[5B-108]

네트워크 보안 시뮬레이션을 위한 SSFNet 기반 침입탐지시스템 구현

윤주범, 서정택, 최대식, 박응기*
국가보안기술연구소*
{netair,seojt,dschoi,ekpark}@etri.re.kr

Implementation of IDS for network security simulation based on SSFNet

National Security Research Institute

요 약

오늘날 네트워크의 방대화 및 복잡화로 인하여 현실세계를 정확하게 반영하는 네트워크 시뮬레이션을 진행하기는 쉽지 않다. 특히 사이버 침입 및 이에 따른 네트워크 행동 변화를 시뮬레이션 하기 위해서는 실제 네트워크의 정확한 모델링은 물론 각 서브 시스템의 특성을 네트워크 모델에 반영하여야 한다. 특히 정보보호 요소를 고려한 네트워크 시뮬레이션을 실시하기 위해서는 침입차단시스템과 침입탐지시스템의 모델링이 필요하다고 판단된다. 이에 본 논문에서는 프로세스 기반 사건 중심 시뮬레이션 시스템인 SSFNet을 기반으로 네트워크 보안 시뮬레이션의 핵심 요소인 침입차단시스템 클래스를 구현하였다. 정책 기반 오용 행위 탐지 방식의 네트워크 침입탐지 시스템을 시뮬레이터에 표현하고자 하였으며 그 구현을 위한 새로운 구조를 제안하였다.

1. 서 론

대규모 네트워크 상에서 벌어지는 사이버 침입을 가상의 시뮬레이션을 통해 관찰하기 위해서는 실제 네트워크 구조를 반영할 수 있는 네트워크 구성과 현실 세계의 컴퓨터 구성과 유사한 호스트 모델링을 기반으로 하는 시뮬레이션 환경이 갖추어 져야 한다.

NS-II와 함께 대표적인 네트워크 시뮬레이터인 SSFNet(SSF Network Models)은 DML(Domain Modeling Language)을 이용하여 손쉽게 대규모 네트워크를 디자인 할 수 있다. 또한 SSFNet이 현실 세계를 반영하는 호스트 모델링을 바탕으로 네트워크를 구성하기 때문에 사이버 침입과 관련해 현실 세계에서 벌어지는 모습을 보다 잘 관찰할 수 있다.

본 논문에서는 SSFNet 환경하에서 네트워크 보안 시뮬레이션의 핵심 요소인 침입탐지시스템 클래스를 구현하였다. 침입탐지시스템은 필수적인 인터넷 서비스의 접근을 허락함과 동시에 기관의 보안 레벨을 확실히 증가시킬 수 있는 최선의 솔루션을 제공하는 한 방식이다. 이는 완벽한 보안을 제공해 주지는 않지만 침입차단시스템과 더불어 네트워크의 보안도를 높이는 솔루션이다. 구현된 침입탐지시스템 클래스는 SSFNet과 같이 Java 기반으로 작성되었으며 사용자가 정한 탐지 규칙에 의해 내부 네트워크와 인터넷을 연결하는 사이에서 침입 패킷을 탐지하거나 비정상 패킷을 탐지하는 기능을 수행한다.

본 논문 구성은 2장에서는 관련연구를 살펴보고, 3장에서는 사이버 침입과 관련된 시뮬레이션 시스템 전체 구성에 대한 설명을, 그리고 4장에서는 새롭게 구현된 침입탐지시스템 클래스에 대해 좀 더 자세히 기술하였다. 끝으로 5장과 6장에서는 각각 본 논문에서 구현한 침입탐지시스템의 작동 결과와 결론에 대해 기술하였다.

2. 관련연구

SSFNet은 인터넷 프로토콜과 네트워크의 모델링과 시뮬레이션을 위한 자바 기반의 컴포넌트 집합이다. 네트워크를 위한 DML 작성 시 호스트 범위를 이용하여 서브 네트워크 중심으로 네트워크를 구성할 수 있다. 또한 각 호스트 설정을 미리 정의한 템플릿으로 구성할 수 있게 하는 DICTIONARY를 이용하여 각 호스트에 대한 프로토콜의 설정을 손쉽게 할 수 있다[2][3]. 그러나 DNS나 FTP 서버와 같은 모듈을 지원하고 있지 않아서 사용자가 직접 각 모듈을 구현하여 사용하여야 한다.

기존의 네트워크 보안 시뮬레이터[1]에는 침입탐지 시스템 모듈이 존재하지 않았다. 또한 기존의 네트워크 보안 시뮬레이터는 SSFNet의 IP 클래스를 확장하여 침입차단시스템 모듈 구현을 제안하였다. 이에 본 논문에서는 SSFNet의 IP 클래스를 확장하여 IDS_IP 클래스를 통해 침입탐지시스템을 구현하고자 하였다.