Design of User Authentication Mechanism based on WPKI

Cheol-seung Lee [*], Do-jun Park[*], Myung-souk Shin[*], Jeong-gi Lee[*], Joon Lee[*]
Dept. of Computer Engineering, Chosun University, Gwangju 501-759, Korea
Tel : +82-62-230-7758 Fax : +82-62-230-7381 E-mail: cheolseung@hotmail.com

Abstract : In this paper we challenge the user Authentication using KerberosV5 authentication protocol in WFKI environment. 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 layer all and all, and it provides one counterproposal. Therefore, We offer authentication way solution that connected X.509 V3 with using WIM for complement an authentication protocol KerberosV5 and its disadvantages.

1. INTRODUCTION

A change of these paradigms has made popularization of wireless communication and new service called wireless Internet. Wireless communication has developed into a base on audio service as such the existing telephone services, because the Internet has developed into a base by data service, a service offer method, a characteristic of traffic have a very different characteristic.

It did a definition with a protocol that the wireless Internet overcame the restriction point that had by a WAP forum in this, and can efficient use ring resources.

WAP was adopted as important technology in construction of wireless Internet environment recently by a lot of development enterprises. WAP structure composed a gateway for wire, wireless protocol conversion and Internet content conversion.

It had a wireless environment and vulnerability of E2E security of wire environment, offered a solution with various ways in this E2E problem.

The authentication that compunction contents provider comes for WAP, can provide user privacy between users is authentication proceeded actively. But, it cannot offer a perfect solution about a user authentication problem, develops into wireless Internet technology of WAP, becoms a large obstacle.

A purpose of 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, a server-client holds for user authentication of an application level all and all. it provides one counterproposal.

This paper quotes the encryption algorithm experiment results in a wireless terminal for a performance analysis of authentication of an application level and analyzes performance. We offer authentication way solution that connect X.509 with using WIM for complement an authentication protocol Kerberos and its disadvantages.

2. BACKGROUND

2.1 WIM (Wireless Identity Module)

WIM is designed by ISO/IEC7816 and PKCS#15 base smart card standard. Also, it is Authentication security module that set interface between wireless terminal and smart card except standard of smart card that can use based on WAP, WIM contains WPKI(Wireless Public Key Infrastructure) and digital signature function, can use convenience of wireless system keeping confidentiality of PKI(Public Key Infrastructure), confidentiality, integrity, and transaction stability.

Also, achieves WTLS handshaking for transmission layer security part that support digital signature in application layer [2].

2.2 Kerberos

Kerberos has a safe authentication server host operating system, is authentication service being able to authentication users. KerberosV5 is decided by Internet draft standard (RFC1510) after modification Kerberos security defect [8].

Kerberos provides a means of verifying the identities of principals (e.g. a workstation user or a network server) on an open network. This is accomplished without relying on assertions by the host operating system, without basing trust on host addresses, without requiring physical security of all the hosts on the network, and under the assumption that packets traveling along the network can be read, modified, and inserted at will [9].

The basic Kerberos authentication process proceeds as follows : client sends a request to the authentication server (AS) requesting credentials for a given server.

The AS responds with these credentials, encrypted in the client's key.

The credentials consist of a "ticket" for the server and a temporary encryption key (often called a "session key").

The client transmits the ticket (which contains the client's identity and a copy of the session key, all encrypted in the server's key) to the server.

The session key (now shared by the client and server) is used to authenticate the client, and may optionally be used to authentication the server. It may also be used to encrypt further communication between the two parties or to exchange a separate sub-session key to be used to encrypt further communication.

KerberosV4 has an authentication applying tickets through the limit of time and using.

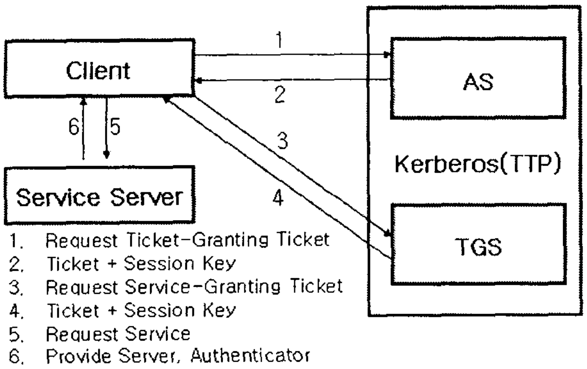


Fig.1. Kerberos authentication.

KerberosV5 composed a perfect Kerberos environment consisted of Kerberos server and majority's client, application server to introduce area (Realm) concept [1].

2.3 X.509 V3

The use of X.509 certificates within Internet applications for those communities wishing to make use of X.509 technology. Such applications may include WWW, electronic mail, user authentication, and IPsec.

User of a public key shall be confident that the associated private key is owned by the correct remote subject (person or system) with which an encryption or digital signature mechanism will be used.

This confidence is obtained through the use of public key certificates, which are data structures that bind public key values to subjects.

The binding is asserted by having a trusted CA (Certificate Authority) digitally sign each certificate.

X.509 V3 is public key certificate that is related to each user. Certificate that is published CA located to directory by use and CA, and information expressed in certificate is consisted of user ID, user public key, CA information and digital signature.

Certificate attach creating digital signature to CA's private key, and Directory server has a responsibility about creation or the function of authentication of public key, that user can only serve a connection place getting certificate easily [3].

2.4 Problem of existing authentication system

Because most authentication protocols use private key base in wireless Internet environment, is impossible to manage private key effectively in network of bulky scale and information is lost in process that encipher document that is encrypted again after do decryption from WAP gateway or offers attacker a tapping possibility opportunity.

Thereby Adaptedness availability about WAP Forum's wireless public key encryption technique is used presented as new problem. However, public key encryption notation does not fit in wireless environment because of low transfer rate wireless terminal and narrow bandwidth of wireless Internet environment, WML is available transposition through HTML (hypertext markup language) and filtering, but current WAP protocol is operated WTLS only the place of operation and security authentication between web server and terminal is not offered.

Also, problem that additional hardware and software equipment do inevitability in network subordinate and WAP gateway construction for protocol conversion happened [6] .

Thereby, the study for user authentication through wireless X.509 V3 certificate is progressing. However, because the place that do digital signature in X.509 V3 certificate is CA, user must have CA's original public key for confirming digital signature. And if user confirms a certificate, problems that should be shared through certain save medium that public key produced integrity and authentication to user are given [7] .

3. AUTHENTICATION MECHANISM OF WIRELESS INTERNET ENVIRONMENT.

3.1. KXW authentication system.

In this chapter, we design user authentication mechanism based on WPKI.

We Estimate and analyze adaptedness availability of wireless environment after considering problems of existing authentication systems techniques and authentication system and requirements and components of KXW authentication system.

CA solutions for existing wire create certificate using RSA algorithm. When we apply this to wireless environment, we can not use actually by performance degradation. Therefore, the first solving is problem that the creation of X.509 V3 certificate using fast KerberosV5 algorithms must construct security infra of wireless environment.

KerberosV5 has to be exchanged private key of [N(N- 1)]/2 in the advance certainly for Realm and interaction.

This is created key management problem. But, we can solve easily, if we use X.509 V3 directory authentication service of public key method and have 10,000 security keys although the number of outside area's is 10,000.

KXW authentication system creates user information certificated in CA possible in validity in wireless Internet environment.

Reasoning of apply WIM is because it can store inside password, encryption key etc. safely, security is excellent, and useful in large scale information memory, and carrying along and popularization are profitable.

KXW authentication system introduces a mutual authentication concept outside area by authentication chain in WPKI base structure, And Strengthened security about server for controlling service server for user to use KerberosV5 authentication protocol formality.

Client creates digital signature creation key (Private Key) after do identification through interview, and is given reference code (ID/Password) for principal confirmation directly in registrar to be created certificate.

Client does issuance request information to make certificate issuance requiring information by CA included digital signature verification key and personal information.

By CA signs about client's digital signature verification key with using own digital signature creation key, creates client certificate and publishes certificate to client [4].

3.2 Joins KerberosV5 and X.509 V3

3.2.1 Connection and user authentication.

User transmits own quotation and message on wanting ticket approval server (TGS) to Kerberos authentication (AS).

After KerberosAS searches user information in user database (UserDB), and searches in Directory server (DirServer) which area a required TGS is that require if it is a lawful user.

If it is TGS within same area, authentication with outside area and The process of getting public key of DirServers of outside area do not need.

3.2.2 Outside area and directory connection.

In case that there is TGS that user wants in other area, connect path to other area using X.509 V3 is as follows Fig. 2.

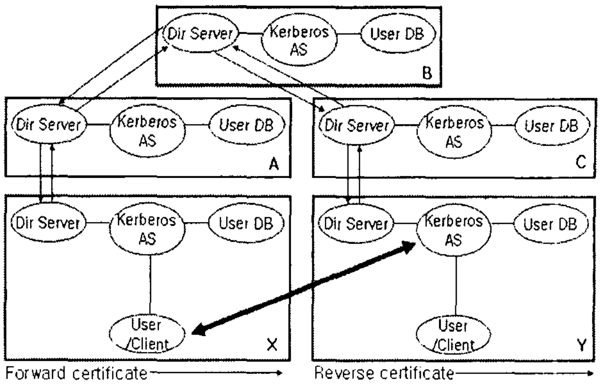


Fig.2. X-Y area connection after authentication between directories

In case that there are a lot of Kerberos areas, DirServer of each area does only, The role of connection set and user authentication takes complete charge in AS.

Create forward authentication chain using TGS of Y area, when wish to get public key (PK_Y) of Y area in X area. In contrast, when wish to get public key (PK_X) of X area in Y area, creates reverse authentication chain.

After direct conneption of X area and Y area is consisted, and we know PK_Y in X area, therefore, user of X area shall had send on encrypting own ID and wanting TGS to PK_Y [5].

Table 1 Authentication chain

Forward authentication chain	A<<B>>B<<C>>C<<Y>>
Reverse authentication chain	C<<B>>B<<A>>A<<X>>

3.2.3 Key exchange between two areas.

If connection between X area and Y area is consisted directly, formality that quote user is as follows Fig. 3.

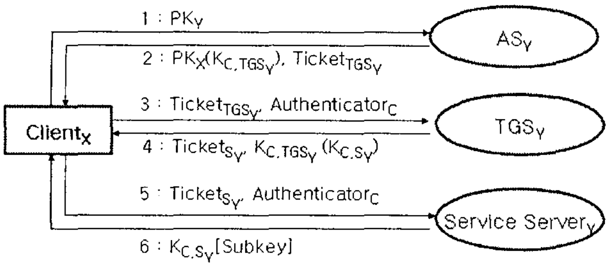
User encrypts user authentication information by PK_Y and transmits it to authentication that gets using X.509 V3.

AS_Y decrypts message received by own private key and encrypts session key ($K_{C.TGS_Y}$) sharing Cliert X and TGS by PK_X to Client X again and transmits it.

And session key ($K_{C.TGS_Y}$) sends together TGS access approval ticket ($Ticket_{TGS_Y}$) of Y area, and it is included session key ($K_{C.TGS_Y}$) have too.

This method divides session key by secreting method to TGS of Y area and user.

Without using public key between two areas from the next, processes message authentication switching by secret key. Remainder process is same as message switching formality of KerberosV5.


1 : PK_Y
2 : PK_X(K_C.TGS_Y), Ticket_TGS_Y
3 : Ticket_TGS_Y, Authenticator_C
4 : Ticket_S_Y, K_C.TGS_Y (K_C.S_Y)
5 : Ticket_S_Y, Authenticator_C
6 : K_C.S_Y[Subkey]
Client_X
AS_Y
TGS_Y
Service Server_Y

$Ticket_{TGS_Y}$ = Ticket approval ticket of Y area.

$Ticket_{S_Y}$ = Service approval ticket of Y area.

Authenticator = Client's authenticator.

Fig.3. Key exchange between X-Y area

3.2.4 Proposal algorithm

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 $Server_Y \rightarrow Client_X{:}M(EK_{C,S_Y}(TS2, [Subkey, Seq\#]))$

Fig.4. Proposal algorithm

Characteristic of a proposed KXW system is mechanisms that provide cascade system authentication service to use AS and TGS in server client environment.

DirServer have a interconnection with outside area on dividing areas in stead of Realm's role with X.509 V3 connecting with KerberosV5.

Transmit and encrypt it in other person public key without plaintext transmission of password at authentication service switching stage using X.509 V3 directory authentication standard. This is albe to take user authentication without tapping and intercept threat from AS.

The connection of WIM combining strengthened security of proposed system. It is secure CA's certificate to forgery WIM.

Proposed authentication system is based on RSA digital signature algorithm and Kerberos V5 authentication protocol, and X.509 V3 directory standard protocol.

Algorithm that authentication information is exchanged between user and server is follows Fig. 4.

4. AUTHENTICATION SYSTEM ASSESSMENT AND ANALYSIS.

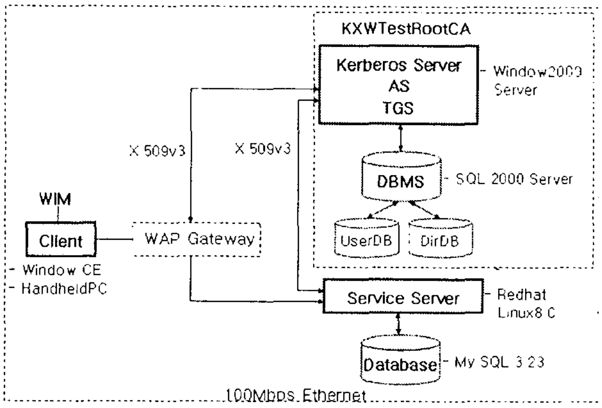


Fig.5. The diagram of proposal system structure.

After user stores user name, user's digital signature, digital signature mode used in certificate publish, serial number of certificate, certificate term of validity time, Certificate Authority name to UserDB of KXW-TestRootCA for certificate publish, user is given reference code for authentication from KXWTestRootCA. User uses WindowCE HandheldPC to use KXWTestRootCA and shared specification service server. And User transmits TGS message to AS of KXWTestRootCA.

After As searches if it is a reasonable user to use UserDB, it searches TGS user wants at DitDB, and transmits X.509 V3 certificate if user is lawful.

User selects WIM by certificate store medium, and is published certificate after inputing new passwords to certificate publish. User uses a published certificate and service server in outside area.

For encryption algorithm achievement performance verification of KXW authentication system, achievement performance of HandheldPC is compared to Table 2.

Compared encryption algorithm achievement performance of KXW authentication system that use HandheldPC in Table 2.

Table 2 compare of Encryption algorithm.

	Creation	Sign	Verification
RSA-1024bit	5.234	0.253	0.010
ECDSA(ECC)-160bit	0.022	0.022	0.034
KXW-160bit	0.143	0.012	0.023

In Case of RSA using most widely in digital signature, were required a lot of times.

However, because ECDSA and KXW is small one dimension of key when offer security level such as RSA, can confirm that key creation time required is short.

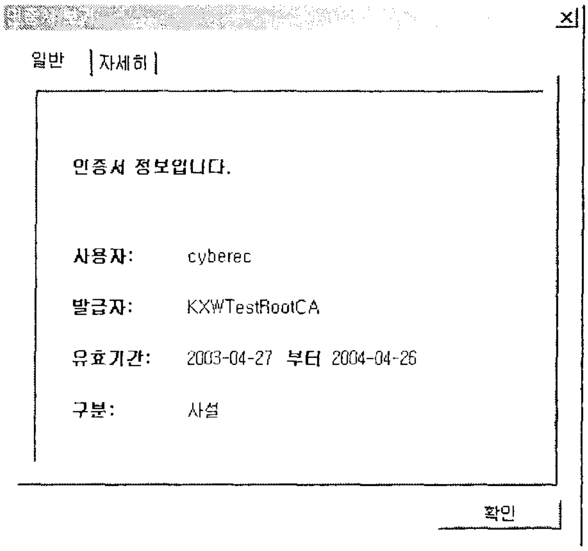
We can confirm that ECDSA's key creation time is shorter than KXW because the process such as decimal analysis does not need.

RSA is more profitable than ECDSA or KXW in key verification. But, when consider throughput of wireless terminal, RSA does not fit in wireless environment, and we could know to profit more a proposed KXW than ECDSA in signature and verification part.

And KXW authentication system does easily key management and prevented opening effect of network in bulky scale networks.

Existent wireless Internet environment using private key encryption method should manage a lot of keys in authentication with other area. However, KXW certification system problem solved session key division process by public key encryption method.

The speed to encryption authentication information of the propose system in slower than existing Kerberos because the proposal system uses public key method.



인증서 정보입니다.

사용자: cyberec

발급자: KXWTestRootCA

유효기간: 2003-04-27 부터 2004-04-26

구분: 사설

Fig.6. Certificate of KXWTestRootCA

5. CONCLUSION

In this paper we analyzed for user authentication of wireless Internet environment, and found problems for existing authentication system and proposed KXW authentication system.

We used method such as encryption technology, hash function, digital signature, and key management to make a secure of proposal system.

Proposal authentication system is composed by KerberosV5, X.509 V3 and WIM.

Most of peoples are using a wireless Internet. But there are not provided mutual lawful authentication between Client and Server.

KXW authentication system is formed strong authentication chain of CA and wireless Internet environment improving security and key management more than existing Kerberos environment.

We have focused on authentication. But, there must to be provided additional services. For example, after authentication is done, authorization service must be provided.

Finally, for the realization of the pervasive wireless Internet environment, application for this environment must be developed.

References

[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,

[6] R. Housley and other, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile.", Jan, 1999.

[7] P.Gutmann, "Internet X.509 Public Key Infrastructure operational protocols.", Internet Draft, <draft-ietf-pkix-certstore-http-05.txt>, 2003.

[8] S.Hartman, K.Raeburn, "The Kerberos Network Authentication Service v5", Internet-Draft,

[9] Note that this can make applications based on unreliable transports difficult to code correctly. If the transport might deliver duplicated messages, either a new authenticator must be generated for each retry, or the application server must match requests and replies and replay the first reply in response to a detected duplicate.