Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

A Method for Authentication Services in Wireless Networks

Huy Hoang Ngo
Monash University, hhngo1@student.monash.edu.au

Xian Ping Wu
Monash University, xpwu1@student.monash.edu.au

Phu Dung Le
Monash University, phu.dung.le@infotech.monash.edu.au

Campbell Wilson
Monash University, campbell.wilson@infotech.monash.edu.au

Recommended Citation

Ngo, Huy Hoang; Wu, Xian Ping; Le, Phu Dung; and Wilson, Campbell, "A Method for Authentication Services in Wireless Networks" (2008). *AMCIS 2008 Proceedings*. 177.
http://aisel.aisnet.org/amcis2008/177

A Method for Authentication Services in Wireless Networks

Huy Hoang Ngo[1], **XianPing Wu**[2], **Phu Dung Le**[3], **Campbell Wilson**[4]

School of Information Technology, Monash University

[1]{hhngo1},[2]{xpwu1}@student.monash.edu.au,
[3]{phu.dung.le},[4]{campbell.wilson}@infotech.monash.edu.au,

ABSTRACT

With the widespread use of wireless network services and applications, security is a major concern. From wireless network security aspects, authentication for services is very important especially in Internet banking. In this paper, an authentication method for wireless networks using dynamic key theory is presented. The dynamic key theory is used to produce "one time keys" for authentication. These one time keys will improve the efficiency and security of wireless authentication. It can be applied for Internet banking and services in wireless networks.

Keywords

Dynamic key, authentication, wireless networks, services.

INTRODUCTION

In the recent year, the rapid growth of wireless network services has brought not only convenience but also security challenge. With the ability of providing access to information from anywhere and anytime, wireless networks can bring flexibility and accessibility to the services. However, due to the radio transmission nature, communication in wireless network services is more vulnerable than in wired networks. In wireless networks, an adversary can mount attacks by capturing, replaying and even modifying the messages to obtain authorised access to the services.

To protect the wireless network services from malicious attacks, authentication is an important component in security for wireless network services. Especially in Internet banking and services, authentication is the utmost crucial service. The most common approaches (Adoba and Simon, 1999;Harbitter and Menasce, 2001;Raju, 2007) are using asymmetric cryptography to enhance the security of the authentication systems. On the other hand, mobile devices using in wireless networks often have limitations such as low power processors, small memory and limited battery powers. The asymmetric cryptography in these proposed authentication protocols decreases the performance and consumes a lot of battery power on the mobile devices. There are some authentication protocols (Fox and Gribble, 1996; Pirzada and McDonald, 2004; Chien and Jan, 2003) extends adapt Kerberos authentication method (Neuman and Ts'o, 1994) for wireless networks. However, the security of these proposed protocols depends on long term shared keys for exchange session keys which are may be vulnerable under cryptanalysis attacks (Tang and Mitchell, 2006). Furthermore, re-using the same session key for different services provided by the same system can be a real problem for wireless users even this is acceptable under wired environments.

In this paper, an authentication method for wireless networks using dynamic key theory is presented. We propose a new approach for authentication based on dynamic keys for wireless users accessing service. The re-used cryptography keys are replaced by dynamic keys. Based on the dynamic keys, the proposed work provides a better authentication solution to many systems which provide different confidential services, especially banking systems.

In the following sessions we will begin with the discussion of the Kerberos authentication method. We will then introduce the new proposed method and analyze the security and efficiency of the proposed method. Finally, we give a conclusion on our paper and discuss possible future work.

RELATED WORKS

The Kerberos Authentication Method (Neuman and Ts'o, 1994) uses a trusted third party named Key Distribution Center (KDC) to distribute session keys via tickets. With these tickets and session keys, clients can authenticate to servers. The Kerberos authentication protocol can be described in five steps. Client finds the Service and KDC in the network. In the first step, he sends the request to authenticate to KDC. After that, KDC issues a ticket for Client to authenticate to KDC in the second step. In order to request service ticket and service session key in the third step, Client sends the KDC ticket and the authenticator to KDC. After being authenticated with KDC, he is able to obtain the service session key via ticket in step 4. In the final step, Client creates a new service authenticator and sends it with the ticket to Service to authenticate. The five steps protocol is shown as in Figure 1.

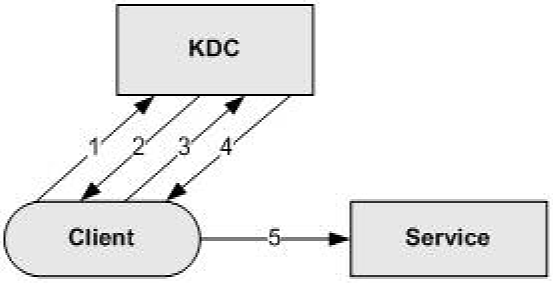

Figure 1. The Kerberos Authentication Method

Kerberos authentication method has been used for many authentication systems. The original Kerberos method relies on symmetric key encryption for authentication and the concept of dual authentication. It has been used for most of the standard Authentication Services in Unix and Windows for many years.

There are several projects of adding public key infrastructure into Kerberos method. Tung et all proposed the Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) (Tung, 2001), Public Key Cryptography for Inter-realm Authentication (PKCROSS) (Tung, 1998) and Public Key Utilising Tickets for Application Server (PKTAPP) (Medvinsky, 1997).

There are also a few extensions of Kerberos Authentication Method for wireless networks. In Charon method, Fox and Gribble (Fox and Gribble, 1996) proposed to add proxies in the Kerberos to authenticate on the behalf of wireless clients. In another effort to reduce the traffic, Pirzada and McDonald proposed one phase authentication in Kaman (Pirzada and McDonald,. 2004). These methods are based on symmetric cryptography and timestamp to prevent replay attacks.

In the Kerberos and its extensive authentication method, there are two types of cryptography keys: session key and long term shared key. Session key is the encryption key for normal communication between parties. On the other hand, long term shared key is used to encrypt the messages that exchange session keys. In Kerberos method, there are three long term encryption keys using to encrypt the KDC and service tickets sharing between KDC, Service and Client. Although these long-term shared keys are never transferred directly between parties, the cryptography systems are quite often vulnerable to brute force attacks.

To reduce the above risks, the major solution is to increase the key sizes of the cryptography. However, increasing the key sizes often lead to higher computation cost especially in asymmetric cryptography systems. Furthermore, Lenstra (Kirk 2007) said the 1024 bit RSA encryption using in most banking and e-commerce systems may not be effectual in a few more years. Therefore, the key sizes of permanent keys and the cryptography itself in authentication methods are the major issues for wireless networks.

Besides permanent keys, timestamp is also an issue in Kerberos. Most of the authentication systems in Kerberos method are based on timestamp to verify the freshness of the messages and detect replay attacks from intruders. If the clocks on clients, Services and KDC are not synchronized, the authentication systems are vulnerable under suppress-replay attacks(Gong 1992). Besides vulnerable security of the current time synchronization services (Bellovin and Merritt 1990), it is also inefficient to maintain clock synchronization for all parties in the authentication method regularly.

THE PROPOSED AUTHENTICATION METHOD

In this section, we describe our proposed authentication method. Along with the authentication method is the dynamic key generation and dynamic key management which is used to generate and synchronize the dynamic authentication and cryptographic keys. The final part describes the authorisation verification.

Notation

The notations used throughout this paper are listed as follows:

▪ C	:	Client
▪ U	:	user identity
▪ AS	:	KDC or Authentication Server
▪ N_1, N_2	:	nonces (random numbers)
▪ add	:	Network address of mobile client
▪ K_S’	:	dynamic key sharing between service and AS

- K_U’ : dynamic key sharing between user and AS
- K : session key
- Tc,s= {U, C, S, add, N_2, K}K_S’: ticket
- Ac,s= {C, N_2}K: the service authenticator

The Proposed Method

The proposed method is derived from the Kerberos authentication. In the method, there are three entities: Client, Service and Authentication Server. The method is shown in Figure 2. KDC named as Authentication Server is still used as the trusted third party to issue the ticket for authentication to the service server.

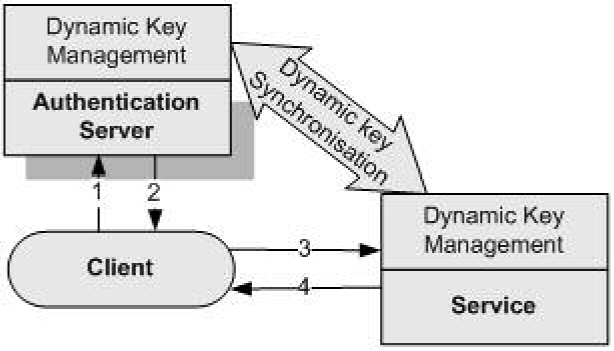

Figure 2. The Proposed Authentication Method

To authenticate to a service, Client sends a ticket request to Authentication Server. Authentication Server sends back to Client a ticket and a session key encrypted by secret key. By decrypting the message, Client can combine the authenticator from the session key. In the next step, he sends both the ticket and the authenticator to Service to verify legitimation. If the system needs mutual authentication, service sends back to Client a successful message. The message flow in the authentication can be formalized as follows:

1. C → AS: U, C, AS, S, N_1

2. AS → C: {K, N_1, N_2} K_U’, Tc,s

3. C → S: Tc,s, Ac,s

[4]. S → C: {N_2+1}K

Message 4 is optional for mutual authentication.

The main difference between Kerberos and this method is the dynamic key system. In this method, there is no long term pre-shared encryption key. Instead of the long term shared crytographic keys, the dynamic keys K_U’ and K_S’ are used to encrypt the ticket and the authenticator. After every successful authentication request, both dynamic keys K_U’ and K_S’ are regenerated the new value. These dynamic keys are generated, managed and distributed by a Dynamic Key Management.

At Service Server, Authentication Module comprises two main units: The Dynamic Key Management and the Ticket Verification Module. The structure of Authentication Module at Service Server is shown in the Figure 3. The Dynamic Key Management module is used to manage dynamic key KS’. In turn, the Ticket Verification Module validates the ticket Tc,s and authenticator Ac,s. If the ticket and authenticator are valid, the client is authenticated.

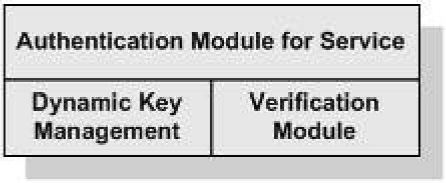

Figure 3. The Structure of Authentication Module at Service

The Authentication Server structure in Figure 4 includes two main modules: The Dynamic Key Management and the Ticket Granting Module. At first, the Dynamic Key Management module at authentication server manages both dynamic key K_U’ and K_S’. Meanwhile, the Ticket Granting Module validates the authorization of user U on service S to generate the ticket Tc,s.

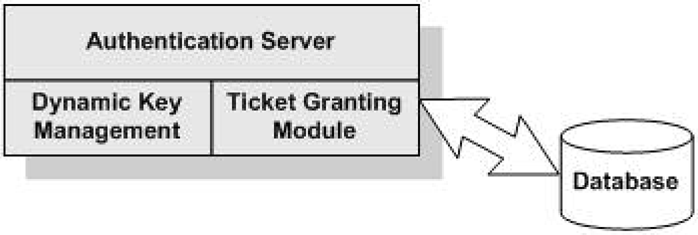

Figure 4. The Structure of Authentication Service

Dynamic Key in Authentication Method

The Dynamic Key Generation Technique

Several techniques (Rubin and Wright, 2002) (Li and Zhang, 2004) have been proposed to generate dynamic keys offline using for cryptography and authentication. We offer to use the Limited Used Key Generation Scheme (Kungpisdan et al., 2003) for generate the sequence of dynamic keys in our authentication method. The key generation scheme is based on:

- Master key K_{AB} sharing between client and authentication server. Although this key is permanent, it is only used once to be the seed for key generation.
- “Distributed key” DIK sharing between client and authentication server. This key is renewed regularly by key exchange system, and
- Finally the key hash function h(M, K) of the message M and key K.

The dynamic key generation is described in six steps as follows:

1. Authentication Server generates the distributed key DIK and sends it to client via authenticated key exchange protocol.
2. Both client and Authentication Server calculate the set of preference keys:

   $K_1 = h(DIK, K_{AB})$
   $K_2 = h(DIK, K_1)$
   ..
   $K_m = h(DIK, K_{m-1})$
3. Authentication Server generates a random number r and send it to client.
4. From the random number r, both Authentication Server and client calculate the middle keys and the SIK as follows:

   w = r mod m
   K_{Mid1} is the middle key of $\{K_1 \ldots K_w\}$
   K_{Mid2} is the middle key of $\{K_1 \ldots K_{Mid2}\}$
   and SIK = $h(K_{Mid1}, K_{Mid1})$.
5. Both Authentication Server and client generate the sequence of dynamic keys based on the SIK and DK as follows:

   $SK_1 = h(SIK, DK)$
   $SK_2 = h(SIK, SK_2)$
   ...
   $SK_n = h(SIK, SK_{n-1})$

When all the keys in the key sequence are used, Authentication Server and Client generate a new key sequence. The dynamic key SK_n will be used as the new distributed key DIK and the process to generate the set of dynamic key is restarted from step 2.

The Dynamic Key Management

To manage the dynamic keys in authentication system, the Dynamic Key Management modules are used in Authentication Server and Service Server. The dynamic key management module has two main functions: dynamic key generations and key distribution (or synchronization). However, because the characteristics of dynamic key K_U' are different from K_S', the Dynamic Key Management module in Service Server is different from the module in Authentication Server.

After every authentication request, the ticket $T_{c,s}$ is already used. To make this ticket become ineffective and un-reusable, the value of dynamic key K_S' sharing between Authentication Servers and Service Server is required to be changed. This operation is mandatory even if an un-successful authentication request is made. This requirement can help to prevent spoofing attack from breaking the ticket cryptography with the key K_S'. After Service Server receives and validates the ticket $T_{c,s}$ and authenticator $A_{c,s}$ in message 3, the Dynamic Key Management module in Service Server generates the new value for K_S' and distributes the new value of K_S' to Authentication Servers. In other cases, when the ticket $T_{c,s}$ is invalid and the authentication request is rejected or Service Server is failed to receive ticket $T_{c,s}$ and authenticator $A_{c,s}$, it is also generates and distributes the new value for K_S'.

Similar to the dynamic key K_S', after being re-used for long period of time, the key K_U' becomes vulnerable under cryptoanalysis attacks. The dynamic key K_U' sharing between client and Authentication Server is used to encrypt the session key K. To reduce the risk from being exposed under cryptoanalysis attacks, the dynamic key K_U' is required to re-generate its value.

However, updating the dynamic key K_U' is more complicated than that of the updating the dynamic key K_S'. If the key value is changed after every authentication request, the client has to update keys even when the intruders make false authentication requests. Furthermore, client is more vulnerable under Denial of Service attacks risk. On the other hand, if key value is changed only after every successful authentication request, the key K_U' will be re-used after unsuccessful authentication requests. Therefore the key K_U' is vulnerable under cryptoanalysis attacks. We propose to update key value for K_U' in a shorter period when the population is not high and longer period of time when the population is high.

Authorization Verification

The authorization verification and ticket verification are the most important parts of authentication process in the method. The authorization verification is done at Authentication Service after receiving message 1. The ticket verification is done at Service Server after receiving message 3.

Authorization Verification and Ticket Granting

In Authentication Server, the Ticket Granting Module connects to the Authorization Database to verify authorization. If the authorization is confirmed, it uses the dynamic key K_S' to combine the ticket $T_{c,s}$ and generates the session key K. Before sending the ticket and session key to client, at the final step, Ticket Granting Module encrypts them with the dynamic key K_U'.

Before granting the ticket, Authentication Server will verify whether user U has authorization to access Service Server S from Authorization Database. If the authorization verification process is successful, the ticket is issued and sent to user. Because of the encryption using dynamic key K_S', the ticket in the proposed method cannot be re-used. It is "*one time authentication ticket*".

Ticket Verification

At the Service Server, Ticket Verification Module includes five basic tasks. The first task is decrypting the ticket $T_{c,s}$ using the dynamic key K_S'. The second task is extracting the session key K from the ticket $T_{c,s}$. In the third task, it uses the session key K to decrypt the authenticator $A_{c,s}$. Later on, it validates the content of ticket $T_{c,s}$ and authenticator $A_{c,s}$ by verifying the network address *add* and matching the nonce value N. If the network address is correct and the nonce value is matched, the ticket and authenticator are validated. Therefore, authorization of client on Service Server is granted. Because of the *one time ticket*, if an intruder tries to performance the replay attacks, the ticket verification module can detect and reject the replay messages. The final task is sending the confirmation of the verification result to client.

DISCUSSION

In this section, we analyse the protocol and security that are raised in our proposed method. After the security analysis, the efficiency of the authentication method is discussed. Finally, the future work is described in the end of the discussion.

Notation

The following notations are used in BAN Logic to analyze and verify the security of the protocol

comma	Conjunction of statements
$P \mid\equiv X$	P believes X.

$P \triangleleft X$	P sees X.
$P \mid\sim X$	P said X.
$P \Rightarrow X$	P has jurisdiction over X.
#(X)	X is fresh.
$P \xleftrightarrow{K} Q$	P and Q share a secret key K.
{X}K	X encrypted under K.
(X, Y)	concatenation of X and Y

The Protocol Analysis

The authentication protocol is analyzed using BAN Logic (Rubin and Honeyman, 1993) to verify the security of the protocol. First, it is transformed into idealized form.

1. C → AS: N_1
2. AS → C: $\{ C \xleftrightarrow{K} S, N_1, N_2\}K_U', \{N_2, C \xleftrightarrow{K} S\}K'_S$
3. C → S: $\{N_2, C \xleftrightarrow{K} S\} K'_S, \{N_2, C \xleftrightarrow{K} S\}K$
4. S → C: $\{N_2+1\}K$

We have the following assumptions:

A1. $C \mid\equiv C \xleftrightarrow{Ku'} AS$, $AS \mid\equiv C \xleftrightarrow{Ku'} AS$, $S \mid\equiv AS \xleftrightarrow{Ks'} S$, $AS \mid\equiv AS \xleftrightarrow{Ks'} S$

A2. $AS \mid\equiv C \xleftrightarrow{K} S$

A3. $C \mid\equiv AS \Rightarrow C \xleftrightarrow{K} S$, $S \mid\equiv AS \Rightarrow C \xleftrightarrow{K} S$

A4. $C \mid\equiv \#(N_1)$, $S \mid\equiv \#(N_2)$

C sees the message 2 that including the session key K generated by AS.

$$C \triangleleft \{C \xleftrightarrow{K} S, N_1, N_2\}K_U', \{C \xleftrightarrow{K} S, N_2\}K_S'$$

By decrypting the first part of the message 2 by using K_U', C can verifies the nonce N_1. Apply the message-meaning rule to the first part, we have

$$C \mid\equiv AS \mid\sim \{C \xleftrightarrow{K} S, N_1, N_2\}$$

With the assumption that $C \mid\equiv \#(N_1)$, by applying the nonce verification rule and the jurisdiction rule, we get

$$C \mid\equiv C \xleftrightarrow{K} S$$

C trusts the session key K and generates message 3 then sends to S. S sees the message 3 as follows.

$$S \triangleleft \{N_2, C \xleftrightarrow{K} S\}K_S', \{N_2\}K$$

Consider the first part and do the similar to the one described above, we can deduce

$$S \mid\equiv C \xleftrightarrow{K} S$$

Applying the message meaning rule to the second part of message 3, we can get

$$C \mid\equiv S \mid\equiv C \xleftrightarrow{K} S$$

S generates message 4 and sends it to C, analyzing this message, we get

$$S \mid\equiv C \mid\equiv C \xleftrightarrow{K} S$$

The final believes between S and C can be summarized as follows:

$$C \mid\equiv C \overset{K}{\longleftrightarrow} S \ , \ S \mid\equiv C \overset{K}{\longleftrightarrow} S$$

$$C \mid\equiv S \mid\equiv C \overset{K}{\longleftrightarrow} S \text{ and } S \mid\equiv C \mid\equiv C \overset{K}{\longleftrightarrow} S$$

This final believes explain that C trusts that S uses the shared session key K to encrypt the communication messages and vice versa. These final believes show that the protocol has idealized the final goals of authentication.

The Security

Kerberos method and its extensive authentication methods are based on cryptography to build up the security for their authentication. Moreover, both symmetric and asymmetric cryptography can be used in the above authentication methods. However, each cryptography system has its own advantages and drawbacks. At the key size matter only, under brute-force attacks, an 128 bits symmetric cryptography is as secure as a 2304 bits asymmetric cryptography (PGP, 2005). Furthermore, symmetric cryptography is significantly faster (Bruce, 1996). However, asymmetric cryptography is more secure in key distribution and exchange approach (Bruce 1996). In general, with certain computation resources and amount of time, every cryptography system, even the most secure one, can be broken under cryptoanalysis attacks (PGP 2005). Therefore, the authentication systems using re-used long term cryptographic keys are only secure within a certain period.

The proposed authentication method based on the dynamic keys can minimize the key compromised risk under cryptoanalysis attacks. After every authentication request, the Dynamic Key Management module generates new dynamic keys. Therefore, the cryptographic keys are never re-used for encryption and authentication. With these dynamic keys, if the cryptography system is broken and the cryptography keys are exposed under cryptoanalysis attacks, adversaries cannot use those keys to authenticate with the system. Those keys become ineffective in next authentication requests.

Furthermore the dynamic keys in the proposed method can also help to prevent replay attacks. Unlike the Kerberos authentication using timestamp, the proposed authentication method employs the dynamic key K_S' to prevent the re-usable of the authentication ticket. Because the dynamic key K_S' changes after every authentication attempt, the authentication ticket $T_{c,s}$ can be validated only once. If an adversary tries to perform the replay attacks, the previous used tickets are invalid because the old dynamic keys are expired after previous authentication attemps. Hence, the authentication method can detect and avoid replay attacks.

The Efficiency

There are two major considerations that affect the efficiency in the authentication method: communicational cost and computational cost.

Communication costs

As in the above description, the communication cost of the method is lower than the Kerberos Authentication Method. For every authentication request, the authentication protocol in proposed method has fewer messages in Kerberos method. Besides that, it does not need maintain time synchronization for the parties in the system like in Kerberos. Furthermore, in compare with the other authentication methods, there is no secure tunnel like SSL to exchange session keys in the proposed method.

Computational costs

The security of this authentication method does not depend on the security of employed cryptographic algorithms. Because dynamic keys are not re-usable, cryptoanalysis attacks on the message to extract cryptographic keys become ineffective. The dynamic keys make attacks on the cryptography for authentication extremely difficult. The cryptography algorithm does not required large key size to prevent cryptanalsysis attacks. Instead of using strong cryptography like public key infrastructure which may be consume a lot of power processing on mobile devices in wireless networks; the proposed authentication method can employ any fast and efficient symmetric cryptographic algorithm. Without degrading the security of the system, the fast and efficient symmetric cryptographic algorithms can be employ to optimizes the performance.

Furthermore, in compare with Kerberos authentication method, the proposed authentication is much better in performance. For each authentication request, Client and Authentication Server involve in only half number of cryptographic operations. The proposed method also verifies fewer number of nonces. It does not use time stamp and time synchronization as well. The comparison between the proposed authentication method and Kerberos is shown in Table 1.

	Kerberos Method	**The Proposed Method**
Number of messages	5	3
Time synchronization	All parties	None

Cryptography operation at Client	4	2
Cryptography operation at Authentication Server	6	2
Cryptography operation at Service	2	2
Number of Nonce verifications	7	3
Time stamp verification	1	0

Table 1. Comparison between Kerberos and proposed authentication method

CONCLUSION

In this paper, we present our authentication method for Internet banking over wireless networks. The method is extended from Kerberos authentication method. Mobile users can authenticate to the service via authentication servers with dynamic keys based on key distribution service. The advantages of the proposed method are its simplicity, efficiency, reliability and security. The authentication method can be applied as authentication protocol for service-based applications and services in wireless networks.

As further work, we investigate the synchronization problem for dynamic keys. Due to the reason dynamic keys are generated offline by the Dynamic Key Management at both parties, the dynamic keys have synchronization problem. After an unsuccessful authentication attempt is made, the dynamic keys are no longer match between C and AS. Therefore a mechanism will be developed to synchronize the dynamic keys securely and efficiently.

REFERENCE

1. Adoba, B. and Simon, D. (1999) PPP EAP TLS Authentication Protocol, *http://www.ietf.org/rfc/rfc2716.txt*
2. Harbitter, A. and Menascé, D.A. (2001), The performance of public key-enabled kerberos authentication in mobile computing applications, *Proceedings of the 8th ACM conference on Computer and Communications Security*, 78 - 85.
3. Raju, G.V.S. (2007) "Authentication in Wireless Networks", *Proceedings of the 40th Hawaii International Conference on System Sciences*, 207a.
4. Fox, A. and Gribble, S. (1996), Security on the move: Indirect Authentication using Kerberos, *Proceedings Of the Second Annual International Conference on Mobile Computing and Network*, 155-164.
5. Pirzada, A. and McDonald, C. (2004) Kerberos Assisted Authentication in Mobile Ad-hoc Networks, *Proceedings of the 27th Australasian Computer Science Conference (ACSC)*, 26, 1, 41-46.
6. Chien, H.Y. and Jan, J.K. (2003) A hybrid authentication protocol for large mobile network, *Journal of Systems and Software archive*, 67, 2, 123-130.
7. Neuman, B. and Ts'o, T. (1994) Kerberos: An Authentication Service for Computer Networks, *IEEE Communications*, 32, 9, 33-38.
8. Tang, Q. and Mitchell, C.J. (2006) Cryptanalysis of a hybrid authentication protocol for large mobile networks, *Journal of Systems and Software*, 79, 4, 2006, 496-501.
9. Tung, B. (2001) Public Key Cryptography for Initial Authentication in Kerberos, *http://ww.ietf.org/internet-drafts/draft-ietf-cat-kerberos-pk-init-12.txt.*
10. Tung, B. (1998) Public Key Cryptography for Cross-Realm Authentication in Kerberos, *http://ww.internic.net/internet-drafts/draft-ietf-cat-derberos-pk-cross-03.txt.*
11. Medvinsky, A. (1997) "Public Key Utilizing Tickets for Application Servers (PKTAPP)", *http://www.ietf.org/internet-drafts/draft-ietf-cat-kerberos-pk-tapp-03.txt.*
12. Kirk, J. (2007), Researcher: RSA 1024-bit encryption not enough, *http://www.infoworld.com/article/07/05/23/RSA-1024-bit-encryption-not-enough_1.html.*
13. Gong, L. (1992) A Security Risk of Depending on Synchronized Clocked, *Operating Systems Review 1992*, 49-53.
14. Bellovin, S. and Merritt, M. (1990), Limitations of the Kerberos authentication system, *ACM SIGCOMM Computer Communication Review,* 20, 5, 119–132.
15. Rubin, A.D and Wright, R.N (2002), Off-line Generation of Limited Use Credit Card Number, *LNCS*, 2339, 196-209.

16. Li, Y. and Zhang, X. (2004) A Security-Enhanced On-Time Payment Scheme for Credit Card, *Proceedings of the International Workshop on Research Issues on data Engineering: Web Service for E-Commerce and E-Government Application*, 40-47.
17. Kungpisdan, S., Srinivasan, B. and Le, P.D. (2003) "Lightweight Mobile Credit-Card Payment Protocol". *LNCS,* 2904, 295-308
18. Rubin, A.D. and Honeyman, P. (1993) Formal methods for the analysis of authentication protocol, *CITI Technical Report 93-7.*
19. PGP (2005), PGP Attack FAQ: The asymmetric cipher, *http://www.iusmentis.com/technology/encryption/pgp/pgpattackfaq/asymmetric/.*
20. Bruce, S. (1996), Applied Cryptography, *John Wiley & Sons*.