MIPRO 2013, May 20-24, 2013, Opatija, Croatia

Knowledge based authentication requirements

K. Skračić, P. Pale, B. Jeren
Faculty of Electrical Engineering and Computing, University of Zagreb
Unska 3, 10000 Zagreb, Hrvatska
E-mail: kristian.skracic@fer.hr

Abstract – Published evaluation criteria for knowledge based authentication (KBA) methods do not provide a sufficiently formed framework to use as a guideline during design and testing of KBA methods and tools. The aim of this paper is to define a set of requirements for creating a secure user authentication method based on the user's knowledge. The requirements address four issues in user authentication. The first refers to eavesdropping an authentication session and using the intercepted information in the next session. By repeating the recorded response an attacker should not be able to authenticate himself as a legitimate user. The second issue is the ability to predict an authentication challenge by analyzing previous challenges. If an attacker can record a set of challenges over a long period, he should not be able to learn the next challenge beforehand. The third issue is the guessability of correct responses to authentication challenges. In general, multiple sources of information about the user are available to an attacker. The correct response to a challenge should not be obvious from such sources. The fourth issue is the authentication server's vulnerability. By this any information system component that is used to authenticate users is meant. If an attacker manages to gain partial or complete access to the authentication server and its data, the user's digital identity should not be compromised. These for requirements are proposed as a generic checklist against which KBA methods and tools should be checked.

I. INTRODUCTION

User authentication is a prerequisite for meeting basic security requirements like access control or document authenticity. Smart cards, tokens, biometric and other methods of authenticating users in information systems are gaining in popularity. However, password based authentication methods are still the dominant way of authenticating users [1], despite their numerous documented shortcomings. As stated in [1], new authentication mechanisms are yet to achieve the necessary popularity to replace passwords. Some of the reasons are explained in the next section.

In general, there are three formally accepted ways of authenticating users [21]: using something the user has, something the user knows or something the user is. These are often called authentication factors. Some research has been done to introduce a fourth factor: [22] proposes the fourth factor to be the user's location, while the research in [23] proposes using user's acquaintances. Neither of these proposals have been formally accepted yet. In this paper we focus on knowledge based authentication methods which use the factor of something a user knows.

This paper analyzes the key requirements a secure user authentication method based on user knowledge should meet. To the best of our knowledge, there are no formal requirements for user knowledge based authentication methods. However, there are several methods for evaluating knowledge based authentication methods presented in the literature. Therefore, we analyze existing evaluation methods for user knowledge based authentication methods.

The analysis of different types of knowledge base authentication (KBA) methods is outside the scope of this paper. Some insight can be found in [16] and [17]. This paper is organized as follows. Section 2 provides an overview of existing evaluation methods for knowledge based authentication. The focus is only on fact based knowledge authentication methods and textual passwords. Evaluation methods for graphical and visual passwords are beyond the scope of this paper. Section 3 describes the new proposal for user knowledge based authentication requirements. Finally, Section 4 presents authors' conclusions.

II. EVALUATION METHODS

There are several ways to evaluate authentication methods based on user knowledge. Most existing evaluation criteria are based on the experience of researchers, described as a set of security properties.

Fact based authentication methods are often called "personal verification questions". This is because most authentication questions are based on personal information from the user. However, fact based authentication methods may use any other information relating to the user. Fact based authentication methods can be divided into two types depending on the questions used to authenticate a user [25]. Static KBA constitutes authentication methods that use predetermined facts to authenticate users. For example, the user's date of birth or mother's maiden name. The use of static KBA has been widely criticized and is considered to be a weak authentication method [18]. The second type is dynamic KBA. It is similar to static KBA in that it is also based on personal information about the user. However, in dynamic KBA the user does not share the secret information beforehand. Rather the questions and answers could be derived from various data collections about user's activities like: banking, shopping, etc. This form of knowledge based authentication is new and has not been sufficiently researched. The primary problem is the acquisition of data needed to create a unique question for the user. Some research has been done on creating dynamic KBA authentication methods [24]. At this time there are no widely used authentication methods based on dynamic KBA.

Since textual passwords are the dominant authentication method in this category, the analysis begins with them. The goal is to analyze the advantages password based authentication methods have that makes their use so widespread in today's information systems.

The research conducted in [1] introduces a wide list of properties that define user authentication methods. These properties are separated into three categories. The first category questions usability benefits. These benefits evaluate how easy it is for users to authenticate themselves to the system. For example, how easy it is to memorize the information which is needed to authenticate, does the user need to carry anything with them or how easy it is to recover from loss. The second category focuses on deployability. This is an important requirement since many authentication methods in general have been discarded because of the difficulty of deploying them on a large scale. Textual passwords have a clear advantage in this area as they are remarkably easy to implement and they scale well. Furthermore, most systems implement them by default. The final category examines security benefits. Although extensive, the list of properties in [1] is not complete, as the authors themselves conclude. It can be concluded that the popularity of authentication methods is primarily based on usability and deployability, rather than security. The authors of [1] conclude that the marginal gains of new authentication mechanisms are not enough to overcome the large cost of transitioning from one authentication method to another. In conclusion, the research provided in [1] gives a clear overview of why some authentication methods are more prevalent than others. However, the proposed security properties offer no insight into how a secure authentication method should be designed. Therefore, the security properties described in [1] cannot be used as a set of requirements for a secure user authentication method.

Another evaluation method for knowledge based authentication methods can be found in [2]. Although it focuses on introducing a new authentication method based on questions and answers, it establishes a useful set of properties. For example, users should find it easy to remember the correct answers. Also, the question set should be fairly large in order to avoid repeating the same question several times. This would make it more difficult for an attacker to use the recorded answer. A complete overview of the proposed properties is accessible in [2]. It should be noted that these properties only apply to knowledge based authentication methods based on facts. Also, these rules overlap with the usability and security benefits introduced in [1]. This overlap could confirm the usefulness of the properties in [1] and [2]. However, they are used only for comparing and evaluating authentication methods. The proposed properties should not be considered as a set of requirements for two reasons. First, their purpose is strictly aimed at evaluating authentication methods. Second, they do not express a requirement that needs to be fulfilled in order to create a secure authentication method.

One of the first formal evaluation methods for knowledge based authentication systems can be found in [3]. However, like the work in [2], these criteria are aimed at authentication systems with challenge questions and they relate to their privacy, security and usability. Also, as far as the criteria are concerned, they are mostly similar to the previous two evaluation methods. The research in [3] also establishes an overview of question based authentication methods and their qualities, but such an overview is beyond the scope of this paper. We note that the research in [3] suggests creating challenges based on user's preferences or intimate data.

Comparing these three evaluation methods, we conclude that they are similar to one another. Each of them is based on its own, limited set of properties that the authors have identified as relevant when evaluating the security of user authentication methods. Furthermore, the evaluated methods address the same issues. For example, the problem of intercepting data, guessing the correct response to an authentication question and resistance to Phishing. In essence these methods enumerate properties which can be expected to change over time. It is difficult to base a design of a new authentication method on such a list. Rather, a small number of generic requirements for user authentication could be better suited and is proposed in this paper in next chapters.

III. User authentication requirements

The previous Section reviews a set of techniques for evaluating user authentication methods. To the best of our knowledge, there is not a single knowledge based authentication method that satisfies all evaluation methods presented in [1], [2] and [3]. Therefore, this paper proposes that current evaluation methods for user authentication are not constructive enough. It is authors' opinion that creating an authentication method by merely satisfying a set of properties may lead to the creation of vulnerable methods. This opinion is based on the fact that the properties described in [1], [2] and [3] represent the most common ways to bypass user authentication methods. They do not represent an exhaustive set of possible vulnerabilities. For example, the research in [1] suggests a number of criteria that are supposed to guard against intercepting secret data. One of them is resilience to physical observation. This constitutes a potentially endless set of attacks because physical observation constitutes a number of things. For example, an attacker can observe a user's monitor or keyboard. Guarding sensitive information on a monitor is different from guarding information on a keyboard. Another problem represents the meaning of the word observation. Does this constitute only visual observation, or can listening to and analyzing keystrokes be considered physical observation [10]?

Therefore, it can be concluded that a set of properties for secure user authentication methods does not constitute an exhaustive list of guidelines and cannot provide more information for future vulnerabilities. Therefore, it is proposed that the solution may be found by using more generic requirements to encompass all current and future vulnerabilities.

There are countless opportunities for data to be intercepted in an information system. Enumerating concrete ways of intercepting data may prove useful in reducing their occurrence. However, such a static list will be insufficient for guarding against future attacks.

Based on this, it can be concluded that there is no finite subset of properties that can ensure that an authentication method will never be compromised. Instead, a set of higher level requirements is proposed that a user authentication method should satisfy. Such higher level requirements are usable for evaluating a wide range of knowledge based authentication methods.

The following chapters define a set of (generic) requirements that an authentication method must satisfy in order to be secure. In order to be applicable for all knowledge based authentication methods, the requirements are intentionally generic. In other words, the requirements do not specify how to achieve security, but what is needed to achieve security.

A. One time challenges

When thinking about a secure authentication method, the first question one needs to ask is: what needs to be stolen in order to compromise a digital identity? Information can be intercepted in a variety of ways. Since communication is often carried out across the Internet, a lot of attention has been given to securing communication networks against eavesdropping. However, experience has proven that even the most secure mechanisms have flaws that make it possible to intercept secret data. For example, recent work [4] has shown that there are ways of circumventing SSL/TLS protection. Another obvious flaw is the inherent trust in user judgment. As explained in [5], an attacker can easily insert himself in a secure communication channel if the end user accepts the attacker's forged certificate.

Additionally, in a large information system, data can be intercepted in a non technical way with the use of social engineering techniques. For example, extracting secret data from an employee or "Dumpster diving"[6].

In the case of textual passwords, user authentication comes down to a single piece of information: the user's password. Once an attacker acquires the user's password, he can authenticate himself as that user as many times as he wants. Some policies address such issues by forcing users to change their passwords on a regular basis (usually once a month). According to [7] and [8], this leads to more problems as people tend to choose passwords that are easier to remember. At best, such a strategy only makes it slightly more inconvenient for an attacker to compromise a user's digital identity. There is still a formidable period in which the attacker can use the obtained secret information and pose as another user.

Amongst the more unusual eavesdropping techniques is the work done in [9] where the researchers managed to differentiate the sound made by using a keyboard. Their research showed that an eavesdropper can recognize what the user typed by the sound of the keys. Further research [10] has improved this to use keyboard characteristics and statistics of the text to decipher a recording of text typed for a period of ten minutes on a random keyboard. It is worth noting that the software used needs no previous training to recognize keystrokes. A similar experiment was conducted in [11]. The researcher has shown that a VDU's screen content can be recovered optically even from diffuse light reflected off room walls or the users face.

Based on the above, we propose that a secure authentication method must use one time passwords to authenticate users. If a password is used more than once, the authentication method can be compromised. Since passwords are not meant to be changed after every authentication, a more generic approach could be used in which a user must respond to an arbitrary challenge presented by the authentication server. Each challenge must be unique in order to satisfy the one time rule. An exception can be made if the challenge is constructed in a way that makes the correct response different every time. That way, even if the challenge is repeated several times the response cannot be misused in another authentication attempt. An example of such a challenge can be the user's phone bill. Since this is something that changes every month. Additionally, the information used for such a challenge can have a shorter lifespan. For example, the number of phone calls a user made today.

B. Challenge predictability

Considering that a secure authentication must use one time challenges, the next step to ensure secure authentication is that the challenge has to be unpredictable. One time challenges technique by itself does not ensure that the challenges will be sufficiently random.

Generally speaking, there are two ways of predicting a one time challenge. The first is to try to use a number of previously recorded challenges to predict the next one. The idea is that a challenge is generated using an algorithm. In case the attacker manages to reverse engineer the algorithm based on recorded previous challenges, he can learn how to predict the next one.

The second way to predict a one time challenge is the adaptive "Chosen message attack". This attack is based on adaptively querying the authentication server in order to gain information. If an attacker discovers how his inquiries influence creation of server's challenges, then he may be able to predict them. This can be the case if the challenges are functionally dependant on some form of user data. For example, user data can be the time the system is being accessed, the location of the user or the user's web browser. Research conducted in [13] calls such an attacker an interrogative adversary. The difference in this and the first approach is that the attacker managed to limit the possible set of queries to be issued. Both attacks assume some form of algorithm based approach to generation of challenges.

Based on this it can be concluded that the predictability is not only influenced by the algorithm used to create the challenges, but also by the type of attacker. Thus, it should be required that the probability that an interrogative adversary can guess the authentication challenge must be equal to or smaller than the probability of a non interrogative attacker guessing the challenge. Furthermore, all authentication challenges must be independent of each other in order to make it impossible to predict the next challenge based on a sample of the previous challenges. It is important that not even the legitimate user cannot predict challenges he will receive in the future. It should not only protect him from blackmailing situations but could also reduce blackmailing attempts if that property of KBA would be publicly known. Based on this, it is proposed that the challenges should not be algorithm based.

C. Response guessability

The evaluation methods proposed in [1], [2] and [3] covered guessability issues in great detail. For this reason it is further explained only where guessability concerns influence onetime challenges. When using onetime challenges, guessability is less risky. Even if an attacker manages to guess a correct response, he will not be able to use the same guessed value the second time. Still, this does not condone the practice of using challenges to which answers are easy to guess. Obvious counterexamples are the static KBA questions for fallback authentication. As described in [19], responses challenges based on personal questions tend to be extremely guessable. Given the power of social media and public records, a lot of user information is accessible to attackers. One such example is described in [18]. Research [20] has proven that challenges based on dates of birth, family members and partners are often easily guessable.

It can be concluded that a single challenge should be impervious to educated guessing attacks. In other words, if an attacker has some knowledge about the user or the system, he should not be able to guess the correct response to a challenge. Ideally, the challenges should be based on private data. By this we mean the use of data which the user is unlikely to share with friends and aquantances or make public via social networking sites. We recognize that such challenges may pose a privacy concern. However, the construction of the challenges is beyond the scope of this paper.

D. Independence of the authentication server security

Knowledge based user authentication is based on shared information. When authenticating a user, the authentication server must have a piece of information that it shares or knows about the user. This means the server has to keep this information in a local storage. If an attacker manages to acquire the shared information from the server, the user's digital identity is compromised. This poses an even bigger problem if a user uses the same information on several servers.

Therefore, there should be a requirement that the authentication method must implement the use of shared knowledge in such a way which makes it independent of the authentication server security. In other words, if an attacker manages to compromise the authentication server he should not be able to compromise the user's digital identity.

Obvious counterexamples are textual passwords, even if they are stored in some encrypted form and are salted. In cryptography, password salting is the process of adding a random value to a user password before hashing it with a one way function. When an attacker gains access to a server that uses salted passwords for authentication he can extract the salt value and the hash generated from the salt and the user's password. Using dictionary or brute force password guessing attacks, the original password can be retrieved in finite time. However, the attacker does not know what the salt value is without gaining access to the authentication server. So the attacker cannot compute the dictionary before knowing the salt value. This slows the process of guessing the password because the attacker has to generate a dictionary for every salt value. Recent work [12] demonstrates that salting only complicates password guessing, but does not prevent it. Given the number of CPU/GPU cores today, salting user passwords will not be an obstacle to attackers for long. Also, some work has been done on using FPGAs [15] to parallelize dictionary attacks. Coupled with smarter algorithm [14], guessing hashes is becoming easier and increasingly faster

To the best of authors' knowledge, currently there is no authentication method that meets this requirement. The obvious reason is that most information systems use only one server for authentication and this server usually holds all the information needed for authenticating users. For example, a server has a database of user credentials.

Based on this, it can be concluded that an authentication server needs to be distributed in order to meet this requirement. In other words, the server that implements user authentication must not be the server that the user wishes to gain access to. This mechanism only creates an additional step in the process of compromising security. The attacker now needs to gain access to the server that is used for authenticating users. The level of security could be further significantly improved by using multiple different servers to hold parts of shared information. Thus an attacker would need to gain access to them all.

IV. CONCLUSION

This paper proposes a set of requirements for authentication methods based on user knowledge. Based on the research of current evaluation methods for user authentication, it is believed that proposed requirements are sufficient to evaluate the security of existing and future authentication methods based on the user's knowledge.

Although the proposed requirements seem generic, they were not evaluated against authentication methods that use tokens or biometrics. However, further research may involve expanding the requirements so as to include authentication methods based on other authentication factors.

REFERENCES

[1] Bonneau, J.; Herley, C.; van Oorschot, P.C.; Stajano, F.; , "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," Security and Privacy (SP), 2012 IEEE Symposium on, vol., no., pp.553-567, 20-23 May 2012

[2] L. O'Gorman, A. Bagga, and J. Bentley, "Query-directed passwords," Computers & Security, vol. 24, no. 7, pp. 546–560, Oct. 2005.

[3] M. Just, "Designing Authentication Systems with Challenge Questions," in Security and Usability: Designing Secure Systems That People Can Use, 1st ed., O'Reilly Media, 2005, pp. 143–160.

[4] W. El-Hajj, "The most recent SSL security attacks: Origins, implementation, evaluation, and suggested countermeasures," Security and Communication Networks, vol. 5, pp. 113-124, 2012.

[5] Zhe Chen; Shize Guo; Rong Duan; Sheng Wang; , "Security Analysis on Mutual Authentication against Man-in-the-Middle Attack," Information Science and Engineering (ICISE), 2009 1st International Conference on , vol., no., pp.1855-1858, 26-28 Dec. 2009

[6] Janczewski, L.J.; Lingyan Fu; , "Social engineering-based attacks: Model and new zealand perspective," Computer Science and Information Technology (IMCSIT), Proceedings of the 2010 International Multiconference on , vol., no., pp.847-853, 18-20 Oct. 2010

[7] Patterson B; , letter to Communications of the ACM, vol 43, no. 4., Apr. 2000

[8] R. J. Anderson, "Chapter 2.4.3 Naïve Password Choice" in Security Engineering: A Guide to Building Dependable Distributed Systems, 1st ed. New York, NY, USA: John Wiley & Sons, Inc., 2001.

[9] Asonov, D.; Agrawal, R.; , "Keyboard acoustic emanations," Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on , vol., no., pp. 3- 11, 9-12 May 2004

[10] Zhuang L., Zhou F., Tygar JD., "Keyboard Acoustic Emanations Revisited", 12th ACM Conference on Computer and Communications Security, 2005

[11] Kuhn, M.G.; , "Optical time-domain eavesdropping risks of CRT displays," Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on , vol., no., pp. 3- 18, 2002

[12] F. Milo, M. Bernaschi, and M. Bisson, "A fast, GPU based, dictionary attack to OpenPGP secret keyrings," Journal of Systems and Software, vol. 84, no. 12, pp. 2088–2096, Dec. 2011.

[13] K. Fu, E. Sit, K. Smith, and N. Feamster, "Dos and don'ts of client authentication on the web," in Proceedings of the 10th conference on USENIX Security Symposium - Volume 10, Berkeley, CA, USA, 2001, pp. 19–19.

[14] A. Narayanan and V. Shmatikov, "Fast dictionary attacks on passwords using time-space tradeoff," in Proceedings of the 12th ACM conference on Computer and communications security, New York, NY, USA, 2005, pp. 364–372.

[15] Dandass, Y.S.; , "Using FPGAs to Parallelize Dictionary Attacks for Password Cracking," Hawaii International Conference on System Sciences, Proceedings of the 41st Annual , vol., no., pp.485, 7-10 Jan. 2008

[16] Agarwal, G.; Singh, S.; Indian, A.; , "Analysis of knowledge based graphical password authentication," Computer Science & Education (ICCSE), 2011 6th International Conference on , vol., no., pp.588-591, 3-5 Aug. 2011

[17] Gkarafli S.; Economides AA.; , "Comparing the Proof by Knowledge Authentication Techniques", International Journal of Computer Science and Security, vol. 4, no. 2, pp. 237-255, May 2010

[18] Lemos R.; , Are Your "Secret Questions" Too Easily Answered?, Technology Review, MIT, 2009.

[19] A. Rabkin, "Personal knowledge questions for fallback authentication: Security questions in the era of Facebook," in SOUPS 2008 - Proceedings of the 4th Symposium on Usable Privacy and Security, 2008, pp. 13–23.

[20] V. Griffith and M. Jakobsson, "Messin' with texas deriving mother's maiden names using public records," in Proceedings of the Third international conference on Applied Cryptography and Network Security, Berlin, Heidelberg, 2005, pp. 91–103.

[21] Guidance on Multi-factor Authentication, State Services Commission, June 2006, Version 1.0

[22] Choi, Sung; Zage, David; , "Addressing insider threat using "where you are" as fourth factor authentication," Security Technology (ICCST), 2012 IEEE International Carnahan Conference on , vol., no., pp.147-153, 15-18 Oct. 2012

[23] J. Brainard, A. Juels, R. Rivest, M. Szydlo, and M. Yung. Fourth Factor Authentication: Somebody You Know. In ACM CCS, pp. 168-78. 2006.

[24] A. Alkhalifah and G. D. Skinner, "Enhanced knowledge based authentication using iterative session parameters," World Academy of Science, Engineering and Technology, vol. 71, pp. 293–299, 2010.

[25] S. Chokhani, Knowledge Based Authentication (KBA) Metrics, Orion Security Solutions, 2004.