# 무선 인터넷 프로토콜 시큐리티

신 °원†, 이경현‡
† 부경대학교 전자계산학과, ‡ 부경대학교 전자컴퓨터정보통신공학부

# Wireless Application Protocol and Its Security

Weon °Shin†, Kyung-Hyune Rhee‡
† Dept. of Computer Science, PKNU
‡ Division of Electronics, Computer and Information Communication Engineering, PKNU

요 약

본 논문에서는 사실상 무선 인터넷 프로토콜의 표준인 WAP(Wireless Application Protocol)의 구조 및 동작을 살펴보고, 안전한 통신을 위한 WTLS(Wireless Transport Security) 프로토콜 동작 및 그 취약성에 대해 논의한다. 또한 WAP 및 HTTP 상에서 안전한 유·무선 통합 서비스를 위한 여러 방안을 살펴보고 결론을 유도한다.

## 1. 서론

컴퓨터 보급의 확대와 정보 통신 기술의 발달로 인하여 다양한 네트워크가 구성되고 있으며, 새로운 기술을 도입한 각종 서비스들이 등장하고 있다. 특히, 인터넷 기술을 기반으로 서비스 제공을 위한 상용 및 공개 서버가 구축되고 있으며 이를 효과적으로 사용하기 위한 많은 클라이언트 시스템이 구성되고 있다. 최근 전자상거래 확산에 힘입어 상용 네트워크가 구성되고 있으며 정부·연구기관, 대학 등을 중심으로 인터넷 기술을 활용하여 업무, 교육, 연구에 적용하고 있다.

최근에는 기존 인터넷 환경에 무선 통신을 결합한 무선 인터넷 및 네트워크 기술이 등장하여 새로운 시장을 형성하고 있다. IMT-2000 서비스의 상용화, PDA(Personal Data Association) 및 HPC(Handheld PC)를 이용한 이동 컴퓨팅 기술, 컨텐츠 표현을 위한 XML(eXtensible Markup Language) 기반의 WML(Wireless Markup Language), Bluetooth 등의 무선 홈네트워크 기술 등에 힘입어 세계 어디서나 인터넷에 접속하여 원하는 정보를 검색하거나 서비스를 받을 수 있는 무선 인터넷 환경이 도래하고 있다. 여러 조사 기관에 따르며 무선 인터넷을 사용하는 단말기가 2002년에는 6억개 이상이 될 것으로 예측하고 있으며[], 1999에 7%에 불과하던 무선 데이터 통신 이용자가 2002년에는 32%, 2004년에는 61%로 예측하고 있다[]. 이미 네트워크 기술의 유·무선 통합은 빠른 속도로 이루어지고 있으며 이미 인터넷 기술의 대세로서 굳어져가고 있다.

그러나 무선 인터넷 환경은 기존의 유선 인터넷 환경에 비교하여 전송 속도, 전력 소모량, 메모리 크기, 사용자 인터페이스, 안전성 등에서 많은 취약성을 가지고 있으므로 유선 인터넷의 환경을 그대로 적용시키기에는 무리가 있는 것이 사실이다. 따라서, 기존의 표준을 그대로 수용하면서 무선 인터넷 환경에 적합한 프로토콜인 WAP(Wireless Application Protocol)이 개발되었다. 또한, 무선 인터넷 환경 특성상 이동성이 상당히 중요한 위치를 차지하고 있으나 이로 인해 발생하는 여러 시큐리티 취약성도 함께 존재하므로 기존 유선 인터넷과 연동이 가능한 WTLS(Wireless Transport Layer Security)가 등장

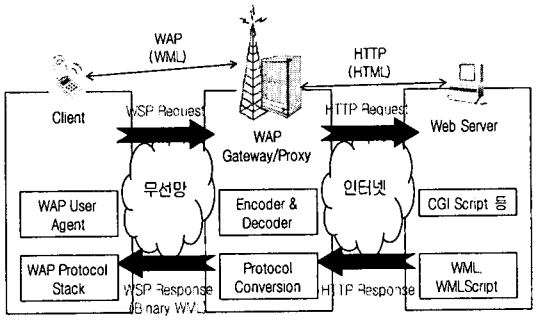
하게 되었다.

본 논문에서는 무선 인터넷을 위한 프로토콜인 WAP과 보안 프로토콜인 WTLS의 동작을 분석하고 가능한 시큐리티 취약성을 살펴본다.

2장에서는 네트워크를 통한 시스템 침입 단계에 대해서 논하고, 3장에서는 네트워크 및 시스템 정보수집 과정을 중심으로 시스템 침입 및 방어 방법을 살펴본다. 마지막으로 4장에서는 결론을 유도하고 향후 연구과제에 대하여 기술한다.

## 2. WAP 프로토콜 스택

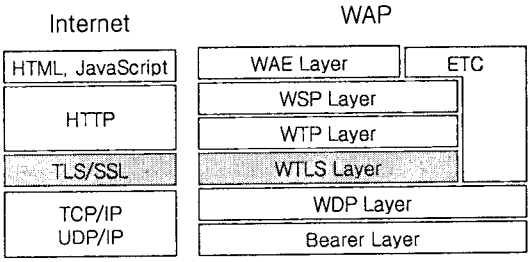
현재 WAP은 무선 이동 통신 기술의 여러 회사 Phone.com, Ericsson, Motorola, Nokia 등 전세계 200여 업체가 참여중인 WAP Forum에서 제정한 무선 통신 프로토콜로 기존의 유선 인터넷과 유사하게 동작한다. WAP에서는 Standard Naming Model, Contents Type, Markup Language, Protocol에 대한 메커니즘을 제공한다. <그림 1>은 유선 인터넷 망과 연동한 WAP의 동작 방식을 보여준다.




<그림 1> WAP의 동작 방식

WAP은 무선 환경에 적합하도록 구성되어 있지만 근본적으로는 기존 클라이언트/서버 환경에 기반하므로 유선 인터넷과 유사한 구조를 가진다. 특히, 프로토콜 스택을 두어 물리적으로는 이동통신 사업자에서부터 어플리케이션을 사용하는 일반 사용자에 이르는 다양한 환경을 수용하도록 하고 있다. 즉, 각 계층은 자신의 상하위계층에만 접근하도록 하여 독립적으로 구현함으로써 보다 유연성 있는 동작 방식들을 제공하고 있다. WAP은 하위 계층에서부터 Bearer, WDP, WTLS, WTP, WSP, WAE 계층을 두고 있다. 무선 인터넷 환경은 네트워크 상의 제한으로 인한 지연 시간이 길고 좁은 대역을 가지는 환경이므로, WSP, WTP, WDP 계층에서 지연을 고려한 연결지속(Long-lived Session), 신뢰/비신뢰(Reliable/Unreliable) 데이터 통신 구현으로 인한 안정적인 네트워킹 지원, WTLS의 무선 인터넷 통신 보안, Bearer의 서로 다른 전송 시스템 지원, 서비스 및 어플리케이션간의 상호동작 등을 해결하고 있다. <그림 2>는 유선 인터넷 계층에 해당하는 WAP 계층을 보여 주고 있다

.




<그림 2> WAP의 구조

(1) Bearers

WAP은 다양한 전송 서비스(Bearer Service) 위에서 작동 가능하도록 설계되었으므로 무선 시장의 다양한 전송 서비스를 포함한다. 현재 GSM, CDMA, PHS, IS-136, IMT-2000 등을 지원하고 있다.

(2) WDP(Wireless Datagram Protocol)

WDP는 무선 네트워크 용 데이터 전송 프로토콜로 다양한 네트워크 토폴로지 지원한다. 물리적 네트워크에 상관없이 작동 가능하고, 상위 계층에 대해 일관된 인터페이스 제공으로 무선 네트워크 구성에 관계없이 독립적인 기능 수행할 수 있다.

(3) WTLS(Wireless Trusted Layer Security)

무선 환경을 위한 보안 프로토콜로 SSL(Secure Socket Layer) 기반의 산업 표준인 TLS(Transport Layer Security)의 변형이다. WAP 전송 프로토콜과 함께 사용하도록 설계되어 좁은 대역에서도 사용가능하도록 최적화되어 있다. 데이터에 대한 무결성, 비밀성, 신뢰성을 보장하고, 어플리케이션은 필요에 의해 WTLS의 항목들을 활성화 또는 비활성화가 가능하다.

(4) WTP(Wireless Transaction Protocol)

이동 네트워크 환경에서 구현에 적합하도록 구성된 트랜잭션 프로토콜로, 인터넷 접속 단말기에서의 단순한 트랜잭션을 위한 프로토콜로 신뢰할 수 없는 단방향 요청, 신뢰할 수 있는 단방향 요청, 신뢰할 수 있는 양방향 요청을 지원한다.

(5) WSP(Wireless Session Protocol)

세션 서비스를 위한 인터페이스로, WTP 위에서 동작하는 연결형 서비스와 WDP 위에서 동작하는 비연결형 서비스로 구성되고 푸시, 중지, 재생 기능을 포함한다. 낮은 대역과 긴 응답시간을 지닌 네트워크에서 동작하도록 최적화되어 있다.

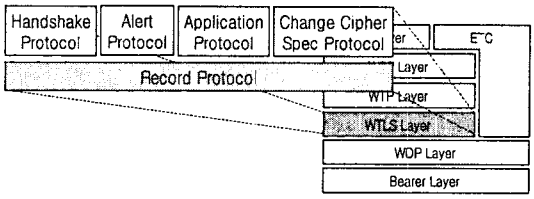
**(6) WAE(Wireless Application Environment)**

어플리케이션 환경 설정을 위한 계층으로 정의되어, 서비스 제공자와 개발자가 상호 작용할 수 있는 환경을 제공하여 다양한 무선 환경에서 어플리케이션과 서비스를 효율적으로 구축하도록 해준다. WAP Browser, WML, WMLScript, WTA(Wireless Telephony Application), WTAI(Wireless Telephony Application Interface) 등을 포함하고 운영체제 디바이스, WAP 네트워크, 사용자 브라우저 등을 지원한다.

## 3. WTLS 계층

### 3.1 WTLS의 동작

WAP Forum에서는 TCP/IP의 SSL(Secure Socket Layer)과 TLS(Trusted Layer Security)를 기반으로 하는 별도의 무선 환경에 적합한 프로토콜을 정의하는 작업을 진행하고 있는데, 그 산물이 바로 WTLS이다. 즉, WTLS는 유선 인터넷 프로토콜을 무선 환경에서 사용할 경우에 발생하는 문제들을 해결하고, 기존 인터넷 중심의 데이터 서비스를 무선 환경에서 효율적으로 처리하기 위해 제안된 프로토콜이다. 따라서, 통신 하는 두 어플리케이션 사이에 안전한 채널을 형성하고 통신 내용의 안전을 보장한다. 또한, WTLS는 WDP와 WTP 사이에서 수행되기 때문에 특정 어플리케이션에 종속되지 않으므로 WAP에서 사용되는 모든 어플리케이션 지원이 가능하다. 현재 WTLS는 비밀성, 사용자 인증, 데이터 무결성은 제공하지만 부인 방지는 제공하지 않는데, 세부적으로 살펴보면 핸드셰이크를 통해 키를 교환하고 DES, IDEA를 사용한 암호화하는 두 어플리케이션간의 비밀성 서비스, RSA 암호와 X.509 인증서를 이용한 상호 인증하는 클라이언트와 서버간의 상호 인증, MAC을 사용한 데이터 무결성을 보장하는 메시지 무결성 서비스이다. 부인 방지는 어플리케이션 계층에서 제공하고 WMLScript Crypto Library의 전자 서명을 이용하여 해결한다. <그림 3>은 WAP에서 WTLS의 위치와 구조를 보여주고 있다. Handshake Protocol, Alert Protocol, Change Cipher Spec Protocol은 SSL/TLS와 마찬가지로 WTLS의 동작에 대한 관리를 위해 사용되며, 실질적인 보안 서비스는 Record Protocol에서 제공한다. 클라이언트와 서버가 WTLS를 이용해 연결을 할 경우, 먼저 Handshake Protocol을 수행하여 한 세션 동안 보안 서비스 제공에 사용되는 세션키, 암호 알고리즘, 인증서 등과 같은 암호 매개변수를 서로 공유하고, 여기에서 생성된 세션 정보는 Record Protocol에서 보안 서비스를 제공하는데 이용한다.




<그림 3> WTLS의 구조

그 중 Handshake Protocol은 Record Protocol에서 사용될 보안 파라미터 결정, 클라이언트와 서버 인증, 오류 처리 등에 이용되는데, 다시 Handshake Protocol, Alert Protocol, Change Cipher Spec Protocol 등 3개의 하위 프로토콜로 구성된다. Alert Protocol에서는 오류 메시지가 정의되며, 클라이언트나 서버에서 오류가 발생했을 때 오류 메시지를 보내서 오류가 발생한 사실을 상대방에게 알리는 역할을 수행하고, Change Cipher Spec Protocol은 하나의 메시지로 구성되며, 이 메시지가 전송된 이후의 메시지는 새로운 보안 파라미터에 의해서 암호화되어 전송됨을 알리는 역할을 수행한다. Handshake Protocol에서 교환되는 정보는 Session Identifier, Protocol Version, Peer Certificate, Compression Method, Cipher Spec, Master Secret, Sequence Number Mode, Key Refresh, Is Resumable 등이다.

### 3.2 WTLS의 취약성 분석

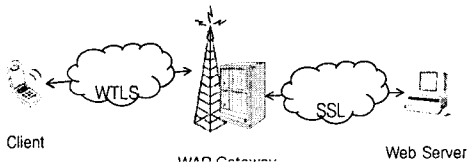
WTLS의 Handshake Protocol은 Full Handshake, Abbreviated Handshake, Optimized Full Handshake의 3가지로 구분된다. 이 중 Full Handshake와 Abbreviated Handshake는 SSL/TLS에서도 사용되는 방법으로 Full Handshake는 새로운 세션을 시작할 때 사용되고, Abbreviated Handshake는 기존의 세션을 재개해서 다시 이용할 경우에 사용되며, Optimized Full Handshake는 WTLS에서 새롭게 추가된 것으로 서버는 클라이언트 인증을 위해 클라이언트의 인증서를 요청하지 않고, 서버 내에 보관하거나 저장소를 통해 제공되는 클라이언트 인증서를

통해 클라이언트 인증을 수행한다.

WTLS는 SSL과 TLS를 기반으로 무선 네트워크 환경에 적합하도록 수정하는 과정에서 몇가지 취약성이 존재한다. 첫째, Change Cipher Spec 메시지 손실로 인한 공격으로 공격자가 통신 상에서 Change Cipher Spec 메시지를 가로채어 제거하더라도 클라이언트 및 서버는 그 사실을 알지 못한채 비밀키 암호로 NULL을 선택하고 데이터 무결성 서비스만을 제공하는 WTLS 연결을 설립하게 된다{}. 둘째, Master Secret을 이용한 공격이다. SSL 및 WTLS에서 매우 중요한 정보로써 네트워크를 통해 전송하지 않고 클라이언트와 서버 각각에서 생성하도록 하지만 Abbreviated Handshake에서는 이전 세션의 Master Secret을 그대로 사용하여 여러 메시지와 Finished 메시지를 전송한다. 이 Finished 메시지는 생성 방법이 알려져 있으므로 클라이언트를 가장한 공격자가 요청하여 받을 수 있으므로 이를 이용하여 기지 평문 공격을 통하여 공격할 수 있는 취약점을 가진다. 셋째, Handshake Protocol 설계상의 취약점으로 인하여 공격자에 의한 단순한 데이터 도청 및 클라이언트 또는 서버의 비밀키 노출시 위장을 통한 수정, 변조가 사실상 가능하다. 키교환시 서버의 인증만을 수행하는 경우 man-in-the-middle attack을 통하여 클라이언트 및 서버의 위장이 가능하다.

## 4. 여러 가지 WAP 보안 방안

실제 WAP 구현에서 휴대용 단말기와 웹서버 사이에는 WAP Proxy인 WAP Gateway가 존재하는데, 이 WAP Gateway는 WAP 프로토콜과 HTTP 프로토콜을 중간에서 번역하는 기능을 수행함으로써 컨텐츠나 어플리케이션이 표준 웹서버에 존재할 수 있게 하고 CGI 스크립트와 같은 기존의 웹기술을 그대로 이용할 수 있는 장점이 있다. 그리고 안전한 통신을 하기 위해 <그림 4>와 같은 방식으로 통신하는데 WAP에서는 WTLS를, HTTP에서는 SSL을 적용하여 구현하고 있다.




<그림 4> 기존의 WAP 보안

그러나, 이 방식에서 WAP Gateway는 WTLS 또는 SSL을 복호화하여 다시 암호화를 수행하기 때문에 본래의 평문 정보를 얻는 것이 가능하므로 종단간 보안(End-to-End Security) 문제가 발생하여 관리자 및 WAP Gateway 공격시 정보가 누출될 수 있는 취약점을 가진다. 이를 보완하기 위한 방안으로는 WAP Gateway는 단순한 중계 역할만 담당하고 유·무선 전 구간을 SSL을 이용하여 정보보호 서비스 제공하는 SSL 또는 WTLS를 이용한 방식, 웹서버 앞에 또 하나의 WAP Gateway 설치하는 Secure WAP Gateway를 이용한 방식, 클라이언트와 서버는 전용 프로그램을 설치하고 이를 통해 통신함으로써 종단간 보안을 해결하는 어플리케이션을 이용한 방식으로 나뉜다. 방식에 따라 장·단점이 존재하며 현재 여러 방안이 서비스 및 환경에 따라 사용되고 있고 앞으로도 새로운 보안 방식이 등장할 예정이다.

## 5. 결론

본 논문에서는 무선 인터넷 프로토콜의 사실상 표준인 WAP의 구성에 대하여 살펴보고, 안전성 보장을 위한 WTLS를 분석하였다. WAP 보안을 위한 무선 네트워크 구조를 설명하였고 취약성을 논의하였다.

오늘날 다양한 사용자의 요구에 맞추어 인터넷을 기반으로 하는 수많은 서비스가 등장하였다. 그 중 무선 인터넷 기술은 기존 유선 인터넷과의 통합을 시도할 뿐만 아니라 새로운 시장으로까지 인식되고 있다. 따라서 무선 환경에서 기존 유선 환경과 마찬가지로 다양한 응용 서비스에 응용하기 위해서는 정보보호 기술의 적용이 필수적이며 심도있게 논의되어야 하는 분야이다.

## 참 고 문 헌

[1] 문종철, 원유재, 유이중, "WTLS handshake 프로토콜의 분석", WISC 2000, pp.253~266, 2000.

[2] J.Sami, L.Jouni, "Security in the WTLS", 1999.

[3] S.Markku-Juhani, "Attacks Against The WAP WTLS Protocol"

[4] http://www.wapforum.org