제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

리눅스 상에서 PDA를 이용한 WPKI 인증 방안에 관한 연구

박상현*,신승호*
*인천대학교 컴퓨터공학과
e-mail : tank1862@incheon.ac.kr, shin0354@incheon.ac.kr

A Study on Wireless PKI authentication Scheme using of PDA on Linux.

Sang-Hyun Park, Seung-Ho Shin
Dept. of Computer Science & Engineering, University of Incheon

요 약

무선 단말기 기반 기술의 발달에 따라 많은 이용자들이 있고, 일반 PC 에서만 사용되던 기술들을 무선의 시간 공간 제약이 없는 작업환경에서 이용하고자 하는 욕구의 증가로 점차 확산되고 있다. 이에 발 맞추어 2003 년 중반 4 개 은행이 PC 에서 사용되던 인터넷 뱅킹을 무선 단말기를 이용하는 서비스로 확장 시행하였다. 현재 단말기는 PPC(Pocket PC)와 Palm, 사용되는 운영체제로는 Window CE 와 Palm 을 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 Linux 를 OS 로 하는 단말기에서의 WPKI 인증 기술을 구현한다.

1. 서론

무선 단말기 기술의 기반인 정보통신 기술의 발달로 사용자는 장소의 구별 없이 무선 통신을 사용한 서비스 이용이 급증하고 있으며, PC 에서 이용하는 기술도 무선단말기를 이용하는 작업환경으로 바뀌어 가고 있다. 이에 따라 PC 를 이용한 증권거래, 카드 판독기, 인터넷 뱅킹등과 같은 서비스들이 무선 단말기를 이용한 서비스를 제공한다. 그 중 인터넷 뱅킹은 2003 년 중반부터 4 개 은행(한미은행, 우리은행, 조흥은행, 농협)에서 서비스를 제공한다. 그러나 PC 와 마찬가지로 OS 의 제약을 두고 있어 Windows CE, Palm 을 OS 로 하는 단말기에서만 서비스를 제공하고 있는 실정이다. 하지만 더 많은 사용자들이 무선 인터넷의 편리한 기능을 제공 받기 위해서는 현재 고가로 제공되는 무선 단말기의 가격의 인하와, 디바이스의 적은 용량의 배터리, 작은 크기의 화면, 낮은 성능의 CPU, 적은 메모리 등의 디바이스 환경에서의 제약이 있다. 단말기의 성능저하 없는 가격인하를 위해서는 하드웨어의 가격보다는 소프트웨어의 가격 하락을 이용하는 방안이 제시되고 현재 국·내외 에서는 OS 를 Linux 로 이용하여 성능저하 없는 저가의 단말기를 제공하고 있다.

본 연구에서는 기존의 WPKI 이용 Linux 를 OS 로 하는 단말기에서 무선 인터넷 뱅킹이 가능한 무선 PKI(Public Key Infrastructure) 인증 기술을 구현하는데 목적이 있다.

본 논문의 구성은 다음과 같다. 2 장에서는 무선 PKI 의 기반이 되는 무선 인터넷 기술과 무선 PKI 기술에 대해서 알아본다. 3 장에서는 리눅스 환경에서의 무선 PKI 인증방안에 대해서 알아본다. 4 장에서는 리눅스 환경에서의 무선 PKI 인증 구현에 대해서 알아본다. 5 장에서는 결론 및 향후 연구 계획에 대해 언급한다.

2. 관련 연구

무선 환경에서 ME(Mobile Explore), WAP(Wireless Application Protocol), i-mode 가 있는데, WAP 은 WAP forum 에서 개발을 하여 주로 모바일 단말기에서 사용

본 연구는 한국과학재단 지정 동북아전자물류 연구센터의 지원에 의한 것입니다.

되고, ME 는 MS(Microsoft)의 무선 인터넷을 위한 브라우저에서 사용되고 TCP/IP 를 이용한다. i-mode 는 일본의 NTT 에서 개발하여 c-HTML 을 사용한다.

유선과 마찬가지로 무선 인터넷의 안정한 서비스를 제공 받기 위해서는 기밀성 (confidentiality), 무결성 (integrity), 인증 (authentication), 부인방지와 같은 서비스를 제공하기 위한 무선 PKI 가 필요하다.

무선 PKI 란 기존의 유선 PKI 를 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 PKI 도 PKI 와 같이 키 · 인증서 방식을 이용한 무선 네트워크 전자 상거래의 활성화를 위해 제안된 기반 구조이다. 기본적으로 무선 환경에서 WTLS(Wireless Transfer Layer Security)와 WMLScript(Wireless Markup Language Script) Crypto Library 에서 제공하는 signText() 함수를 이용하여 단대단 보안을 보장한다.

2.1 무선 인터넷 기술

1) WAP

WAP 방식은 공개된 표준으로, 전세계적으로 많이 사용한다. 그러나 기존의 HTTP 를 지원하지 않으며, 유 · 무선 구간의 연결을 위한 별도의 WAP 게이트웨이를 필요로 하기 때문에 ME 방식에 비해 비용이 많이 든다는 단점이 있다. 반면에 기존 기술과의 호환성을 제공하고, 어플리케이션의 개발이 가능하기 때문에 다른 방식에 비하여 많은 유연성을 가지고 있는 서비스와 차별화된 서비스를 개발하기에 유리하다는 장점을 가지고 있다. 또한 게이트웨이 내에서 WAP 와 HTTP 간의 변화 과정에서 발생하는 원문의 노출문제는 Cryto.signText()를 이용하여 해결하고 있다.

2) ME

ME 방식에서는 WAP 게이트웨이가 수행하는 작업을 무선 단말기 내의 브라우저가 수행하며, 일반 인터넷 표준인 HTTP 방식과 호환된다. 또한, HTML 을 축약한 m-HTML(micro Hypertext Markup Language)을 컨텐츠 기술 언어로 사용하기 때문에 이동통신사업자에게는 투자비를 절감할 수 있도록 해주고, 기존의 HTML 컨텐츠를 그대로 이용할 수 있다는 점에서 컨텐츠 제공자에게는 편의를 제공한다. ME 에서의 보안 메커니즘은 HTTP 에 기반하고 있으므로 유선 인터넷에서 사용되고 있는 SSL(Secure Sockets Layer) 정보보호 메커니즘의 수용이 가능하다. 또한, ME 는 운영체제의 종류에 상관없이 사용 가능한 브라우저를 제공하는 장점이 있다. 반면 브라우저의 오버헤드가 크며, 브라우저에서 지원하지 않는 파일을 이용한 서비스를 제공하지 못하는 단점을 갖는다.

2.2 무선 PKI 기술

무선 PKI 는 기존의 유선 PKI 의 구성요소를 그대로 이용하지만, 무선 환경의 여러 제약 조건을 고려하여 기능을 최소화 하였다. 유선 PKI 에서 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.

1) 무선 PKI 구조

무선 PKI 를 구조로는 사용자의 정보를 받아 인증서 등록 및 사용자 신원 확인을 대행하는 등록기관(RA : Registration Authority), 인증서를 발행하고 효력정지 및 폐지 기능을 수행하는 인증기관(CA : Certification Authority), 인증서 폐지 목록을 저장하는 디렉터리(Directory), 그리고 인증서를 신청하고 사용하는 사용자(EE : End Entity)가 있다. [그림 1]은 기본적인 무선 PKI 의 구조이다.

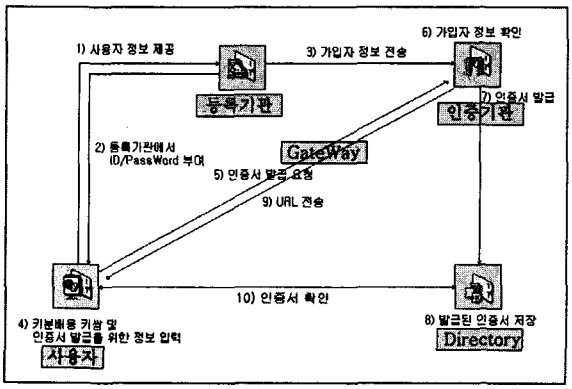

그림 1 무선 PKI 의 구조

2) 무선 PKI 모델

무선 PKI 에서는 단말기의 여러 제약 조건을 고려하여 무선용 X. 509 인증서 WTLS 인증서 또는 갱생주기가 24~48 시간인 Short-lived 인증서를 사용하며, 인증서를 발행 받을 경우 인증서의 URL 만을 이용하기도 한다.

서명 알고리즘으로는 RSA(Rivest Shamir Adleman) 알고리즘 수준을 갖는 ECDSA(Elliptic Curve Digital Signature Algorith) 사용하며, 암호화 알고리즘으로는 RC4, RC5, SEED 중 SEED 를 사용하며, 해쉬 알고리즘으로는 MD5, SHA-1 중 SH-1 을 사용한다.

2.3 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 Directory 에 인증서를 저장

해 두었다가 사용자의 요청 시에 이를 이용하여 인증서를 확인하고 서비스를 제공하는 방식이다.

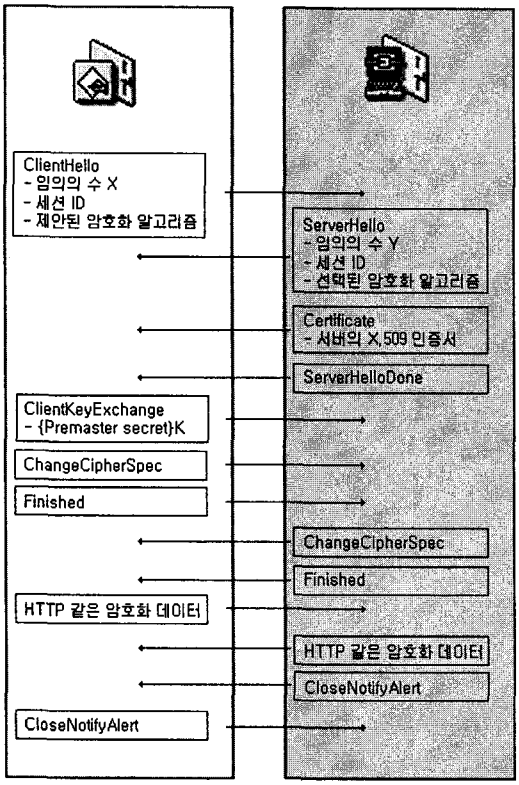

그림 2 서버 인증서만 보유하는 SSL

유선 인터넷 뱅킹을 이용 할 때 서버에 접속하는 사용자는 Xecure Client 라는 프로그램이 설치가 되어 웹 페이지에서 작업하는 내용에 대하여 보안 작업을 한다. Xecure Client 는 ActiveX 와 SSL 인증 방식을 이용한다. SSL 은 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 개인 키를 가지는 경우, SSL 은 클라이언트가 서버를 인증하고, 클라이언트와 서버 모두가 알고 있는 비밀 키를 안전하게 만들어 내는 데 사용 될 수 있다.

3. 리눅스 환경에서의 WPKI 인증방안

Linux 상에서 Xecure Client 프로그램을 구현하기 위해서는 기존 윈도우에서 사용하는 AcriveX 기술과 Internet Explore 에서 기본 제공하는 SSL 기술을 제공할 수 없으므로 자체적으로 제작을 해 주어야 한다. ActiveX 는 자체적인 업데이트 기능을 제공하기 위한 방안이므로 여기서는 구현하지 않겠다.

리눅스에서 운영체제로 하는 단말기의 특성은 Window CE 나 Palm 을 운영체제로 하는 기기와는 달리 기본적으로 지원하는 브라우저가 없다는 사실이다.

Linux 에서의 구현을 위하여 BSD 소켓 인터페이스(Interface)를 이용한다. BSD 소켓 인터페이스는 다양한 형태의 네트워킹뿐만 아니라 프로세스간 통신도 지원하는 일반적인 인터페이스이다. 소켓통신은 통신 연결의 한쪽 끝으로 생각할 수 있는데, 통신하고 있는 두 프로세스는 통신연결에서 자신 쪽 끝에 해당하는 소켓을 가지고 된다. 소켓을 특별한 종류의 파이프로 생각할 수도 있지만, 파이프와는 달리 소켓은 거기에 담을 수 있는 데이터의 양에 제한이 없다.

4. 리눅스 환경에서의 WPKI 인증 구현

4.1 구현환경

무선 PKI 에서는 인증서 요청 시 사용자 인증을 위해 사용자 아이디와 패스워드를 사용한다. 이때 아이디와 패스워드는 제안된 알고리즘에 의해 암호화 되어 해당 공개 키를 가진 무선 PKI 포탈에 전송해야 하며, POP(Proof Of Posessesion)을 수행하여야 한다. POP 는 인증서 요청 시, 인증서에 포함되는 공개 키에 해당하는 비밀 키를 알고 있다는 것을 무선 PKI 포탈에 증명하는 과정으로서, 인증서 요청 프로토콜 그리고 인증서에 따라 여러 방법이 사용되고 있다.

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

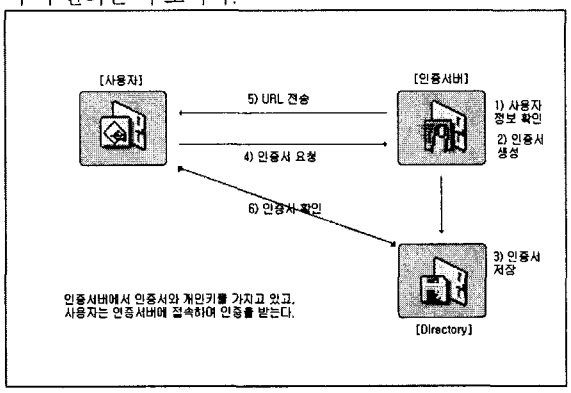

그림 3 구현 구조

무선 액세스 접근을 위한 방식으로는 802.11 의 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 분배

하여 둔다. [9]

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

사용자가 URL 을 이용하여 접속하기 위한 클라이언트 프로그램을 실행하고 작성된 개인 정보는 SSL 을 이용한 SEED 암호화 알고리즘과 공개 키를 이용하여 암호화를 하고 서버에 전송해 준다. 전송 받은 서버는 미리 저장되어 있는 비밀키를 이용하여 암호화된 내용을 풀고 인증서와 대조하여 인증결과를 사용자에게 전송하여 준다.

5. 결론

본 논문에서는 리눅스를 OS 로 하는 단말기에서의 무선 PKI 인증 방안에 대하여 구현하였다. 현재 제공되고 있는 여러 가지 기능을 모두 수렴하기에는 리눅스라는 운영체제의 특성상 호환성이 부족한 것이 사실이다.

윈도우 환경에서의 구현과는 다르게 인터넷 익스플러로의 도움 없이 서버에 접근하여야 하는 문제 때문에, BSD 소켓 인터페이스를 이용한 소켓 프로그래밍을 이용하여 서버에 접속하는 클라이언트 프로그램을 제작하였으며, 서버에 접근하는 방법으로는 URL 을 이용한 접근 방법을 사용하였다. URL 을 통하여 접속하는 ID 와 패스워드를 공개키를 이용한 암호화 기법에 의해 암호화된 내용을 서버에 전송하며, 서버에서는 비밀키를 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. 어려운 커널을 알아야 하고 비쥬얼적이 프로그램이 없다는 것이다.

그러나 윈도우 환경보다 뛰어난 리눅스의 보안 기법을 활용하고, 저가 단말기의 보급과 윈도우 환경의 속박에서 벗어나기 위해서는 지속적인 발전을 하여야 한다.

향후에, 리눅스용 브라우저가 개발된다면 더욱 보안사항이 이루어진 인증기법의 구현이 가능하다고 본다.

참고문헌

[1] 정영석, 김수진, 서인석, 서상원, 원동호, "무선 PKI 기술 및 서비스 동향에 관한 연구", pp. 1-4, 2002.11

[2] 정철현, "PKI 전자성명과 인증제고", pp. 53-69, 2003.01

[3] 제 1 회 전자서명 인증 워크샵, 정보통신부 정보기획과, 전성배, "무선 PKI 정책 방향", 2000.08

[4] 배민희, 정소영, 최은조, 최지현, "WPKI (Wireless Public Key Infrastructure)"

[5] 이현주, 최문석, "RSA 서명 기법을 이용한 무선 전자상거래", 한국정보처리학회, 2002.11

[6] 이호웅, 김기창, "Hash chain 을 이용한 선불방식의 소액 전자지불 시스템의 설계", 2000

[7]http://www.linuxkorea.co.kr/main/solution/network/dynaradius.html

[8]http://ko.gotdotnet.com/quickstart/winforms/doc/WinFormsAxHosting.aspx

[9] Mattbew S.Gast, "802.11 Wireless Networks", pp. 185-190, 339-376, April 2002.