산업기술연구(강원대학교 산업기술연구소 논문집), 제29권 B호, 2009.
Journal of Industrial Technology, Kangwon Natl. Univ., Korea, No. 29 B, 2009.

제한된 자원의 무선 단말기를 위한 종단간 보안을 제공하는 WTLSW 프로토콜 및 프록시 모델

A WTLSW Protocol and a Proxy Model to Ensure End-to-End Security for Mobile Devices with Limited Resources

이 헌 길*
Lee, Heon-Guil

Abstract

The need for end-to-end security has been increased with the widespread use of mobile devices in wireless internet access applications such as mobile commerce. The WAP1.x has an end-to-end security problem that the message transmitted between the mobile device and the Web server is decrypted inside the gateway within a short time. To overcome this problem, several protocols including WAP2.0 has been proposed. These protocols require that the heavy modules such as TLS or data compression modules should be installed on the mobile device with limited resources. This paper proposes a new WTLSW(WTLS-TLS at Web server) protocol and a new WAP2.0 proxy model in order to ensure end-to-end security between the mobile device and the Web server and to be appropriate for mobile devices with limited resources.

키워드 : *종단 간 보안, WAP, 무선단말기*
Keywords : *end-to-end security, WAP, wireless mobile device*

1. 서론

휴대폰, PDA 등 이동 무선단말기가 mobile commerce 분야에서 성공적으로 사용되기 위해서는 무선 인터넷 액세스 기능이 필수적이라고 할 수 있다. WAP (Wireless Application Protocol)은 무선통신 네트워크에서 운영되는 응용을 개발하기 위해 관련 산업체로 구성된 WAP Forum에서 제안한 표준 프로토콜이다[1][3].

WAP1.x는 무선단말기의 낮은 CPU 성능, 적은 메모리, 제한된 전력 및 화면 등을 고려하여 기존 인터넷 및 HTTP 프로토콜을 무선 환경에 적합하도록 축소한 것이다. WAP1.x로 인터넷으로 연결된 시스템과 데이터 통신을 할 때 인터넷 프로토콜과 WAP 프로토콜을 변환해 주기 위한 WAP1.x 게이트웨이가 무선단말기와 웹서버 사이에 존재한다[1]. WAP1.x에서는 보안 프로토콜로 WTLS (Wireless Transport Layer Security Protocol)를 제안하고 있다[2]. WTLS는 인터넷에서 TCP/IP의 보안에 사용하는 TLS(Transport Layer Security Protocol)[14]를 무선통신 환경에 맞도록 최적화한 것이다. WAP1.x에서 무선단말기와 게이트웨이 사이에서 이루어지는 데이터 통신은 WTLS로 보호하고, 게이트웨이와 웹서버 사이는 TLS로 보호한다. 무선단말기와 웹 서버 사이 종단간 보안 통신을 할 때, 게이트웨이에서 WTLS와 TLS 간 프로토콜을 변환해야 하는데, 이 때 매우 짧은 시간이지만, 메시지 암호문이 평문으로 복원되어 노출되는 문제점이 발생한다[8][9][10][12][13][15].

WAP1.x의 문제점을 개선하기 위해 제안된 WAP2.0은 무선단말기에 표준 인터넷 프로토콜인

* 강원대학교 컴퓨터정보통신공학 교수, 공학박사, 교신저자

TCP/IP, HTTP를 지원한다. 또한, TLS를 무선단말기에 탑재하여 TLS 터널링으로 무선단말기와 웹 서버 사이에 종단간 보안을 제공할 수 있다[5]. 따라서 WAP1.x에서처럼 프로토콜 변환을 수행하는 게이트웨이가 필요 없어 메시지 노출 문제가 없다. 그러나, WAP2.0은 보안을 위해 무선단말기에 TLS를 채택함으로써 WAP1.x의 WTLS에 비해 많은 자원과 처리 시간을 요구한다. 이는 제한된 자원과 대역폭을 가진 무선 환경에서 문제점으로 지적된다[11].

WAP1.x 게이트웨이에서의 메시지 노출 문제를 해결하기 위해 ITLS (Integrated Transport Layer Security) 프로토콜이 제안되었다[13]. 이 방식은 무선단말기에서 웹 서버를 위한 TLS와 WAP1.x 게이트웨이를 위한 WTLS 등 두 번의 암호화/복호화를 수행함으로써 게이트웨이에서의 프로토콜 변환 문제를 해결하였다. 그러나, 낮은 CPU 성능, 적은 메모리, 제한된 전력의 무선단말기에서 계산량이 많은 TLS와 WTLS 방식으로 암호화/복호화를 두 번 수행하는 것은 무선단말기에 너무 부담이 많다.

표준 인터넷 프로토콜을 사용하는 WAP2.0의 과도한 무선 대역폭 사용을 줄이고 효율적으로 종단간 보안을 지원하기 위해 데이터 압축 기능을 가진 WAP 프록시 아키텍처가 제안되었다[8][9]. 이 기법은 무선단말기와 WAP2.0 프록시 사이에 데이터를 압축하여 송수신함으로써 무선 대역폭을 줄일 수 있고, 또한, WAP2.0 프록시는 TLS로 보호되는 데이터를 복원하지 않고 중계만 하는 TLS 터널링 기법을 사용하기 때문에 메시지 노출 문제가 일어나지 않는다. 하지만, 무선단말기에 인터넷 프로토콜과 TLS 프로토콜뿐 아니라 데이터 압축/복원 기능도 구현해야 하기 때문에 제한된 자원을 가진 무선단말기에 부담을 많이 준다.

본 논문에서는 제한된 자원을 가진 무선단말기 환경에서 효율적으로 종단간 보안을 지원하기 위해 WAP1.x에서 제안한 WTLS를 무선구간에서 사용하고, 유선구간에서는 TLS를 사용하는 새로운 WTLSW(WTLS/TLS at Web server) 프로토콜과 WAP2.0 프록시 모델을 제안한다. WTLSW 프로토콜에서는 웹 서버에서 무선단말기와 WAP2.0 프록시를 위해 각각 WTLS와 TLS 프로토콜로 전송 메시지에 대해 암호화/복호화를 두 번 수행한다. 이렇게 함으로써 WAP2.0 프록시에서 프로토콜 변환을 하지 않아도 되므로 메시지 내용이 노출되는 문제를 해결하고, 무선단말기의 부담을 감소시킨다.

본 논문의 2장에서는 WAP 프로토콜에서의 보안문제와 이를 해결하기 위해 기존에 제시된 프로토콜 및 관련 연구를 소개하고 분석한다. 3장에서는 본 논문에서 제안한 WTLSW 프로토콜과 WAP2.0 프록시 모델을 소개한다. 4장에서는 제안된 WTLSW 프로토콜과 다른 방법들을 비교 분석한다. 마지막으로 5장에서 결론을 기술한다.

2. WAP에서의 보안문제 및 관련 연구

2.1 WAP1.x에서의 보안 문제

그림 1에서 보듯이 WAP1.x의 시스템 구성에서 WAP1.x 게이트웨이가 반드시 있어야 한다. 게이트웨이는 무선단말기와 WSP, WTP, WTLS, WDP 등으로 구성된 WAP1.x 프로토콜을 사용하여 메시지를 교환하고, 웹 서버와는 HTTP, TLS, TCP/IP 등으로 구성된 표준 인터넷 프로토콜을 사용하여 메시지를 교환한다[1]. 무선단말기와 웹 서버 사이의 종단 간 보안을 제공하기 위해 WAP1.x에서는 무선구간에서 WTLS를, 인터넷에서는 TLS를 사용하여 기밀성, 무결성, 사용자 인증 등의 보안 서비스를 지원하고 있다. 그러나, 무선단말기인 WAP 클라이언트와 웹 서버간 통신 과정 중에 게이트웨이에서 WTLS와 TLS 간 프로토콜 변환을 수행한다. 즉, 무선단말기로부터 전송된 암호문을 평문으로 복원한 후, 다시 TLS 방식으로 암호문을 작성하여 웹 서버로 전송한다 (역방향의 메시지 전송도 유사). 이 과정에서 메시지 원본이 평문으로 잠시 노출되어 보안에 심각한 문제가 발생할 수 있다[8][9][10][13].

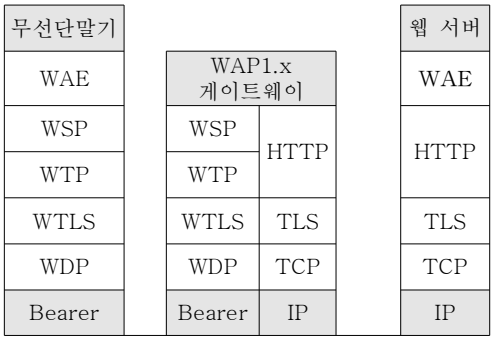

그림 1. WAP1.x 시스템 구성 및 프로토콜 스택

2.2 WAP2.0 TLS 터널링 기법

그림 2는 WAP2.0의 시스템 구성과 프로토콜 스택을 보여 준다. WAP2.0에서는 무선단말기와 웹 서버 사이에 프록시 없이 직접 연결하거나 프록시를 중간에 두어 필요한 기능을 수행하면서 연결할 수 있다. 무선단말기에는 WP(Wireless Profiled)-HTTP, WP-TLS, WP-TCP/WP-IP [6,7] 등 무선 환경 프로파일 인터넷 프로토콜을 지원하여 HTTP, TLS, TCP/IP 등 인터넷 프로토콜을 지원하는 웹 서버와 중간에 프로토콜을 변환하지 않고 바로 메시지를 교환한다[3][4]. 무선단말

기와 웹서버 간에 TLS 터널링 기법을 사용하여 WAP1.x 게이트웨이의 경우처럼 데이터를 노출시키지 않고 종단간 보안을 제공할 수 있다[5]. 그러나, 그림에서 보듯이 무선단말기에 표준 인터넷 프로토콜을 구현해야 하므로 제한적인 자원을 가진 무선단말기인 경우 많은 부담이 될 수 있다. 또한, WAP1.x의 WSP에 비해 HTTP를 사용하므로 더 많은 비트 전송이 필요하고, TCP를 사용하기 때문에 WTP를 사용하는 것보다 더 많은 트랜잭션을 요구한다[8][9].

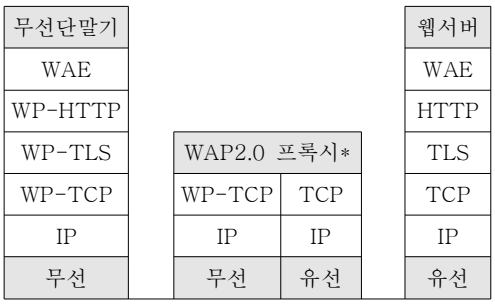

그림 2. WAP2.0 시스템 구성 및 프로토콜 스택
(* : 선택적)

2.3 ITLS (Integrated Transport Layer Security) 프로토콜

ITLS (Integrated Transport Layer Security) 프로토콜은 WAP1.x 게이트웨이에서의 메시지 노출 문제를 해결하기 위해 제안되었다[13]. 이 방식은 무선단말기에서 전송메시지에 대해 웹 서버를 위한 TLS 암호화/복호화와 게이트웨이를 위한 WTLS 암호화/복호화 등 두 번의 암호화/복호화를 수행함으로써 게이트웨이에서의 메시지 노출 문제를 해결하고 있다. ITLS에서 무선단말기는 WAP1.x 프로토콜 스택과 웹 서버와의 종단간 보안을 위한 TLS를 지원해야 한다(그림3).

무선단말기는 웹 서버에 메시지를 안전하게 보내기 위해 먼저 TLS로 암호화하고 이를 다시 WTLS로 암호화하여 게이트웨이로 보낸다. 게이트웨이는 WTLS 암호메시지를 복호화와 암호화를 거쳐 TLS 암호메시지로 변환하지 않고, WTLS로 복원한 TLS 암호메시지를 바로 웹 서버에 전송함으로써 메시지 원본의 노출을 방지하고 있다. 그러나, 이 프로토콜은 무선단말기에 WTLS 뿐 아니라 TLS 기능도 구현해야 하며, 또한 무선단말기에서 암호화/복호화를 두 번 수행하기 때문에 처리 시간이 많이 걸린다.

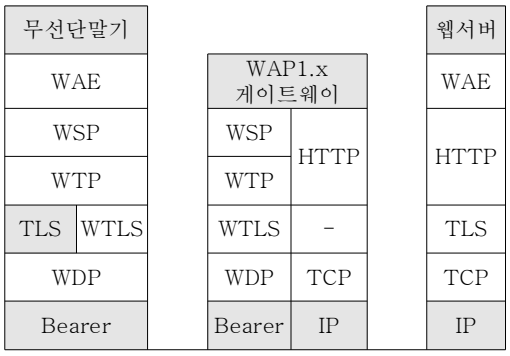

그림 3. ITLS 시스템 구성 및 프로토콜 스택

2.4 데이터 압축을 활용한 WAP2.0 프록시 아키텍처

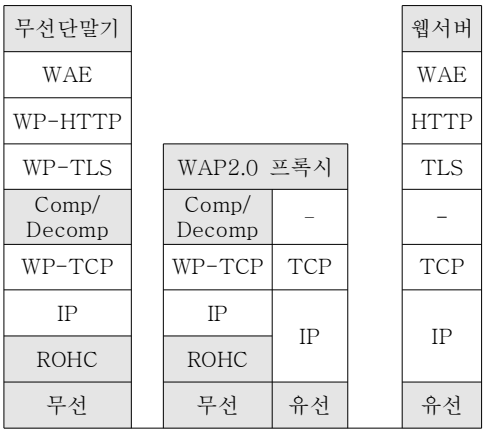

그림 4. 압축 프록시를 가진 WAP2.0 시스템 구성 및 프로토콜 스택

Yin은 WAP2.0의 단점을 해결하기 위해 무선단말기와 웹 서버 사이에 데이터 압축 기능을 가진 WAP2.0 프록시 아키텍처를 제안하였다[8][9]. 무선구간에서 전송되는 데이터를 압축함으로써 무선통신 트래픽을 최소화하고, 프록시에서 프로토콜 변환이 필요하지 않으므로 WAP1.x의 메시지 노출 문제를 해결하고 있다. 그림 4는 이 기법의 시스템 구성과 프로토콜 스택을 보여 준다. 그림에서 보듯이 기본적으로 WAP2.0의 프로토콜 스택과 같으나 무선단말기와 프록시에는 무선구간에서 효율적으로 데이터를 전송하기 위해 압축/복원을 수행하는 Comp/Decomp와 ROHC (Robust Header Compression) 계층이 추가되었다. 따라서, 무선단말기에는 WAP2.0의 프로토콜 스택 외에 압축/복원 기능을 추가로 구현해야 하므로 무선단말기에

많은 부담을 준다.

2.5 WTLS와 TLS의 비교

WTLS는 ECC 알고리즘, 간결한 인증서, 짧은 보안 파라미터 등을 사용하여 TLS를 제한적인 자원을 가진 무선단말기에 맞도록 최적화한 것이다[2]. 표 1은 Vogler가 수행한 WTLS와 TLS의 성능 분석 결과를 보여 준다[16]. TLS는 3G 단말기의 대표적인 모델로 20 MIPS CPU, 20 MB 플래시 메모리, 1MB RAM, 14.4 kbps에서 384 kbps까지의 대역폭을 가진 시스템에서 측정한 것이고, WTLS는 2G 단말기의 대표적인 모델로 5 MIPS CPU, 100 KB 플래시 메모리, 100 KB RAM, 100 bps에서 9.6 kbps의 대역폭을 가진 시스템에서 측정한 것이다. ECC를 사용하는 WTLS를 고려하면 테스트를 실행한 무선단말기 테스트베드의 성능차가 4배 이상임에도 불구하고 종단간 메시지 전송 성능의 차이는 크게 차이가 나지 않아 WTLS가 TLS에 비해 경량화되어 있음을 확인할 수 있다.

표 1. TLS와 WTLS의 성능 분석 결과

단위 : ms

프로토콜	서버 인증	서버 및 클라이언트 인증		응 용 데이터
	RSA	RSA	ECC	
3G & TLS	1365	3851	2050	617
2G & WTLS	1886	9660	2440	982

3. 제안된 WAP2.0 프록시 모델 및 보안 프로토콜

3.1 WAP2.0 프록시 모델

WAP1.x 게이트웨이에서의 메시지 노출 문제를 해결하고, 제한적인 자원을 가진 무선단말기 환경에서 종단 간 보안을 지원하기 위해 본 논문에서는 그림 5와 같은 WAP2.0 프록시 모델을 제시한다. 그림에서 보듯이 종단 간에 전송되는 메시지를 보호하기 위해 프록시와 WAP2.0 무선단말기 사이의 무선 구간에서는 WTLS 프로토콜을 적용하고, 프록시와 웹 서버 사이의 유선 구간에서는 TLS 프로토콜을 적용한다. 이렇게 하기 위해 무선단말기에는 WP-TLS 대신 WAP1.x에서 채택한 보다 경량의 WTLS 프로토콜을 사용한다. 웹 서버에는 TLS와 WTLS 두 프로토콜을 모두 설치하여 무선단말기로 송수신되는 메시지에 대해 두 번의 암호화(혹은 복호화)를 수행하도록 한다. 프록시에는 TLS를 설치하여 웹 서버에서 TLS 방식으로 암호화되어 전송된 메시지를 복호화한 결과의 메시지(WTLS 방식의 암호문)를 평문으로 복원하지 않고 바로 무선단말기로 전달한다. 또한, 무선단말기로부터 WTLS 방식으로 암호화되어 전송된 메시지를 평문으로 복원하지 않고, 이 암호 메시지를 TLS로 다시 암호화하여 웹 서버로 전달한다. 따라서, 제안된 프록시 모델은 WAP1.x 게이트웨이와 달리 WTLS와 TLS 간 프로토콜 변환이 필요 없으므로 메시지 평문을 노출하지 않는다.

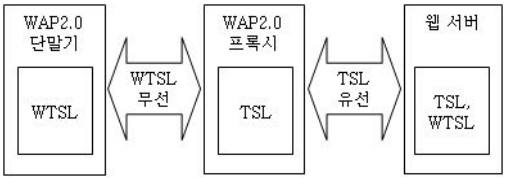

그림 5. 종단간 보안을 지원하는 WAP2.0 프록시 모델

그림 6은 그림 5의 프록시 모델을 채택한 WTLSW (WTLS-TLS at Web server) 프로토콜의 시스템 구성과 각 구성 요소들이 채택하고 있는 프로토콜 스택을 보여준다. 그림에서 보듯이 웹 서버에는 WTLS 계층이 추가되고, 프록시는 TLS 계층을 지원하여 무선단말기와 웹 서버간 암호 메시지를 중계하는 기능을 수행한다. 무선단말기에는 WAP2.0의 WP-TLS 계층을 WTLS 계층으로 대치하였다.

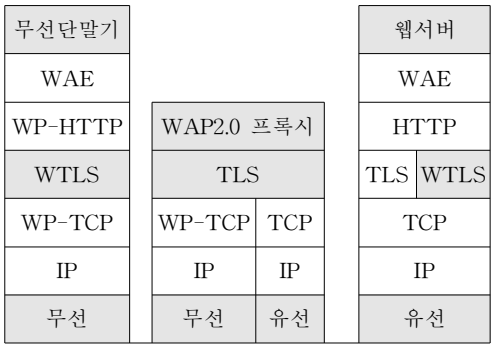

그림 6. WTLSW 시스템 구성 및 프로토콜 스택

3.2 WTLSW 핸드쉐이크 프로토콜

WTLSW 레코드 계층 위에서 동작하는 WTLSW 핸드쉐이크(handshake) 프로토콜은 무선단말기와 웹 서버 사이의 데이터 전송 세션에서 사용되는 세션키, 암호 알고리즘, 인증서 등 보안

파라미터들을 상호 설정하기 위한 프로토콜이다. WTLSW에서는 무선단말기와 웹 서버 사이의 보안 파라미터 설정을 위해 WTLS 핸드쉐이크 프로토콜[2]을 사용하고, WAP2.0 프록시와 웹 서버 사이의 보안 파라미터 설정은 TLS 핸드쉐이크 프로토콜[14]을 사용한다. WTLS와 TLS의 핸드쉐이크 프로토콜은 기본적으로 같으며, 단지 각 파라미터의 크기에서 차이가 있다. 그림 7은 WTLSW의 전체 핸드쉐이크 프로토콜의 메시지 흐름을 보여 준다.

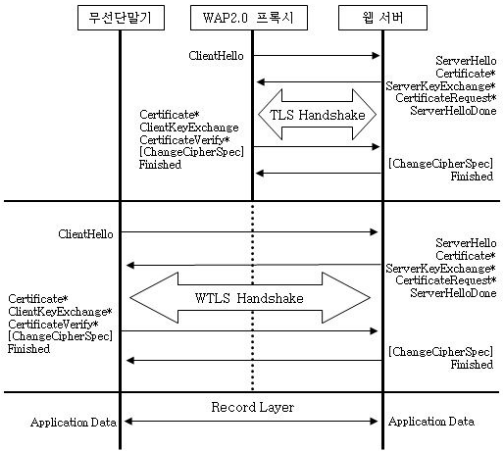

그림 7. WTLSW의 전체 핸드쉐이크 프로토콜
(* : 상황에 따라 선택적인 메시지)

그림 7에서 보여주는 WTLSW 핸드쉐이크 프로토콜은 무선단말기와 웹 서버간, 프록시와 웹 서버간 응용 데이터 전송을 위한 세션키를 계산하기 위해 다음의 TLS(혹은 WTLS) 핸드쉐이크 과정을 수행한다.

1. 사용할 보안 알고리즘 합의를 위한 Hello 메시지들과 보안 파라미터 계산에 필요한 난수 값들을 교환
2. 클라이언트와 서버가 pre-master secret을 생성하는데 필요한 보안 파라미터를 교환
3. 클라이언트와 서버가 상호 인증하는데 필요한 인증서와 보안 정보를 교환
4. 1과 2에서 교환한 난수와 pre-master secret으로부터 master secret을 생성하고 서로 확인
5. 레코드계층에서 사용할 세션키를 생성하여 제공
6. 마지막으로, 클라이언트와 서버가 보안 공격을 받지 않고 동일한 보안 파라미터를 생성했음을 검증

3.3 WTLSW 레코드 프로토콜

핸드쉐이크 프로토콜에서 계산된 세션키를 사용하여 응용 데이터에 대한 실질적인 보안 서비스를 제공하는 것이 레코드 프로토콜이다. 그림 8은 무선단말기와 웹서버 사이에 응용 데이터의 흐름을 보여 준다. 그림 8에서 사용하는 기호의 의미는 다음과 같다.

K_m : 무선단말기와 웹 서버간 세션키
K_p : 프록시와 웹 서버간 세션키
$W.E_K(M)$: 키 K로 메시지 M을 WTLS 방식으로 암호화
$W.D_K(C)$: 키 K로 암호문 C를 WTLS 방식으로 복호화
$T.E_K(M)$: 키 K로 메시지 M을 TLS 방식으로 암호화
$T.D_K(M)$: 키 K로 암호문 C를 TLS 방식으로 복호화

그림에서 보듯이 웹 서버는 TLS와 WTLS 방식으로 각각 1회씩 암호화(혹은 복호화)를 2회 수행함으로써 프록시에서의 메시지 노출을 방지하고 있다. 프록시에서는 프로토콜 변환 없이 수신한 메시지에 대해 TLS 방식으로 암호화(혹은 복호화)를 수행하여 각각 웹 서버(혹은 무선단말기)에게 메시지를 전달한다. 즉, 프록시에서는 WTLS 방식의 암호문에 대해서는 복호화를 수행하지 않는다. 그림에서 메시지 인증을 위한 HMAC 적용 등 자세한 내용은 생략하였다.

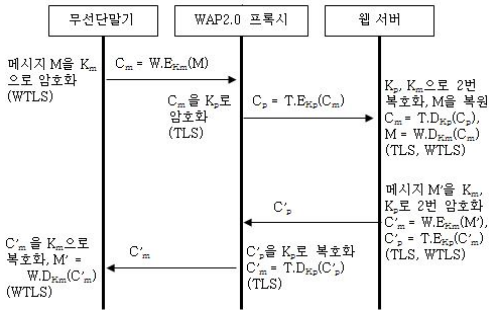

그림 8. WTLSW 응용 데이터 흐름도

4. WTLSW 프로토콜의 분석 및 평가

본 논문에서 제안한 WTLSW에서 채택한 WTLS는 2.5절에서 언급했듯이 ECC 알고리즘, 간결한 인증서, 짧은 보안 파라미터 등을 사용하여 TLS를 제한적인 자원을 가진 무선단말기에 맞도록 최적화한 것이다. 표 2는 본 논문에서 제안한 WTLS 프로토콜과 기존에 제시된 방식들을 보안성능 측면에서 분석 비교한 것이다.

암호화/복호화 횟수를 살펴보면 제안된 프로토콜은 메시지 송수신 시 무선단말기에서 WTLS 방식으로 암호화(혹은 복호화)를 1회만 수행하여 메

시지를 빠르게 처리할 수 있다. 따라서, 낮은 CPU 성능, 적은 용량의 메모리 및 배터리를 가진 무선단말기 환경에서 종단간 보안을 제공하는데 적합하다고 할 수 있다. 이에 비해 프록시에서는 TLS 방식의 암호화(혹은 복호화)를 1회 수행하고, 웹 서버에서는 WTLS 방식 1회, TLS 방식 1회 등 총 2회의 암호화(혹은 복호화)를 수행해야 하기 때문에 다른 프로토콜에 비해 프록시와 웹 서버의 부담을 증가시킨다.

표 2에서 보듯이 WAP1.x 프로토콜을 제외하고 모든 프로토콜들이 WAP1.x 게이트웨이 혹은 WAP2.0 프록시에서의 메시지 노출문제를 해결하고 있다. 또한, WAP1.x와 WTLSW를 제외한 다른 세 프로토콜들은 모두 WTLS보다 크기가 큰 TLS 모듈 외에 WTLS나 혹은 압축/복원 모듈을 추가로 무선단말기에 탑재해야 하므로 무선단말기의 많은 자원을 요구한다.

결론적으로 제안된 WTLSW는 WAP2.0 프록시와 웹서버의 부담을 증가시키는 문제가 있으나, WAP2.0 프록시에서 메시지 원본을 노출하지 않으면서 제한적인 자원을 가진 무선단말기에 활용할 수 있는 하나의 방안이 될 수 있다.

표 2. 제안된 프로토콜의 보안성 및 성능 비교 (* : Data Compression)

		WAP1.x	ITLS	WAP 2.0	WAP 2.0 DC*	WTLSW
암호화/복호화 횟수	무선단말기	WTLS 1	WTLS 1 TLS 1	TLS 1	TLS 1	WTLS 1
	게이트웨이/프록시	WTLS 1 TLS 1	WTLS 1	-	-	TLS 1
	웹 서버	TLS 1	TLS 1	TLS 1	TLS 1	WTLS 1 TLS 1
게이트웨이/프록시에서의 메시지 노출		노출	노출 안됨	노출 안됨	노출 안됨	노출 안됨
무선단말기 탑재 모듈		WTLS	WTLS, TLS	TLS	TLS, 압축/복원	WTLS

5. 결론

본 논문에서는 낮은 CPU 성능, 적은 용량의 메모리 및 배터리 등 제한된 자원을 가진 무선단말기의 자원 소모를 가능한 줄이면서 종단간 보안을 지원하기 위한 WTLSW 프로토콜과 WAP2.0 프록시 모델을 제안하였다. WTLSW 프로토콜은 WAP2.0의 무선 구간에서 WTLS 보안 프로토콜을 채용하여 무선단말기에서의 응용 처리 시간과 자원의 소모를 감소시켰다. 또한, 무선단말기를 위해 WTLS 방식으로 메시지를 암호화하고 WAP2.0 프록시를 위해 다시 TLS 방식으로 암호화 하는 등 메시지를 송수신할 때 두 번의 암호화/복호화를 웹 서버에서 수행함으로써 WAP2.0 프록시에서의 메시지 노출을 방지하고 있다. 제안된 WTLSW 프로토콜 및 WAP2.0 프록시 모델은 상대적으로 TLS에 비해 보안성이 떨어지는 WTLS를 채택함으로써 TLS를 채택한 시스템에 비해 보안 공격에 취약할 수 있으며, 프록시와 웹 서버의 부담을 증가시키는 문제가 있으나, 자원의 제약을 가진 무선단말기의 부담을 줄이면서 종단간 보안을 지원할 수 있는 하나의 방안으로 사용할 수 있다.

참 고 문 헌

[1] WAP Forum, *Wireless Application Protocol Architecture Specification*, Nov 1999.

[2] WAP Forum, *Wireless Transport Layer Security Protocol Specification*, Nov 1999.

[3] WAP Forum, *WAP Architecture Specification*, version 12-July-2001, http://www.wapforum.org/what/technical.htm.

[4] WAP Forum, *WAP 2.0 technical White Paper*, Jan 2002.

[5] WAP *Forum, Wireless Application Protocol TLS Profile and Tunneling Specification*, version 11-April-2001.

[6] WAP Forum, *Wireless Profiled TCP*, version 31-March-2001.

[7] WAP Forum, *Wireless Profiled HTTP*, version 29-March-2001.

[8] Zhanping Yin and Victor C. M. Leung, "A Proxy Architecture to Enhance the Performance of WAP 2.0 by Data Compression," *Proc. of Wireless Communications and Networking Conf. 2003,* Vol. 2, pp. 1322-1327, IEEE, Mar 2003.

[9] Zhanping Yin and Victor C. M. Leung, "A Proxy Architecture to Enhance the Performance of WAP 2.0 by Data Compression," *EURASIP Journal on Wireless Communications and Networking*, Issue 1, pp.57-66, Hindawi Publishing Corp, Mar 2005.

[10] Baris Kayayurt and Tugkan Tuglular, "End-to-End Security Implementation for Mmobile Devices using TLS Protocol," *Journal in Computer Virology*, Vol. 2 No. 1, pp.87-97, Springer Paris, Aug 2006.

[11] M. Badra and A. Serhrouchni, "A New Secure Session Exchange Key Protocol for Wireless Communications," *Proc. of the 14th IEEE 2003 Int'l Symposium on Personal, Indoor and Mobile Radio Communications*, Vol. 3, pp.2765-2769, IEEE, Sep 2003.

[12] N.C. Juul and N. Jørgensen, "Security Issues in Mobile Commerce using WAP." *Proc. of 15th Bled Electronic Commerce Conference*, e-Reality: Constructing the e-Economy, Bled, Slovenia, Jun 2002.

[13] Eun-Kyeong Kwon, Yong-Gu Cho, Ki-Joon Chae, "Integrated Transport Layer Security : End-to-End Security Model between WTLS and TLS," *Proc. of the 15th International Conference on Information Networking*, pp.65-71, IEEE Feb 2001.

[14] T. Dierks and C. Allen, *The TLS Protocol Version 1.0*, RFC2246, Jan 1999.

[15] 최진규, 이헌길, "무선 환경에서 안전한 종단간 보안을 제공하는 AWTLS 프로토콜," *정보통신 논문지 6집*, pp.46-51, 강원대 정보통신연구소, 2002년 2월.

[16] Dean Vogler, "Security Issues in Wireless Environments," *Talk in 2000 Fall CEPS Conference*, Oct 2000, http://www.iccip.csl.uiuc.edu/conf/ceps/2000/vogler.pdf. Proce-ssing, A Remote Sensing Perspective, Second Edition", *Prentice Hall*, 1996.