Analysis of the Secure Remote Password Protocol Using CPSA

Erin Lanus,[1] Alan T. Sherman, Moses Liskov,[2] Edward Zieglar,[3]
Richard Chang, Enis Golaszewski, Ryan Wnuk-Fink, Cyrus Jian Bonyadi,
Mario Yaksetig, Ian Blumenfeld[4]
Cyber Defense Lab
Department of Computer Science and Electrical Engineering
University of Maryland, Baltimore County (UMBC)
Baltimore, MD 21250 USA
email: lanus@vt.edu, sherman@umbc.edu

March 23, 2020

Abstract

We analyze the *Secure Remote Password (SRP)* protocol for structural weaknesses using the *Cryptographic Protocol Shapes Analyzer (CPSA)* in the first formal analysis of SRP (specifically, Version 3).

SRP is a widely deployed *Password Authenticated Key Exchange (PAKE)* protocol used in 1Password, iCloud Keychain, and other products. As with many PAKE protocols, two participants use knowledge of a pre-shared password to authenticate each other and establish a session key. SRP aims to resist dictionary attacks, not store plaintext-equivalent passwords on the server, avoid patent infringement, and avoid export controls by not using encryption. Formal analysis of SRP is challenging in part because existing tools provide no simple way to reason about its use of the mathematical expression "$v + g^b \mod q$".

Modeling $v + g^b$ as encryption, we complete an exhaustive study of all possible execution sequences of SRP. Ignoring possible algebraic attacks, this analysis detects no major structural weakness, and in particular no leakage of any secrets. We do uncover one notable weakness of SRP, which follows from its design constraints. It is possible for a malicious server to fake an authentication session with a client, without the client's participation. This action might facilitate an escalation of privilege attack, if the client has higher privileges than does the server. We conceived of this attack before we used CPSA and confirmed it by generating corresponding execution shapes using CPSA.

Keywords. Cryptographic protocols, cryptography, Cryptographic Protocol Shapes Analyzer (CPSA), cybersecurity, formal methods, Password Authenticated Key Exchange (PAKE) protocols, protocol analysis, Secure Remote Protocol (SRP), UMBC Protocol Analysis Lab (PAL).

[1] Now with Intelligent Systems Lab, Hume Center, Virginia Tech, Arlington, VA 22309.

[2] The MITRE Corporation, Burlington, MA 01720.

[3] National Security Agency, Fort George G. Meade, MD 20755.

[4] Two Six Labs, Arlington, VA 22203.

Acknowledgments

Thanks to John Ramsdell (MITRE) and other participants at the Protocol eXchange for fruitful interactions.

This research was supported in part by the U.S. Department of Defense under CySP Capacity grants H98230-17-1-0387 and H98230-18-1-0321. Sherman, Golaszewski, Wnuk-Fink, Bonyadi, and the UMBC Cyber Defense Lab were supported also in part by the National Science Foundation under SFS grant DGE-1753681.

See Sherman, et al. [SLL$^+$20] for our full paper, and see Wu [Wu98, Wu00, Wu02] for a description of SRP.

References

[SLL$^+$20] Alan T. Sherman, Erin Lanus, Moses Liskov, Edward Zieglar, Richard Chang, Enis Golaszewski, Ryan Wnuk-Fink, Cyrus Jian Bonyadi, Mario Yaksetig, and Ian Blumenfeld. Formal methods analysis of the secure remote password protocol, February 2020. Submitted to Springer LNCS for Andre Scedrov's Festschrift. Available as `https://arxiv.org/pdf/2003.07421.pdf`.

[Wu98] Thomas Wu. The Secure Remote Password Protocol. In *Proceedings of the Internet Society on Network and Distributed System Security*, 1998.

[Wu00] Thomas Wu. The SRP Authentication and Key Exchange System, RFC 2945, September 2000.

[Wu02] Thomas Wu. SRP-6: Improvements and Refinements to the Secure Remote Password Protocol, October 2002.