2012 International Conference on Information and Computer Applications (ICICA 2012)
IPCSIT vol. 24 (2012) © (2012) IACSIT Press, Singapore

Candidate Password Analysis of User-Interactive Password Schemes

Sung-Hwan Kim , Hwan-Gue Cho

Dept. of Computer Science Pusan University, Korea
sunghwan@pusan.ac.kr hgcho@pusan.ac.kr

Abstract. A number of password schemes have recently been developed based on the challenge-response method to overcome the risk of shoulder-surfing attacks. There is, however, a lack of understanding about the fundamentals and general properties of password schemes. Moreover, although researchers have recognized the limits of security, no formal statement has been made about it. In this paper, we introduce a general approach to those password schemes. Regarding the concept of candidate passwords, we conducted a general analysis of user-interactive password schemes using probabilistic methods. Finally, we state the limitation of user-interactive password schemes under the certain assumption of the most powerful adversaries.

Keywords: Shoulder-Surfing, Candidate Passwords, User Interactive Authentication, Security Limit

1. Introduction

The password is the most common and widely used authentication method. Users are asked to input the username and its corresponding pre-registered password. The basic assumption on this password authentication is that the password is securely shared and nobody but the user and the system know the secret. The traditional password authentication method is vulnerable to certain kinds of attacks. In particular, shoulder-surfing is an effective and simple attack method for stealing a password. Today's wide use of graphical user interfaces such as a virtual keyboards make user input more observable [1].

To address this problem, a number of password schemes have been developed based on the challenge-response method. User-interactive protocols, however, should be simple and easy to use while providing the required security level. Unlike zero-knowledge authentication, mathematically difficult problems cannot be applied since the computation is performed by human users. It is impossible to be feasibly immune to shoulder-surfing attacks; i.e., an adversary can get even more information whenever an authentication session is exploited. Researchers have recognized these leaks of information; there are, however, no clear statements about them.

In this paper, we formally describe challenge-response–based password schemes. After defining some measures to quantify the security level of password schemes, we perform a general analysis. Finally, we show the limitation of security of user-interactive challenge-response authentication under certain assumptions..

2. Related Work on Shoulder-Surfing–Resistant Schemes

One approach to overcoming the shoulder-surfing problem is to shield user inputs from observation. Some password interfaces provide a systematic mechanism to this end [2,3]. This method is based on the limitation of the human memory capacity, so it is still vulnerable when an adversary records all interactions that are observed in a session. To handle this problem, some interaction methods have been designed not to be captured. Tactile signals are used to transfer hidden challenges that are not observable by adversaries [4,5,6]. Transferring challenges through auxillary devices such as one-time password tokens can also prevent adversaries from obtaining the entire challenge information that is necessary to log in. However, under a

certain assumption that an adversary can capture and observe all interactions between a user and a system, these methods are hardly effective in defeating shoulder-surfing problems.

Another method consists of making user inputs not directly correspond to the password. Most schemes using this method are based on the challenge-response protocols [7,8,9,10]. In this method, users are asked to make a correct answer to the given indirect questions from the system. Since the user does not make any direct input to the password, an adversary cannot easily steal the secret. Our focus is to formally describe this user-interactive challenge-response–based authentication scheme and present a general approach to analyzing it based on the concept of candidate passwords.

3. User-Interactive Challenge-Response Authentication

Challenge-response authentication consists of 4 steps of interaction between users and the system; (i) the system poses a question (challenge); (ii) the user recognizes the challenge and performs a mental operation combining it and his password; (iii) the user provides a valid answer (response) to the system; and (iv) the system verifies the answer.

An interactive password scheme generally consists of a set of challenges. A challenge is identified by possible responses, passwords, and their relationships. A response maps to several passwords to provide a mechanism for a user to make an indirect input. Since different challenges have a different correlations with the set of responses to the set of passwords, a challenge can be represented as a verification function that determines whether a response is valid for a given user password. A password scheme is then identified by responses, passwords and verification functions. More formally, a password scheme **S** is a triplet <**R**, **X**, **F**>, where:

- **R** is a set of responses
- **X** is a set of passwords
- **F** is a set of verification functions f: $R \times X \rightarrow \{True, False\}$

Compared with system-to-system authentication protocols, there are at least 2 strict limitations of in the design of a user-interactive password authentication scheme. (i) The size of the password space must be finite and much smaller than system-to-system authentication. Users may have trouble memorizing a password from a large password space; imagine that you have to memorize >100 digits of a numeric password to log in. (ii) Another limitation is that operations, which indicate **F**, used to calculate what responses are valid for a given password should be quite simple. Due to the limitation of the human capacity of computations, user-interactive password schemes cannot be based on mathematically difficult problems such as prime factorization or discrete logarithm that are widely used in system-to-system authentication. Even the multiplication of 2 numbers or modulo operations can be difficult and costly operations to a human user.

4. Candidate Password Analysis: A General Approach

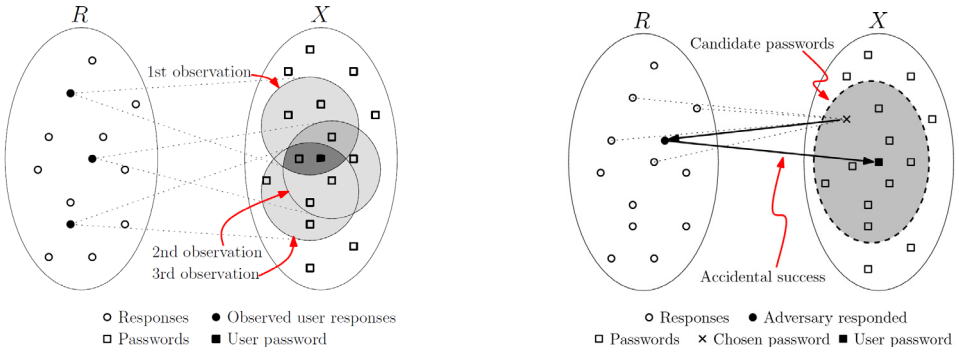
By observing several authentication sessions of a user, an adversary can gain some information about the user's password. Here we assume a powerful adversary who can intercept the entire interactions from the observed session and can extract as much information as possible. As such, a shoulder-surfing–resistant method based on the limitations of the human memory capacity does not work in our threat model.

The attack in our threat model consists of 2 parts: (i) the adversary observes a successful session of the user, and (ii) he deduces the passwords and tries one of them. Of course, the adversary can try a password without any knowledge about it. Moreover, repeated observations are available; for example, an adversary can try a password after observing 3 of a user's authentication sessions.

Once an adversary observes a user's authentication session, the adversary can deduce what the user's password is; only the passwords making the verification function recognize a valid response can possibly be the user password. We call these deduced passwords *candidate passwords*. Note that candidate passwords are initially all of the passwords shown in $\boldsymbol{X}$. The number of candidate passwords usually decreases as observations accumulate. Figure 1(a) demonstrates an example of repeated observations. As repeated observations occur, much smaller numbers of passwords belong to the intersections of each corresponding

password set from each response. The first observation consists of 5 candidate passwords. After 2 more observations occur, we can note that only 2 passwords remain

If the user password is specified, each password has its own probability of being chosen by the user in a valid authentication session. For example, the user password $\boldsymbol{x}$ has a probability of 1.0 because it is always chosen in a legal authentication session whatever the session response might be. For a password $\boldsymbol{x}$, we denote by $\boldsymbol{p}(\boldsymbol{x};\boldsymbol{x}^*)$ the probability that $\boldsymbol{x}$ is chosen in a valid session that is executed by the user whose password is $\boldsymbol{x}^*$. The expected number of candidate passwords $\boldsymbol{N}(\boldsymbol{k})$ after a $\boldsymbol{k}$ observed session can then be expressed as $p(x;x^*)$. Note that $\boldsymbol{N}(0)=|\boldsymbol{X}|$.



(a) (b)

Fig 1. An adversary can deduce candidate passwords after several observations and then try one of them. (a) The number of candidate passwords is reduced as more observations occur. (b) There are accidental cases in which the adversary successfully logs in even if he tries the wrong password.

$$N(k)=\sum_{x\in X}\left(p(x;x^*)\right)^k$$

For example, in a traditional alphanumeric password scheme, which does not have any means to defend shoulder-surfing attack, $p(x;x^*)=1$ if $x=x^*$ but $p(x;x^*)=0$ otherwise. As a result, $\boldsymbol{N}(\boldsymbol{k})=1$ for every $\boldsymbol{k}\geq 1$. In Roth's scheme [8] as another example, $p(x;x^*)=(4/9)^{\boldsymbol{m}}$ where $\boldsymbol{m}$ is the hamming distance between $\boldsymbol{x}$ and $\boldsymbol{x}^*$. If $\boldsymbol{x}=\boldsymbol{x}^*=$ "1234," then $\boldsymbol{m}=0$ and $p(x;x^*)=(4/9)^0=1$. Likewise, if $\boldsymbol{x}=$ "1111" and $\boldsymbol{x}^*=$ "1234," then $\boldsymbol{m}=3$ and $p(x;x^*)\fallingdotseq 0.088$. Since there are $9^{\boldsymbol{m}}\boldsymbol{B}(\boldsymbol{4},\boldsymbol{m})$ different passwords that have the hamming distance of $\boldsymbol{m}$ from the fixed password $\boldsymbol{x}^*$ with a length of 4 where $\boldsymbol{B}(\boldsymbol{n},\boldsymbol{m})$ is the binomial coefficient "$\boldsymbol{n}$ choose $\boldsymbol{m}$," $\boldsymbol{N}(1)=\sum_{\boldsymbol{m}} 9^{\boldsymbol{m}}\boldsymbol{B}(4,\boldsymbol{m})(4/9)^{\boldsymbol{m}}=5^4$.

Observing k successful sessions of a user, an adversary can obtain $N(k)$ candidate passwords. The adversary can choose one of the candidate passwords and try it to log in. If the chosen password is the user's password, the adversary successfully logs in. The probability that the chosen password is the user's password decreases as $\mathbf{N}(\mathbf{k})$ increases. As Figure 1(b) shows, however, although he chooses a wrong password, the chance for accidental success exists. This occurs in the case that a chosen response associated with the chosen password also maps to the user password. From the perspective of information that the adversary can obtain, the event that the adversary successfully logs in is the equivalent of observing an additional valid login session. The probability that the login is successful is the same as the probability that the chosen password remains in the set of candidate passwords after one additional observation. Denoting $\boldsymbol{S}(\boldsymbol{k})$ as the probability that the adversary successfully logs in after k observations, we have:

$$S(k)=\frac{N(k+1)}{N(k)}$$

Since the user password itself is always among the set of candidate passwords regardless of the number of observations, $\boldsymbol{N}(\boldsymbol{k})$ should not be smaller than 1. Moreover $\boldsymbol{N}(\boldsymbol{k+1})$ cannot be larger than $\boldsymbol{N}(\boldsymbol{k})$, so finally we have:

$$\lim_{k\to\infty} S(k) = 1$$

This equation tells us that there is a finite positive integer k that the adversary who observes k times of valid sessions of a user can log in with the probability of roughly 1. As we discussed in the previous section, the size of the password space $|\mathbf{X}|$ cannot be very large. Also, since $N(k)$ decreases exponentially as k increases, a positive integer k^* such that $S(k^*)>1-\varepsilon$ is not large enough for any a small positive real number ε

5. Conclusion

Based on the candidate password concept, we have presented a general approach to the analysis of user-interactive password schemes. Using the candidate password concept, it is possible to estimate the scheme resistance against several successive shoulder-surfing attacks. We also show that it is theoretically impossible to design a scheme that is completely resistant to shoulder-surfing assuming the most powerful adversaries who can observe all information transmitted between a user and a system

Nevertheless, our result does not imply that the development of a shoulder-surfing resistant password scheme is meaningless. Since we assume the most powerful passive adversaries, the practical aspects are weakly considered here. These practical issues include such subjects as the chance to be observed, the complexity to get the candidates inversely, and so on. A practical general framework that considers these issues should be developed in future work

6. ACKnowledgements

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No.2011-0003157)

7. References

[1] F. Tari; A. A. Ozok; S. H. Holden. A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords, In Proc. SOUPS, 2006, PP:56-66.

[2] R. Dhamija; A. Perrig. Déjà vu: A User Study Using Images for Authentication, In Proc USENIX SSYM, 2000, PP:45-58.

[3] D. S. Tan; P. Keyani; M. Czerwinski. Spy-resistant Keyboard: More Secure Password Entry on Public Touch Screen Displays. In Proc. OZCHI, 2005, PP:1-10.

[4] A. Bianchi; I. Oakley; D. S. Kwon. The Secure Haptic Keypad: A Tactile Password System. In Proc. CHI, 2010, PP:1089-1092.

[5] A. D. Luca; E. von Zezschwitz; H. Husmann, Vibrapass: Secure Authentication based on Shared Lies. In Proc. CHI, 2009, PP:913-916.

[6] H. Sasamoto; N. Christin; E. Hayashi. Undercover: Authentication Usable in front of Prying Eyes. In Proc. CHI, 2008, PP:183-192.

[7] S. Wiedenbeck; J. Waters; L. Sobrado; J.-C.Birget. Design and Evaluation of a Shoulder-surfing Resistant Graphical Password Scheme. In Proc. AVI, 2006, PP:177-184.

[8] V. Roth; K. Richter; R. Freidinger. A Pin-entry Method Resilient against Shoulder Surfing. In Proc. ACM CCS, 2004, PP:236-245.

[9] A. D. Luca; K. Hertzschuch; H. Hussmann. Colorpin: Securing Pin Entry through Indirect Input. In Proc. CHI, 2010, PP:1103-1106.

[10] X. Bai; W. Gu; S. Chellappan; X. Wang; D. Xuan; B. M. Pas. Predicate-based Authentication Services against Powerful Passive Adversaries. In Proc. ACSAC, 2008, PP:433-442.