제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

종단간 보안으로 개선한 e-WAP 에서의 보안모델

원대희*, 추승우, 오정석, 이재영
한 림 대 학 교 컴 퓨 터 공 학 과
e-mail : dhwon@center.cie.hallym.ac.kr

Security Model Improved by End-to-end Security in e-WAP

D.H Won* S.W.Chu J.S.Oh J.Y. Lee
* Dept. of Computer Engineering, Hallym University

요 약

기존의 WAP 게이트웨이 모델에서의 게이트웨이는 많은 기능을 수행하였다. 이에 따른 게이트웨이 오버헤드가 증가하는 문제를 지니고 있기 때문에 이러한 문제를 해결하기 위해 상대적으로 수행 기능이 적고 각 content 제공자에 따라 나누어있는 Web 서버에 게이트웨이의 일부 기능을 이식하여 설계한 e-WAP 모델을 제시하였다. 하지만 e-WAP 의 보안 모델은 이전 WAP 게이트웨이 모델에서 사용되는 보안 방식을 사용하였기 때문에 종단간 보안 (end-to-end Security)을 보장하지 못하는 기존 WAP 의 보안 문제를 그대로 가지고 있다. 이에 본 논문은 기존의 SSL 과 WTLS 를 이용한 암호화 통신 프로토콜을 이용한 보안 모델에 서버와 무선 단말기 사이에 전송되는 데이터에 대해 암호화 한번 더 수행하여 종단간 보안을 보장하는 새로운 e-WAP 보안 모델을 제안하고자 한다.

1. 서론

무선 인터넷 이용자들은 무선 단말기를 통한 인터넷 및 전자상거래, 데이터 전송, 그리고 계좌이체 등의 은행 서비스 이용에 이르기까지 폭넓은 서비스를 원하고 있으며 관련 업체들 역시 이에 대한 서비스를 제공하기 위하여 현재 활발한 연구가 진행 중이다. 또 한 무선 단말기에 맞는 프로토콜과 기술이 점점 발전되어 등장하고 있어, 무선 인터넷 사용의 특성과 편리성에 대한 인식이 급속도로 확산되고 있다.

무선 인터넷에서 전자상거래를 비롯한 데이터 서비스가 성공적으로 제공되기 위해서는 반드시 해결되어야 할 문제가 바로 보안이다. 보안 기술은 기존의 인터넷 기술에서도 가장 중요한 요소로 인식되고 있다. 특히 증권거래나 경매, 은행에서의 예금 계좌 이체등과 같은 분야에 있어서 유선 인터넷과 마찬가지로 무선 인터넷이 안전한 전자상거래 서비스를 제공하기 위해서는 통신 정보에 대한 기밀성, 개체 인증기능 등의 정보 보호를 위한 기능과 부인 방지 기능 등을 제공해야 한다. 하지만 무선 인터넷은 유선 인터넷과는 달리 여러가지 제약성을 가지고 있다. 무선 단말기의 경우 PC 와 같은 계산 능력과 저장 능력을 가지지 않으며 무선 통신은 유선 통신보다 낮은 데이터 전송률과 대역폭을 가진다. 이러한 무선 환경의 제약성을 극복하기 위해 여러 무선 인터넷 기술들이 개발되었다. 현재 가장 보편적으로 사용되는 무선 인터넷 프로토콜인 WAP 는 보안 이외에도 여러가지 문제를 지니고 있는 상황이다. 따라서 기존의 WAP 프로토콜 플랫폼을 개선한 e-WAP 모델을 제안하였다 [1].

이전의 e-WAP(enhanced-Wireless Application Protocol)은 게이트웨이의 몇몇 기능을 e-WAP 서버로 이전함으로써 성능을 향상시키는 효과를 볼 수 있지만 이전의 WAP 프로토콜이 가진 종단간 보안을 지원하지 않는 문제는 여전히 가지고 있었다. 이전에 제안된 e-WAP 은 e-WAP 서버에서 데이터 가공을 하는 형태이기 때문에 게이트웨이에서는 데이터를 건드리지 않게 된다. 따라서 프로토콜 변환으로 인하여 복호화하는 사이에도 무선 단말기 혹은

서버로 전송되는 데이터들은 평문으로 들어나지 않게 하기 위해 무선 단말기와 서버에서 두 번의 암호화를 하게 함으로써 기존의 WAP 이 가지는 종단간 보안 문제를 해결하고자 한다. 본 논문에서는 WAP 이 가지는 보안 취약점들을 살펴보고 이러한 취약점들에 대해 강화된 보안성을 지신 향상된 e-WAP 프로토콜 플랫폼을 제안하고자 한다.

2. e-WAP (enhanced-Wireless Application Protocol) 시스템

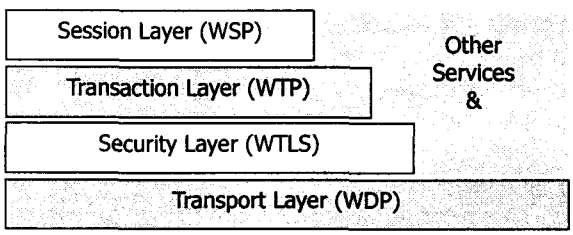
이전의 WAP 서버는 WML page 로 구성된 content 를 제공하는 기능만을 수행하였다. 그러나 제안된 e-WAP 모델에서는 단순히 이 기능뿐만 아니라 WAP 게이트웨이의 일부 수행 기능을 e-WAP 서버로 이전함으로써 WAP 게이트웨이의 오버헤드 발생 문제를 해결 할 수 있다. 즉, 기존의 WAP 게이트웨이에서 수행하는 프로토콜 스택 레이어의 5 단계 중 최상위 계층인 WAE(Wireless Application Environment)에서 수행하는 기능을 WAP 서버에서 실행하도록 개선하였다 [1].

2.1 e-WAP 게이트웨이

기존의 WAP 게이트웨이는 무선 단말기의 낮은 성능으로 인하여 많은 기능을 단말기 대신 수행하도록 설계되었다. 기존의 게이트웨이에서 수행되는 작업은 다음과 같다.

(1) 서로 다른 두 네트워크 프로토콜 변환 (HTTP ↔ WAP)
(2) 각 네트워크간의 서비스 연결성 (연결형, 비연결형, 보안연결형, 비보안연결형) 에 따른 WAP 프로토콜 스택 레이어의 실행
(3) WML content 의 Encoding/Decoding 변환
(4) WMLScript 컴파일링
(5) 네트워크 프로토콜에 따른 보안 지원
(6) 네트워크간의 필터링
(7) 접근제어 (Access Control)

위의 수행 작업 중 WML content 의 Encoding /Decoding 변환과 WMLScript 컴파일링은 WAE 계층에서 수행되는 기능으로서 이 작업을 e-WAP 서버로 이전함으로써 수행 작업을 감소시킬 수 있다.



[그림 1] e-WAP 게이트웨이의 프로토콜 스택 레이어의 수행 영역

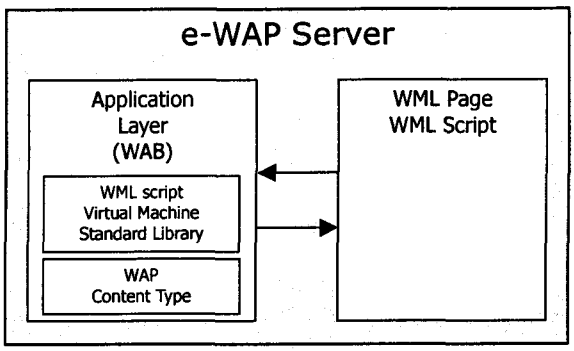
다음의 [그림 1]은 e-WAP 게이트웨이에서 수행하는 프로토콜 스택 영역을 나타낸 그림이다. 총 다섯 단계로 구성된 프로토콜 스택 레이어 중에서 최상위의 WAE 계층이 생략된 것을 볼 수 있다. WAE 계층은 e-WAP 서버에서 수행하게 된다.

2.2 e-WAP 서버

기존의 WAP 서버는 일반적인 Web 서버와 크게 다르지 않다. 따라서 지금까지는 WAP 과 web 에서 제공되는 content 를 web 서버에서 동시에 제공해 왔다. 즉, 서버 소프트웨어(Apache, IIS 등)의 MIME 타입을 추가하는 간단한 설정만으로 WML(Wireless Markup Language) 문서를 무선 단말기로 전송이 가능하다. 하지만 e-WAP 서버에서는 서버 소프트웨어를 확장하여 게이트웨이의 WAE 계층에서 수행하던 기능을 서버에서 수행하는 변환 모듈을 추가하였다. e-WAP 서버에서 수행하는 기능을 살펴보면 다음과 같다.

(1) WML 문서의 파싱
(2) WML script 컴파일링
(3) WML content 의 Encoding/Decoding 을 수행

다음의 [그림 2]는 e-WAP 서버의 시스템 구성과 내부적으로 수행되는 기능 구성을 나타낸다.



[그림 2] e-WAP 서버 시스템 구성도

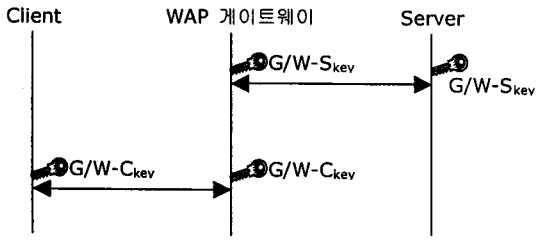
3. e-WAP 의 보안 모델

e-WAP 은 기존의 WAP 에서 보안과 관련되어 제공되는 WTLS, WMLScript Crypto Library, WIM 과 WPKI 등의 보안 요소를 지원한다 [2].

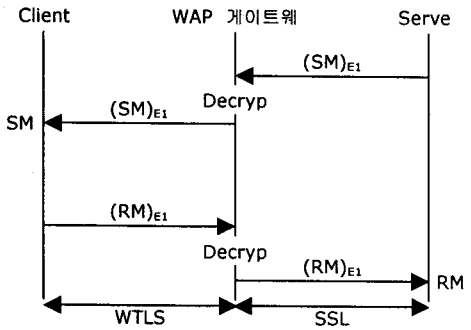
WAP 에서 지원되는 각각의 보안 요소들을 간단히 살펴보면, WTLS 는 WAP 프로토콜 스택의 WTP 와 WDP 사이에 위치하면서 클라이언트와 서버의 인증 및 세션 키 분배하는 기능을 가진다. WMLScript Crypto Library 는 WTLS 에서 지원할 수 없는 전자 서명 메커니즘으로서 Application 계층에서 트랜잭션의 인증 및 부인 봉쇄 서비스를 제공하고,

WIM 은 사용자 데이터의 안전한 저장을 위해 존재하는 요소로 스마트 카드로 구현되어 WTLS 와 WMLScript Crypto Library 에서 필요한 비밀키 및 인증서를 저장하는 역할을 한다. 그리고 WPKI 는 무선 환경에 적합한 공개키 기반 구조 모델이다 [2].

[그림 3]과 같이 e-WAP 게이트웨이는 WTLS 와 SSL 사이에 존재한다. 게이트웨이에서의 WTLS 와 SSL 의 변환은 매우 짧은 순간에 일어나고 가능한 빠른 시간 내에 메모리에서 삭제되도록 처리한다. WTLS 는 TSL 1.0 버전에 근거하지만 데이터그램, 최적화된 핸드쉐이크, 동적인 키 최신화(Key refreshing)와 같은 가능이 더 추가되었다 [3]. 그러나 게이트웨이에서 평문으로 복호화 된 메시지가 존재한다는 취약점으로 인해서 악의적 목적으로 접근한 해커가 평문 메시지를 얻을 수 있다. 또한 e-WAP 서버에서 발급되는 인증서가 무선 단말기에 발급되는 것이 아니라 게이트웨이에 발급되어 실질적으로 인증기관이 게이트웨이를 인증하는 결과가 초래되는 문제가 발생된다. 이러한 인증 문제를 해결하기 위해 게이트웨이의 관리 기관에 인증기관의 역할을 부여하기는 어렵다. 따라서 게이트웨이를 서버와 동일한 기관에 설치하는 방법이 제안되고 있지만, 이는 content 제공자에게 각각의 네트워크와 SMSC (Short Message 서버 Center) 별로 다른 구성을 설정해야 되는 게이트웨이까지 관리하는 문제를 초래할 뿐만 아니라, 가입자와 무선 네트워크 운영자 모두에게 여러가지 어려움을 안겨준다.



[그림 4] e-WAP 에서의 키공유



[그림 5] e-WAP 에서의 암호화 데이터 전송

e-WAP 에서의 키교환 방식은 게이트웨이와 서버가 보안 통신을 위한 비밀키 G/W-S_{key} 를 공유하고 있고 이 키를 사용하여 서버에서 암호화된 메시지를 게이트웨이에서는 복호화한다. 게이트웨이와 클라이언트 사이에서는 G/W-C_{key} 키를 공유하고 있다. 이 키를 사용하여 복호화 된 메시지를 다시 암호화하여 클라이언트로 전송한다. 다음의 [그림 4]은 위에서 언급한 내용을 도식화한 것이다.

이렇게 공유된 키는 각각 서버와 WAP 게이트웨이 사이의 SSL 로 통신하기 위해서 사용되고, WAP 게이트웨이와 클라이언트 사이에서의 키는 WTLS 에서 사용된다. 다음의 [그림 5]은 공유된 키를 사용하여 각 암호화 전송 프로토콜에 따른 데이터의 전송 흐름을 보여주고 있다.

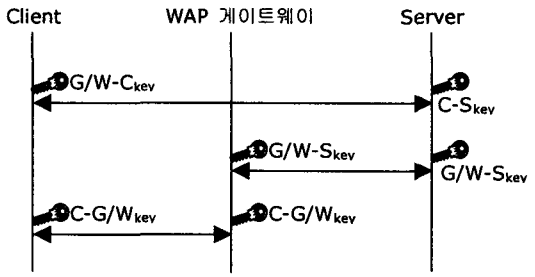
4. 종단간 보안이 개선된 e-WAP 보안 모델

기존의 WAP 보안 모델이 종단간 보안 (end-to-end Security)을 지원하지 못하는 원인은 유/무선 네트워크간 사용되는 프로토콜이 서로 다르게 설계된 WAP 게이트웨이모델이 가장 큰 원인이 된다. 패킷 암호화가 아닌 전송 데이터만을 암호화하는 것도 게이트웨이에서 WAE 계층에서 수행하는 기능으로 인하여 데이터 암호화도 불가능하다. 하지만 e-WAP 에서는 WAE 계층이 WAP 서버에서 수행되기 때문에 전송 데이터만 전송이 가능해 진다.

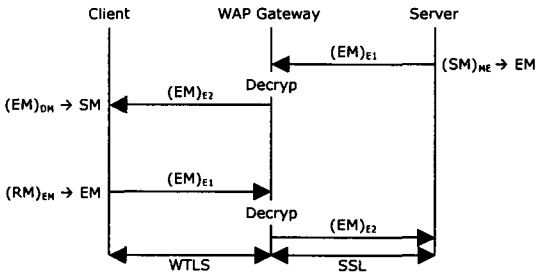
개선된 e-WAP 보안 모델은 게이트웨이에서 평문을 보유하지 않아야 한다는 보안의 투명성을 제공한다. 이전의 WAP 에서는 클라이언트와 게이트웨이 사이에 비밀키를 공유하고 게이트웨이와 서버 사이에서 또 다른 비밀키를 공유한다. 개선된 e-WAP 에서는 이 키와 함께 클라이언트와 서버에 하나의 키를 더 공유하게 된다.

4.1 종단간 보안이 개선된 e-WAP 에서의 키 공유와 보안 전송

개선된 e-WAP 에서는 서버와 클라이언트가 두 개의 키를 공유하게 된다. 즉, 서버에서는 두 번의 암호화가 이루어진다. 게이트웨이는 서버에서 온 메시지를 복호화한 후, 다시 암호화하여 클라이언트로 전송된다. 하지만 이미 전송 데이터만이 암호화 되어 있으므로 게이트웨이에서는 평문의 데이터가 드러나지 않는다. 클라이언트에서는 두 번의 암호화가 된 데이터가 전송되고 클라이언트는 두 번의 복호화를 통해 비로소 평문의 데이터를 받게 된다.



[그림 6] 개선된 e-WAP 에서의 키 공유



[그림 7] 개선된 e-WAP 에서의 데이터 전송

[그림 6]과 [그림 7]은 개선된 e-WAP 에서의 키 공유와 데이터 전송 흐름을 각각 나타낸 그림이다. 다음은 [그림 7]의 도식에 사용된 기호의 설명이다.

(1) SM : 서버에서 클라이언트로 전송되는 평문의 전송 데이터 (Plain text)
(2) RM : 클라이언트에서 서버로 전송되는 평문의 전송데이터 (Plain text)
(3) EM : 서버에서 SM 을 한번의 암호화하여 나온 암호화된 데이터
(4) $(EM)_{E1}$: 서버에서 게이트웨이까지 SSL 프로토콜을 사용하여 전송되는 두 번의 암호화된 데이터
(5) $(EM)_{E2}$: 게이트웨이에서 클라이언트까지 WTLS 프로토콜을 사용하여 전송되는 두 번의 암호화된 데이터

4.2 종단간 보안이 개선된 e-WAP 보안 모델 분석

제안된 e-WAP 보안 모델은 e-WAP 서버에서 WAE 계층의 기능을 수행하기 때문에 가능해 진다. 하지만 본 논문에서 제안된 e-WAP 보안 모델은 이동단말기의 오버헤드가 증가한다는 문제점을 가지고 있다. 기존의 한번의 암호화와 복호화를 하던 WAP 보안 모델에 비해 무선 단말기에서 두 번의 암호화와 복호화를 하게 되기 때문이다. 따라서 최대 두 배의 작업량이 증가하게 되겠으나 현재 무선 단말기의 성능이 급속히 향상되므로 그리 심각하다고 보이지 않는다.

지금까지 설명된 e-WAP 보안 모델의 핵심은 WAP 에서의 종단간 보안 (End-to-End Security)을 제공하는 것이다.

5. 결론

현재 대중적으로 사용되는 유선 인터넷에서 이동성이 강화된 무선 인터넷으로 진행 중이다. 전자상거래, 데이터 전송, 그리고 계좌이체 등의 은행 서비스 이용이 증가할수록 확장가능하며 단대단까지 안전한 content 가 요구된다. 이에 본 논문에서는 무선 인터넷 환경에서 종단간 보안이 보장되는 개선된 e-WAP 보안 모델을 제안하였다.

e-WAP 은 게이트웨이의 증가되는 오버헤드를 줄이기 위해 제안된 WAP 모델이다. 본 논문에서는 이 e-WAP 모델을 개선하여 새로운 보안 모델을 제안하였다. 이는 기존의 보안 모델(WTLS 와 SSL 보안 프로토콜을 사용하는 기존의 방식)에 서버와 무선 단말기 사이의 데이터 암호화를 하여 종단간 보안 (end-to-end Security)을 제공하도록 제안하였다. 이는 e-WAP 서버에서 WAE 계층을 수행하기 때문에 가능해 진다. 하지만 무선 단말기에서 두 번의 암호화와 복호화를 수행하게 된다. 이로 인해서 상대적으로 성능이 낮은 무선 단말기에 오버헤드가 증가되는 문제점을 가진다. 이는 향후 구현되어 통계적인 성능 저하치의 연구가 진행되어야 될 것이다.

참고문헌

[1] 원대희, "WAP 게이트웨이와 WAP Server 의 기능 분산 모델", 한국정보처리학회, 춘계정보처리학회지, 2003.4
[2] 이동근외 5 인, " 무선 응용 프로토콜 보안 기술" , 한국정보과학회, 2002
[3] 조현숙, "WAP 보안과 표준화 동향", 한국정보보호학회, 정보보호학회지, 2000
[4] "Wireless Application Wireless Transport Layer Security Specification", WAP forum, Nov. 1999
[5] "Wireless Application Protocol", WAP forum, Nov. 1999
[6] 문종철, 원유재, 윤이중, "WTLS handshake 프로토콜의 분석", Proceedings of The 12th Workshop on Information Security and Cryptography (WISC2000), 2000.9
[7] 김소진, 박지환, 신성한, "SSL / TLS 와 WTLS 의 프로토콜 취약성 분석", 한국멀티미디어학회, 한국멀티미디어학회, 2001