WTLS 와 TLS 간의 단대단 보안 모델 : ITLS

권은경*,조용구**,채기준***
계원조형예술대학 정보통신과*
영동대학교 컴퓨터공학과**
이화여자대학교 컴퓨터학과***
e-mail : ekkwon@mercury.kaywon.ac.kr

End-to-End Security Model between WTLS and TLS : ITLS

Eun-kyeong Kwon*,Yong-gu Cho**, Ki-Joon Chae***
Dept of Information Communication, Kaywon School of Art and Design*
Dept of Computer Engineering, Youngdong University**
Dept of Computer Science & Engineering, Ewha Womans University***

요 약

WAP 은 무선환경에서 발견되는 저 대역폭, 높은 지연하에서 기존의 TCP/ IP/ HTTP/ HTML 을 최적화해서 적용하기 위한 일련의 프로토콜이다. WAP 은 웹컨텐츠를 이동전화나 PDA 등에서 받아 볼수 있게 해준다. 그러나 WAP 게이트웨이가 컨텐츠제공자에게 속해있지 않다면 단대단 보안을 지원하지는 못한다. 본 논문은 ITLS 를 제안하여 WAP 게이트웨이에서 평문의 메시지를 보지 못하게 한다. 기본원리는 웹서버의 보안 상대를 게이트웨이가 아닌 클라이언트로 변경하고, 클라이언트는 웹서버와 게이트웨이를 위해 두번 암호화하도록 하는 것이다. 즉 게이트웨이는 클라이언트로부터 수신한 암호문을 한번만 복호화하고 재암호화없이 바로 웹서버에게 보내는 것이다. 반대방향도 유사한 형태이다. 이러한 기능을 제공하기 위해 WTLS 핸드쉐이크 프로토콜에 새로운 메시지 유형을 추가하고, 응용데이터 암호화 또는 복호화 규칙도 변경하였다.

1. 서론

인터넷은 급격한 비율로 성장하고 있고, 그 성장에서의 주요경향은 전자상거래 시장의 확대에 기인한다. 또한 이동전화, PDA(Personal Digital Assistants), HPC(Handheld PCs)등의 보편화로 무선가입자가 2001년에 5 억이 넘을 것으로 추정된다. 세계는 점점 더 연결되고, 시간과 공간과 방법을 초월하여 통신할 수 있게 된다. 즉 무선인터넷은 인터넷의 다음 물결이다. 이동 단말에서의 인터넷 서비스가 급격히 증가하고 이를 안전하고 확장성있고 관리하기 쉽게 지원하기 위해 새로운 프로토콜이 필요하게 되었다. WAP (Wireless Application Protocol)은 무선환경에서 발견되는 저 대역폭, 높은 지연하에서 기존의 TCP /IP /HTTP /HTML 을 최적화해서 적용하기 위한 일련의 프로토콜이다. 이를 사용하면 HTTP/TCP/IP 를 사용할 때보다 패킷의 수가 반 이하로 줄어들게 된다[1].

점점 많은 가입자가 WAP 서비스를 사용하여 M-Commerce 시장이 확대될수록 무선인터넷 보안의 필요성도 함께 증가한다. 1998 년까지 TLS(Transport Layer Security)를 이용한 보안구조와 암호화가 전자상거래시장에 기여하여 왔고, WTLS(Wireless Transport Layer Security) 가 WAP 보안을 제공하도록 설계되었다. WAP 게이트웨이는 WTLS 와 TLS 간의 브리지역할을 하며, 이동단말에서 보내진 데이터는 게이트웨이에서 복호화되고, 다시 암호화되어 웹서버에게 전달된다. 게이트웨이내에서 평문으로 남아있는 시간이 아무리 짧다 하지만, 보안 문제의 근원이 될 수 있고 결과적으로 이동단말과 웹서버간의 단대단 보안은 지원하지 못하는 단점을 안고 있다.

본 논문에서는 ITLS (Integrated TLS)라 불리는 단대단 보안모델을 제안하고자 한다. 기존의 TLS 부분

에는 변화를 주지 않고 WTLS 부분의 변화만을 필요로 한다. ITLS 의 목표는 WAP 게이트웨이에서 복호화된 평문을 일순간도 가지지 못하게 한다. 제 2 장에서는 WAP 의 기본구성과 WAP 보안에 대해 살펴보고, 제 3 장에서는 제안된 ITLS 의 개념과 프로토콜을 제시하며 제 4 장에서 ITLS 를 간략히 분석하고 제 5 장에서 결론을 맺는다.

2. WAP and WAP Security

WAP 은 인터넷과 무선환경에서 존재하는 표준의 특성과 기능을 물려받은 일련의 프로토콜이다. 인터넷은 고정된 컴퓨터를 위해 생성된 것이고 WAP 은 낮은 클럭 주파수와 적은 메모리를 가진 장비를 다루어야 하기 때문에, 그들 간의 연결은 낮은 대역폭과 적은 안정성을 갖게 된다[2]. 그래서 TCP/IP 와 같은 기존 프로토콜이 아닌 새로운 구조를 필요로 한다. WAP 은 6 개의 계층으로 나뉜다[3]. 상위부터 언급해서 WAE(Wireless Application Environment)는 이동전화와 웹기술의 혼합에 기반하여 WML (Wireless Markup Language), WTA (Wireless Telephony Application), 캘린더 정보, 전화번호부 기록과 같은 것으로 구성되는 마이크로 브라우저 환경을 포함한다.[4] WSP(Wireless Session Protocol)는 연결과 비연결 세션을 지원하고, 무선단말과 WAP 게이트웨이간 세션을 관리한다[5]. WTP(Wireless Transaction Protocol) 는 이동단말에 적합한 단순한 트랜잭션 용 프로토콜로서 WSP 와 함께 HTTP 와 유사한 역할을 한다[6]. WTLS 는 TLS 에 기반하여 좁은 대역폭에서 사용되도록 최적화된 보안 프로토콜로서 인증(Authentication), 기밀성(Privacy), 데이터 무결성 (Data Integrity) 등을 지원한다 [7]. WDP(Wireless Datagram Protocol)는 인터넷의 TCP/IP 와 동등한 역할을 한다[8]. 마지막 계층은 SMS(Short Message Service), CDMA(Code Division Multiple Access), CDPD(Cellular Digital Packet Data)와 같은 베어러 서비스등을 의미한다.

WAP 게이트웨이는 다음의 그림 1 과 같이 WTLS 와 TLS 사이에 존재한다. WTLS 와 TLS 간의 변환은 최대의 안전을 위해 게이트웨이의 메모리내에서 매우 짧은 순간에 일어나고 가능한 빨리 메모리에서 사라지도록 처리한다. WTLS 는 TLS1.0 에 근거하지만 데이터그램지원, 최적화된 핸드쉐이크, 동적인 키 최신화(key refreshing)와 같은 새로운 특성도 갖는다[9]. 그러나 게이트웨이에서 평문의 메시지가 존재한다는 것은 보안의 허점이 될 수밖에 없다. 슈퍼유저의 권한을 가진 자는 그 평문을 얻을 수 있고, WAP 게이트웨이의 관리기관에게 인증기관의 역할을 부여하기는 어렵다. 이를 해결하기 위해 게이트웨이를 웹서버와 동일한 기관에 설치하는 방법이 현재 제안되고 있다. 이는 컨텐츠제공자에게 각각의 네트워크와 SMSC(Short Message Service Center)별로 다른 구성을 설정하는 게이트웨이까지 관리하는 짐을 지우게 될 뿐만 아니라, 가입자와 무선네트워크 운영자 모두에게 여러가지 어려움을 안겨준다[9].

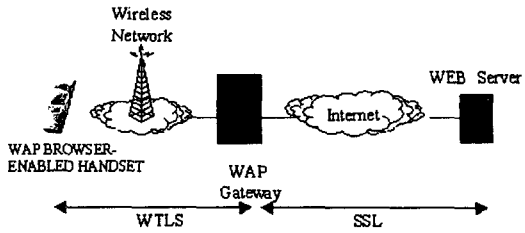

그림 1. WAP 보안 모델

3. 제안된 단대단 보안모델: ITLS

ITLS 의 목적은 다음과 같이 무선 인터넷 보안을 TLS 와 투명하게 통합하는 것이다. 첫째 WAP 게이트웨이는 평문을 잠시라도 보유할 수 없어야 한다. 둘째 WAP 게이트웨이의 공급자는 컨텐츠 제공자와 독립되어야 한다. WTLS 에서 클라이언트와 게이트웨이는 하나의 비밀키를 공유하고 게이트웨이와 웹서버가 또 다른 비밀키를 공유한다. ITLS 는 간단히 말해서 비밀키의 공유자를 바꾸는 것이다. 즉, 클라이언트와 게이트웨이간 공유는 그대로 두고, 게이트웨이가 아닌 다시 클라이언트와 웹서버가 또 다른 비밀키를 공유하게 한다. 즉 웹서버와 보안상대는 게이트웨이가 아니라 클라이언트가 되는 것이다. 다음의 그림 2 는 이러한 개념을 보여주는데 이는 SET (Secure Electronic Transaction)에서의 소비자와 상점과 CA(Certificate Authority) 간의 관계와 유사한 맥락이다[10].

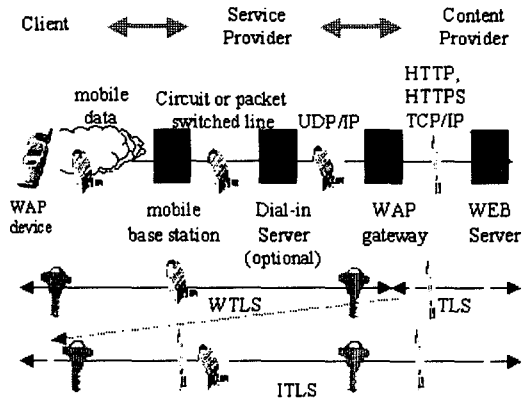

그림 2. ITLS 보안 모델

3.1 ITLS 핸드쉐이크 프로토콜

기존의 WTLS 게이트웨이는 클라이언트와의 비밀키를 가지고 클라이언트로부터 온 메시지를 복호화하고, 웹서버와의 비밀키를 가지고 다시 암호화를 한

다. 반면에 ITLS 에서는 클라이언트가 웹서버를 위해 한번, 게이트웨이를 위해 두번 순서에 맞추어 암호화를 한다. 그리고 게이트웨이는 클라이언트로부터 온 메시지를 복호화한 후, 다시 암호화하지 않고 웹서버로 보낸다. 그러나 이 메시지 또한 이미 암호화된 것이다. 단지 게이트웨이가 아닌 클라이언트에서 암호화했다는 점만 다르다. 웹서버에서의 동작에는 변화가 없다. 반대로 웹서버로부터 온 메시지를 게이트웨이는 복호화하지 않고, 다시 암호화만 해서 클라이언트로 보내면 클라이언트는 순서대로 두번 복호화를 한다. 이러한 메커니즘을 적용하기 위해 다음의 그림 3 처럼 새로운 핸드쉐이크 흐름이 제안된다. 클라이언트는 웹서버와의 Pre-Master Key 를 보내야 하고, 웹서버의 공개키를 알아야 그 Pre-Master Key 를 안전하게 보낼 수 있다. (키교환 프로토콜이 RSA 인 경우) 그래서 웹서버의 인증서를 포함한 IntCertificate 메시지와 클라이언트에서 생성한 Pre-Master Key 를 포함한 IntkeyExchange 를 추가하였다. 게이트웨이에서는 그림 3 의 화살표처럼 Certificate 을 IntCertificate 으로 IntKeyExchange 를 ClientKeyExchange 로 적절히 매핑시키는 것이 필요하다.

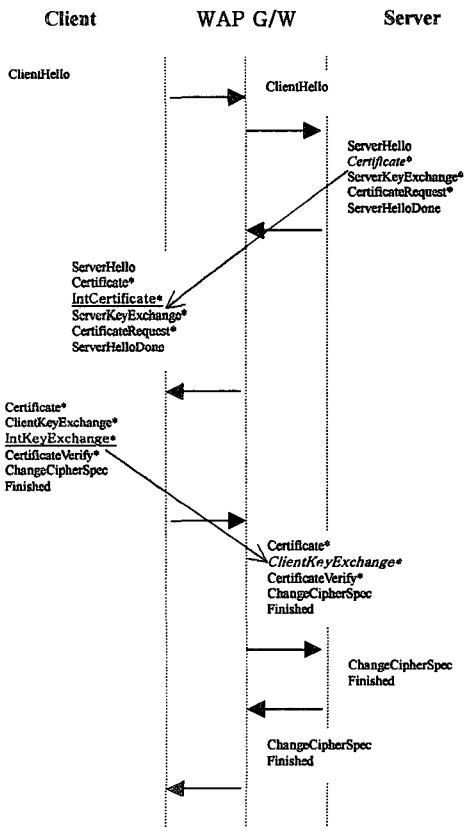

그림 3. ITLS Full Handshake

3.2 ITLS 레코드 프로토콜

레코드 프로토콜은 핸드쉐이크 프로토콜에서 넘어온 보안 파라미터에 포함된 키들을 사용해서 실제로 메시지를 암호화 또는 복호화하여 송수신하는 부계층이다. ITLS 응용 데이터 송수신 과정을 다음의 그림 4 에서 쉽게 보여준다. 다음은 그림 4 에서 사용한 기호에 대한 설명이다.

SM_o : original fragment (plain text) from a client
SM_e : encrypted fragment (cipher text) of SMo and decrypted fragment of SM_{e2} for a client and a server
SM_{e2} : encrypted fragment of SMe for a client and a gateway
RM_o : original fragment (plain text) from a server
RM_e : encrypted fragment (cipher text) of RMo and decrypted fragment of RM_{e2} for a client and a server
RM_{e2} : encrypted fragment of RM_e for a client and a gateway

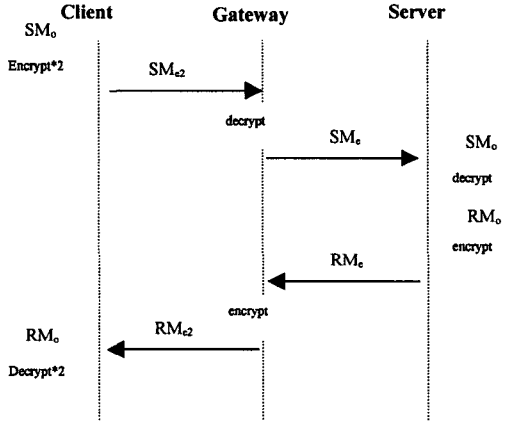

그림 4. ITLS 응용 데이터 흐름

4. ITLS 분석

ITLS 구현에 있어서 고려 사항을 언급하고자 한다. 첫째는 이동단말에서의 증가된 부하를 들 수 있다. 왜냐하면 WTLS 에 비해서 두번 암호화하고 복호화하기 때문이다. 이는 이동단말의 성능이 급속히 향상되기 때문에 심각한 것으로 보이지 않는다. 성능 저하에 대한 통계적 수치는 아직 없다. 둘째는 웹서버에서 보낸 메시지가 오류를 포함하고 있어도 게이트웨이는 인식하지 못한다. 그러나 그 문제는 결국 클라이언트에서 확인되기 때문에 안전에는 문제가 없고 단지 불필요한 정보를 클라이언트까지 보내는 낭비만을 초래한다. 셋째는 게이트웨이 설계에 있어서 위의 그림 3 처럼 두개의 세션이 실시간으로 상호 처리되도록 해야 한다[11][12][13].

지금까지 설명된 ITLS 의 핵심은 레코드 프로토콜에서의 기밀성와 데이터 무결성을 제공하는 것이다. 그런데 ITLS 를 확장하여 단대단 인증과 부인봉쇄를

제공하는 것도 가능하다. 즉, 핸드쉐이크 프로토콜에서 서로를 인증하는 것 또한 게이트웨이가 아닌 상대방 (클라이언트 또는 웹서버)으로 교체할 수 있다. 그러면 게이트웨이의 책임은 점점 줄어들고, 부가적으로 발생하는 영향들을 해결해야 한다.

5. 결론

이제 산업계는 무선환경으로 향하는 다음 번 도약으로 가고 있다. 고도의 이동 상거래 시장이 증가할수록 융통성있고 확장가능하며 단대단까지 안전한 컨텐츠가 요구된다. 이제까지 설명한 ITLS 는 무선인터넷 환경에서 이러한 단대단 보안모델을 제시한다. ITLS 는 게이트웨이가 컨텐츠제공자와 독립된 상태에서 안전하게 암호화된 메시지를 전달할 수 있게 해준다. 단, 무선단말에서 이중으로 암호화와 복호화를 해야 하는 것과 게이트웨이에서 무결성을 검사하지 못하는 부분의 통계적 성능 저하치의 연구가 요구된다.

참고문헌

[1] "The Wireless Application Protocol, Wireless Internet Today", Unwired Planet, Inc., Feb. 1999.

[2] Tobias Eidem, "The effect of the WAP gateway on a WAP network", Royal Institute of Technology, 1999.

[3] WAP Forum, "Wireless Application Protocol Architecture Specification, version 1.2", WAP Forum, Apr. 1998, available at http://www.wapforum.org/tech/.

[4] WAP Forum, "Wireless Application Environment Overview, version 1.2", Nov. 1999.

[5] WAP Forum, "Wireless Session Protocol Specification, version 1.2", Nov. 1999.

[6] WAP Forum, "Wireless Transaction Protocol Specification, version 1.2", Jun. 1999.

[7] WAP Forum, "Wireless Transport Layer Security Specification, version 1.2", Nov. 1999.

[8] WAP Forum, "Wireless Datagram Protocol Specification, version 1.2", Nov. 1999.

[9] "Understanding Security on the Wireless Internet", Phone.com, Jan. 2000.

[10] "The SET™ Specification – Business Description 1.0", MasterCard & Visa, May 1997.

[11] Rikard Kjellberg, "Ellipsus Communication Server Architecture Issue <1.0>", Ellipsus, May 2000.

[12] "WAP gateway Corporate Version White paper", S.E.S.A. Software and System AG.

[13] "WAP Security Toolkit [WST], A Baltimore Technologies White Paper", Baltimore™.