Cryptology ePrint Archive: Report 2013/127

Oblivious PAKE and Efficient Handling of Password Trials

Franziskus Kiefer and Mark Manulis

Abstract: An often neglected problem for potential practical adoption of Password-based Authenticated Key Exchange (PAKE) protocols on the Internet is the handling of failed password trials. Unlike the currently used approach, where a server-authenticated TLS channel (involving constant number of public key-based operations on both sides) is set up once and can then be used by the client to try a limited number of passwords essentially for free, any new password trial using PAKE would result in the repetition of the entire protocol. With existing PAKE protocols, the minimum number of public key-based operations on both sides is thus lower-bounded by $O(n)$, where n is the number of trials. This bound is optimal for the client (that tries n passwords in the worst case) but is clearly not optimal for the server, which uses the same reference password of the client in each trial. This paper presents a secure and practical approach for achieving the lower bound of $O(1)$ public key operations on the server side.

To this end, we introduce Oblivious PAKE (O-PAKE), a general compiler for a large class of PAKE protocols, allowing a client that shares one password with a server to use a set of passwords within one PAKE session, which succeeds if and only if one of those input passwords matches the one stored on the server side. The term ``oblivious'' is used to emphasize that no information about non-matching passwords input by the client is made available to the server, which contrasts for instance to the aforementioned TLS-based approach, where any tried password is disclosed to the server. The $O(1)$ bound on the server side is obtained in our O-PAKE compiler using special processing techniques for the messages of the input PAKE protocol. We prove security of the O-PAKE compiler under standard assumptions using the latest variant of the popular game-based PAKE model by Bellare, Rogaway, and Pointcheval (Eurocrypt 2000). We identify the requirements that PAKE protocols must satisfy in order to suit the compiler and give two concrete O-PAKE protocols based on existing PAKE schemes. Both protocols are implemented and the analysis of their performance attests to the practicality of the compiler.

The use of O-PAKE further eliminates another practical problem with password-based authentication on the Web in that users no longer need to remember the actual association between their frequently used passwords and corresponding servers and can try several of them in one execution without revealing the entire set to the server.

Category / Keywords: cryptographic protocols / Password Based Authenticated Key Exchange

Publication Info: Not published yet

Date: received 1 Mar 2013, last revised 4 Mar 2013

Contact author: f kiefer at surrey ac uk

Available formats: PDF | BibTeX Citation

Version: 20130305:125136 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]