응용계층 무선 보안 시스템 데이터 무결성 평가 도구 구현

김기욱*, 김창수*, 박지환*, 정민수**, 심규박***

*부경대학교 전자계산학과
**경남대학교 컴퓨터공학과
***동국대학교 전산통계학과

Implementation of Data Integrity Evaluation Tool for Mobile Security Systems in Application Layer

Ki-Uk Kim, Chang-Soo Kim, Ji-Hwan Park, Min-Soo Jung, Kyu Bark Shim
Dept. of Computer Science, PuKyong Nat'l University
Dept. of Computer Engineering, Kyungnam University
Dept. of Information Statistic, Dongguk University

요 약

이동 네트워크 기술의 발달과 이의 활용도가 증가함에 따라 무선 보안 시스템에 대한 연구 및 솔루션 개발이 활발히 진행중이다. 그러나 개발된 제품들의 신뢰성과 안정성을 검증할 만한 평가 도구 및 연구가 매우 미비하다. 따라서 본 논문에서는 이동 네트워크 보안 장비들의 안전성을 검증할 수 있는 응용계층 전송 데이터 무결성 평가 도구를 설계 및 구현하였다. 설계된 무결성 평가 도구는 Web서버와 이동 단말간에 전송되는 패킷의 데이터 변조 기능을 수행하는 변조서버 시스템과 무선 보안 시스템의 무결성 모듈이 변조된 데이터의 무결성 위반을 탐지하는지를 검증하는 무결성 검증 시스템으로 구성된다.

1. 서론

최근 CDMA기술의 발전과 이를 이용한 PDA 및 휴대폰 등의 무선 데이터 서비스 활성화로 이동 네트워크를 이용한 무선 인터넷 서비스가 활성화되고 있다. 그리고 안전한 무선 인터넷 서비스 사용을 위해 무선 인터넷 보안 솔루션 및 연구가 활발히 진행중이다. 하지만 현재 개발되어 있는 대부분의 무선 인터넷 보안 솔루션들은 보안 표준의 부재로 대부분 자체 표준에 근거하여 개발되었기 때문에 이들에 대한 신뢰성 검증이 필요하다. 국내·외의 정보보호제품 평가에 관한 연구는 1990년대부터 활발히 진행중이며, 국내에서도 1998년부터 침입탐지시스템(IDS)과 침입차단시스템(Firewall)에 대한 평가 기준을 마련하고 평가를 실시하고 있으며, 현재 약 20개의 Firewall제품과 10여개의 IDS제품의 평가가 완료된 상태이다[6]. 하지만 아직 이동 네트워크 보안 제품들에 대한 평가 기준 및 평가 방법은 미비하며, 국내에서 정보보호제품의 평가를 담당하고 있는 KISA(한국정보보호 진흥원)의 향후 제품 평가 일정에도 아직 포함되어 있지 않다. 따라서 본 논문에서는 국내·외의 정보보호제품의 평가 제도와 동향을 분석하고, '유선 VPN제품의 무결성 평가 방법'을 토대로 응용계층 무선 보안 시스템 데이터 무결성 검증 도구를 설계 및 구현하였다.

2. 관련 연구

2.1 국내·외 정보보호제품 평가제도

(1) 국외 정보보호제품 평가제도

국외 정보보호제품 평가 제도는 미국, 캐나다, 영국, 프랑스 등을 중심으로 1980년대 후반부터 연구가 시작되었으며, 각기 자국의 환경에 적합한 평가 제도와 평가 기준을 만들어 자국의 정보보호 제품 평가를 시행하고 있다. 미국은 NSA, NCSC주관으로 1985년부터 TCSEC(Trusted Computer System Evaluation Criteria)를 평가 기준으로 제정하고 운영체제, 네트워크 컴포넌트, 데이터 베이스 등의 제품에 대한 평가를 실시하고 있으며, C1, C2, B1, B2, B3, A1등 6개의 평가 기준을 제시하고 있다. 영국, 프랑스, 독일 등은 1990년 유럽 공통 평가 기준인 ITSEC (Information Technology Security Evaluation Criteria)를 제정하고 E1~E6의 6등급의 평가 기준을 근거로 정보보호 제품의 평가를 실시하고 있다[1,14].

(2) 국내 정보보호제품 평가제도

국내 정보보호제품 평가는 1998년부터 침입탐지시스템과 침입차단시스템을 대상으로 시행하고 있으며, 현재 정보통신부와 KISA를 중심으로 평가를 수행하고 있다. 국내 평가기준은 K1~K7의 7등급으로 구성되며, 2002년 8월부터 국제공통표준인 CC를 정보보호 제품 평가에 적용하고 있다. 현재까지 국내의 평가는 Firewall, IDS 제품에 제한되어 있지만, 향후 Smart Card, PKI 제품으로 확대될 예정이다[7,8].

(3) 국제공통평가제도(CC)

각국마다 다른 평가 기준으로 인한 비관세 장벽과 상호 접속 거부 등의 문제점으로 1993년 6월부터 각 나라의 정보보호제품 평가 기준을 통합하여 단일화된 평가 기준을 제정하려는 CC프로젝트가 결성되어 1999년 10월 2.1버전의 CC제정이 완료되었다. CC는 소개 및 일반모델(Part1), 보안기능요구사항(Part2), 보증요구사항(Part3) 등 3개 부분으로 구성되어 있으며 EAL1~EAL7 등 7개 등급 체계로 이루어져 있다[4].

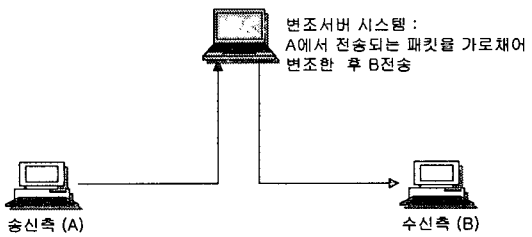
2.2 기존의 무결성 평가 연구 분석

(1) 무결성

데이터 무결성이란 송·수신되는 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 하는 기능을 말하며, 데이터 무결성이 보장되지 않는다면 정보 교환 시 메시지 도청 및 수정, 삽입, 송신자의 위장 문제 등이 발생할 수 있다. 따라서 데이터의 변조 공격으로부터 안전성을 제공하는 무결성 기능은 중요하며 보안 시스템들이 제공하는 무결성의 적합성을 검증할 필요가 있다[13].

(2) 유선 VPN제품의 무결성 평가 방법

현재까지 연구된 무결성 평가 방법은 KISA의 평가팀에서 제시한 '유선 VPN 제품의 무결성 평가 방법'이 있으며, [그림 1]은 KISA에서 제시한 평가 환경이다.



[그림 1] 유선 VPN제품의 무결성 평가

[그림 1]에서처럼 A에서 B로 전송되는 패킷을 중간의 변조서버 시스템에서 가로챈 후 패킷을 변조하여 B로 전송한다. 그리고 수신측의 VPN제품이 변조된 데이터를 인식하는지에 따라 무결성 평가를 수행한다. KISA에서 제시한 VPN제품의 무결성 평가 방법은 다음과 같다[12].

① 송신측(A)에서 암호화되어 전송되는 패킷을 변조서버 시스템에서 변조하여 수신측(B)로 전송

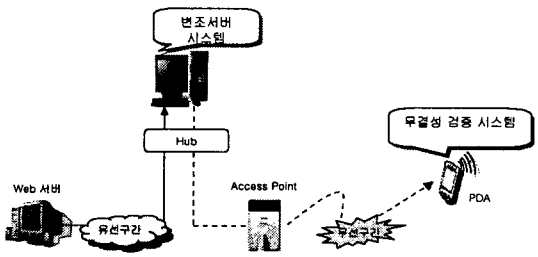
② 송신측(A)에서 암호화되어 전송되는 패킷을 변조서버 시스템에서 변조 없이 수신측(B)로 전송

3. 응용계층 무선 보안 시스템 데이터 무결성 평가 도구 설계 및 구현

3.1 시스템 전체 구성

본 장에서는 응용계층 무선 보안 시스템 데이터 무결성 평가 도구의 설계 및 구현에 대해 설명한다. 무결성 평가 도구는 크게 변조 서버 시스템과 무결성 검증 시스템으로 구성되며, 전체 구성도는 [그림 2]와 같다. 테스트 환경 구축을 위해 Web 서버와 이동 단말(PDA)사이의 이동 네트워크 환경을 내부망으로

구성하고 전송되는 데이터는 응용계층의 보안 프로토콜인 SSL(Secure Socket Layer)로 터널링 시킨다. 본 시스템을 통한 응용계층 무선 보안 시스템 데이터 무결성 평가 과정은 다음과 같다. 우선 무선 보안 시스템이 무결성을 제공하는지 검증하기 위해 변조서버 시스템에서 전송되는 데이터를 임의로 변조시켜서 PDA로 전송한다. 그리고 PDA에 탑재된 무선 보안 시스템이 변조를 확인하는지 여부는 무결성 검증 시스템에서 확인한다.



[그림 2] 무결성 평가 도구 전체 구성도

3.2 변조서버 시스템

본 단락에서는 구현한 시스템 중 변조서버 시스템에 대해 설명한다. 변조서버 시스템은 무선 보안 시스템으로 전송되는 데이터를 중간에서 가로채어 변조시킨 후 목적지로 전송하며 패킷 변조는 사용자가 선택한 조건에 따라 동적으로 수행된다. 변조서버 시스템은 RedHat Linux O/S와 gcc를 이용하여 구현하였다. 패킷 변조를 위한 변조 모듈과 동적인 변조정보 입·출력을 위한 사용자 인터페이스 모듈에 대한 설명은 다음과 같다.

(1) 변조 모듈

변조모듈은 Linux 시스템의 패킷 전송 원리를 이용하였다. Linux커널은 패킷이 전송될 때 효율적인 전송을 위해 네트워크 디바이스와 TCP/IP 계층사이에 3종류의 소켓버퍼(ip_input, ip_forward, ip_output)를 사용한다. 즉, Link Layer를 통과한 패킷은 우선 ip_input버퍼에 저장된다. 패킷의 목적지가 해당 호스트라면 전송계층으로 패킷이 전달되지만, 만약 그렇지 않다면 ip_forward와 ip_output버퍼를 통해 외부로 전송된다. 변조서버 시스템은 패킷 변조 모듈을 ip_forward 버퍼루틴에 구현하였다. 변조모듈에서 변조된 데이터는 ip_output버퍼를 거쳐 원래의 목적지로 전송된다[2,5].

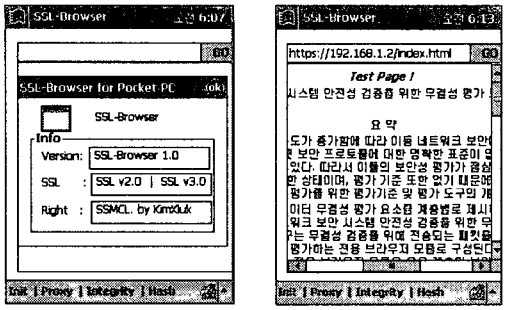
(2) 사용자 인터페이스 모듈

사용자 인터페이스 모듈은 변조 패킷에 대한 정보를 동적으로 생성하기 위해 구현하였다. 즉, 사용자가 선택한 조건에 따라 패킷을 변조하고, 패킷이 변조되었는지 확인하기 위해 변조 전·후의 패킷의 내용을 출력한다. 사용자 인터페이스를 통해 동적으로 생성할 패킷 변조 정보는 다음과 같다.

- Src Address : 변조할 패킷의 송신지 주소
- Dest Address : 변조할 패킷의 수신지 주소
- Packet No : 변조할 패킷의 순서 번호
- Interval : 변조할 패킷의 간격
- Location : 패킷의 변조 시작점

3.3 무결성 검증 시스템

무결성 검증 시스템은 무선 보안 시스템이 제공하는 무결성을 검증한다. 대부분의 무선 보안 시스템들이 무결성을 제공한다고 제품 스팩에서 제시하지만, 무결성이 위배된 데이터 처리 루틴을 별도로 구현하지 않기 때문에 사용자는 제품의 무결성을 검증할 수가 없다. 따라서 무결성 검증 시스템에서는 무결성이 위배된 데이터를 수신했을 때 처리하는 루틴을 구현하였다. 테스트를 위해 무선 보안 시스템을 Windows CE를 이용하여 SSL기능을 제공하는 전용 브라우저 형태로 구현하였고, 전용 브라우저에 무결성 검증 모듈을 첨가하였다. 그리고 무결성을 제공하는 해쉬 알고리즘의 적합성 평가를 전용 브라우저에서 수행할 수 있도록 하였다. [그림 3]은 무결성 검증 시스템의 실행화면이다. 좌측화면의 인터페이스를 통해 해쉬 알고리즘의 적합성을 평가하며, 적합한 해쉬 알고리즘은 미국 NIST의 표준 해쉬 알고리즘을 근거로 선정하였다. 우측의 그림은 SSL기능을 내장한 전용 브라우저의 실행화면으로 'https'접속 결과이다[3,9,10,11].



[그림 3] 무결성 검증 시스템 실행 화면

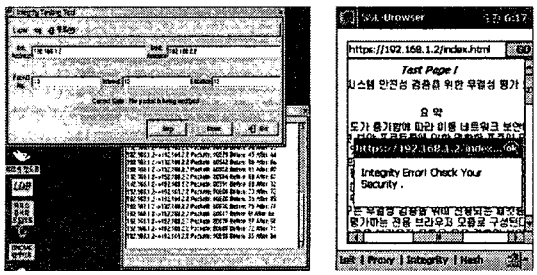
4. 구현 결과 및 평가

본 장에서는 본 시스템의 구현결과를 설명하고, 기존 연구와의 비교를 통해 본 구현물을 평가한다.

4.1 구현결과

(1) 무선 보안 시스템 데이터 무결성 평가

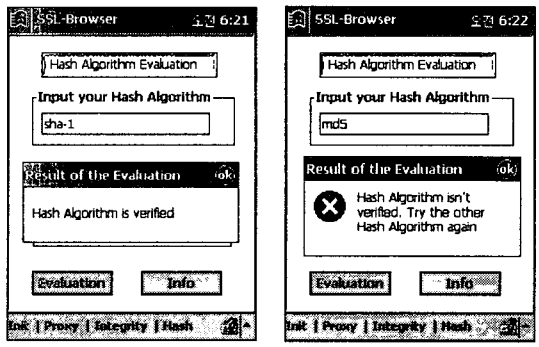
본 시스템을 테스트하기 위해 변조서버 시스템에서는 전송되는 데이터를 변조한 후 목적지로 전송하고, 데이터 변조를 무결성 검증 모듈에서 검증하는지 테스트하였다. [그림 4]는 무선 보안 시스템 데이터 무결성 평가 화면이다. 좌측화면은 변조서버 시스템의 출력 화면이고, 우측화면은 변조된 데이터를 수신했을 때 무결성 검증 시스템의 출력 화면이다. 변조서버 시스템의 사용자 입력 인터페이스를 통해 변조할 패킷 정보를 입력하고 변조 전·후의 패킷 내용을 확인할 수 있으며, 무결성 검증 모듈에서는 변조된 데이터를 수신하면 무결성 에러 메시지를 출력한다.



[그림 4] 무선 보안 시스템 데이터 무결성 평가

(2) 표준 해쉬 알고리즘 평가

무결성 모듈에 대한 평가를 위해서는 우선 사용된 알고리즘의 적합성이 검증되어야 한다. 따라서 본 논문에서는 무결성을 제공하는 해쉬 알고리즘에 대한 평가를 미국 NIST에서 제시한 표준 해쉬 알고리즘을 기준으로 수행하였다. [그림 5]는 표준 해쉬 알고리즘에 대한 평가 결과이다. 알고리즘 평가 과정은 다음과 같다. 무결성 검증 시스템의 알고리즘 평가 인터페이스에서 무선 보안 시스템에 사용된 해쉬 알고리즘을 사용자가 입력한다. 무결성 검증 시스템은 입력된 알고리즘이 NIST에서 제시한 표준 해쉬 알고리즘인지 검증하여 결과를 화면에 출력한다.



[그림 5] 표준 해쉬 알고리즘 평가

4.2 기존 연구와의 비교 및 평가

무선 보안 시스템 개발이 활발하지만 현재 이들의 신뢰성과 안전성을 보장할 수 있는 평가 방법 및 평가 도구는 미비하다. 따라서 본 논문에서는 무선 보안 시스템 데이터의 안전성을 검증할 수 있는 무결성 평가 도구를 구현하고 평가 방법을 제시하였다. 다음은 무결성 평가에 관한 기존연구와 본 시스템을 비교한 것이다.

(1) 평가 환경 측면

[표 1]은 평가 환경 측면에서 본 연구를 평가한 것이다. 기존의 무결성 평가는 유선 네트워크 환경의 네트워크 계층 보안 제품 평가를 수행하였다. 하지만 본 연구에서는 기존 연구의 평가 방법을 토대로 이동 네트워크 응용계층 보안 제품의 평가 방법을 마련하고 평가를 수행하였다.

[표 1] 평가 환경 비교

	기존 연구	본 시스템
네트워크 환경	유선 네트워크	이동 네트워크
평가 계층	네트워크 계층	응용계층
평가 제품	유선 VPN 제품	무선 SSL 제품

(2) 평가 내용 측면

[표 2]는 평가 내용 측면에서 본 연구를 평가한 것이다. 기존 연구가 데이터 무결성 만을 평가한데 반해 본 시스템은 보안 모듈 평가에 선행되어야 하는 알고리즘 평가를 추가하여 개선된 보안모듈 평가를 수행하였다.

[표 2] 평가 내용 비교

	기존 연구	본 시스템
평가 내용	데이터 변조 평가	- 데이터 변조 평가 - 해쉬 알고리즘 평가

5. 결론 및 향후 연구

이동 네트워크 보안 제품들의 신뢰성 향상과 발전을 위해서는 이동 네트워크 보안 시스템들에 대한 평가 방법 및 자동화된 평가 도구의 개발이 필요하다. 하지만 국내·외로 이동 네트워크 보안 시스템에 대한 평가 기준 및 평가 연구는 미비하다.

따라서 본 논문에서는 응용계층 무선 보안 시스템의 데이터 무결성 평가 도구를 구현하였고, 구현한 시스템은 변조서버 시스템과 무결성 검증 시스템으로 구성된다. 본 논문에서는 유선 VPN제품의 평가 방법을 참조하여 응용계층 무선 보안 시스템의 무결성 평가 방법을 도출하고 평가를 수행하였으며, 보안 모듈 평가에 중요한 요소인 알고리즘 평가를 수행하였다.

본 논문에서는 응용계층의 무선 보안 시스템 평가를 수행하였지만, 향후 연구에서는 응용계층뿐만 아니라 최근 이동 네트워크 보안에 활발히 적용되는 네트워크계층 무선 보안 제품에 대한 무결성도 함께 평가할 수 있는 평가 시스템 개발이 필요하다.

[참고문헌]

[1] National Computer Security Center, "Trusted Network Interpretation of The TCSEC", NCSC-TG-005, 1987.

[2] W Richard Stevens "TCP/IP Illustrated Vol. I" pp. 223-228 1995.

[3] Wagner,D. and Schneier,B., "Analysis of the SSL 3.0 Protocol," 2nd USENIX Workshop on Electronic Commerce Proceedings, 1996

[4] "Common Criteria for Information Technology Security Evaluation(CC)", Ver 2.0, http://scrc.ncsl,gov, 1998.

[5] R Magnus, U Kunitz, M Dziadzka, DVerworner, M Beck, H Böhme "Linux Kernel Internals" pp. 258-315, 1999.

[6] 한국정보보호센터, "정보보호시스템 평가·인증 가이드", http://www.kisa.or.kr, 2000.

[7]"정보통신망 침입차단시스템 평가 기준" http://www.kisa.or.kr/sysevaluation/menu1/sub2/index.html, 2000.

[8] "정보통신망 침입탐지시스템 평가 기준" http://www.kisa.or.kr/sysevaluation/menu1/sub2/index.html, 2000.

[9] Eric Rescorla "SSL and TLS", Addison-Wesley Press, 2001.

[10] 김기욱, 정경훈, 장용호, 김창수, "무선 인터넷 보안을 위한 SSL활용 연구", 한국멀티미디어학회 추계 학술발표 대회 논문집 제 4권 2호, pp.690~694, 2001.

[11] 김기욱, 정경훈, 김창수, "무선 인터넷 보안모듈 설계 및 검증도구에 관한 연구", 한국정보보호학회 영남지부 학술발표대회 논문집, pp.162 ~ 166, 2002, 2.

[12] "유선 VPN 제품 무결성 평가 방법", http://www.kisa.or.kr.

[13] 이만영, "전자상거래 보안기술", 생능출판사, 1999.

[14] Europen Commuication, "information Security Evaluation Criteria(ITSEC)", Ver 1.2, http://www.itsec.gov.uk