공격 기법에 대한 연구 결과에 의존하였기 때문에, 최근 대규모 인프라 공격에 대한 대응책을 마련하지 못하였다. 2003년 초에 일어난 인터넷 대란은 대규모 인프라 공격에 대한 연구의 필요성을 일깨운 계기가 되었으며, 유비쿼터스 컴퓨팅처럼 네트워크로 상호연결된 인프라는 더욱 대처방안 마련이 시급하다. 따라서 본 논문의 목적은 위와 같은 문제점을 해결하기 위한 것으로, 사용자의 개입을 최소화해야만 하는 유비쿼터스 컴퓨팅 환경을 위해 네트워크 중심의 자동 대응 패러다임을 마련하기 위한 수학적인 분석 모델링을 제시한다. 또한 공격 유형을 공격 속도 특성에 부합되는 분포도와 유비쿼터스 컴퓨팅 인프라를 구성하기 위한 노드 중 공격에 적절히 대응하고 있는 노드수로 분류하여, 지역적인 탐지 결과에 따른 수동적 대응 및 단기적 정보에 의존한 탐지에 따른 높은 오류율을 감소하기 위한 방법을 제안한다. 그리고 제안한 분석법의 적용 방법에 대한 예제를 위해 Cod-Red 웜 공격을 분석한다.

This work is supported in the 21st Century Frontier Research and Development (R&D) Program "National Center of Excellence in Ubiquitous Computing and Network" from the Ministry of Science and Technology (MOST).
이 논문은 2004년도 두뇌한국21사업에 의하여 지원되었음.

2. 정량적 분석법

유비쿼터스 컴퓨팅을 위한 인프라의 공격을 탐지 및 대응하기 위한 정량적인 분석은 노드 i 가 공격을 받아 오동작 및 결함이 발생하는 시간을 기준으로 이뤄진다. 해당 시간은 고정적인 요소(Fixed Effect, β)와 임의의 요소(Random Effect, u)에 의해서 영향을 받는다. 고정적인 요소는 인프라 구성을 위한 노드의 CPU 처리속도, 메모리 크기, 디스크의 용량, 네트워크 대역폭 등이며, 임의의 요소는 방화벽, 설치된 OS 버전, 보안 메커니즘 갱신 정보, 공격자의 능력 등이다. 전형적으로 고정적인 요소와 임의의 요소는 노드의 위험요소(Risk Factor, η_i)의 벡터로 아래와 같이 표현되며, x_i와 z_i는 그리드 및 네트워크로 상호연결된 컴퓨터 시스템을 구성하기 위해 사용되는 시스템 명세서에 명시된 임의의 값이다.

$$\eta_i = x_i\beta + z_i u$$

노드의 위험요소가 정의되면, 적어도 주어진 시간 t까지 노드가 공격에 대응하여 정상적인 서비스를 수행할 수 있는 확률을 얻을 수 있는데, 이 확률값을 노드의 존속성(Survivality)이라 한다. 또한 공격을 받고 노드가 오동작을 하는데까지 걸리는 시간(T_i)이 주워지고, 이에 대한 밀도함수($f(t;\eta_i)$)와 누적분포함수($F(t;\eta_i)$)에 대해 정의할 수 있으면 존속성에 대한 분석을 위한 존속 함수($S(t;\eta_i)$)를 모델링할 수 있다.

$$S(t;\eta_i) = \Pr(T_i \geq t) = 1 - F(t;\eta_i) = \int_t^{\infty} f(w;\eta_i)\,dw$$

또한 다수 노드($i \geq 2$)로 이뤄진 시스템의 경우 전체 시스템의 존속성($S_R(k,n,t)$)은 단일 노드의 존속성($S(t;\eta_i)$)에 의해 결정되며, n개 노드 중 k개의 노드가 공격으로부터 영향을 받지 않은 상태에 머무를 확률은 아래와 같이 구할 수 있다.

$$S_R(k,n,t) = \sum_{i=k}^{n} \binom{n}{i} S(t;\eta_i)(1 - S(t;\eta_i))^{n-i}$$

그림 1은 정량적 분석법의 아이디어의 출발점을 정립하기 위한 개념으로써 복잡도 이론을 적용하여 공격 유형을 분류하기 위한 기본적인 개념이다. 이는 최초 공격을 시작하여 한 노드의 오동작을 일으킬 때까지의 공격시간(MTTA)을 기준으로 분류한 것으로 결함허용 시스템에서 신뢰도 분석을 수행하는 MTTF(Mean Time to Failure)와 유사한 개념이다. 다시 말해서 본 정량적 분석법의 적용범위를 정의하기 위해서 공격자가 한 노드에 대해 공격을 수행하였더라도 해당 노드가 오동작을 하지 않거나 노출되지(Compromised) 않아서 공격자의 의도대로 동작하지 않는다면 그것은 공격이 성공하지 못한 상태로 존속성을 유지하고 있다고 가정한다. 따라서, 유비쿼터스 컴퓨팅 인프라의 노드 중 일정시간(t)까지 완전히 공격자의 의도에 따라 공격을 당한 노드의 수($C(t)$)와 공격 특징과 부합되는 분포도를 가지고 공격 유형을 다음 3가지로 분류하는데, 공격 특성을 표현하기 위한 분포도는 결함허용 시스템에서 신뢰도를 분석할 때 사용하는 일반적인 분포도를 사용한다.

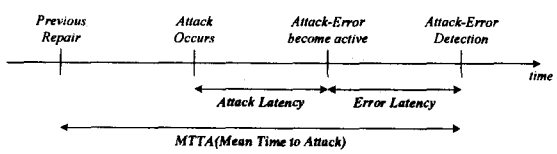

그림 1 MTTA (Mean Time to Attack)

• 상수 시간 공격 (Constant Time Attack): 공격율을 최대한으로 달성한 후 공격이 끝날 때까지 최대 공격율을 유지하는 특성을 가지는 것이며 Weibull 분포로 표현된다.

$$C(t) = \begin{cases} 0 & if\ t \leq p, \\ n & otherwise \end{cases}$$

• 급격한 추이 변동을 보이는 공격(Pulsing Attack): 공격 여부에 대한 시스템 관리자의 감시를 피하기 위해서 공격율을 임의의 기간(p_1, p_2, p_3)에 따라 최대 공격율을 유지하는 경우과 공격을 하지 않는 경우를 반복하는 특징을 보유한 것으로 Erlang 분포의 특징과 유사하다.

$$C(t) = \begin{cases} 0 & if\ t \leq p, \\ a & if\ p_1 < t \leq p_3 \\ b & otherwise \end{cases}$$

• 증가 추이 공격(Increasing Time Attack): 공격율을 점진적으로 높여가며, 노출되는 노드수를 하나씩 증가시키는 특징을 보이는 것으로 Hypoexponential 분포로 표현 가능하고 $C(t)$값은 한 노드를 공격하는데 걸리는 시간(p)와 공격 지속 시간(t)의 관계로 표현한다.

3. 사례연구(Code-Red 웜 공격)

본장에서는 제안한 정량적 분석법을 적용한 Code-Red 웜 공격[4] 분석을 통한 적용 예제를 살펴본다. Code-Red 웜의 경우 다단계 진행 상태를 포함할 수 있는 Erlang 분포, Hypoexponential 분포 또는 Hyperexpo-nential 분포로 정량적인 분석 모델링이 가능하다.

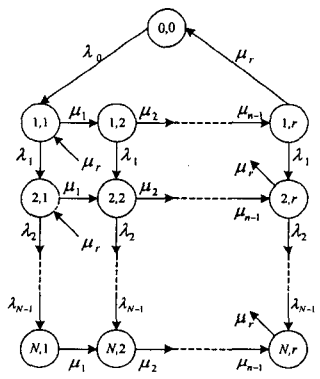

그림 2 Code-Red 웜 공격의 정량적 분석을 위한 모델

그러나 Code-Red 웜의 경우 점차 감염된 노드수가 늘어날수록 다음 피해를 받을 노드수가 기하급수적으로 증가하기 때문에 증가 추이 공격에 해당되며, 이와 같은 특성을 표현하기 위해서는 하이퍼 지수분포가 적당하다. 그러므로 한 노드가 감염되어 오동작을 일으키거나 공격자의 의도대로 컴퓨터가 작동되기 위한 단계를 r이라 하고 감염된 노드의 수를 N이라 할 때, 분석 모델은 그림 2와 같다. 노드 상태는 (감염된 노드수, 공격 단계)의 쌍으로 표현되며, 초기 및 정상 상태는 (0,0)이다. λ_i는 공격율이고, μ_i는 공격 단계 성공률이며, μ_r은 감염된 노드가 치료를 위해 필요한 서비스율이다. 그림 2에서 모든 상태가 안정 상태(steady-state)일때 균형방정식을 구하면 아래와 같다.

$$\mu_r P_{n,r} = \lambda_{n-1} P_{n-1}, \quad \mu_r P_{1,i} = (\lambda_1 + \mu_{i+1}) P_{1,i+1}$$
$$\mu_r P_{n,i} = (\lambda_n + \mu_{i+1}) P_{n,i+1} - \lambda_{n-1} P_{n-1,i+1}$$
$$, \text{where } < n >\equiv \{(n,i) \mid i = 1, \ldots, r\}$$

위의 균형 방정식과 각 상태에서 머물 확률의 총합이 1이 되는 보존(conservation) 방정식을 결합한 연립 방정식을 풀면, 시스템이 평형일 때, 각 상태에 머물 확률을 다음과 같이 얻을 수 있다.

$$P_{n,i} = \lambda_o G^*(1; i, r-1) P_0$$
$$P_{n,i} = \lambda_{n-1} \left\{ G^*(n; i, k-1) P_{n-1} - \sum G^*(n; i, k-2) P_{n-1,k} \right\}$$
$$, \text{where } G^*(n; i, k-1) \equiv \prod_{j=1}^{k-1} \frac{(\lambda_n + \mu_{j+1})}{\mu_j}$$

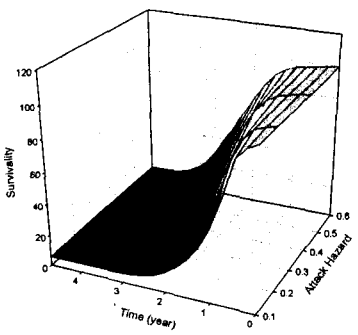

그림 3 Code-Red 웜 공격에 대한 존속성 변화

그림 3은 다수의 노드로 구성된 유비쿼터스 컴퓨팅 인프라에서 Code-Red 웜 공격에 따른 존속성의 변화를 분석한 것이다. 이는 공격 유형 모델링과 정량적 분석을 통해 얻은 존속성에 대한 확률값으로 공격에 대한 위험 요소가 0에서 0.6까지 존재할 경우의 변화다. 결과에서 보듯, 공격 위험 요소가 존재하고 있는 경우 인프라 운영 시간이 길어질수록 존속성은 매우 급격히 떨어지게 된다.

4. 결 론

유비쿼터스 컴퓨팅은 상호연결된 네트워크 인프라로 구성되며, 이와 같은 구조는 대규모 인프라 공격에 매우 취약하다. 따라서 이러한 공격에 대응할 수 있는 적절한 대응책 마련이 시급하다. 본 논문에서 제안한 정량적 분석법은 공격 발생 이후에 수동적으로 대처하거나 정성적인 분석에 의존한 지엽적인 대응책에 비해, 공격 유형 모델링과 존속성 모델링을 통한 대응으로 공격 탐지 시점을 앞당길 수 있는 능동적/예방적 차원의 보안 유지가 가능하게 되므로, 결국 전체 인프라의 신뢰성을 향상시킬수 있다.

향후 정성적인 분석법 및 대응책에 대한 연구 및 정량적 분석법과의 통합/연계 보안 유지 정책을 통해 보다 강력한 공격 대응책 마련이 필요하다.

참고 문헌

[1] M. Weiser, "Some Computer Science Problems in Ubiquitous Computing," Communications of the ACM, Vol. 36, pp. 75-84, 1993.

[2] B. Madan, K. Gŏseva-Popstojanova, K. Vaidya - nathan, and K. Trivedi, "Modeling and Quantification of Security Attributes of Software Systems," Proceedings of the International Conference on Dependable Systems and Networks, pp. 505-514, 2002.

[3] J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the Source," Proceedings of the 10th IEEE International Conference on Network Protocols, pp. 312-321, 2002.

[4] S. Hunter and W. Smith, "Code-Red: a Case Study on the Spread and Victims of an Internet Worm," Proceedings of the 2nd ACM SIG-CCMM Workshop on Internet Measurement Workshop, Analysis and Synthesis, pp. 273-284, 2002.