NGSS 시뮬레이션을 위한 SSFNet 환경에서의 보안 모듈 구현에 관한 연구

*박원주, *나중찬, **권오준, ***김대영
*한국전자통신연구원 정보보호연구단 네트워크보안그룹,
**동의대학교 소프트웨어공학과, ***충남대학교 정보통신공학과
*[wjpark,njc]@etri.re.kr, **ojkwon@deu.ac.kr, ***dykim@cnu.ac.kr

A study on the security module implementation for NGSS simulation on the SSFNet environment

*Won-Joo Park, *Jung-Chan Na, **Oh-Jun Kwon, ***Daeyoung KIM
*Information Security Development Division, ETRI
**Department Software Engineering, Dongeui University
***Information Communications Engineering, ChungNam National University

요 약

NGSS 는 전역통신망환경에서 공중망이나 ISP 망과 같은 전달망을 통과하는 트래픽에 대한 총체적인 보호와 함께 네트워크에 대한 침입을 능동적으로 탐지하고, 대응할 수 있는 고성능 네트워크 종합침해 대응시스템이다. NGSS 시스템을 실제 네트워크 환경에 적용하기 전에 설치와 유지보수에 따른 시간과 비용이 많이 소요될것으로 예상된다. 따라서 본 논문은 NGSS 의 각 인터페이스를 네트워크 시뮬레이션 도구 중 SSFNet 을 이용하여 모델링 및 시뮬레이션한다. SSFNet 을 사용하여 NGSS 이 기본 구성 요소인 SRS, SGS, SMS 를 구현하기 위하여 실제 네트워크를 모델링하고 IPS 를 구현한다. 또한 다양한 침입 요소를 적용하여 문제점을 파악하고, NGSS 의 성능을 평가한다.

I. 서론

현대 사회에서의 인터넷은 삶의 한 부분으로 자리잡고 있으며, 이 네트워크를 통한 타인의 불법적인 자료 유출 및 네트워크의 자체 마비 및 특정 서비스 서버로의 트랙픽 폭주등과 같은 사이버상의 위협적인 문제들이 빈번하게 발생하고 있다. 이런 위협방법들이 날로 다양하고 복잡하게 발전하고, 이 문제들을 해결하기 위해 부단한 노력을 기울이고 있는 상황이다.

그러나, 현재의 네트워크 보안은 기능 및 성능 면에서 많은 문제점을 가지고 있으며, 특히 정보보호 서비스는 통합보안시스템이 아닌 개별시스템 중심으로서 보안 시스템이 네트워크 접속 점에 위치하여 자기 도메인에 대한 보안만을 담당하고 있기 때문에 기능 집중 및 중복에 의한 전체 네트워크의 성능 저하는 물론 해킹 및 사이버 테러에 취약하다. 따라서 네트워크를 대상으로 한 사이버 테러 급증에 따라 네트워크 노드에서 실시간으로 대응할 수 있는 네트워크 보안 기술과 지식 정보화 사회를 안전하게 유지하고 네트워크 테러에 강력하게 대응할 수 있는 정보보호 인프라 구축이 절실히 필요하다.

이와 같이 네트워크 보안 분야는 기술적인 측면으로는 침입탐지 /차단에서 침입방지로 변화되었고, 시장적인 측면에서는 단일제품에서 통합제품으로 발전하고 있다. 이제는 공격자를 탐지하고 차단하는 것이 목적이 아니라, 공격자로부터 정상적인 사용자의 서비스에 대한 안전성 및 신뢰성을 제공하는 것이 더 중요해지고 있다는 것을 보여주고 있다. 특히, 공중망이나 ISP 망과 같은 전달 망의 액세스 망에 위치하여 전달 망을 통과하는 트래픽에 대한 총괄적인 보호를 통하여 차세대 네트워크 보안 서비스를 고객 사이트에게 제공하기 위해 개발한 시스템이 NGSS(Next Generation Security System)이다.

NGSS 시스템을 실제 네트워크 환경에 적용하기 전에 설치와 유지보수에 따른 시간과 비용이 많이 소요될것으로 예상된다. 따라서 본 논문은 NGSS 의 각 인터페이스를 네트워크 시뮬레이션 도구 중 SSFNet[1]을 이용하여 모델링 및 시뮬레이션한다. SSFNet 을 사용하여 NGSS 이 기본 구성 요소인 SRS, SGS, SMS 를 구현하기 위하여 실제 네트워크를 모델링하고 IPS 를 구현한다. 또한 다양한 침입 요소를 적용하여 문제점을 파악하고, NGSS 의 성능을 평가한다.

II. 본론

II.1 NGSS 시스템의 정의 및 구성

NGSS 는 전역통신망환경에서 공중망이나 ISP 망과 같은 전달망을 통과하는 트래픽에 대한 총체적인 보호와 함께 네트워크에 대한 침입을 능동적으로 탐지하고, 대응할 수 있는 고성능 네트워크 종합침해 대응시스템이다.

NGSS 시스템은 이상징후 수집 및 분석 기능을 포함한 보안 관리기능을 수행하는 SMS(Security Management System, 보안관리시스템)와 침입 탐지 및 이상 트래픽 감지 스템, 침입 차단 및 대응 시스템기능을 수행하는 보안 노드인 SGS(Security Gateway System,