Volume 3, Issue 1, January 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Guessing Human-Chosen Secrets

Rajeshwari Sangolli* Dept of Computer Applications CMJ University Bangalore, India

Dr. G Mahadevan Dept of Computer Applications AMC Engineering College Bangalore, India

Badri H.S Dept of Computer Applications Presidency College Bangalore, India

Abstract: Authenticating humans to computers remains a notable weak point in computer security despite decades of effort. Although the security research community has explored dozens of proposals for replacing or strengthening passwords, they appear likely to remain entrenched as the standard mechanism of human-computer authentication on the Internet for years to come. Even in the optimistic scenario of eliminating passwords from most of today's authentication protocols using trusted hardware devices or trusted servers to perform federated authentication, passwords will persist as a means of "last-mile" authentication between humans and these trusted single sign-on deputies.

Keywords: Authentication, Computers, Computer Security, Internet, Password.

I. INTRODUCTION

Secret knowledge stored in human memory remains the most widely deployed means of human computer authentication. Most notably, text passwords dominate authentication over the
Internet and numeric PINs dominate authentication for payment card transactions. Most security engineers believe both are weak points whose security continues to decline with the increasing number of third parties seeking to authenticate users [21, 44]. Reliable data on damages caused by weak human-chosen secrets is hard to come by [41], but a recent study of corporate data breaches commissioned by Verizon [12] suggested that nearly a third are due to stolen login credentials. This surpasses classic technical exploits such as SQL injection or buffer overflows. Of attacks using stolen login credentials, over a quarter were estimated to be stolen by some form of a guessing attack. Guessing attacks have had major business implications, such as a 2009 incident in which a vandal guessed a Twitter executive's password and was able to leak all of the company's internal documents [75].

There also exists a significant threat to individuals' private online accounts. A 2008 study by Symantec [7] of online black markets found a vibrant economy trading in stolen passwords. Due to the widespread re-use of passwords across sites [52], an emerging attack model is to compromise accounts by a guessing attack against a low-security website and attempt to re-use the credentials at critical websites [40]. At the same time as attacks on passwords are becoming an industrial-scale threat, the past few years have seen massive data sets of passwords available for study for the first time. While passwords and PINs have long been considered weak secrets, computer security researchers have lacked a standard way for analyzing how resistant these credentials actually are to guessing. The literature lacks sound methodology to answer simple questions such as "Do passwords provide better security against guessing than PINs?" or "Do users of website A pick more secure passwords than users of website B?".

In cryptographic terms, authentication is a protocol between a principal claiming a certain identity, called the prover or claimant, and a sceptical principal called the verifier requesting
proof. In remote human-computer authentication, the prover is often called the user and the verifier called the server. Software operating on behalf of the user is called the user agent or browser. The term client may refer to either the user, the user agent, or their combination. In static authentication protocols, the prover sends a password x, also called a secret or token, to the verifier along with a claimed identity. We will often use the term password in a generic sense to refer to any fixed secret knowledge, which may be a PIN, graphical password, or some other item. When clarity is needed, we will use the term text password to mean a traditional short, human-chosen character string. Upon receipt of an authentication request the verifier checks it against a database, ideally in hashed format, and makes an authentication decision. Because the prover must be granted or denied access the verifier acts as an oracle to test whether arbitrary pairs are valid. Together, a valid pair is referred to as a credential. An attacker's goal is typically to obtain one or more valid credentials from a target verifier.

Some knowledge-based authentication schemes require the verifier to send a specific challenge c to the prover prior to receiving the password. In some schemes c is fixed for each prover, such as a personal knowledge question or an image on which to click secret points. A fixed challenge is usually called a prompt. In other schemes, referred to as challenge-response protocols, c is unique for each authentication attempt and is called a nonce, timestamp or counter. Varying challenges must be incorporated by responding with some function f(x; c) instead of simply x. The computed value f(x; c) is often called a one-time password. The function f might be executed by a computer, in which case it can provide cryptographic security, or designed to be simple enough for humans to compute with sub-cryptographic security.

Any attacker attempting to find credentials by guessing likely passwords can be considered a guessing attacker. An online guessing attack consists of submitting guessed credentials (i; x) to the verifier to test their validity. A well-designed verifier will employ rate-limiting techniques to limit the number of guesses which can be made, for example by limiting the number of authentication attempts in a given time period, forcing a user to reset his or her password after too many failed attempts, or requiring the prover to solve puzzles such as CAPTCHAs.

In an online guessing attack, the attacker has obtained some value cryptographically derived from x which can be used to verify guesses. Often this is the password hash H(x) obtained through a database compromise, but it may also be the value f(x; c) for a known challenge c obtained by eavesdropping. No rate-limiting is possible in this scenario so the attacker is only throttled by available computational resources. Online attacks are also called brute-force attacks or password cracking. Further it is possible classify guessing attacks by the attacker's goals. In a targeted or vertical attack, the attacker only seeks to determine x for a fixed value of i. Targeted attackers can research the targeted user i to enhance their guessing strategy or attempt to steal x outside of the authentication protocol completely. In a trawling or horizontal attack, an attacker has a large list of identities i1, . ,.,.ik and is interested in discovering the correct x for as many as possible. A trawling attacker typically won't have user-specific information for any of the available identities and will instead guess the most likely population-wide passwords. Security economics suggests that on the Internet, trawling attacks scale more efficiently than targeted attacks [39].

Although the compiler is an unusually well-developed Preventing the attacker from assembling a large list of valid identities is one defense against a trawling attack. An adversary may attempt to test if an identity i is valid without knowing the correct password x to prevent wasted guessing effort. This is referred to as user probing. A securely implemented verifier should return a generic error if either the identity i does not exist or the wrong x is supplied to prevent user probing. While all combinations of online/online and targeted/trawling attack are possible, some literature assumes that online attacks are always trawling attacks and online attacks are always targeted which are the most common cases. An attacker may steal credentials without guessing them. One approach is to masquerade as a valid verifier and attempt to collect credentials when provers attempt to authenticate. This is called phishing. Alternately, an attacker may try to observe authentication between a valid prover and verifier. The most common mechanism is by running malicious software (or malware) on a victim's computer which silently records credentials as they are entered, often called a keylogging attack. Credentials can also be observed during transmission if they are not encrypted in an eavesdropping attack, also referred to as password sniffing or password snooping. Finally, an attacker may physically observe a user entering credentials in a physical observation attack. This is often referred to as shoulder-surfing if the attacker personally observes the entry of credentials, but a physical observation attack may also involve video cameras or other automated equipment. This dissertation will focus exclusively on guessing and not consider these attacks any further.

II. CONCEPTUAL BACKGROUND

The use of secret words to authenticate humans has ancient origins. The concept dates at least as far back as the military of ancient Rome, which developed a careful procedure for circulating daily signa or “watchwords" to prevent infiltration as documented by the historian Polybius in 118 BCE [237]. It also appears in folklore, famously in the tale of Ali Baba and the forty thieves (first translated into English in 1785 [96]), with the protagonist using the phrase “open sesame" to unseal a magical cave. Ominously, Ali Baba's greedy older brother Qasim forgets this password during the course of the story with disastrous consequences. With the development of the first multi-user computer operating systems in the early 1960s, human-computer authentication was needed for the first time to prevent unauthorized access to other users' files. The Compatible Time-Sharing System at MIT [66] is often considered the first computer system to deploy passwords, storing a password for each account in an unencrypted master file. The primary security threat was users stealing scarce computing time rather than secret data [70]. Indeed, Alan Scherr admitted to committing the likely first-ever password compromise as a doctoral student in 1962 to increase the computing time available for his own jobs [30]. The CTSS implementation also saw the first-ever password database leak in 1965 when a bug sent the password file to a public printer, requiring administrators to reset every users' password by hand [30].

Multics brought the first commercial deployment of a secure time-sharing operating system in 1968, though by 1974 designers concluded that passwords were “surprisingly easy to guess" [57]. Based on the Multics experience, Morris and Thompson improved password hashing and introduced per-user salts during the development of UNIX. They also cracked over 80% of accounts in the first published dictionary attack in 1979, warning that user-chosen passwords were a major vulnerability. A password-cracking club, the `Computer Freaks,' arose as early as 1981 [70]. Password insecurity first gained widespread notoriety in 1988 with the launch of the infamous Morris worm,1 which guessed passwords on every reachable host using a 431-word dictionary.

The publicity surrounding the worm and the onset of the World Wide Web in the early 1990s motivated a surge of research into replacing or improving passwords for remote human computer authentication. Proposals for cryptographic password verification protocols [31, 32, 33] and proactive password-checking systems [36, 77, 33] saw little adoption though and text passwords quickly proliferated as the dominant means of authentication on the web. Neither Microsoft's propriety Passport system [77] nor the community-driven open-source OpenID project [46] succeeded in bringing federated authentication to the web, while graphical and cognitive authentication schemes have failed to gain significant adoption. Passwords have garnered publicity again in the past few years with the first massive leaks of password databases.

III. PRACTICAL ASPECTS OF PASSWORD AUTHENTICATION

Roger Needham and Michael Guy are credited with first proposing the one-way scrambling of stored passwords in the 1963 Titan system [31]. By storing the result of a one-way function H(x), instead of simply x, and recomputing H(x0) for any submitted password x0, theft of the password file does not reveal plaintext passwords. In the absence of standard cryptographic hash functions, several ad hoc algorithms were proposed [61, 42]. The proprietary scheme deployed by Multics was broken by Downey in 1974 [91]. This motivated Morris and Thompson's development of the UNIX crypt() function [21], consisting of 25 iterations of a tweaked DES cipher5 and 12-bit random values for each user called salts, with passwords limited to 8 ASCII characters. This has influenced most designs since and is still occasionally used on the web; it was ultimately proved cryptographically secure in 2000 [30].

Feldmeier and Karn noted in 1989 [99] that increasingly fast implementations of crypt() would soon allow brute-forcing the entire input space. Manber proposed increasing the cost of brute-force by using secret salt values in 1996 [97] which must be brute-forced during verification. Kelsey et al. formally studied the key strengthening problem in 1997 and advocated increased iterations and mixing the salt into every round [70]. Provos and Mazi_eres implemented Kelsey et al.'s approach with bcrypt() in 1999 using a parameterized iteration count [241]; this approach has been widely adopted and was standardized as the Password- Based Key Derivation Function (PBKDF2) in 2000 [64]. Despite this broad literature, Falk et al.'s 2008 study observed over 31% of banking websites failing to hash passwords [98]. Thus, estimated a rate of 29{50%} in the survey [47].

IV. CONCLUSION

It has long been of interest to analyze how secure a given data set of passwords is against guessing attacks, dating at least to Morris and Thompson's seminal 1979 analysis of 3,000 passwords [21]. They recovered 84% of available passwords by trying all 6-character ASCII strings, variations of available usernames and every entry in the 250,000-word system dictionary. Unfortunately, they reported the results of all approaches mixed together, while noting that the dictionary approach was more efficient. They also reported some basic statistics such as password lengths (71% were six characters or fewer) and frequency of non-alphanumeric characters (14% of passwords). These two approaches, password cracking and semantic evaluation have been the basis for many studies in the thirty years since. Authenticating humans to computers remains a notable weak point in computer security despite decades of effort. Although the security research community has explored dozens of proposals for replacing or strengthening passwords, they appear likely to remain entrenched as the standard mechanism of human-computer authentication on the Internet for years to come. Even in the optimistic scenario of eliminating passwords from most of today's authentication protocols using trusted hardware devices or trusted servers to perform federated authentication, passwords will persist as a means of “last-mile" authentication between humans and these trusted single sign-on deputies.

ACKNOWLEDGMENT

I am indebted to Dr. G. MAHADEVAN for his valuable insights and guidance.

REFERENCES

[1] John the Ripper. http://www.openwall.com/john/.
[2] Data Encryption Standard. Technical Report FIPS PUB 46, National Institute of Standards and Technology, 1977.
[3] Password Usage. United States Federal Information Processing Standards Publication 112, 1985.
[4] Automated Password Generator (APG). Technical Report FIPS PUB 181, National Institute of Standards and Technology, 1993.
[5] Pubcookie Design Speci_cations. http://www.pubcookie.org/docs/specs.html,2003.
[6] EMV Integrated Circuit Card Standard for Payment Systems version 4.2. EMVco, 2008.
[7] Symantec Report on the Underground Economy, 2008. Symantec Corporation.
[8] Veri_ed by Visa. www.visa.com/verifiedbyvisa/, 2010.
[9] ISO 9564:2011 Financial services|Personal Identi_cation Number (PIN) management and security. International Organisation for Standardisation, 2011.
[10] Microsoft Passport, 2011. https://www.passport.net.
[11] PassWindow. http://www.passwindow.com, 2011.
[12] Data Breach Investigative Report. Verizon, Inc., 2012.
[13] The Unicode Standard Version 6.1. The Unicode Consortium, 2012.
[14] Anne Adams and Martina Angela Sasse. Users are Not the Enemy. Communications of the ACM, 42(12):40{46, 1999.
[15] Anne Adams, Martina Angela Sasse, and Peter Lunt. Making Passwords Secure and Usable. In HCI 97: Proceedings of HCI on People and Computers XII, pages 1{19,London, UK, 1997. Springer-Verlag.
[16] Ben Adida. Beamauth: Two-Factor Web Authentication with a Bookmark. In CCS '07: Proceedings of the 14th ACM Conference on Computer and Communications Security, pages 48{57, New York, NY, USA, 2007. ACM.
[17] Ben Adida. EmID: Web Authentication by Email Address. In W2SP '08: Proceedings of Web 2.0 Security and Privacy Workshop, 2008.
[18] Petar S. Aleksic and Aggelos K. Katsaggelos. Audio-Visual Biometrics. In Proceedings of the IEEE, volume 94, pages 2025{2044, 2006.

[19] Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot. Revisiting Defenses Against Large-Scale Online Password Guessing Attacks. IEEE Transactions on De- pendable and Secure Computing, 9(1):128{141, 2012.
[20] James P. Anderson. Information Security in a Multi-User Computer Environment. volume 12 of Advances in Computers, pages 1{36. Elsevier, 1972.
[21] Ross J. Anderson. Cryptography and Competition Policy | Issues with `Trusted Computing'. In PODC '03: Proceedings of the 22nd Annual Symposium on Principles of Distributed Computing, pages 3{10, New York, NY, USA, 2003. ACM.
[22] Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, New York, 2nd edition, 2008.
[23] Harald R. Baayen. Word Frequency Distributions. Text, Speech and Language Technology. Springer, 2001.
[24] Lucas Ballard, Seny Kamara, and Michael K. Reiter. The Practical Subtleties of Biometric Key Generation. In Proceedings of the 17th USENIX Security Symposium, pages 61{74, Berkeley, CA, USA, 2008.
[25] Lucas Ballard, Daniel Lopresti, and Fabian Monrose. Evaluating the Security of Handwriting Biometrics. In 10th International Workshop on Frontiers in Handwriting Recognition. Universit_e de Rennes 1, Suvisoft, 2006.
[26] Davide Balzarotti, Marco Cova, and Giovanni Vigna. ClearShot: Eavesdropping on Keyboard Input from Video. In SP '08: Proceedings of the 2008 IEEE Symposium on Security and Privacy, pages 170{183, Washington, DC, USA, 2008. IEEE Computer Society.
[27] Gregory V. Bard. Spelling-Error Tolerant, Order-Independent Pass-Phrases via the Damerau-Levenshtein String-Edit Distance Metric. In ACSW '07: Proceedings of the 5th Australasian Symposium on ACSW Frontiers, volume 68, pages 117{124, Darlinghurst, Australia, 2007. Australian Computer Society, Inc.
[28] Ben F. Barton and Marthalee S. Barton. User-friendly password methods for computermediated information systems. Computers & Security, 3:186{195, 1984.
[29] Bernardo B_atiz-Lazo and Robert J.K. Reid. The Development of Cash-Dispensing Technology in the UK. IEEE Annals of the History of Computing, 33:32{45, 2011.
[30] J. Beirlant, E. J. Dudewicz, L. Gy□or_, and E. C. Meulen. Nonparametric Entropy Estimation: An Overview. International Journal of Mathematics, Statistics and Science, 6(1), 1997.
[31] Steven M. Bellovin and Michael Merritt. Encrypted Key Exchange: Password-Based Protocols SecureAgainst Dictionary Attacks. In SP '92: Proceedings of the 1992 IEEE Symposium on Security and Privacy, pages 72{84, Washington, DC, USA, 1992. IEEE Computer Society.
[32] Steven M. Bellovin and Michael Merritt. Augmented Encrypted Key Exchange: A Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise. In CCS '93: Proceedings of the 1st ACM Conference on Computer and Communications Security, pages 244{250, New York, NY, USA, 1993. ACM.
[33] F. Bergadano, B. Crispo, and G. Ru_o. Proactive Password Checking with Decision Trees. In CCS '97: Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 67{77, New York, NY, USA, 1997. ACM.
[34] Vittorio Bertocci, Garrett Serack, and Caleb Baker. Understanding Windows Cardspace: An Introduction To the Concepts and Challenges of Digital Identities. Addison-Wesley Professional, 1st edition, 2007.
[35] Robert Biddle, Sonia Chiasson, and P.C. van Oorschot. Graphical Passwords: Learning from the First Twelve Years. Technical Report TR-11-01, Carleton University, 2011.
[36] Matt Bishop. A Proactive Password Checker. Technical report, Hanover, NH, USA,1990.
[37] Matt Bishop and Daniel V. Klein. Improving System Security via Proactive Password Checking. Computers & Security, 14(3):233{249, 1995.
[38] Elizabeth Ligon Bjork and Robert Bjork, editors. Memory: Handbook of Perception and Cognition. Academic Press, Inc., 1998.
[39] Burton H. Bloom. Space/Time Trade-O_s in Hash Coding with Allowable Errors. Communications of the ACM, 13(7):422{426, 1970.
[40] Mike Bond. Comments on grIDsure authentication.
http://www.cl.cam.ac.uk/~mkb23/research/GridsureComments.pdf, 2008.
[41] Mike Bond and Piotr Zieli_nski. Decimalisation table attacks for PIN cracking. Technical Report UCAM-CL-TR-560, University of Cambridge, 2003.
[42] Joseph Bonneau. Getting web authentication right: a best-case protocol for the remaining life of passwords. In 19th International Workshop on Security Protocols, 2011.
[43] Joseph Bonneau. Statistical metrics for individual password strength. In 20th Interna-tional Workshop on Security Protocols, 2012.
[44] Joseph Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In SP '12: Proceedings of the 2012 IEEE Symposium on Security and Privacy, 2012.
[45] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In SP '12: Proceedings of the 2012 IEEE Symposium on Security and Privacy, 2012.
[46] Joseph Bonneau, Mike Just, and Greg Matthews. What's in a name? Evaluating statistical attacks against personal knowledge questions. In FC '10: The 14th International Conference on Financial Cryptography and Data Security. Springer-Verlag, 2010.

[47] Joseph Bonneau and S□oren Preibusch. The password thicket: technical and market failures in human authentication on the web. In WEIS '10: Proceedings of the 9th Workshop on the Economics of Information Security, 2010.
[48] Joseph Bonneau, S□oren Preibusch, and Ross Anderson. A birthday present every eleven wallets? The security of customer-chosen banking PINs. In FC '12: The 16th Interna-tional Conference on Financial Cryptography and Data Security. Springer-Verlag, 2012.
[49] Joseph Bonneau and Ekaterina Shutova. Linguistic properties of multi-word passphrases. In USEC '12: Workshop on Usable Security, 2012.
[50] Serdar Boztas. Entropies, Guessing, and Cryptography. Technical Report 6, Department of Mathematics, Royal Melbourne Institute of Technology, 1999.
[51] John Brainard, Ari Juels, Ronald L. Rivest, Michael Szydlo, and Moti Yung. Fourth-Factor Authentication: Somebody You Know. In CCS '06: Proceedings of the 13th ACM Conference on Computer and Communications Security, pages 168{178, New York, NY, USA, 2006. ACM.
[52] Thorsten Brantz and Alex Franz. The Google Web 1T 5-gram corpus. Technical Report LDC2006T13, Linguistic Data Consortium, 2006.
[53] Peter Bright. RSA _nally comes clean: SecurID is compromised. Ars Technica, 2011.
[54] Sacha Brosto_ and Angela Sasse. \Ten strikes and you're out": Increasing the number of login attempts can improve password usability. In Proceedings of CHI 2003 Workshop on HCI and Security Systems. John Wiley, 2003.
[55] Sacha Brosto_ and M. Angela Sasse. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In People and Computers XIV: Usability or Else!: Proceedings of HCI 2000, 2000.
[56] Daniel R. L. Brown. Prompted User Retrieval of Secret Entropy: The Passmaze Protocol. Cryptology ePrint Archive, Report 2005/434, 2005. http://eprint.iacr.org/.
[57] Julie Bunnell, John Podd, Ron Henderson, Renee Napier, and James Kennedy-Mo_at. Cognitive, associative and conventional passwords: Recall and guessing rates. Computers & Security, 16(7):629{641, 1997.
[58] William E. Burr, Donna F. Dodson, and W. Timothy Polk. Electronic Authentication Guideline. NIST Special Publication 800-63, 2006.
[59] Eric Butler. Firesheep, 2011. codebutler.com/firesheep.
[60] Christian Cachin. Entropy Measures and Unconditional Security in Cryptography. PhD thesis, ETH Z□urich, 1997.
[61] John Andrew Campbell, Kay Bryant, Mary-Anne Williams Sue Williams Steve Elliot, Carol Pollard, and Carol Pollard. Password composition and Security: An Exploratory Study of User Practice. 2004.
[62] Claude Castelluccia, Markus D□urmuth, and Daniele Perito. Adaptive Password-Strength Meters from Markov Models. In NDSS '12: Proceedings of the Network and Distributed System Security Symposium, 2012.
[63] Joseph A. Cazier and B. Dawn Medlin. Password Security: An Empirical Investigation into E-Commerce Passwords and Their Crack Times. Information Systems Security, 15(6):45{55, 2006.
[64] William Cheswick. Johnny Can Obfuscate: Beyond Mother's Maiden Name. In Proceed-ings of the 1st USENIX Workshop on Hot Topics in Security, pages 31{36, Berkeley, CA, USA, 2006. USENIX Association.
[65] Sonia Chiasson, Alain Forget, Robert Biddle, and P.C. van Oorschot. Inuencing Users Towards Better Passwords: Persuasive Cued Click-Points. In BCS-HCI '08: Proceedings of the 22nd British HCI Group Annual Conference on HCI 2008, pages 121{130, Swinton, UK, 2008. British Computer Society.
[66] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P.C. van Oorschot, and Robert Biddle. Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords. In CCS '09: Proceedings of the 16th ACM Conference on Computer and Communications Security, pages 500{511, New York, NY, USA, 2009. ACM
[67] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle. A Usability Study and Critique of Two Password Managers. In Proceedings of the 15th USENIX Security Symposium, 2006.
[68] Angelo Ciaramella, Paolo D'Arco, Alfredo De Santis, Clemente Galdi, and Roberto Tagliaferri. Neural Network Techniques for Proactive Password Checking. IEEE Trans- actions on Dependable and Secure Computing, 3:327{339, 2006.
[69] Aaron Clauset, Cosma Rohilla Shalizi, and M. E. J. Newman. Power-Law Distributions in Empirical Data. SIAM Review, 51:661{703, 2009.
[70] Michael Comer. Password breaking. Computer Fraud & Security Bulletin, 4(3):7{8, 1981.
[71] Richard M. Conlan and Peter Tarasewich. Improving Interface Designs to Help Users Choose Better Passwords. In CHI '06: Extended Abstracts on Human Factors in Com- puting Systems, pages 652{657, New York, NY, USA, 2006. ACM.
[72] Microsoft Corporation. Security con_guration guidance support, 2010. http:// support.microsoft.com/kb/885409.
[73] Baris Coskun and Cormac Herley. Can \Something You Know" Be Saved? In ISC '08: Proceedings of the 11th International Conference on Information Security, pages 421{440, Berlin, Heidelberg, 2008. Springer-Verlag.
[74] Johanna Bromberg Craig, Wes Craig, Kevin McGowan, and Jarod Malestein. The Cosign Web Single Sign-On Scheme. http://cosign.sourceforge.net/media/ cosignscheme2006a.rtf, 2006.
[75] Nik Cubrilovic. The Anatomy Of The Twitter Attack. TechCrunch, July 2009.
[76] John Daugman. New Methods in Iris Recognition. IEEE Transactions on Systems, Man, and Cybernetics, Part B, 37(5):1167{1175, 2007.
[77] Chris Davies and Chris Ganesan. BApasswd: A New Proactive Password Checker. In Proceedings of the 16th National Computer Security Conference, 1993.

[78] Darren Davis, Fabian Monrose, and Michael K. Reiter. On User Choice in Graphical Password Schemes. In Proceedings of the 13th USENIX Security Symposium, 2004.
[79] A. De Santis, A.G. Gaggia, and U. Vaccaro. Bounds on Entropy in a Guessing Game. IEEE Transactions on Information Theory, 47(1):468{473, 2001.
[80] Khosrow Dehnad. A simple way of improving the login security. Computers & Security, 8:607{611, 1989.
[81] Matteo Dell'Amico, Pietro Michiardi, and Yves Roudier. Password Strength: An Empirical Analysis. In INFOCOM'10: Proceedings of the 29th Conference on Information Communications, pages 983{991. IEEE, 2010.
[82] Dorothy E. Denning. An Intrusion-Detection Model. IEEE Transactions on Software Engineering, 13(2):222{232, 1987.
[83] Dorothy E. Denning and Peter J. Denning. The Tracker: A Threat to Statistical Database Security. ACM Transactions on Database Systems, 4:76{96, 1979.
[84] Martin M.A. Devillers. Analyzing Password Strength. Technical report, Radboud University Nijmegen, 2010.
[85] Arkajit Dey and Stephen Weis. PseudoID: Enhancing Privacy for Federated Login. In HotPETS '10: Hot Topics in Privacy Enhancing Technologies, 2010.
[86] R. Dhamija and L. Dusseault. The Seven Flaws of Identity Management: Usability and Security Challenges. IEEE Security & Privacy Magazine, 6(2):24{29, 2008.
[87] Rachna Dhamija and Adrian Perrig. D_ej_a vu: A user study using images for authentication. In Proceedings of the 9th USENIX Security Symposium, Berkeley, CA, USA, 2000. USENIX Association.
[88] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why Phishing Works. In CHI '06: Proceedings of the 24th ACM SIGCHI Conference on Human Factors in Computing Systems, pages 581{590, New York, NY, USA, 2006. ACM.
[89] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) protocol, 2006. RFC 4346.
[90] Paul Dourish, E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. Personal Ubiquitous Computing, 8(6):391{401, 2004.
[91] Peter J. Downey. Multics Security Evaluation: Password and File Encryption Tech- niques. Ft. Belvoir Defense Technical Information Center, 1977.
[92] Sever S. Dragomir and Serdar Boztas. Some Estimates of the Average Number of Guesses to Determine a Random Variable. In Proceedings of the 1997 IEEE Interna- tional Symposium on Information Theory, page 159, 1997.
[93] Saar Drimer, Steven J. Murdoch, and Ross Anderson. Optimised to Fail: Card Readers for Online Banking. In FC '09: The 13th International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2009.
[94] Cynthia Dwork. Di_erential Privacy. In Automata, Languages and Programming, volume 4052, pages 1{12. Springer Berlin / Heidelberg, 2006. 10.1007/11787006 1.
[95] Bradley Efron and R. J. Tibshirani. An Introduction to the Bootstrap. Chapman and Hall/CRC, 1st edition, 1993.
[96] Serge Egelman, Joseph Bonneau, Sonia Chiasson, David Dittrich, and Stuart Schechter. Its Not Stealing If You Need It: On the ethics of performing research using public data of illicit origin (panel discussion). In WECSR '12: The 3rd Workshop on Ethics in Computer Security Research, 2012.
[97] Carl Ellison, Chris Hall, Randy Milbert, and Bruce Schneier. Protecting Secret Keys with Personal Entropy. Journal of Future Generation Computer Systems, 16(4):311{318, 2000.
[98] Laura Falk, Atul Prakash, and Kevin Borders. Analyzing Websites for User-Visible Security Design Flaws. In SOUPS '08: Proceedings of the 4th Symposium on Usable Privacy and Security, pages 117{126, New York, NY, USA, 2008. ACM.
[99] David C. Feldmeier and Philip R. Karn. UNIX Password Security|Ten Years Later. In CRYPTO '89: Proceedings of the 9th Annual International Conference on Advances in Cryptology, pages 44{63, London, UK, 1990. Springer-Verlag.

