네트워크 프로세서를 이용한 초고속 침입 탐지 시스템 설계 및 구현

조혜영[0] 김주홍 장종수* 김대영
한국정보통신대학교, 한국전자통신연구원
(hycho[0], scarlet, kimd)@icu.ac.kr, jsjang@etri.re.kr*

Design and Implementation of high speed Network Intrusion Detection System using Network Processor

Hye-Young Cho[0] Ju-Houng Kim Jong-Su Jang Daeyoung Kim
Dept. of Computer Science & Engineering, Information and Communications University, ETRI*

요 약

네트워크 관련 기술들이 테라급으로 급속히 발전하고 있는데 비해, 상대적으로 네트워크의 발전 속도에 뒤지고 있는 네트워크 침입 탐지 시스템의 성능 향상을 위해서, 기존의 소프트웨어 방식으로 구현된 침입 탐지 시스템을 고속의 패킷 처리에 뛰어난 성능을 가지고 있는 네트워크 프로세서를 이용하여 재설계 및 구현하였다. 네트워크 침입 탐지 시스템에서 대부분의 수행시간을 차지하는 네트워크 패킷을 분류하고, 이상 패킷을 탐지 하는 기능을 인텔의 IXP1200 네트워크 프로세서의 마이크로엔진이 고속으로 패킷을 처리하게 함으로써 네트워크 침입 탐지 시스템의 성능 향상을 도모하였다.

1. 서 론

최근 인터넷 사용이 활발해 지면서, 네트워크를 통한 해커들의 공격이 급속히 증가하고 또한 그 심각성이 날로 심해지고 있다. 이에 정보보호의 중요성이 더욱 부각되고 있으며, 이러한 네트워크를 통한 해커들의 공격을 탐지하고 그에 대응 하기 위한 네트워크 침입 탐지 시스템에 대한 연구가 매우 활발히 진행되고 있다.

그러나 초고속 인터넷 구축을 위한 네트워크 관련 기술들이 테라급으로 급속히 발전하고 있는데 비해, 상대적으로 침입 탐지 기술들은 네트워크의 발전 속도를 따라잡지 못하고 있다. 그 이유로는 대부분의 네트워크 침입 탐지 시스템들이 소프트웨어로 구현된다는 데 있다. 네트워크의 백본이나 액세스 망에서의 침입 탐지 시스템 구현을 위해서는 고속 침입 탐지 기술이 필수적으로 요구된다.

본 논문에서는 IXP1200 네트워크 프로세서를 이용한 고속 네트워크 침입 탐지 시스템 구조를 설계하였다. IXP1200 네트워크 프로세서는 칩 내부에 고속 패킷 처리가 가능한 여섯 개의 마이크로 엔진들과 이들을 제어하고 소프트웨어 수행이 가능한 StrongArm 마이크로 프로세서로 구성되어진다. 기존에 호스트 프로세서에서 소프트웨어 적으로 수행되던 패킷 분류나 침입 탐지를 위한 패턴 매칭과 같은 기능을 네트워크 프로세서가 탑재된 네트워크 정합 장치(Network Interface Card)로 최대한 이동함으로써 침입 탐지 시스템의 네트워크 트래픽 감시 속도를 향상 시킨다.

본 논문은 다음과 같이 구성된다. 기존 네트워크 침입 탐지 시스템의 문제점과 연구 방향을 제시한 서론에 이어 2장에서는 관련 연구를 통해 네트워크 프로세서와 기존 침입 탐지 시스템 특징에 대해서 분석하고 3장에서는 네트워크 프로세서를 이용한 고속 탐지 시스템 구조 설계 및 각 모듈의 기능을 설명한다. 마지막으로 4장에서는 결론 및 향후 연구 방향에 대하여 설명한다.

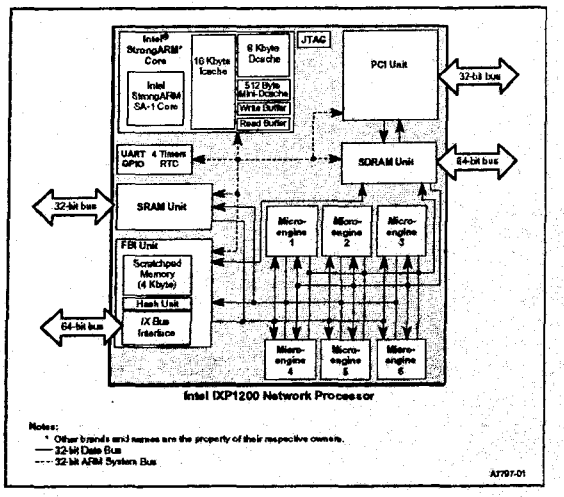
2.관련 연구

2. 1 네트워크 프로세서

네트워크 프로세서는 네트워크 프로토콜 처리 성능 향상을 위해 패킷 처리 기능을 강화한 특화된 구조를 가지며, 다양한 프로토콜을 수용할 수 있도록 설계된 프로그래밍 가능한 네트워크 전용 프로세서이다. 일반적으로 네트워크 프로세서는 현 네트워크상에 존재하는 다양한 패킷을 보다 효율적이고 신속하게 처리할 수 있는 다중 패킷 처리 구조를 제공한다. Intel, Agere(루슨트), Vittesse, IBM 등에서 상용 네트워크 프로세서를 공급하고 있으며, Network Processor Forum을 통해 표준화 작업들을 수행하고 있다.

2.2 IXP1200 네트워크 프로세서 구조

그림 1에 도시된 인텔의 네트워크 프로세서인 IXP1200은 StrongArm과 6개의 마이크로엔진 그리고 SDRAM, SRAM, PCI 버스 인터페이스로 구성된다. 6개의 마이크로엔진은 각기 4개의 하드웨어 쓰레드를 제공하며, 이는 고속 다중 패킷 처리에 효율적인 구조이다. 마이크로엔진의 수행능력은 ASIC의 속도보다 조금 떨어지지만 초당 300만개이상의 이더넷 패킷을 처리할 수 있을 정도의 처리 능력을 가지고 있으며, 고속의 패킷이나 프로토콜 처리에 효율적이다.[1]

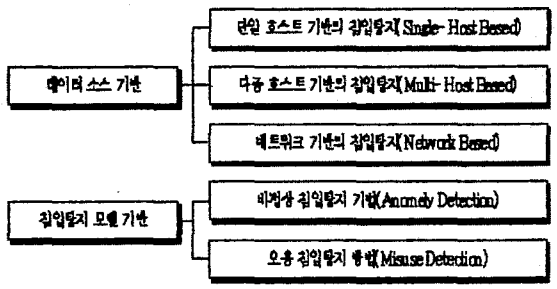


[그림1]네트워크 프로세서 IXP1200 블록 다이어그램

2.3 침입 탐지 시스템

침입 탐지 시스템은 네트워크이나 시스템으로부터 비정상적인 사용, 오용, 남용 등 미심쩍은 점을 조사 및 감시하여 침입 및 침입시도의 징후를 찾아내고, 필요한 조치를 취하는 시스템이다.

침입 탐지 시스템은 원시 데이터의 근원지에 따라 호스트 기반 방식과 네트워크 기반 방식 시스템으로 구분된다. 그리고 탐지 분석 방법에 따라 오용 기반 침입 탐지 방식과 비정상 기반 침입 탐지 시스템으로 나누어 질 수 있다. 오용 기반 침입 탐지 방식은 미리 정의된 침입 정보에 따라 비정상 패킷을 탐지하는 시그너쳐 분석 방법을 많이 쓰고 있고, 비정상 기반 침입 탐지는 침입 정보가 없는 미상의 침입 공격을 탐지 하는 기법으로 통계적 방법, 데이터 마이닝 기법, 또는 전문가 시스템 등을 많이 사용한다. 본 논문에서는 네트워크 기반 방식의 시그너쳐 분석 방식을 기본으로 채택한다. [2][3]



[그림2] 미국 COAST(Computer Operations, Audit, and Security Technology)의 분류

2.4 Snort

Snort는 현재 널리 사용되고 있는 네트워크 침입 탐지 시스템 중에 하나로 공개 소프트웨어이며, 다양한 플랫폼에서 사용될 수 있고, 성능이 우수하며, 유연성이 뛰어난 장점을 가지고 있다. Snort는 규칙(Rule)을 기반으로 하여, 탐지 엔진에서 패킷을 탐지 하고, 규칙에 기술 된 경고 조건에 따라, 일반 로그, tcpdump 포맷 로그, 실시간 경과, 윈도우즈 팝업 등 다양한 포맷으로 침입을 알려준다.[4]

Snort의 패턴 매칭 알고리즘은 처음에는 부분적인 Boyer-Moore 패턴 매칭 알고리즘을 사용하여 구현되었다. 그후 되풀이 되는 노드를 사용하는 (recursive node walking) 2차원 링크 리스트를 이용하는 방법이 도입되었고, 이 방법을 통해 snort 성능을 200~500% 높였다. 현재는 함수 포인터의 링크 리스트, 즉 3차원 링크 리스트를 사용하고 있다. 그리고 snort는 패킷을 캡처하기 위해서 libpcap을 사용한다. [5]

3. 고속 네트워크 침입 탐지 시스템 설계 및 구현

3.1 고속 네트워크 침입 탐지 시스템 설계 개념

현재 많이 사용되고 있는 소프트웨어 방식 침입 탐지 시스템은 패킷 처리속도가 낮아서, 고속 침입 탐지 시스템에는 적합하지 않다. 기존 소프트웨어 방식의 침입 탐지 시스템의 기능을 분석해 보면, 패킷을 실시간으로 모니터링 하면서, 침입 이상을 탐지 하고, 이상이 탐지 되면 그에 대한 보고등 반응을 보이는 구조로 되어 있다. 이러한 침입 탐지 시스템의 구조에서 가장 시간을 많이 소모하는 부분은 각 패킷이 이상이 있는지 분석 하는 탐지 엔진 부분이다. 이러한 소프트웨어 방식의 침입 탐지 시스템의 문제점을 해결하기 위해 인텔 IXP1200 네트워크 프로세서를 사용하여 고속으로 패킷을 처리 함으로써 성능을 향상시킨다.

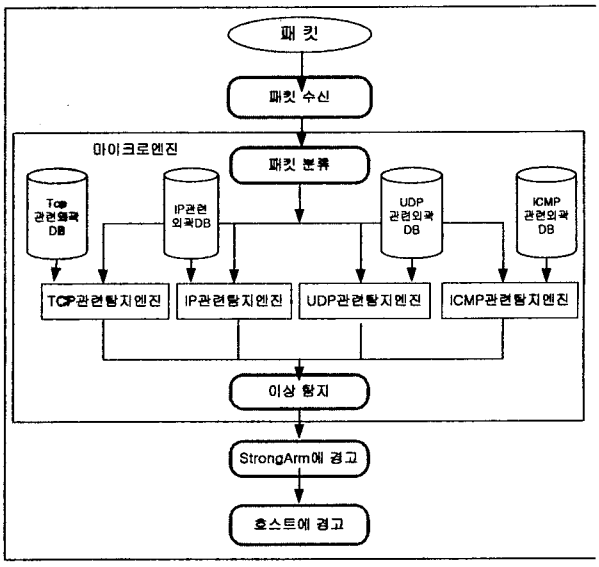
3.2 네트워크 프로세서를 이용한 침입 탐지 시스템 설계

아래의 그림3은 네트워크 프로세서를 이용한 네트워크 침입 탐지 시스템의 패킷 처리 절차도를 나타내고 있다. 마이크로 엔진은 IXP1200의 MAC 디바이스로부터 수신된 패킷을 프로토콜 종류에 따라 TCP, IP, UDP, ICMP로 분류한다. 각 프로토콜마다 하나 이상씩 존재하는 탐지 엔진 하드웨어 쓰레드가 미리 저장된 침입 규칙 데이터베이스와 패킷의 정보를 비교하여 이상 패킷을 탐지한다. 이상이 발견되면 마이크로엔진은 StrongArm에게 알리고, StrongArm은 호스트에 그 내용을 전달한다.

침입 시그너쳐 데이터는 IXP1200의 StrongArm이 호스트에 있는 룰 파일로부터 얻어서 SDRAM아나 SRAM에 저장한 것을 사용한다.

IXP1200의 마이크로 엔진은 각각 4개의 하드웨어 쓰레드를 가지는 RISC 엔진으로 StrongARM의 지원없이

고속으로 패킷 분류와 침입 탐지 엔진 기능을 처리할 수 있다. 마이크로엔진에서 사용되는 명령어 세트는 패킷을 최대한 빠르고 효율적으로 처리하기 위해 bit, byte, word, long word operation 을 포함하고 있으며, 패킷 처리 속도가 초당 300만개이상의 이더넷 패킷을 처리 할 수 있다. 침입 탐지 시스템에서 가장 많은 시간을 소모하는 부분인 패킷 분류와 각 패킷을 저장된 침입 시그너쳐 데이터베이스와 비교하여 이상 패킷을 탐지하는 부분을 속도가 빠른 마이크로엔진에서 처리함으로써 소프웨어방식의 침입 탐지 시스템에 비해 보다 향상된 처리 속도를 얻을 수 있다.



[그림3] 고속 네트워크 침입 탐지 시스템 패킷 처리 절차도

4.결론 및 향후 연구 과제

본 논문에서 구현하는 고속 네트워크 침입 탐지 시스템의 기본 설계 개념은 소프트웨어방식으로 처리되던 침입 탐지 시스템을 고성능 패킷 처리에 뛰어난 성능을 가지고 있는 네트워크 프로세서를 이용하여 구현하여 처리속도를 향상시키는 것이다. 이를 위해 본 연구에서는 소프트웨어 방식으로 구현되던 침입 탐지 시스템의 기능을 호스트 시스템과, 네트워크 프로세서인 IXP1200의 StrongArm과 마이크로엔진에 분배하여 처리하였다. 특히 고속 패킷 처리가 뛰어난 마이크로엔진에서 이상 패킷 탐지 엔진을 구현함으로써 침입 탐지 시스템의 성능향상을 도모하였다.

설계된 네트워크 프로세서를 이용한 고속 네트워크 침입 탐지 시스템에 따라, 현재 인텔 IXP1200 네트워크 프로세서가 장착된 Radisys ENP-2506p 보드를 사용하여 구현중에 있다. IXP1200 네트워크 프로세서는 개별 마이크로엔진의 명령어 저장 용량이 1024개로 제한되어 있기 때문에 1차 구현은 제한된 수의 시그너쳐 규칙을 이용하여 침입 탐지 시스템을 구현 중이다.

향후 계획으로는 구현 결과의 성능을 측정하고 기존의 소프트웨어 방식의 침입 탐지 시스템과 비교 분석할 것이다. 그리고 차후 발표될 IXP2400과 IXP2800을 이용하여 모든 시그너쳐 규칙을 수용할 수 있는 침입 탐지 시스템을 설계 및 구현할 것이며, 또한 현재 소프트웨어 방식의 침입 탐지 시스템에서 제공하는 다양한 기능을 추가해 나갈 것이다.

참고 문헌

[1] Intel, " IXP1200 Hardware Reference Manual" , Dec. 2001.
[2] Korea Information Security Agency, http://www.kisa.or.kr
[3] COAST(Computer Operations, Audit, and Security Technology), http://www.cerias.purdue.edu/coast/coast.html.
[4] Snort 홈페이지, http://www.snort.org.
[5]Neil Desai, "Increasing Performance in High Speed NIDS," A look at Snort' s Internals, 2002.