제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003.5)

모바일 시스템의 인증을 위한 표준 플랫폼 제안

김태연*, 임승채*, 정채영**

*조선대학교 대학원 전산통계학과
e-mail: deer38317@hotmail.com

Standard platform suggestion for authentication of mobile system

Tae-Yeun Kim*, Sung-Chea Lim*, Chai-Yeoung Jung**

*Dept. of Computer Science and Statistics, Graduate School, Chosun Univ.
**Dept. of Computer Science and Statistics, Chosun Univ.

요약

IMT-2000 상용화를 눈앞에 둔 시점에서 다양한 모바일 서비스들이 성장세를 보임에 따라 무선 인터넷 환경에서의 보안 문제가 큰 이슈로 대두되고 있다. 본 논문에서는 무선 인터넷상의 Data 전송에 쓰이는 보안 솔루션(WAP, ME, I-Mode)을 비교·분석하며, End-To-End Security 문제를 해결할 수 있는 플랫폼을 제시한다. 제안된 모바일 인증 플랫폼은 표준화된 암호화 패킷을 사용함으로써 보다 높은 보안 수준을 제공하고 기존의 WAP의 WAP Gateway에서의 평문의 내용 유출을 막음으로서, 안전한 모바일 환경을 제공할 수 있는 가능성을 제시한다.

1 서론

WWW(World Wide Web) 서비스로 대변이 되는 유선 인터넷 환경이 Handset(휴대폰, PDA등)의 급속한 성장함 따라 무선 컨텐츠로 이식되어 무선인터넷 시장이 활성화되고 있다. 이에 따라 향후 IMT-2000 서비스가 도입되면 더욱더 무선인터넷 시장으로의 전환이 가속화 될 전망이다.[1]

현재 무선인터넷 시장을 형성하고 있는 솔루션으로는 WAP포럼의 WAP과 MS의 Stinger 프로젝트 그리고 현재 상용화되어 일본에서 많이 쓰이는 NTT DoCoMo의 I-Mode가 대표적이라 할 수 있다.[2] WAP포럼의 WAP의 경우, 무선통신환경 부분에서 고효율의 이용이 가능하며, MS의 ME(Mobile Explorer)는 기존의 HTML을 베이스로 사용하여 손쉽게 풍부하고 다양한 컨텐츠를 제작할 수 있다. I-Mode의 경우, 기존 음성전화를 이용하여 다양한 서비스를 제공한다.

위의 각 솔루션들의 보안적 측면을 살펴보면, WAP은 WapGateway에서 Data가 노출될 가능성을 가지고 있으며, ME의 경우는 유선의 SSL기술을 사용함으로써, 무선환경에 적합하지 않다. I-Mode의 경우 I-Mode Center와 무선단말기간의 전송계층의 보안이 이루어지지 않는 단점을 지니고 있다.

본 논문에서는 각 솔루션들의 보안기술의 개요 및 장단점을 비교·분석하여, 효율적인 종단간 보안 프로토콜(End-To-End Security Protocol)방식을 제안하고자 한다.

본 논문의 구성은 2장에서 무선인터넷 전용 프로토콜의 보안 요건을 살펴보고, 3장에서는 솔루션별 특징 및 장단점을 비교하며, 4장에서 제안하고자 하는 보안 플랫폼을 제시하여, 무선 어플리케이션 상의 종단간 보안의 구성 방안을 살펴본다. 마지막으로 5장에서 결론을 맺는다.

2. 무선인터넷 전용 보안 프로토콜

무선인터넷 통신기반은 유선과 달리 제한된 대역폭과 이동통신사업자의 종속적인 성향을 지니고 있다. 따라서 유선인터넷 환경과는 다른 통신 프로토콜을 사용해야 한다.

무선인터넷 전용 프로토콜은 다음과 같은 보안요건을 갖추어야 한다.**[3][4]**

① 데이터그램의 지원

TLS/SSL은 기본적으로 TCP 세션을 전제로 설계되어 있다. 하지만, 무선인터넷은 WDP(또는 UDP)라는 데이터그램을 기반으로 하고 있기 때문에 데이터그램을 지원할 수 있어야 한다.

② 느린 응답 속도

단말기와 서버 사이에서 데이터가 전송될 때 유선에 비하여 무선은 시간이 많이 걸릴 수 있다. 10초 이상의 시간이 소요될 수 있기 때문에 이러한 상황에 맞추어 프로토콜을 튜닝하여야 한다.

③ 낮은 전송률

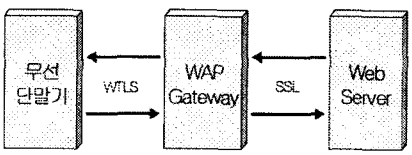
아직은 무선인터넷의 대역폭이 크지 않으므로 많은 양의 데이터를 주고받는 형태로 설계되어서는 안 된다.

④ 낮은 처리 속도와 적은 메모리

단말기에 내장된 마이크로프로세서와 메모리는 처리속도와 용량 면에서 개인용 컴퓨터에 비해 충분치 않으므로 복잡하거나 많은 메모리를 차지하는 알고리즘이나 다양한 알고리즘 지원이 어렵다.

3. 솔루션별 비교

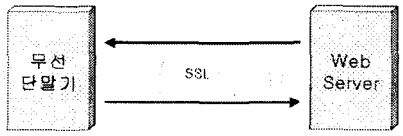
3.1 WAP(Wireless Application Protocol)



[그림 2] WAP의 보안(WTLS)

WAP의 보안(WTLS)은 [그림 2]와 같이 Web 혹은 컨텐츠 Server와 WAP Gateway사이에 유선인터넷상에 사용되는 SSL이나 새로운 버전인 TLS를 사용하여 보안되어지며 WAP Gateway와 사용자의 무선단말기와는 WTLS를 사용하여 기밀성, 무결성, 사용자 인증을 하는 모델을 제시하고 있다.**[7]**

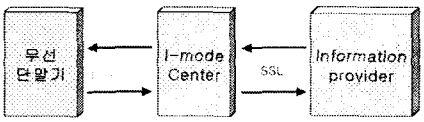
3.2 Stinger Project



[그림 4] ME(Mobile Explorer)의 보안

WAP에서는 보안을 위해 WTSL등을 사용하지만 MME에서는 SSL이 포함되어 있지 않으므로 무선인터넷 뱅킹 등의 서비스를 하기 위해서는 별도의 보안 레이어를 구성해야 한다. 국내에서는 SSL솔루션을 채택하여 유선망의 SSL과 바로 보안통신이 가능하다.

3.3 I-Mode



[그림 6] I-Mode의 보안

I-Mode도 MME(Microsoft Mobile Explorer)와 마찬가지로 유선인터넷의 보안방식인 SSL을 사용한다. 그러나 I-Mode는 DoCoMo의 I-Mode Center와 가입자의 무선단말기 사이에 전송계층의 보안이 이루어지지 않는다.

3.4 솔루션별 비교 · 분석

	WAP	Stinger	i-Mode
개발주도업체	WAP 포럼(Nokia, Phone.com, Ericsson등)	MicroSoft	NTT Docomo
컨텐츠 기술 언어	WML/WMLScript	m-HTML	C-HTML
전송 프로토콜	WSP/WTP/WDP	HTTP	HTTP
단말기 브라우저	WAP 브라우저	Mobile Explorer	Compact NetFront
보안 메커니즘	WTLS	SSL	SSL

[표 1] 솔루션 별 비교

각 솔루션의 개요와 [표 1]를 살펴보면, 다음과 같은 단점을 도출해 낼 수 있다.**[5]**

① WAP(Wireless Application Protocol)

WAP Gateway내에서 유선망과 무선망의 교환이 이루어진다. SSL의 Decryption와 WTLS의 Encryption가 이루어지는 과정에서 평문의 내용이 이동통신사업자와 WAP Gateway Administrator에게 노출되는 보안상의 허점을 가지게 된다.

② MME(Microsoft Mobile Explorer)

유선인터넷과 무선 단말기를 유선망의 SSL을 이용하여 연결됨으로 무선단말기의 System Resource 낭비가 심하게 일어나 속도의 저하문제가 발생한다. 또한, 유선망과 무선망의 환경의 차이점으로 인한 문제가 발생할 수 있다.

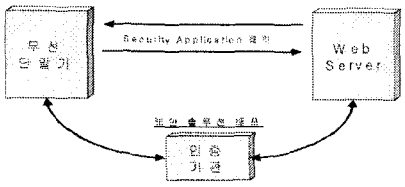
③ I-Mode

단말기 사용자와 I-Mode Center와의 사이에 평문 Data를 전송함으로 보안이 이루어지지 않는다. 또한 WAP에서와 같이 I-Mode Center에서 평문이 노출되는 문제점을 지닌다.

4. 제안된 End-To-End 플랫폼 보안 방식

본 논문에서는 기존의 무선 플랫폼의 End-To-End Security 문제를 해결하기 위한 방안을 제안한다.

기존의 End-To-End Security 문제의 일반적인 해결 방식은 [그림 7]과 같이 Application에서의 보안 레이어를 구성하는 형태를 취한다.[6]



[그림 7] Application 방식의 구성도

이 방식을 살펴보면, 무선 단말기 사용자가 유선망의 Web-Server에 접속하여 필요한 서비스를 이용하고자 할 때 필요한 인증 절차는 다음과 같다.

① 공인된 인증기관(Certification Authority)을 통하여 무선 단말기와 Web-Server에 인증서를 배포한다.

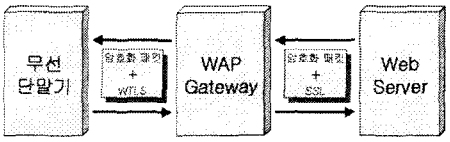
② 인증서의 공개키를 이용하여 Web-Server에서 무선단말기로 암호화 패키지를 전송한다.

③ 전송된 암호화 패키지를 이용하여 무선단말기에서 Web-Server로 로그인한다.

④ 암호화 패킷을 이용한 서비스를 제공받는다.

이 방식은 보안적 측면에서는 안정적이지만, 각 컨텐츠 제공 업체들간의 보안 솔루션의 표준화를 이룰 수 없어 다른 서비스를 제공받고자 할 때 메모리의 제약 및 자원의 낭비가 심해지는 단점을 지니고 있다.

본 논문에서 제안한 방식은 [그림 8]와 같이 모바일 환경의 표준이라 할 수 있는 WAP환경에 기존의 SSL과 WTLS에 표준화된 암호화 패킷을 포함하여 Web Server와 무선 단말기간을 전송하는 방식이다.



[그림 8] 제안된 End-To-End Security 플랫폼

이 방식은 Web-Server에서 암호화 된 패킷을 SSL을 통해 WAP Gateway로 전송하여 복호화 한 후 다시 WTLS로 암호화하여 무선 단말기로 전송한다.

표준화된 암호화 패킷 생성요건은 보안 수준이 높지 않아도 됨으로 빠른 속도와 적은 시스템 리소스를 사용하는 암호화 알고리즘을 사용해야 한다.

이 방식의 전송 알고리즘은 다음과 같다.

① 공인된 인증기관을 통하여 패킷 암호화 알고리즘을 무선 단말기와 Web Server에 배포한다.

② Web Server에서는 배포된 패킷 암호화 알고리즘으로 Data를 암호화한다.

③ 암호화된 패킷을 유선인터넷의 보안 프로토콜인 SSL을 통하여 WAP Gateway로 전송한다.

④ WAP Gateway에서 SSL을 복호화 한 후 WTLS를 통하여 무선단말기로 전송한다.

⑤ 전송된 패킷을 WTLS로 복호화 후 배포된 암호화 알고리즘으로 복호화하여 무선단말기의 출력장치로 출력한다.

반대의 경우도 같은 과정을 거쳐 전송된다.

이 방식은 기존의 WAP에서의 전송방식을 이용하면서 새로운 암호화 알고리즘을 덧붙인 플랫폼을 제시한다.

보안 수준의 질은 SSL과 WTLS에서 보장하고 2번에 걸친 암호화로 WAP Gateway에서의 평문 노출을 차단하고, 암호화 알고리즘의 전제조건인 빠른 암호화 알고리즘을 사용함로써 WAP의 단점을 극복하는 방안을 제시하고자 한다.

5. 결론

본 논문에서는 무선 인터넷상의 안전한 전송을 위한 보안 플랫폼의 방안을 연구하였다. 제안한 플랫폼은 표준화된 암호화와 WAP의 WTLS, 모바일 인증 알고리즘을 사용하여 End-To-End Security 플랫폼을 구성함으로서 모바일 Data의 안전한 전송이 가능하였고, WAP의 단점을 보완할 수 있는 가능성을 제시하였다. 이후 연구 과제로는 구현한 End-To-End Security 플랫폼을 구성할 표준 보안 알고리즘을 구현하고 실제 모바일 환경에 적

용 가능하도록 하는 연구가 수행되어져야 한다고 사료된다.

참고 문헌

[1] 김재홍외, "무선인터넷 기술동향" (주)퓨처시스템 암호체계센터 Technical Report 2000.

[2] 무선인터넷백서편찬위원회, "무선인터넷 백서 2001" 소프트뱅크, 2000.

[3] "무선인터넷 표준화 정책방안" 정보통신정책국, 2001.

[4] 박창섭, "암호이론과 보안" 大英社, 1999

[5] 박남제외, "모바일 서비스 플랫폼 기반의 무선 전자상거래 보안기술" 정보보안학회지 제11권 4호 pp. 9~28, 2001. 8

[6] 조동욱외, "이동통신환경에 적합한 상호인증을 제공하는 키분배 프로토콜의 설계" 통신정보보안학회논문지 제10권 2호 pp. 21~30, 2000. 2

[7] WAP Forum, "http://www.wapforum.org"