무선 인터넷 환경의 WPKI 기반 사용자 인증에 관한 연구

이철승* · 박영옥* · 이호영** · 이준***

*조선대학교 대학원 컴퓨터공학과 · **초당대학교 정보통신공학과 · ***조선대학교 전자정보공과대학 컴퓨터공학부

A Study on User Authentication of Mobile Internet Environment Based on WPKI -

Cheol-seung Lee* · Young-ok Park* · Ho-young Lee** · Jeon-Lee***

*Dept. of Computer Engineering Graduate School. Chosun University.

**Dept. of Information Communication. Chodang University.

***Dept. of Computer Engineering. Chosun University.

E-mail : cyberec@sslab1.chosun.ac.kr

요 약

본논문은 WPKI환경에서 Kerberos 인증프로토콜을 이용한 사용자 인증문제를 해결하고자 한다. WAP Forum에서 정의한 보안구조 및 요소, 기존 인증시스템과 관련된 각종 암호 관련 기술을 살펴본 후, 무선 공개키 기반구조와 전송계층 보안등을 이용하여 응용레벨에서의 사용자 인증을 위해 서버 클라이언트가 지니는 설계상의 문제점과 E2E 보안상 취약점을 찾아 대안을 제공한다. 인증프로토콜인 Kerberos 와 그 단점을 보완 할 수 있도록 무선용 X.509 v3를 결합한 보안성이 우수한 WIM를 저장매체로 활용한 올바른 인증방법 해결책을 제시하고자 한다.

ABSTRACT

In this paper describes for use Authentication with the WPKI and Kerberos protocol. this paper is the security structure that defined in a WAP forum and security and watches all kinds of password related technology related to the existing authentication system. It looks up weakness point on security with a problem on the design that uses wireless public key-based structure and transmission hierarchical security back of a WAP forum, and a server-client holds for user authentication of an application level all and all, and it provides one counterproposal. Therefore, We offer authentication way solution that connected X.509 with using WIM for complement an authentication protocol Kerberos and its disadvantages.

키워드

WPKI, Authentication, Kerberos, X.509, WIM

Ⅰ. 서 론

무선 인터넷 기술이 가속화되면서 유선 상에서 제공받았던 여러 콘텐츠들을 무선 상에서도 제공받을 수 있게 되었지만 정보의 공유와 개방을 목표로 개발된 인터넷이 갖고 있는 기본적인 취약성, 무선네트워크, 무선단말기 의 제약성 때문에 유선의 콘텐츠를 그대로 수용할 수 없는 문제가 발생하고 있다. 이에 WAP(Wireless Application Protocol) Forum은 무선 인터넷이 가지는 제약점을 극복하고 효율적인 망 자원을 사용할 수 있도록 프로토콜을 정의함으로써 WAP을 통한 멀티 콘텐츠 제공자 와 사용자 사이의 프라이버시를 제공할 수 있는 인증이 활발히 진행되고 있다.

그러나 WAP의 구조는 유·무선간의 프로토콜 변화를 수행할 게이트웨이에서 보안의 취약점을 지님으로써, 무선의 단말기와 유선의 콘텐츠 제공자 사이의 단대 단 보안을 보장하지 못하는 단점을 지니고 있다. 이는 실제로 보안이 필요한 여러 응용 서비스에서 WAP을 적용하기 힘들게 됨으

로써 WAP을 채택한 무선 인터넷 인프라스트럭처에 커다란 문제를 지적되고 있다.

본 논문에서는 기존 인증시스템과 관련된 각종 암호 관련 기술을 살펴본 후 WAP Forum의 무선 공개키 기반구조 와 전송계층 보안등을 이용하여 응용레벨에서의 사용자 인증을 위해 서버 클라이언트가 지니는 설계상의 문제점과 단대 단 보안상 취약점을 찾아 대안을 제공함으로써 인증 프로토콜인 Kerberos[1]와 그 단점을 보완 할 수 있도록 무선용 X.509v3를 결합하여 보안성이 우수한 WIM(Wireless Identifier Module)[2]을 저장매체로 활용한 올바른 인증방법 해결책을 제시하고자 한다.

II. 인증시스템 기반 기술

1. WIM(Wireless Identifier Module)

WIM은 스마트카드 규격인 ISO/IEC 7816 과 PKCS#15에 기반해 설계됐다. WAP Forum에서 WAP기반에 사용할 수 있는 스마트 카드의 규격 외에 단말기와 스마트 카드간의 인터페이스를 맞춘 인증·보안 모듈이며, WIM은 무선 공개키 기반구조(WPKI) 와 전자서명 기능을 담고 있어서 유선방식의 PKI와 동급의 기밀성, 무결성, 거래 안정성을 유지하면서도 무선방식의 편리함을 누릴 수 있다. 또한 전송계층 보안을 위한 WTLS 핸드세이킹과 응용계층에서의 전자서명을 지원하는 역할을 수행한다.

2. Kerberos 인증 프로토콜

Kerberos는 중앙집중식 으로 하나의 안전한 인증 서버를 두어 사용자들을 인증할 수 있도록 한 인증 서비스이다. Kerberos v4가 가장 널리 사용되고 있으며, 보안결함을 몇 가지 수정하여 v5 가 Internet draft표준(RFC1510)으로 발표되었다.

Kerberos는 사용자에게 티켓(ticket)을 발급하여 사용 및 시간제한을 적용시켜 인증을 하기 때문에 안전하다. Kerberos v5에서는 영역(realm)이라는 개념을 도입하여 Kerberos서버와 여러 개의 클라이언트, 그리고 여러 개의 응용 서버로 구성된 완전한 서비스의 Kerberos환경을 구성하였고 다음과 같은 조건을 필요로 한다.

a. Kerberos 서버는 사용자ID와 해쉬 된 패스워드를 데이터베이스에 가지고 있어야 한다.
b. Kerberos 서버는 각 서비스를 제공하는 서버와 비밀키를 공유하여야 한다.
c. 외부 영역과 상호 인증을 지원하기 위해 각 상호운영 영역에 있는 Kerberos서버는 비밀키를 다른 영역에 있는 서버와 공유한다.

Kerberos는 3단계에 거쳐 인증절차 수행한다. 1단계는 인증 서비스 교환 단계, 2단계는 티켓 승인 서비스 교환단계 마지막 으로 3단계는 클라이언트서버 인증 교환 단계를 거쳐 인증을 한다.

3. X.509 인증서

X.509는 각 사용자와 관계된 공개키 인증서를 말한다. 사용자 인증서는 CA에 의해 발행된 것이며 CA나 사용자에 의해 디렉토리에 위치하게 된다. 인증서에 표현되는 정보는 사용자의 ID, 사용자의 공개키, CA의 정보, 서명으로 크게 구분되며, 각 인증서는 다른 인증서와 구별된다. 인증서는 인증기관의 비밀키로 전자서명을 생성하여 첨부한다. 디렉토리 서버 자체는 공개키의 생성이나 인증 기능에 대한 책임이 없으며, 단지 사용자가 인증서를 쉽게 얻을 수 있는 접속 장소를 제공할 뿐이다[3].

4. 기존 인증시스템 문제점

무선 인터넷 환경에서 대부분의 인증프로토콜은 비밀키 기반을 사용하기 때문에 확장이 힘들다는 단점을 지녔다. 이에 WAP Forum의 무선 공개키 기법 사용에 대한 적합성 여부가 새로운 문제점으로 제시되었다. 공개키 암호화 기법이 무선환경에 맞지 않고, 무선단말기의 연산능력의 제한으로, 공개키 암호화 기반의 암호화 기법을 사용할 경우 비밀키 기반의 암호화 기법의 사용시보다 약 1000배의 비용이 증가하게 되며, 네트워크 부하, 추가적인 하드·소프트웨어 설치가 불가피 하는 문제점이 있다. 이로 인해 무선용 X.509 v3 인증서를 통한 사용자 인증에 대한 연구가 활발이 진행 중에 있지만 X.509 인증서에 전자서명을 하는 곳은 CA 이기 때문에 사용자는 반드시 전자서명을 확인하기 위하여 CA의 고유 공개키를 가지고 있어야 한다. 사용자의 인증서를 확신하려면 공개키는 사용자에게 무결성과 인증이 제공되는 어떤 저장매체를 통해서 분배되어야 하는 어려움이 있다.

III. 무선 인터넷 환경의 인증 메커니즘

본 논문에서는 Kerberos v5, 무선용 X.509 v3, WIM을 결합한 인증시스템을 제안 한다.

먼저 무선인터넷 환경에서 안전하고 편리한 인증서비스를 지원하기 위해 보안성, 신뢰성, 가용성, 재사용공격 봉쇄, 투명성, 키 관리 용이성, 규모 등의 보안 요구사항을 반영하여 기존 인증시스템 의 단점을 해소하고 인증시스템에 대한 무선 환경에 적합성 여부를 평가 및 분석을 한다.

1. KXW 인증 시스템

기존 유선용 CA 솔루션들은 RSA 알고리즘을 이용한 인증서를 발급하고 있으며, 이를 무선 환경에 이용할 때에는 성능저하로 인해 현실적으로 이용할 수 없는 상태이다.

그러므로 빠른 Kerberos 알고리즘을 이용한

X.509 인증서 발급이 무선환경의 보안 인프라를 구축하는데 가장 시급한 문제이다.

본 논문에서는 KXW(Kerberos-X.509-WIM) 인증시스템을 제안한다. 모든 Kerberos는 영역과 상호 작용을 하기 위해서는 반드시 [N(N-1)]/2 개의 비밀키가 사전에 교환되어야 하며, 이는 키 관리의 문제점을 발생시킨다. 그러나 X.509 디렉토리 인증 서비스를 이용하여 쉽게 해결할 수 있다. X.509는 공개키 방식을 사용하기 때문에 외부 영역의 수가 10,000개가 되어도 비밀키를 10,000개만 보유하면 된다.

KXW 인증시스템은 CA에서 인증한 사용자 정보를 무선 인터넷 환경에서 유효 기간 내에 직접 인증이 가능하도록 해 주며, WIM을 적용하는 이유는 내부에 패스워드, 암호키 등을 안전하게 저장할 수 있어 보안성이 우수하고, 대규모 정보기억에 유용하며, 휴대가 가능하고 편리하여 대중화가 유리하기 때문이다.

KXW 인증시스템은 WPKI 기반구조에서 인증사슬에 의한 외부 영역의 상호 인증 개념을 도입한 것이다. 또한 Kerberos인증 프로토콜 절차를 응용하여 사용자가 이용하려는 서비스 서버를 통제하여 서버에 대한 보안성을 강화하였다.

가입자는 인증서를 발급 받기 위해 등록기관에서 직접대면을 통한 신원확인을 하며 신원이 확인된 가입자는 인증서 요청시 사용할 본인확인을 위한 참조코드(ID/Password)를 부여받는다. 가입자는 자신이 서명에 사용하는 전자서명 생성키(Private Key)를 생성한 후 전자서명 검증키와 개인 정보를 담은 인증서 발급요청정보를 작성하여 CA로 발급요청을 한다. CA는 자신의 전자서명 생성키로 가입자의 전자서명 검증키에 대하여 서명함으로써 가입자인증서를 생성하여 가입자에게 인증서를 발행하게 된다[4].

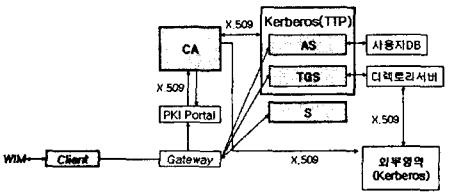

그림 1. KXW 인증시스템 구성도

2. Kerberos와 X.509 결합한 인증시스템 제안

2.1 접속 및 사용자 인증

a. 사용자는 Kerberos AS에게 자신의 인증과 원하는 TGS 서버에 관한 메시지를 전송한다.
b. Kerberos AS는 User DB에서 사용자 정보를 검색한다.
c. 정당한 사용자라면 요청한 TGS가 어느 영역에 있는지를 Directory Server에서 검색하게 된다.

만약 동일한 영역 내에 있는 TGS 서버라면 타 영역과의 인증, 외부 영역에 있는 디렉토리서버들의 공개키를 얻는 과정은 필요가 없다.

2.2 외부 영역과 디렉토리 연결

사용자가 원하는 TGS가 타 영역에 있을 경우 이를 원하는 타 영역까지 경로를 연결하는 과정을 그림2 에서 나타내고 있다. 많은 Kerberos영역이 있을 경우, 각 영역마다 존재하는 디렉토리 서버는 단지 연결설정의 역할만 할 뿐 인증 기능은 갖지 못하며, 인증에 관한 제반사항은 Kerberos에서 전담하기 때문이다.

X영역에서 Y영역의 PK_Y를 얻고자 할 경우 X영역과 A영역 연결, A영역과 B영역 연결, B영역과 C영역연결, 그리고 C영역과 Y영역 연결로서 이는 Y영역에 있는 TGS를 사용하기 위해 다음과 같은 전방인증체인을 생성한다. 이때 X영역은 Y영역의 PK_Y를 획득하게 된다.

A<<B>>B<<C>>C<<Y>>

이와 반대로 Y영역 에서는 X영역의 PK_X를 얻고자 할 때는 후방인증체인을 생성하는데 그 과정은 전방인증체인의 역순으로 다음과 같다.

C<<B>>B<<A>>A<<X>>

이제 사용자가 있는 X영역과 Y영역의 직접적인 연결이 이루어지며, Y영역의 PK_Y를 X영역에서 알게되었으므로 X영역의 Client는 Y영역의 PK_Y로 자신의 ID, 원하는 TGS 등을 암호화하여 전송하게된다[5].

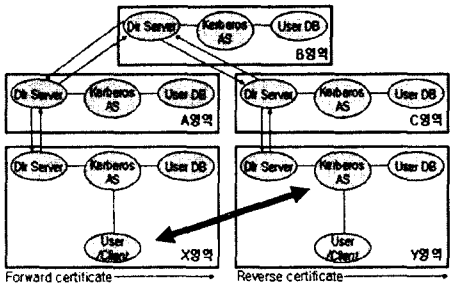

그림 2. 외부 영역과 디렉토리 연결

2.3 두영역간 키 교환

X영역과 Y영역간 연결이 직접적으로 이루어졌으며, 타 영역간에 있어 사용자를 인증하는 절차가 필요하게 된다. Y영역의 PK_Y를 X영역의 Client가 알고 있으므로 타 영역의 공개키로 자신이 보내고자 하는 메시지를 암호화하여 전송하게 된다. 그림3은 Y영역에서 X영역으로 공개키 PK_Y가 전송된 다음 직접적으로 두 영역간 키 교환이 이루어지는 모습을 보인다.

$Ticket_{TGS_Y}$ = Y영역의 TGT

$Ticket_{S_Y}$ = Y영역의 SGT
Authenticator = 클라이언트의 인증자

$Client_X$는 AS_Y에게 X.509를 이용하여 얻은 Y 영역의 공개키 PK_Y로 사용자 인증정보를 암호화하여 전송한다. AS_Y는 자신의 비밀키로 수신된 메시지를 복호화한 다음 다시 $Client_X$에게 X영역의 공개키 PK_X로 세션키 K_{C,TGS_Y}를 암호화하여 전송한다. 이때 $Ticket_{TGS_Y}$도 같이 보내는데 역시 여기에는 세션키 K_{C,TGS_Y}가 포함되어 있다. 이것은 $Client_X$와 Y영역의 TGS에게 은밀한 방법으로 세션 키를 분배하는 방법으로 이후부터는 두 영역간에 공개키를 사용하지 않고 비밀키로 메시지 인증교환 단계를 하게 된다. 나머지 과정은 Kerberos v5의 메시지 교환절차와 같다.

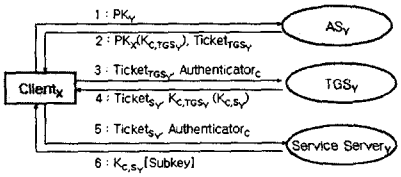

그림 3. 두 영역간 키 교환

IV. 제안 알고리즘

제안한 인증시스템 KXW의 특징은 클라이언트와 서버의 환경에서 AS 및 TGS를 두어 다단계 인증 서비스를 제공하는 메커니즘을 제공하고 있다. 즉, Kerberos의 다단계 인증 서비스 장점을 활용하였으며, Keberos v5에서 영역(Realm)은 제안하는 알고리즘에는 필요가 없다. 이는 X.509를 Kerberos와 접목하면서 디렉토리서버가 영역(Realm)의 역할을 대신하여 영역들의 구분을 해주며 외부 영역과의 상호 연결을 해주기 때문이다. X.509디렉토리 인증표준을 이용하여 인증서비스 교환단계에서 패스워드의 평문 전송 없이 상대방의 공개키로 암호화해서 전송하여 AS로부터 인증을 받을 수 있도록 하였다. 이는 패스워드 전송에 대한 도청 및 가로채기 위협을 방어해준다.

WIM의 접목은 제안한 시스템의 보안성을 강화시켰다. 또한 카드를 위조하기 위해서는 CA의 인증서를 위조해야하기 때문에 안전하다고 할 수 있다.

제안한 인증시스템은 RSA 전자서명 알고리즘과 Kerberos인증프로토콜, 그리고 X.509 디렉토리 표준 프로토콜을 기본으로 하고 있으며 $Client_X$와 $Server_Y$사이에서 인증 정보가 교환되는 알고리즘은 다음과 같이 제안한다.

① $Client_X \rightarrow AS_X$:M([Option], ID_C, ID_{TGS_Y}, Times, Nonce1)
② $AS_X \rightarrow Client_X$:M($ID_C$, EK_C (PK_Y, Times, Nonce1, ID_{TGS_Y}))
③ $Client_X \rightarrow AS_Y$:M($EPK_Y$([Option], ID_C, ID_{TGS_Y}, Times, Nonce2))
④ $AS_Y \rightarrow Client_X$:M($ID_C$, $Ticket_{TGS_Y}$, EPK_X(K_{C,TGS_Y}, Times, Nonce2))
$Ticket_{TGS_Y}$= EK_{TGS_Y}([Flags], K_{C,TGS_Y}, ID_C, AD_C, Times)
⑤ $Client_X \rightarrow TGS_Y$:M([Option], $Ticket_{TGS_Y}$, $Authenticator_C$, Times, Nonce3, ID_{S_Y})
$Ticket_{TGS_Y}$= EK_{TGS_Y}([Flags], K_{C,TGS_Y}, ID_C, AD_C, Times)
$Authenticator_C$= EK_{C,TGS_Y}(ID_C, TS1)
⑥ $TGS_Y \rightarrow Client_X$ M(ID_C, $Ticket_{S_Y}$, EK_{C,TGS_Y}(K_{C,S_Y}, Times, Nonce3, ID_{S_Y}))
$Ticket_{S_Y}$= EK_{S_Y}([Flags], K_{C,S_Y}, ID_C, AD_C, Times)
⑦ $Client_X \rightarrow Server_Y$:M([Option], $Ticket_{S_Y}$, $Authenticator_C$)
$Ticket_{S_Y}$= EK_{S_Y}([Flags], K_{C,S_Y}, ID_C, AD_C, Times)
$Authenticator_C$= EK_{C,S_Y}(ID_C, TS2, [Subkey, Seq#])
⑧ $Server_Y \rightarrow Client_X$:M($EK_{C,S_Y}$(TS2, [Subkey, Seq#]))

그림 4. 제안 알고리즘

V. 결론 및 향후 연구 방향

본 논문은 무선인터넷 환경의 사용자 인증에 대해 분석하고 기존 인증시스템에 대한 문제점을 찾아 KXW인증시스템을 제안하였다.

제안한 인증시스템의 보안을 달성하기 위한 기술적인 방법은 암호기술, 해쉬함수, 전자서명, 키 관리 등과 같은 방법을 사용하였다. 그리고 인증시스템의 구성요소로 다단계 인증서비스를 지원하는 Kerberos 와 Kerberos의 단점을 보안을 위한 디렉토리 인증프로토콜인 X.509, 인증서 그리고 무선단말기의 열악한 환경을 극복하기 위해 자체 연산 능력과 메모리를 보유하고 있는 WIM으로 구성하였다. KXW 인증시스템은 기존의 Kerberos보다 보안성 및 키 관리의 효율성을 높였다. 무선인터넷 시장의 보안 및 인증에 관한 연구는 활발히 진행 중에 있다. 무선인터넷 시장 규모가 크지 않지만 앞으로 그 시장규모는 확산될 것이며, 이에 따라 좀 더 안전한 무선인터넷 환경 구현을 위해서는 BlueTooth 기술들을 접목시킨 연구를 통해 보안성 및 효율성이 강화된 강력한 무선인터넷 환경을 더 연구해야 될 것이다.

참고문헌

[1] K. Raeburn, "Encryption and Checksum Specifications for kerberos 5.", March 2003.
[2] WAP Forum, WAP Identity Module Specification, 18 February 2000,
[3] M.Myers, "X.509 Internet Public Key Infrastructure On-line Certificate Status Protocol-OCSP." Network Working Group, 1999.
[4] "Wireless Application Protocol Public Key Infrastructures Definition", WAP forum, Feb. 2000
[5] R.Hously, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile." Network Working Group, RFC2459, January,