Telecommun Syst (2010) 44: 181–190
DOI 10.1007/s11235-009-9265-7

A novel user's authentication scheme for pervasive on-line media services

Neng-Wen Wang · Han-Chieh Chao · Ing-Yi Chen · Yueh-Min Huang

Published online: 15 January 2010

Abstract Due to the explosive growth of the Internet and the pervasion of multimedia, protection of intellectual property (IP) rights of digital content in transactions induces people's concerns. Current security requirements and copyright protection mechanisms especially need to work in real-time and on-line for communication and networking. For media service systems in the Internet, user's authentication is most essential in association with the access control of the media system. The authentication scheme is a trivial but crucial issue for maintaining user's information. Up to now, many one-time password-based authentication schemes have been proposed. However, none is secure enough. The purpose of a one-time password (OTP) is to make it more difficult to gain unauthorized access to restricted resources. Traditionally static passwords can more easily be obtained by an unauthorized intruder given enough attempts and time. By constantly altering the password, as is done with a one-time password, this risk can be greatly reduced. These schemes are specially fit for media services in the Internet since they will frustrate the attacker's attempt. Lin, Shen and Hwang proposed a strong-password authentication scheme in association with one-time password by using smart cards, and claimed their scheme can resist guess attack, replay attack, impersonation attack and stolen attack. Later, Ku, Tsai, and Chen showed that Lin-Shen-Hwang's scheme suffers from a replay attack and a denial-of-service attack. Furthermore, Ku proposed a hash-based strong-password authentication scheme to enhance the security. In this paper, we show the weaknesses and devise some attacks against Ku's scheme. Then, we revise Ku's scheme and propose a novel user's authentication scheme in pervasive on-line media services for current communication and networking.

Keywords One-time password · User authentication · Password-based authentication · Replay attack · Denial-of-service attack

N.-W. Wang
Department of Electronic Engineering, Kao-Yuan University, Kaohsiung County, Taiwan, Republic of China
e-mail: nwwang@cc.kyu.edu.tw

H.-C. Chao
Department of Electronic Engineering and Institute of Computer Science & Information, Engineering, National Ilan University, I-Lan, Taiwan, Republic of China
e-mail: hcc@niu.edu.tw

H.-C. Chao
Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan, Republic

I.-Y. Chen
Department of Computer Science and Information Engineering, National Taipei University of Technology, Taiwan, Republic of China
e-mail: ichen@ntut.edu.tw

Y.-M. Huang (✉)
Department of Engineering Science, National Cheng Kung University, Tainan City, Taiwan, Republic of China
e-mail: huang@mail.ncku.edu.tw

1 Introduction

The explosive growth of the network and the pervasion of multimedia have encouraged many flourishing media services on the Internet. However, the protection of IP rights of digital content in transactions induces people's concerns. Inexpensive tools with easy manipulation have deteriorated the circumstance. Many significant research progresses have been developed secure communications protocols which primarily work offline in this decade. However, current security

requirements and copyright protection mechanisms need to work in real-time and on-line for current communication and networking.

For media service systems in the Internet, user's authentication is most essential in association with the access control of the media system. For decades, Password has been the major means for user authentication on computer systems. Password-based authentication mechanism is the most extensively used authentication mechanism in the Internet and mobile communication systems. However, those weak passwords are prone to dictionary attacks. Nowadays, other alternative methods are possible for user authentication [1]. Some people use smart card and identification card to store their secret tokens [2]. Such methods usually need special sensing devices. Moreover, theft and counterfeit are serious threats to these systems. To have a token does not necessarily imply to possess a legitimate ownership. Other people may use biometric methods. Biometric methods identify individuals based on distinguishing human features [3, 4]. Counterfeit and theft are generally more expensive than they are with other methods since these biometric features can not be easily substituted. However, biometric methods generally require more costly and specialized hardware.

Password is the most convenient mechanism in the Internet and mobile communication systems. Most people use easy-to-remember passwords in the network environments. However, those weak-passwords [1–10] are prone to dictionary attacks. The strong-passwords mechanism [11–17] is the other kind of password-based authentication mechanism, which uses a password and a random number with the assistance of tamper-resistant devices. Weak-password authentication password authentication schemes usually lead heavy computational load to the whole application system because of using public-key cryptographic techniques. In contrast, most strong-password authentication schemes use only simple operations, e.g., one-way hash function and XOR operation. Hence, strong-password authentication schemes have advantage over weak-password authentication schemes in terms of easy implementations cost. Strong-password authentication schemes are especially suitable for some constrained environments, although using strong passwords may increase the memory burden of the user.

Up to now, many one-time password-based authentication schemes have also been proposed. However, none is secure enough. The purpose of a one-time password (OTP) is to make it more difficult to gain unauthorized access to restricted resources. Traditionally static passwords can more easily be accessed by an unauthorized intruder given enough attempts and time. By constantly altering the password, like one-time password, this risk can be greatly reduced. These schemes are specially fit for media services in the Internet since they will frustrate the attacker's attempt. Both OTP and strong-password authentication schemes motivate us to propose a novel password authentication scheme for on-line media services. Ku [20] proposed a hash-based strong-password authentication scheme in association with one-time password to enhance the security. However, there are some weaknesses in its scheme. In this paper, we reinforce its security and facilitate its implementation and propose a novel password authentication scheme for on-line media services.

The rest of this article is organized as follows. Section 2 surveys the related works. Section 3 briefly reviews the Ku's authentication scheme. Section 4 points out the weaknesses of Ku's scheme. In Sect. 5, we propose a revised scheme: a novel password authentication scheme for future on-line media services. Section 6 analyzes the security of our scheme. Section 7 evaluates its efficiency. Finally, some brief conclusions are made in Sect. 8.

2 The related works

Lin, Shen, and Hwang [18] proposed a strong-password authentication scheme using smart cards and claimed their scheme can resist guess attack, replay attack, impersonation attack and stolen attack. Later on, Ku, Tsai, and Chen [19] showed that Lin-Shen-Hwang's scheme suffers from a replay attack and a denial-of-service attack. Hereafter, Ku [20] proposed a hash-based strong-password authentication scheme to enhance the security. We will show the weaknesses and devise some attacks against Ku's scheme in this article. The smart card may become very convenient and the day is at hand for user in current communication and networking. Hence, by using the smart card, Wang and Huang [23] revised Ku's scheme and proposed a User's Authentication in Media Services by using One-Time Password Authentication Scheme. In this paper, we revise Ku's scheme and propose a novel password authentication scheme for on-line media services. Our scheme mainly emphasize on reinforcing the security and facilitating the implementation. During all sessions of the user's login (after a successful registration), Ku's scheme sends the same time stamp in plaintext and keeps unchanged in the next session. It will not increase the security of verifier. We omit this timestamp in our model. It helps our scheme with a better time-saving solution. In each login phase, we use the hash value of a new secret in our scheme to guarantee the freshness of updated verifier. In comparing with the Ku's scheme, Ku uses a plaintext nonce. We can efficiently prevent the stolen verifier attack as described in Sect. 4. Hence, our system can be more secure. The most advantage of our scheme over Ku's is that we can provide mutual authentication between user and server.

Recently, some papers use public key to increase the security on One-Time Password [26, 27]. Others incorporate

the biometric methods such as fingerprint features [28, 29]. However, those systems will also increase some overheads. Those are difficult to be implemented in some platform with limited computational power and memory.

3 Review of the Ku's scheme

Notation and definitions

The following notation and definitions [20] are used throughout this paper.

Table 1 Notation and definitions in Ku's scheme

Notation	Definitions
A	User identity
S	Identity of the authentication server
E	Adversary
P	User's password
N	A positive integer indicates the number of the authentication session
T	A timestamp indicates the latest time A initially registers or re-registers to S
k	S's secret key used for generating a unique storage key for each user. k is under strict protection
r_n	A random nonce generated by S for session n
$h()$	A strong one-way hash function
$\oplus$	Bitwise exclusive or XOR operation
$\|$	String concatenation

Registration protocol

This protocol is invoked whenever A initially registers or re-registers to S. Let T denote the latest time A initially registers or re-registers to S and N denote a sequence number starting from 1 since A's initial registration.

Step R1. A sends his registration request to S.

Step R2. S sets T to the value of his current timestamp. If it is A's initial registration, S sets $N = 1$. Otherwise, S sets $N = N + 1$. Next, S sends N and T to A through an authenticated confidential channel.

Step R3. A computes the verifier $h^2(S\|P\|N\|T)$, and then sends it to S through an authenticated confidential channel.

Step R4. S computes the storage key $k_A^{(T)}$:

$$k_A^{(T)} = h(A\|h(k\|T)) \tag{1}$$

and then computes the sealed verifier $sv_{(N)} = h^2(S\|P\|N\|T) \oplus k_A^{(T)}$. Next, S stores $sv_{(N)}$, T, and N in his password file. Note that $k_A^{(T)}$ is computed whenever necessary.

A should re-register to S once his verifier or his password is compromised. If it is in the latter case, A should also select another password prior to Step R3.

Login protocol

This protocol is invoked whenever A logins S. Suppose that $N = n$ for session n and $T = t$.

Step L1. $A \rightarrow S$: *login request*.

Step L2. $S \rightarrow A : n, r_n, t$. (note: r_n is a random nonce selected by S.)

Step L3. A computes

$$d_1 = h^2(S\|P\|n\|t) \oplus h(S\|P\|n\|t) \tag{2}$$

$$d_2 = h(S\|P\|n\|t) \oplus h^2(S\|P\|n+1\|t) \tag{3}$$

$$d_3 = h(h^2(S\|P\|n+1\|t)\|r_{(n)}) \tag{4}$$

Step L4. $A \rightarrow S : d_1, d_2, d_3$.

Step L5. S retrieves t from his password file and computes $k_A^{(t)} = h(A\|h(k\|t))$, and then uses the computed $k_A^{(t)}$ to derive the verifier $h^2(S\|P\|n\|t)$ from the stored sealed verifier $sv_{(n)} = h^2(S\|P\|N\|t) \oplus k_A^{(t)}$. Next, S computes

$$u_1 = d_1 \oplus h^2(S\|P\|n\|t) \tag{5}$$

$$u_2 = d_2 \oplus u_1 \tag{6}$$

If $h(u_1)$ equals the retrieved $h^2(S\|P\|n\|t)$ and $h(u_2\|r_{(n)}) = d_3$ holds, S authenticates A. Otherwise, S rejects A's login request and terminates this session. Then, S computes $sv_{(n+1)} = u_2 \oplus k_A^{(t)} = h^2(S\|P\|n+1\|t) \oplus k_A^{(t)}$, replaces $sv_{(n)}$ with $sv_{(n+1)}$, and sets $N = n + 1$ for A's next login. In the login protocol, the value of T is unchanged, i.e., $T = t$.

4 The weaknesses of the Ku's scheme

On-line stolen-verifier attack

Suppose that the adversary has captured A's past authentication messages. If the adversary also knows an ever used verifier, say $h^2(S\|P\|i\|t)$ for A by some means in session i $(1 \le i \le n-1)$, he can compute all. A's old verifiers, including the oncoming verifier $h^2(S\|P\|n\|t)$ (that is, all verifiers $h^2(S\|P\|i+1\|t), h^2(S\|P\|i+2\|t), \ldots, h^2(S\|P\|n\|t)$ can be sequentially derived from all messages d_1 and d_2 on