Research Taxonomy

by

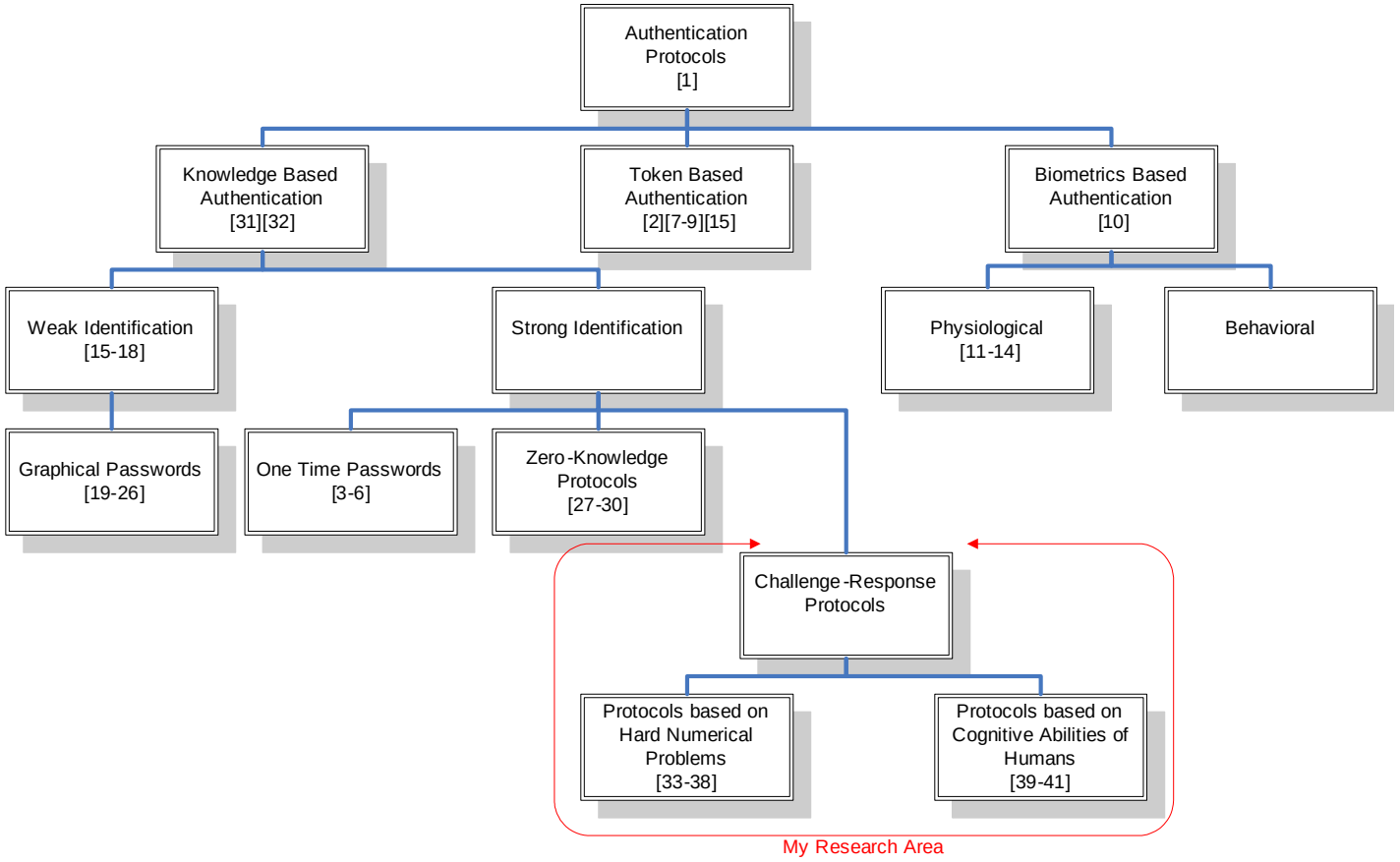
Hassan Jameel, PhD Fellow

u-Security Research Group
hassan@oslab.khu.ac.kr

Research Taxonomy

Taxonomy of Human Identification Protocols

By: Hassan Jameel



Introduction

The task of developing protocols for humans to securely authenticate themselves to a remote server has been an interesting topic in cryptography as a replacement for the traditional less secure password based systems. The protocols proposed in literature are based on some underlying difficult mathematical problem, which are tuned so as to make them easily computable by humans. As a result these protocols are easily broken when desired to be efficiently executable. Our goal is to develop Human Identification Protocol based on the cognitive ability of humans, which are both efficient and secure in the cryptographic sense.

Bibliography

[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press Series on Discrete Mathematics and Its Applications. CRC Press, Inc., 1996. Available online at http://www.cacr.math.uwaterloo.ca/hac.

[2] Hans-Peter K?br> onigs. Cryptographic identification methods for smart cards in the process of standardization. IEEE Communications Maganize, 29(6):42?8, 1991.

[3] Leslie Lamport. Password authentication with insecure communication. Communications of the ACM, 24(11):770?72, 1981.

[4] Aviel D. Rubin. Independent one-time passwords. Computing Systems, 9(1):15?7, 1996.

[5] Neil Haller. The S/KeyTM one-time password system (also known as Internet RFC 1760). In Proc. 1994 Symposium on Network and Distributed Systems Security (NDSS'94), pages 151?57. IEEE Computer Society, 1994.

[6] Liqun Chen and Chris J. Mitchell. Comments on the S/KEY user authentication scheme. Operating Systems Review, 30(4):12?6, 1996.

[7] Moni Naor and Benny Pinkas. Visual authentication and identification. In Advances in Cryptology - CRYPTO'97, Lecture Notes in Computer Science 1294, pages 322?36. Springer-Verlag, Berlin, 1997.

[8] Ching-Nung Yang, Y. B. Yeh, and Chi-Sung Laih. A dynamic password visual authentication scheme through Internet. In Proc. 16th Int. Telecommunication Symp. (ITS'98), pages 163?67, 1998.

[9] Kazukumi Kobara and Hideki Imai. Limiting the visible space visual secret sharing schemes and their application to human identification. In Advances in Cryptology - ASIACRYPT'96, Lecture Notes in Computer Science 1163, pages 185?95. Springer-Verlag, Berlin, 1996.

[10] Marc Boroditsky and Bruce Pleat. Security the edge: Making security and usability a reality with SSO. Available at http://www.passlogix.com/media/pdfs/security_at_the_edge.pdf, 2001.
[11] UK Biometrics Working Group. Use of biometrics for identification and authentication: Advice on product selection. Issue 1.0, Available online at http://www.cesg.gov.uk/technology/biometrics/media/Biometrics%20Advice.pdf, 23 November 2001.
[12] Tony Mansfield, Gavin Kelly, David Chandler, and Jan Kane Biometric product testing final report. Issue 1.0, CESG/BWG Biometric Test Programme, Available online at http://www.cesg.gov.uk/technology/biometrics/media/Biometric%20Test%20Report%20pt1.pdf, 19 March 2001.
[13] Ton van der Putte and Jeroen Keuning. Biometrical fingerprint recognition: Don't get your fingers burned. In Proc. IFIP TC8/WG8.8 4th Working Conference on Smart Card Research and Advanced Applications, pages 289?03. Kluwer Academic Publishers, 2000. Also available online at http://cryptome.org/fake-prints.htm.
[14] Crypto-Gram. Biometrics: Truths and fictions. Available online at http://www.counterpane.com/crypto-gram-9808.html#biometrics1998.
[15] Peter J. Denning. Passwords. American Scientist, 80(2):117?20, 1992.
[16] Robert Morris and Ken Thompson. Password security: A case history. Communications of the ACM, 22(11):594?97, 1979.
[17] David C. Feldmeier and Philip R. Karn. UNIX password security - ten years later. In Advances in Cryptology - CRYPTO'89, Lecture Notes in Computer Science 435, pages 44?3. Springer-Verlag, Berlin, 1990.
[18] Anne Adams and Martina Angela Sasse. Users are not the enemy. Communications of the ACM, 42(12):41?br> 46, 1999.
[19] Real User Corporation. The science behind Passfaces. Available at http://www.realuser.com/published/ScienceBehindPassfaces.pdf,Sep., 2001.
[20] Real User Corporation. PKI and PassfacesTM: Synergistic or competitive? Available at http://www.realuser.com/published/PassfacesAndPKI.pdf,Oct., 2001.
[21] Sacha Brostoff and M. Angela Sasse. Are Passfaces more usable than passwords? a field trial investigation. In S. McDonald, Y. Waern, and G. Cockton, editors, People and Computers XIV - Usability or Else (Proceedings of HCI 2000), pages 405-24, Sunderland, UK, September 5th - 8th 2000. Springer, Berlin.
[22] Rachna Dhamija and Adrian Perrig. Deja Vu: A user study using images for authentication. In Proc. 9th USENIX Security Symposium, pages 45?8, 2000. Available at http://www.usenix.org/events/sec2000/dhamija.html.
[23] Vince Sorensen. PassPic - Visual password management. Please visist http://www.authord.com/PassPic,2002.
[24] Passlogix Inc. Welcome to passlogix. Please visit http://www.passlogix.com,2002.
[25] Marc Boroditsky. v-GOTM: Usable security technology. Available at http://www.passlogix.com/media/pdfs/usable_security.pdf, 2000.

[26] David Bensinger. Human memory and the graphical password. Available at http://www.passlogix.com/media/pdfs/bensinger.pdf, 1998.
[27] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Advances in Cryptology - CRYPTO'86, Lecture Notes in Computer Science 263, Springer-Verlag, Berlin, 1987.
[28] Uriel Feige, Amos Fiat, and Adi Shamir. Zero knowledge proofs of identity. In Proc. the 9th annual ACM conference on Theory of computing (STOC'87), pages 210-217. ACM Press New York, 1987.
[29] Louis C. Guillou and Jean-Jacques Quisquater. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. In Advances in Cryptology - EUROCRYPT'88, Lecture Notes in Computer Science 330, pages 123-128. Springer-Verlag, Berlin, 1988.
[30] C.P. Schnorr. Efficient identification and signatures for smart cards. In Advances in Cryptology - CRYPTO'89, Lecture Notes in Computer Science 435, pages 239-252. Springer-Verlag, Berlin, 1990.
[31] Ross J. Anderson. Why cryptosystems fail. Communications of the ACM, 37(11), 1994.
[32] searchSecurity.com. Shoulder surfing. Available online at http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci802244,00.html, Feb 14, 2002.
[33] Tsutomu Matsumoto and Hideki Imai. Human identification through insecure channel. In Advances in Cryptology - EUROCRYPT'91, Lecture Notes in Computer Science 547, pages 409-421. Springer-Verlag, Berlin, 1991.
[34] Chih-Hung Wang, Tzonelih Hwang, and Jiun-Jang Tsai. On the Matsumoto and Imai's human identifi-cation scheme. In Advances in Cryptology - EUROCRYPT'95, Lecture Notes in Computer Science 921, pages 382-392. Springer-Verlag, Berlin, 1995.
[35] Tsutomu Matsumoto. Cryptographic human identification. In Analysis, Design and Evaluation in Human-Computer Interaction, volume III of Proc. 6th Int. Conf. on Human-Computer Interaction (HCI International'95), pages 147-152, 1995.
[36] Tsutomu Matsumoto. Human-computer cryptography: An attempt. In Proc. ACM Conf. on Computer and Communication Security, ACM Press, 1996.
[37] Nicholas J. Hopper and Manuel Blum. A secure human-computer authentication scheme. Technical Report of Carnegie Mellon University CMU-CS-00-139, Available online at http://reports-archive.adm.cs.cmu.edu/anon/2000/abstracts/00-139.html, May, 2000.
[38] Nicholas J. Hopper and Manuel Blum. Secure human identification protocols. In Advances in Cryptology - ASIACRYPT 2001, Lecture Notes in Computer Science 2248, pages 52?6. Springer-Verlag, Berlin, 2001.
[39] Aladdin Center of Carnegie Mellon University. The CMU HumanAut project. Available at http://www.captcha.net/humanaut, 2002.
[40] Lius von Ahn, Manuel Blum, and John Langford. Telling humans and computers apart (automatically) or How lazy cryptographers do AI. Technical Report CMU-CS-02-117, Carnegie Mellon University, Feb. 2002.

[41] DaphnaWeinshall: Cognitive Authentication Schemes Safe Against Spyware (Short Paper). 2006 IEEE Symposium on Security and Privacy. (2006) 295–300