이학석사 학위논문

무선 보안시스템 응용계층 무결성 평가 도구 설계 및 구현

지도교수 김 창 수

이 논문을 이학석사 학위논문으로 제출함

2003年 2月

부경대학교 대학원

전자계산학과

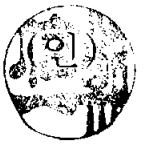
김 기 욱

김기욱의 이학석사 학위논문을 인준함

2002년 12월 26 일

주 심 이학박사 박 홍 복 

위 원 공학박사 박 지 환 

위 원 공학박사 정 신 일 

<차 례>

<그 림 차 례>

<표 차례>

Design and Implementation of Integrity Evaluation Tool for Application Layer of Wireless Security Systems

Ki-Uk Kim

Dept. of Computer Science Graduate School of Pukyong National University

Abstract

In these days, the applications of the wireless internet have been continuously increasing in mobile system such as PDA or HPC. And then wireless security systems which especially provide secure function of transmitting data in mobile environment have been actively studied. But the researches for evaluation tool which is able to verify reliability of security products do not provide to compare with wireless security systems.

In this thesis, we design and implement the evaluation tool which can verify integrity function for only application layer of wireless security products. The proposed integrity evaluation tool is largely composed of two components which are modification server system

and integrity verification system. The former provides function to be able to modify some bits of transmitting data between the mobile devices and web server, the letter has the function for verification whether it can detect or not data integrity for modified bits of transmitting data with wireless SSL(secure socket layer) function between source and destination node. To evaluate that is exactly operated integrity function of wireless SSL module, we apply the integrity evaluation tool made itself with SSL module contained in the WinInet library of Windows CE API. To the resuls of various control methods by itself evaluation tool, it is correctly to detect integrity violation of modified bits.

1. 서 론

1.1 연구 배경 및 필요성

최근 PDA 및 휴대폰 등을 이용한 무선 인터넷 서비스가 활성화되고 있다. 그러나 전자 상거래 등의 급속한 유·무선 인터넷 사용의 활성화는 정보유출, 파괴(crack), 위·변조(fabrication & modification), 바이러스(virus), 서비스 방해(denial of service), 불건전 정보 유통, 해킹(hacking)등 정보화 역기능을 가져왔으며, 이러한 정보화 역기능으로부터 데이터를 보호하기 위해 국내·외로 유·무선 인터넷의 데이터를 보호하기 위한 정보보호 제품의 개발과 연구가 활발히 진행 중이다[1]. 하지만 성능과 신뢰도가 증명되지 않은 제품의 사용은 보안 취약성이 존재할 수 있기 때문에 정보보호 제품 평가가 필요하다. 특히 보안 표준이 미약한 무선 보안제품의 평가는 더욱 중요하다. 정보보호 제품의 평가를 위해 국외에서는 10여 년 전부터 자국의 환경에 적합한 평가기준을 마련하여 평가·인증 제도를 시행하고 있으며, 국내에서도 1998년 2월부터 침입탐지시스템(IDS), 침입차단시스템(Firewall)에 대한 평가기준을 마련하고 이를 근거로 정보보호 제품을 평가 해오고 있다. 하지만 실제 정보보호 제품 평가에 적용할 평가방법 및 평가 자동화 도구가 없으며, 보안 요구사항들의 적합성을 검증하는 보안 모듈에 대한 평가 기준 및 연구는 아직 미약해 이들에 대한 연구가 필요하다[2].

따라서 본 논문에서는 국내·외의 보안성 평가 기준 및 방법들과 유선

VPN제품의 무결성 평가방법을 토대로 무선 보안시스템 응용계층 무결성 평가도구를 설계 및 구현하였다.

1.2 논문의 구성

본 논문은 서론, 관련연구, SSL 프로토콜 분석, 무선 보안시스템 응용계층 무결성 평가도구 설계 및 구현, 결과 분석, 그리고 결론으로 구성하였다.

제2장에서는 국내·외 정보보호 제품의 평가기준을 분석하였다. 그리고 기존의 무결성 평가에 관한 연구를 살펴보았다.

제 3장에서는 응용계층 무선 보안제품에 가장 활발히 활용되는 SSL 프로토콜을 분석하였다.

제 4장에서는 본 논문에서 제안한 평가 도구의 설계 및 구현에 대해 기술하였다.

제 5장에서는 본 논문에서 구현한 평가도구의 구현결과에 대한 결과를 분석하였다.

마지막으로 제 6장에서는 결론을 제시하였다.

2. 관련 연구

본 장에서는 국내·외 정보보호 제품 평가 방법 및 보안 모듈 평가에 대해 분석하고 무결성 평가에 관한 기존 연구를 분석하였다.

2.1 국내·외 정보보호 시스템 평가 체계 분석

2.1.1 정보보호 시스템 평가 기술 분석

정보보호 시스템 평가란 보안기능의 성능과 신뢰도가 증명되지 않는 제품의 사용으로 인한 피해를 막기 위해 평가 기준 및 지침서를 근거로 적합성을 검증하는 것을 말한다[3]. 정보보호 시스템 평가 기술은 알고리즘 평가, 암호 모듈 평가, 정보보호 제품 평가, 응용 시스템 평가로 구분된다.

(1) 암호 알고리즘 평가

암호 알고리즘 평가는 정보보호 제품을 평가하기 위해 가장 기본적이며 우선시 해야 하는 평가이다. 정보보호 제품에 탑재된 암호 알고리즘에 대한 안전성을 평가하는 것으로 알고리즘 자체만을 평가하므로 탑재된 제품이나 시스템과 독립적으로 평가가 가능하며, 일반적으로 알고리

즘 자체의 이론적 안전성만을 평가한다. 국내의 경우 현재 비밀성 기능을 제공하는 블록암호 알고리즘에 대한 안전성 평가를 수행중이다. 하지만 이론적 안전성 평가만을 수행하고 있어 구현물에 대한 안전성 평가가 요구된다.

(2) 암호 모듈 평가

암호 모듈 평가는 정보보호 제품들이 제공하는 보안 요구 사항들에 대한 평가로써 기밀성 모듈, 무결성 모듈 등에 대한 안전성을 평가한다. 이론적으로 검증된 암호 알고리즘을 사용하더라도 구현상의 취약점이나 기타 환경 등의 문제로 인한 취약점이 존재할 수 있기 때문에 암호 모듈에 대한 평가는 중요하다. 하지만 현재 암호 모듈에 대한 평가는 미약하며, 대표적인 암호 모듈 평가는 FIPS 140-2를 평가기준으로 수행되는 CMVP(Cryptographic Module Validation Program)가 있다[4].

따라서 국내·외로 안전한 정보보호 제품 사용의 기반을 마련하기 위해 암호모듈 평가 방법에 관한 연구가 필요하다.

(3) 정보보호 제품 평가

정보보호 제품 평가는 암호 모듈을 탑재한 정보보호 제품들에 대한 안전성을 평가하는 것으로 제품별로 다른 평가기준이 적용되며, 제품을 구성하는 각 모듈의 안전성 외의 기능 및 성능에 대한 안전성을 평가한다.

정보보호 제품의 평가 기준은 나라별로 다른 평가기준이 존재하며, 1996년에 국제공통표준(CC)이 완성되었고, 국내의 경우는 현재 IDS, Firewall에 대한 평가기준이 제정되어 있다.

(4) 응용 시스템 평가

각 제품을 상호연동 하여 구성되는 시스템에 대한 안전성 평가로써 각 시스템마다 독립적이며, 평가받은 제품을 사용하더라도 시스템 자체의 안전성이 취약할 수 있다. 따라서 이들에 대한 평가가 가장 어려우며, 같은 시스템이라 하더라도 사용환경이나 구성환경에 따라 평가기준이나 방법이 다르다.

이처럼 정보보호 시스템의 평가는 정보보호 시스템을 구성하는 암호 알고리즘 평가와 암호 알고리즘들로 구성되는 암호 모듈 평가, 그리고 암호 모듈로 이루어지는 정보보호 제품 평가 등으로 구성된다. 그리고 보다 정확한 정보보호 제품의 평가를 위해서는 이들이 순차적으로 평가되어야 한다[5].

따라서 본 논문에서는 무선 보안시스템의 무결성을 평가하기 위해 해쉬 알고리즘 적합성 검증과 데이터 무결성을 평가할 수 있는 평가 도구를 설계 및 구현하였다.

2.1.2 국내 · 외 정보보호 시스템 평가 제도 분석

(1) 미국의 평가 제도 및 평가 방법

미국은 NSA(National Security Agency), NIAP(National Information Assurance Partnership)주관으로 1985년 TCSEC(Trusted Computer System Evaluation Criteria), 1987년 TNI(Trusted Network Interpretation of TCSEC), 1991년 TDI(Trusted Database Interpretation of TCSEC)등 정보보호 시스템 평가 기준을 제정하고 TPEP(Trusted Product Evaluation Program)평가 프로그램에 의하여 정보보호 시스템을 운영 체제, 네트워크 컴포넌트 등으로 분류하여 평가를 시행해 왔으며, 1997년 이후로 NIST와 NSA가 공동으로 계획한 민간 평가 프로그램인 TTAP(Trusted Technology Assessment Program) 절차에 의해 평가를 시행하고 있다. 미국의 평가기준인 TCSEC는 가장 오래된 정보보호 시스템 평가 기준으로 최초에는 운영체제 보안 제품의 평가가 주목적이었지만 점차로 그 범위를 확대하여 데이터 베이스, 네트워크, O/S등 다양한 분야의 보안 제품 평가 기준을 확립하였다. TCSEC의 평가기준의 요구사항은 보안정책, 책임추적, 보증의 통제목적을 만족시키기 위해 필요한 특성, 각 등급에서 요구하는 사용자 지침, 설명서, 시험 및 설계문서에 대한 문서형식이 증거를 요구하는 사항들로 구성된다. TCSEC의 평가 등급은 C1, C2, B1, B2, B3와 가장 높은 등급인 A1, 부적격 등급인 D급으로 이루어져 있으며, B등급에서는 가장 중요한 요구사항으로 보안 레이블의 무결성을 보장하도록 규정하고 있다[6].

(2) 유럽의 평가 제도 및 평가 방법

영국, 독일, 프랑스 및 네덜란드 등은 각각 자국의 평가기준을 제정하여 평가를 수행하였지만, 평가 제품의 상호 인정 및 평가기준이 상이함에 따른 정보보호 제품의 평가에 소요되는 시간, 인력 및 소요 비용을 절감하기 위해 4개국의 공통 평가 기준인 ITSEC(Information Technology Security Evaluation Criteria)를 제정하였다. 그리고 CESG, CCSC의 두 기관이 공동으로 참여하여 ITSEC를 기준으로 정보보호 제품 평가를 시행하고 있다. ITSEC는 E2, E3, E4, E5 및 최저등급인 E1, 최고등급인 E6로 구성되며, 부적합 판정등급은 E0로 정의한다. ITSEC는 보안 기능 요구사항과 보증 요구사항으로 이루어져 있으며, 보안 기능에는 무결성, 가용성, 전송 데이터 무결성, 비밀성, 전송 데이터 비밀성 등의 기능을 정의하였으며, 보증 부분은 효용성 및 정확성을 평가할 수 있도록 정의하였다. ITSEC는 TCSEC와는 달리 단일 기준으로 모든 정보보호 제품을 평가하며 평가를 수행하기 위한 지침으로 ITSEM(Information Technology Security Evaluation Manual)이 개발되어 있다[7][8].

(3) 한국의 평가 제도 및 평가 방법

국내 평가 제도는 1996년 8월 재정된 정보화 촉진 기본법 제15조 및 동법 시행령 제15, 16조를 근거로 1998년 2월 정보통신망 침입차단시스템 평가 기준 및 평가 지침서를 제정·고시하여 한국정보보호센터(KISA)에서 침입차단시스템에 대한 평가를 시행해 오고 있다. 국내에서

보안 제품에 대한 평가는 KISA에서 수행하며, 수행된 평가결과는 국가정보원에서 인증한다[9]. 국내의 평가 등급은 K1~K7등급으로 구성되며 보안기능 요구사항과 보증 요구사항으로 구성된다. 현재 국내에서는 침입탐지시스템(IDS)과 침입차단시스템(Firewall)에 대한 기준만을 제정하여 이들 제품에 대한 평가를 수행하고 있다. 침입차단시스템의 보안기능 요구사항은 신분확인, 접근통제, 무결성, 비밀성, 감사기록 및 추적, 보안관리의 6가지 요구사항으로 이루어진다. 그리고 침입탐지시스템의 보안기능 요구사항은 축약감사데이터 생성, 보안위반 분석, 보안감사 대응, 신분확인, 데이터 보호, 보안감사, 보안관리, 보안기능 보호의 8가지로 구성된다. 현재 침입탐지시스템, 침입차단시스템 각각에 대해 10여 개의 업체가 평가 인증을 받았다[10][11]. 하지만 아직 무선 보안제품에 대한 평가연구는 미약하다.

따라서 기밀성, 무결성 등이 보장된 무선 인터넷 사용을 위해서는 무선 인터넷 보안 시스템 평가에 관한 연구가 시급하다.

(4) 국제공통평가기준(CC)분석 및 평가 방법

세계 각국의 평가 기준이 상이하여 평가에 소요되는 비용과 시간이 많이 소요되며 TCSEC, ITSEC, CTCPEC, FC등의 평가 기준 통합의 필요성이 대두되면서 미국(NIST, NSA), 캐나다(CSE), 프랑스(SCSSI), 독일(BSI), 네덜란드(NS-NCSA) 및 영국(CESG) 등 6개국의 참여로 국제공통평가기준(CC)이 제정되었다. CC는 크게 5가지 부분으로 구성되어 있다. Part1에서는 소개 및 일반모델을 제시하고 있으며, Part2는 보안기능

요구사항, Part3는 보증 요구사항, Part4는 이미 정의된 보호 프로파일을 기술하고 있으며 Part5에서 보호 프로파일을 등록하는 절차를 포함하고 있다. CC의 핵심은 Part2와 Part3로써 정보보호 제품이 구비해야 하는 기능 및 보증 요구사항을 기술하고 있으며 기술된 요구사항을 참조하여 정보보호 제품을 개발할 수 있다. CC의 평가등급은 EAL1~EAL7까지 있으며, EAL1부터 EAL4등급까지는 사용된 특별한 암호 기술을 소개하지 않고 일반적으로 기존에 있었던 제품과 시스템을 재정비하기 위한 관점에서 적용될 수 있으며, EAL4 이상의 등급은 응용기술로 사용된 보안 기술까지 평가대상 범위를 넓히고 있다. 국내의 경우 2002년 8월부터 CC기반의 평가를 시작하였으며 IDS, Firewall, VPN에 대해 우선적으로 평가를 위한 보호프로파일 개발이 이루어지고 있다[12][13][14].

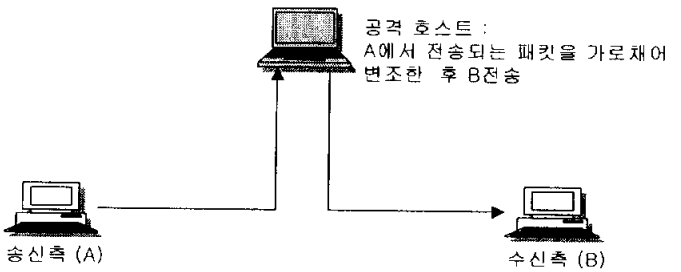
2.2 기존 정보보호 시스템 무결성 평가 연구 분석

2.2.1 무결성

데이터 무결성이란 송·수신되는 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 하는 기능을 말한다. 만약 데이터 무결성이 보장되지 않는다면 정보교환 시 메시지 도청 및 수정, 삽입, 송신자의 위장 문제 등이 발생할 수 있으며, 이는 이동 네트워크를 통한 개인 정보 유출이 야기하는 여러 문제를 발생시킬 수 있다. 따라서 데이터의 변조 공격으로부터 안전성을 제공하는 무결성 기능은 중요하다[15].

2.2.2 기존의 무결성 평가 방법

현재까지 연구된 무결성 평가방법은 KISA(정보보호 진흥원)의 평가팀에서 제시한 '유선 VPN 제품의 무결성 평가방법'이 있으며, KISA에서는 유선 VPN제품 무결성 평가 방법을 제시하였다. 본 논문에서는 유선 VPN제품의 무결성 평가 방법을 이용하여 무선 보안시스템 응용계층 무결성 평가 도구를 구현하였다. [그림 1]은 KISA에서 제시한 평가 환경이다.



[그림 1] 유선 VPN의 무결성 평가 방법

KISA에서 제시한 무결성 평가 방법은 다음과 같다. 즉, [그림 1]에서처럼 A에서 B로 전송되는 패킷을 중간의 공격 호스트에서 가로챈 후 패킷을 변조하여 B로 전송한다. 그리고 수신측이 변조된 데이터를 인식하느냐에 따라 무결성 평가를 수행한다. 유선 VPN제품의 무결성 평가방법을 정리하면 다음과 같다[16].

① 송신측(A)에서 수신측(B)로 암호화되어 전송되는 패킷을 공격 호스트에서 변조하여 수신측(B)으로 전송

② 송신측(A)에서 수신측(B)로 암호화되어 전송되는 패킷을 공격 호스트의 변조 없이 수신측(B)으로 전송

3. 응용계층을 위한 무선 보안 프로토콜 분석

본 장에서는 무선 보안 프로토콜 중 응용계층의 보안 프로토콜로 가장 활발히 사용되는 SSL프로토콜에 대해 설명하였다.

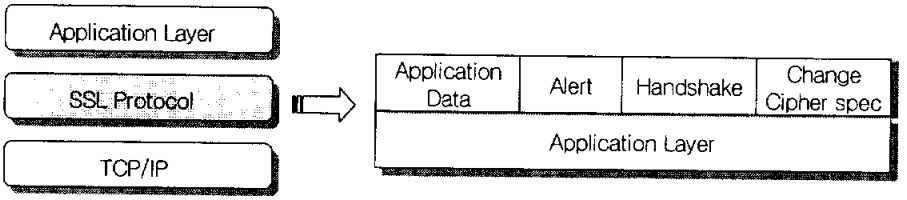
3.1 SSL(Secure Socket Layer)사용의 필요성

무선 인터넷을 이용한 전자상거래 등의 서비스가 활성화됨에 따라 무선 인터넷 전송 데이터 보호에 관한 연구 및 솔루션 개발이 계층별로 활발히 진행중이다. 즉, 링크계층에서는 WLAN(Wireless LAN)의 보안 프로토콜인 WEP(Wired Equivalent Privacy)을 적용한 보안표준 및 연구가 진행중이며, 네트워크 계층에서는 유선 VPN의 개념을 도입한 MVPN(Mobiel VPN)솔루션 개발이 국내·외로 활발히 진행되고 있다. 무선 보안 기술로 가장 활발히 연구가 진행 중인 계층은 전송계층과 응용계층으로 WAP Forum과 Microsoft 및 일본의 NTT DoCoMo를 중심으로 표준 및 보안 프로토콜에 관한 연구가 활발히 진행되었다. 그리고 각각이 제시한 보안 프로토콜은 WTLS(Wireless Transport Layer Security), SSL(Security Socket Layer) 및 TLS(Transport Layer Security)등이 있다. 하지만 WAP(Wireless Application Protocol)의 보안 표준인 WTLS는 End-to-End 보안의 문제로 인해 논란이 많았다. 이에 WAP 2.0 스팩에서는 보안 프로토콜로써 유선 응용계층의 보안 프로토콜인 SSL 및 TLS를 채택하였고, 대부분의 무선 인터넷 보안 솔루션 및 연구는 SSL을 기반으로 하고 있다[17][18]. 따라서 본 논문에서는 무선

SSL 모듈을 대상으로 무결성 평가 도구를 구현하였다.

3.2 SSL 프로토콜의 구조

SSL(Secure Socket Layer)은 Netscape Communications사에서 웹 보안을 위해 개발한 보안 프로토콜로 현재 유선 환경뿐만 아니라 이동 네트워크를 이용한 무선 인터넷에서도 활발히 사용되고 있다. SSL 프로토콜은 응용계층과 TCP/IP계층 사이에 존재하며 무결성, 기밀성, 사용자 인증 등의 보안 서비스를 제공한다. SSL 프로토콜의 구조는 [그림 2]와 같다[19].



[그림 2] SSL 프로토콜 구조

Handshake Layer는 암호화된 통신을 하기 위한 비밀키, 암호화 알고리즘, 비밀 파라메터 등의 정보를 통신 종단간에 교환하며, Record Layer에서는 교환된 정보를 바탕으로 데이터를 암호화하여 전송한다. 또한 Record Alert 프로토콜은 에러 제어 기능을 제공하며, Change Cipher Spec 프로토콜은 암호 알고리즘 및 해쉬 알고리즘 등의 정보를 제공한다[20].

3.3 무선 SSL 프로토콜의 특징

유·무선 SSL 프로토콜의 기능 및 내용은 유사하지만 무선 인터넷 환경의 제약으로 구현 방법 및 유·무선에 사용된 암호 알고리즘, 구현 용량 등에 차이가 있다[21]. 현재 무선 SSL에 대한 정확한 표준이 없고, 상용화된 대부분의 무선 SSL 제품들은 업체 자체의 기준에 따라 구현되고 있다. [표 1]은 업체별 SSL 솔루션들의 특징이다.

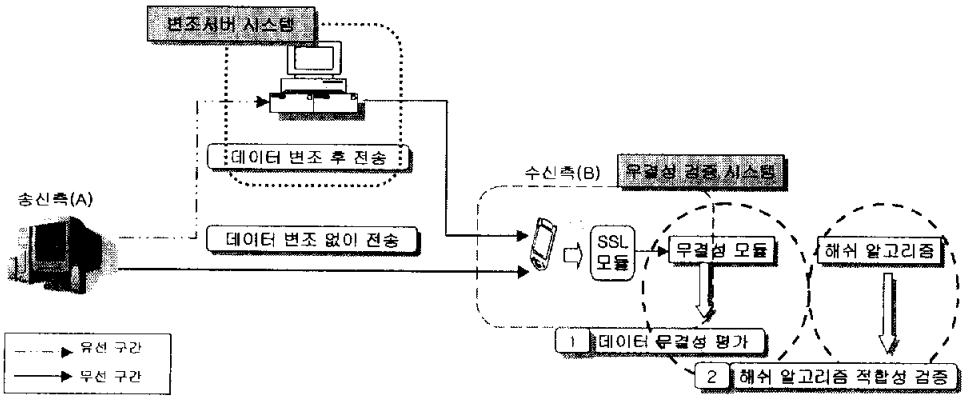
[표 1] 무선 SSL 솔루션

	이니텍	드림 시큐리티	IA Security	소프트포럼
제품명	Inisafe Mobile	Trust-M	Internet-Appliance	MSSL
유선 SSL에서 추가된 알고리즘	ECC	ECC	ECC	ECC
적용 플랫폼	PDA 휴대폰	PDA 휴대폰	PDA 휴대폰	PDA 휴대폰
대상 o/s	Windows CE Cellvic Palm OS Embedded Linux	Windows CE Cellvic Palm OS	Windows CE Cellvic Palm OS	Windows CE Cellvic Palm OS

4. 무선 보안시스템 응용계층 무결성 평가 도구 설계 및 구현

4.1 제안한 평가도구의 평가 방법

본 논문에서는 무선 보안시스템 응용계층 무결성 평가 방법을 제안하였다. 제안한 평가 방법은 무결성 모듈에 대한 평가와 알고리즘 적합성 검증으로 구성된다. 무결성 모듈 평가는 구현한 평가 도구의 2.2절에서 설명한 '유선 VPN제품의 무결성 평가 방법'을 근거로 제안하였고, 알고리즘 적합성 검증은 'NIST의 해쉬 알고리즘 권고안'을 근거로 적합한 해쉬 알고리즘 기준을 마련하였다. [그림 3]은 제안한 평가도구의 평가 방법이다. '데이터 무결성 평가'에서 SSL모듈의 무결성 기능을 평가하고 '해쉬 알고리즘 적합성 검증'에서 SSL제품에 사용된 해쉬 알고리즘의 적합성을 검증한다.



[그림 3] 응용계층의 무선 보안시스템 무결성 평가 방법

(1) 데이터 무결성 평가

'데이터 무결성'이란 송·수신되는 데이터가 전송 중 불법적으로 변경 또는 삭제되거나 생성되지 않도록 하는 보안 기능이다. 따라서 데이터 무결성 평가를 위해서는 무선 보안 시스템이 수신된 데이터의 변조를 인식하는지 평가해야 한다. 다음은 제안한 데이터 무결성 모듈 평가 방법이다.

① 송신측(Web Server)에서 수신측(Mobile Host)으로 전송되는 데이를 중간의 변조 서버에서 변조 후 전송
: 데이터 변조를 무선 보안 시스템 무결성 모듈이 인식하는지 평가

② 송신측(Web Server)에서 수신측(Mobile Host)로 변조없이 데이터 전송
: 변조되지 않은 데이터의 수신을 무선 보안 시스템 무결성 모듈이 인식하는지 평가

(2) 해쉬 알고리즘 적합성 검증

보안 모듈 평가를 위해서는 보안 기능을 제공하는 암호 알고리즘의 적합성을 우선 검증해야 한다. 무결성 기능을 제공하는 암호 알고리즘은 해쉬 알고리즘이다. 따라서 본 논문에서는 무선 보안시스템의 무결성 평가를 위해 보안 시스템에 사용된 해쉬 알고리즘의 적합성을 검증한다. 알고리즘의 검증 기준은 NIST에서 안전성을 평가하여 권고한 해쉬 알고

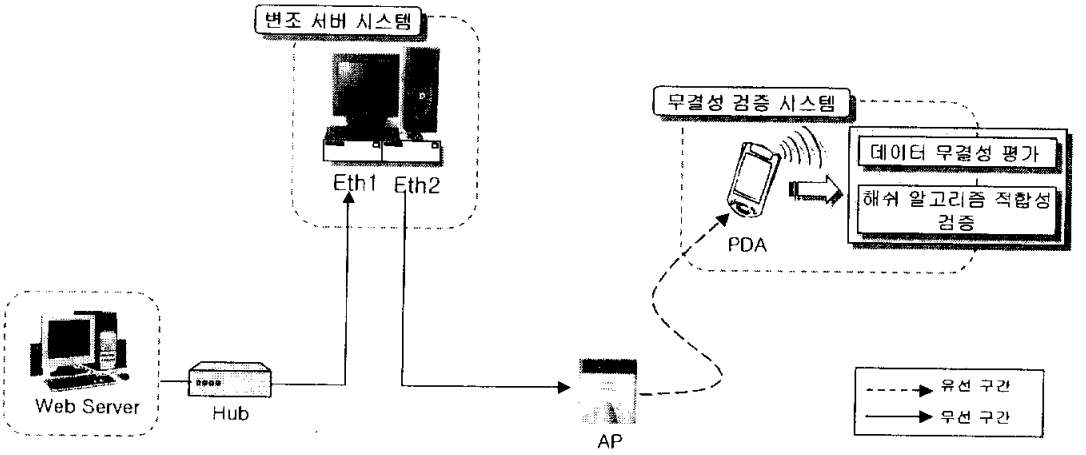
리즘을 근거로 하였다[22]. NIST에서 권고하는 표준 해쉬 알고리즘은 [표 2]와 같다.

[표 2] NIST 권고안의 표준 해쉬 알고리즘

표준문서	FIPS-1	FIPS-2		
알고리즘	SHA-1	SHA-256	SHA-384	SHA-512

4.2 평가 도구의 전체 구성

본 논문에서는 4.1절에서 제안한 평가 방법으로 응용계층 무선 보안시스템의 무결성을 평가 할 수 있는 평가도구를 구현하였다. 구현한 평가도구는 변조 서버 시스템과 무결성 검증 시스템으로 구성된다. 변조 서버 시스템은 무선 보안시스템 응용계층 무결성 모듈이 전송 데이터의 변조를 검증하는지 평가하기 위해 전송되는 데이터를 변조한다. 그리고 무결성 검증 시스템은 WinInet 라이브러리가 제공하는 SSL기능을 대상으로 무결성 평가를 수행하기 위해 전용 SSL 브라우저를 구현하고, 구현한 브라우저에 데이터 무결성 평가 모듈과 해쉬 알고리즘 적합성 검증 모듈을 구현하였다. [그림 4]는 구현한 평가 도구의 전체 구성도이다. Web Server와 PDA의 Gateway를 변조서버의 주소로 설정하여 Web Server에서 PDA로 전송되는 데이터는 무선 변조서버를 통과하게 구성하였다. 그리고 Forwarding 옵션을 설정하여 변조서버는 Web Server에서 전송된 데이터를 변조한 후 PDA로 전송할 수 있게 하였다.

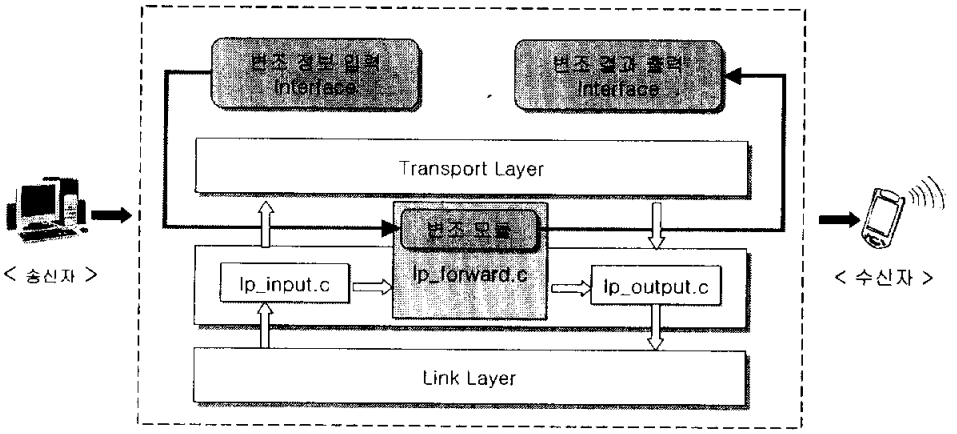


[그림 4] 평가 도구 전체 구성도

4.3 변조 서버 시스템 설계 및 구현

4.3.1 변조 서버 시스템 설계

변조 서버 시스템은 무선 인터넷을 통하여 전송되는 데이터를 동적인 변조 정보에 따라 변조하고, 변조된 데이터를 확인하기 위해 변조 전·후의 데이터 내용을 출력한다. 변조 서버 시스템은 데이터 변조를 수행하는 '변조 모듈'과 동적인 변조 정보 생성을 위한 '변조 정보 입력 인터페이스', 그리고 변조된 데이터 정보를 출력하는 '변조 정보 출력 인터페이스'로 구성된다. 변조 서버 시스템의 전체 구성도는 [그림 5]와 같다.



[그림 5] 변조 서버 시스템 전체 구성도

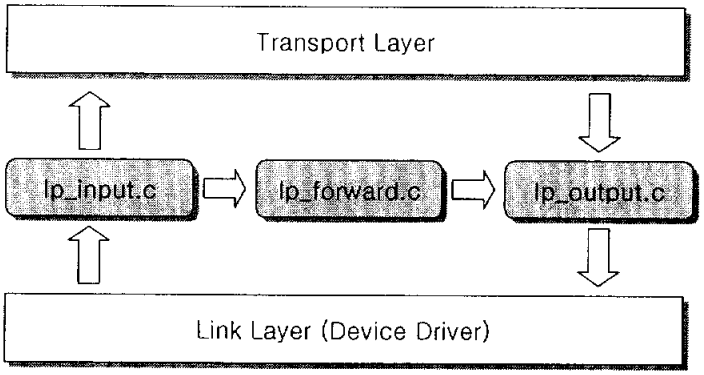
(1) 변조 모듈

변조 모듈은 데이터 무결성 평가를 위해 전송되는 데이터를 전송도중 가로채어 변조한다. 변조 모듈은 소스가 공개된 Linux 커널의 패킷 전송 원리를 이용하여 구현하였다. 변조 모듈에서 사용한 Linux 커널의 패킷 전송 원리 및 TCP Checksum 계산 원리는 다음과 같다.

▶ Linux 커널의 패킷 Forwarding 원리

Linux 커널의 패킷 Forwarding 원리는 [그림 6]과 같다. 리눅스 네트워크 인터페이스로 전송된 패킷은 sk_buff라는 버퍼의 형태로 저장된다. sk_buff 버퍼 형태로 저장된 패킷은 상위 계층인 네트워크 계층을 통과한 후 전송계층으로 전달된다. 이때 리눅스 커널에서는 전송의 효율을

위해 네트워크 계층의 패킷 전송을 [그림 6]에서처럼 ip_input.c, ip_forward.c, ip_output.c 루틴에서 처리한다. 만약 sk_buff에 저장된 패킷의 목적지가 자신의 주소와 동일하다면 sk_buff는 ip_input.c 루틴을 통해 전송계층으로 전송되지만, 만약 다르다면 패킷은 전송계층으로 전달되지 못한다. 여기서 리눅스 시스템이 Forwarding 옵션을 허용한다면 목적지 주소와 자신의 주소가 다른 패킷을 ip_forward.c 루틴을 통해 다른 네트워크 인터페이스로 전송한다[23][24]. 본 논문에서는 IP계층의 패킷 처리 루틴 중 패킷 변조를 위한 변조 모듈을 ip_forward.c 루틴에 구현하였다.

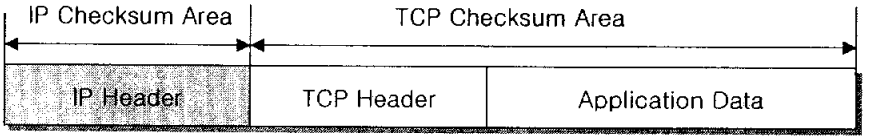


[그림 6] Linux 커널의 패킷 Forwarding 원리

▶ TCP 헤더 Checksum

TCP 계층에서는 전송 데이터의 오류를 검출하기 위해 TCP Checksum값을 TCP헤더에 포함한다. 그리고 [그림 7]에서처럼 TCP Checksum은 TCP 헤더와 Application Data를 포함시켜 계산한다. 따라

서 구현된 데이터가 응용계층 보안 시스템 TCP 프로토콜의 TCP Checksum을 통과하기 위해서는 TCP Checksum 재 계산이 필요하며, 논문에서 구현한 변조 서버 시스템은 변조된 데이터의 TCP 헤더 Checksum 재 계산을 수행하였다. TCP 헤더 Checksum계산 원리는 다음과 같다. 즉, TCP 헤더 Checksum은 16 비트 워드를 사용하여 계산하며 이를 위해 pseudo header를 추가하여 계산한다. 그리고 만약 데이터의 길이가 홀수 일 경우 checksum의 계산을 위해 1byte의 패드 byte를 추가한다.



[그림 7] TCP 헤더 Checksum

(2) 변조 정보 입력 인터페이스

변조 서버 시스템의 변조 정보 입력 인터페이스는 동적인 변조 정보 생성을 위해 변조를 원하는 패킷의 위치, 변조 개수, 변조 간격 등의 정보를 사용자로부터 입력받은 후 변조 모듈로 전송한다.

(3) 변조 결과 출력 인터페이스

변조 서버 시스템의 변조 결과 출력 인터페이스는 변조하기 전의 패킷

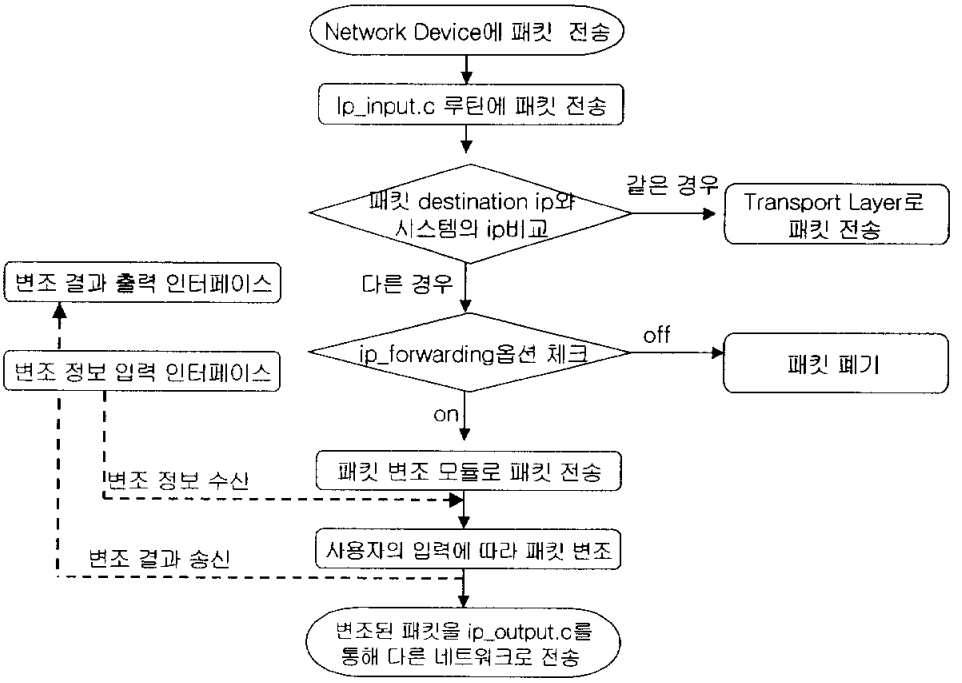
내용과 변조 후의 패킷 내용을 비교·출력한다. 그리고 사용자는 변조 결과 출력 인터페이스를 통해 데이터의 변조 여부를 확인한다.

4.3.2 변조 서버 시스템 구현

본 논문에서 설계하고 구현한 변조 서버 시스템은 커널 수정을 위해 소스를 공개하고 있는 리눅스 시스템을 기본환경으로 하였으며, 세부적인 시스템 구현 환경은 다음과 같다.

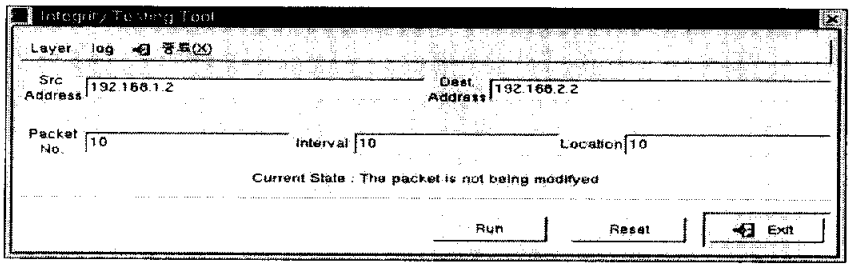
- Target OS : RedHat Linux
- 컴파일러 : gcc
- 사용 라이브러리 : GTK (리눅스 그래픽 툴킷 라이브러리)

변조 서버 시스템의 동작 원리는 [그림 8]과 같다. 변조 서버 시스템은 이동 단말로 전송되는 데이터를 전송 중 가로챈 후 ip_input.c 루틴으로 전송한다. 만약 가로챈 데이터의 목적지 주소가 변조 서버 시스템의 주소라면 Transport Layer를 통해 응용계층으로 패킷을 전송한다. 하지만 목적지 주소가 변조 서버 시스템의 주소가 아니라면 패킷 변조 모듈로 패킷을 전송한다. 그리고 이때 목적지 주소가 자신이 아닌 패킷이라도 수신할 수 있는 'forwarding'옵션이 꺼져 있다면 패킷을 폐기한다. 패킷 변조 모듈로 전송된 패킷은 변조 정보 입력 인터페이스에 입력된 정보에 따라 패킷을 변조하여 ip_output.c 루틴을 통해 원래의 수신자에게 전송된다. 그리고 변조전의 패킷 내용과 변조 후의 패킷 내용을 변조 정보 출력 인터페이스에 출력한다.



[그림 8] 변조 서버 시스템 동작 원리

[그림 9]는 변조 정보 입력 인터페이스이다. 그림에서처럼 변조 정보 입력 인터페이스를 통해 전송할 데이터의 소스 주소, 목적지 주소, 변조할 패킷의 초기 위치, 변조 간격 등의 정보를 사용자가 입력한다. 그리고 입력된 변조 정보는 변조 모듈로 전송되어 변조 정보에 따라 패킷을 변조한다.



[그림 9] 변조 정보 입력 인터페이스

- Src Address

  : 변조할 패킷의 송신지 주소

- Dest Address

  : 변조할 패킷의 수신지 주소

- Packet No

  : 변조할 패킷의 순서 번호, 프로그램 실행 시점에서는 패킷 번호는 1부터 시작한다.

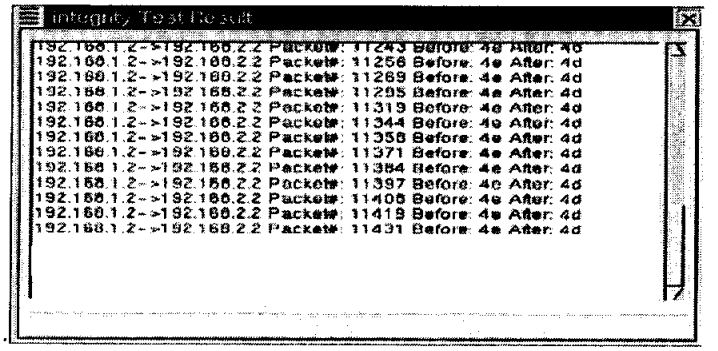
- Interval

  : 변조할 패킷의 간격, 즉 Location을 시작점으로 하여 Interval 위치에 있는 패킷을 변조한다.

- Location

  : 패킷의 변조 시작점, 즉 Location을 시작점으로 패킷을 변조하며, 이는 목적지로의 데이터 전송을 위해 IP헤더 이후부터 변조한다.

[그림 10]은 변조 결과 출력 인터페이스 화면이다. 변조 결과 출력 인터페이스는 패킷 변조 시 변조된 패킷 정보를 동적으로 출력하며, 패킷의 송·수신지 IP와 패킷이 변경되기 전·후의 값을 출력한다

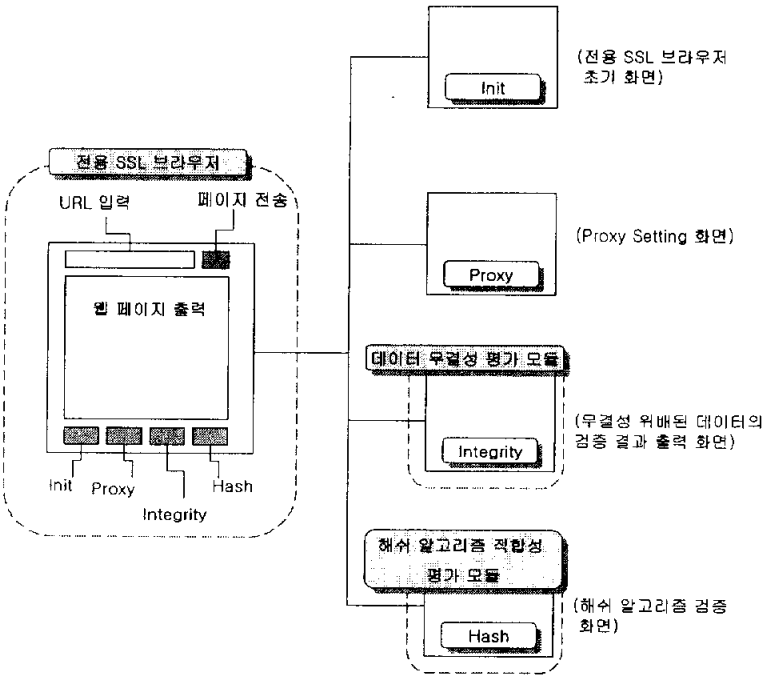


[그림 10] 변조 결과 출력 인터페이스

4.4 무결성 검증 시스템 설계 및 구현

4.4.1 무결성 검증 시스템 설계

본 논문에서는 Windows CE API의 WinInet 라이브러리가 제공하는 SSL기능을 대상으로 무결성 평가를 수행하였다[25]. 이를 위해 [그림 11]에서처럼 웹 브라우저 형태로 SSL 시스템을 구현하고, 구현된 SSL 시스템의 무결성을 평가하였다.



[그림 11] 무결성 검증 시스템 전체 구성도

(1) 전용 SSL 브라우저

전용 SSL 브라우저는 WinInet 라이브러리의 SSL모듈 평가를 위해 Windows CE API를 이용하여 웹 브라우저를 구현하고, 구현한 브라우저에 WinInet 라이브러리의 SSL 모듈을 삽입하였다.

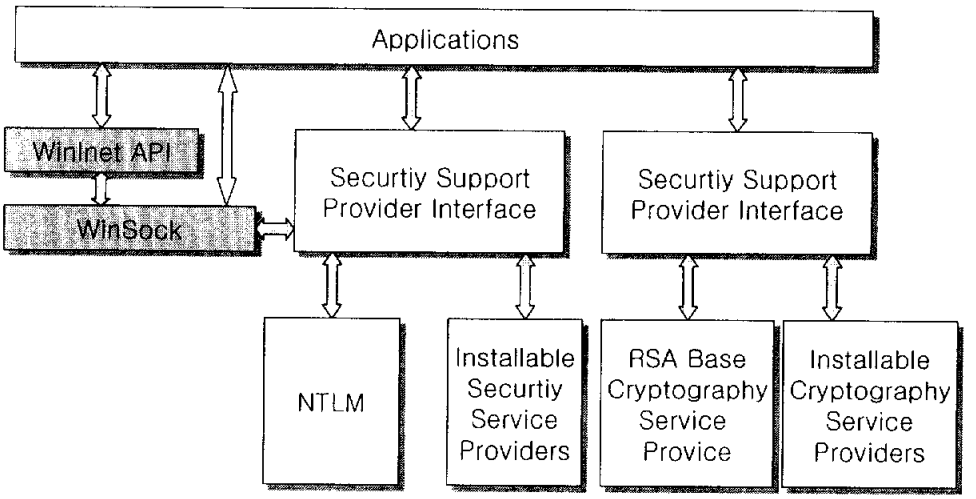
▶ Windows CE가 지원하는 WinInet 라이브러리

Windows CE는 이동 컴퓨팅 환경에서 사용하는 32비트 운영체제로써 현재 version 2002까지 나와 있으며, 국내에서 출시되고 있는 많은 PDA

와 H/PC에서 Windows CE를 운영체제로 사용하고 있다. Windows CE는 인터넷 서비스 제공을 위해 WinInet 라이브러리를 지원하며, 본 논문의 전용 SSL 브라우저는 WinInet 라이브러리를 사용하였다. WinInet 라이브러리는 인터넷 클라이언트 어플리케이션을 개발하기 위해 사용하는 라이브러리로 ISO/OSI 참조 모델에서 WinInet은 세션 계층에서 동작하며 윈속, TCP/IP 그리고 인터넷 프로토콜을 사용한다.

▶ Windows CE의 보안 프로토콜 액세스

Windows CE는 PCT(Private Communications Technology) 1.0과 SSL(Secure Socket Layer) 버전 2.0, 3.0, SGC(Server Gated Cryto) 보안 프로토콜을 지원한다. Windows CE에서 보안 프로토콜을 액세스 하는 방법은 [그림 12]와 같다. 즉, WinInet 라이브러리를 이용하는 방법과 Winsock을 이용하는 방법, Microsoft사가 제공하는 Security Support Provider Interface를 이용하는 방법과 CryptoAPI를 이용하는 방법이 있다. 이들 중 본 논문에서는 WinInet 라이브러리를 이용하여 SSL기능을 제공하는 전용 SSL 브라우저를 구현하였다[26].



[그림 12] Windows CE의 보안 프로토콜 액세스

(2) 데이터 무결성 평가 모듈

데이터 무결성 평가 모듈은 전용 SSL 브라우저의 WinInet SSL 모듈에 대한 무결성 평가를 수행한다. 전용 SSL 브라우저의 SSL 모듈에 무결성 검증을 처리하는 루틴을 구현하였으며, 무결성이 위배된 데이터를 수신하면 무결성 에러 메시지를 출력한다.

(3) 해쉬 알고리즘 적합성 검증 모듈

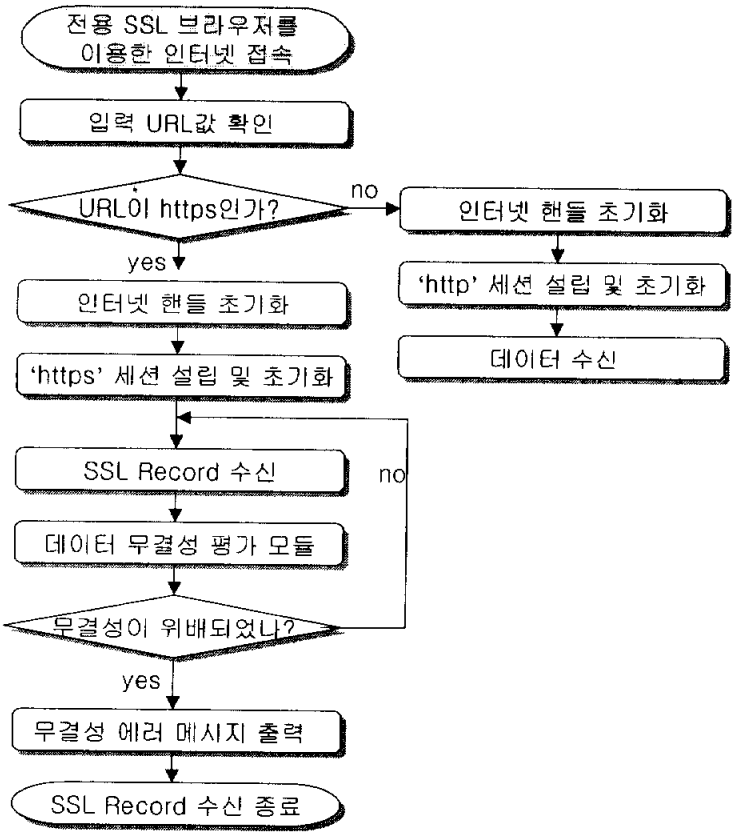
해쉬 알고리즘 적합성 검증 모듈은 전용 SSL브라우저의 SSL모듈에 사용된 해쉬 알고리즘의 적합성을 평가한다. 그리고 적합성 평가는 NIST에서 안전성을 평가하여 권고하고 있는 해쉬 알고리즘을 기준으로 평가를 수행한다.

4.4.2 무결성 검증 시스템 구현

본 논문에서 구현한 무결성 검증 시스템은 Winodws CE기반의 PDA 이동 컴퓨팅 단말을 기본 환경으로 하였으며, 시스템 구현 환경은 다음과 같다.

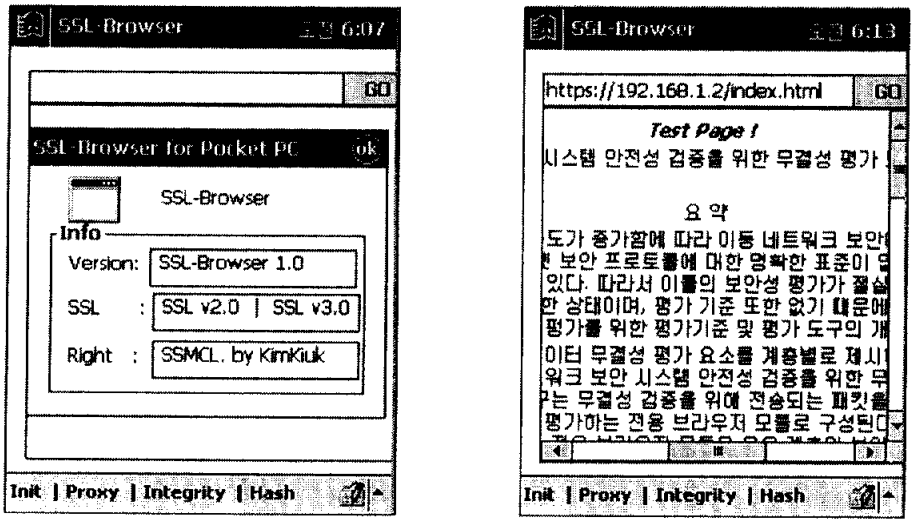
- Target OS : Windows CE 2002
- Target H/W : Pocket PC (ARM)
- 구현 도구 : Embedded Visual C++ 3.0

무결성 검증 시스템의 동작 원리는 [그림 13]과 같다. 무결성 검증을 위해 전용 SSL 브라우저에 입력된 URL을 체크하여 SSL프로토콜 적용 여부를 결정한다. 만약 'https'접속일 경우는 SSL 프로토콜을 적용하여 무결성 검증을 시도하지만, 'http'접속일 경우는 일반 웹 서비스를 제공한다. 'https'로 접속한 경우는 보안 세션을 설립하고 암호화된 SSL Record를 수신하며, 수신된 SSL Record는 데이터 무결성 평가 모듈로 전송되어 데이터 변조 여부를 검증한다. 이때 무결성 에러가 없는 SSL Record를 수신했다면, 데이터를 전용 SSL 브라우저에 출력한 후 다음 SSL Record를 수신하지만, 만약 무결성 에러가 발생한 Record라면 무결성 에러 메시지를 출력하고 SSL Record 수신을 종료한다.



[그림 13] 무결성 검증 시스템의 동작 원리

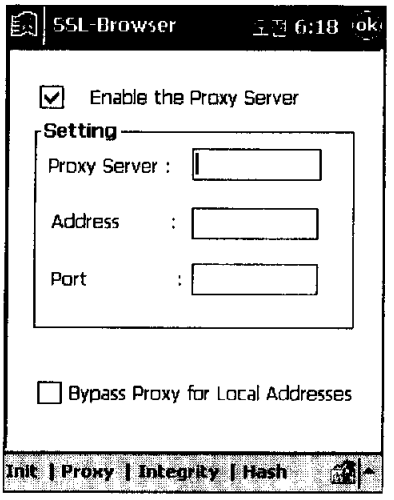
[그림 14]의 (a)는 전용 SSL 브라우저의 초기 화면이며, (b)는 전용 SSL 브라우저로 "https"(SSL Connection)로 접속한 결과 화면이다.



(a) 초기화면 (b) 브라우저 실행 화면

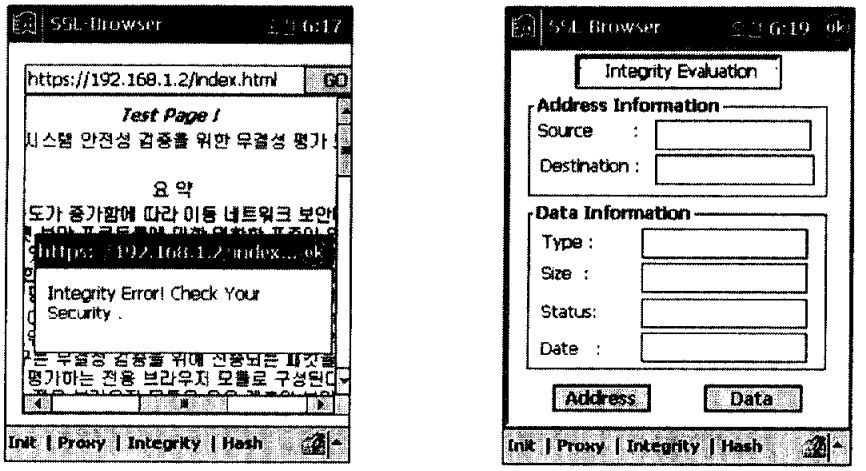
[그림 14] 전용 SSL 브라우저 실행 화면

[그림 15]는 Proxy 기능을 제공하는 다이얼로그 화면이다. Proxy 셋팅 기능을 이용하여 SSL 전용 브라우저를 Proxy형태의 SSL 제품 평가에 사용할 수 있다. Setting탭의 Proxy Server에서는 연결할 프럭시 서버의 형태를 입력하고, Address와 Port 항목에는 Proxy 연결을 위한 주소와 포트 정보를 입력한다.



[그림 15] Proxy 메뉴 화면

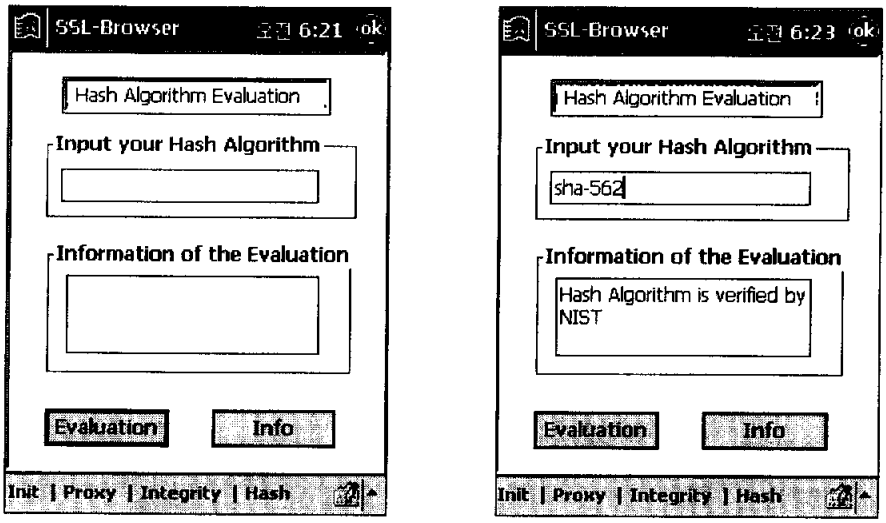
[그림 16]은 무결성 평가 모듈의 실행 결과이다. 변조된 데이터를 전용 SSL 브라우저가 수신했을 때 무결성 평가 모듈은 무결성 에러 메시지를 출력한다. 하지만 만약 WinInet SSL 모듈의 무결성 기능이 잘못되었다면 에러정보를 무결성 평가 모듈에 전달하지 못하며, "무결성 에러 메시지"가 출력되지 않는다. 그리고 후자의 경우엔 SSL모듈의 무결성 기능이 잘못되었다고 평가한다. 무결성이 위배된 소스의 정보는 Integrity 메뉴를 통해 재확인 할 수 있다. [그림 16]의 (a)는 변조된 데이터를 수신했을 때 무결성 평가 모듈에서 검증한 결과 화면이고, (b)는 Integrity 메뉴의 초기 화면이다. Integrity 다이얼로그의 Address Information을 통해 무결성이 위배된 데이터의 소스·목적지 주소 정보를 확인하며, Data Information을 통해 변조된 데이터 Type과 크기, 그리고 보안 프로토콜이 적용된 데이터였는지에 대한 상태정보와 변조된 날짜 정보를 알 수 있다.



(a) 무결성 검증 (b)Integrity 메뉴 화면

[그림 16] 무결성 평가 모듈 실행 결과

[그림 17]은 해쉬 알고리즘 적합성 검증 결과이다. 대부분의 무선 SSL 제품에서는 해쉬 알고리즘으로 SHA-1, SHA, MD5등을 사용하지만 미국 NIST에서 안전한 해쉬 알고리즘으로 권고한 표준 해쉬 알고리즘에서는 SHA-1, SHA-256, SHA-384, SHA-512등을 권고하고 있다. 따라서 무선 SSL 제품에서 사용하는 해쉬 알고리즘이 NIST 권고안에서 권고한 알고리즘인지에 대한 검증을 해쉬 알고리즘 적합성 검증 모듈에서 검증한다. 해쉬 알고리즘 검증 모듈은 전용 SSL 브라우저에 포함하여 구현하였다. [그림 17]의 (a)는 Hash 메뉴를 통해 제공되는 해쉬 알고리즘 검증 다이얼로그의 초기 화면이며, (b)는 해쉬 알고리즘 적합성 검증 결과이다.



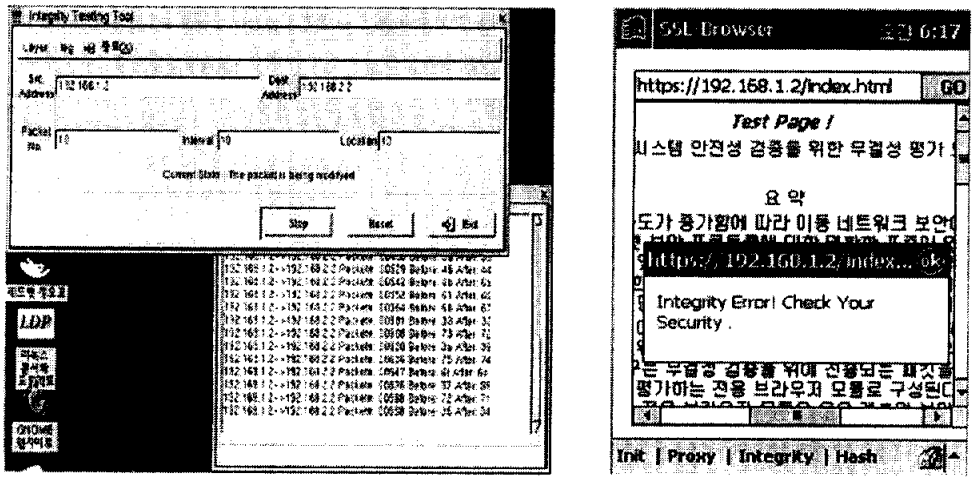
(a) Hash 메뉴 화면 (b) 알고리즘 적합성 검증 수행

[그림 17] 해쉬 알고리즘 적합성 검증 결과

4.5 구현 결과

본 절에서는 4.1절에서 제안한 평가 방법으로 논문에서 구현한 WinInet SSL 모듈의 무결성을 평가하였다.

[그림 18]은 데이터를 변조해서 WinInet SSL 모듈로 전송했을 경우의 결과화면이다. [그림 18]의 (b)에서처럼 SSL 전용 브라우저의 무결성 검증 모듈에서 무결성 에러 메시지를 출력함을 확인하였다. 따라서 본 논문에서 검증 대상으로 구현한 WinInet 라이브러리의 SSL 모듈이 무결성을 제공함을 평가하였다.

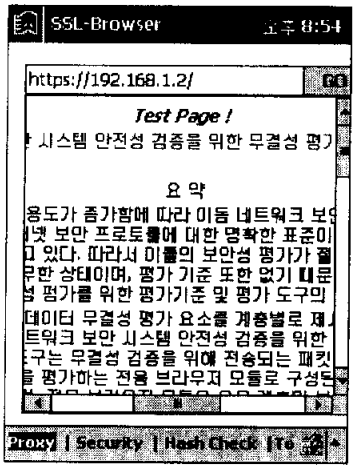


(a) 변조 서버 결과 (b) 무결성 검증 결과

[그림 18] 전송 중 데이터를 변조할 경우

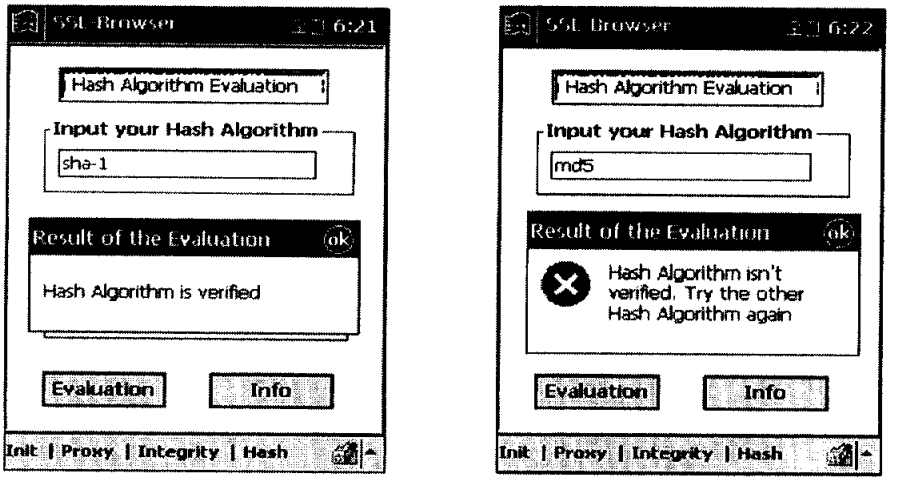
[그림 19]는 변조 서버에서 패킷을 변조하지 않고 전송했을 때 전용 SSL 브라우저에서 무결성이 제공된 데이터를 출력하는지를 확인하는 테스트 화면이다.

본 테스트에서는 무결성 에러가 없는 데이터를 수신했을 때 올바르게 브라우저 화면에서 전송 결과를 출력하는지 확인하기 위해 전용 네비게이터에서 웹 서버로 SSL을 이용한 보안 접속을 시도한 후 서버로부터 전송된 웹 페이지가 제대로 보여지는지 확인하였다.



[그림 19] 데이터를
변조없이 전송할 경우

[그림 20]은 해쉬 알고리즘 적합성 검증의 수행 결과 화면이다. 그림에서처럼 NIST 권고안의 표준 해쉬 알고리즘을 기준으로 SSL 모듈에 사용된 해쉬 알고리즘의 적합성을 검증하였다.



[그림 20] 해쉬 알고리즘 적합성 검증 결과

5. 기존 연구와의 비교 및 결과 분석

최근 정보보호 제품 평가에 관한 연구가 활발하게 진행되고 있다. 하지만 무선 보안제품 평가에 대한 연구는 미약하며, 무선 보안제품을 평가할 수 있는 평가 방법 및 평가 도구의 개발이 필요하다.

본 논문에서는 응용계층 무선 보안제품의 무결성을 평가하기 위해 '유선 VPN제품의 무결성 평가' 방법을 기반으로 무선 보안시스템 무결성 평가 방법을 제시하고 평가 도구를 구현하였다. 본 논문에서 구현한 응용계층 무선 보안시스템 무결성 평가도구의 구현 결과를 '유선 VPN제품의 무결성 평가' 연구와 비교하면 [표 3]과 같다. 표에서처럼 본 논문에서 구현한 평가 도구는 유선 VPN의 무결성 평가 방법을 이용하여 응용계층 무선 보안시스템의 무결성을 평가할 수 있는 평가 도구를 구현하였다. 본 논문에서 구현한 평가도구의 특징은 다음과 같다. 무선 보안시스템 무결성 평가를 위해 평가도구는 변조 서버 시스템과 무결성 검증 시스템으로 구성된다. 그리고 무선 보안시스템의 평가는 유선 VPN제품에서 제시한 데이터 무결성 평가와 함께 알고리즘 적합성 검증도 수행한다.

[표 3] 기존 연구와의 비교

	유선 VPN 제품 평가	본 논문의 평가 도구
네트워크 환경	유선 네트워크	이동 네트워크
평가 계층	네트워크 계층	응용계층
평가 대상	유선 VPN 제품	무선 SSL 제품
평가 시스템 전체 구성	- 송·수신 Host - 변조 서버 시스템	- 송·수신 Host - 변조 서버 시스템 - 무결성 검증 시스템 : 전용 SSL 브라우저 : 데이터 무결성 평가 모듈 : 해쉬 알고리즘 적합성 검증 모듈
평가 내용	데이터 무결성 평가	- 데이터 무결성 평가 - 해쉬 알고리즘 적합성 검증 : FIPS 140-2 근거

6. 결론

최근 무선 인터넷 서비스가 활성화되고 있다. 이와 더불어 안전한 무선 인터넷 사용을 위한 정보보호 제품의 개발과 연구가 활발히 진행중이지만 이들의 신뢰성에 관한 연구는 아직 부족하다. 안전성과 신뢰성이 검증된 정보보호시스템을 사용하기 위해 미국, 영국, 독일, 프랑스, 캐나다 등을 중심으로 자국의 환경에 적합한 평가·인증 제도를 마련하여 정보보호 제품을 평가해 오고 있으며, 국내에서도 1998년 2월부터 평가·인증 제도를 시행 중에 있다. 하지만 아직 평가기준을 바탕으로 정보보호제품을 평가할 수 있는 평가도구의 개발은 미비하며, 특히 무선 보안시스템의 안전성을 검증하기 위한 평가기준 및 평가도구의 개발은 더욱 부족하다.

따라서 본 논문에서는 응용계층 무선 보안시스템의 무결성 평가 방법을 제시하고 평가 도구를 설계 및 구현하였다. 제안한 평가방법은 다음과 같다. 즉, 무선 보안시스템으로 전송되는 데이터를 전송 중 불법적으로 변조시킨 후 무선 보안시스템으로 전송한다. 그리고 무결성이 위배된 데이터를 무선 보안시스템에서 검증하는지 확인하여 무선 보안시스템의 무결성을 평가한다. 제안한 방법으로 무선 보안시스템의 무결성을 평가하기 위해 본 논문에서 구현한 평가도구는 변조서버 시스템과 무결성 검증 시스템으로 구성하였으며, PDA에서 동작하는 Windows CE WinInet API의 SSL기능을 대상으로 무결성 평가를 하였다. 변조서버 시스템은 리눅스 커널의 패킷 전송 원리를 이용하여 리눅스 커널 모듈에 패킷변조 루틴을 구현하였다. 그리고 전송되는 데이터를 불법적으로 캡쳐하고 이

를 변조시키기 위해 변조서버 시스템은 2개의 이더넷 카드를 이용하여 웹 서버와 PDA사이에 위치시킨다. 그리고 웹 서버와 PDA사이에 전송되는 패킷은 반드시 변조서버 시스템을 통과하도록 구성하였다. 변조서버 시스템에서 패킷을 변조할 때는 사용자로부터 변조할 패킷의 목적지 주소, 소스 주소, 변조 간격, 변조할 패킷 번호 등의 정보를 화면 인터페이스를 통해 입력받은 후 이 정보에 해당하는 패킷을 변조한다. 무결성 검증 시스템은 Windows CE기반의 PDA에서 동작하는 브라우저를 구현하고, 구현한 브라우저에 WinInet API의 SSL기능을 이용하여 SSL기능이 내장된 전용 브라우저를 무결성 평가 대상으로 구현하였다. 그리고 구현한 SSL 전용 브라우저에 WinInet SSL모듈의 무결성 기능을 검증하는 모듈과 SSL에 사용된 해쉬 알고리즘의 적합성 검증 모듈을 구현하여 구현한 SSL 전용 브라우저의 무결성을 평가하였다.

본 논문을 통해 아직 연구가 부족한 무선 보안시스템의 안전성을 평가할 수 있는 무결성 평가 방법을 제시하였으며, 제시한 평가방법에 따라 평가 도구를 구현하였다. 그리고 제안한 평가도구로 논문에서 구현한 SSL 전용 브라우저의 무결성을 평가하여 무선 보안시스템 응용계층 무결성 평가도구의 적합성을 증명하였다. 하지만 현재 상용화되어 있는 무선 보안시스템들이 동일한 SSL모듈을 사용하는 것이 아니라 업체별로 Windows CE 환경의 SSL라이브러리를 구현하고, 이를 이용하여 무선 보안시스템을 개발하는 상황을 고려할 때 다양한 SSL모듈에 대해 호환성 있는 무결성 검증 모듈의 개발 작업이 필요하다.

[참고 문헌]

[1] 이종후, 류재철 "인터넷 보안", Telecommunications review, 제 10권 5호, 2000.

[2] 한국정보보호센터, "정보보호 시스템 평가제도", http://www.kisa.or.kr/sysevaluation/menu2/sub1/index.html.

[3] 한국정보보호센터, "정보보호시스템 평가·인증 가이드",

[4] NIST, "Cryptographic Module Validation (CMV)Program" http://csrc.nist.gov/cryptval.

[5] 이성재, 김영백, 홍시환, 김승주 "암호제품 평가체계 분석", 정보보호학회지, 제 12권 3호, 2002.6.

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

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

[8] "평가기준 지침서 - ITSEC", http://www.kisa.or.kr/sysevaluation/menu1/sub2/itsec.html.

[9] "평가기준해설", http://www.kisa.or.kr.

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

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

[12] "Common Evaluation Methodology for Information Technology

Security, Part 1 Introduction and general model", Ver 0.6, 1997.

[13] "Common Evaluation Methodology for Information Technology Security, Part 2 Evaluation Methodology", Ver 0.6, 1997

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

[15] 이만영, "전자상거래 보안기술", 생능출판사,1999.

[16] "정보보호시스템 보안기능 통합 평가 도구 개발", 한국정보보호센터, 2000.12

[17] 김기욱, 정경훈, 장용호, 김창수, "무선 인터넷 보안을 위한 SSL활용 연구", 한국멀티미디어학회 춘계 학술발표 대회 논문집, 2001.

[18] 이석준, 정병호, 정교일 "무선 전자상거래를 위한 보안 기술", 한국정보보호학회지, 제 12권 3호, 2002.6.

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

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

[21] Steve F. Russell "Wireless Network Security for Users', IEEE, 2001.

[22] NIST, "Security Requirments for Cryptographic Modules", FIPS 140-2, 2001.

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

[24] R Magnus, U Kunitz, M Dziadzka, D Verworner, M Beck, H Böhme "Linux Kernel Internals" pp. 258-315, 1999. http://www.kisa.or.kr, 2000.

[25] 김기욱, 정경훈, 김창수, "무선 인터넷 보안모듈 설계 및 검증도구에

관한 연구", 한국 정보보호학회 영남지부 학술발표대회 논문집, 2002.

[26] 조재만, 곽선정 "임베디드 Windows CE 프로그래밍", PCBOOK, 2001.

감사의 글

어느덧 길고도 짧았던 2년의 대학원 생활을 마무리하고 졸업을 앞두게 되었습니다. 돌이켜보면 많은 프로젝트와 세미나 등으로 힘들고 바쁜 시간들이었지만, 그런 어려운 시간이 있었기에 부족하고 마냥 어리기만 했던 제가 지금의 저로 성장할 수 있었습니다. 그리고 2년간의 대학원 생활과 이 논문을 완성할 수 있도록 도움을 주셨던 많은 분들께 이 지면을 빌어 감사의 말씀을 전합니다.

먼저 학부 시절부터 언제나 따뜻한 애정으로 보살펴 주시고, 학문적으로 많은 가르침을 주셨던 김창수 지도교수님께 감사드립니다. 그리고 저의 논문이 완성되기까지 세심한 지도를 해 주셨던 박홍복 교수님, 박지환 교수님, 정신일 교수님, 그리고 많은 지도를 해 주셨던 박만곤 교수님, 여정모 교수님, 윤성대 교수님, 박승섭 교수님, 김영봉 교수님, 정순호 교수님, 이경현 교수님께도 감사의 말씀을 드립니다.

학부시절부터 언제나 귀여워 해주고 아껴주신 전태건 선배, 정경훈 선배, 고민이 있을 때 많은 조언을 해 주신 미경 언니와 은미 언니, 그리고 사모님께 감사드립니다. 그리고 연구실에서 함께 생활하면서 많은 도움을 주셨던 나호준 선생님과 남진 선배, 진호씨, 진수 선배에게 감사드리며, 학부동기로써 힘이 되주었던 형원, 성석 오빠에게 감사드립니다. 후배 경순, 수진, 미선에게도 감사드리며, 김봉제 선생님과 산업 대학원, 교육 대학원 선생님들께도 감사드립니다. 그리고 2년 동안 서로 용기가 되어 주었던 대학원 동기 소진, 희연, 명진, 지철, 상수 오빠에게 감사 드리며, 같은 연구실에서 생활하면서 많은 도움을 주었던 덕현 선배와 힘들고 어려울 때 옆에서 격려와 조언을 아끼지 않았던 종우 선배에게 감사드립니다.

마지막으로 딸이 가고자 하는 길을 묵묵히 후원해 주셨던 아버님, 늘 뒤에서 지원해 주시고 제가 올바른 길을 갈 수 있도록 기원해주신 어머님께 감사드리

며, 철없는 동생의 한결같은 버팀목이 되 주었던 오빠에게 감사드립니다. 그리고 어릴 적부터 저를 보살펴 주셨던 할머니께 감사의 말씀을 전하며 이 논문을 저의 사랑하는 가족들에게 바칩니다.