# 침입감내시스템의 실시간 자원정보 모니터링 기술 구현

유진택*, 소우영*
*한남대학교 컴퓨터공학과

# Implementation of Realtime Resource Information Monitoring Technology of Intrusion Tolerant System

Jin-Taeg Yoo, Woo-Young Soh
Dept. of Computer Engineering, HanNam University

요 약

침입 예방 및 탐지 기술에 대해서는 많은 연구가 진행되어 왔으나 침입이 발생한 후, 즉 공격이 성공한 후에도 필수 서비스가 유지되도록 하는 침입감내 연구는 아직 초기 단계이며, 최근 빈번한 침해 사고로 인하여 시스템에 대한 침입이 발생한 상황 하에서도 특정 서비스를 제공할 수 있는 침입감내시스템에 대한 요구가 매우 높다. 본 논문에서는 침입감내시스템에서 필수 서비스를 지속적으로 유지하기 위해 요구되는 실시간 자원정보 모니터링 모듈을 구현했다. 본 모듈은 프로세스 정보, 하드웨어 정보, 메모리 사용량, CPU 사용량, 네트워크 송·수신량 등을 모니터링 해주며 이 정보들은 관리자에게 제공되어 필수서비스를 선택 유지하는데 필요한 중요 정보로 활용될 수 있다.

## 1. 서 론

침해사고를 예방하고 효과적인 대응방법을 마련하기 위해 침입차단기술, 침입탐지기술 등 여러 가지 정보보호기술들이 개발되어 왔다. 그러나, 이와 같은 기술들은 알려진 취약점에 대한 예방과 탐지에 대해서는 좋은 결과를 보여주지만, 알려지지 않은 취약점이나 공격에 대해서는 적절한 대응이 쉽지 않은 단점이 있다. 또한 대개의 침해사고 피해 발생 시 중요한 서비스를 중단하게 되며 이 경우 매우 중대한 문제를 야기 시킬 수도 있다. 이와 같이 알려지지 않은 취약점이나 공격에 의한 침해사고 대응 방법이 요구되며, 침입감내시스템이 이에 대한 한 가지 해결책으로 제시되고 있다[1].

침입감내시스템은 시스템에 대한 악의적 공격이 발생하여도 일정한 수준이상의 서비스를 지속적으로 제공할 수 있도록 고안된 시스템이다[2]. 이러한 시스템은 시스템의 의존성 특징을 만족시키기 위한 여러 가지 기술을 적용함으로써 구축될 수 있다. 침입을 예방하고 탐지하는 기술에 대해서는 많은 노력을 해왔으나 침입이 발생한 후, 즉 공격이 성공한 후에도 필수 서비스가 유지되도록 하는 침입감내는 아직 연구초기 단계이다. 어떠한 상황에서도 임무를 반드시 완료해야 하는 시스템에서는 침입감내의 요구가 매우 높다. 일반적인 실시간 결함허용 시스템에 비하여 침입감내시스템은 보다 폭 넓은 유형의 결함에 대비할 수 있어야 한다. 하드웨어 결함이나 소프트웨어 결함뿐만 아니라 침입에 의해 발생할 수 있는 임의의 또는 악의적인 결함에 대한 대비책이 있어야 한다.

본 논문에서는 침입감내시스템에서 필수 서비스를 지속적으로 유지하기 위해 시스템 보안 정보 모니터링 모듈을 구현했다. 모니터링 모듈에서는 프로세스 정보, 하드웨어 정보, 메모리 사용량, CPU 사용량, 네트워크 송·수신량 등을 모니터링 해준다. 이러한 보안 정보들을 관리자에게 모니터링 해줌으로써 관리자는 필수서비스를 선택하고 유지할 수 있다.

본 논문은 다음과 같이 구성된다. 2장은 한국정보보호진흥원에서 연구되고 있는 필수 서비스 선택, 자원 재할당 및 중복구조에 대해서 설명하고 3장은 필수 서비스를 선택 유지하고 여분의 서비스를 중지 및 활용하기 위해 실시간 자원정보 모니터링 기술 설계 및 구현에 대해 논하고 4장에서 결론을 맺는다.

## 2. 관련연구

한국정보보호진흥원(KISA)에서 연구중인 침입감내시스템은 한 컴퓨팅 노드가 침입을 당한 경우에도 필수 서비스를 유지할 수 있도록 하는 필수 서비스 선택,

자원 재할당 방법, 중복 구조를 통하여 서비스 연속성을 제공한다[3].

### 2.1 필수 서비스 선택

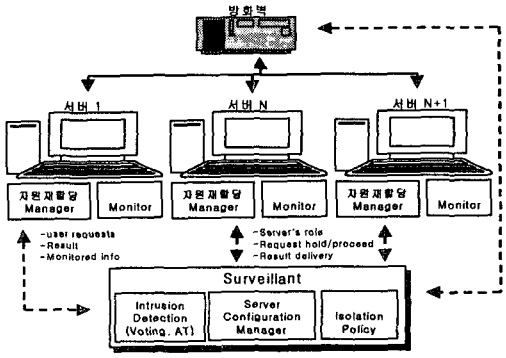
한 노드가 침입을 받으면 그 행위로 인해 노드가 가지고 있던 프로세서, 메모리 같은 컴퓨팅 자원과 통신할 수 있는 네트워크 자원의 손실이 발생하게 된다. 이 손실이 많아지면 정상적으로 수행하던 서비스를 제공할 수 없는 상태에 이르게 된다. 한국정보보호진흥원에서는 이러한 상황에 적응력을 발휘할 수 있도록 하기 위해 서버 관리자가 침입이 발생한 후에도 유지되어야 하는 필수 서비스를 사전에 선택하도록 한다. 선택된 필수 서비스를 실행하기 위한 최소한의 자원을 확보해두면 침입을 당한 후에도 서비스를 유지할 수 있다는 것이다. 물론 선택되지 않은 비필수, 즉 양보할 수 있는 서비스는 포기할 수도 있다.

### 2.2 자원 재할당

자원 재할당이란 필수 서비스가 필요로 하는 최소한의 자원이 존재하지 않는 경우 같은 노드 내에서 자원을 많이 보유하고 있는 양보 가능한 서비스로 하여금 자원을 반납하고 정지하게 하는 것이다. 즉, 동적으로 자원이 재할당되게 하여 필수 서비스가 생존하게 하자는 것이다. 필수 서비스가 생존하기 위해서는 일정 수준 이상의 CPU, 메모리, 네트워크 자원이 필요한데, 그 수준이 어느 정도인지 판단하기 어렵기 때문에 기준선(baseline)을 정하여 정상적인 경우에 필수 서비스의 자원 사용량은 기준선을 초과하게 되어 있다는 것이다. 기준선 초과 누적시간은 순간적인 자원 사용량의 변화에 대응하기 위한 것으로 일정 시간 간격 동안 기준선을 초과한 누적 시간인데 이를 기준선을 초과한 것을 판단하기 위한 임계값이다.

### 2.3 중복 구조

노드 내에서의 자원 재 할당으로도 필수 서비스의 품질을 유지하는데 필요한 자원이 확보되지 않으면 다른 노드에서 필수 서비스 제공이 유지되도록 N+1 서버 중복 방안을 제시한다[4]. N+1 중복 구조(그림 1)는 수용성 시험과 선출 방법을 같이 이용하는 방법이며 N개의 능동 노드와 항상 재 시도가 가능한(hot standby) 상태의 1개의 백업 노드로 구성된다.




(그림 1) 중복 방안이 적용된 시스템 구조

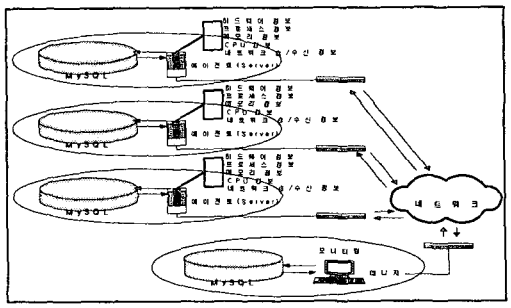
첫 번째 침입이 발생한 후에는 침입 감내 기능을 유지하지 못하는 문제를 해결하기 위해 일반 사용자는 접근할 수 없는 별도의 네트워크를 통해 연결된 감독자(Surveillant)가 이들을 관장하고 백업 노드는 침입 발생 시 재구성에 대비하고 있어서 신속한 재구성이 가능할 뿐만 아니라 재구성 후에도 계속되는 다른 공격에 대응할 수 있도록 하였다.

본 논문에서는 침입감내시스템에서 필수 서비스를 계속 생존 및 유지시키고 여분의 서비스를 활용 및 중지시키기 위한 실시간 자원정보 모니터링 모듈을 구현했다.

## 3. 설계 및 구현

### 3.1 네트워크 운용 환경

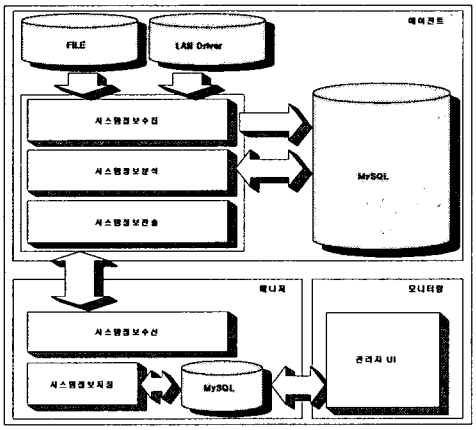
본 논문에서 구현된 Agent와 Manager는 네트워크 환경(그림 2)으로 운용될 수 있다. Agent는 다수의 서브넷에 설치될 수 있으며, 설치된 Agent로부터 시스템 주요 보안정보를 소켓 통신을 통해 실시간으로 전송 받아 저장하고 GUI 환경으로 모니터링 해주는 매니저 모듈로 구성된다.




(그림 2) 네트워크 운용환경

### 3.2 시스템 자원정보 모니터링 설계

본 논문에서 구현된 전체 시스템 구성도는 아래 (그림 3)와 같으며, 주요 서비스를 제공하는 시스템에 자원 정보를 얻어오기 위한 시스템 구성도이다. 이 구성도는 Agent 부분, Manager 부분, Monitoring 부분으로 나뉜다. Agent 모듈은 시스템의 파일이나 Lan Driver에서 시스템 주요 정보를 수집·분석하고 Agent 모듈 DB에 시스템 보안 정보를 저장한다.




(그림 3) 시스템 보안정보 모니터링 설계

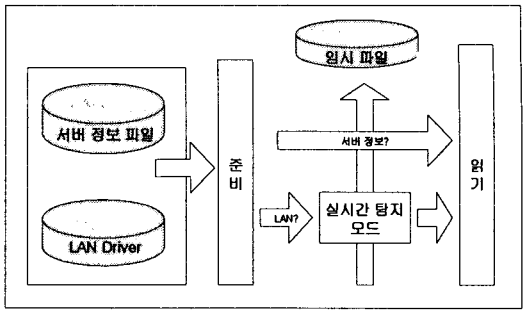
Agent 모듈에서 수집·분석하는 시스템 주요 정보들은 다음 표와 같다.

[표 1] Agent 모듈이 수집·분석하는 주요 정보

| 모 듈 | 시스템 주요 정보 |
|---|---|
| Agent 모듈 | 시스템 하드웨어 정보<br>시스템 프로세스 정보<br>시스템 메모리 사용량<br>SWAP된 메모리 양<br>시스템 CPU 사용량<br>시스템 네트워크 송·수신량 |

### 3.3 Agent 모듈

Agent 모듈은 자료수집의 모든 기능을 담당하고 있다. 각 Agent 서버로부터 CPU 사용량, Memory 사용량, 하드웨어 정보, 네트워크 트래픽 정보를 분석하는 등 다양한 자료를 수집하여 실시간으로 Manager 서버에 제공한다. 아래 (그림 4)는 주요 서버 시스템 안에 있는 파일로부터 데이터를 수집하고 네트워크 트래픽 분석을 위한 트래픽 량 정보를 네트워크 드라이버로부터 읽어 들인다. 본 논문에서 구현된 Agent 모듈은 리눅스 시스템에서 구현되었다.

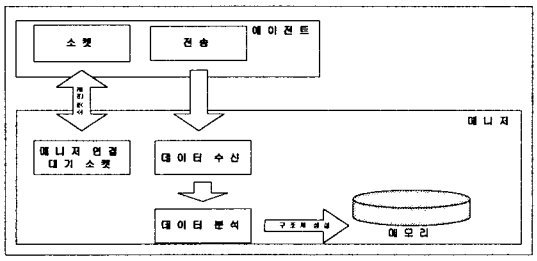



(그림 4) Agent 시스템 정보 수집

리눅스 시스템에서 시스템에 대한 정보는 /proc 디렉토리 안에 있으며 CPU 정보는 /proc/stat란 파일을 읽어 들임으로써 알 수 있고 메모리에 대한 정보는 /proc/meminfo란 파일을 읽어 들임으로써 알 수 있다. 네트워크 송·수신 패킷 수 및 양은 /proc/net/dev를 통하여 알 수 있다. 하드웨어에 관련된 정보는 여러 가지가 있다. CPU 정보는 /proc/cpuinfo, PCI 정보는 /proc/pci, 하드디스크 정보는 /proc/ide 디렉토리에 있다.

### 3.4 Manager 모듈

Manager 모듈은 소켓 연결 대기상태로 Agent의 접속을 기다리며 Agent의 연결이 성립되면 Agent로부터 전송되는 시스템 정보 데이터를 수신 받는다. 실시간으로 수신된 데이터들은 필드별로 분석되어 메모리에서 대기된다. (그림 5)는 Agent 모듈과 Manager 모듈 간에 시스템 정보 데이터 수신기능을 보여준다.

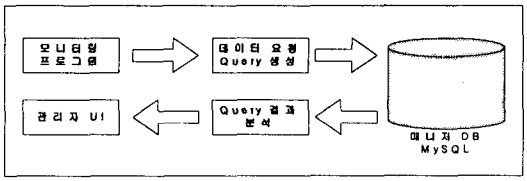



(그림 5) Manager 시스템 정보 데이터 수신

### 3.5 Monitoring 모듈

모니터링 모듈은 Agent에 의해 수집되어 Manager에 의해 축약되어진 DB로부터 다양한 시스템 정보 데이터들을 요청 및 수신한다. 수신된 시스템 정보 데이터들은 모니터링 모듈에 의해서 다양한 통계 정보를 생성함으로써 관리자에게 각 Agent 시스템에 관한 모니

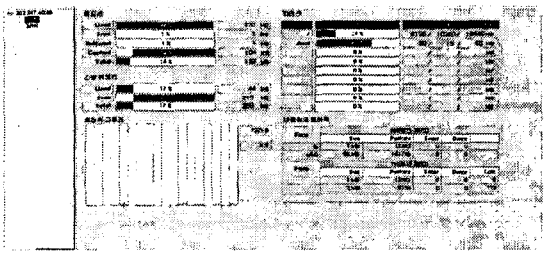
터링 기능을 제공한다. (그림 6)은 Agent 모듈과 Manager 모듈간에 시스템 정보 모니터링 기능을 보여준다.



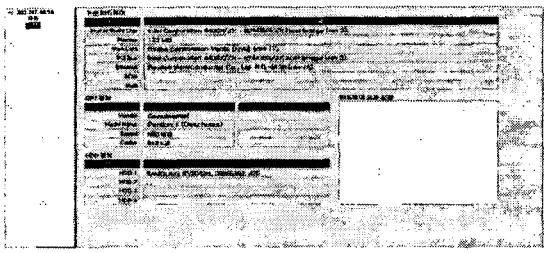

(그림 6) 모니터링 모듈의 시스템 정보 요청과 UI

### 3.6 구현

구현된 Manager UI 환경은 Delphi로 구현하였고 Agent하고 연결되면 아래 (그림 7) 왼쪽부분에 Agent IP주소가 보인다. Agent IP 주소에는 Agent 서버가 사용하고 있는 자원의 상태와 장비를 보여준다. 또한 메모리 정보와 하드디스크 파티션 정보, 네트워크 트래픽 량을 그래프와 수치 데이터로 표시하였다.



(그림 7) Agent 서버의 자원 사용량을 보여주는 UI



(그림 8) Agent 서버의 장비 상태를 보여주는 UI

(그림 8)은 Agent 서버의 장비 상태를 보여주는 것으로 Agent 서버의 하드웨어 장비 상태, CPU 장비 정보, 하드디스크 장비 정보를 보여준다.

이렇게 구현된 UI 환경은 Agent의 서비스 프로그램의 버전, 하드웨어 장비 상태, 자원(메모리, 하드용량, 스왑) 정보 등을 분석할 수 있고 윈도우 UI 환경에서 통합적으로 파악 할 수 있다. 또한 Agent 시스템의 네트워크 트래픽 량을 분석하여 접속 트래픽량 분포를 파악하고 네트워크 과부하 발생 시 원인을 파악할 수 있다.

이런 UI 환경 운용은 네트워크 침입 감내 시스템을 구축하는데 있어서 필요한 서비스와 자원 사용량을 파악하여 필수 서비스의 생존성을 높이는데 기본자료로 활용될 수 있을 것이다.

## 4. 결론

침해사고를 예방하고 효과적인 대응방법을 마련하기 위해 침입차단기술, 침입탐지기술 등 여러 가지 정보보호기술들이 개발되어 왔다. 그러나, 이와 같은 기술들은 알려진 취약점에 대한 예방과 탐지에 대해서는 좋은 결과를 보여주지만, 알져지지 않은 취약점이나 공격에 대해서는 적절한 대응이 쉽지 않다. 알려지지 않은 취약점이나 공격에 의한 침해사고 발생했을 경우에도 필수적인 서비스를 지속적으로 제공할 수 있는 침입감내시스템 기술이 요구되고 있다.

본 논문에서는 침입감내시스템에서 필수 서비스를 지속적으로 유지하기 위해 실시간 자원정보 모니터링 모듈을 구현했다. 모니터링 모듈에서는 프로세스 정보, 하드웨어 정보, 메모리 사용량, CPU 사용량, 네트워크 송·수신량 등을 모니터링 해준다. 이러한 보안정보들은 관리자에게 제공됨으로써 관리자가 필수서비스를 선택하고 유지하는데 필요한 매우 중요한 정보의 역할을 할 수 있다. 구현된 모니터링 모듈의 Agent는 현재 리눅스 상에서만 작동되기 때문에 유닉스 시스템, 윈도우즈에서도 작동되기 위해 별도의 Agent 모듈 개발이 필요하다.

## 참고문헌

[1] 최충섭, 이경구, 김홍근, "침입감내기술 연구 동향", 정보보호학회, 제13권 1호, 2003, 2.

[2] Matti A. Hiltunen, et. al., "Survivability through Customization and Adaptability: The Cactus Approach", DARPA Information Survivability Conference & Exposition, 2000

[3] 한국정보보호진흥원, "컴퓨터 보안기술의 진화", 정보보호심포지움, 2002, 7

[4] 민병준, 김성기, "서비스 거부 공격에 대비한 자원 재할당 및 서버 중복 방안", 정보처리학회논문지A, 제10-A권 1호, 2003, 3.