Cybersecurity – Identity Management
Prof. Dr. Anja Lehmann

Master Project | Winter Term 24/25

Asymmetric Password Authenticated Key Exchange: Better Models and Proofs

Description

Passwords are the most common form of user authentication on the Internet. In the traditional "password-over-TLS" method, a user sends her password to the server over a secure TLS channel, where it is verified against a stored password hash, created during user registration. While the passwords at rest are (somewhat) protected through hashing, the server learns the plaintext passwords during every login. This is a significant concern, as it requires a lot of trust in the server to handle these passwords securely, which has not always been reliably ensured in the past. Even major companies such as Twitter or Github have inadvertently mishandled these plaintext passwords in the past [1].

Asymmetric Password Authenticated Key Exchange (aPAKE) [2] offers a more secure alternative for password-based user authentication. Therein, a client and a server engage in a protocol to establish a strong key derived from the password. This key provides mutual authentication: If a party derives a key (which later protects the secure session), the other party must have used the correct password. Unlike "password-over-TLS", the server does not see the password in clear, and the messages exchanged within this aPAKE protocol leak no information that can be exploited in offline attacks by the server or any network eavesdropper. Preventing offline attacks is crucial for password-based schemes, as passwords typically have low-entropy and can be guessed by an attacker with non-negligible probability as soon as it gets information to verify it's guesses. Furthermore, aPAKE also ensures that passwords at rest are protected through password hashing.

The security guarantees of aPAKE have been formalized within two different frameworks: simulation-based security [3] and game-based security [4]. Simulation-based security is the de-facto gold standard for aPAKE, as it makes no assumption on the distribution of passwords. However, proofs within this framework often depend on idealized and/or non-standard assumptions.

Meanwhile, game-based definitions, which are usually easier to understand, are rarely used for aPAKE security proofs due to some inherent modeling challenges. Nevertheless, the game-based model offers the potential for proofs based on more standard assumptions as it does not need to use advanced proof techniques in order to extract information from adversarial messages (which is necessary in the simulation-based model).

Goals

Several aPAKEs have been proven secure within the simulation-based framework, relying on idealized or non-standard assumptions. A prominent example is the proof for the Secure Remote Password protocol (SRP-6a) [5]. SRP-6a is the most widely deployed aPAKE protocol, used by companies such as Apple, Telegram or 1Password. Although invented in

1998, it did not have a security proof until recently but this proof in the simulation-based framework relied on non-standard assumptions. Two other recent aPAKE protocols, KHAPE [6] and OKAPE [7], both designed for their efficiency, have been shown secure in the simulation-based framework. However, their proofs also relied heavily on exploiting properties of idealized assumptions such as the random oracle model and the ideal cipher model.

The goal of the master project is to prove one of these protocols secure in a game-based security framework, ideally using less idealized/non-standard assumptions. To achieve this, we will first analyze the existing game-based aPAKE security model of [4] and evaluate its security guarantees. We will address gaps in the existing security definition, such as the assumption that the server always stores user password *hashes*, whereas in general aPAKE, the server might store passwords in different formats. After refining the game-based definition, we will select one of the mentioned protocols and show its security using our refined model. Ultimately, the goal of the project is to produce a research paper suitable for publication at a cryptographic conference.

Requirements

We expect a solid understanding and interest in cryptography in general, and provable security in particular. You should have attended one of the lectures from our chair (or similar) and ideally passed with very good grades.

Contact

You're welcome to visit us in H-1.11/12 (main building first floor), or send us an email:
Dennis Dayanikli dennis.dayanikli@hpi.de
Cavit Özbay cavit.oezbay@hpi.de
Anja Lehmann anja.lehmann@hpi.de

References

[1] https://www.bleepingcomputer.com/news/security/twitter-admits-recording-plaintext-passwords-in-internal-logs-just-like-github/

[2] Bellovin, S. M., & Merritt, M. (1992). Encrypted key exchange: Password-based protocols secure against dictionary attacks. ACM CCS 1993

[3] Gentry, C., MacKenzie, P., & Ramzan, Z. (2006, August). A method for making password-based key exchange resilient to server compromise. CRYPTO 2006

[4] Benhamouda, F., & Pointcheval, D. (2013). Verifier-based password-authenticated key exchange: New models and constructions. Cryptology ePrint Archive.

[5] Dayanikli, D., & Lehmann, A. (2023). Provable security analysis of the secure remote password protocol. CSF 2024

[6] Gu, Y., Jarecki, S., & Krawczyk, H. (2021). KHAPE: asymmetric PAKE from key-hiding key exchange. CRYPTO 2021

[7] Dos Santos, B. F., Gu, Y., Jarecki, S., & Krawczyk, H. (2022, May). Asymmetric PAKE with low computation and communication. EUROCRYPT 2022