논문 2004-41TC-9-8

무선인터넷 상에서 Embedded Linux를 이용한 WPKI의 설계 및 구현

(Design and Implementation of WPKI Using Embedded Linux on the Wireless Internet)

박 상 현*, 강 찬 휘**, 신 승 호*

(Sang Hyun Park, Chan Hee Kang, and Seoung Ho Shin)

요 약

무선 단말기 기반 기술의 발달에 따라 많은 이용자들이 있고, 일반 PC에서만 사용되던 기술들을 무선의 시간 공간 제약이 없는 작업환경에서 이용하고자 하는 욕구의 증가로 점차 확산되고 있다. 이에 발 맞추어 2003년 중반 4개 은행이 PC에서 사용되던 인터넷 뱅킹을 무선 단말기를 이용하는 서비스로 확장 시행하였다. 현재 단말기는 PPC(Pocket PC)와 Palm, 사용되는 운영체제로는Window CE와 Palm을 운영체제로 하는 기기에서 서비스를 제공하고 있어, 위의 단말기를 제외한 이 기종에서 서비스 사용이 어렵다. 더 많은 사용자들의 사용을 위해서는 다양한 단말기에서의 사용이 가능하여야 하기 때문에 이 논문에서는 Linux를 OS로 하는 단말기에서의 WPKI인증 기술을 구현한다

Abstract

Because the Internet diffusion has been increased, the service that used at the offline has been applied to the online, the saving time and portability has been emphasized, and the service has been increased from the wire to the wireless by the development of the mobile communication technology. There are a Pocket PC, Palm and so forth as devices that are used for it and the services are already used. However, because it is used at only limited operating systems like PCs have, there is the restriction to use for much more users. In order to allow various devices used by much more people the access services, the WPKI authentication should be implemented for devices using Linux OS.

Keywords: WPKI, Embedded, Linux

I. 서 론

정보 기술의 발달로 오프라인에서 이용하던 서비스를 온라인상으로 적용하기 시작했으며, 수요의 증가에 의하여 서비스의 질적 향상을 위에 무료에서 유료로의 전환이 많이 이루어지고 있다. 유료로 전환을 한 서비스 업체와 고객은 지불에 따른 보안상의 문제에 대하여 우려와 관심이 높아져, 정보통신 기술을 전자지불 서비스 분야에 도입하여 기업과 소비자에게 보다 효율적인 지불방법을 제공하려는 움직임이 활발하다. 이와 더불어 사용자의 사용상의 편의를 위한 일환으로 유선에서 제공되던 서비스를 무선에서도 적용하는 사례가 빈번해지면서 유선 상에서와 같이 무선에서도 안전한 서비스 제공을 위한 방법이 필요하게 되었다.

PDA와 핸드폰 등의 단말기를 이용한 서비스를 위하여 많은 투자가 이루어 졌고, 현재 서비스들은 은행, 증권, 등에서 사용자의 정보보호를 위하여 사용하고 있다. 사용되는 단말기로는 Palm과 Windows CE를 운영체제로 하는 장비에 국한되어 서비스를 제공한다.

* 정회원, 인천대학교 컴퓨터공학과
(Dept. of Computer Engineering, University of incheon)
** 정회원, 상지영서대학교 디지털영상과
(Dept. of Digital Information Of Sangji Youngseo Colleage)
※ 본 연구는 과학기술부 지정 동북아 전자물류 연구센터의 지원에 의한 것입니다
접수일자: 2004년6월18일, 수정완료일: 2004년9월8일

윈도우를 운영체제로 하는 장비의 경우에는 운영체제가 기본적으로 용량이 크고 빠른 처리속도를 요구하기 때문에 단말기 역시 빠른 CPU와 큰 용량을 가진 메모리가 있어야 하고, 운영체제 역시 라이선스가 있어야 사용이 가능하다. 이 모든 요소가 단말기 가격 상승의 원인이 된다.

단말기의 가격인하와 운영체제의 라이선스 문제를 해결하기 위한 방안으로 Linux를 운영체제로 하는 장비들이 제시되고 있다. 그러나 현재 Linux를 운영체제로 사용하는 장비들은 인터넷 뱅킹 등의 서비스가 사용되고 있지 않다.

본 연구에서는 유선에서 사용되고 있는 SET 프로토콜 암호화 방식을 무선 환경에서 Embedded Linux를 이용하여 WPKI방식을 구현하는 방법을 제안하려고 한다.

II. 본 론

1. SET 프로토콜

유선에서 사용되는 프로토콜은 SET 프로토콜로써 암호화 기술로는 RSA, DES, SHA-1 알고리즘을 사용하여 보안기능을 제공하고 있으며, 공개키 기반 (PKI : Public Key Infrastructure)에 대한 인증을 수행하기 위하여 X.509 Ver.3증명서를 채용한다. 각종 신용카드 번호, 비밀번호, 개인 신상에 관한 정보를 클라이언트에서 암호화 알고리즘을 이용하여 서버로 전송하고 서버에서는 사용자에 대한 확인 유무를 통하여 다시 클라이언트에 전송하는 방식을 사용한다.

가. WPKI

무선 환경에서 ME(Mobile Explore), WAP(Wireless Application Protocol), i-mode가 있는데, WAP은 WAP forum에서 개발을 하여 주로 모바일 단말기에서 사용되고, ME는 MS(Microsoft)의 무선 인터넷을 위한 브라우저에서 사용되고 TCP/IP를 이용한다. i-mode는 일본의 NTT에서 개발하여 c-HTML을 사용한다.

유선과 마찬가지로 무선 인터넷의 안정한 서비스를 제공 받기 위해서는 기밀성 (confidentiality), 무결성 (in-tegrity), 인증 (authentication), 부인방지와 같은 서비스를 제공하기 위한 무선PKI가 필요하다.

무선 PKI란 기존의 유선 PKI를 무선 환경에 적합하게 확장, 적용시킨 무선 공개키 기반구조로 무선 인터넷을 이용해 사용자간에 주고받는 정보의 변경 여부를 확인하고 사용자의 신분확인을 위한 인증 서비스를 제공하는 기술이다. 무선 PKI도 PKI와 같이 키 인증서 방식을 이용한 무선 네트워크 전자 상거래의 활성화를 위해 제안된 기반 구조이다. 기본적으로 무선 환경에서 WTLS(Wireless Transfer Layer Security)와 WML-Script(Wireless Markup Language Script) Crypto Library에서 제공하는 signText() 함수를 이용하여 단대단 보안을 보장한다.

2. 임베디드 리눅스 (Embedded Linux)

가. 리눅스 (Linux)

리눅스란 인텔 80386 이상을 사용하는 PC에서 운영되는 유닉스 운영체제의 공개버전이다. 기본적인 환경은 POSIX 사양 및 SYSV, BSD와 같으나 독자적인 소스로 개발되었다. Linus B. Torvalds에 의해 커널이 개발되고 인터넷을 통하여 점차 발전되었다. 완전한 멀티태스킹, 가상 메모리, 공유 라이브러리, 효율적인 메모리 관리, TCP/IP 네트워킹 등 소규모 유닉스 운영체제로 안성맞춤이다.

나. 임베디드 리눅스 (Embedded Linux)

임베디드 리눅스는 낮은 성능의 프로세서와 작은 크기의 메모리를 가진 내장형 시스템용으로 개발된 리눅스이다. 임베디드 장치는 작은 크기의 메모리 밖에 장착할 수 없다는 제약으로 인하여 리눅스 자체의 크기와 기능이 최소화, 경량화, 맞춤화 되어야 하며, 낮은 성능의 프로세서를 사용하는 제약을 극복하기 위하여 성능의 최적화 되어야 한다는 특징을 가지고 있어야 한다.

3. Embedded Linux 환경에서의 WPKI 인증방안

무선 PKI는 기존의 유선 PKI의 구성요소를 그대로 이용하지만, 무선 환경의 여러 제약 조건을 고려하여 기능을 최소화 하였다. 유선 PKI에서 사용되는 X. 509 인증서보다 부피가 작고 간단한 구도를 가진 WTLS (Wireless Transfer Layer Security)인증서를 사용하여 저 용량 단말기에서 암호화 및 인증 업무를 효율적으로 사용할 수 있도록 구성 되었다.

가. 무선 PKI 구조

무선 PKI의 구조로는 사용자의 정보를 받아 인증서 등록 및 사용자 신원 확인을 대행하는 등록기관 (RA : Registration Authority), 인증서를 발행하고 효력 정지 및 폐지 기능을 수행하는 인증기관(CA : Certification

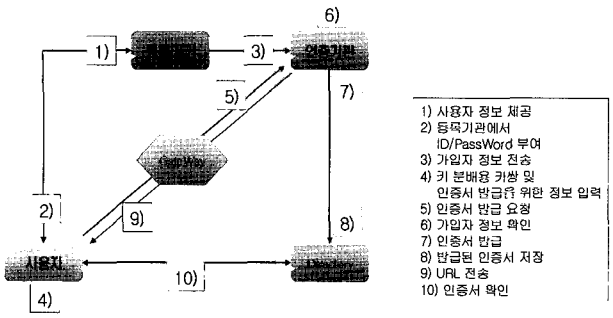

그림 1 무선 PKI의 구조
Fig. 1. Wireless PKI Structure.

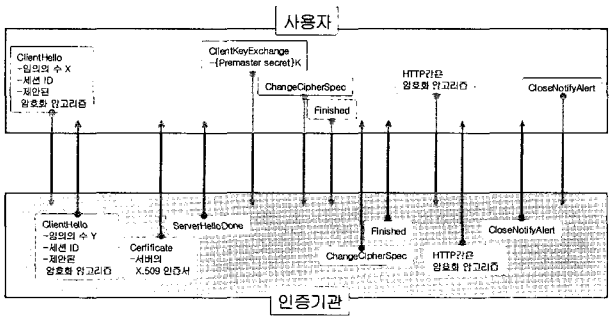

그림 2. 서버 인증서만 보유하는 SSL
Fig. 2. SSL with only a Certificate of Attestation.

Authority), 인증서 폐지 목록을 저장하는 디렉터리(Di-rectory), 그리고 인증서를 신청하고 사용하는 사용자(EE: End Entity)가 있다. 그림 1은 기본적인 무선 PKI의 구조이다.

나. 무선 PKI 모델

무선 PKI에서는 단말기의 여러 제약 조건을 고려하여 무선용 X. 509 인증서 WTLS 인증서 또는 갱생 주기가 24-48시간인 Short-lived 인증서를 사용하며, 인증서를 발행 받을 경우 인증서의 URL만을 이용하기도 한다.

서명 알고리즘으로는 RSA(Rivest Shamir Adleman) 알고리즘 수준을 갖는 ECDSA(Elliptic Curve Digital Signature Algorithm) 사용하며, 암호화 알고리즘으로는 RC4, RC5, SEED중 SEED를 사용하며, 해시 알고리즘으로는 MD5, SHA-1중 SH-1을 사용한다.

다. 무선 PKI 인증 방법

WPKI 인증방법은 일반사용자가 단말기를 이용하여 사용자 정보를 직접 생성하나 단말기의 처리속도나 용량의 문제로 인하여, 서버용 전자 서명키는 인증기관에서 생성을 한 후 자체 Directory에 인증서를 저장해 두었다가 사용자의 요청 시에 이를 이용하여 인증서를 확인하고 서비스를 제공하는 방식이다.

유선 인터넷 뱅킹을 이용 할 때 서버에 접속하는 사용자는 Xecure Client라는 프로그램이 설치되어 웹 페이지에서 작업하는 내용에 대하여 보안 작업을 한다. Xecure Client는 ActiveX와 SSL인증 방식을 이용한다. SSL은 공개키 기술을 사용해서 데이터 무결성과 데이터 프라이버시를 제공하지는 않지만, 대신 비밀 키를 만드는 데 필요한 정보를 교환할 때 공개키 암호화를 사용하고, 그런 다음 SEED, RC4 같은 암호화 알고리즘과 비밀 키를 통해서 데이터 무결성과 프라이버시를 제공한다.

서버만이 인증서와 개인키를 가지는 경우, SSL은 클라이언트가 서버를 인증하고, 클라이언트와 서버 모두가 알고 있는 비밀 키를 안전하게 만들어 내는 데 사용될 수 있다.

Ⅲ. 실 험

1. Embedded Linux 환경에서의 WPKI 인증방안

가. 구현 모델

무선 PKI에서는 인증서 요청 시 사용자 인증을 위해 사용자 아이디와 패스워드를 사용한다. 이때 아이디와 패스워드는 제안된 알고리즘에 의해 암호화 되어 해당 공개키를 가진 무선 PKI포탈에 전송해야 하며, POP (Proof Of Possession)을 수행하여야 한다. POP는 인증서 요청 시, 인증서에 포함되는 공개키에 해당하는 비밀 키를 알고 있다는 것을 무선 PKI포탈에 증명하는 과정으로서, 인증서 요청 프로토콜 그리고 인증서에 따라 여러 방법이 사용되고 있다.

구현에서는 ME방식을 이용하여 웹 기반의 클라이언트 프로그램을 제작하였다. 사용자의 접속을 담당하는 클라이언트 프로그램은 리눅스의 BSD소켓 인터페이스 소켓 프로그래밍을 이용하여 작업을 하며, 제작된 프로그램을 단말기에 설치하는 방법을 사용한다. 서버의 경우는 사용자의 정보와 인증서의 목록을 가지고 있는 디렉터리로 구성을 한다. 그림 3은 본 연구에서 구현되는 구조이다.

무선 액세스 접근을 위한 방식으로는 802.11의 요구에 따라 유선 동등 프라이버시 (WEP:Wired Equivalent Privacy)를 구현하고 있는 모든 스테이션에게 공유키 인증을 구현한다. 공유키 구현은 이름이 의미하는 것처럼 인증 전에 공유키를 스테이션에 분배하여 둔다[9].

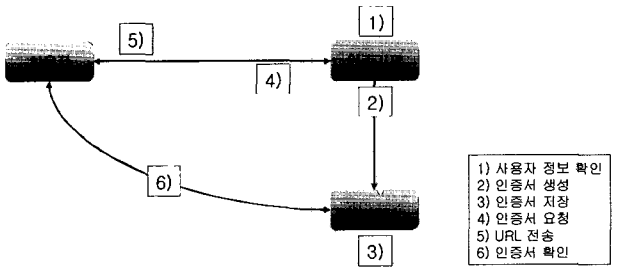

그림 3. 구현 구조
Fig. 3. Implementation Structure.

사용자 정보를 입력 받은 인증서버에서는 사용자 정보를 확인 후 인증서를 생성하여 Directory폐기 목록 저장을 한다. 인증서의 생성 후 사용자의 접속을 통해 인증서 내용 요청 시 서버에서 사용자의 고유한 코드를 생성하여 사용자에게 전송하고 사용자는 이를 이용하여 접속을 시도한다. 고유한 코드 발행은 이중사용방지를 위한 것이다.

사용자가 URL을 이용하여 접속하기 위한 클라이언트 프로그램을 실행하고 작성된 개인 정보는 SSL을 이용한SEED 암호화 알고리즘과 공개키를 이용하여 암호화를 하고 서버에 전송해 준다. 전송 받은 서버는 미리 저장되어 있는 비밀 키를 이용하여 암호화된 내용을 풀고 인증서와 대조하여 인증결과를 사용자에게 전송하여 준다.

Ⅳ. 결 론

본 논문에서는 리눅스를 OS로 하는 임베디드 시스템에서의 무선 PKI인증을 기존에 사용하고 있는 유선 PKI을 이용하여 리룩스 환경에 맞게 새롭게 설계 및 구현 하였다. 현재 사용되고 있는 인터넷 보안 기술을 그대로 적용하기에는 임베디드 시스템의 기능적 제약과 운영체제로 사용하는 운영체제의 호환성 문제가 있다.

서버와 클라이언트의 접근을 위한 방식으로 BSD소켓 인터페이스를 이용한 소켓 프로그래밍을 이용하여 서버에 접속하는 클라이언트 프로그램을 제작하였으며, 서버에 접근하는 방법으로는 URL을 이용한 접근 방법을 사용하였다. URL을 통하여 접속하는 ID와 패스워드를 공개키를 이용한 암호화 기법에 의해 암호화된 내용을 서버에 전송하며, 서버에서는 비밀 키를 가지고 전송 받은 내용을 복구하여 인증서의 내용과 대조 확인하여 사용자 정보를 확인하는 방법을 사용하였다.

대부분의 사용자들이 리눅스라는 환경에 거부감을 느끼는 것은 예전의 어려운 설치와 텍스트 기반 구조에 의해 조작이 어렵다는 점이 있다. 그러나 현재 리눅스도 점차 사용자 인터페이스를 제공하면서 설치 및 동작이 윈도우 사용자만큼이나 편해졌다.

사용자의 거부감만큼 프로그래머들 역시 거부감을 가지고 있는 것이 사실이다. 복잡한 커널을 알아야 하고 비주얼적인 프로그램이 없다는 것이다.

윈도우 환경보다 뛰어난 리눅스의 보안 기법을 활용하고, 저가 단말기의 보급과 윈도우 환경의 속박에서 벗어나기 위해서는 지속적인 연구가 이루어져야 한다.

참 고 문 헌

[1] 정철현, "PKI 전자성명과 인증제도", 다산출판사, pp. 53-69, 2003.01
[2] 전성배, 제1회 전자서명 인증 워크샵, 정보통신부 정보기획과, "무선 PKI 정책 방향", 2000.08
[3] 이현주, 최문석, "RSA 서명 기법을 이용한 무선 전자상거래", 한국정보처리학회, 2002.11
[4] 칼리스 아담스, 스티브 로으드, "보안을 위한 효율적인 방법 PKI", Addison Wesley, p.125-139, 2003.09
[5] 이연조, "임베디드 리눅스 프로그래밍", PCBOOK, 2002.05
[6] 송호중, "Trolltech Qt 리눅스 프로그래밍" Dream-Book, p.31-50, 2000.11
[7] Michael Welschenbach, "Cryptography in C and C++", Apress, p.390-399, 2003.01
[8] Mattbew S.Gast, "802.11 Wireless Networks", pp. 185-190, 339-376, April 2002.
[9] William Stallings, "Cryptography and Network Security Principles and Practice" Green, p.377-400, 2001.02

저 자 소 개

신 승 호(정회원)
1979년 경희대학교
전자공학과 (공학사)
1981년 경희대학교
전자공학과 (공학석사)
1985년 경희대학교
전자공학과 (공학박사)
1986년~현재 인천대학교 컴퓨터공학과 교수
<주관심분야: 컴퓨터통신, 신호처리, 암호학>

강 찬 휘(정회원)
1980년 경희대학교
전자공학과 (공학사)
1982년 경희대학교
전자공학과 (공학석사)
1994년 경희대학교
전자공학과 (공학박사)
1989년~현재 상지영서대학교 디지털영상과 교수
<주관심분야: 영상처리, 컴퓨터 통신, 신호처리>

박 상 현(정회원)
2003년 인천대학교
컴퓨터공학과 (공학사)
<주관심분야: 컴퓨터 통신, 임베디드 리눅스, 암호학>