침입탐지 기법의 발전과정에 관한 연구

김지숙° 정유석 홍만표
아주대학교 정보통신전문대학원
{vipas°, j8508, mphong}@ajou.ac.kr

A Study on the Development Process of Intrusion Detection Methods

Jisook Kim° Yoosuk Jung Manpyo Hong
Graduate school of Information communication, Ajou university

요 약

공격이 다양해짐에 따라 침입탐지 기술기법에 관한 연구도 활발히 진행되고 있으나, 전반적인 연구 흐름에 관한 연구는 부족한 실정이다. 본 논문에서는 침입탐지 분야에서 오랜 기간 연구를 수행하여 대표적인 침입탐지시스템 프레임워크까지 제안한 세 그룹(SRI, UC Davis, Purdue)에서의 연구 내용을 분석했다. 그 결과 'The First IDS', 'Multi Target IDS', 'IDS Framework', 'IDS Framework Component and Application'의 4단계로 분류했으며, 이에 대한 각 그룹의 세부적인 연구 내용을 기술하고 각 기법들간의 발전 원인 및 전체적인 연구 방향을 살펴보고자 한다.

1. 서 론

정보통신기술의 비약적 발전은 정보화시대로의 전환을 가져왔고 인간의 삶을 더욱 풍요롭게 하는데 일조 했다. 그러나 이와 같은 긍정적인 측면의 증가와 함께 다양한 발전된 형태의 공격 도구를 등장시키는 원인이 되어, 현재에는 은닉화, 분산화 등의 특징을 지니고 짧은 시간에 큰 피해를 줄 수 있는 분산 서비스거부공격(DDoS)과 같은 복합적인 공격까지 등장했다.

특정 시스템의 버그나 취약점을 이용했던 초기의 공격 방법들은 단일 호스트에서 다른 호스트로의 일대일 공격이 대부분이어서 공격자 및 공격대상의 범위가 협소하고 그 피해 또한 현재에 비해 상대적으로 적었다. 이와 같은 공격에 대응하기 위해 1980년대에 들어서 다양한 침입탐지 기법이 연구되었는데, 이후 공격방법들이 다양해짐에 따라 그것을 탐지하고 대응하기 위한 공격방어기술도 함께 병행되어 발전되어 왔다. 그 결과 현재 GrIDS, EMERALD, AAFID로 대표되는 침입탐지시스템 프레임워크에 대한 연구까지 이루어졌다.

본 논문에서는 침입탐지 분야에서 오랜 기간 연구를 수행하여 대표적인 침입탐지시스템 프레임워크까지 제안한 SRI, UC Davis, Purdue의 세 그룹에서의 연구 내용을 분석하려고 한다. 이를 위해 각 그룹의 세부적인 연구 내용을 기술하고 각 기법들 간의 발전 원인 및 전체적인 연구 방향을 살펴 보고자 한다.

2. 관련연구

침입탐지 기법에 관한 연구는 컴퓨터과학의 다른 분야에 비해 짧은 역사지만, 괄목할만한 발전이 있었고 또한 많은 연구들이 진행되어 왔다. 따라서 초기의 침입탐지 기법에서부터 현재의 침입탐지시스템 프레임워크까지의 연구 흐름에 대한 구체적 분석은 관련 분야의 발전에 커다란 도움이 될 수 있다.

UC Davis에서는 1994년에 그때까지 발표된 침입탐지 기법들에 대한 포괄적 기술을 포함한 연구 보고서를 발표했다. 그 보고서에서는 초기의 침입탐지 기법부터 네트워크 기반 침입탐지 기법의 시초 모델들을 기술했다[1]. 그러나 현 시점을 기준으로 상당히 과거의 연구이기에 최근의 탐지 기법에 대한 내용이 포함되어 있지 않다는 단점이 있다. 또 다른 연구로 2000년에 발표된 침입탐지 현황에 관한 보고서[2]에는 최근 발표된 침입탐지시스템 프레임워크까지 소개하고 있으나 각 연구에 대한 단편적인 내용을 서술하는데 그치고 있다.

3. 본 론

3.1 침입탐지 기법의 분류

초기의 침입탐지기법부터 현재의 침입탐지시스템 프레임워크까지를 발전방향에 따라 다음의 4단계로 구별할 수 있다.

첫 번째 단계는 'The First IDS'로, 단일 호스트를 대상으로 이루어지는 공격을 탐지하기 위한 초기의 기법들이다. 이 기법들은 네트워크가 복잡화되기 이전에 제안된 것으로 단일 호스트 내에서 모아진 감사자료(audit data)를 통해 오용탐지 및 비정상적인 행위를 탐지한다.

두 번째 단계는 'Multi Target IDS'로, The First IDS에서부터 탐지 대상의 확장에 초점을 맞춘 기법들이다. 이 기법들은 멀티 호스트나 네트워크에서 이루어지는 공격을 탐지하기 위한 것으로 다수의 탐지 대상들로부터 수집된 감사 정보를 탐지 시스템에서 종합하여 판단한다.

세 번째 단계는 'IDS Framework'로, 새로운 공격 방법들에 대한 대응 기법의 확장을 가능하게 하는 프레임워크를 제시한 기법들이다. 이 기법들은 특정 공격 방법에 대한 구체적인 대처법을 제안하는 것 대신 사용자 재구성에 의한 침입탐지시스템의 확장에 초점을 맞추었다.

마지막 네 번째 단계는 'IDS Framework Component and Application'으로, 'IDS Framework' 기법 제시 이후에 수행된 세부적인 컴포넌트들, 실험, 공격대응 방법 및 시스템 최적화에 관한 연구들을 포함한다.

3.2 침입탐지 기법 분류에 따른 기존 연구들의 적용

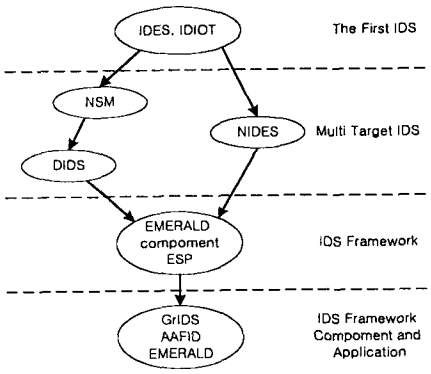

그림 1. 침입탐지 기법의 발전 단계

그림 1은 SRI, UC Davis, Purdue의 세 연구 그룹에서 제안된 대표적인 침입탐지 기법들의 발전 단계를 나타낸다. 그 중 초기 모델인 IDES와 IDIOT는 'The First IDS'에 속하고 NSM, DIDS 그리고 NIDES는 'Multi Target IDS'에 속하며 GrIDS, AAFID, EMERALD는 'IDS Framework'에 속한다. 또한 EMERALD Component 및 ESP는 'IDS Framework Component and Application'에 속한다. 이에 대한 세부 내용은 다음과 같다.

3.2.1 The First IDS

SRI의 IDES(intrusion detection expert system)는 단일 호스트의 감사자료(audit data)를 통해 통계적 절차를 사용하는 프로파일 기반 침입탐지와 룰 베이스를 이용한 전문가 시스템(expert system)인 규칙기반 침입탐지를 한다[3].

Purdue 대학에서 개발된 IDIOT(intrusion detection in our time)는 다중 페트리 네트워크(colored petri net)를 적용한 패턴 매칭 모델로, 감사 정보나 네트워크 패킷등의 데이터에 적용 가능한 오용탐지 모델이다[4].

The First IDS에 속하는 시스템들은 탐지하려는 대상이 단일 호스트이며, 따라서 단일 호스트에서 감사자료를 모아 침입을 탐지한다.

3.2.2 Multi Targer IDS

1990년대 들어서 SRI의 NIDES(Next generation IDES)는 두 가지 접근법을 사용하였다[5]. 그 중에서 첫 번째는 일반적인 사용자들에 의해 생성된 행동 표준으로 비정상적인 행위를 탐지하는 통계적 절차방법이고, 두 번째는 알려진 침입 시나리오 및 시스템 취약성을 전문가 시스템 규칙기반(expert system rule-base)을 이용해 탐지하는 방법이다. 여러 개의 에이젠(agen)은 각각의 대상 호스트로부터 감사자료를 받아 NIDES 포맷으로 변경한 뒤 에이알풀(Arpool)로 보내며. 에이알풀은 전달받은 감사자료를 모아서 분석요소에게 자료를 제공한다. 규칙기반 분석(rulebased analysis)과 통계적 분석(statistical analysis)을 통해 분석된 결과들은 응답기(resolver)에게 보내지고 여기서 중복된 경고(alert) 메세지는 걸러진 후 사용자 인터페이스를 통해 관리자에게 보내진다.

UC Davis에서는 1990년대에 들어 네트워크 기반의 침입탐지가 시작되었다. 이 연구그룹에서 처음 개발된 NSM(network security monitor)은 단일 브로드캐스트 랜에 관련된 보안 문제를 다루고 있으며, 이는 기존의 호스트기반 침입탐지시스템에서 사용된 방법론과 네트워크 모니터링을 잘 조화시키는데 초점을 두고 있다[6]. 그러나 단일 랜(LAN) 상의 커넥션(connection)만을 모아서 판단을 하기 때문에 인터 네트워크 기반의 공격을 탐지하기에는 부족한 점이 많다.

그 후 발표된 DIDS(distributed intrusion detection system)는 여러 개의 랜으로 이루어진 보다 큰 네트워크에서의 침입 탐지를 목적으로 한 연구로, NSM에 비해 정보수집 범위가 확대되었다[7]. 분산된 각 모니터로부터 수집된 정보는 이벤트의 형태로 수집되어 중앙에서 처리되므로 다양한 탐지 대상으로부터 모은 데이터를 종합해서 볼 수 있다. 기존 NSM의 범위를 확대시켰으며, 호스트 기반의 IDS도 활용하고 있다. 그러나 네트워크가 너무 커질 경우 그 규모를 감당할만한 구조는 되지 하여 추후 GrIDS를 통해 이와 같은 단점을 해결하려 했다.

Multi Target IDS에 속하는 시스템들은 멀티 호스트나 단일 네트워크 혹은 멀티 네트워크상에서 단일 호스트를 공격하는 것은 탐지하려는 것으로 여러 호스트로부터 감사자료를 받아서 보안시스템에서 분석하게 된다.

3.2.3 IDS Framework

SRI의 EMERALD(event monitoring enabling response to anomalous live distribution)는 감시와 응답의 작업 이원화로 분산된 감시 모니터를 통해 네트워크 요소들의 모니터링을 지향하고 있다. 각각의 모니터에서 독립적인 분석이 이루어지고 필요에 따라 관련 정보들을 상호 전달하여 종합적인 재분석이 가능한 구조로 되어 있다. 또한 이종 환경에서의 상호운용성과 재사용성 및 확장성을 제공한다.

Davis의 GrIDS(graph based intrusion detection system)은 계층적인 통합(hierarchical aggregation)을 통해서 상위 계층으로 정보가 전달되면서 필요 없는 정보를 제거하고 남는 정보들을 축약시켜서 보다 큰 네트워크를 관리할 수 있도록 하였다[9]. 또한 호스트들의 행위나 트래픽에 대한 정보를 수집하여 그래프로 그리므로 실시간으로 공격을 탐지하는 것이 가능하다.

Purdue의 AAFID(autonomous agent for intrusion

detection)는 모니터링을 수행하는 계층적 구조의 에이전트(agent)들을 이용해 침입을 탐지한다[10]. 에이전트는 시스템의 요구조건에 따라 추가, 삭제가 용이하며 오퍼레이터(operator)에 의해 시스템 환경에 적합하도록 설정할 수 있으며, 시스템의 오버헤드를 줄이고 새로운 공격에 대응할 수 있도록 수정될 수 있다. 또한 에이전트의 추가를 통해 인터 네트워크의 레벨로 확장이 가능하다.

IDS Framework에 속하는 시스템들은 대규모 네트워크상에서 단일 호스트 혹은 여러 호스트들의 공격을 탐지하기 위한 프레임워크를 제시하고 있다.

3.2.4 IDS Framework Component and Application

침입탐지시스템 프레임워크와 관련된 연구 결과물들은 기능적 측면의 확장과 더불어 시스템의 확장에만 초점을 맞추고 있기 때문에 이들을 실제 환경에 바로 적용시키기 위해서는 몇 가지 요소가 추가되어야 하며, 현재 관련된 연구가 한창 진행 중에 있다.

IDS Framework Component and Application으로는 보안 모니터링을 위한 application-integrate data collection에 관한 연구[11], 프로토타입을 이용한 EMERALD의 능력에 영향을 주는 요인에 관한 실험, 그리고 베이지안 네트워크를 이용한 탐지 메소드 제시[12]와 멀티센서로 이루어진 IDS에서 각 센서간의 경고를 효율적으로 활용하는 방안, P-BEST를 통한 오용탐지[13] 등이 있다. 이들은 실제로 IDS framework에 적용 가능한 구체적인 컴퍼넌트 기술들을 제시하고 있다.

또한 IDS Framework의 실제적 적용을 위해 AAFID의 호름을 이어받아 시작된 ESP(embedded sensor project)는 분산 침입탐지시스템의 한 형태로 시스템의 처리 시간을 감소시키기 위해 에이전트 대신 센서의 개념을 도입하였다[14]. AAFID의 에이전트는 단지 감사 정보나 네트워크 패킷 정보로부터 침입에 관련한 데이터를 모니터링하는 반면, 센서는 감사 정보를 발생시키는 시스템 자체의 특정 변수나 행동, 조건 등을 직접 모니터링한다. 이렇게 함으로 시스템에 주는 로드를 최소화하고, 수많은 감사 정보에서 필요한 내용을 추출하는 과정을 제거하였다.

4. 결 론

최근 20년간 다양한 침입탐지 기법들이 많이 연구되었고 또 계속적으로 진행되고 있으며 네트워크의 발전 또한 가속화되고 있다. 그러므로 공격방법들은 더욱 다양하게 변화되고 이에 따라 침입탐지 기법도 더욱 발전될 것으로 본다.

따라서 본 논문에서는 침입탐지 기법의 발전과정을 4단계로 분류하고, 기존의 침입탐지 기법들이 중점을 두었던 세부내용들을 분석함으로써 이들 모두 분류 방법에 따라 나뉠 수 있는 것을 보였다. 이는 사회적·기술적 배경 하에 시대적으로 유사한 흐름의 양상을 띠며 발전되어 온 것을 볼 수 있다. 각 단계별 특징과 원인 그리고 개선하고자 했던 요인들을 본 연구를 통해 살펴봄으로써 기존의 침입탐지 기법들을 정리하고 새롭게 나아갈 방향을 제시할 수 있을 것으로 본다.

5. 참고문헌

[1] Biswanath Mukherjee, L. Todd Heberlein, and Karl N. Levitt, "Network Intrusion Detection", *IEEE Network*, 1994.

[2] 김병구, 정태명 "침입탐지 기술의 현황과 전망", *정보과학회지*, 2000.

[3] Teresa F. Lunt, R. Jagannathan, Rosanna Lee,Sherry Listgarten, David L. Edwards, Peter G. Neumann, Harold S. Javitz and Al Valdes, "IDES: The Enhanced Prototype. A Real-Time Intrusion-Detection Expert System", *SRI*, SRI-CSL-88-12, october 1988.

[4] S. Kumar, E. H. Spafford, "A Software Architecture to support Misuse Intrusion Detection", 1995.

[5] D.Anderson, T. frivoid, and A. Valdes, "Next-generation intrusion-detection expert system (NIDES)", Technical report, *Computer Science Laboratory, SRI International*, Menlo Park, May 1995.

[6] L.T. Heberlein, "Network Security Monitor (NSM)", Final Report, *Lawrence Livermore National Laboratory project deliverable*, 1995.

[7] S. Snapp et al. "DIDS motivation, architecture and an early prototype.", *Proceedings of COMPCON*, 1991.

[8] Phillip A. Porras and Peter G. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", *1997 National Information Systems Security Conference*, pp.353-365, October 1997.

[9] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, D. Zerkle, "GrIDS -- A Graph-Based Intrusion Detection System for Large Networks", 1996.

[10] E. H. Spafford, D. Zamboni,"Intrusion detection using autonomous agents", 2000. (AAFID)

[11] Magnus Almgren and ULF Lindvist, "Application-Integrated Data Collection for Security Monitoring", *RAID 2001*, pp. 22 - 36, October 2001.

[12] Valdes, A. and Skinner, S., "Adaptive, Model-based Monitoring for Cyber Attack Detection", *Recent Advances in Intrusion Detection (RAID 2000)*, October 2000.

[13] Ulf Lindqvist , Phillip A. Porras, "Detecting Computer and Network Misuse Through the Production-Based Expert System Toolset (P-BEST)", *IEEE*, PP.146 - 161, May 1999.

[14] D. Zamboni, "Doing intrusion detection using embedded sensors - thesis proposal", *CERIAS Tech Report*, August 2000.