WAP환경에서 안전한 종단간 보안을 제공하는 TLS(Transport Layer Security)-Plus 프로토콜

최진규[U] , 이헌길
강 원 대 학 교 컴 퓨 터 · 정 보 통 신 공 학 과
rookiej@hitel.net , hglee@cc.kangwon.ac.kr

An End to End Security in the WAP environment : TLS(Transport Layer Security)-Plus Protocol

Jin-Kyu Choi[U] Heon-Guil Lee
Dept. of Computer and Information, Kangwon National University

요 약

WAP은 WAP Forum에서 제정한 무선 환경에서의 데이터 통신을 위한 표준 프로토콜이다. WAP에서는 보안 통신을 위한 프로토콜로서 WTLS(Wireless Transport Layer Security)를 제안하고 있다. 이것은 TCP/IP 상의 TLS(Transport Layer Security)를 바탕으로 무선 환경에 맞게 최적화한 것이다. 그러나, WAP은 기본적으로 게이트웨이 모델에 따른 프로토콜이라는 점과 무선 구간에서의 전송 효율을 높이기 위한 인코딩 기능 때문에 게이트웨이에서 클라이언트와 서버 사이에 교환되는 정보가 노출되는 이른바 종단간의 보안(End-to-End Security) 문제가 존재한다. 이러한 이유로 유선에서와는 달리 안전한 종단간 보안을 제공하지 못하고 있다. 이에 본 논문에서는 기존 TLS와 WTLS를 합친 새로운 TLS(Transport Layer Security)-Plus 프로토콜을 제안하여 무선 환경에서 무선 단말기에 부담을 주지 않는 안전한 종단간 보안을 제공하려고 한다.

1. 서 론

WAP(Wireless Application Protocol)은 Mobile-Commerce에서 가장 널리 사용되고 WAP Forum에서 제정하고 있는 무선환경에서 동작하는 표준 프로토콜이다. WAP은 무선 단말기의 낮은 CPU속도, 적은 메모리, 제한된 전력, 제한된 화면 등을 고려하여 기존의 유선 프로토콜을 축약한 형태이다.[1]

WAP에서 기존 인터넷으로 연결된 시스템과 데이터 통신을 할 때 인터넷 프로토콜과 WAP을 변환해주기 위한 WAP 게이트웨이가 존재한다.[2]

WAP에서는 보안 프로토콜로 WTLS(Wireless Transport Layer Security)를 제안하고 있다. WTLS는 인터넷 프로토콜에서 TCP/IP의 보안에 사용하는 TLS(Transport Layer Security)를 무선 환경에 맞도록 최적화한 것이다. [그림 1]와 같이 무선 단말기와 WAP 게이트웨이 사이에서 이루어지는 통신은 WTLS로 보호하고, WAP 게이트웨이와 웹서버 사이는 TLS로 보호한다. WAP 게이트웨이에서는 서로 다른 프로토콜 스택의 변환이 일어나는데, 쌍방간의 프로토콜 변환을 위해 WAP 게이트웨이에서는 매우 짧은 시간이지만, 암호문이 평문으로 변환되어 노출되는 문제점이 생기게 된다. 따라서, 유선과 달리 안전한 종단간의 보안을 제공하지 못하고 있다.[3][4]

최근에 안전한 종단간 보안을 위한 방법으로 ITLS(Integrated Transport Layer Security) 프로토콜이 제시되었다. ITLS에서는 무선 단말기에서 두 번의 암호화/복호화를 수행하여 WAP 게이트웨이에서 메시지를 노출하지 않고도 유선 인터넷에 연결된 시스템과 안전한 종단간 보안을 제공한다.[5]

그러나, 현재 무선 단말기의 낮은 CPU 속도, 적은 메모리, 전력 소비의 제한 및 무선 네크워크의 낮은 대역폭, 많은 대기지연시간, 비안정적 연결상태 등의 제약이 있어 무선 단말기에서 두 번의 암호화/복호화를 수행하는 것이 무선 단말기에 많은 부담을 준다.[6]

이에 본 논문에서는 무선 단말기의 부담을 줄이면서 안전한 종단간의 보안을 제공하는 새로운 TLS(Transport Layer Security)-Plus 프로토콜을 제안한다. TLS-Plus 프로토콜에서는 유선 인터넷에 연결된 서버에서 무선단말기와 WAP 게이트웨이를 위한 암호화/

그림 1. WAP 게이트웨이의 역할

복호화를 두 번 수행함으로써 WAP 게이트웨이에서 메시지 내용이 노출되는 문제를 해결한다.

2장에서는 WAP 보안의 문제점을 기술한다. 3장에서는 제안된 TLS-Plus 프로토콜의 Handshake 프로토콜과 Record 프로토콜을 기술한다. 4장에서는 TLS-Plus프로토콜에 대해서 비교·분석을 하고 5장에서 결론을 맺는다.

2. WAP에서의 보안문제

WTLS를 사용하는 구간에서는 기밀성, 무결성, 사용자 인증의 보안 서비스를 해결할 수 있다.[6][8][9] 그러나, 서론에서 말했듯이, 무선 단말기인 클라이언트와 유선 인터넷의 서버간 통신을 위해서 WAP 게이트웨이에서 WTLS와 TLS간 상호 프로토콜 변환이 이루어지는데 여기에서 데이터 원본이 노출되는 보안의 문제가 발생한다. [그림2] 물론, 통신사업자가 WAP 게이트웨이의 대부분을 운영하는 현재 상황에서 통신사업자를 믿는다면 어느 정도는 신뢰할 수 있지만 비즈니스에 따라서는 이러한 신뢰도는 사업상 큰 위험으로 작용할 수 있다. 따라서, WAP을 이용한 무선 통신에서는 어느 정도 신뢰할 수 있는 보안을 제공하되 유선 통신에서와 같은 안전한 종단간 보안은 제공하지 못하고 있다.

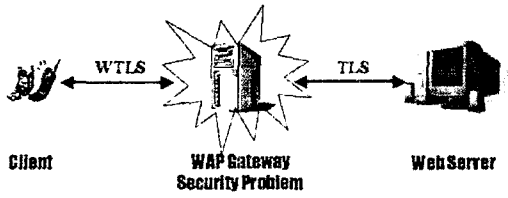

그림 2. WAP 게이트웨이의 문제점

3. 제안된 프로토콜

이 장에서는 새로운 WAP 보안 프로토콜인 TLS-Plus를 소개한다. 제안된 보안 프로토콜 TLS-Plus가 기존 유선의 TLS와 같은 종단간 보안을 만족하기 위해서는 다음과 같은 전제 조건이 필요하다.

- WAP 게이트웨이는 보안을 요하는 암호화된 데이터를 프로토콜 변환을 위해 평문으로 복호화해서는 안된다.
- 서버는 클라이언트와 WAP 게이트웨이에서 보낸 암호문을 복호화할 수 있어야 한다.

WTLS에서 무선단말기와 WAP 게이트웨이는 서로 비밀키를 공유하게 된다. 또한 TLS에서는 WAP 게이트웨이와 서버가 서로 비밀키를 각각의 세션동안 공유하게 된다. TLS-Plus에서 추가된 기능은 한번 더 암호화/복호화를 하기 위해서 무선 단말기와 서버가 서로 비밀키를 하나 더 공유하는 것이다. 이렇게 함으로써 WAP 게이트웨이에서는 암호화된 메시지를 복호화하지 않고 암호문에 한번 더 암호화를 수행함으로써 WAP 게이트웨이에서 일어날 수 있는 메시지 노출 문제를 해결할 수 있다.

3.1 TLS-Plus Handshake Protocol

Handshake 프로토콜은 클라이언트와 서버가 Record Layer에서 사용할 Security Parameters를 설정하는 과정이다. 따라서, TLS-Plus에서는 클라이언트와 서버, WAP 게이트웨이와 서버가 Security Parameters를 설정하기 위한 Handshake 프로토콜을 제안하였다. TLS-Plus의 Full Handshake Protocol은 [그림 3]과 같다.

다음은 주고받는 메시지에 대한 설명이다. 여기서 M은 무선단말기 즉, 클라이언트를 의미하고 N은 WAP 게이트웨이를 말한다.

- <M, N> Message : M과 N에서 서버로 보내는 메시지
- Message(M, N) : 서버에서 M과 N으로 보내는 메시지

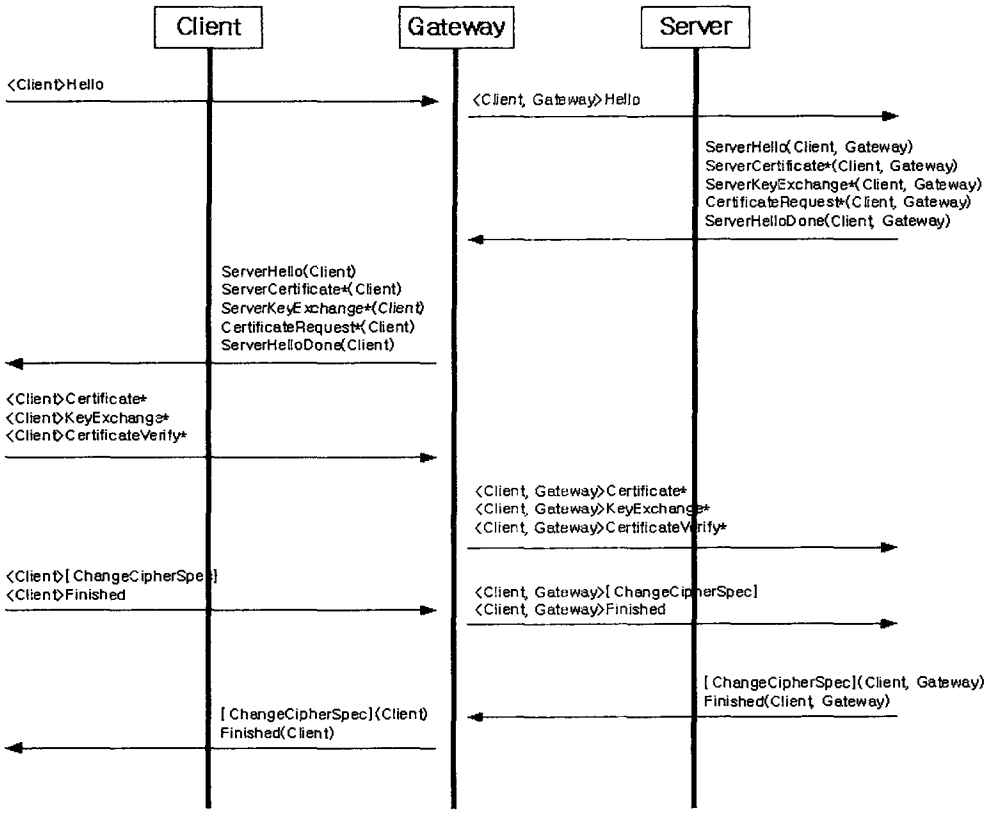

그림 3. TLS-Plus Full Handshake Protocol

3.2 TLS-Plus Record Protocol

Record 프로토콜에서는 Handshake 프로토콜에서 협상으로 결정된 보안 파라미터(Security Parameters)를 이용하여 키를 생성·사용한다. TLS-Plus에서는 클라이언트와 서버, WAP 게이트웨이와 서버가 각각 키를 공유한다. 그리고 그 키를 이용하여 암호화/복호화를 하여 전송을 한다는 것이다. TLS-Plus에서 어플리케이션 데이터 흐름은 다음 [그림4, 5]와 같다.

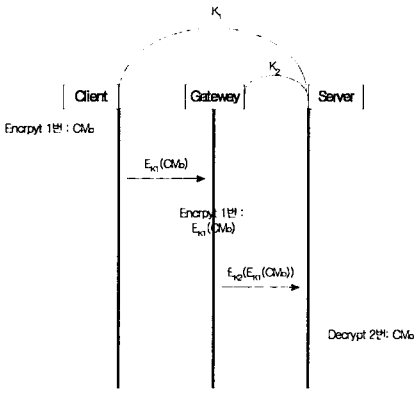

그림 4. TLS-Plus Application Data Flow
(Client → Server)

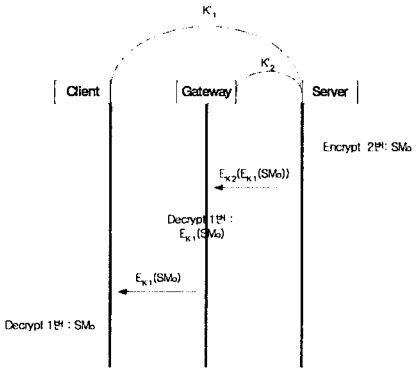

그림 5. TLS-Plus Application Data Flow
(Server → Client)

4. 비교 및 분석

TLS-Plus의 요점은 서버에서 클라이언트로 메시지를 보낼 때는 두 번의 암호화, 받을 때는 두 번의 복호화를 수행한다는 것이다. 따라서, 기존의 WTLS와 TLS의 방식에 비해 서버에 상당한 부담이 될 것이나. 그러나 장점으로는 WAP 게이트웨이에서의 메시지 노출이 없고, 서론에서 제시된 ITLS에 비해 TLS-PLUS에서는 클라이언트에 부담이 없다는 것이다. [표 1]은 클라이언트에서 암호화 메시지를 보낼 때 일어나는 암호화 횟수 및 WAP 게이트웨이에서의 평문 노출 여부를 비교한 표이다.

ITLS에서와 같이 무선 단말기(클라이언트) 쪽에 암호화/복호화 부담을 준다는 것은 낮은 CPU 파워, 적은 메모리, 전력 소비의 제한, 낮은 대역폭, 많은 대기지연시간 등의 무선 단말기 제약 때문에 현실적으로 맞지 않는다고 볼 수 있다.[6][7]

표 1. 암호화/복호화 횟수 비교 및
WAP 게이트웨이에서의 평문 노출 여부

	WTLS/SSL	ITLS	TLS-Plus
클라이언트	1	2	1
게이트웨이	2	1	1
서버	1	1	2
WAP게이트웨이에서의 평문 노출여부	노출됨	노출 안됨	노출 안됨

TLS-PLUS에서는 ITLS에 비해 클라이언트보다 서버에서 부담이 생기게 되지만 서버는 쉽게 확장이 가능하므로 그렇게 크게 문제가 되지 않는다고 볼 수 있다.

5. 결론

오늘날 무선통신은 사회전반에 확산되어 빠르게 발전하고 있다. 누구나 편리하게 장소에 구애받지 않고 안전한 무선통신을 하기 위해서는 보안정책이 선행되어야 한다. 사용자의 소중한 정보를 안전하게 보호하지 못할 경우, 무선통신의 심각한 문제점으로 대두되어 성장이 저하될지도 모른다. 이에 본 논문에서는 WTLS와 TLS를 합친 TLS-Plus를 제시하여 무선환경에서의 안전한 종단간 보안을 제공하였다.

제안된 TLS-Plus에서는 무선 단말기에서 보낸 암호문이 WAP게이트웨이에서 보낸 암호문이 변환을 위해 잠시나마 평문으로 복호화되는 것이 아니라 다시 한번 암호화함으로써 WAP게이트웨이에서 일어날 수 있는 본문의 노출을 막을 수 있다.

6. 참고 문헌

[1] WAP Forum, "Wireless Application Protocol Architecture Specification", version 12-July-2001, http://www.wapforum.org, 2001.

[2] T. Dierks and C. Allen, The TLS protocol version 1.0, RFC 2246 Jan. 1999.

[3] WAP Forum, "WAP Transport Layer E2E Security Specification", Version 11-July-2000, 2000.

[4] WAP Forum, "Wireless Application Protocol(WAP) Wireless Transport Layer Security(WTLS) Specification", Version 18-Feb-2000, 2000.

[5] Eun-Kyeong Kwon, Yong-Gu Cho, Ki-Joon Chae, "Integrated Transport Layer Security : End-to-End Security Model between WTLS and TLS", IEEE, 2001.

[6] 이동훈, 임재훈, "WTLS와 TLS비교 분석(Technical Report)", Oct. 13, 2000.

[7] S. Sengodan, T. Luo, R. Bansal, H. Herlin, "End-to-End Security Issues in Wireless-IP Networks", IASTED Applied Informatics, Austria, February 15-17, 2000.

[8] 박창섭, "암호 이론과 보안", 人英社, 1999.

[9] H. Krawczyk, M. Bellare and R. Canetti, "HMAC : Keyed-Hashing for Message Authentication", RFC2104, Feb, 1997.