PDA환경의 응용계층 보안모듈 무결성 검증 시스템 설계 및 구현

김남진, 김창수
부경대학교 전자계산학과

Design and Implementation of Data Integrity Evaluation System for Application Layer Security Module in PDA Environment

Nam-Jin Kim, Chang-Soo Kim
Dept. of Computer Science, PuKyong Nat'l University

요 약

PDA를 이용한 무선 네트워크에 대한 활용도가 높아짐에 따라, PDA상에서 이루어지는 무선 네트워크 보안에 대한 관심이 증가하고 있다. PDA 무선 네트워크 보안 문제를 해결하기 위해 많은 연구 및 솔루션 개발이 진행되고 있으나, 이들의 신뢰성을 검증할 만한 시스템 및 연구는 제대로 이루어지지 않고 있다. 본 논문에서는 PDA환경의 무선 네트워크 응용계층 보안모듈들이 무결성 기능을 제대로 제공하는지를 검증 및 관리할 수 있는 시스템을 설계 및 구현하였다.

1. 서론

개인의 정보통신에 대한 수요 증가와 더불어 유선 통신에서 무선통신으로 그 무게중심이 이동하고 있다. 이러한 무선통신에 있어서도 데이터 중심의 비중이 높아지면서 등장한 것이 인터넷과 이동통신의 결합인 무선인터넷이다. 시장조사 전문 업체인 IDC에 따르면 2002년이면 이미 무선인터넷 인구가 유선인터넷 인구를 앞질러 7억 여명에 이를 것이라고 예상하고 있으며, 세미코 리서치는 2004년 인터넷 접속기기 시장에서 무선인터넷 접속용 전화기가 차지하는 매출 비중이 무려 42.1%에 달할 것으로 보고 있다[1-2]. 이러한 무선인터넷의 활용에 있어 PDA의 비중이 점차 확대되고 있고[4], 무선인터넷의 사용범위가 전송되는 데이터의 보안이 필수적인 모바일 커머스, 모바일 뱅킹, 모바일 트레이딩 등으로 확대됨에 따라 안전한 무선인터넷 서비스 사용을 위한 무선인터넷 보안 솔루션에 대한 연구가 활발히 진행되고 있다. 하지만, 현재 개발중이거나 개발되어 있는 대부분의 무선인터넷 보안 솔루션들은 무선인터넷에 대한 보안 표준의 부재로 인하여 대부분 자체적인 표준에 근거하여 개발되었기 때문에 이들의 신뢰성과 안정성을 검증할 만한 시스템 및 연구의 필요성이 대두되고 있다. 현재 국내에서는 1990년대부터 국내·외의 정보보호 제품 평가에 대한 연구가 활발히 이루어지고 있으며, 현재 침입탐지시스템(IDS)과 침입차단시스템(Firewall)에 대한 평가 기준을 제정하여 이에 따른 보안 제품들에 대한 평가가 이루어지고 있으며, 2003년 3월까지 25개의 침입차단시스템과 16개의 침입탐지시스템의 평가가 완료되었고, 약 10개의 제품들에 대한 평가가 진행중이다[5]. 하지만 아직 이동 네트워크 보안 제품들에 대한 평가 기준 및 평가 방법은 취약하며, 국내에서 정보보호제품의 평가를 담당하고 있는 KISA(한국정보보호 진흥원)의 향후 제품 평가 일정에도 아직 포함되어 있지 않다[3].

따라서 본 논문에서는 PDA 환경에서의 응용계층 보안모듈의 무결성을 검증하는 방법을 제안하여 PDA에 탑재되는 무선 보안제품들의 무결성 기능이 제대로 동작하는지를 확인할 수 있는 방법을 설명하고, 이를 위하여 무결성의 효율적인 검증 및 무결성 위배 유무 정보를 관리하기 위한 PDA 환경의 응용계층 보안모듈 무결성 검증 시스템을 설계 및 구현하였다.

2. 관련연구

본 연구는 대학 ITRC 연구지원에 의해 수행되었음.

2.1 국내·외 정보보호제품 평가제도

(1) 미국의 평가제도 및 평가방법

미국은 NSA, NIAP 주관으로 1985년 TCSEC (Trusted Computer System Evaluation Criteria)를 정보보호 시스템 평가 기준을 제정, 평가를 진행하고 있다. 미국의 평가기준인 TCSEC는 가장 오래된 정보보호 시스템 평가기준으로 DB, Network, O/S 등 다양한 분야의 보안제품에 대한 평가를 실시하고 있다. TCSEC는 가장 높은 등급인 A1부터 B3, B2, B1, C2, C1, 그리고 부적격 등급인 D급으로 나누어 평가등급을 적용하고 있다[7].

(2) 유럽의 평가제도 및 평가방법

영국, 독일, 프랑스 및 네덜란드 등은 정보보호 제품의 평가에 소요되는 시간, 인력, 소요비용을 줄이기 위하여 4개국 공동 평가기준인 ITSEC (Information Technology Security Evaluation Criteria)를 제정하였다. ITSEC는 최고등급인 E6, E5, E4, E3, E2, E1 등급과 부적합 판정등급인 E0 등급으로 나누어지며, 보안기능 요구사항과 보증 요구사항으로 이루어져 있다[8].

(3) 한국의 평가제도 및 평가방법

국내 평가제도는 1996년 8월에 제정된 정보화 촉진 기본법을 바탕으로 침입차단시스템 평가기준과 침입탐지시스템 평가기준을 제정하여 한국정보보호센터에서 평가를 시행하고 그 결과는 국정원에서 인증하고 있다. 국내의 평가등급은 최고등급인 K7부터 K1등급의 7등급으로 구성되어 있으며, 보안기능 요구사항과 보증 요구사항으로 구성된다. 현재 국내의 평가기준은 침입차단시스템과 침입탐지시스템의 두 가지 제품에 대해서만 평가가 이루어지고 있으나 향후 스마트카드나 PKI 제품으로 확대될 예정이며, 2002년 8월부터 국제공통평가기준(CC)을 정보보호 제품 평가에 적용하고 있다.

(4) 국제공통평가제도(Common Criteria)

각 나라마다 서로 다른 정보보호 제품 평가기준으로 인한 비용과 인력문제, 제품간 상호 인증 문제 등으로 인해 평가기준 통합 필요성이 대두됨에 따라 미국, 캐나다, 프랑스, 독일, 네덜란드 및 영국 등 6개국의 참여로 통일된 정보보호제품 평가기준인 국제공통평가기준(Common Criteria : CC)이 제정되었다. CC는 소개 및 일반모델(Part1), 보안기능 요구사항(Part2), 보증 요구사항(Part3), 정의된 보호 프로파일(Part4), 보호 프로파일 등록절차(Part5)의 5개 부분으로 구성되어 있으며, EAL1~EAL7 등급의 7개 등급 체계로 이루어져 있다[9].

2.2 무선 SSL(Secure Socket Layer) 솔루션

SSL은 Netscape Communication사에서 웹 보안을 위해 개발한 응용 계층의 보안 프로토콜로 데이터의 암호화 및 서버인증, 메시지 무결성을 제공한다[6]. 유선과 무선에서의 SSL 프로토콜의 기능 및 내용은 유사하나 무선 인터넷 환경의 제약으로 구현방법 및 암호 알고리즘, 구현용량 등에 차이가 있으며, 상용화된 대부분의 무선 SSL 제품들은 자체 표준에 의해 구현되고 있다.

(1) 소프트포럼[10]

무선환경에서 SSL을 적용한 MSSL을 개발하여 End-to-End Security를 제공하며, SEED 암호 및 전자서명을 지원한다. SSLv3.0 프로토콜을 사용하고 있다.

(2) IA Security[11]

타원곡선 알고리즘을 TLS 1.0에 적용한 무선 인터넷 보안 솔루션을 개발하였고, 현재 제정중인 무선 공개키 인증서 프로파일을 이용하여 WPKI 인증 시스템과 연동이 가능한 제품을 개발하고 있다.

(3) 이니텍[12]

무선인터넷 보안 프로토콜인 WTLS 1.2를 기반으로 하고, WAP 프로토콜을 사용하는 무선 단말기 등에 이식이 가능한 무선 보안 솔루션을 개발하였다.

(4) 드림 시큐리티[13]

WAP 스팩을 기반으로 WAP과 ME 프로토콜 양쪽에 모두 보안 서비스를 제공할 수 있는 WTLS 솔루션을 개발하였다.

표 1. 업체별 무선 SSL 솔루션 특징

	소프트포럼	IA Security	이니텍	드림 시큐리티
제품명	MSSL	Internet Appliance	Inisafe Mobile	Trust-M
추가 알고리즘	ECC	ECC	ECC	ECC
플랫폼	PDA,휴대폰	PDA,휴대폰	PDA,휴대폰	PDA,휴대폰
대상 O/S	WinCE, Cellvic, PalmOS	WinCE, Cellvic, PalmOS	WinCE, Cellvic, PalmOS, Embedded Linux	WinCE, Cellvic, PalmOS

3. 무결성 검증 시스템 설계 및 구현

3.1 전체 시스템 구성

본 장에서는 PDA환경의 응용계층 보안모듈 무결성 검증 시스템의 전체 구성과 테스트 방법 및 테스트를 위해 필요한 각 모듈들에 대해 설명한다. 무결성 검증 시스템의 전체구성은 그림 1.과 같다.

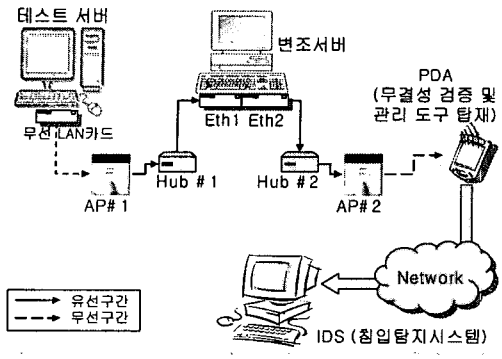

그림 1. 전체 시스템 구성도

PDA환경의 무선환경의 응용계층 보안모듈의 무결성 검증을 위해 테스트 서버와 PDA사이에 AP (Access Point)를 이용하여 내부 네트워크를 구성하고, 종단 시스템은 응용계층 보안모듈을 탑재한 S/W를 통하여 암호화된 데이터를 주고받게 된다. 이때 PDA환경의 응용계층 보안모듈이 데이터 무결성 기능을 제공하는지 검증하기 위하여, 전송되는 데이터를 변조서버를 통해 임의의 값으로 변조시킨 데이터를 PDA로 전송하였을 때 변조된 데이터를 받은 PDA상의 응용계층 보안모듈이 변조 유무를 체크하는지 무결성 검증 시스템을 통해 확인하게 된다. 만약 변조가 되었음을 표시하는 모듈이 동작을 하면 무결성 기능이 제대로 동작한다는 것이고, 그렇지 않고 데이터를 받아들이거나 반응을 보이지 않으면 무결성 기능에 문제가 있을 수 있다는 것으로 판단할 수 있게 된다. 무결성 검증과 관련된 데이터는 로그파일에 기록되어 관리 모듈을 통해 관리되며, Log 데이터를 IDS(침입탐지시스템)로 전송하여 관리할 수 있게 한다.

3.2 데이터 변조 모듈

데이터 변조 모듈은 무선 응용계층의 전송 데이터를 중간에서 가로채어 변조시킨 후 목적지로 전달하는 역할을 수행한다. 데이터 변조 모듈은 패킷 변조 모듈과 사용자 인터페이스 모듈로 구성된다.

(1) 패킷 변조 영역

패킷 변조 모듈은 전송 패킷의 실제 변조를 담당하며, 리눅스 시스템의 패킷 전송원리를 이용하여 구현되었다[14]. Link Layer를 통과한 패킷은 ip_input 버퍼에 저장되어 패킷의 목적지 주소를 확인한 후, 목적지가 해당 호스트이면 전송계층으로, 그렇지 않으면 ip_forward와 ip_output버퍼를 통해 외부로 패킷을 전송한다. 본 논문에서는 ip_forward 버퍼루틴에 패킷 변조 모듈을 구현하여 변조 모듈에서 변조된 데이터는 ip_output버퍼를 거쳐 원래의 목적지로 전송하게 한다.

(2) 사용자 인터페이스 Part

사용자 인터페이스 모듈은 사용자가 선택한 패킷의 정보를 입력하여 패킷을 변조하고, 패킷의 변조 전·후 내용을 출력하는 기능을 수행한다. 변조를 위한 입력항목은 다음과 같다.

표 2. 패킷변조 입력정보 항목

항목	내 용
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 데이터 무결성 검증 및 관리 모듈

데이터 무결성 검증 및 관리 모듈은 PDA상의 보안모듈이 제공하는 무결성을 검증하고, 검증된 데이터를 기록 및 관리하는 기능을 수행한다.

(1) 데이터 무결성 검증 모듈

데이터 무결성 검증 모듈은 PDA상의 응용계층 무선 보안모듈이 제공하는 무결성을 검증하는 기능을 수행한다. 본 시스템에서는 무결성이 위배된 데이터를 수신했을 때 처리하는 루틴을 구현하여 무선 보안모듈을 탑재한 프로그램이 무결성을 제공하는지를 검증할 수 있도록 하였다. 응용계층 보안모듈의 테스트를 위해 SSL 기능을 제공하는 OpenSSL 기반의 보안모듈을 탑재한 프로그램을 구현하였고, 무결성 검증 모듈에서 응용계층 보안제품의 무결성 지원 여부를 확인할 수 있게 한다[15].

그림 2.는 PC와 PDA에 탑재된 프로그램이 SSL을 사용하여 보안연결을 설정하였음을 보여준다. 오른쪽은 PDA상의 프로그램 실행화면이고 왼쪽은 PC에서 구동한 프로그램 실행화면이다. 그림 3.은 데이터의 무결성을 검증한 결과이다. 왼쪽의 그림은 변조서버에서 변조를 하지 않았을 경우 테스트서버에서 보낸 데이터를 PDA환경의 무선보안모듈을 탑재한 프로그램이 정상적으로 동작하는 것을 나타내고[16], 변조된 데이터가 들어왔을 경우는 왼쪽의 그림처럼 무결성 검증 모듈을 통해 에러가 발생했음을 알려준다.

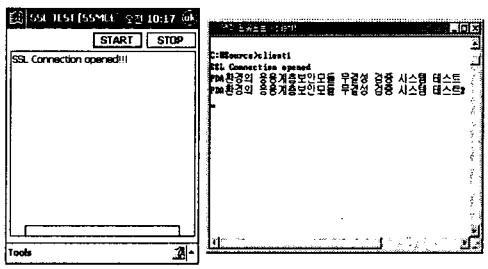

그림 2. 무결성 검증모듈 연결화면

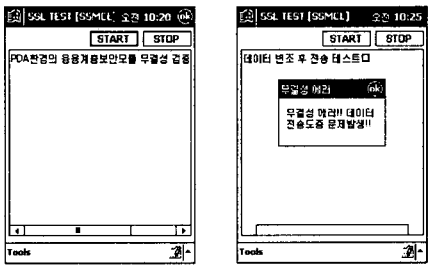

그림 3. 데이터 무결성 검증 결과

(2) 데이터 무결성 관리 Part

무결성 관리 모듈은 무결성 검증 모듈을 통해 검증된 데이터의 무결성 위배 유무를 로그파일에 기록하고 관리하는 기능을 가지며, IDS로 무결성 검증 데이터를 전송하는 작업을 수행한다.

그림 4.의 왼쪽그림은 무결성 관리 모듈을 실행시킨 화면이고, 오른쪽그림은 보안통신을 했을 경우에 대한 무결성 위배유무 기록을 정렬하여 보여주는 화면이다. 그림 5.의 오른쪽 그림은 무결성 검증 시스템의 환경설정화면(로그데이터를 IDS로 보내기 위한 설정, 데이터를 주고받을 곳의 IP Address 설정, 현재 상태 표시)을 나타내며, 왼쪽은 설정한 IDS로 로그 데이터를 전송하는 화면을 나타낸다.

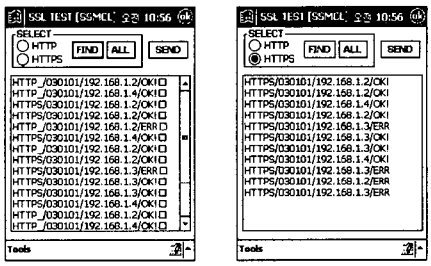

그림 4. 관리모듈의 실행 화면

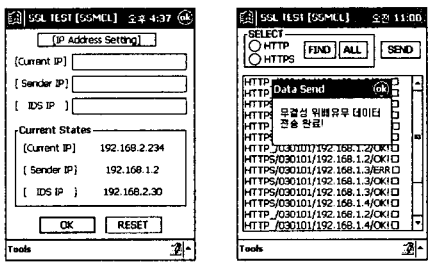

그림 5. 환경설정 및 데이터 전송

4. 결론 및 향후연구

본 논문에서는 PDA환경의 응용계층 보안모듈의 신뢰성 향상과 발전을 위해서 PDA환경의 응용계층 보안 모듈 데이터 무결성 검증 시스템을 설계 및 구현하였다. 본 논문에서 구현한 시스템은 변조서버 시스템과 무결성 검증 및 관리 시스템으로 구성되어 PDA 환경의 응용계층 보안모듈을 탑재한 제품의 무결성 평가에 대한 방법을 도출하고 평가를 실제 수행하였으며, 무결성 검증 유무 정보를 저장하여 PDA를 통해 전송되는 데이터의 무결성 관리가 가능하도록 하였다. 그리고 이러한 무결성 위배 정보들의 효율적인 관리를 위해 침입탐지시스템과 연계한 통합 관리시스템을 제안하고 설계하였다.

향후 연구에서는 응용계층 보안모듈 뿐만 아니라 네트워크계층의 무선 보안모듈에 대한 무결성도 함께 평가할 수 있는 평가 시스템 개발이 필요하며, IDS와 연계한 통합 관리시스템에 대한 구현을 진행할 계획이다.

[참고문헌]

[1] "세계 무선인터넷 동향 및 전망", 지식정보센터, 주간기술동향 통권 963호, 2000. 9. 14.

[2] "무선인터넷 보안기술의 동향과 향후 전망", ETRI IT정보센터, 2000.09.14.

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

[4] "2006년 포스트PC가 PC시장 추월", 전자신문 기사, 2003.02.07.

[5] 한국정보보호센터, "평가인증제품 현황", http://www.kisa.or.kr, 2003. 3.

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

[7] NCSC, "Trusted Network Interpretation of the TCSEC", NCSC-TG-005, 1987.

[8] EC, "Information Security Evaluation Criteria (ITSEC)", Ver1.2, http://www.itsec.gov.uk

[9] "Common Criteria for Information Technology Security Evaluation (CC)", Ver 2.0.

[10] Softforum, http://www.softforum.com

[11] IA Security, http://www.iasecurity.com

[12] Initech, http://www.initech.com

[13] Dream Security, http://www.dreamsecurity.co.kr

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

[15] J. Viega, M. Messier, P. Chandra, "Network Security with OpenSSL", O'REILLY, 2002. 6.

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