A Survey of Alternative Authentication Methods

Robert G. Rittenhouse
Department of Computer Engineering,
Keimyung University, Daegu, Republic of Korea.
rrittenhouse@acm.org

Junaid Ahsenali Chaudhry
Department of Computer Science,
Innopolis University, Kazan, Russia.
j.chaudhry@innopolis.ru

***Abstract*—The traditional and most common authentication method employs usernames and passwords composed of alphanumeric text possibly combined with some symbols. This method has proven to be insecure in practice as passwords that can resist attack are difficult or impossible for users to remember. This paper includes a survey of alternative authentication methods and their possible application areas and describe an authentication system in common use in Korea that combines multiple authentication methods.**

Keywords—user authentication; biometrics; graphical passwords; client certificates

I. Introduction

Proper authentication of users is critical to the proper operation of secure systems such as those used in e-commerce. The traditional method of system authentication is for the user to supply a username and associated password. This has been increasingly inadequate in practice since users tend to use passwords that are too simple, rarely use password management systems, and often use the same password for multiple sites [1], [2]. Thus the traditional method needs to be replaced or augmented with other methods.

It is important to distinguish between the various scenarios for authentication. These include: authenticating to a device (such as a mobile phone or computer), remote authentication via the web, and remote authentication via other protocols. The best choice for an authentication method varies for different scenarios. An authentication method that is acceptably secure in some instances would be insecure in others. For example passwords are harder to guess in an environment, such as an ATM that limits the number of guesses than in a file encryption scenario [3]. This paper focuses on remote authentication via the Internet.

In searching for a replacement (or more likely additional) authentication method it is important to avoid replacing a weak authentication method with another that is just as bad or worse.

Users have to live with the security arrangements the institutions they interact with provide. We discuss typical authentication schemes found on the Internet and provide an example of a complex security system involving multiple authentication methods that is in use in Korea.

II. Previous research

User identification and authentication methods take one of three general forms [4]

1. Something the user possesses such as a one-time password generator, certificate, or smart card
2. Something the user knows, such as a password or the answer to a security question. The system must then have a method of checking the user response.
3. Something that the user is, as represented by a fingerprint or iris scan.

Or “something you had once, something you’ve forgotten, or something you once were” (attributed to Stimson Garfinkel) [3]. The common username and password authentication method would be classified as “something you’ve forgotten”.

There have been several alternative authentication methods proposed including biometrics [5] graphical passwords [6] and public key authentication. These have their own limitations and drawbacks and none have replaced the username and password combination in common use though some have served as secondary authentication methods.

A. Token-Based Authentication

Token-Based authentication is based on “something you have”. This would include code books or cards, smart cards and public key based (PKI) certificates. User PKI certificates are rarely found in practice due to difficulties in deploying them and because users generally don’t understand them [7], [8] Aside from the obvious risk that the token may be lost or stolen the system must protect against replay attacks [8]. To protect against theft the token itself may be protected by a password [9].

B. Biometric Authentication

Biometric authentication systems are used to identify and/or authenticate users based on their physical characteristics. Common methods include fingerprint recognition, iris recognition, and facial recognition. Biometric authentication systems suffer from a number of problems:

- Confidentiality is a desirable criteria for an authentication system but this is difficult for biometric systems [5]
- Biometric systems are subject to imitation attacks unless monitored [3], [5]
- In the general case it is not practical to use biometrics for remote authentication across the internet as users may lack appropriate sensors.

- It is also important to note that biometrics, such as fingerprints, are not as unique to the individual as commonly assumed [3]

C. *Alternative Knowledge-Based Systems*

A number of alternatives to text based passwords have been proposed. Graphical authentication systems are one such method. Proponents claim that it is easier for humans to remember pictures than text [10] but claims often depend on overly optimistic estimates of human memory capabilities and are limited in usability [11]. Many graphical authentication systems are vulnerable to "shoulder surfing" [12].

De Angeli, Coventry, and Renaud classify graphical authentication schemes into three categories [11]:

- Drawmetric schemes ask users to create a drawing or pattern. Users then recreate this to authenticate. Patternlock [13] in Android Phone authentication and Picture Password [14] in Microsoft Windows 8 are examples of drawmetric schemes.
- Searchmetric, also known as Cognometric systems, requires a user to select a known (usually pre-selected by the user) image from a set of distractors [15].
- Locimetric systems, also known as cued-recall based systems [16], [17], require identifying a series of positions within an image.

Graphical authentication systems are fairly commonly used to authenticate to personal devices such as smart phones. Some are also usable across the Internet. They represent a promising approach and, while they have not displaced text based passwords, are sometimes used as a secondary authentication scheme.

The other common knowledge based authentication scheme is the security question. In this scheme a user provides the answer to a question that presumably no one else knows such as mother's maiden name. In practice, however, such information is rarely truly private and is often easily discovered [18].

III. Common Authentication Practice

The most common means of authentication is via username and password with security questions as fallback. The security questions are used to help reset passwords and in some cases when the user's computer is not recognized by the server. Unfortunately security questions may be both difficult for users to answer and too easy for others to guess [19]–[21]. To avoid making questions too easy for others to guess some analysts recommending lying [22] but research has found lies to be more difficult to remember [21].

Another password recovery method is via sending an SMS message or calling the user's phone. This has the drawback that it depends on the user actually having their phone which may not be the case when the user is traveling. Research shows this to be more reliable than security questions [21]. An alternative email address is another possibility that has also proven more reliable than security questions although SMS is apparently more reliable than email [21].

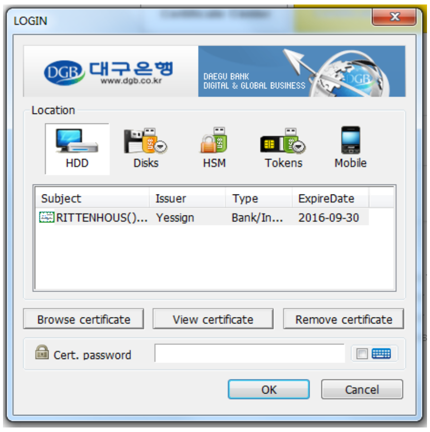
While the website provider can enforce more complex passwords there is little the provider can do about users who use the same username and password for multiple sites [1], [2]. The user's dilemma is the requirement to remember the username and password, as well as the answers to security questions for multiple sites. The easy solution for the user is just to use the same information across multiple sites.

A more secure solution is for users to use a password manager to generate and store strong random passwords, answers to security questions and usernames. This advice is somewhat controversial [23] but in the words of Warren Buffett: "Keep all your eggs in one basket, but watch that basket closely." In addition, rather than just using one email address for password resets, we recommend users consider having separate email addresses for different accounts and use one email address, which is not used for logins to other sites, to collect messages from the others.

IV. Extreme Authentication: Korean Banking

South Korea is an exception to the rule that user PKI certificates are rarely found. PKI is widely used in Korea covering approximately 60 percent of the population [24], [25]. This has helped enable Korean banks to build sophisticated authentication systems. For example: this is the sequence of steps a user of one Korean bank must follow to transfer a substantial sum of money to another bank:

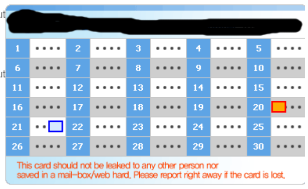
1. Prior to authentication the user must install four or more ActiveX plugins and obtain a digital certificate.
2. The user then can login to the bank using the user's digital certificate by entering the certificate password



Subject	Issuer	Type	ExpireDate
RITTENHOUS()...	Yessign	Bank/In...	2016-09-30

Cert. password

3. The user needs to enter the account PIN
4. The user also needs to enter a set of two numbers found on a card which the bank has provided


[redacted]

1	••••	2	••••	3	••••	4	••••	5	••••
6	••••	7	••••	8	••••	9	••••	10	••••
11	••••	12	••••	13	••••	14	••••	15	••••
16	••••	17	••••	18	••••	19	••••	20	▨••
21	••□	22	••••	23	••••	24	••••	25	••••
26	••••	27	••••	28	••••	29	••••	30	••••

This card should not be leaked to any other person nor saved in a mail-box/web hard. Please report right away if the card is lost.

5. The bank will send a number to the user's cell phone via SMS which the user needs to enter
6. The user confirms again with their certificate

This method combines two things the user knows (PIN and certificate password) and three things the user has (certificate, code card and cell phone). While this may appear to provide bullet-proof security in practice there are some weaknesses and two major side effects. The plugins which provide the encryption protocol, anti-virus, anti-keystroke logging and a firewall are inadequate to the task [25]. Users typically store their certificates on their hard disks or USB keys and the password protection can be bypassed by malware by key logging or brute-force attack [25]. The major side effects are that the use of ActiveX has made Korea a virtual Microsoft monopoly and left Korea with poor web accessibility [26]. In addition, Korean web users habitually install ActiveX controls without being aware of how easily an ActiveX control can compromise security. Korean users are conditioned to "Click on O.K. all the time. Never, ever choose No!" [26]

V. FUTURE WORK

Alternative authentication methods are often promoted in the literature with a lot of partiality. This is because traditional authentication methods are often easily compromised. In our observation this is because of wrongly configured infrastructure, overused/underused security measures, and context obscured policies. In our opinion it is important that the authentication methods are tied to multi-faceted keys that are distributed, maintained, and created on a different channel of communication. It is often observed that the keys/credentials are transferred on the same network as the data which creates doors for common channel attacks.

Authentication servers are maintained through a directory service i.e. LDAPs, Active Directory, etc. The security measures are applied to the authentication server itself but connections to these directory servers are not secured or the database itself is transparent to the front-world facing services. Moreover, the authentication mechanism that is novel to the legacy systems needs developing infrastructure which could be developed atomically without changing "everything" in the existing infrastructure.

VI. CONCLUSION

Computer security is difficult. It is made more so by users who are much like babes in the woods and by providers that only do the minimum required. It has proven difficult to move beyond standard username password authentication methods. There are, however, actions that users can take to improve their security.

REFERENCES

1. A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, Dec. 1999.
2. D. Florencio and C. Herley, "A large-scale study of web password habits," *Proc. 16th Int. Conf. World Wide Web WWW 07*, vol. 20, no. 3, p. 657, 2007.
3. R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. New York: Wiley, 2008.
4. C. W. Beardsley, "Is your computer insecure?," *IEEE Spectr.*, vol. 9, no. 1, pp. 67–78, Jan. 1972.
5. F. A. Qazi, "A Survey of Biometric Authentication Systems," in *Proceedings of the International Conference on Security and Management (SAM 04)*, 2004, pp. 61–67.
6. R. G. Rittenhouse, J. A. Chaudry, and M. Lee, "Security in Graphical Authentication," *Int. J. Secur. Its Appl.*, vol. 7, no. 3, pp. 347–356, 2013.
7. D. Balfanz, G. Durfee, D. K. Smetters, and R. E. Grinter, "In search of usable security: five lessons from the field," *IEEE Secur. Priv. Mag.*, vol. 2, no. 5, pp. 19–24, Sep. 2004.
8. K. Fu, E. Sit, K. Smith, and N. Feamster, "The Dos and Don'ts of Client Authentication on the Web.," *USENIX Secur. Symp.*, 2001.
9. K. I. P. Patil and J. Shimpi, "A Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devices," *Int. J. Innov. Technol. Explor. Eng.*, vol. 2, no. 4, pp. 155–157, 2013.
10. W. Hu, X. Wu, and G. Wei, "The Security Analysis of Graphical Passwords," in *2010 International Conference on Communications and Intelligence Information Security*, 2010, pp. 200–203.
11. A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," *Int. J. Hum. Comput. Stud.*, vol. 63, no. 1–2, pp. 128–152, Jul. 2005.
12. A. H. Lashkari, S. Farmand, D. O. Bin Zakaria, and D. R. Saleh, "Shoulder Surfing attack in graphical password authentication," *Int. J. Comput. Sci. Inf. Secur.*, vol. 6, no. 2, p. 10, Dec. 2009.
13. A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Glezer, "Google Android: A Comprehensive Security Assessment," *IEEE Secur. Priv. Mag.*, vol. 8, no. 2, pp. 35–44, Mar. 2010.
14. W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture password: a visual login technique for mobile devices," US Department of Commerce, National Institute of Standards and Technology, NISTR 7030, 2003.
15. K. Renaud, "On user involvement in production of images used in visual authentication," *J. Vis. Lang. Comput.*, vol. 20, no. 1, pp. 1–15, Feb. 2009.
16. S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords," in *Proceedings of the 2005 symposium on Usable privacy and security - SOUPS '05*, 2005, pp. 1–12.
17. W. Z. Khan, M. Y. Aalsalem, and Y. Xiang, "A Graphical Password Based System for Small Mobile Devices," *Int. J. Comput. Sci.*, vol. 8, no. 2, pp. 145–154, 2011.
18. National Academy of Sciences; Royal Society, *Cybersecurity Dilemmas: Technology, Policy, and Incentives: Summary of Discussions at the 2014 Raymond and Beverly Sackler U.S.-U.K. Scientific Forum*. The National Academies Press, 2015.
19. S. Schechter, A. J. B. Brush, and S. Egelman, "It's No Secret. Measuring the Security and Reliability of Authentication via &#147;Secret&#148; Questions," in *2009 30th IEEE Symposium on Security and Privacy*, 2009, pp. 375–390.
20. A. Rabkin, "Personal knowledge questions for fallback authentication," in *Proceedings of the 4th symposium on Usable privacy and security - SOUPS '08*, 2008, p. 13.
21. J. Bonneau, E. Bursztein, I. Caron, R. Jackson, and M. Williamson, "Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google," pp. 141–150, May 2015.
22. [22] D. Kearns, "Lie your way to password security | Network World," *Network World*, 2010. [Online]. Available: http://www.networkworld.com/article/2191598/security-vulnerability-mgmt/lie-your-way-to-password-security.html. [Accessed: 29-Oct-2015].
23. [23] A. Hern, "Do we really want to keep all our digital eggs in one basket?," *The Guardian*, 2015. [Online]. Available: http://www.theguardian.com/technology/2015/jun/17/do-we-really-want-to-keep-all-our-digital-eggs-in-one-basket. [Accessed: 29-Oct-2015].

24. [24] D. Park, “Social Life of PKI: Sociotechnical Development of Korean Public-Key Infrastructure,” *IEEE Ann. Hist. Comput.*, vol. 37, no. 2, pp. 59–71, Apr. 2015.

25. [25] H. Kim, J. H. Huh, and R. Anderson, “On the Security of Internet Banking in South Korea–a lesson in how not to regulate security,” 2011.

26. [26] H. M. Park, “The Web Accessibility Crisis of the Korea’s Electronic Government: Fatal Consequences of the Digital Signature Law and Public Key Certificate,” in *2012 45th Hawaii International Conference on System Sciences*, 2012, pp. 2319–2328.