Title: One-time password based on hash chain without shared secret and re-registration

Author: Chang-Seop Park

PII: S0167-4048(18)30139-1
DOI: https://doi.org/10.1016/j.cose.2018.02.010
Reference: COSE 1295

To appear in: *Computers & Security*

Received date: 3-9-2017
Revised date: 5-2-2018
Accepted date: 19-2-2018

Please cite this article as: Chang-Seop Park, One-time password based on hash chain without shared secret and re-registration, *Computers & Security* (2018), https://doi.org/10.1016/j.cose.2018.02.010.

One-Time Password based on Hash Chain without Shared Secret and Re-Registration

Chang-Seop Park
Department of Software, Dankook University
152, Jukjeon, Suji, Yongin, 16890, Republic of Korea
csp0@dankook.ac.kr

Chang-Seop Park has been with the Department of Software at Dankook University since 1990. He has a Ph.D. and a M.Sc from Lehigh University (1990 and 1987), as well as a B.A. from Yonsei University (1983). He has been working on the wireless mobile network security during the last 10 years. His research interests include network security, cryptographic protocols, and coding theory.

Abstract

Lamport's one-time password (OTP) was originally proposed to address the weaknesses of a simple password system. However, it has been widely used to design key management and authentication mechanisms. OTP is based on a hash chain constructed using only the cryptographic hash function, in which the hash chain is a main engine for OTP generation. Thus, the structural property of the hash chain determines the advantages and disadvantages of the OTP system that employs it. A main weakness of *Lamport*'s OTP is that the length of the hash chain is finite, meaning that OTP generation is also finite. In this paper, a new hash chain is designed and constructed for infinite OTP generation without a pre-shared secret between two parties (prover and verifier). Instead of a single long hash chain as in *Lamport*'s OTP, the hash chain in the proposed OTP consists of multiple short hash chains. This paper shows that the proposed OTP addresses the weaknesses of *Lamport*'s OTP while preserving its advantages.

Keywords: Lamport; One-Time Password; Cryptographic Hash Chain; Authentication; Registration; Shared Key

1. Introduction

Lamport's one-time password (OTP) based on a hash chain [1] was proposed essentially to address three security weaknesses of a simple password system: a fixed password, the low entropy of the password, and the proactive sharing of the prover's password with the verifier. In particular, the concept of a hash chain, which is a crucial cryptographic primitive, has been widely used to design key management and authentication mechanisms. Three standard OTP systems exist for real-world applications: hash-chain-based OTP (HOTP) [2], counter-based OTP (COTP) [3], and time-based OTP (TOTP) [4]. The HOTP is a standard adapted from *Lamport*'s OTP for use at the user level. Here, an output from the hash function is converted into a word consisting of a few characters.

The aforementioned OTP systems each have advantages and disadvantages. For the purpose of comparison, *Lamport*'s OTP is compared with the COTP and TOTP because it is more general in concept than the HOTP. First, both the COTP and TOTP require the prover to share a secret with the verifier in advance, whereas no shared secret is required for *Lamport*'s OTP. Thus, *Lamport*'s OTP is robust under an adversarial model such as a server (verifier) compromise attack. Second, if the OTP indices (time, counter, or hash index) on both the prover and verifier are out of synchronization, a compensation process should be conducted to synchronize them. In the case of COTP and *Lamport*'s OTP, the synchronization can be conducted on the fly during prover authentication. However, an out-of-band method for synchronization is required for the TOTP. Third, *Lamport*'s OTP has a weakness in that a new hash chain must be generated and re-registered with the verifier which eventually reduces the usability of *Lamport*'s OTP. Because of its weakness, in many countries including South