무선인터넷 종단간 보안을 위한 인증시스템에 관한 연구

김정태, 이현우, 현창희
{acroo, lhwoo, chhyun}@etri.re.kr
한국전자통신연구원

요약

유선인터넷 환경에서는 SSL 또는 PKI 기반의 인증시스템이 널리 사용되며 전자상거래가 활성화 되어 있는 것에 반해, 무선인터넷 환경에서는 무선인터넷의 활성화가 상대적으로 뒤쳐짐에 따라 특정한 기술이 주도적으로 선도하고 있지 못하다. 2004년 말로 예정된 무선인터넷 공인인증서비스가 시작되면 이러한 무선인터넷에서의 종단간 보안을 위한 인증시스템에 대한 요구가 증가할 것으로 보인다. 따라서, 무선인터넷 환경에서 활용될 수 있는 다양한 인증시스템의 장단점을 분석하는 것은 향후 국내 인증시스템 도입에서 참고가 될 수 있을 것이다.

I. 서론

최근 휴대폰, PDA 등의 무선단말을 이용한 무선인터넷 사용이 증가하면서, 무선인터넷 은행거래, 무선인터넷 증권거래와 같은 무선인터넷을 통한 전자상거래가 확산되고 있다. 기업들도 기존의 유선 정보화 시스템에 무선시스템으로 추가하거나, 전체 시스템을 무선화하는 경향이 나타나고 있다. 이러한 무선인터넷 사용자 서비스는 점진적으로 다양해질 것으로 예상되며, 무선인터넷에서 구현하고자 하는 서비스의 수준이 유선인터넷의 수준으로 높아지기 위해서는 무선환경에서의 보안이 필수적인 사항이 될 것이다. 이를 위해서는 현재 유선인터넷에서 널리 사용되고 있는 PKI 기술의 핵심인 비밀성, 무결성 및 신원 확인과 부인 방지 같은 서비스를 무선 환경에서 구현되어야 한다.

그러나 기존의 유선인터넷 환경에서 사용해온 보안 솔루션을 가져가 무선환경에 적용하는 것은 여러 가지 기술적 한계가 있으며, 이러한 한계를 극복하기 위해서는 고려하여야만 하는 사항들이 많다. 일반적으로 무선단말은 널리 사용되고 있는 유선인터넷 환경에서의 개인용컴퓨터에 비해 좁은 대역폭, 낮은 디스플레이 해상도, 입력장치의 불편함 등의 약점이 있다. 이러한 약점들은 향후 지속적인 기술 개발로 인해 어느 정도 개설되는 것이 가능하리라 보인다. 그러나, 현 상황에서의 약점이 존재한다는 점과, 향후에도 유선인터넷 환경과의 격차는 일정부분 존재할 수 밖에 없다는 점은 과제로 남아 있을 것이다.

또한 무선인터넷 환경은 일반적으로 유선인터넷 환경과 혼재하여 네트워크가 구성되는 경우가 대부분이다. 전자상거래 지불결재의 경우, 이용자와 쇼핑몰간의 직접적인 통신이 이루어지는 것이 아닌, 지불결재에 필요한 금융권, 네트워크 업체 등의 다양한 요소들에 트랜잭

션이 이루어지게 된다. 따라서 특정 구간 만을 위한 보안 기술로는 각 요소들의 신뢰성을 보장하는 것은 어렵기 때문에, 종단간 보안의 필요성은 더욱 중요해진다. 본 고에서는 이러한 종단간 보안을 위한 인증시스템의 구현 방법들에 대해 살펴보고 각 방법이 지닌 장단점을 통해 국내 환경에 적합한 방안을 찾아보고자 한다.

II. 종단간 무선인터넷 보안시장의 현황 및 전망

1. 시장현황

유선인터넷 환경에서는 SSL(Secure Socket Layer) 또는 TLS(Transport Layer Security) 방식에서 PKI 방식으로 전환이 상당부분 이루어진 상황이다. 전자상거래 지불결제에서 SSL 방식은 이용자와 쇼핑몰간의 지불결제 정보만 암호화하는 데 비해, PKI 방식은 이용자와 쇼핑몰, 지불결제대행서비스(PG, Payment 게이트웨이) 회사, 부가가치통신(VAN, Value Added Network) 회사 등의 중간과정은 제외하고 카드사만이 신용카드 정보를 인지함으로써 종단간 보안을 구현하여 보다 강력한 안정성을 확보할 수 있게 되었다. 현재 인터넷 복권, 인터넷 뱅킹 등에서는 PKI 방식으로 많이 바뀌어 가고 있지만 아직도 많은 쇼핑몰에서는 SSL 방식이 사용되고 있다.

무선인터넷 환경에서는 2002년에 국내에서 WPKI 기술 표준이 제정된 이후, 여러 상용 솔루션이 개발되어오고 있다. 이를 바탕으로 한 무선인터넷 공인인증서비스가 2004년 하반기에 실시될 여정으로 있으며, 무선인터넷 공인인증서비스가 본격화된 다면 관련 수요의 급속한 증가가 뒤따를 것으로 예상되고 있다. 응용계층에서의 보안으로는 주로 무선 결제 단말, 무선 의료정보사업 등과 같은 범용이 아닌 특정 서비스 영역에 한정되어 주로 사용되고 있다.

2. 시장전망

유선인터넷환경은 현재 계속 PKI 방식으로 전환되어 가고 있으며, 무선인터넷환경은 2002년의 WPKI 표준의 완성 이후, 종단간 보안시장에서 그 수요가 급속히 증가할 것으로 예상되고 있다. 2002년 말, 상용서비스가 시작된 WIPI 플랫폼은 여러 가지 문제로 인해 상용화가 늦어져 단말기 출시가 연기되었다. 2003년 하반기에 문제들이 해소됨에 따라서, 국내 이동통신 산업의 표준 플랫폼으로 채택된 WIPI의 보급은 점차 증가할 것으로 보인다[1] 이로 인해 무선인터넷에서의 종단간 보안에 대한 요구도 급증할 것으로 전망된다. 무선인터넷에서 종단간 보안이 주로 요구되고 있거나, 향후 확장해나갈 것으로 전망되는 분야를 살펴보면 다음과 같다.

- 무선인터넷 보험/증권/뱅킹 등 금융분야
- 무선인터넷 전자지불/인터넷 복권 등 응용 서비스 분야
- CAS(수신 제한 시스템) 등 디지털 방송분야

그 밖의 PKI에 강력한 인증을 위해 생체인식 등의 접목이 고려되고 있다. 응용계층에서의 보안은 필요한 부분만을 암호화하여 성능과 크기가 무선단말에 유리해 다음의 분야에서 주로 그 수요가 점차 증가할 것으로 기대된다.

- 구매전용카드를 위한 무선 결제 단말
- 무선 의료정보사업 등

III. 무선 종단간 보안

1. 무선단말과 웹 서버간의 종단간 보안기술

앞에서 언급한 바와 같이 무선인터넷 환경의 경우 네트워크 단계에서의 문제(낮은 대역폭, 시간지연, 연결의 불안전성 등) 및 단말 단계에서의 문제(낮은 연산능력의 중앙처리장치, 적은 메모리, 배터리시간, 작은 디스플레이, 입력장치 등)로 인해 유선인터넷 환경과는 차이가 존재할 수 밖에 없다. 이러한 무선단말과 웹 서버간의 종단간 보안을 위한 기술로 현재 표준화되거나 주로 사용되고 있는 기술에 대해 살펴본다. 또한, 이에 앞서 용어에 대한 정확한 정의의 범위를 설정하는 것이 필요할 것이다.

인증시스템이란, 실체가 드러나지 않는 사이버 공간에서 공인된 인증기관이 사용자에게 법적 효력이 있는 전자인증서를 제공함으로써 비인가로부터 개인의 프라이버시 정보와 인터넷상에서 유통되는 지불 정보의 위조 및 변조를 방지하는 중요한 수단을 말한다. 또한, 종단간 보안이란, 서비스를 제공하는 서비스 제공자로부터 그 서비스를 수용하는 소비자의 단말이기에 이르기까지 모든 과정에서 정보가 변경되거나 훼손되지 않고 안전하게 전송되는 것이다.

전송계층보안은 WTLS처럼 전송계층에서의 종단간 보안을 보장하기 위해 웹 서버에 보안 프록시 서버를 두어 안전한 도메인을 포함하는 새로운 구조를 구성하는 것이며, 응용계층보안은 응용계층에서 WMLScript 등을 이용해 전송되는 메시지의 일부분에 정보보호 서비스를 제공할 수 있도록 하는 것이다. 본 고에서는 전송계층보안과 응용계층보안의 두 계층에서의 보안기술에 대해서 검토하고자 한다.

	전송계층보안 (SSL/TLS/WTLS)	응용계층보안 (ECDH/SEED)
계층	HTTP와 TCP 사이	응용 계층
기능	기밀성, 무결성, 사용자 인증	비밀성
암호화	모든 데이터	선택된 데이터
부하	큼	작음
크기	중량 (200~300kByte)	경량 (40~60kByte)

성능	보통	빠름 (ECC의 고속 키 생성)
결론	모든 데이터를 암호화 인터넷 표준 프로토콜에 대한 호환성 확보 목적	필요한 부분만을 암호화 성능과 크기상 무선기기에 유리

<표 1> 종단간 보안 기법간의 비교

2. 무선 종단간 보안상의 문제점

WTLS 기술을 사용하는 구간에서는 기밀성, 무결성, 사용자 인증의 보안 문제를 해결할 수 있으나, 무선 단말과 유선 인터넷의 웹 서버가 통신을 위해서는 WAP 게이트웨이에서 WTLS와 SSL 간 상호 프로토콜 변환이 이루어지는데 여기에서 데이터의 원본이 노출되는 보안의 문제가 발생하게 된다. WAP 게이트웨이와 웹 서버의 통합, 응용 계층의 비표준 보안 방식 적용 등을 통해서 해결이 가능하다. 국내에서는 WAP 방식의 WTLS를 사용한 보안 제품을 사용하기 보다는 응용계층에서 데이터 부분만 암호화하여 이를 전송하는 비 표준 방식으로 종단간 보안을 제공하고 있는 실정이다.

IV. 무선 종단간 보안 문제의 해결방안

1. SSL을 이용한 방법

이 방법은 유무선 전구간에서 SSL 기술을 이용해 정보보호 서비스를 제공하는 방법이다. SSL을 이용할 경우, 게이트웨이는 무선 네트워크 구간과 유선 네트워크 구간의 중계 역할만을 담당하며, 무선단말과 웹 서버의 통신에 개입하지 않기 때문에 무선단말과 웹서버 간의 종단간 보안이 가능하게 되는 것이다. 현재 SSL이 가장 범용적으로 사용되고 있기 때문에, 정보보호서비스를 위해 특별한 수정이 요구하지 않기 때문에 기존에 구축돼 있는 시스템을 그대로 사용할 수 있다는 장점이 있다.

이와 같은 서비스를 제공하려면 무선단말에서 SSL의 처리가 가능해야 한다는 단점이 존재한다. 그러나, 현재 무선단말의 CPU나 메모리 용량으로는 일반 개인용컴퓨터에서와 같이 사용자가 불편하다고 느끼지 않을 정도의 빠른 속도로 SSL을 처리하는 것이 불가능하다는 약점이 존재한다.

2. 응용 프로그램 이용하는 방법

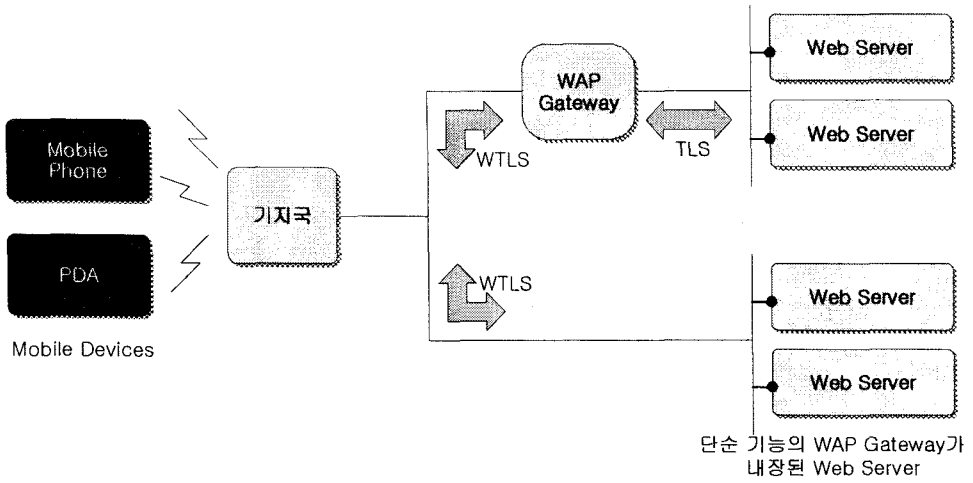
이 방법은 정보보호 서비스와 관련된 모든 작업을 응용 프로그램의 레벨에서 처리하는 방법이다. 무선단말과 웹 서버는 정보보호 서비스를 위한 전용 프로그램을 설치하고 이를 통해 통신함으로써 종단간 보안 서비스를 제공 받을 수 있다. 즉 WAP 게이트웨이는 단순히 무선 네트워크 구간과 유선 네트워크 구간 사이의 중계 역할만을 수행해 통신 내용을 알지 못하므로 안전성이 높다.

SSL을 이용한 방법과 마찬가지로, 이 방법 역시 무선단말의 성능이 문제가 될 수 있다. 그러나, 기존 표준 규격을 따르는 것이 아니고, 새로운 프로그램을 개발하여 보안기능을 수행하는 것이기 때문에 무선단말에 최적화된 프로그램의 개발에 대한 여지가 많으며, 응용분야에 적합하게 프로그램의 수정이 가능하다는 장점이 있다.

3. WAP 게이트웨이를 거치지 않는 방법

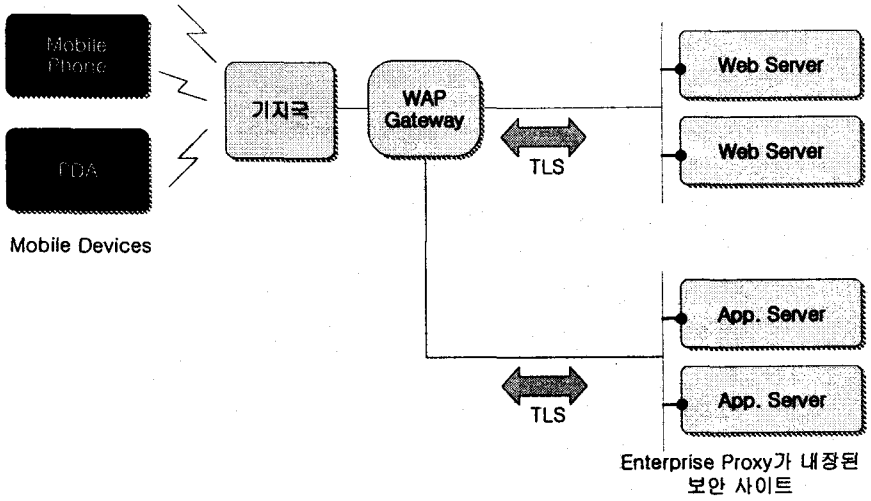
이 방법은 무선단말에서 은행이나 증권사 같은 보안에 대한 요구가 많은 사이트를 접속할 경우에 WAP 게이트웨이의 IP 주소 대신에 보안이 확보된 사이트의 웹 서버 IP 주소를 직접 입력하여 접속하는 방법이다. 이 경우, WAP 게이트웨이를 거치지 않기 때문에, 각 웹 서버는 전송된 데이터를 변화하여 처리할 수 있는 단순 기능의 WAP 게이트웨이를 내장하고 있게 된다.

이 방식의 최대 단점은 사용자가 보안 사이트를 접속하고자 할 경우에는 항상 IP 주소를 바꾸어 입력해야 하기 때문에 사용하기 어렵고 불편하다는 점이다. 그리고 현재 국내 대부분의 무선 단말에서는 사용자가 WAP 게이트웨이의 IP 주소를 직접 입력하지 못하고 고정되어 있어 이러한 방법을 사용하기 위해서는 무선단말의 수정이 필요하다는 약점이 있다.



<그림 1> WAP 게이트웨이를 거치지 않는 방법

4. 보안 데이터에 대한 Bypass기능을 이용하는 방법

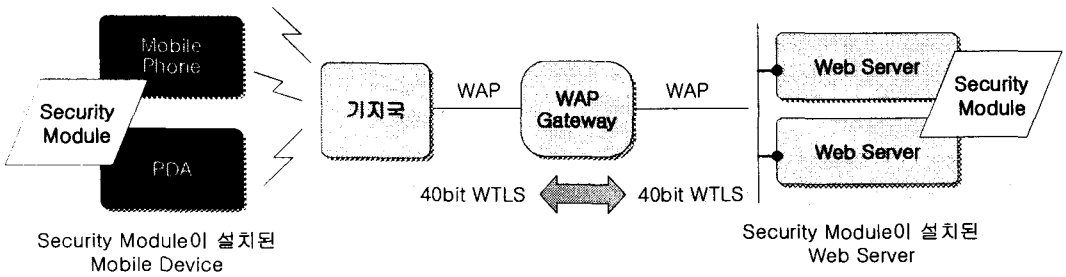


<그림 2> 보안 데이터에 대한 Bypass기능을 이용하는 방법

이 방법은 보안이 요구되는 사이트에 대한 데이터일 경우에 WAP 게이트웨이 단계에서 이 데이터를 Bypass 하는 방법이다. 각 보안 사이트의 어플리케이션 서버 앞에는 Enterprise Proxy 서버가 위치하여 Bypass 된 데이터를 처리하는 역할을 담당하도록 구성되어야 한다.

이러한 방법을 사용할 경우 사용자들의 무선단말에 수정을 가하지 않고도 완벽하게 종단간 보안을 지원할 수 있는 장점이 있으나, WAP 게이트웨이에 연결된 보안 사이트마다 설치해야 하는 Enterprise Proxy Server의 비용이 문제가 될 수 있다. 현재 이와 같은 방법으로 Openwave社를 비롯한 많은 WAP 게이트웨이 개발업체들이 무선 인터넷의 보안 문제를 해결하는 솔루션을 제시한 바 있다.

5. 특정한 데이터 Type을 이용하는 방법



<그림 3> 특정한 데이터 Type을 이용하는 방법

이 방법에서는 무선 인터넷 사이트를 일반 사이트와 보안이 요구되는 사이트로 구분하지 않는다. 단, 일반 사이트와는 달리 보안 사이트에서는 암호화하고자 하는 데이터를 단말과

미리 약속된 방법으로 암호화하고 전송하게 된다. 무선단말과 보안 사이트 간의 미리 약속된 방법을 사용하는 예로 MIME Type을 이용한 방법이 있다. 무선단말에는 특정 MIME Type을 처리할 수 있는 보안 모듈이 내장되며 웹서버에서도 동일한 기능을 가지는 모듈을 이용하여 종단간 보안 문제를 해결할 수 있다.

보안 모듈을 얼마나 무선단말에 적합하게 개발하느냐가 이 방법의 중요한 부분이다. 이 방법 역시 무선단말의 성능이 제약조건으로서 작용하기 때문에, 무선단말에 최적화된 프로그램의 개발이 필수적이며, 무선단말과 보안 사이트간의 약속을 적절히 규격화하여야만 안정적인 보안을 유지할 수 있을 것이다.

V. 결론

2002년, 국내에서 WPKI 기술 표준이 제정된 이후 급속히 무선인터넷의 활용도가 증가하리라는 전망이 많았다. 그러나 그러한 전망과는 달리 주류구매 전용카드, 담배구매 전용카드, 양곡구매 전용카드 등 일부 분야에서 활용되고 있는 것 외에는, 아직 무선인터넷에서의 전자거래의 규모가 그다지 크지 않은 상황이다. 이는, 올해 하반기로 예정되어 있는 무선인터넷 공인인증서비스가 본격화되는 시점부터, 다양한 분야에서 무선인터넷을 도입하려는 움직임이 본격화 될 것으로 예상된다.

현재 무선인터넷 공인인증서비스가 시작되지 않은 상황에서 특정한 종단간 보안 기술이 우세하다고 볼 수는 없다. 각 기술 모두가 무선단말이나 서버, 또는 WAP 게이트웨이 단계에서의 수정이 불가피하기 때문에, 인증서비스가 활성화에 따라 국내 무선통신업체들과 관련 업체들이 어떠한 적절한 합의점을 마련하느냐가 중요하다. 기술적으로 충분한 보안을 제공하고, 경제적으로 효율적인 방안을 도출하기 위해서는 각 주체들의 긴밀한 협조가 요구된다. 또한 정부는 세계 최초로 WPKI 기술 표준을 제정한 성과를 지속시키기 위해서라도 다양한 방면에서의 협조와 지원이 있어야 할 것이다.

참고문헌

[1] 김상태, 김한주, "무선인터넷 서비스 시장현황 및 전망," 주간기술동향, 2003

[2] IDC, "Mobile Internet Survey: An End-User Perspective," 2003

[3] IDC, "Asia/Pacific Wireless Internet Trends," 2004

[4] Frier, A., Karlton, P., Kocher, P., "The SSL3.0 Protocol Version 3.0," see http://home.netscape.com/eng/ssl3/

[5] Dierks, T., Allen, C., "The TLS Protocol Version 1.0," see http://www.ietf.org/rfc/rfc2246.txt

[6] Wagner, D. and Schneier, B., "Analysis of the SSL 3.0 protocol," 2nd USEN IX Workshop on Electronic Commerce, 1996

[7] Murray, E., "SSL Server Security Survey,"

see http://www.lne.com/ericm/papers/sslserverstats.html
[8] WAP Forum, "Wireless Transport Layer Security Specification,"
see http://www.wapforum.org/what/technical.htm
[9] Cobb, S., "Dealing with WAP-gap security risks,"
see http://www.serverworldmagazine.com/sunserver/2001/01/wapgap.shtml
[11] Miranzadeh, T., "Understanding Security on the Wireless Internet",
see http://www.bitpipe.com/data/detail?id=974317351_760&type=RES