New Identity Management Scheme and its Formal Analysis

Jeonghoon Han, Hanjae Jeong, Dongho Won, and Seungjoo Kim

Open Science Index, Computer and Information Engineering Vol:3, No:1, 2009 publications.waset.org/14412.pdf

Abstract**—** As the Internet technology has developed rapidly, the number of identities (IDs) managed by each individual person has increased and various ID management technologies have been developed to assist users. However, most of these technologies are vulnerable to the existing hacking methods such as phishing attacks and key-logging. If the administrator's password is exposed, an attacker can access the entire contents of the stolen user's data files in other devices. To solve these problems, we propose here a new ID management scheme based on a Single Password Protocol. The paper presents the details of the new scheme as well as a formal analysis of the method using BAN Logic.

Keywords**—**Anti-phishing, BAN Logic, ID management.

I. Introduction

As the Internet technology has developed, the number of the Internet users has increased rapidly. Most of the users use a simple and identical password to access different websites. Thus, the exposure of the password registered in a single website affects many other websites. To solve this problem, various ID management technologies have been developed such as CardSpace, AlPass, OpenID, Sxipper, KeePass, and RoboForm. However, these technologies are still vulnerable to the existing hacking methods such as phishing attacks and key-logging [1]. Furthermore, if the administrator's password is compromised, an attacker can access the entire contents of the stolen user data file in the other devices [2]. To solve these problems, we propose a new ID management scheme in this paper.

This paper is organized as follows: Section II explains details of related work which are base technologies for our ID management scheme. Section III proposes a new ID management scheme based on the Single Password Protocol. Section IV introduces the "BAN Logic" and presents a formal analysis of the proposed scheme and finally, Section V concludes the paper.

II. Related Works

In this section, we summarize the results of our previous related research [2] to set the scene for the current work. In addition, we introduce the Single Password Protocol (SPP) and two authentication methods using a device's unique information [3, 4, 5].

A. Previous Research

Vulnerability analysis of the ID management technologies in previous research has been performed and Table 1 describes the results for each technology (where O means that the technology is vulnerable to the form of hacking indicated and X means it is resistant). Fig. 1 describes a general behavior of the ID management technologies.

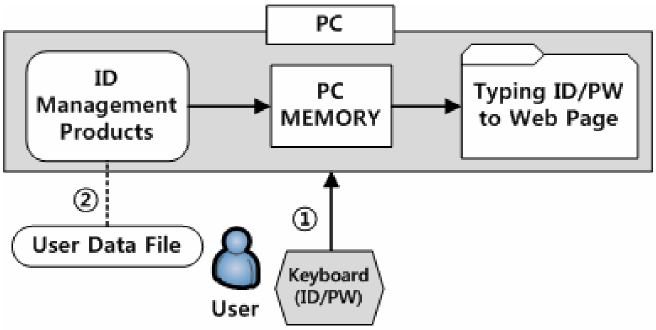

Fig. 1 Behavior of General ID Management Technologies

In the previous research, we examined whether an administrator's password and a user data file are exposed by using hacking tools in the section of ① and ②. We used "SKIn2000" and "NetBus" as the hacking tools [6, 7]. "SKIn2000" is a key-logging tool and provides not only "Static Text" information, but also "Edit Controls" information. "NetBus" is used for stealing the user data file.

"This research was supported by the Ministry of Knowledge Economy, Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)" (IITA-2008-C1090-0801-0016)

J. Han, D. Won and S. Kim are with the Information Security Group, Sungkyunkwan University, 300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Korea (phone: 82-31-290-7213; fax: 82-31-290-7686; e-mail: {jhhan, dhwon, skim}@security.re.kr).

Corresponding author: Seungjoo Kim.

TABLE I
VULNERABILITIES OF ID MANAGEMENT TECHNOLOGIES

Technology	Phishing attack	key-logging	Illegal use of the stolen user data file
CardSpace	X	X	X
AlPass	X	O	O
OpenID	O	O	(No user data in PC)
Sxipper	X	O	O
KeePass	X	O	O
RoboForm	X	O	O

CardSpace is secure against phishing attacks and key-logging and an attacker cannot access the contents of the stolen user data file in other devices. However, to use CardSpace, “Microsoft .NET Framework” (requiring more than 1 GBytes) should be installed in the user’s PC. Moreover, it is dependent on the operating system (OS) such as “Microsoft Windows” so it is difficult to apply this technology to mobile devices that have a limited memory resource and other various simpler OS platforms.

AlPass, Sxipper, KeePass and RoboForm are secure against phishing attacks. They store the websites’ URLs in the user’s data file and detect the correct website by using the stored websites’ URLs. However, if the administrator’s password is exposed, an attacker can access the contents of the stolen user data in other devices; this user data can include important information such as account numbers, identification numbers, and etc, so the data must be managed extremely securely.

Hence, to solve the above problems, we propose a new ID management scheme that provides the properties of anti-phishing and good protection of the user data file. Furthermore, it allows users to be able to use a single ID and a password to access to different websites.

B. Single Password Protocol

In 2007, Gouda, et al. proposed a single password protocol (SPP) which is based on the SSL protocol. Nowadays, as most website use the SSL protocol to protect user information in a secure manner adopting it as the basis for the SPP is felt to be appropriate for current situation. Furthermore, the SPP allows a user to access different websites through a single password. The notations used in SPP are presented in Table II.

TABLE II
NOTATION USED IN SPP

Notation	Explanation
C / S	Client identity / Server’s URL
P	Password remembered by client
n, n_i	Random numbers
$MD()$	Message digest (one-way hash) function
$MD^2()$	$MD(MD())$
$\vert$	Concatenation

Fig. 2 describes the normal behavior in SPP; since SPP is based on the SSL protocol, all messages are encrypted by the session key.

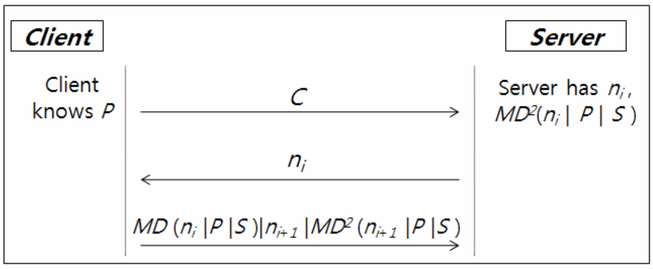
Client
Server
Client knows P
C
n_i
$MD(n_i|P|S)|n_{i+1}|MD^2(n_{i+1}|P|S)$
Server has n_i, $MD^2(n_i|P|S)$

Fig. 2 Behavior of SPP

Step 1. *Client* knows password P corresponding to C, and sends C to *Server*. *Server* has verification information $MD^2(n_i|P|S)$.

Step 2. When *Server* receives C from *Client*, *Server* sends random number n_i stored in *Server* to *Client*.

Step 3. *Client* calculates $MD(n_i|P|S)|n_{i+1}$ $|MD^2(n_{i+1}|P|S)$, and sends it to *Server*. Then, *Server* hashes the received value $MD(n_i|P|S)$, and compares the hashed value with the stored value $MD^2(n_i|P|S)$. If the comparison process is successful, *Server* replaces n_i, $MD^2(n_i|P|S)$ with n_{i+1}, $MD^2(n_{i+1}|P|S)$.

In the registration phase, the server calculates and stores the server’s URL in the message digest value $MD^2(n_i|P|S)$. In the authentication phase, by comparing the S value stored in the server with another value received from the client, the SPP provides an anti-phishing feature. The password P transmitted to the server is included in the message digest value $MD(n_i|P|S)|n_{i+1}|MD^2(n_{i+1}|P|S)$. Thus, the server cannot know what the real password is.

C. Authentication Method using Device’s Unique Information

In this section, two methods that authenticate legitimate users using a device’s unique information are introduced. The first method is the “System and method for breaking illegal use for movable storage devices” [4].

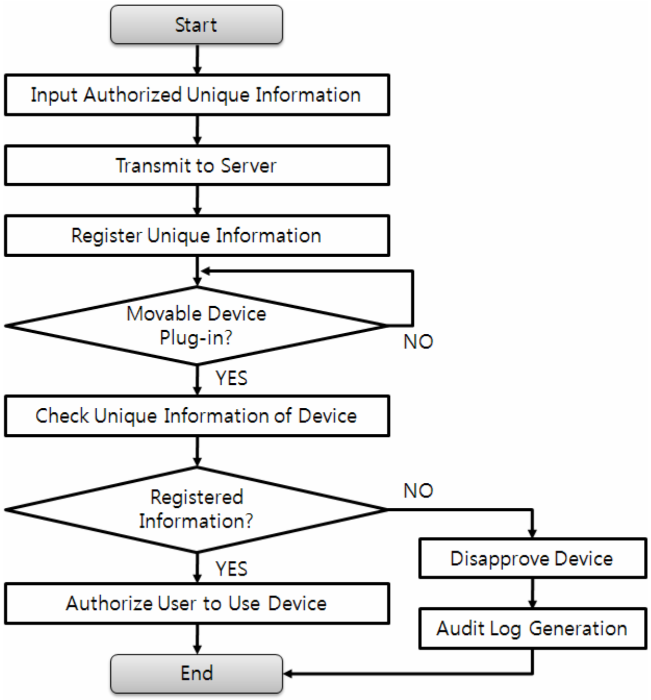
Start
Input Authorized Unique Information
Transmit to Server
Register Unique Information
Movable Device Plug-in?
NO
YES
Check Unique Information of Device
Registered Information?
NO
YES
Disapprove Device
Authorize User to Use Device
Audit Log Generation
End

Fig. 3 Process followed in “system and method for breaking illegal use for movable storage devices”

Fig 3 describes the authentication procedure used in this method where the movable storage device’s unique information is a serial number or a vendor ID. By registering the information on the main server, only the registered devices can be used in the system. Currently, this method is used in Ministry of National Defense and subordinate units to protect classified information from illegal exposure.

The second method is the “Method for authentication of subscribers using the MAC address” [5]. Fig 4 describes the overall architecture of this method where the gateway’s MAC address is used and the Gate Keeper prevents unregistered illegal access to the gateway. Currently, this method is used in VoIP service provider to authenticate legitimate subscriber.

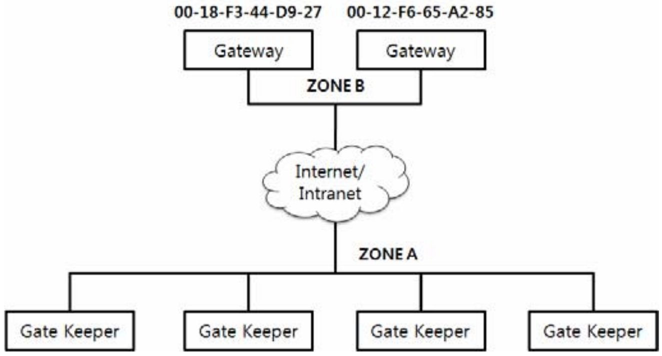

Fig. 4 Method for authentication of subscriber using the MAC address

III. New ID Management Scheme

In this section, a new ID management scheme is proposed and the security requirements for this new scheme are presented in Table III.

TABLE III
Security Requirements of the New Scheme

No.	Security Requirements
1.	All private information is stored in the user’s PC or a mobile device for user privacy.
2.	The scheme should be secure against phishing attack.
3.	Anti-key logger solution should be installed in the user’s devices.
4.	By using the device’s unique information, an attacker cannot access the contents of the stolen user data file in other devices.

The notation used in the new proposed scheme is presented in Table IV.

TABLE IV
Notation Used in the New Proposed Scheme

Notation	Explanation
U_{ID}	A identity of the user U
S_{URL}	A URL of the server S
C_i	Random number generated by user
EK_i	User data file encryption key
$Salt$	Salt used in generation of EK through the PBKDF(·)
P	User password
I_{Uniq}	The unique information of a device
$Auth\_Result$	Authentication result of the server
$X \mid Y$	Concatenation of X and Y
$(X)_K$ / $(X)_K^{-1}$	Encrypt X using K / Decrypt X using K
$PBKDF(\cdot)$	Password-Based Key Derivation Function
$PRNG(\cdot)$	Pseudo-Random Number Generator
$H(\cdot)$	Secure one-way hash function
$H^n(\cdot)$	Iterate n times of hash function
T / T_{i+1}	$H(C_i \mid P \mid I_{Uniq} \mid S_{URL})$ / $H(C_{i+1} \mid P \mid I_{Uniq} \mid S_{URL})$

Because the proposed scheme is based on the SPP, we assume that the communication channel between the user and the server is protected by SSL protocol. We also assume that *PBKDF*(·) and *PRNG*(·) functions are cryptographically secure and the new scheme has two phases, namely the user registration and the user authentication phases.

A. *User Registration Phase*

Fig. 5 describes the behavior of the user registration phase used in the proposed protocol.

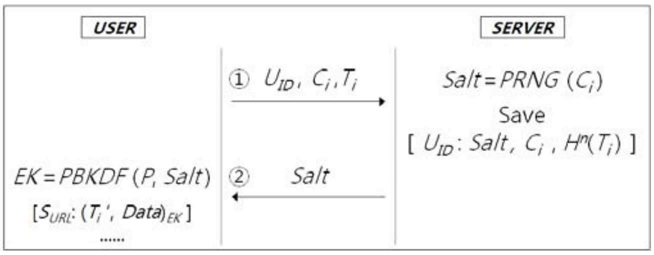

Fig. 5 The user registration phase

The user registration phase consists of the following two steps:

Step 1. *User* calculates T_i=H(C_i|P|I_{Uniq}|S_{URL}). *User* generates a random number C_i, and sends U_{ID}, C_i, T_i to *Server*. Then, *Server* calculates *Salt*=*PRNG*(C_i) and saves [U_{ID} : *Salt*, C_i, H^n(T_i)].

Step 2. *Server* sends *Salt* to *User*. *User* can calculates data file encryption key *EK*=*PBKDF*(*P*, *Salt*) and encrypts T_i and *Data* with *EK*. Then, *User* saves [S_{URL} : (T_i´, *Data*)$_{EK}$].

B. User Authentication Phase

In this phase, the user authentication process is performed by making a comparison between the authentication information H^n(T_i´´) and H^n(T_i) stored in the server. Fig. 5 describes the overall behavior of the user authentication phase in the new proposed scheme.

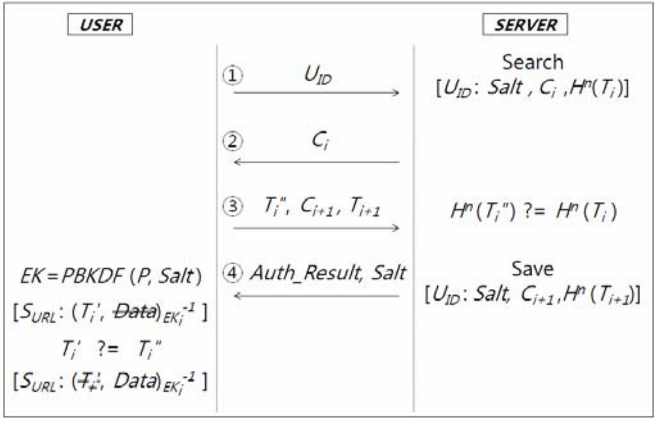
USER
SERVER
① U_{ID}
Search
[U_{ID}: Salt , C_i ,$H^n(T_i)$]
② C_i
③ T_i", C_{i+1}, T_{i+1}
$H^n(T_i")$?= $H^n(T_i)$
$EK = PBKDF(P, Salt)$
④ Auth_Result, Salt
Save
[U_{ID}: Salt, C_{i+1},$H^n(T_{i+1})$]
[S_{URL}: (T_i', ~~Data~~)$_{EK_i^{-1}}$]
T_i' ?= T_i"
[S_{URL}: (~~T_i~~', Data)$_{EK_i^{-1}}$]

Fig. 6 The user authentication phase

Step 1. *User* sends U_{ID} to *Server*. *Server* searches authentication information matching up to U_{ID}. If U_{ID} exists, *Server* performs next step.

Step 2. *Server* extracts C_i from the authentication information, and sends C_i to the *User*.

Step 3. *User* calculates T_i´´=H(C_i | P | I_{Uniq} | S_{URL}) and T_{i+1}= H(C_{i+1} | P | I_{Uniq} | S_{URL}). *User* sends T_i´´, C_{i+1}, T_{i+1} to *Server*. *Server* compares H^n(T_i´´) with H^n(T_i).

Step 4. If the comparison process is successful, *Server* sends *Auth_Result* and *Salt* to *User*. *Server* saves [U_{ID} : *Salt*, C_{i+1}, H^n(T_{i+1})]. Then, *User* searches location of data corresponding S_{URL}, and decrypts T_i´. If T_i´ is the same as T_i´´, *User* decrypts *Data* by using *EK*.

The security assurance of the proposed scheme is dependent on whether the scheme satisfies the security requirements. Thus, in the next section, we present a formal analysis of the proposed scheme and explain its security properties.

IV. Formal Analysis and Security Properties

A. Introduction of BAN Logic

BAN logic has been used for performing a formal analysis of the security protocol. And this comprises four analysis phases: initial assumption, protocol idealization, protocol goals and protocol verification [8].

TABLE V
Notations of The BAN Logic

Notation	Explanation
$P \mid\equiv Q$	Principal *P* believes *X*.
$P \triangleleft X$	*P* sees *X*.
$P \mid\sim X$	Principal *P* once said *X*.
$P \Rightarrow X$	Principal *P* has jurisdiction over *X*.
$\#(X)$	The formula *X* is fresh.
$P \xleftrightarrow{K} Q$	*P* and *Q* may use a shared key *K* to communicate.
$\overset{K}{\mapsto} P$	*P* has a public key *K*.
$P \overset{X}{\Leftrightarrow} Q$	The formula *X* is a secret known only to *P* and *Q*.
$\{X\}_K$	*X* is encrypted using key *K*.
$\langle X \rangle_Y$	*X* is combined with the formula *Y*.

There are three entities in BAN logic; principals, encryption keys and logical formulas. The symbols *P* and *Q* are principals, and *K* is an encryption key. The basic notation used in the BAN Logic is presented in Table V.

There are various inference rules in BAN logic and these rules can be applied to each message of the idealized protocol repeatedly until the goals of protocol are achieved.

(R1) Message Meaning Rules

For shared secret keys:

$$\frac{P \mid\equiv P \xleftrightarrow{K} Q, P \triangleleft \{X\}_K}{P \mid\equiv Q \mid\sim X}$$

If *P* believes that session key *K* is shared only with *Q*, and sees a message *X* encrypted using session key *K*, then *P* believes that *Q* once said the message *X*.

For public keys:

$$\frac{P \mid\equiv \overset{K}{\mapsto} Q, P \triangleleft \{X\}_{K^{-1}}}{P \mid\equiv Q \mid\sim X}$$

If *P* believes that key *K* is *Q*'s public key, and sees a message *X* encrypted with *Q*'s private key K^{-1}, then *P* believes that *Q* once said the message *X*.

For shared secrets:

$$\frac{P \mid\equiv Q \overset{Y}{\Leftrightarrow} P, P \triangleleft \langle X \rangle_Y}{P \mid\equiv Q \mid\sim X}$$

If *P* believes that the secret *Y* is shared with *Q*, and sees a message *X* combined with the secret *Y*, then *P* believes that *Q* once said the message *X*.

(R2) Jurisdiction Rule

$$\frac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$$

If *P* believes that *Q* has jurisdiction over *X*, and believes that *Q* believes a message *X*, then *P* believes the message *X*.

(R3) Nonce Verification Rule

$$\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$$

If *P* believes the freshness of a message *X*, and believes that *Q* once said the message *X*, then *P* believes that *Q* believes the message *X*.

(R4) Freshness Rules

$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)} \qquad \frac{P \mid\equiv \#(X)}{P \mid\equiv \#(\alpha^X)}$$

If one part of a formula is known to be fresh, then the entire formula must also be fresh. If *P* believes that a message *X* is fresh, then the transformed formula in virtue of *X* is also fresh.

(R5) Belief Rules

$$\frac{P \mid\equiv X, P \mid\equiv Y}{P \mid\equiv (X,Y)} \qquad \frac{P \mid\equiv (X,Y)}{P \mid\equiv X} \qquad \frac{P \mid\equiv Q \mid\equiv (X,Y)}{P \mid\equiv Q \mid\equiv X}$$

If and only if *P* believes a separated message, then *P* believes a set of messages.

(R6) Additional Rule

$$\frac{P \mid\equiv Q \mid\sim (X,Y)}{P \mid\equiv Q \mid\sim X}$$

If *P* believes that *Q* once said a message (*X*, *Y)*, then *P* believes that *Q* once said the message *X*.

B. Formal Analysis

Initial Assumptions

Since our scheme is based on SSL protocol, each message is encrypted with the session key. This session key is called *SK*. To analyze our scheme, we first give the initial assumptions:

(A1) $User \mid\equiv \#(SK)$

(A2) $Server \mid\equiv \#(SK)$

(A3) $User \mid\equiv User \xleftrightarrow{SK} Server$

(A4) $Server \mid\equiv User \xleftrightarrow{SK} Server$

(A5) $User \mid\equiv Server \mid\equiv User \xleftrightarrow{SK} Server$

(A6) $Server \mid\equiv User \mid\equiv User \xleftrightarrow{SK} Server$

(A7) $Server \mid\equiv User \Rightarrow T_i^{''}$

(A8) $User \mid\equiv Server \Rightarrow Salt$

Idealized Scheme

In the idealized scheme, Step 1 is omitted, since the user identity does not contribute to the logical properties of the scheme.

(M1) $Server \rightarrow User : (C_i)_{SK}$

(M2) $User \rightarrow Server : (T_i'', C_{i+1}, T_{i+1})_{SK}$

(M3) $Server \rightarrow User : (Salt)_{SK}$

Authentication Goals

Because *Server* authenticates *User* by validating whether $H^n(T_i'')$ is same with $H^n(T_i)$, the goal that *Server* authenticates *User* is defined as (G1). Furthermore, *User* should be able to decrypt the data file with *EK*. *EK* is generated by *PBKDF*(·) through *Salt* and *P*. Thus, the goal is defined as (G2).

(G1) $Server \mid\equiv T_i^{''}$

(G2) $User \mid\equiv Salt$

Verification

(M1) $$User \triangleleft C_i, User \mid\equiv Server \mid\sim C_i \qquad (1)$$

$$\text{(M2)}\qquad Server \lhd T_i^{''}, C_{i+1}, T_{i+1}, \tag{2}$$

$$Server \mid\equiv User \mid\sim T_i^{''}, C_{i+1}, T_{i+1} \tag{3}$$

$$\text{(3, R6)}\qquad Server \mid\equiv User \mid\sim T_i^{''} \tag{4}$$

$$\text{(A2, R4)}\qquad Server \mid\equiv \#(T_i^{''}, C_{i+1}, T_{i+1}) \tag{5}$$

$$\text{(3, 5, R3)}\qquad Server \mid\equiv User \mid\equiv (T_i^{''}, C_{i+1}, T_{i+1}) \tag{6}$$

$$\text{(6, R5)}\qquad Server \mid\equiv User \mid\equiv T_i^{''} \tag{7}$$

$$\text{(7, A7, R2)}\qquad Server \mid\equiv T_i^{''} \tag{8}$$

$$\text{(M3)}\qquad User \lhd Salt, \tag{9}$$

$$User \mid\equiv Server \mid\sim Salt \tag{10}$$

$$\text{(A1, R4)}\qquad User \mid\equiv \#(Salt) \tag{11}$$

$$\text{(10, 11, R3)}\qquad User \mid\equiv Server \mid\equiv Salt \tag{12}$$

$$\text{(12, A8, R2)}\qquad User \mid\equiv Salt \tag{13}$$

Through the deduction described above, we derive the following beliefs (G1, G2):

$$Server \mid\equiv T_i^{''} \qquad User \mid\equiv Salt$$

This means that we have achieved the goals of our scheme (8, 13).

C. Security Properties

Anti-Phishing

Let us assume that there are two websites; an original website "*www.original.com*" and a malicious website "*www.original- phishing.com*". When a user log on a malicious website which attempts to fool the user through a phishing attack, the user sends $T_i{}^{''}$, C_{i+1}, T_{i+1} to the server.

$$H(C_i \mid P \mid I_{Uniq} \mid \text{www.original-phishing.com}),\ C_{i+1},$$
$$H(C_{i+1} \mid P \mid I_{Uniq} \mid \text{www.original-phishing.com})$$

At this time, $T_i^{''}$ includes S_{URL} which is the malicious website's address "*www.original- phishing.com*". Therefore, the user authentication process will be failed, because the server has an original website's address "*www.original.com*" in $H^n(T_i)$.

$$H^n(C_i \mid P \mid I_{Uniq} \mid \text{www.original.com}).$$

In this example, we assume that user's browser, the original website "*www.original.com*" and the malicious website "*www.original-phishing.com*" are running our scheme. If the malicious website "*www.original-phishing.com*" does not run our scheme, user's browser should alert user that this website could be malicious.

Preventing the Stolen User Data File from Illegal Use

In the existing ID management technologies, if the administrator's password has been exposed, an attacker was able to access the contents of the user's data file. In order to assess the security properties of the new scheme, assume that an attacker has obtained the user's data file and the administrator's password. If the attacker tries to attempt a login to the desired website using the stolen user's data file and password in the attacker's device, the authentication process will be failed, because $T_i^{''}$ includes I_{Uniq} which is unique information of the attacker's device.

As mentioned previous section, the device's unique information can be a serial number. There is a tool which can change drive's serial number [9]. If the unique information is stored in file system in HDD, an attacker can change the device's unique information and access the contents of the stolen user data file by using this tool. Thus, when the unique information is applied to our scheme, it should be a hardware serial number that comes from the manufacturer. Since the hardware serial number is in the chip itself, the attacker should have additional hardware equipments which are used for developing embedded system to forge the unique information.

V. CONCLUSIONS

The existing ID management technologies are vulnerable to phishing attacks and illegal use of the stolen user data file. In this paper, a new ID management scheme to solve the problems has been presented and proved to be effective using formal methods in computing. In future work, it is intended to apply the new scheme to the mobile environments using Trusted Platform Module (TPM), so that more efficient and secure ID management technologies can be developed.

REFERENCES

[1] Simon Willison, "OpenID phishing demo", http://feeds.feedburner.com/~r/PlanetIdentity/~3/299657206/

[2] J. Han, B. Lee, S. Hong, S. Kim, D. Won, and S. Kim, "Analysis on Vulnerability of ID/PW Management Solution and Proposal of the Evaluation Criteria", The Transactions of the KIPS (Korea Information Processing Society), Vol.15-C/No.2, 2008, pp.125-132.

[3] Mohamed G. Gouda, Alex X. Liu, Lok M. Leung and Mohamed A. Alam, "SPP: An anti-phishing single password protocol", Computer Networks, 2007, pp. 3715-3726.

[4] J. S. Lee, S. J. Kim and S. R. Choi, "System and Method for Breaking Illegal Use for Movable Storage Device", WaterwallSystems Co., Ltd., Korea Patent 10-0688258-0000, 2007.

[5] P. B. Lim and J. S. Seong, "Method for Authentication of Subscriber using the MAC Address", Samsung Electronics Co., Ltd., Korea Patent 10-0418398-0000, 2004.

[6] SKIn2000, "http://www.keylogger.biz"

[7] NetBus, "http://www.netbus.org/"

[8] Michael Burrows, Martín Abadi and Roger Needham, "A Logic of Authentication", ACM Transactions on Computer Systems, 8(1), 1990, pp.18-36.

[9] Changing volume's serial number, "http://www.codeproject.com/KB/system/change_drive_sn.aspx"

Jeonghoon Han received his B.E. degree in Computer Engineering from Sungkyunkwan University, Korea, in 2007. He is currently a M.S. course of Electrical and Computer Engineering in Sungkyunkwan University. His current research interest is in the area of cryptography, digital ID management, reverse engineering.

Hanjae Jeong received the B.S. degree in Computer Engineering from Sung-kyunkwan University, Korea, in 2006 and the M.S. degree in Electrical and Computer Engineering from Sungkyunkwan University, Korea, in 2008. He is currently a Ph.D. course of Mobile systems engineering in Sungkyunkwan University. His current research interest is in the area of cryptography, authentication protocol, and mobile security.

Dongho Won received his B.E., M.S., and Ph.D. degrees from Sungkyunkwan University in 1976, 1978, and 1988, respectively. After working at ETRI (Electronics & Telecommunications Research Institute) from 1978 to 1980, he joined Sungkyunkwan University in 1982, where he is currently Professor of School of Information and Communication Engineering. His interests are on cryptology and information security. Especially, in the year 2002, he was occupied the president of KIISC (Korea Institute of Information Security & Cryptology).

Seungjoo Kim received his B.S. (1994), M.S. (1996), and Ph.D. (1999) in information engineering from Sungkyunkwan University (SKKU) in Korea. Prior to joining the faculty at SKKU in 2004, he had an appointment as the Director of the Cryptographic Technology Team & the (CC-based) IT Security Evaluation Team of the Korea Information Security Agency (KISA) for 5 years. Now he is Associate Professor of School of Information and Communication Engineering at SKKU. Also, he has served as an executive committee member of Korean E-Government, and advisory committee members of several public and private organizations such as National Intelligence Service of Korea, Digital Investigation Advisory Committee of Supreme Prosecutors' Office, Ministry of Justice, The Bank of Korea, ETRI(Electronic and Telecommunication Research Institute), and KISA(Korea Information Security Agency), etc. His research interests include cryptography, information security and information assurance.