전자거래의 데이터 무결성 분석 자동화 시스템 설계 및 구현*

김 점 구**

요 약

전자거래상의 각종 사이버 침해 사고에 대처하기 위한 네트워크 보안 제품이 보급되고 있으나, 유지 관리 면에서 보안 전문가 정도의 전문 기술력이 요구되는 관계로 기업체나 공공기관에서 보안 제품의 설치 운영의 필요성은 절실하게 느낌에도 실제 보안제품의 보급이 빠르게 이루어지지 않아 국내 각종 사이트들에 대한 보안 취약성이 심각한 실정이다. 본 논문은 이러한 전자거래 환경의 보안관리를 비전문가도 효율적으로 관리할 수 있는 데이터 무결성 분석의 자동화 도구를 설계 구현하였다.

Design and Implementation of System for Integrity Evaluation on E-commerce*

Jeom Goo Kim**

ABSTRACT

Security products were developed and diffused for defense all emergency on cyberspace on E-commerce, but it requires special technique of information security in maintenance. The operation and need of security system was required in a public corporation and company, but it isn't provided in an appropriate time. Therefore, the domestic sites were vulnerable by security vulnerability. In this paper, we propose on the design and implementation of the data integrity analysis system that a novice manage usefully and automatically for management of E-commerce security products.

Key words : E-commerce Security Products

* 본 논문은 2004년도 산학협동재단 학술연구과제 지원에 의해서 이루어졌습니다.
** 남서울대학교 컴퓨터학과

1. 서 론

인터넷 이용자가 급증함에 따라 거기에 따른 해킹 및 바이러스에 의한 사이버 범죄, 개인정보 유출, 스팸메일·음란·폭력과 같은 정보의 범람 등은 사이버 공간에 대한 위협과 부작용이 심각한 사회문제로 되고 있다[13].

또한, 해킹를 하는 의도 역시 영웅심에서 직접적인 실리를 추구하는 경향으로 바뀌어 다종 다양화되고 일반화되었으며, 가장 실질적인 정보시스템인 전자거래 시스템을 직접 공격하는 예가 많아져 최근 들어 미국이나 유럽을 비롯한 선진국에서는 이러한 정보시스템의 보안성 인증을 위한 평가와 기존에 설치된 정보보호시스템의 보안성 유지 차원의 평가 방법에 대한 연구가 활발히 진행되고 있으며, 많은 평가 도구도 선보이고 있다. 그러나 국내는 그러한 도구가 전무한 실정으로 국내 기업체 등에서는 외국 보안 컨설팅 업체에 자사의 보안성 분석을 의뢰하거나 외국 분석 도구를 도입하여 운용하고 있다[12].

따라서 본 논문은 전자거래의 데이터 무결성 분석을 제안하고, 제안된 내용을 설계·구현한 전자거래 시스템의 무결성 분석 자동화 도구를 구현하였다. 전자거래 무결성 분석도구는 보안 비전문가도 쉽게 조직의 정보보호시스템 보안성 분석에 활용할 수 있으며, 분석 결과에 대한 객관적 신뢰를 가질 수 있도록 1999년 6월에 국제표준평가기준(ISO/IEC15408)으로 공식 인정된 국제공통평가기준(Common Criteria, CC)을 기반으로 하였다.

2. 보안 침해 유형

2.1 비밀성 침해

비밀성은 정보의 소유자가 원하는 대로 정보의 비밀이 유지되어야 함을 말한다. 비밀성 침해 공격은 사용자 시스템의 자원을 불법적으로 획득하는 행위가 해당된다. 파일시스템, 프로세스/쓰레드, 메모리 등이 그 주요 공격 대상이 된다. 주로 사용자의 파일시스템에 있는 사용자의 개인 정보 또는 시스템 정보를 유출하는 경우이다. 비밀성 침해 공격은 자바 Applet 및 자바스크립트를 이용한 침해 유형 중 가장 위험한 경우에 속한다고 할 수 있다. 인터넷의 활성화에 힘입어 온라인 뱅킹, 홈 트레이딩을 통한 주식거래 등이 도입됨에 따라 직접적으로 금전과 직결되는 주요 정보가 개인용 컴퓨터에 저장된 경우가 많다. 이러한 정보가 비밀성 침해 공격에 노출될 경우 아주 치명적인 결과를 낳을 수 있다[1].

2.2 무결성 침해

무결성은 데이터의 내용이 인가되지 않은 방식에 의하여 변경 또는 삭제되는 것을 방지하는 서비스로서 복구 기능을 갖는 접속 무결성, 복구 기능이 없는 접속 무결성, 선택 영역 접속 무결성, 비접속 무결성, 선택 영역 비접속 무결성 등과 같이 다섯 가지 형태로 구분된다. 무결성 침해 공격은 사용자 시스템의 자원을 불법적으로 수정 또는 변경하는 행위가 해당된다. 파일시스템, 프로세스/쓰레드, 메모리 등이 그 주요 공격 대상이 된다. 주로 사용자 파일시스템의 프로그램 또는 정보를 변경하거나 삭제하는 행위와 프로세스/쓰레드의 변경 및 강제 종료 등의 행위를 하는 경우를 말한다.

2.3 가용성 침해

가용성은 허가된 사용자가 원할 경우 자원을 이용하거나 접근할 수 있는 성질을 말한다.가용성 침해 공격은 사용자 시스템의 자원을 과도하게 사용하여 사용자의 정상적인 사용을 방해하는 행위가 해당된다. 파일시스템, 프로세스/쓰레

드, 메모리, 중앙처리장치(CPU) 등 기타 입출력 장치가 그 주요 공격 대상이 된다. 가용성 침해 공격은 비밀성 침해 공격이나 기밀성 침해 공격에 비하여 쉽게 구현 할 수 있기 때문에 그 코드의 개발 및 사용 빈도가 높다.

2.4 기존 무결성 분석 도구

2.4.1 AnalyZ

① 시스템 구조

(그림 1)의 Project Data Input은 위험관련질문을 통한 시스템 관련 정보를 입수하는 단계이다. Analyze Risks & Countermeasures는 입수된 정보를 토대로 위험분석기법을 이용한 위험수준측정 및 위험대책을 제시한다. Report Output은 결과를 정리 및 출력해 주며, Complete & Audit은 Project Data Input 단계와 Analysis Risks & Countermeasures 단계를 통해 얻어진 자료를 검증하고 선택되어진 위험대책을 저장한다[5].

② 특 징

AnalyZ는 비교적 사용이 용이하고 위험분석 과정이 간단하다. AnalyZ의 자체 보안구조 또한 만족할 만 하다. 그러나 위험 질문의 유형이 지나치게 외국 전산환경 및 상업 조직 등에 편중되어 있어 국내 실정에 정확히 맞지 않는 점이 단점이라 할 수 있겠다.

2.4.2 BDSS(Bayesian Decision Support System)

① 시스템 구조

BDSS는 정성적 외형 요소의 전반적인 구조와 정량적 취약성 및 위협의 행렬, 그리고 1900여 개의 제한된 대응책 등을 60여 개가 넘는 위협요소에 대하여 비용 효과를 포함하여 분석한다. BDSS는 운영상에서 발생될 수 있는 작은 위험요소들과 치명적인 주요 위험요소들의 관리체계를 지원함으로써, 정보시스템 환경운영의 비용 효과를 향상시킨다. BDSS는 위험을 받아들이거나, 피하거나, 이동시키는데 대한 결정을 만들기 위하여, 위험 관리능력을 직접적으로 지원한다[6].

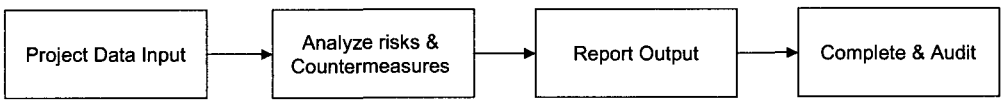
② 특 징

BDSS는 여러 위협, 자산, 대응책, 시나리오 등을 그래프에 근거한 종합적인 보고서를 산출한다. 이는 관리자로 하여금 분석결과의 이해를 돕고, 위험관리결정에 정확성과 확신성을 향상시킨다. BDSS는 정량 및 정성 분석 기술의 전문가에 의해 디자인되어졌으며, 기존 방식의 복잡하고 모순적이며 비효율적인 분석과정을 개선하였다.

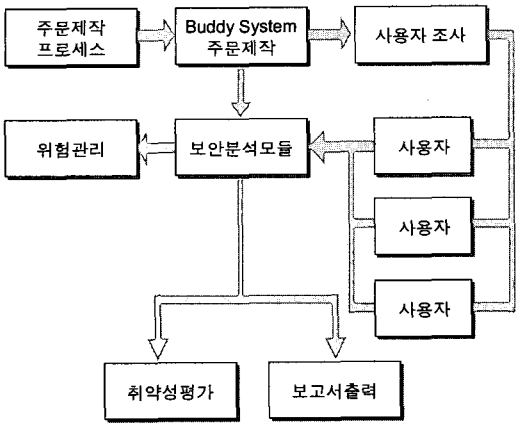
2.4.3 Buddy System

① 시스템 구조

버디 시스템의 전체 구조는 (그림 2)과 같이 3개 주요 부문으로 구성되어 있다. 보안 분석 모듈, 운용 모듈, 그리고 사용자 질문 모듈 등이다. 보안 분석 모듈은 취약성 분석, 위협과 대응책 확인, 그리고 기대 손실 값의 결과를 산출하는 분석 알고리즘을 이용한다. 운용 모듈은 보안 대응책의 실시, 감독 등 보안 관리 운영의 대부분을 조정한다. 모듈이 지니고 있는 과거 분석 로그는 향후 분석 자료로 쓰이며, 분석 결과에 대한 위험 관리자의 결정은 감리 분석을 위하여 기록되고 운영된다[10].



(그림 1) AnalyZ 보안성 분석 체계



(그림 2) Buddy 시스템 구조

또한 운영 모듈은 버디 시스템을 분석 대상 시스템의 환경에 맞추기 위하여 각각의 위협 요소와 대응책에 대한 무게 값을 변환시킬 수 있는 특성화 과정을 지원한다.

② 특 징

사용자 질문 모듈은 시스템 사용자의 이해를 돕고 쉽고 정확한 답변을 유도하고 있다. 또한 소형과 중·대형 등의 시스템 기종에 따라 시스템 사용자나 운영자로부터 시스템의 상태를 파악할 수 있게 하여준다. 분석을 진행하면서 보안 관리자에 의해 제안된 보안 규정의 정확한 준수를 위하여 질문 모듈을 통한 분석 조사는 전산망을 통하여 정기적으로 이루어진 후 보안 분석가에게 보내질 수 있다. 질문 모듈을 통하여 조사되고 수집된 시스템의 정보는 분석 모듈로 이식된다.

결과 및 보고 과정을 통하여 7개의 주요 보안 분석 보고서가 산출된다. 보안 분석 보고서, 사용자의 시스템 정보 종합, 취약성 종합, 감리·준수 측정, 다중 시스템 취약성 분석, 보안 관리 보고서, 그리고 현존 대응책 보고서 등이다. 결론에 따라 보안 관리자는 대상 시스템의 각 책임자로 하여금 적정한 조치를 요구하게 된다.

3. 전자거래 무결성 도구 설계

3.1 무결성 분석 요구사항

데이터 무결성에 대한 분석은 관리자의 오용, 환경 설정, 실수 등으로 인하여 안전한 데이터 전송이 되는지 여부를 분석한다. 무결성 분석도구는 VPN의 데이터 무결성 분석이 주목적이므로 데이터 근원지에서 목적지로 전송되는 패킷을 중간 가로채기와 변조, 재전송을 할 수 있는 기능을 가져야 한다. 그 밖의 기본적인 요구사항은 다음과 같다.

① 기존 보안성 분석 도구의 문제점들을 보완하고, CC의 분석기준을 바탕으로 한 표준화된 한국형 자동화 데이터 무결성 분석이 이루어질 수 있어야 한다.
② 분석 결과는 날짜별로 저장되어야 하며, 데이터 변조 시간, 재전송 시간이 출력되어야 한다.
③ 수시, 정기적, 그리고 반복 분석의 편의성 제공과 도구 사용자 인증이 필요하다
④ 분석 대상에 대한 무결성 기능의 정확한 동작 여부를 분석할 수 있어야 하며, 지속적으로 발전하고 있는 VPN제품과 더불어 새로운 기능 추가를 할 수 있는 확장성이 고려되어야 한다.
⑤ 수행 후 결과 분석을 쉽게 할 수 있도록 리포트 기능, 출력 기능 등의 부가적인 기능을 활용할 수 있어야 한다.
⑥ 사용자의 인터페이스를 시각화하여 활용의 편리함을 제공한다[11].

3.2 무결성 분석 제한사항

데이터 무결성 분석을 위해서는 송신측 패킷을 라우터에서 수신하여 패킷 변조모듈을 거쳐 새로운 패킷을 생성하여 수신측 호스트에 보내게 되고, 라우터에서는 수신측 응답 메시지를 받

아 패킷 수신의 상태를 파악하여 데이터의 무결성 여부를 판별한다. 세부적인 제한사항은 아래와 같다.

① 전송데이터의 무결성 기능을 실시간으로 측정하고, 분석하기 위해 국제 표준으로 자리잡고 있는 IETF에서 제정한 RFC 2401의 IPsec을 근간으로 한 암호화 및 인증 보안 기능을 커널에 포함시킨다.
② 호스트간에 교환되는 패킷을 변조하기 위해서는 Router가 필요하므로, Router 역할을 할 수 있도록 가상 네트워크를 구성한다.
③ IPsec이 적용된 환경 하에서의 데이터 통신의 무결성을 검증하기 위해서 Router의 커널을 패치하여 패킷 변조 기능을 커널에 포함시킨다.
④ IPsec이 적용된 환경에서 Router를 통하여 통신을 하도록 하고, Gateway에서 Attack을 했을 경우와 하지 않았을 경우 수신측에서 데이터의 무결성을 검사하는 것을 보인다.
⑤ 패킷 변조에 대한 정보를 사용자 입력을 통해 동적으로 설정하고 변경된 패킷에 대한 정보를 보여주기 위해 커널과 사용자간에 정보를 주고받는 방법을 커널 모듈을 통하여 구현한다.
⑥ 변조하는 패킷의 변조위치와 패킷 번호, 변조위치 등을 사용자 입력을 통해 동적으로 설정하고 무결성 보장 여부를 실시간 적으로 측정한다.
⑦ 응용 계층에서의 무결성 검증을 위해서는 패킷이 변조된 경우라도 트랜스포트 계층의 체크섬을 통과하여야 함으로 체크섬 값을 변경시키지 않고 변조하는 방법을 체크섬 계산 방식에 따라 구현한다.
⑧ 사용자가 편리하게 사용할 수 있도록 X-Window 프로그래밍을 통하여 사용자 인터페이스를 구현한다.

3.3 무결성 분석 방법

3.3.1 IPSec의 터널링 무결성 분석

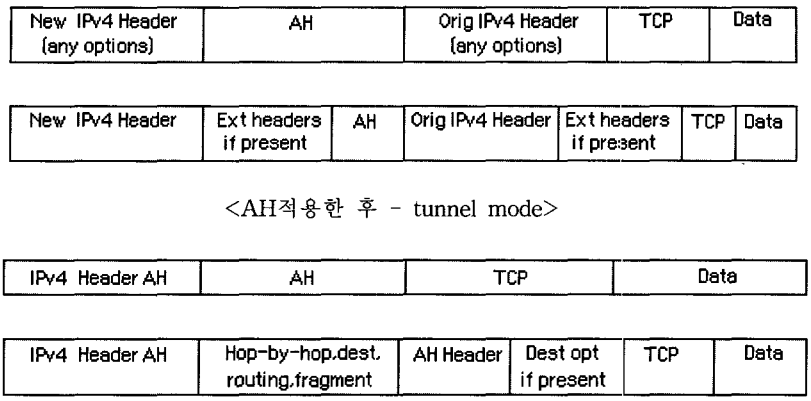
IPSec은 네트워크 통신의 패킷처리 계층 보안을 위해 지금도 발전되고 있는 표준으로서 VPN 구현에 가장 널리 사용되고 있는 보안 프로토콜이다. IPSec은 터널링뿐만 아니라 이에 필요한 각종 암호기술이나 무결성, 인증 등을 위한 총체적 보안을 제공하는 현존하는 가장 강력한 VPN 구현 기술이다[9].

무결성 분석도구에서는 이러한 IPSec이 적용된 환경 하에서의 데이터 통신의 무결성을 검증하기 위해서 게이트웨이의 커널을 패치하여 패킷 변조 기능을 커널에 포함시킨다. 그리고 IPsec이 적용된 환경에서 게이트웨이를 통하여 통신을 하도록 하고, 게이트웨이에서 Attack을 했을 경우와 하지 않았을 경우 수신측에서 데이터의 무결성을 검사하는 것을 보인다.

3.3.2 패킷 재전송 분석

인증헤더는 IP 데이터그램을 인증하기 위해 필요한 정보를 포함하며, 헤더 정보는 송신자가 인증된 데이터그램을 송신하기 직전에 구성하고 수신한 다음에 해제된다. 인증헤더를 사용함으로써 메시지 인증을 담당하는 코드에 의해 계산되어진 각 필드의 합산 값으로 수신자가 확인하여 데이터 무결성을 보장받으며, 데이터 인증 시에는 인증 시 필요한 키와 인증 알고리즘을 SA(Security Association)와 연계, 지정된 알고리즘을 수행하여 보장받는다. 또한 인증헤더에 있는 일련번호의 값으로서 재전송 방지를 할 수 있다[10].

AH(Authentication Header)는 받은 데이터의 근원지를 인증하기 위해서 MD5나 SHA-1과 같은 해쉬 알고리즘을 사용하여 데이터의 무결성을 보장하며, 또한 일련번호를 부여하면서 재전송공격을 방지할 수 있다. IPv4일 경우에 (그림 3)와 같이 AH는 IP 패킷의 IP헤더 뒤에 추가함



<AH적용한 후 - tunnel mode>

<AH 적용한 후-transport mode>

(그림 3) AH 적용 전과 적용 후의 IPv4 와 IPv6

으로서 인증을 보장하고, 터널링이 되었을 때 내부 IP헤더를 보호하게 된다.

그러므로 무결성 분석도구에서의 패킷 재전송에 대한 분석은 패킷제어모듈에서 전송되어지는 패킷과 동일한 일련번호의 패킷을 재전송모듈에서 재전송 공격케함으로써 재전송 되었을 때의 VPN이 이를 발견하는 지 여부로 패킷 재전송 분석을 하게 된다[8].

3.3.3 기밀성 분석

ESP(Encapsulation Security Payload)는 암호화 기법을 사용하여 AH에서 제공하지 못한 기밀성을 제공한다. 또한 무결성과 재전송 방지의 기능을 제공하는 프로토콜로서 사용하는 암호 알고리즘에 따라 인증 기능까지 제공할 수 있다. 인증헤더와 마찬가지로 ESP 키 관리는 철저한 보안이 되어야 하며, 키 관리 메커니즘과 보안프로토콜 메커니즘이 독립적으로 구현된다. 트랜스포트 모드에서 ESP의 기능은 원래의 IP 헤더는 보호하지 않고 IP 페이로드만을 보호하지만 터널 모드에서는 기존의 IP 헤더와 페이로드는 보호하고, 새로운 IP헤더는 보호하지 않는다. 또한 트랜스포트 모드는 데이터그램과 IP 헤더는 계속 유지되고, 원래 IP 데이터그램의 페이로드와 ESP 트레일러(Trailer)가 암호화되기 때문에 IP 헤더가 전송되는 동안 공격자에 노출될 수 있다. 터널 모드에서는 새로운 IP헤더가 만들어져서, 원래 IP 데이터그램과 ESP 트레일러는 암호화된다. 따라서 전송되는 동안 공격자가 헤더의 내용을 볼 수 없게 된다. 무결성 분석도구는 VPN 호스트간에 전송되는 패킷에 AH헤더와 ESP헤더가 IP헤더에 추가되었는지 전송 패킷의 프로토콜번호를 확인하고, 패킷제어모듈에서 수신측으로 보내지는 IP패킷의 헤더를 제외한 임의의 위치를 변조하여 수신측으로 보내에 VPN이 이를 찾아내는지를 확인함으로써 VPN의 기밀성 보증 여부를 분석한다.

무결성 분석도구 분석 모드에서 공통적으로 패킷 변조에 대한 정보를 보안 관리자가 분석시 입력을 통해 동적으로 설정하고 변경된 패킷에 대한 정보를 보여주기 위해 커널과 사용자간에 정보를 주고받는 방법을 커널 모듈을 통하여 구현하고, 변조하는 패킷의 변조위치와 패킷 번호, 변조 위치 등을 사용자 입력을 통해 동적으로 설정하여 무결성 보장 여부를 실시간 측정하도록 하였다[9].

4. 시스템 구현

4.1 구현 환경

무결성 분석도구를 이용하기 위한 분석 환경 구성은 라우터 역할을 하는 시스템에서 송신지와 수신지의 주소가 VPN을 적용한 호스트인지를 판단하여 IP 패킷을 변조, 혹은 재전송하여 무결성 분석을 수행하게 된다. 게이트웨이를 구성하기 위해서는 전송 데이터를 실시간으로 분석하여 패킷 변조와 재전송을 할 수 있도록 모듈이 탑재되었으며, 그 모듈은 gcc로 설계되었다.

(그림 4)에서처럼 Host A와 Host C간의 통신은 IPsec을 적용하여 무결성을 보장한다. 본 연구에서는 데이터 무결성을 탐지하기 위해 Free-BSD운영체제를 기반으로 하여 VPN을 구현해 보았다. 연구의 주요 핵심은 VPN을 구성하는 것이 아니라 데이터를 변조하여 무결성을 검증하는 것이므로 현재 본 연구에서는 Free-BSD로 무결성 검증 도구를 구현해 보았다. (그림 4)는 Host A와 C간에 통신을 할 때 Host B를 반드시 거쳐가야만 한다. 그러기 위해서는 Host B가 Gateway이어야만 하지만 실제로 Gateway를 설치하는데는 비용적인 측면이나 인터넷 주소 적인 측면에서 힘들기 때문에 Host B에 두 개의 이더넷 카드를 설치하고 라우터 역할을 하도록 하는 가상 네트워크를 구성하였다.

4.2 시스템 구성요소

① 관리 인증 모듈

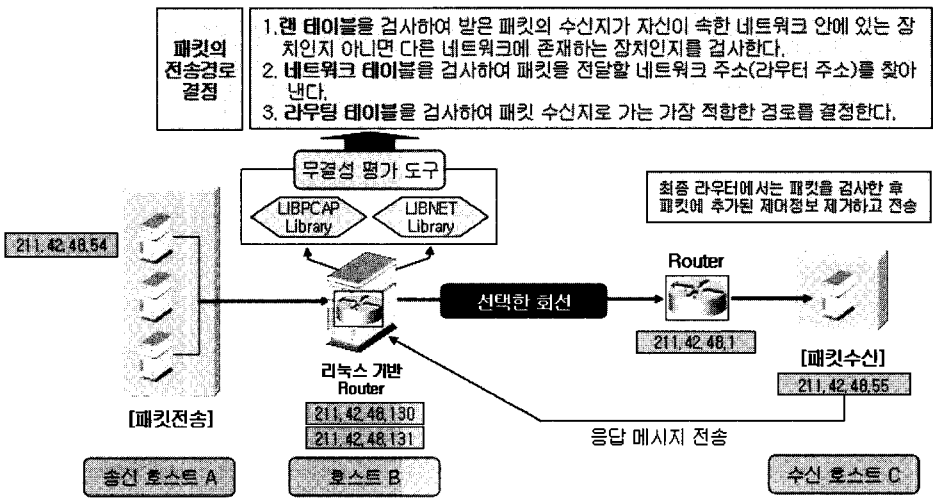
프로그램을 설치 후 실행했을 경우 Root 권한인지를 체크하고 분석을 하는 관리자의 인적사항을 등록하여 분석보고서 출력시 인적사항을 출력한다.

② 분석 설정 모듈

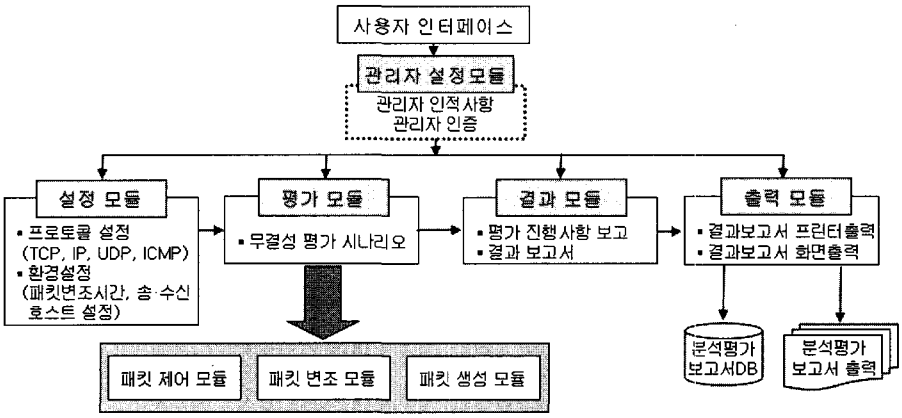
- 패킷 제어를 위한 프로토콜(TCP, IP, UDP, ICMP) 설정
- 패킷 변조를 위한 설정으로 송신측 호스트와 목적지 호스트를 설정 및 분석 시간 설정

③ 무결성 분석 모듈

- 패킷 변조 시간을 설정된 시간 간격으로 라우터에서 패킷을 받아 변조한 후 목적



(그림 4) 데이터 무결성 검증 도구 개발을 위한 구현 환경



(그림 5) 데이터 무결성 검증 도구 개발을 위한 전체 구성도

지 호스트로 새로운 패킷을 전송한다.

◦ 패킷 변조 결과를 저장 여부를 설정한다.

④ 분석 실행 모듈

◦ 위 단계에서 설정한 사항을 가지고 라우터에서 송신측 호스트의 패킷을 받아 목적지 주소와 네트워크 관리를 위한 제어 정보를 포함하여 패킷을 변조한 후 선택한 회선으로 패킷을 전송한다.

◦ 라우터에서 목적 호스트에서 변조 된 패킷 전송을 확인하여 패킷이 무결성 보장 여부를 체크한다.

⑤ 실행결과

◦ 인증모듈에서 등록한 관리자 인적사항을 출력하고 분석 시간을 출력한 다음 패킷 변조전의 내용과 목적지 호스트로 전송한 패킷과 목적지 호스트에서 받은 패킷을 출력한다.

⑥ 보고서 출력 모듈

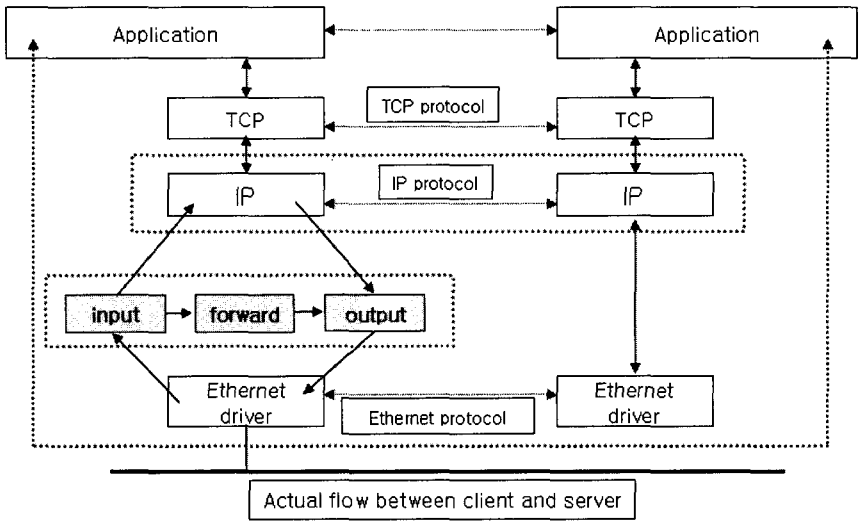
◦ 분석한 결과값을 관리자가 선택하여 분석 분석 보고서 데이터베이스에 저장하여 분석 DB를 만들거나 보고서 형태로 출력할 수 있다.

4.3 시스템 기능 모듈

4.3.1 IP 계층의 패킷 처리 과정

Gateway에서 데이터를 변조시키기 위해서는 우선 패킷이 IP계층에서 어떻게 처리되는지가 중요하다. LINUX에서 IP 처리과정은 (그림 6)와 같다.

먼저 네트워크 인터페이스에서는 들어오는 패킷을 인터럽트 큐에 차례대로 저장한다. 그리고 저장된 패킷을 큐가 빌 때까지 차례로 꺼내어 처리한다. 패킷을 조립할 것이 있으면 조립하여 데이터그램으로 만들어서 상위 프로토콜로 보내게 된다. 여기서 목적지 주소가 이 시스템의 주소와 맞지 않는다면 그 패킷은 forward를 따라서 output으로 보내져서 다시 네트웍으로 내 보내지게 된다. forward는 패킷을 전달해 주는 역할을 하는데 시스템이 라우터 역할을 할 수 있게 구성되어 있어야 한다. output이 하는 역할은 나가는 패킷에 대해 IP헤더를 완전하게 만들어 주는 역할을 한다. 그리고 output은 두 군데서 패킷을 받게 된다. 상위 프로트콜에서 오는 패킷과 다음 시스템으로 전달해 주는 역할을 하는 forward로부터 패킷을 받는다. Gateway에서 패킷을 변조시키려면 위에 설명된 세 부분 중 어



(그림 6) 리눅스 내부의 IP 패킷 처리 과정

〈표 1〉 IP 패킷 처리 모듈 기능

Module	Library	Function
input	LIBPCAP	네트워크에서 패킷을 capture하는 라이브러리를 사용하여 사용자 레벨에서 저수준의 네트워크 모니터링을 가능하게하는 인터페이스를 제공한다.
forward	없음	수신된 패킷이 현재의 시스템 주소와 맞지 않을 경우 output으로 포워딩한다.
output	LIBNET	네트워크 패킷을 만들 수 있도록 도와주는 라이브러리를 사용하여 로레벨에서의 패킷 생성 및 조작을 가능하게 한다.

디에서도 가능하지만 본 연구에서는 패킷을 포워딩 시켜주는 forward에 패킷 변조 처리 루틴을 추가한다

4.3.2 입력 모듈

입력 모듈에서는 송신측에서 보낸 패킷을 수신하여 ip헤더 및 체크섬 검사를 하고 패킷 변조를 위한 패킷 저장을 수행한다.

4.3.3 포워딩 모듈

수신된 패킷이 현재의 라우터 시스템 주소와 맞지 않을 경우, 패킷 포워딩을 위해 두 가지 주요 역할을 수행한다.

① Classifier and route selection : 패킷의 포워딩과 트래픽의 제어를 위해 유입되는 패킷들은 적절한 트래픽 클래스로 대응되어져야 한다. 클래스의 선택은 IP 헤더 내의 필드를 기반으로 결정된다. 이 기능은 패킷의 클래스와 목적지 IP 주소를 기반으로 각 패킷에 대한 다음 홉의 주소를 결정한다.

② Packet scheduler : 이 기능은 각 출력 포트에 대해서 하나 또는 그 이상의 큐를 관리한다. 즉, 대기하고 있는 패킷들의 전송 순서를 결정하며 필요시 폐기할 패킷을 선별하는 것이

다. 이 결정은 패킷이 속한 클래스, 트래픽 제어 데이터베이스의 내용, 그리고 해당 출력 포트의 현재와 과거 상태를 기반으로 이루어진다. 또한, 패킷 스케줄러는 플로우에서 패킷 트래픽이 요청된 용량을 넘어서는지에 대한 감시와 더불어 과도하게 유입된 패킷에 대하여 policing 기능도 포함한다.

4.3.4 출력 모듈

패킷을 포워딩 시켜주는 forward에 패킷 변조 처리 루틴을 거친 정보를 패킷을 새롭게 생성하여 목적지 호스트로 출력한다.

4.3.5 시스템 운용 효과 분석

VPN을 사용하는 기업이나 기관들이 정보가 누출되는지의 여부를 확인하고 신뢰할 수 있다는 것은 사용자와 개발자의 경쟁력 향상을 제공한다. 또한 제안된 분석 모델은 테스트 과정을 자동화하며 분석 결과를 통계화 할 수 있기 때문에 효율적인 관리를 할 수 있다.

〈표 2〉 입력 모듈 함수 처리 기능

함 수	기 능
pcap_t *pcap_open_live(char *device, int snaplen, int promisc, int to_ms, char *ebuf)	실시간으로 NIC를 통해 패킷을 가져오기 위해 사용되는 pcap_open_live()와 저장된 파일로부터 읽을 수 있도록 하는 pcap_open_offlie()이 제공
int pcap_dispatch(pcap_t *p, int cnt, pcap_handler callback, u_char *user)	패킷을 읽을 때 사용한다. 읽어서 분석하는 루틴은 파라미터인 callback으로 넘겨 처리한다
pcap_dumper_t *pcap_dump_open(pcap_t *p, char *fname)	캡쳐한 내용을 파일에 저장하기 위해서 파일을 오픈한다.
int pcap_compile(pcap_t *p, struct bpf_program *fp, char *str, int optimize, bpf_u_int32 netmask)	스트링 형태의 필터링 룰을 해석해 bpf_program 구조체에 저장한다
char *pcap_lookupdev(char *errbuf)	패킷을 캡쳐할 적당한 네트워크 디바이스(NIC : Network Interface Card)를 찾아 그 디바이스를 지칭하는 스트링을 리턴한다.
u_char *pcap_next(pcap_t *p, struct pcap_pkthdr *h)	다음 패킷의 포인터를 리턴한다. 내부적으로 pcap_dispatch()를 호출한다.

〈표 3〉 출력 모듈 함수 처리 기능

함 수	기 능
libnet_open_raw_sock (IPPROTO_RAW);	네트워크 삽입 인터페이스를 가져오기 위해 IPPROTO_RAW 프로토콜로 사용하여 처리하고 IP_HDRINCL과 raw소켓을 반환한다
libnet_build_ip (UDP_H + DNS_H + pl_len, 0, 7350, 0, 2, IPPROTO_UDP, src_ip, dst_ip, NULL, 0, tpack);	IP레벨에서 패킷을 생성하기의 함수이며 TCP 레벨에서는 libnet_build_tcp() 로 생성하며 Link 레벨에서는 libnet_build_ethernet()를 호출하여 사용
libnet_do_checksum (tpack, IPPROTO_UDP, UDP_H + DNS_H + pl_len);	패킷 체크섬을 계산하기 위한 함수
libnet_write_ip (sock, tpack, UDP_H + IP_H + DNS_H + pl_len);	IP 레벨에서 패킷을 기록하기 위한 함수

〈표 4〉보안성 분석 도구 비교

구 분	무결성 분석도구	BUDDY System	BDSS	AnalyZ
사용법	비전문가 용이	비교적 용이	전문가 용이	비교적 용이
시스템 가 격	저 가	중 가	고 가	상당 고가
방법론	정 성	정 성	정량/정성	정량/가능
유지비	저렴하다	비교적 고가	상당 고가	상당 고가
특 성	◦ 공공기관에서 개발 비영리) ◦ 국내최초(한글화, 위험분석 기본기능) ◦ NCA 개발 표준과 연계가능	◦ 민간기업에서 개발 ◦ 미 연방정부 정보 보안관리 규정 만족	◦ 위험의 기술적 측정을 그래픽화 ◦ 주요 위험요소들의 관리가 지원되어 운영비 효과 향상	◦ 자료입력의 순위 체계로 최대한 정확한 자료 제공 ◦ 질문을 통해 결과를 도출하기 위해 위험 질문의 분석 필요
신뢰도	◦ 시험적용 필요	◦ 미 연방정부를 포함한 20여개 이상의 공공기관에서 사용	◦ 축적된 DB와 Bayesian 모델과 결합하여 신뢰성 향상	◦ 질문의 유형을 세부항목으로 나뉘어 정확한 답변 유도.
보안관리	적용가능	적 용	적 용	적 용
단 점	◦ 정보수집을 위한 DB의 부족	◦ 분석가에 의한 자료 점검이 필요	◦ 이산적인 수량가치와 관리가 어렵고 높은 비용과 노동비용이 들어간다.	◦ 자료수집에 있어 사용자의 주관적 입장이 개입

〈표 5〉 도입 효과 분석

구 분	직접적인 효과	간접적인 효과
항 목	◦ 보안관리 효율 증대 ◦ 보안성 분석 비용 절감 ◦ 비전문가 활용가능	◦ 생산성 향상 ◦ 신뢰성 증대 ◦ 정보 보호의 제고 ◦ 경쟁력 향상
특 성	◦ 경비 절감 효과 ◦ 소극적인 효과	◦ 업무 효율의 제고 ◦ 적극적인 효과

5. 결 론

인터넷을 이용하여 데이터 전송 시에 무결성 확보는 매우 중요하다. 그러나 VPN을 비롯한 정보보호시스템이 예상치 못한 보안 문제가 발생하거나, 인터넷과 같은 공중망 보안취약점을 위협함으로써 작게는 개인에서부터 크게는 국가·사회 간접자원에 이르기까지 심각한 문제가 야기될 우려가 있다. 국내·외적으로 정보보호시스템의 성능과 신뢰성이 사용자로 하여금 충분히 검증될 수 있도록 객관적 분석 결과를 제공해 줄 수 있는 도구가 절실히 요구되며, 특히 보안 전문가가 턱없이 부족한 국내의 경우 보안성 분석 자동화 도구는 더욱 절실하게 요구되어지고 있다.

따라서 본 논문은 정보 통신망 정보보호 대책의 일환으로 국제공통분석기준을 기반으로 데이터 무결성 분석과 취약성 정보수집을 자동화할 수 있는 무결성 분석도구를 개발하였다. 그리고 이를 이용함으로써 망 차원의 데이터 무결성 보증이 용이하도록 하고, 나아가 기업이나 공공기관의 VPN 도입 확산과 국내 정보보호 산업의 활성화에 기여할 수 있을 것이다. 또한 무결성 분석도구는 비전문가도 쉽게 조작할 수 있도록

인터페이스와 도움말 기능을 한글화하였고, 분석 결과 역시 최대한 그래픽 기능을 이용하여 시각화하였다.

향후 연구 방향은 정보보호 서비스 전반을 보증할 수 있는 통합분석 도구의 개발에 대한 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] Internet Security - Mission Critical, Techpress Inc, 2001.

[2] W.Richard Stevens, "UNIX Networking Programming", Vol.1, 2nd Ed., 1998.

[3] Robert L. Ziegler, "Linux Firewalls", New Riders, 1999.

[4] Sean Walton, "Linux Socket Programming", SMS, 2001.

[5] AnalyZ Demonstration Copy User Guide, Zergo Limited, June 1993.

[6] Welcome to the World of BDSS, and OPA Inc. The Integrated Risk Management Group, OPA Inc., Janury 1995.

[7] ZUM Strarten hier kicken, "IP VPN Solution for Service Provider", Cisco Systems, May 1999.

[8] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[9] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload(ESP)", RFC 2406, November 1998.

[10] Zenkins, Buddy, Security Analysis and Management Manual, Countermeasures Inc, 1994.

[11] 한국정보보호진흥원, "국제공통평가기준(v.2.0)", 1998.

[12] 펜타 시큐리티 시스템(주), "자동화된 위험분석 툴의 구현", 2000.

[13] 정보통신부,"정보보호 중장기(2002~2006) 기본계획안", 2002.

김 점 구

광운대학교 전자계산학과 이학사

광운대학교 전자계산학과 이학석사

한남대학교 컴퓨터공학과 공학박사

(주) 제성프로젝트 연구원

(주) 시사컴퓨토피아 인터넷사업본부장

현재 남서울대학교 컴퓨터학과 교수

관심분야 : 정보보호, 컴퓨터 네트워크, 무선통신