November 20, 2018

A METHOD FOR PASSWORD RECOVERY USING A QUORUM OF COMPANION DEVICES

HP INC

A Method for Password Recovery Using a Quorum of Companion Devices.

Abstract: A threshold-signature-based password recovery technique uses a quorum of user devices to recover a password of the user more securely than prior techniques.

This disclosure relates to the field of computer security.

A technique is disclosed for a threshold-signature-based password recovery method generated by a quorum of user devices to recover a password for the user. The user neither needs to choose a weak recovery mechanism nor remember any secrets.

The security of various accounts and services utilized by users relies on the authentication mechanism used by the service to authenticate users. Even though the main login system used by many online services is secure, the "forgotten your password" technique faces both security and usability issues. The password recovery mechanism often relies either on answers to recovery questions that are easily obtainable, and/or relies on unsecured email to deliver a reset URL or temporary password, both of which are security concerns. In addition, users often also forget the answers to their recovery questions, leaving them unable to recover their accounts.

Text message or phone call based recovery mechanisms rely on the user having their phone available and being within their coverage area. Moreover, text messages may be lost or delayed in transit and in any case are not considered secure. Popular two-factor authentication schemes utilize a hardware or software token that produces a randomly changing value. However, users have to carry their one-time-pads with them for account recovery, and an attacker can initiate the account recovery process if they get access to the token.

According to the present disclosure, and as understood with reference to the Figure, a threshold signature-based authentication scheme uses extant devices, including those in possession of the user and in the vicinity, to help the user recover their user account password. The technique may be implemented using Shoup's Practical Threshold Signatures scheme or other threshold signature schemes.

A user 10 owns a user account. Devices 20 closely associated with the user or related contextual information (e.g. location), and capable of storing data, performing basic computation, and communicating cryptographic values, serve as shareholders. These devices may include, for example, a mobile phone, laptop, smart watch, or health monitor. A dealer 30 serves as a credential manager and is responsible for creating a key for the user and distributing shares of this key to the participating devices 20. The dealer 30 establishes cryptographic material to create secure authenticated channels with the devices 20 to facilitate secure distribution of the data. Finally, the dealer 30 registers the public key with a verifier 40, an authentication service to establish the identity of the user 10 for the purpose of password recovery. The verifier 40 performs signature-based authentication to verify the purported identity of the user 10 at the time of password recovery. The dealer 30 can be located on any device trusted to receive user secret shares such as a laptop, smartphone, or other personal device.

At the time of password recovery, the dealer 30 creates a group signature by combining the partial signature shares that it receives from the participating devices 20. It then submits the group signature to the verifier 40 to authenticate the user 10.

The protocol has three phases: setup, password recovery and update.

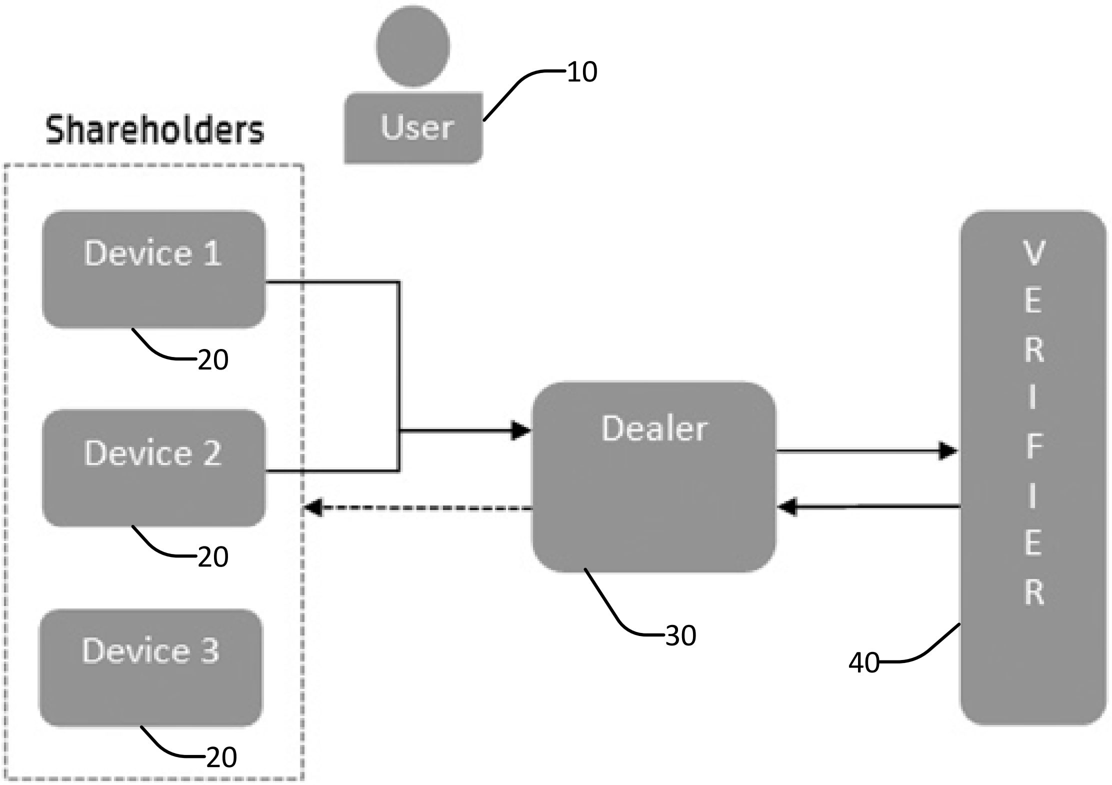
The setup phase is responsible for creating a key for the user 10, registering it with the user’s personal devices 20, and submitting the public key to the verifier 40 for association with the user’s account.

The password recovery phase is initiated by the user 10 identifying himself to the verifier 40 by signing a challenge with the minimum threshold of devices 20. The dealer 30 requests a nonce and submits it to the user’s devices 20, which sign the nonce using their shares. These partial signatures are sent to the dealer 30 to produce a group signature. The dealer 30 then submits this to the verifier 40, which checks with the public key associated with the user identity that the signed nonce was produced by the user’s set of devices 20.

The update stage allows the user 10 to add and remove devices 20, as well as update security parameters such as the threshold number of devices 20 required for authentication.

The disclosed technique advantageously performs user identification for the purpose of password recovery by using multiple devices in user’s possession. The secret that is required for identification is distributed among the devices and a user is not required to memorize or select password recovery security questions. This makes it easier to apply different secrets to different accounts. Even if a user's device is stolen by an attacker, it does not give attacker the ability to recover or reset the user’s passwords. Therefore, loss or theft of fewer than all the devices neither compromises the account nor locks the user out of their account.

Disclosed by Gurchetan Grewal and Joshua Serratelli Schiffman, HP Inc.


10
User
Shareholders
Device 1
20
Device 2
20
Device 3
20
Dealer
30
VERIFIER
40