Mutual Authentication and Secure Session Termination Scheme in iATA Protocol

Ivy Ong, Shirly Lee, Hoon-Jae Lee and Hyotaek Lim*, *Member, KIMICS*

Abstract— **Ubiquitous mobile computing is becoming easier and more attractive in this ambient technological Internet world. However, some portable devices such as Personal Digital Assistant (PDAs) and smart phones are still encountering inherent constraints of limited storages and computing resources. To alleviate this problem, we develop a cost-effective protocol, iATA to transfer ATA commands and data over TCP/IP network between mobile appliances and stationary servers. It provides mobile users a virtual storage platform which is physically resided at remote home or office. As communications are made through insecure Internet connections, security risks of adopting this service become a concern. There are many reported cases in the history where attackers masquerade as legitimate users, illegally access to network-based applications or systems by breaking through the poor authentication gates. In this paper, we propose a mutual authentication and secure session termination scheme as the first and last defense steps to combat identity thief and fraud threat in particular for iATA services. Random validation factors, large prime numbers, current timestamps, one-way hash functions and one-time session key are deployed accordingly in the scheme. Moreover, we employ the concept of hard factorization problem (HFP) in the termination phase to against fraud termination requests. Theoretical security analysis discussed in later section indicates the scheme supports mutual authentication and is robust against several attacks such as verifiers' impersonation, replay attack, denial-of-services (DoS) attack and so on.**

Index Terms— **Hard Factorization Problem, iATA Protocol, Mutual Authentication, Secure Session Termination**

I. INTRODUCTION

DUE to the fast-emerging of ubiquitous technology, more and more mobile devices such as PDAs and smart phones are used in our daily life. This has led to the tremendous increase of storage demands for storing and processing data on mobile devices. iATA protocol [1] has been introduced as an alternative solution to provide users a remote storage, seemingly the storage is attached to the local device's operating system. It acts as a transport agent to assist users to access their valuable data which geographically located at home or office via the network anytime anywhere. Nonetheless, the use of iATA protocol in opened ubiquitous environment without any security protections is obviously exposed to security threats [2]. The sensitive IP blocks of data transferred over TCP/IP network provides opportunities for attackers to perform malicious attacks such as unauthorized access, snooping, sniffing, connection hijacking, DoS attack and so forth which subsequently cause the compromise of the whole remote storage system.

Some existing authentication methods that originally developed for remote user access or the well-known Internet Protocol Security (IPsec) suite may not suitable to apply directly on iATA due to the limitation of mobile devices' computation recourses. It probably causes the degradation of the protocol's performance. With the objective to provide a robust and lightweight security solution for iATA protocol, we propose a mutual authentication scheme that allows user and remote server authenticate to each other. It is crucial to protect not only the server, but also the legitimate user from security threats. The scheme ensures data stored at remote server are safe from unauthorized disclosure, where only authenticated user is allowed to access or modify the information. HFP concept has been included to avoid the possible DoS attacks at the same time.

II. RELATED WORKS

A. iATA Architecture Overview

iATA [1] is a block level protocol operates on application layer at client-server circumstance, as shown in Fig. 1. There are two primary modules: *iATA Client* that runs on Windows CE platform and *iATA Server* that runs on Linux platform. When a TCP connection is established successfully between two end points, commands or data in ATA form are encapsulated into iATA Protocol Data Unit (PDUs) before transmitting over Internet to another end point. Once iATA PDUs reach to the opposite side, the corresponding driver will perform de-capsulation to retract the original ATA commands and

Manuscript received July 7, 2010; revised July 13, 2010; accepted July 21, 2010.

Ivy Ong and Shirly Lee are with the Department of General, Dongseo University, Busan, 617-716, Korea (Email: ivy_ong2000@yahoo.com, l_shirly@yahoo.com)

Hoon-Jae Lee and Hyotaek Lim* are with the Department of Computer & Information Engineering, Dongseo University, Busan, 617-716, Korea (Email: hjlee@dongseo.ac.kr, htlim@dongseo.ac.kr)

* Corresponding author

data before delivering them to the upper layer for subsequent process.

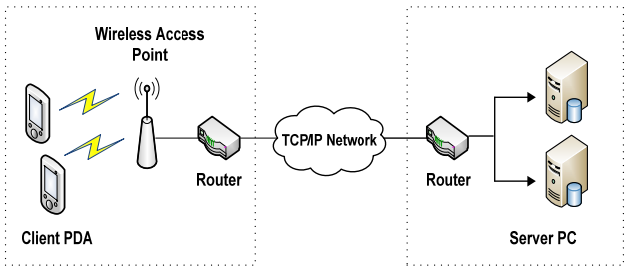

Fig. 1. iATA Client-Server Architecture.

B. Security in Storage Area Network (SAN)

Differs from network-attached storage (NAS) technology, SAN supports block-level remote storage services. Small Computer System Interface (SCSI), Internet SCSI (iSCSI), ATA over Ethernet (AoE) and Fibre Channel are some popular examples of SAN. As commands and data are transmitted over Internet/Ethernet, strong security protection is extraordinary needed to prevent those potential points where security breaches may occur.

Lee and et al. [2] has implemented a lightweight security solution to safeguard iSCSI-based remote storage for mobile devices. Referring to iSCSI Request for Comments (RFC) memorandum, IPsec is ideal to use against passive/active attacks. Nevertheless, this may not suitable for resource limited mobile devices. Alternatively, Secure Remote Password based on Elliptic Curve Cryptography (EC-SRP) is used to provide equivalent security as public key schemes but with shorter key lengths. The generated session key is served as a secret key for Dragon stream cipher cryptographic algorithm to encrypt iSCSI Protocol Data Unit (PDUs). The output cipher text is input to HMAC-SHA256 hash function to generate 32 bytes Message Authentication Code (MAC). Experimental test result reveals this security module performs better than IPsec approach in both Read/Write operations.

C. Mutual Authentication

Mutual authentication is a dual way authentication process used to increase the assurance that both legitimate parties in a communication link authenticate each other suitably. For example in a client-server environment, unlike the unilateral authentication that normally functions as a means of allowing server to verify the genuine users have the identities they claim; in mutual authentication, users will verify the server at the same time to confirm if they are dealing with the correct server.

Shu and et al. [3] introduce a scheme by using Short Message Service (SMS) and Public Key Infrastructure (PKI) technology to improve the performance of mobile authentication. Through the combination of SMS messaging with digital signature and PKI verification with digital certificate, a strong bidirectional authentication medium is established between a mobile terminal and a server gateway. A session key and validation factors are included to achieve non-repudiation and stronger resistances against replay attack and secret key guessing attack. However, using PKI is costly in practices.

Another remote mutual authentication and key agreement scheme with smart cards has been presented by Li [4]. It applies *challenge-response mechanism* to overcome the antecedent unilateral flaw where an attacker may gain services access right by intercepting legal user's login message from eavesdropped communication without the awareness of remote server. Besides, *nonce mechanism* is added to manage session key agreement and been used as a substitution to the previous timestamp element that having complicated time synchronism problem.

Considering the fact that smart card readers may not be available everywhere and in anytime, Hsiang and et al. [5] propose a secure scheme without using smart cards. It exists with three main phases: *Registration Phase, Login Phase, Authentication and Key Agreement Management Phase*, is practical to be implemented in real world and resists against masquerade attack, privileged insider's attack and stolen-verifier attack. Among methods studied from the literature, we modify Hsiang's scheme accordingly to fit in the client-server virtual storage environment to achieve mutual authentication without using external devices or tokens.

D. Random Number Generator (RNG)

RNG is a computational software or physical hardware that produces a series of random numbers/symbols, frequently used as unpredictable codes in security system in contrast to seldom-updated static codes. RNG can be classified as *Pseudo-random (PRNG)*, which is easier to be implemented in software using cryptographic primitives and *True-random (TRNG)* that is more costly and normally built on top of hardware [6]. In our scheme, we select NLM-128 generator [7] to generate the one-time session key, which only valid for a single login session.

E. NLM-128 Generator

NLM-128 is an enhanced LM-type summation generator designed by Lee and et al. [7]. It combines a *Linear Feedback Shift Register (LFSR)* with a de Bruijn-type Nonlinear Feedback Shift

Register (NFSR) to improve its non-linearity characteristic and unpredictability of the output keystream. Its 258 bits of internal state are contributed from the LFSR length of 127 bits and the NFSR length of 129 bits. It takes a 128-bit key k and a 128-bit initialization vector iv to fill the internal state.

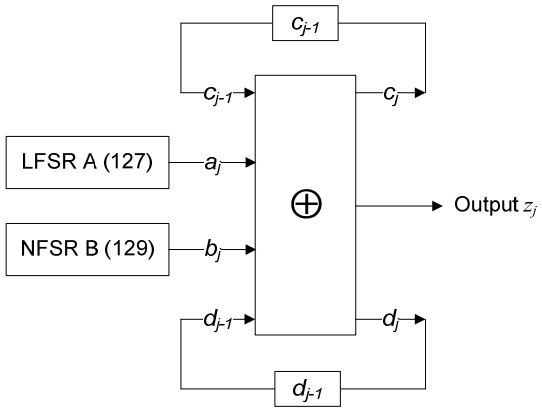

Fig. 2. NLM-128 Generator.

Fig. 2 depicts the XOR-ing of LFSR a_j and NFSR b_j sequences together with the carry c_{j-1} and memory d_{j-1} sequences at time j to yield the output keystream z_j. Empirical result shows NLM-128 able to defeat known attacks on typical and LM-type summation generators, such as divide-and-conquer attack and fast correlation attack.

F. Hard Factorization Problem (HFP)

Nguyen and et al. [8] [9] design a lightweight protocol to prevent 802.11 MAC layer de-authentication/disassociation DoS attack on access point (AP) and WLAN station (STA) in wireless local area network (WLAN). The solution does not depend on cryptographic primitives, but based on HFP concept. For example, N=p*q, where p and q are two random large prime numbers. Given N, it is computationally infeasible to compute p and q. Given p or q, it is easy to compute N. We apply the ideas in our scheme's termination phase to meet the same goal. Even though an attacker eavesdrops N, he is still difficult to guess p or q correctly. The attacker must solve the intractable factorization problem. Furthermore, the factorization of N is unique, there is only one set of (p, q) primes can be multiplied to make N. For instance, let p=2, q=11 and N=p*q=22. There is no pair of (p', q') other than the pair of (2, 11) can be multiplied to get 22. This method is easy to deploy and does not consume much time in generating or calculating the strong prime numbers.

III. PROPOSED SCHEME

Our scheme consists of four major phases: *Registration Phase, Login Phase, Authentication Phase* and *Termination Phase.* Listed below are the notations used throughout the scheme.

- U - The user
- S - The server
- ID - U's identity
- PSW - U's password
- DID - Mobile device's unique serial number
- X - The secret key maintained by S
- $h(.)$ - Collision-resistant one-way hash function
- $\oplus$ - Exclusive-OR operation
- $||$ - String concatenation operation
- N_1 - The random number
- N_c - U's random validation factor
- N_p, N_q - The random large prime numbers
- N_s - S's random validation factor
- T_c - U's current timestamp
- T_s - S's current timestamp
- K_1 - The random one-time session key
- $E_{h(N1 \oplus PSW)}(M)$ - Encryption of message M with a hash function
- $D_{h(N1 \oplus PSW)}(M)$ - Decryption of message M with a hash function

A. Registration Phase

First of all, U needs to register to S as summarized in Fig. 3.

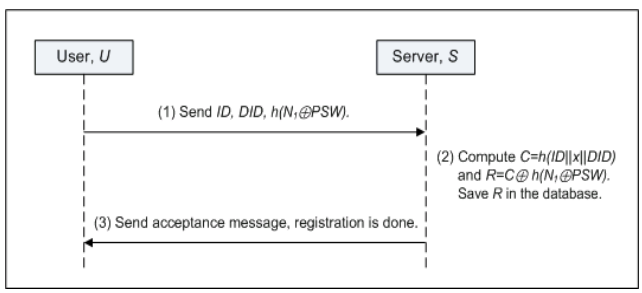

Fig. 3. Registration Phase.

- U selects a random number N_1 and password PSW to compute $h(N_1 \oplus PSW)$.
- U sends ID, DID and $h(N_1 \square PSW)$ to S for initial registration.
- If the request is accepted by S, S computes $C=h(ID||x||DID)$ and the registration value $R=C \square h(N_1 \square PSW)$. S saves R in the database.
- S sends an acceptance message to U. The registration process is done.

B. Login Phase

Fig. 4 illustrates both login and authentication phases.

- *U* computes $a=h(N_1 \square PSW)$ and a random validation factor N_c, where $N_c=N_p*N_q$.
- *U* acquires its current timestamp T_c to compute $MAC=h(T_c||a)$.
- *U* creates the request message $Req\_1=\{ID,DID,MAC,T_c\}$.
- *U* encapsulates N_c with *Req_1* and sends to *S*.

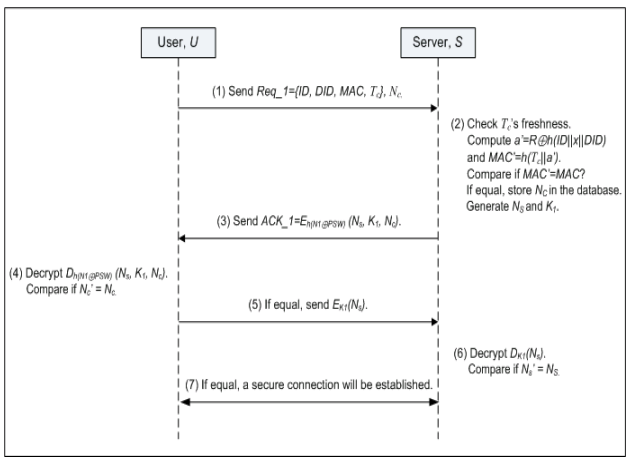

Fig. 4. Login and Authentication Phases.

C. Authentication Phase

When received *Req_1*, *S* performs the following steps.

- *S* checks the freshness of T_c and rejects the request if T_c already existed in a current session of *U*. Otherwise, it continues to the next step.
- *S* computes $a'=R \oplus h(ID||x||DID)$ and $MAC'=h(T_c||a')$. If *MAC'* equals to the received *MAC*, *S* stores N_c in the database and generates a random validation factor N_s. Else, *S* rejects the request.
- *S* uses NLM-128 generator to generate a one-time random session key K_1.
- *S* acquires its current timestamp T_s and stores the paired of timestamps (T_s,T_c) and *ID* temporarily for freshness checking until the end of session.
- *S* encrypts N_s, K_1, N_c in an acknowledgement message *ACK_1* and sends to *U* where $ACK\_1=E_{h(N1 \oplus PSW)}(N_s, K_1, N_c)$.
- Once *U* received *ACK_1*, *U* decrypts the message $D_{h(N1 \oplus PSW)}(N_s., K_1, N_c)$ and checks if N_c' equals to its original N_c.
- If equals, *U* encrypts $E_{K1}(N_s)$ and forwards to *S*. Else *U* stops the authentication process.
- Once *S* received $E_{K1}(N_s)$, *S* decrypts $D_{K1}(N_s)$ and checks if N_s' equals to its original N_s.
- If so, a secure connection will be established between *S* and *U*. The authentication process is completed successfully.

D. Termination Phase

Fig. 5 exemplifies the termination process.

- To stop the service, *U* encapsulates N_p in a termination request message *Ter_1* and sends to *S*.
- Once received *Ter_1*, *S* retrieves N_c from the database and computes if $N_p|N_c$.
- If *S* able to compute N_q prime number from the division, *S* terminates the current session with *U*.

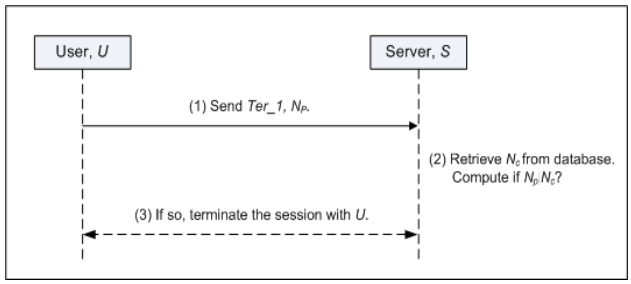

Fig. 5. Termination Phase

IV. SECURITY ANALYSIS

This session discusses about the security analysis of the proposed scheme.

A. Mutual Authentication

In the authentication phase, *S* and *U* authenticate each other securely by verifying if $N_c'=N_c$, and $N_s'=N_s$ respectively.

B. User Spoofing Attack Protection

The scheme resists against user spoofing attack. *U*'s authentication data, $R=h(ID||x||DID) \oplus h(N_1 \oplus PSW)$ is stored in *S*'s database. If an attacker stole *R*, he can obtain $h(N_1 \oplus PSW)$ only if he knows $h(ID||x||DID)$. This means that he has to know the long-term secret key *x*, but *x* is under strict protection as assumed. In this case, for the attacker to obtain $h(N_1 \oplus PSW)$ is infeasible.

C. Server Spoofing Attack Protection

An attacker may masquerade as the legitimate *S*. The scheme is free from such attack as the attacker cannot construct the session key and send a message encrypted with $h(N_1 \oplus PSW)$ to *U* without the knowledge of N_1 and *PSW*. Also, *U* will not able to decrypt the fraudulent message from masqueraded *S*. *U* can detect the fraud immediately and thus terminate the authentication process.

D. Replay Attack Protection

An adversary may conduct a replay attack by intercepting valid data/message and retransmits to the legal party to gain access or trust. The scheme is protected from the attack by including current timestamp variables

for comparisons. Accesses are only granted for which the timestamp values are fresh and within a reasonable tolerance. In addition, random validation factors (N_s, N_c) and one-time session key K_1 are used and valid solely per single authentication process. Therefore, fraudulently repeated messages will not be able to pass through the legality checking process.

E. DoS Attack Protection

DoS attack may occur when an attacker sends fake termination requests to *S*. Given $N_c=N_p*N_q$, where N_c is stored in *S*'s database while *U* keeps N_p value. It is computationally infeasible for the attacker to compute N_p or N_q although he knows N_c value. Only genuine *U* can send a termination request message encapsulated with N_p to *S*. *S* calculates if N_p divides N_c. If it gets N_q prime number from the calculation, *S* confirms the message was sent by the legal *U* and terminates the session.

F. Man-in-the-middle (MITM) Attack Protection

MITM attack happens when an attacker impersonates as the legitimate entity, constructs fraud connections with the victims, intercepts and relays messages between them. In this scheme, *ACK_1* is protected by $h(N_1 \oplus PSW)$, where an attacker will not able to get the content of *ACK_1* without knowing $h(N_1 \oplus PSW)$. Additionally, legality checking at *U* side if $N_c'=N_c$, and at *S* side if $MAC'=MAC$ and $N_s'=N_s$, are preventing the same attack. T_c is used to compute *MAC;* different *MAC* will have different T_c from different sessions. Hence, the attacker will not pass the authentication even he collects all messages from other sessions.

IV. CONCLUSIONS

Internet has no doubts brought a lot of advantages and conveniences to the society. Despite its positive characteristics, Internet has become a new base for adversaries to perpetrate cybercrimes. The volume of identity abuses on network applications particularly in e-commerce business, online banking and remote storage system are significantly increased to date. We propose a secure mutual authentication and termination scheme on iATA protocol to minimize the identity or fraud orchestrated attacks as mentioned in previous sections. Security analysis shows the proposed scheme provides a robust and trustworthy mutual authentication approach with a secure termination function between mobile user and remote server communicated over the insecure network.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0016831).

REFERENCES

[1] Chee-Min Yeoh, Yu-Shu They, Hoon-Jae Lee, and Hyotaek Lim, "Design and Implementation of iATA on Windows CE Platform: An ATA-based Virtual Storage System," *Proc. of International Conference on Communications and Mobile Computing (WRI),* pp. 85-89, Jan 2009.

[2] ErnYu Lee, YuShu They, HyoTaek Lim, and HoonJae Lee, "A Lightweight Secure iSCSI-based Remote Storage Service for Mobile Devices," *Proc. of 2nd International Conference on Communications and Networking in China (CHINACOM),* pp. 361-365, Aug 2007.

[3] Minglei Shu, Chengxiang Tan, and Haihang Wang, "Mobile Authentication Scheme Using SMS," *IITA International Conference on Services Science, Management and Engineering (SSME),* pp.161-164, Jul 2009.

[4] Chun-Ta Li, "An Enhanced Remote User Authentication Scheme Providing Mutual Authentication and Key Agreement with Smart Cards," *5th International Conference on Information Assurance and Security (IAS),* pp. 517-520, Aug 2009.

[5] Han-cheng Hsiang and Wei-Juan Shih, "A Secure Remote Mutual Authentication and Key Agreement without Smart Cards," *Proc. of ANSI Information Technology Journal,* vol. 8, pp. 333-339, 2009.

[6] W. Stallings, *Cryptography and Network Security.* 4th ed. Pearson Education, 2005.

[7] HoonJae Lee, SangMin Sung, and HyeongRag Kim, "NLM-128, An Improved LM-type Summation Generator with 2-bit memories," *4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT),* pp. 577-582, Nov 2009.

[8] Nguyen, T.N., Tran, B.N. and, Nguyen, D.H.M., "A lightweight solution for Wireless LAN: Letter-envelop protocol," *Proc. of 3rd International Conference on Communications and Networking in China (ChinaCom),* pp. 17-21, Aug 2008.

[9] Nguyen, T.D., Nguyen, D., Tran, B.N., Vu, H., and Mittal, N., "A Lightweight Solution for Defending against Deauthentication/Disassociation Attacks on 802.11 Networks," *Proc. of 17th International Conference on Computer Communications and Networks (ICCCN),* pp. 1-6, Aug 2008.

Ivy Ong received her BS of Information Technology, Honors Information Systems Engineering at Multimedia University, Malaysia in 2005. She worked as a software engineer II at Western Digital, Malaysia from 2007 to 2009. At present, she is pursuing the Master of Engineering in Graduate School of General at Dongseo University, Korea. Her research interests include hard disk drive technology, reliability analysis, mobile computing and network management.

Shirly Lee received her BS of Information and Science Technology, Honors Data Communication from Multimedia University, Malaysia in 2005. She is currently a master student in cryptography and network security lab at Dongseo University, Korea. From 2005 to 2007, she was an IT specialist at the Printelli Sdn Bhd Malaysia. She worked as IT Executive with Sunway Group, Malaysia in year 2007 till 2009. Her current research interests include network security and cryptography, cloud computing security, RFID/USN security.

Hoon-Jae Lee received his BS, MS, and PhD Degrees in electronic engineering from Kyungpook National University, Daegu, Korea in 1985, 1987, and 1998, respectively. He is currently a professor in the School of Computer and Information Engineering at Dongseo University. From 1987 to 1998, he was a research associate at the Agency for Defense Development (ADD). His current research interests include developing secure communication system, side-channel attack and USN/RFID security.

Hyotaek Lim received his BS degree in Computer Science from Hongik University in 1988, the MS degree in Computer Science from POSTECH and the PhD degree in Computer Science from Yonsei University in 1992 and 1997, respectively. From 1988 to 1994, he had worked for Electronics and Telecommunications Research Institute as a research staff. Since 1994, he has been with Dongseo University, Korea, where he is currently a professor in the Division of Computer and Information Engineering. His research interests include computer network, protocol engineering, storage networking, IPv6 and mobile application.