Evaluation of resources

Lucian James

April 20, 2022

Name	Evaluation	Cited?
The Secure Remote Password Protocol [16]	Provided me with the information I needed to detail how the secure remote password protocol worked. There were some aspects I did not like about this paper though, such as the confusing use of some symbols (some symbols were used to represent two things at once!), and the use of names to represent the client and the server. I changed these things when I wrote about how the SRP protocol works.	yes
Addressing misconceptions about password security effectively [9]	Contained lots of helpful information about the misconceptions users have which may lead to vulnerabilities. This work also concluded that these misconceptions can be addressed by training, which meant i could say training can be an effective mitigation.	yes
Let's go in for a closer look: Observing passwords in their natural habitat [10]	Provided me with incredibly useful data about real-world passwords which i used in my dataset analysis, this real-world data allowed me to make some comparison between the password dictionaries i had collected, and reliable data about real-world passwords.	yes
PPP Challenge Handshake Authentication Protocol (CHAP) [13]	Provided me with the information i needed about CHAP, although i did expand my explanation of the steps of the protocol a bit.	yes
PPP Authentication Protocols [12]	Provided me with the information i needed about PAP, i didnt need to use the majority of the information on this RFC, all i quoted was a part of a section.	yes
OPAQUE: an asymmetric PAKE protocol secure against pre-computation attacks [7]	was too technical for me to utilise properly, relied mostly on [5] for OPAQUE stuff, but its good to cite the original paper too.	yes
Let's talk about PAKE [5]	Was incredibly useful for my section on PAKE, it did have some issues such as a lack of exact detailing of why salts are protected using OPAQUE (i had to figure this out for myself, had to research discrete log problem a bit).	yes
Math in network security: A crash course [4]	used as a source to quickly learn about the discrete log problem, which i needed to describe salt secrecy in OPAQUE	yes
Twitter advises all users to change passwords after glitch exposed some in plain text [1]	Was a good source on twitter accidentally storing passwords in plaintext.	yes
Facebook admits it stored 'hundreds of millions' of account passwords in plaintext [14]	Was a good source on facebook accidentally storing a lot of passwords in plaintext.	yes
Phishing environments, techniques, and countermeasures: A survey [2]	Provided me with good quality information about phishing, and countermeasures that can be put in place to help the prevention of phishing attacks.	yes
Honeywords: Making password-cracking detectable [8]	Provided me with good quality information about the use of honeypot accounts and "honeywords" to create alerts upon the use of stolen password data.	yes
Is this really you? An empirical study on risk-based authentication applied in the wild [15]	This paper presents some interesting information about "risk-based authentication", but in the end i decided not to include it as it isnt very directly linked to password authentication specifically	no
Password managers: Attacks and defenses [11]	No issues with the quality of this source, but i didnt feel like including password managers in my report as i feel they are often adding an additional authentication factor	no
New directions in cryptography [3]	A technical paper about cryptography, not really relevant enough for me to include in my final report. I think i included it in my bibliography originally because i went on a bit of a tangent looking at all kinds of cryptography at one point, but i realised i was stepping pretty far from my original plans as well as going too deep into mathematics i dont understand	no
Password authenticated key exchange by juggling [6]	Paper about a PAKE protocol, didnt use this because i found [5] which i found to be easier for me to understand.	no

References

[1] Abrar Al-Heeti. Twitter advises all users to change passwords after glitch exposed some in plain text, May 2018.

[2] Ahmed Aleroud and Lina Zhou. Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, 68:160–196, 2017.

[3] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[4] Changyu Dong. Math in network security: A crash course, 2016.

[5] Matthew Green. Let's talk about pake, Oct 2018.

[6] Feng Hao and Peter YA Ryan. Password authenticated key exchange by juggling. In *International Workshop on Security Protocols*, pages 159–171. Springer, 2008.

[7] Stanislaw Jarecki, Hugo Krawczyk, and Jiayu Xu. Opaque: an asymmetric pake protocol secure against pre-computation attacks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 456–486. Springer, 2018.

[8] Ari Juels and Ronald L Rivest. Honeywords: Making password-cracking detectable. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 145–160, 2013.

[9] Peter Mayer and Melanie Volkamer. Addressing misconceptions about password security effectively. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, pages 16–27, 2018.

[10] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. Let's go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 295–310, 2017.

[11] David Silver, Suman Jana, Dan Boneh, Eric Chen, and Collin Jackson. Password managers: Attacks and defenses. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, pages 449–464, 2014.

[12] William Allen Simpson. Ppp authentication protocols, Oct 1992.

[13] William Allen Simpson. Ppp challenge handshake authentication protocol (chap), Aug 1996.

[14] Zack Whittaker. Facebook admits it stored 'hundreds of millions' of account passwords in plaintext, Mar 2019.

[15] Stephan Wiefling, Luigi Lo Iacono, and Markus Dürmuth. Is this really you? an empirical study on risk-based authentication applied in the wild. In *IFIP International Conference on ICT Systems Security and Privacy Protection*, pages 134–148. Springer, 2019.

[16] Thomas D Wu et al. The secure remote password protocol. In *NDSS*, volume 98, pages 97–111. Citeseer, 1998.