R209 Essay: Passwords

Chongyang Shi (*cs940*)

October 31, 2017

1 Summaries of research

In 1979, Morris and Thompson [1] described the principles and implementation details of the then state-of-the-art UNIX password security scheme. Starting with the design goals of the password scheme, they highlighted the need to do away with clear text password files. A simple scheme resembling modern password hashing was then introduced, followed by possible attacks on scheme. The failure of the pseudo-random number generator was also noted. Various mitigations involving augmenting the algorithms and hardware were described. The authors concluded with a potentially pretentious note that their approach to password scheme design had been successful. This would eventually be shadowed by security challenges brought by rapidly advancing hardware capabilities in hashing and factorisation.

Adams and Sasse [2] in 1999 argued that problems with password security mechanisms are often results of their implementation and lack of user education, rather than an inherent carelessness in users. The authors started by summarising the lack of focus on human links in the technical-centred password policies, and followed up with their questionnaire and interview-based study on human factors in password security. Challenges faced by non-technical users navigating password security mechanisms, as well as reasonings behind common user circumventions were noted. The authors then made recommendations on design and practical aspects of password policies. However, observations made by the authors would have been better supported by detailed statistics from their study. Whether their recommendations effectively improve password security can be verified by experimentation and null hypothesis testing.

Bonneau et al. [3] designed an evaluation framework for web authentication schemes, and applied it on a wide range of authentication schemes under several categories, including password managers, graphical and cognitive-based systems, paper and hardware tokens, and biometric systems. Three categories of properties were tested: usability, deployability, and security; which were in turn designed largely based on the strengths and weaknesses of conventional passwords. Justifications were made on design choices of the evaluation framework, whose limitations were also noted. While most schemes have advantages in some properties, their disadvantages in other properties ultimately result in no scheme performing as well as conventional passwords. This motivates further research in devising better authentication schemes.

2 Key themes of research

2.1 Provide the user with adequate security feedback

A highlighted principle in human factors associated with password security is the need to provide users with adequate feedback on their practices, and if improvements are required, with explicit instructions. Morris and Thompson [1, p. 596] noted the need to urge the user to use a more obscure password if their choice is deemed to be too simple, which in modern systems are enforced with minimal password complexity rules. Adams and Sasse [2, p. 6] further noted that reasons why a chosen password is too simple should be explained to the user to refresh their password knowledge. The evaluation framework by Bonneau et al. [3, Sec. II] also included an *Easy-to-Learn* property which can involve feedback to the user.

2.2 Protecting security mechanisms is detrimental to security

All three papers emphasised the need to avoid utilising security-through-obscurity when designing authentication systems, for different reasons. Morris and Thompson [1, p. 594, p.597] described the potential problems of relying on hiding away the password file, as well as the advantages in them publicising their password algorithm designs. Adams and Sasse [2, p. 4] noted that telling users as little as possible about security mechanisms increase their chance of unknowingly choosing weak passwords. An important component of authentication scheme evaluation by Bonneau et al. [3, Sec. IV] is whether a scheme uses proprietary design and implementation, which in turn affect external confidence in its security.

2.3 Lack of user awareness results in security problems

A common theme observed is the user's lack of awareness when dealing with security, an issue being addressed in various ways. Combing through cleartext user passwords, Morris and Thompson [1, p. 596] found that a majority of user-selected passwords were in someway weakened and vulnerable to attack. Adams and Sasse [2, p. 3] observed that as users are unaware of how password cracking works, they may consciously choose a dictionary password, believing that the word they chose could not be easily guessed. It was also noted by Bonneau et al. [3, Sec. V] that when users are unaware of the complementary nature of factors in a two-factor authentication, they may lower their guard and weaken one of the factors, which in turn weaken the whole authentication process.

3 Ideas of current context

As mentioned earlier, many features described as secure by Morris and Thompson [1] are no longer secure under modern computing power and special-purpose hardware. The minimum secure length of six characters is no longer considered sufficient under brute force attacks [4]. While Morris and Thompson evaluated password quality based on length and letter-number composition, more generalised methods to measure password quality have been developed,

such as by Ma et al. [5]. DES is also no longer considered as secure under modern cryptanalysis, which could efficiently attack DES on parallel processing units [6]. It was replaced by the newer AES in 2001 [7].

Despite advancing hardware, security vulnerabilities caused by a cryptographically-insecure pseudo-random number generator (PRNG) as noted by Morris and Thompson [1, p. 596] is still prevalent today, often due to implementation errors which expose seed generation or internal states. Cryptanalysis examples include attacks on the Mersenne Twister PRNG [8] and the recent attack on WPA2 wireless access points [9] with improperly implemented PRNG. Ensuring the cryptographic security of PRNGs is an active area of research.

Adams and Sasse [2] argued that requiring users to change password regularly is detrimental to good security practices. The idea that users are more likely to sequence or write down expiring passwords, and thus impairing security is well accepted in current research [10, 11]. As external conditions often require password expiration to be implemented, compromises such as strength-based password expiration [12] have been suggested.

4 Literature review

Morris and Thompson [1, p. 596] observed that a vast majority of user passwords fall into a category that is easy to crack with brute force or dictionary-based attacks. Klein [13] further studied dictionary-based attacks on a larger sample of passwords, and found that 24.2% of passwords studied could be cracked with a simple dictionary. Wu [14] later demonstrated that even if a password system (such as Kerberos) measures the strength of a user-selected password and rejects perceived-weak ones, passwords vulnerable to dictionary-based attacks can still slip through. The inherent limitations of the password security mechanism proposed by Morris and Thompson were examined by Feldmeier and Karn [15].

Yan et al. [16] studied the effects of giving users different kinds of password advice, and gave statistically-backed recommendations. Dhamija and Perrig [17, Sec. 5] disagreed with Adams and Sasse [2] on whether user training improves the security of passwords selected by users. Their user study showed that as users often prefer convenience over security, more training will likely not help. They in turn proposed to replace password authentication with a graphical method. However, evaluation by Bonneau et al. [3, Sec. IV, D] showed that graphical methods may not hold an advantage over passwords.

While Bonneau et al. [3] demonstrated the general advantage of conventional password over its proposed replacements, its key weaknesses in security were further studied by Das et al. [18] to demonstrate the prevalence of password reuses and potential consequences. This emphasises the need for an ultimate solution to replace conventional passwords. The same three-category evaluation framework was used by Clark and Van Oorschot [19] to evaluate TLS security enhancements. Schaub et al. [20] proposed that implementing graphical authentication on smartphones could better address the shortcomings pointed out by Bonneau et al., and that graphical authentication may encourage users to enable a level of device security when they would otherwise have none.

(1232 words according to texcount.)

References

[1] R. Morris and K. Thompson, "Password security: A case history," *Communications of the ACM*, vol. 22, no. 11, pp. 594–597, 1979.

[2] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[3] J. Bonneau *et al.*, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Security and Privacy (SP), 2012 IEEE Symposium on*. IEEE, 2012, pp. 553–567.

[4] M. Weir *et al.*, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010, pp. 162–175.

[5] W. Ma *et al.*, "Password entropy and password quality," in *Network and System Security (NSS), 2010 4th International Conference on*. IEEE, 2010, pp. 583–587.

[6] E. Biham and A. Shamir, "Differential cryptanalysis of the full 16-round des," in *Differential Cryptanalysis of the Data Encryption Standard*. Springer, 1993, pp. 79–88.

[7] N.-F. Standard, "Announcing the advanced encryption standard (aes)," *Federal Information Processing Standards Publication*, vol. 197, pp. 1–51, 2001.

[8] G. Argyros and A. Kiayias, "I forgot your password: Randomness attacks against php applications." in *USENIX Security Symposium*, 2012, pp. 81–96.

[9] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in wpa2," 2017.

[10] Y. Zhang *et al.*, "The security of modern password expiration: An algorithmic framework and empirical analysis," in *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010, pp. 176–186.

[11] S. Chiasson and P. C. Van Oorschot, "Quantifying the security advantage of password expiration policies," *Designs, Codes and Cryptography*, vol. 77, no. 2-3, pp. 401–408, 2015.

[12] J. M. Johansson *et al.*, "Strength-based password expiration," Nov. 3 2015, uS Patent 9,178,876.

[13] D. V. Klein, "Foiling the cracker: A survey of, and improvements to, password security," in *Proceedings of the 2nd USENIX Security Workshop*, 1990, pp. 5–14.

[14] T. D. Wu, "A real-world analysis of kerberos password security." in *NDSS*, 1999.

[15] D. C. Feldmeier and P. R. Karn, "Unix password security-ten years later," in *Conference on the Theory and Application of Cryptology*. Springer, 1989, pp. 44–63.

[16] J. Yan *et al.*, "Password memorability and security: Empirical results," *IEEE Security & privacy*, vol. 2, no. 5, pp. 25–31, 2004.

[17] R. Dhamija and A. Perrig, "Deja vu-a user study: Using images for authentication." in *USENIX Security Symposium*, vol. 9, 2000, pp. 4–4.

[18] A. Das *et al.*, "The tangled web of password reuse." in *NDSS*, vol. 14, 2014, pp. 23–26.

[19] J. Clark and P. C. van Oorschot, "Sok: Ssl and https: Revisiting past challenges and evaluating certificate trust model enhancements," in *Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE, 2013, pp. 511–525.

[20] F. Schaub *et al.*, "Exploring the design space of graphical passwords on smartphones," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 2013, p. 11.