Strengthening Password-based Authentication

Scott Ruoti
Brigham Young University
ruoti@isrl.byu.edu

Jeff Andersen
Brigham Young University
andersen@isrl.byu.edu

Kent Seamons
Brigham Young University
seamons@cs.byu.edu

1. INTRODUCTION

Even with years of research into new authentication technologies, passwords still dominate the authentication landscape. This is due primarily to a combination of security, deployability, and usability that has been difficult to match [2]. While password alternatives exist, their lack of widespread adoption indicates that for the foreseeable future passwords are here to stay [11].

Our research goal is to strengthen, not replace, password-based authentication. We focus on two serious problems with password-based authentication. First, poor security practices at the web servers leads to stolen password files that are easily compromised using an offline attack. Second, passwords are too easily stolen via phishing attacks.

Both of these problems arise because for the vast majority of authentication flows, servers require users to provide their plaintext passwords. In the case of a legitimate server receiving this password, the user must blindly trust that the server correctly salts and hashes the password. Experience, though, has shown that many websites do not follow proper password storage [5, 9, 1]. Moreover, there is a disconnect between perceived best practices for password storage and actual best practices [9].

Even if websites were to safely store users' passwords, users would still be at risk to phishing attacks. Phishers impersonate legitimate websites in order to trick users into sending their authentication credentials to the phishing website. The problem of phishing is only compounded by password reuse, allowing a single stolen password to potentially compromise many of the user's sites.

In this paper, we describe two methods for strengthening existing password-based authentication: strong password protocols and safe password entry.

2. STRONG PASSWORD PROTOCOLS

Strong password protocols are cryptographic zero-knowledge proofs that allow the user to demonstrate knowledge of their password without actually revealing that password. There are many benefits to strong password protocols. First, the user never sends the website their plaintext password, including at account registration. Instead, users only present a password verifier, which is stronger than a salted and hashed password. Second, in addition to authenticating the user to the website, strong password protocols authenticate the website to the user. Third, a phisher learns nothing about the user's password. Finally, strong passwords protocols do not require a secure connection and are safe from brute-force attacks by an active network attacker.

The adoption of strong password protocols has been stymied by patents. These patents are beginning to expire, and we believe the time may be ripe to reconsider them.

The most efficient strong password protocol is the Secure Remote Password protocol (SRP) [15]. In our research, we have proved the security of SRP in the random oracle model. Further, we have created a three-party, gateway-oriented [3] variant of SRP, that would allow it to be used in password-based OAuth. We believe SRP is an ideal strong password protocol, and our intention is to open source our implementation of SRP to benefit other researchers who are interested in exploring this area.

3. SAFE PASSWORD ENTRY

Strong password protocols alone are insufficient to address phishing attacks because phishers will simply sidestep these protocols. To succeed, strong password protocols must be coupled with spoof-resilient password-entry interfaces where users can safely enter their passwords. Although prior research has explored this problem (PwdHash [12], Password Multiplier [10], Dynamic Security Skins [6]), there is still no optimal solution [4]. Our work seeks to build upon previous research and is based on the principle that users should never enter passwords into untrusted web pages, but should migrate to browser or operating system interfaces for password entry.

We intend to explore the usability and security trade-offs of the following options for deploying safe password entry interfaces.

- *As a trusted web component.* The browser could provide a trusted web component (e.g., `<srp />`), that websites would be required to use in place of password fields. Still, special care would need to be taken to ensure that users could correctly identify legitimate interfaces (i.e., anti-phishing markers).

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22–24, 2016, Denver, Colorado.

- *In the browser's chrome.* Interfaces in the browser's chrome are inaccessible to phishers. Still there is a risk that the phisher could try to create interfaces on their website that appear to be popdowns from the browser's chrome.
- *As an operating system dialog.* This approach would allow for a single safe password entry interface for all applications. Additionally, it could leverage OS-specific protections. Still, research has shown that OS dialogs can be susceptible to phishing.

In the workshop, we are interested in further discussing the benefits and risks of each approach.

4. EVALUATION

Safe password entry solutions will need to be evaluated empirically to ensure that they help protect users from phishing. While there have been previous studies of anti-phishing tools, these studies have all had important limitations: (1) The studies explicitly draw users' attention to the fact that they are trying to detecting phishing, automatically elevating user awareness [8]. (2) The studies are lab-based, making it difficult to know how well solutions work in practice [14]. (3) The studies are short-term, making it difficult to know if habituation will decrease future performance [13].

Our goal is to create a study that addresses each of these limitations. The three key features of our planned study are: (1) we will deceive users, having them install a system and assigning them tasks that are orthogonal to the study's true purposes, while simultaneously trying to phish their passwords; (2) we will require users to complete tasks from their own computers, according to their own schedules; and (3) we will test users' resilience to phishing over the course of several weeks.

As a first step, we intend to use our methodology to study Dynamic Security Skins (DSS) [7]. While it has been a decade since DSS was published, it has never been evaluated with a user study. We hope that by studying DSS we can better understand how safe password entry can be designed. Based on the results of this preliminary study, we intend to implement several prototypes for safe password entry. We will then refine these prototypes using an iterative design paradigm, where we conduct a usability study of the prototype and then address issues that arose during the study. We will continue this process until we have a prototype that successfully protects users from password phishing.

In the workshop, we are interested in discussing the study design, especially in crafting a scenario that supports phishing users' passwords in a natural fashion. A significant challenge is how to balance the goal of a real-world setting with the need to limit the harm to users if the study is to involve actual accounts and passwords.

5. CONCLUSION

In this paper, we have described our vision for augmenting password-based authentication: strong password protocols coupled with safe password entry. Through the combination of these techniques, users' passwords will become resilient to negligent websites and phishers. In order to assure that we have a suitable methodology for evaluating safe password entry, we plan to run usability studies that attempt to phish users' credentials in a natural setting. We hope to discuss both safe password entry and its associated study methodology at the workshop. Additionally, we are interested in discussing how users might be protected during the transition to SRP and safe password entry; specifically, how to protect users from downgrade attacks when SRP and safe password entry are first beginning to be adopted.

6. REFERENCES

[1] Plain text offenders. `http://plaintextoffenders.com/`. Accessed 2016/05/16.

[2] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Symposium on Security and Privacy (SP)*. IEEE, 2012.

[3] J. W. Byun, D. H. Lee, and J. I. Lim. Security analysis and improvement of a gateway-oriented password-based authenticated key exchange protocol. *Communications Letters, IEEE*, 10(9), 2006.

[4] S. Chiasson, P. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In *15th USENIX Security Symposium*, 2006.

[5] N. Cubrilovic. Rockyou hack: From bad to worse. `http://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/`. Accessed 2016/05/16.

[6] R. Dhamija and J. Tygar. The battle against phishing: Dynamic security skins. In *ACM International Conference Proceeding Series*, volume 93, 2005.

[7] R. Dhamija and J. D. Tygar. The Battle Against Phishing : Dynamic Security Skins. *Symposium on Usable Privacy and Security (SOUPS)*, 2005.

[8] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2006. ACM.

[9] D. Florêncio, C. Herley, and P. C. Van Oorschot. An administrator's guide to internet password research. In *28th Large Installation System Administration Conference (LISA14)*, 2014.

[10] J. Halderman, B. Waters, and E. Felten. A convenient method for securely managing passwords. In *Proceedings of the 14th international conference on World Wide Web*. ACM, 2005.

[11] C. Herley and P. Van Oorschot. A research agenda acknowledging the persistence of passwords. *IEEE Security & Privacy*, 10(1), 2012.

[12] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. Mitchell. Stronger password authentication using browser extensions. In *Proceedings of the 14th Usenix Security Symposium*, volume 5, 2005.

[13] S. Schechter and J. Bonneau. Learning Assigned Secrets for Unlocking Mobile Devices. 2015.

[14] M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? *CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2006.

[15] T. Wu. The Secure Remote Password Protocol. *Proceedings of the Symposium on Network and Distributed Systems Security NDSS 98*, 1998.