보안시스템을 위한 비용 기반 계층적 결함허용모델

정유석[0], 박눌, 홍만표
아주대학교 정보통신전문대학원
{j8508[0], nuri282, mphong}@ajou.ac.kr

Cost based Hierarchical Fault Tolerence Model for Security System

Yoo-Suk Jung[0], Nool Park, Man-Pyo Hong
Graduate school of Information and Communication, Ajou University

요 약

시스템 침입은 정보통신기술의 비약적인 발전에 따른 정보화의 역기능으로, 이를 해결하기 위한 다양한 방법들이 제안되어왔다. 그러나 최근 침입 패러다임의 변화로 인해 기존 방법으로 해결하지 못하는 공격이 발생했으며, 그중 보안 시스템 우회나 보안 시스템 자체에 대한 공격은 기존 보안 도구를 무력화시킬 수도 있다. 본 논문에서는 이를 해결하기 위한 방법으로 고전적인 결함허용 기법을 응용한 결함허용 기능을 정의하고 이를 이용한 계층적 시스템 모델을 제안한다. 또한, 보안 시스템의 특성에 맞는 결함 허용 기능 선택을 위한 기준으로 비용 기반 선택 모델을 제안한다.

1. 서 론

최근 정보통신기술의 비약적인 발전과 제반 환경의 보급은 인터넷 기반의 새로운 시장과 문화를 창출할 뿐 아니라 기존 산업사회 전반을 정보사회로 변화시키고 있는 등 인간의 삶을 더욱 풍요롭게 하는데 일조를 하고 있다. 하지만 이와 같은 인터넷의 긍정적인 측면의 증가는 더불어 개인 정보의 유출, 시스템의 오남용, 인터넷을 통한 전산망 해킹 등 매우 위험하고 파괴적인 역기능의 문제를 야기하고 있는데, 이는 정보화가 진전될수록 더욱 확대되는 양상을 보이고 있으며 그 피해 정도 또한 갈수록 심각해지고 있다.

따라서 이와 같은 정보화의 역기능을 막기 위한 다양한 연구들이 진행되어 왔는데, 1970년대와 1980년대 사이에 각종 보안과 관련된 기본 개념들이 소개 된 이후, 특정 호스트나 지역 네트워크의 보안을 위한 단일 보안시스템들이 등장하고[1,2], 인터넷의 사용이 증대됨과 동시에 네트워크 공격의 패러다임이 변하면서 단일 보안시스템으로 해결하기 어려운 문제에 대처하기 위한 다중 보안시스템이 등장했다[3,4,5,6,7]. 그런데 이와 같은 보안에 대한 관심과 연구는 침입 패러다임 변경의 원인이 됨과 동시에 침입 대상의 변화를 야기했다. 즉 침입자들은 대상 서비스 호스트를 우선적으로 공격하는 것이 아니라, 해당 호스트를 보호하는 보안 시스템을 우회하거나 혹은 더 나아가 보안 시스템 자체를 공격하여 무력화시킨 후 대상 서비스 호스트로 침입하는 방법을 사용하게 되었다. 이와 같은 변화는 침입의 판정이 이전에 비해 어려워 졌다는 것 뿐 아니라 보안 시스템 자체에 대한 보안이 매우 중요해졌다는 것을 의미한다.

보안 시스템을 무력화시키기 위한 방법은 보안 시스템의 판단 방법을 우회하는 것과 보안 시스템 자체에 대한 공격을 통해 보안 기능을 파괴하는 것으로 분류할 수 있다.

이 중 우회를 위한 방법은 공격을 오랜 시간에 걸쳐, 즉 다량의 정상적인 요소에 공격을 위한 요소를 조금씩 추가하거나, 다수의 호스트를 통한 공격의 진행을 진행하는 등, 보안 시스템이 공격을 알아내지 못하게 하는 것에 초점을 맞추고 있다. 다양한 보안 방법들의 결합을 통한 결함 허용 기법은 이런 침입들에 대해 보안 판정을 하기 위한 좋은 해결책일 수 있다.

보안 시스템 자체에 대한 공격은 보안 시스템의 성능이 향상될수록 더욱더 빈번하게 시도될 것이다. 즉 서비스 호스트 보안과 관련된 연구가 발전할수록 보안 시스템 자체에 대한 보안은 더욱 더 중요한 문제가 될 수 있다. 그러나, 현재까지의 보안 관련 연구는 초기화 단계였기에, 보안 시스템 자체의 보안에 대한 연구보다는 서비스 시스템에 대한 보안에 초점이 맞추어져 있었으며, 최근의 연구 쟁점 또한 더욱 정확한 보안을 위한 방법의 제안이 주제였다. 그러나, 보안 시스템 자체에 대한 연구는 서비스 시스템의 보호를 위해서도 반드시 필요한 요소이며, 이제는 보안 관련 연구도 보안 시스템 자체에 대한 연구가 필요한 수준까지 도달했음으로 이와 관련된 영역을 연구할 필요가 있다. 결함허용 기법은 병렬·분산 시스템에서 발전·검증되어 왔던 것으로 보안시스템에 대한 공격을 방어하기 위한 좋은 해결책이 될 수 있으며, 또한 보안 시스템의 비의도적인 결함에 대한 대처에도 적용될 수 있다.

따라서, 본 논문에서는 보안 시스템의 우회·공격 및 보안 시스템의 비의도적 결함을 해결할 수 있는 결함허용 모델을 제안한다. 이를 위해 우선 보안시스템의 결함허용을 위한 기능을 분석한 후, 보안시스템의 결함허용을 위한 시스템 모델과 비용 기반 결함허용 기능 선택 모델을 제시하고, 마지막으로 기존 시스템에의 적용을 통해 가능성을 진단한다.

2. 관련 연구

기존의 보안 기술은 특정 조직의 해당 도메인 및 네트웍을 보호하는 것에 초점이 맞추어져 있으며, 이와 관련된 대표적인 도구로는 침입 징후를 탐지하기 위한 침입탐지시스템과, 탐지된 해당 침입자의 트래픽 차단을 주목적으로 하는 방화벽 및 패킷 필터링 라우터 등이 있다. 특히 침입탐지시스템은 수동적인 방어 형태를 띄는 방화벽을 보완하기 위한 능동적인 네트워크 보안 솔루션으로, 그동안 많은 연구가 진행되었다. 1980년대 초 호스트 기반 침입탐지시스템인 SRI CSL의 IDES[1]가 개발된 이래, 멀티 호스트 기반 침입탐지시스템인 NIDES[2]와 네트워크 기반 침입탐지시스템 NSM이 개발되었고, 이들을 바탕으로 대규모의 네트워크 환경에서 침입을 탐지하기 위한 분산 침입탐지시스템의 형태인 EMERALD[3,4], GrIDS[5], JAM[6], AAFID[7] 등이 개발되었다. 그러나 대부분 기존 연구의 초점은 서비스 도메인이나 네트워크로의 보호대상 확장 및 보호 대상에 대한 정확한 보안판정에 있었고, 보안 시스템 자체의 보안을 위한 연구는 거의 없었다. 특정 연구에서 결함허용의 필요성을 언급하거나 일부 분산 보안 시스템에서 부분적인 결함 허용을 채용하고 있으나, 전반적인 보안 도구에 대한 보호 방법은 연구되고 있지 못한 상황이다[3,4,7]. 많은 연

본 논문은 한국전자통신연구원의 지원에 의한 것임

구가들은 보안 관련 연구를 진행하면서 보안 시스템 자체에 대한 보안의 중요성을 어느 정도는 피력하고 있다. 그러나 보안 시스템의 보안 관점 성능이 그동안의 주된 관심사였으며, 결과적으로 보안 시스템 자체의 보안을 주제로 해서 진행된 연구는 아직 부족한 실정이다.

결함허용 기법은 보안 시스템의 보호를 위한 방법 중 하나로 사용될 수 있다. 그러나 현재 보안에서의 결함허용 기법 적용에 관한 연구 중 대부분은 보안 연구를 위한 결함허용 원칙에 대한 제안[8]과 분산 컴퓨팅 환경에서 보안과 결함허용의 결합이었다[9]. 이러한 연구들은 대체적으로 네트워크 상에서 특정한 서비스나 컴퓨터를 보호하기 위한 방법 중 하나로 결함허용 기법을 사용하는 것이며, 따라서 이와 관련해 제안된 결함허용 기법들은 보안 시스템의 보호가 초점이 아니라 결함허용 기법을 통해 제공하려는 서비스를 보호하려는 것에 초점이 맞추어져 있었다. 미 국방성 DARPA에 의해 주도된 보안 관련 연구에서는 보호 대상 시스템의 생존성 향상을 위한 중복성 적용에 대해 연구해 왔으나, 이 역시 서비스 자체에 대한 보호에 초점이 맞추어져 있었다.

보안 시스템 자체에 대한 보안은 반드시 필요하다. 그러나 위에서 언급한 것 같이, 보안 분야의 연구가 초기단계이기에 보안 시스템 자체의 보호를 위한 연구는 거의 진행되지 못했으며, 더군다나 보안 시스템을 보호하기 위한 방법으로 결함 허용 기법을 응용하려는 연구는 전무한 실정이다. 따라서 보안 시스템의 오류 처리라는 관점에서 보안 시스템 보호를 고찰하고 이를 해결하기 위한 결함 허용 모델을 제시하는 것은 보안 시스템을 보호하기 위한 새로운 해결책이 될 수 있다. 또한, JAM 프로젝트의 비용 기반 침입탐지 모델링[10]에서와 같은, 비용의 관점을 고려해 실용 가능한 모델을 제시함으로서 실질적인 응용을 가능하게 할 필요가 있다.

3. 비용기반 결함허용모델

3.1 대상 보안시스템

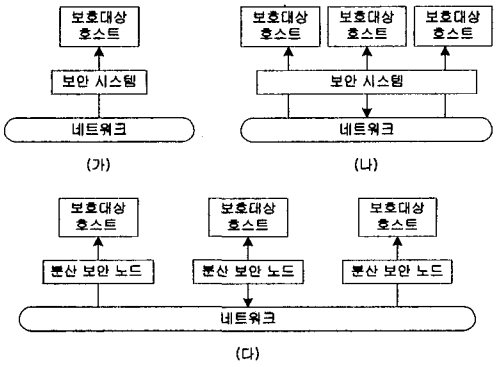

그림 1. 결함허용 대상 보안시스템
(가) 단일호스트 대상 단일보안시스템, (나) 다중호스트 대상 단일보안시스템, (다) 다중호스트 대상 다중보안시스템

본 논문에서 보호하고자 하는 대상 보안시스템은 그림 1과 같은 세 가지로 분류된다. 단일호스트 대상 단일보안시스템[그림1.(가)]은 일반적으로 다른 호스트들에 비해 상대적으로 중요한 서비스 호스트를 보호하기 위해 사용되며, 이때 보안시스템은 하나의 호스트만을 감시함으로 다소 강력한 많은 기능을 제공할 수 있다. 다중호스트 대상 단일보안시스템[그림1.(나)]은 단일호스트 대상 단일보안시스템의 경우보다는 상대적으로 덜 중요한 서비스 호스트들이 특정 네트워크에 연결되어 있는 경우 단일보안시스템으로 해당 네트웍 전체의 호스트의 보안을 처리하는 경우이다. 이때의 보안시스템은 다수의 호스트를 감시하기에 많은 기능을 제공할 경우 보호대상 호스트들의 병목지점(bottleneck)이 될 수 있다. 이에 대한 실례로 일반적인 기업이나 학교 등의 네트웍을 위한 보안시스템들이 있다. 다중호스트 대상 다중보안시스템[그림1.(다)]은 단일보안시스템으로 처리하기 힘든 보안문제를 해결하기 위해 나온 방법으로 다수의 분산된 보안 노드들에 의해 다중 호스트들의 보안을 처리하는 경우이다. 현재 많은 연구가 진행중이며, 아직 상용화되지는 않은 상황이나, 성능에 대한 기대로 인해 추후 많은 기관들에서 채용할 것으로 예측된다.

3.2 결함허용 기능

본 논문에서 정의하는 결함허용 기능은 고전적인 결함허용 기능 중 결함 탐지와 결함 조치이며, 시스템 결함허용과 판정 결함허용에 따라 표 1과 같이 분류한다. 결함허용 기능들의 세부적 구동방식 자체는 병렬·분산 시스템에서 오랜 기간 검증된 것임으로 새로이 정의하지 않는다. 각 기능들의 세부적인 설명은 3.3에서 결함허용 시스템 모델과 함께 기술한다.

표 1. 결함허용 기능

	시스템 결함허용		판정 결함허용
	단일시스템	다중시스템	
결함 탐지	모듈결함 탐지	시스템결함 탐지	판정오류 탐지
결함 조치	복구	재구성 및 복구	판정오류 수정

3.3 결함허용 시스템모델

결함허용 모델은 그림 2와 같이 계층화되어 구성되며 보안 시스템의 보호 대상 특성에 따라 선택된다.

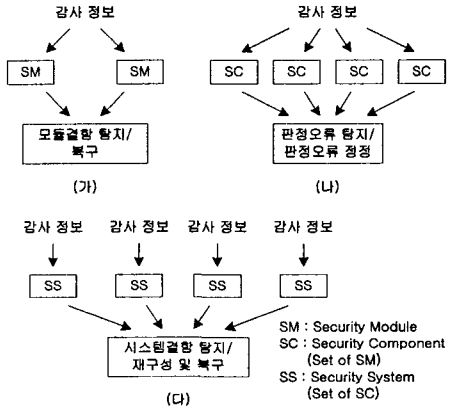

그림 2. 결함허용 시스템 모델
(가) 모듈 결함허용 모델, (나) 판정 결함허용 모델, (다) 시스템 결함허용 모델

모듈 결함허용 모델[그림2.(가)]은 동일 보안 판정을 하는 모듈을 중첩으로 구성하여, 특정 모듈에 문제가 발생한다 하더라도 그 문제를 찾고 해결할 수 있는 구조이다. 이 모델이 다루는 결함의 영역은 모듈의 비논리적 오류이며, 결함을 찾거나 복구하는 방법은 고전적인 결함허용 기법들 중 선택할 수 있다. 판정 결함허용 모델[그림2.(나)]은 모듈 결함허용 모델을 구성 요소로 포함해 보안 컴퍼넌트들의 비논리적 오류를 처리할 수 있으며, 다중 보안 판정을 하는 컴퍼넌트들의 판정을 수

집해 적절치 못한 판정을 한 컴퍼넌트들에 대해 튜닝한다. 이 모델이 다루는 결함의 영역은 컴퍼넌트의 논리적 오류이고, 보안 보안판정의 정확성을 높이는데 초점을 맞춘다. 결함을 찾는 방법은 고전적인 결함 탐지 기법을 선택할 수 있으며, 복구방법은 보안판정방법에 의존적으로 고안될 수 있다. 시스템 결함허용 모델[그림2.(다)]은 판정 결함허용모델을 구성 요소로 포함해 보안시스템의 논리적 오류를 처리할 수 있다. 이 모델은 독립적인 보안 시스템간의 상호 운용에 의해 시스템 오류를 탐지하며, 오류 발생 시 분산 보안시스템의 구조를 재구성하고 오류 발생 시스템을 복구한다. 결함을 탐지하는 방법은 고전적인 결함탐지 기법들 중 선택할 수 있으며, 구조 재구성 및 시스템 복구는 해당 분산 보안시스템의 구조 및 운용에 의존적으로 고안될 수 있다.

위의 세 모델은 계층적으로 배치될 수 있으나, 반드시 하위 계층을 포함할 필요는 없으며, 보호대상 보안시스템의 특성과 보호대상 시스템의 특성에 따라 다양하게 구성될 수 있다. 이를 위해 3.4에서는 결함허용 시스템 구성을 위한 기준이 되는 비용기반 선택 모델을 제안한다.

3.4 비용기반 선택 모델

보안 시스템을 위한 결함허용시스템에서는 다양한 결함허용 기능의 제공보다는 비용에 기반해서 대상 시스템의 특성에 맞는 기능만을 채택해 시스템을 구성할 필요가 있다. 결함허용 기능을 제공하기 위한 비용은 때로는 보안 시스템을 보호하지 못해 발생하는 비용보다 클 경우도 있으므로 두 가지 비용간의 비교를 통한 합리적인 시스템 구성이 필요하다.

다음은 개별 결함허용 기능의 비용 기반 선택 모델이다.

$$\begin{array}{l} \textit{if } (P[A_{FT}]\times C_d + C_{FT} > P[A_{NFT}]\times C_d) \\ \quad \textit{then 해당 결함허용 기능 수용} \\ \quad \textit{else 해당 결함허용 기능 비 수용} \end{array}$$

C_d : 피해 비용 C_{FT} : 결함허용기능 비용
$P[A_{FT}]$: 결함허용 기능 사용 시 문제 발생 확률
$P[A_{NFT}]$: 결함허용 기능 비 사용 시 문제 발생 확률

위의 모델은 세 가지 결함허용 시스템 모델에 모두 적용될 수 있으며, 이를 기반으로 상위 차원에서의 하위 결함기능에 대한 기대비용 $E[C]$을 다음과 같이 구할 수 있다.

$$E[C]=\sum Min(P[A_{FT}]\times C_d + C_{FT}, P[A_{NFT}]\times C_d)$$

기대비용 $E[C]$는 보안 모듈에 대한 보안 컴퍼넌트[그림2.(나)]의 기대비용과 보안 컴퍼넌트에 대한 보안시스템[그림2.(다)]의 기대비용 모두에 적용될 수 있으며, 다음과 같은 총 절약비용 C_S를 정의할 수 있다.

$$C_S=\{\sum(P[A_{NFT}]\times C_d)\}-E[C]$$

4. 기존 시스템에의 결함허용 시스템 모델 적용

제안한 결함허용시스템은 현재 나와 있는 다양한 보안도구에 적용할 수 있으며, 본 장에서는 대표적인 분산보안시스템인 AAFID, EMERALD, GrIDS에의 적용을 기술한다.

세부적인 결함허용 시스템 모델의 적용은 보안시스템의 특성뿐 아니라 보안시스템의 보호대상시스템의 특성에도 영향을 받음으로, 여기에서는 3.에서 제안한 시스템 모델이 각 분산보안 시스템의 어떤 요소에 적용될 것인가를 표 2로 정리한다.

표 2. 기존 분산보안시스템 대비 결함허용 시스템 모델

	모듈 결함허용	판정 결함허용	시스템 결함허용
AAFID	Filter, Agent, Moniter, Transceiver	Transceiver	Moniter
EMERALD	Monitor	Monitor	Monitor
GrIDS	Department (Node)	Department (Node)	Department (Node)

5. 결론

본 논문에서는 보안시스템을 위한 비용 기반 계층적 결함허용 모델을 제안했다. 이를 위한 결함허용 기능 자체는 전통적인 방법 중 선택하게 했으며, 보호 대상 보안시스템의 특성에 따른 기능 선택을 위해 계층적 구조를 갖는 결함허용 시스템 모델과, 이 시스템 모델의 선택을 위한 비용기반 선택 모델을 제안했다. 제안하는 모델은 현재 나와있는 각종 보안시스템에 적용될 수 있으나 보안시스템을 보호하기 위한 결함허용 기법의 초기 모델임으로 추후 각종 보안 사례 별 시스템 모델과 비용 모델에 대한 실제적인 실험 · 분석을 통해, 제안된 모델의 검증 및 세부적인 검토가 필요하다.

6. 참고문헌

[1] Lunt, T., et al. "A Real-time Intrusion Detection Expert System (IDES) - final technical report". *Technical report*, Computer Science Laboratory, SRI International, Menlo Park, California

[2] R. Jagannathan, T., et al. "System Design Document: Next-Generation Intrusion Detection Expert System (NIDES)". *Technical Report A007/A008/A009 /A011/A012/A014*, SRI International, Mar. 1993

[3] Phillip A. Porras and Peter G. Neumann. "EMERALD: event monitoring enabling responses to anomalous live disturbances". *In 1997 National Information Systems Security Conference*, Oct 1997

[4] S.R. Snapp, et al. "A System for Distributed Intrusion Detection". *COMPON Spring '91. Digest of Papers*. San Francisco, CA, 25 Feb.-1 March 1991, pp. 170-176

[5] S. Cheung, et al. "The Design of GrIDS: A Graph-Based Intrusion Detection System". U.C. Davis Computer Science Department Technical Report CSE-99-2, 1999

[6] S.J. Stolfo, et al. "JAM: Java Agents for Meta-learning over Distributed Databases", Proc. KDD-97, 1997

[7] J.S. Balasubramaniyan, et al. "An Architecture for intrusion detection using autonomous agents". In Proceedings of the Fourteenth Annual Computer Security Applications Conference, pages 13-24. IEEE Computer Society, December 1998

[8] Bhargava, A. Bhargava, B., "Applying fault-tolerance principles to security research," *Reliable Distributed Systems, 2001. Proceedings. 20th IEEE Symposium on*, 2001, Page(s): 68-69

[9] Kim, K.H., "Incorporation of security and fault tolerance mechanisms into real-time component-based distributed computing systems," *Reliable Distributed Systems, 2001. Proceedings. 20th IEEE Symposium on*, 2001, Page(s): 74-75

[10] S. Stolfo, et at. ""Cost-based Modeling for Fraud and intrusion Detection : Result from the JAM Project", *Proc. DARPA Information Survivability Conference and Exposition*, IEEE Computer Press, pp. II 130-144, 2000.