2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

WAP 마이크로브라우저와 서버의 종단간 보안 메커니즘 설계

양진욱*, 김순자*
*경북대학교 전자전기공학부
e-mail:jinux@palgong.knu.ac.kr;snjkim@ee.knu.ac.kr

A Design on End-to-End Security Mechanism between WAP Microbrowser and Server

Jin-Wook Yang*, Soon-Ja Kim*
*Dept of Electrical and Electronics,
Kyungpook National University

요 약

최근 무선 인터넷 서비스가 증가함에 따라 무선 전자상거래(Mobile Commerce) 영역으로까지 발전하고 있으나. 이의 실현을 위해서는 보안 문제의 해결이 필수적이다. 현재 WAP은 게이트웨이의 구조적인 문제로 궁극적인 보안이 불가능하며, 이에 많은 대안들이 제시되고 있다. 본 논문에서는 게이트웨이와는 무관하게 마이크로브라우저와 WAP 서버간의 안전한 통신을 하기 위한 보안 메커니즘을 제시하며, 이를 위해 마이크로브라우저 차원에서 인증과 암호화를 위한 모듈을 구성하고 게이트웨이의 포맷 변화를 고려하여 서버 측에서 WML을 효율적으로 암호화하는 방법을 제시한다. 이들을 기반으로 하여 종단간의 암호화와 복호화 메커니즘을 구현한다.

1. 서 론

최근 국내외적으로 이동통신이 급격히 발전하고 있으며, 제공되는 서비스도 음성 중심에서 데이터 중심의 서비스로 그 폭을 넓혀가고 있다. 무선 서비스의 가장 큰 장점은 이동성으로, 사용자는 장소와 시간에 구애받지 않고 전파가 도달하는 어떤 곳에서도 원하는 서비스를 제공받을 수 있다. 아울러 최근에는 무선 환경에서 기존의 유선 인터넷 서비스를 그대로 구현하려는 다양한 시도들이 일어나고 있으며, 초기의 게임, 전자 메일, 채팅에서 전자상거래, 증권, 뱅킹 서비스 등의 비즈니스 영역으로까지 확대되고 있다. 최근 조사된 국내 무선 인터넷 실태 조사[1]에서, 앞으로 무선에서 가장 많이 제공될 서비스로 가장 많은 응답자가 무선 전자상거래(Mobile Commerce)를 꼽은 것은 이 분야에 대한 사람들의 많은 관심과 미래를 반영한다.

현재 무선 인터넷의 양 축은 WAP(Wireless Application Protocol)과 ME(Mobile Explore)진영으로 나눌 수 있다. 이 중 WAP은 무선 환경, 즉 제한된 CPU 성능과 메모리, 전력, 디스플레이, 대역폭 등을 고려하여 최적화된 무선 인터넷 프로토콜이다. WAP의 기본 구조는 유선망과 이동통신망 사이에 게이트웨이를 두어서 양 측의 서로 다른 프로토콜을 변환하여 중계하는 구조를 가진다.

2. WAP 보안 모델

2.1. WAP WTLS(Wireless Transport Layer Security)[2]

안전한 무선 전자상거래가 무선 인터넷에서 구현되기 위해서는 보안성의 제공이 필수적이다. WAP에서 제공하는 WTLS는 SSL/TLS를 기반으로 하여 무선 환경에 최적화된 채널 보안 프로토콜이다. 이는 WAP user agent와 게이트웨이 사이에 안전한 채널을 형성하여 통신 내용의 기밀성, 메시지 무결

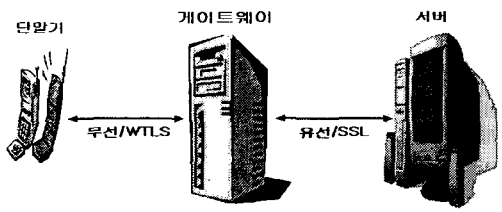
성, 클라이언트와 서버간의 상호 인증을 구현한다. WTLS는 WTP와 WDP층 사이에서 동작하므로 WAP을 사용하는 모든 프로그램을 지원하지만, 부인 방지 기능은 제공하지 않는다.

2.2. WML(Wireless Markup Language) Script Crypto 라이브러리[3]

이는 WTLS가 부인 방지 기능을 제공하지 않으므로, 응용 계층에서 전자 서명을 통해 이를 지원하기 위한 암호 라이브러리로, Crypto.signText()라는 API를 제공한다. 이 기능과 WTLS를 연동하면 기본적인 정보보호 서비스를 제공할 수 있다. 또한 단말기의 처리 능력을 고려하여 스마트 카드와의 연동을 고려한 WIM(WAP Identity Module)[4]도 제안되어 있다.

2.3. 구조적인 보안문제, 게이트웨이와 해결 방안

WAP에서는 위에서 언급한 기본적인 정보 보호 서비스를 제공하지만 이는 게이트웨이와 단말기 사이의 보안이며, 웹 서버와 단말기 사이에 게이트웨이가 들어가는 WAP 구조에서는 필연적인 보안 문제가 존재한다. 대개 무선 보안은 WTLS로, 유선 보안은 SSL로 통신하게 되는데, 게이트웨이는 이들 사이에서 양 측의 프로토콜을 변환하게 되며, 이 과정에서 데이터를 복호화 및 재 암호화하는 과정을 수행하는데, 여기서 원래의 내용(plaintext)이 노출되므로 보안 문제가 발생할 수 있다(그림 1).



<그림 1. WAP 보안 문제>

이 문제를 해결하기 위해서는 유무선 전 구간에서의 SSL 이용, 안전한 게이트웨이의 추가 장착 등이 있으며, 응용 프로그램 차원에서 이를 처리할 수도 있다[5]. 이 경우 게이트웨이는 단말기와 서버간의 암호화된 내용의 중계만을 담당하게 되며, 통신 내용을 알지 못하므로 보안이 유지된다. 최근에는 휴대폰에 Java 가상머신을 탑재한 CLDC(Connected Limited Device Connectivity)/MIDP(Mobile Information Device Profile)[6]기반의 보안 응용 프로그램의 개발이 이루어지고 있다.

본 논문에서는 기본적인 WAP통신에 보안 기능의 제공을 위하여 브라우저 차원에서 서버와의 인증 및 WML[7]과 WBXML(WAP Binary XML)[8]문서의 암호화/복호화 기능을 수행하는 WAP 마이크로브라우저 및 서버와의 보안 메커니즘을 제안한다.

3. 제안한 마이크로브라우저 및 서버의 보안 기능

제안한 마이크로브라우저의 구조는 크게 기본 모듈과 보안 모듈로 나눌 수 있다. 기본 모듈은 통신 모듈, 파싱 모듈, 해석 모듈, 디스플레이 부분으로 구성되며, 보안 모듈은 암호 엔진 및 이를 기반으로 한 인증 모듈의 암호화/복호화 모듈로 구성된다. 이들 모듈을 연동하여 WAP 브라우저에서의 암호화 기능을 설계하였다. 한편, 이 경우 WML 문서의 암호화/복호화 기능이 서버에서 전제되어야 하는데, 이는 <crypto>라는 암호부분을 인식할 수 있는 태그를 새로 정의하여 WML DTD(Document Type Definition)에 추가함으로써 게이트웨이 및 마이크로브라우저가 인식할 수 있도록 하였다.

3.1. 기본 모듈

마이크로브라우저의 기본 모듈은 통신 모듈, 파싱 모듈, 해석 모듈 및 디스플레이부로 구성된다.

- 통신 모듈 : WAP 게이트웨이와의 물리적 연결과 WAP 서버와의 논리적 연결을 담당한다.
- 파싱 모듈 : WBXML 파일의 태그 부분과 데이터 부분을 파싱하여 DOM(Document Object Model)트리 형태로 구조화하여 다른 모듈에서 데이터를 처리할 때 API로 쉽게 참조할 수 있게 한다.
- 해석 모듈 및 디스플레이부 : 이 부분은 DOM 트리 형태의 WBXML 태그의 의미를 해석하여 적절하게 디스플레이해 주는 역할을 수행한다. 암호화된 부분의 경우에는 암호화/복호화 모듈과 연동하여 데이터를 복호화한 후 브라우징한다.

3.2. 보안 모듈

- 암호화 엔진 : 암호화/복호화 모듈 및 인증 모듈의 동작의 기반이 되는 부분이며, 이 두 모듈에서 사용되는 암호 알고리즘은 <표 1>과 같다.
- 인증 모듈 : 단말기와 WAP 서버간의 인증 프로토콜을 수행하여 상호 인증 및 암호화/복호화에 사용될 대칭키 교환 기능을 동시에 수행한다. 인증 프로토콜은 현재 무선통신 유럽 표준으로 채택된

<표 1 : 사용된 암호화 방식과 알고리즘>

방식	암호 알고리즘
공개키 암호화	RSA
대칭키 암호화	DES
디지털 서명	KCDSA
메시지 다이제스트	SHA-1

ASPeCT(Advanced Security for Personal Communications Technologies)[9]를 사용하였다. 인증은 한 세션 단위 동안 유효하다.

- 암호화/복호화 모듈 : 앞의 인증 과정에서 얻은 대칭키로 상호간에 암호화/복호화를 수행하는 부분이다. 제안한 마이크로브라우저에서는 해석 모듈에서의 요청이 있을 경우 해당 데이터를 복호화하여 전송하게 된다.

3.3. 서버측의 WML 문서 암호화

WML 문서를 응용계층에서 암호화하여 전송할 경우 서버는 WAP이라는 구조의 특수성, 즉 게이트웨이를 고려한 종단간 암호 방식을 선택해야 한다. 다시 말해 서버는 게이트웨이가 암호화된 WML 문서의 내용은 알지 못하게 하면서 동시에 정의된 태그를 모두 인식하여 바이너리 XML로 적절하게 변환할 수 있도록 하여야 한다. 따라서 WTLS나 SSL 등의 채널 보안에서처럼 WML 문서 전체를 암호화할 수는 없으며, 태그 및 엔티티를 제외한 데이터만을 암호화할 수 있다.

본 논문에서는 <crypto>라는 태그를 새로이 정의, WML DTD에 추가하여 게이트웨이 및 마이크로브라우저가 이를 인식하여 변환하도록 하였다. 이 태그의 용도는 서버가 암호화한 데이터 영역을 XML 태그로 표시하도록 하는 것이며, 이를 인식하게 하려면 DTD 및 게이트웨이의 인코딩 모듈을 수정하여야 한다. DTD에서 추가될 부분은 다음과 같다.

<!ELEMENT crypto #PCDATA>

태그 내에 들어가는 부분은 PCDATA(Parsed Character DATA)로 선언하였다. 이는 문자열만이 내용으로 포함되게 하여 태그나 엔티티가 암호화되어 WML 문서가 인코딩 과정 중 손실되는 경우를 방지한다.

게이트웨이에서 <crypto>태그를 인식하게 하려면 해당하는 바이너리 값이 정의되어 있어야 한다. WML 1.2 스펙에는 현재 36개의 태그가 정의되어 있으며, 이 중 '3a'를 사용할 수 있으므로 이 값을 <crypto>와 대응하여 사용하였다. 마이크로브라우저의 해석 모듈 역시 이 값을 인식하여 데이터를 복호화할 수 있도록 하였다.

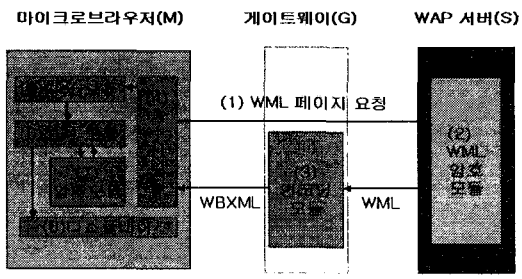
4. 종단간 보안 메커니즘

WAP 마이크로브라우저와 서버의 종단간 보안 통신은 크게 두 가지 방식으로 나누어진다. 하나는 단말기가 WML 문서를 요청할 경우 암호화된 WML을 전송하는 경우이며, 다른 하나는 수신된 WML 문서에 <FORM>, <INPUT>태그가 포함되어 있어서 사용자가 기밀 정보를 입력하여 서버로 전송하는 경우이다. 이 때 암호화 및 복호화는 인증 과정 이후에 생성된 대칭키를 사용하며, 서버는 원하는 부분을 미리 혹은 동적으로 암호화하여 단말기로 전송할 수 있다.

4.1. 마이크로브라우저의 WML 페이지 요청

마이크로브라우저와 WAP서버와의 통신은 일반적인 WWW상에서의 HTTP 프로토콜과 유사하다. 즉 마이크로브라우저가 요청하고 서버가 응답하여 WML 페이지를 전송하게 되며, 이 과정에서 암호화 및 복호화 과정이 추가된다.

(1) 단말기(이하 M)은 서버(이하 S)에 WML페이지를 요청한다.
(2) S는 암호화된 WML을 생성한다.
(3) S는 암호화된 WML을 전송한다. 게이트웨이(이하 G)는 WBXML로 인코딩하여 M으로 전송한다.
(4) M은 WBXML을 수신한다.
(5) 파싱 모듈은 DOM 형태로 구조화한다.
(6) 해석 모듈은 태그의 의미를 해석한다.
(7) <crypto>태그일 경우에는 해당 내용을 복호화하여 전송한다.
(8) 내용을 디스플레이한다.

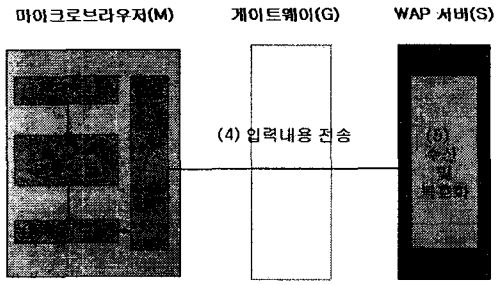


<그림 2. 복호화 과정>

4.2. 사용자가 입력한 내용을 암호화하여 전송

수신된 WML문서에 <FORM>, <INPUT>태그가 있을 때 단말기는 사용자에게 입력을 요구한다. 입력된 내용은 세션 키로 암호화되어 서버로 전송된다.

(1) 사용자는 데이터를 입력한다.
(2) 암호 모듈은 이 데이터를 세션 키로 암호화된다.
(3) 해석 모듈은 암호화된 데이터에 HTTP-like header를 추가하여 송수신 모듈로 보낸다.
(4) 서버로 전송한다. 이 때 게이트웨이는 WBXML 포맷을 텍스트 WML 포맷으로 디코딩한다.
(5) WAP 서버는 이 데이터를 수신하여 복호화한다.



<그림 3. 암호화 과정>

5. 결 론

본 논문에서는 게이트웨이를 고려하여 마이크로브라우저와 WAP 서버간의 종단간 보안을 실현하기 위한 메커니즘을 제시하였다. 이를 위해 마이크로브라우저 차원에서의 인증 및 암호 모듈을 구성하였으며, 서버에서는 WML 부분 암호화 기법을 사용하여 게이트웨이 및 마이크로브라우저가 효과적으로 인식할 수 있도록 하였다.

향후에는 확장된 DTD를 이용, 게이트웨이에 모듈을 추가하여 연동하는 시스템을 구현하며, 이를 기반으로 하여 응용 계층에서의 안전한 무선 쇼핑몰 등 보안 트랜잭션을 구현할 수 있을 것이다.

참고 문헌

[1] 김진우, MIC(Mobile Internet Census)1차 설문조사 결과, 2000. 3. 23., 연세대학교 휴먼 인터페이스 연구실, http://hci.yonsei.ac.kr

[2] WAP WTLS ver. 18-Feb-2000, http://www.wapforum.org

[3] WML Script Crypto Library ver.05-Nov-1999

[4] WAP WIM ver.05-Nov-1999

[5] 이종후, 류재철 "모바일 시스템 보안, 어디까지 왔나" 2000년 8월, 마이크로소프트웨어, pp.290~292

[6] CLDC/MIDP, http://java.sun.com/

[7] WAP WML ver.4-Nov-1999

[8] WAP Binary XML Content Format ver.1.3. 15-May-2000

[9] Gunter Horn, Bart Preneel, "Authentication and Payment in Future Mobile Systems"