WAP에서 무선 PKI기반의 효율적인 인증서 검증

Effective Certificate Verification of Wireless PKI Based in WAP

신정원, 최승권, 지홍일, 이병록, 조용환
충북대학교

Shin Jung-Won, Choi Seong-Kwon, Ji Hong-Il,
Lee Byong-Rok, Cho Yong-Hwan
Chungbuk Univ.

요약

무선 인터넷에서 전자상거래를 비롯한 데이터 서비스가 성공적으로 제공되기 위해 보안 문제가 해결되어야 한다. 무선 인터넷을 위한 보안 프로토콜은 인증과 키 교환을 주목적으로 하며 주로 WPKI(WAP Public Key Infrastructure)을 가정하고 인증서를 이용하여 설계되었다. 이에 무선 환경을 고려한 PKI의 효율적인 인증서 검증을 논의하고자 한다.

Abstract

To data service is offered successfully including electronic commercial transaction in radio Internet, security problem should be solved. Security protocole for radio internet does certification and key exchange by leitmotif and designed because suppose WPKI(WAP Public Key Infrastructure) mainly and use certificate. Wish to discuss efficient certificate verification of PKI that consider radio surrounding hereupon.

Ⅰ. 서 론

무선인터넷 환경에서 원활한 멀티콘텐츠 서비스를 하기 위한 선결과제로 무선인터넷 환경의 보안 문제를 들 수 있으며, 그에 따른 강력한 인증 절차와 데이터 보호를 위한 암호화 기능이 필요하며, 호스트들의 이동성 지원을 위해 무선 환경에 적합한 프로토콜이 구축되어야 한다.

WAP(Wireless Application Protocol)은 기존의 표준을 대부분 수용하면서 무선 인터넷 환경에 적합한 데이터 통신을 위한 표준 프로토콜이다.

WAP에서는 보안 위한 프로토콜로서 WTLS (Wireless Transport Layer Security)를 제안하고 있다. 이는 공개키 교환을 전제로 하고 있는데, 공개키 기반 구조를 사용하여 해결하고 있다. 그러나 무선 인터넷의 경우는 일반 PC와는 달리 많은 제약 조건이 따르고 있다. 휴대폰이나 PDA 단말기 내부의 작은 프로세서들은 메모리 및 장치의 한계 때문에 PC와 유선망의 암호화 및 인증을 사용 하는 것은 불가능하다.[1][2]

PKI에서 가장 중요한 것 중에 하나가 인증서인데, 인증서를 사용하고자 하는 사용자는 인증서를 사용하기 전에 반드시 유효성을 검증하는 안증서 검증 과정을 수행하여야 한다. 이에 기존의 인증서 검증 방법을 살펴보고 사용자의 부담을 줄이고 인증서 검증 성능향상을 위한 검증 방법을 살펴보고자 한다.

Ⅱ. WAP

1. 무선인터넷 프로토콜

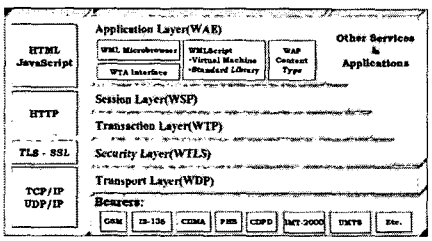
국내 무선인터넷 시장은 1999년 말부터 본격적으

로 성장하여 현재 사용자가 이천만을 넘고 있는 상태이며 제공되는 콘텐츠의 종류도 멀티미디어 다운로드, 메일 송수신에서 인터넷 뱅킹, 증권, 전자상거래까지 다양하다. 특히 인터넷 뱅킹, 증권, 전자상거래 서비스는 사용자의 중요한 정보가 처리되기 때문에 보안이 중요하다. 그러나 무선인터넷에서 보안 서비스를 제공하기에는 제약사항이 많다. 무선망은 상대적으로 낮은 데이터 전송률과 높은 오류 발생률을 가지고 있으며, 무선 단말기들은 낮은 컴퓨팅 능력과 부족한 저장 공간을 가지고 있기 때문에 많은 연산과 그에 따르는 많은 전력 소비를 필요로 하는 유선망의 보안 방식을 무선 단말기에 그대로 적용한다는 것은 어렵다.

무선인터넷의 이러한 제약요소들을 해결하고 공통 플랫폼을 구축하기 위하여 다양한 무선인터넷 표준이 제시되어 왔었다. 대표적인 예로 WAP(Wireless Application Protocol)[3], ME(Microsoft Mobile Explorer)[4], i-mode[5]를 들 수 있다.

2. WAP

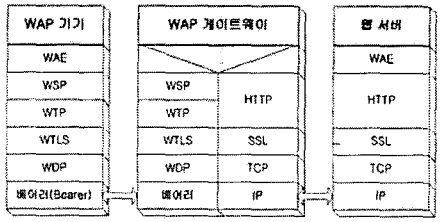
우선 단어부터 풀어놓고 보면, WAP은 Wireless Application Protocol의 머리글자를 따서 만든 단어이다. 이 말을 좀 더 풀어보자면 무선통신이 제공하는 기반 위에서 다양한 서비스를 제공하기 위한 프로토콜이라고 생각할 수 있다. [캡처 1]은 WAP 프로토콜 스택이다.



▶▶ 캡처 1. WAP 프로토콜 스택

WAE(Wireless Application Environment), WSP(Wireless Session Layer),WTP(Wireless Transaction Protocol), WTLS(Wireless Transport Layer Security), WDP(Wireless Datagram Protocol)으로 구성되어 있다.[6]

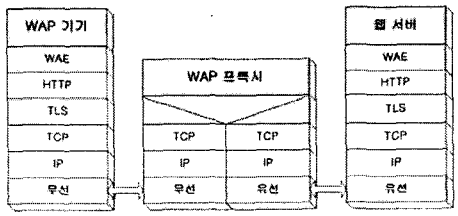
무선단말기와 기지국간의 무선 전파환경에서 데이터를 효율적으로 전송할 수 있는 프로토콜인 WAP 1.x는 망이나 단말기의 종류에 관계없이 다양한 무선환경에서 동작이 가능하다. WAP 1.x 방식에서는 [그림 2]와 같이 무선망과 기존의 유선인터넷망의 연동을 위하여 WAP gateway를 두고 있으며, WAP 1.x 프로토콜과 인터넷 TCP/IP 프로토콜을 중간에서 변환해 주는 역할을 한다.



▶▶ 그림 2. WAP 1.x모델

WAP 2.0은 OMA(Open Mobile Alliance)와 OMAI(Open Mobile Architecture Initiative)가 무선데이터 서비스를 위한 독자적인 WAP1.x 와 XML1.x를 포기하고, XHTML과 SSL, TCP/IP에 이르는 기존 유선인터넷 표준을 지원하는 차세대 무선인터넷의 국제표준규격을 의미한다.

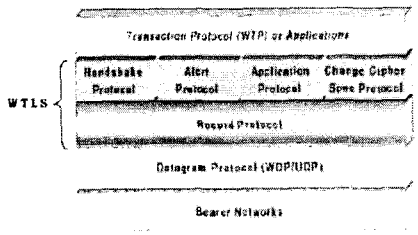
WAP 2.0에서는 단말기와 서버 사이의 데이터 통신이 HTTP 프로토콜을 통해 이루어질 수 있으므로 WAP gateway가 필요하지 않다. 그러나 WAP 2.0에서 WAP 프록시를 사용하면 위치기반서비스, 프라이버시, 접속여부 표시 서비스 등의 부가적인 모바일 서비스를 제공 할 수 있다. 또한 Push 기능을 제공하기 위해서는 반드시 [그림 3]과 같은 WAP 프록시를 사용하여야 한다.[7][8][9][10]



▶▶ 그림 3. WAP Proxy 구조

3. WTLS

정보보호 서비스를 책임지고 있는 계층으로 WAP Forum에서 제안한 WTLS의 Handshake Protocol, Alert Protocol, Change Cipher Spec Protocol은 WTLS의 동작에 대한 관리를 위해 사용되며, 실질적인 보안 서비스는 Record Protocol에서 제공된다. 물론 이를 위해서 공개키 분배 및 인증에 관한 기반 구조가 필요하게 되는데 이를 위한 무선 공개키 기반 구조를 전제로 하고 있다. [그림 4]는 WTLS의 구조를 보여준다.



▶▶ 그림 4. WAP 프로토콜 스택에서 WTLS 구조

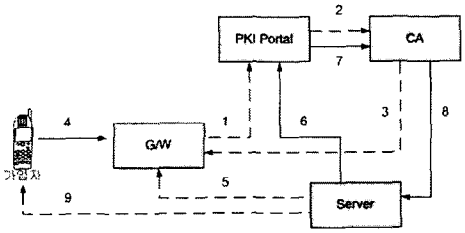
Ⅲ. WAP에서 PKI기반의 인증서 검증

무선환경에 적합하도록 기능을 최소한 변화시킨 것이 무선 PKI이다. 예를 들어 WAP 게이트웨이를 통한 무선 PKI 서비스에서는 기존의 유선 환경에 사용하는 X.509 인증서에 비해 부피가 작고 간단한 WTLS 인증서를 사용한다. 이는 무선 환경에서 사용하는 소용량 단말기에서 암호화 및 인증 업무를 효율적으로 수행할 수 있도록 구성되어 있다.

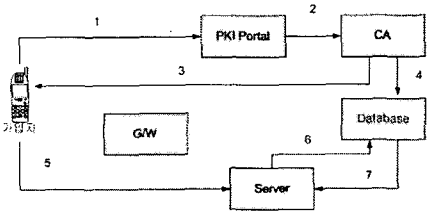
1. WAP PKI

WTLS와 WMLScript Crypto Library와 같은 규격이 모두 공개키 인증서를 가정하고 있으므로 무선 공개키 기반 구조는 WAP에서 보안 메커니즘을 구현하기 위한 기초가 된다고 할 수 있다.

지난 2001년 4월에 승인한 WAP Public Key Infrastructure Definition은 기존의 WAP 요구사항을 지원하는 PKI 표준을 다시 사용하기 위한 것으로 [그림 5]의 WTLS 구현 클래스 2와 공개키 기반 사용자 인증서(CA에서 발급)를 이용한 WAP 무선 공개키 기반구조 모델과 [그림 6]의 WTLS 구현 클래스 3(사용자 인증과 서버 인증 필수)과 공개키 기반의 사용자 인증서를 사용한 signText() 함수의 WAP 공개키 기반구조 모델 두 가지 방안을 제안하고 있다.[11]



▶▶ 그림 5. WTLS Class 2와 WPKI 모델



▶▶ 그림 6. WTLS 클래스 3과 signText WPKI 모델

2. 무선 PKI기반의 인증서 검증

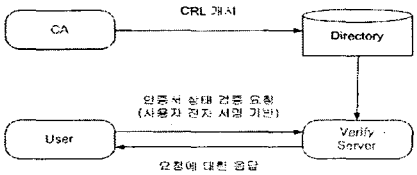
PKI 구축을 위해 사용하는 기술로는 인증서 발급, 갱신, 폐지 등을 다루는 인증서 관리 기술과 보안 알고리즘을 이용하여 전자서명의 생성 및 검증, 암호화를 다루는 보안 기술, 그리고 인증서의 유효성 및 현

재 상태를 다루는 인증서 검증 기술로 크게 구분할 수 있다. 이러한 기술 중 인증서의 검증 기법은 실제 전자거래에 있어 그 거래의 유효성에 관한 것이므로 가장 신중하게 처리되어야 하며 인증서 검증 서비스 응답은 실시간으로 신속하게 이루어져야한다. [12]

2.1 기존의 검증 방법

1) CRL를 이용한 인증서 검증

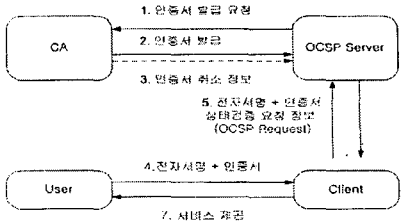
RFC2459에서 정의 되었으며 CRL을 이용한 방식은 현재 가장 널리 사용되고 있는 인증서 상태 검증 방법이다. 이 방식은 사용자가 인증기관에게 인증서를 취소해 줄 것을 요청할 경우 인증기관이 인증서 취소 목록을 생성하여 배포함으로서 다른 사용자의 인증서 사용을 중지시키는 방식으로, 취소된 인증서의 일련번호와 사유를 포함하여 전자서명 한 후, 디렉토리와 같은 공개된 장소에 게시하고 클라이언트는 이를 다운받아 필요로 하는 인증서를 검색하여 인증서의 상태 정보를 획득하는 방법이다.[그림7]



▶▶ 그림 7. CRL기반의 인증서 상태 검증 수행 과정

2) OCSP를 이용한 인증서 검증 방식

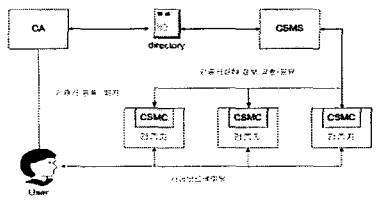
[그림 8]의 OCSP기반의 인증서 검증 방식은 OCSP 클라이언트가 CRL을 요청하지 않고 인증서의 현재 상태를 검증하기 때문에 실시간으로 인증서에 대한 상태 검증을 할 수 있다는 장점이 있는 반면 실시간으로 인증서에 대한 유효성 검사를 수행해야 하기 때문에 많은 통신량으로 인한 네트워크 과부하 문제가 발생시킨다는 단점과 네트워크 상태에 따라 인증서 유효성 검사의 수행시간이 달라진다는 단점이 있다.



▶▶ 그림 8. OCSP기반의 인증서 검증 수행 과정

2.2 효율적인 인증서 상태 검증 방법 제안

실시간 응용 분야에서는 인증서를 검증할 때 보안성과 성능을 보안하면서 항상 CA의 인증서 상태 정보와 동일한 정보를 이용해야 한다. 제안하는 [그림 9]의 CSMP 방법에서는 보안성, 실시간성, 성능 3요소를 모두 보장한다.



▶▶ 그림 9. CSMP의 시스템 구성요소

인증서상태 관리 프로토콜(CSMP)은 응용 프로토콜의 잡합, CSMS의 기능, CSMC의 기능 등을 총칭한다.

인증서상태 관리 서버(CSMS)는 CA에서 관리하는 인증서들의 상태 정보를 CSMC에 제공하는 서버로써 이용자가 상태 정보를 조회한 적이 있는 검증자들을 검증자 목록에 이용자별로 관리한다. 인증서 폐지 처리를 주로 수행하며, 인증서 폐지 신청 처리와 인증서 폐지 완료 처리로 구분된다. 인증서 소유자가 CA에 인증서 폐지를 신청하면, CSMS는 CA와 CSMS의 등록 검증자 목록의 인증서 상태 정보를 변경하지 않고 CSMC에 인증서 폐지 처리를 수행한다. 인증서 상태 목록에 폐지정보가 반영되면 CSMS에 폐지 완료 처리를 전송한다.

인증서상태 관리 클라이언트(CSMC)는 검증자에

게 이용자의 인증서 상태 정보를 제공하며 검증자가 인증서 상태 검증 처리를 효율적으로 수행할 수 있도록 지원한다. 주기능은 인증서 상태 검증과 검증자 등록처리이다. 만약 이용자의 인증서에 해당되는 인증서 상태정보가 검증자가 관리하는 인증서 상태 목록에 없으면 CSMS에 인증서 상태 정보를 요청한다. 최오 거래자의 인증서가 유효한지 CA에 의해 검증 완료되어 검증 목록에도 등록이 되어 응답된 인증서 상태 정보는 CSMC가 인증서 상태 목록에 기록하고 관리한다.

Ⅳ. 실험 결과 및 결론

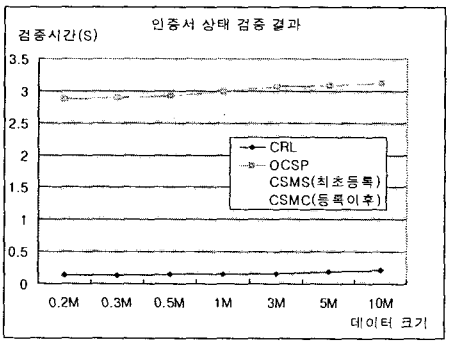
1. 실험결과

실제 운용 중인 사이버트레이딩 시스템과 동일한 테스트용 서이버트레이딩 시스템에 CSMP를 구현했다.

인증서 상태 검증의 경우는 두 가지가 있다.

첫 번째는 최초로 거래할 때이며 인증서 목록에 인증서 상태 정보가 없으므로 CSMS를 이용하여 CA로부터 인증서 상태 정보를 획득하고 인증서 목록에 등록한 후 인증서 상태를 검증한다.

두 번째는 인증서 목록에 인증서 상태 정보가 이미 등록되어 있기 때문에 다른 곳에서 인증서 상태 정보를 획득하려는 노력 없이 인증서 상태를 검증한다.



▶▶ 그림 9. 인증서상태검증 결과

최초 등록의 경우에는 인증서정보를 획득하여 인증서 목록을 등록 후 인증서 상태를 검증하기 때문에 OCSP와 유사한 성능을 보여주지만, CRL인증서 상태 정보가 등록된 후에는 OCSP는 물론이고 CRL방법보다 향상된 결과를 보여준다.

2. 결론 및 향후 방향

CSMP는 인증서 상태 검증 속도를 줄이는 것을 목표로 한다. 또한 보안성, 실시간성, 성능을 확보하였다. 그런데 CSMP성능이 우수하면서 실시간성을 유지하는 것은 인증서 상태 정보를 검증자 목록과 인증서 상태의 등록을 분산시키고, 동시에 인증서 폐지시 실시간으로 동기화시키기 때문이다. 그러나 검증자 목록의 검증자수가 증가 할수록 인증서 폐지 전송 시간이 증가하는 것을 볼 수 있다.

[표 1] 인증서 폐지 전송 시간 **(단위:초)**

검증자수	1	2	5	10	50	100
폐지전송시간	0.04	0.05	0.06	0.18	0.53	1.37

따라서 검증자 수가 제한이 되어 있지 않다면 검증자 목록과 인증서 상태 목록의 동기화는 부하가 많이 걸리게 된다. 이에 향후 연구로 검증자 목록을 만들 때 가상식별번호를 만들어서 전송함으로써, 전송속도를 향상시키며, 서버 과부하 문제를 해결 할 수 있을 것으로 본다.

▌참 고 문 헌▐

[1] 이종후, 서인석, 윤혁중, 류재철, "무선랜 환경에서의 PKI 구축", 정보보호학회지, 제13권, 제1호, 2003.2

[2] 최진규, "WAP 환경에서 종단간 보안을 제공하는 TLS+포토콜의 설계 및 구현", 강원대학교, 석사학위논문, 2002.6

[3] 김용운,·김용진,·박기식,·박치, "WAP의 대안을 위한 무선 인터넷 통신 프로토콜 구조 연구", TELECOMMUNICATIONS REVIEW,·제10권, 6호, 2000.

[4] WAP, ""Wireless Application Protocol Arichtecture Sepcification," WAP Forum, http://www.wapforum.org/WAP, Nov ember 8, 1999.

[5] Microsoft , "Mobile Phones," http://www.microsoft.com/mobile/phones/default.asp"

[6] WAE, Wireless Application Environment Protocol Specification," WAP Forum, November 8, 1999, http ://www .wapforum.org/

[7] WSP, "Wireless Session Protocol Specification", "WAP Forum, November 8, 1999, http://www.wapforum.org/

[8] WTP, "Wireless Transaction Protocol Specification," WAP Frum, November 8, 1999 http://www.wapforum.org/

[9] WTLS, "Wireless Transport Layer Security Protocol Specification," WAP Forum, November 8, 1999, http://www.wapforum.org/

[10] WDP, "Wireless Datagram Protocol Specification ," WAP Forum, November 8, 1999, http://www.wapforum.org/

[11] C. Yae liau, s. Bressan and T. Kian-Lee "Efficient Certificate Revocation : A P2P Approach"' ASIAN 2002 Workshop on southeast Asian Computing Research. (ASIAN 2002)

[12] Jaegwan Park snd Kwangjo Kim, "A New Approach of X.509v3 Certificate for Full Path Validation", The 2002 Symposium on Cryptography and Information Security, January 2002.