Indirect U2F Login

Bernd Borchert
Universität Tübingen
WSI Computer Science Department
Germany
borchert@informatik.uni-tuebingen.de

Abstract. The Universal Second Factor (U2F) authentication architecture is extended by a protocol for an indirect login. That is, even if the end device on which the U2F login is to be executed does not have the communication means to connect to the U2F token still a login is possible via a third device - which is the smartphone of the user.

Keywords. Authentication, indirect login, U2F

I. INTRODUCTION

The Universal Second Factor (U2F) initiative [1] was started in 2012 by an alliance of IT companies (FIDO) led by Google Inc. The intention of U2F is to solve the two main issues of passwords: (1) passwords are insecure because they can be tapped by malware sitting on the end device, and (2) passwords are hard to remember for the users - nowadays there are so many passwords that they have become a kind of modern plague for Internet users.

The solution idea of U2F is that the user carries a small hardware token which stores credentials for his Internet portals. When the user wants to login to some portal on some end device he connects the U2F token to the end device and then the portal server and the U2F token exchange a challenge/response protocol which together with the password represents the 2-factor authentication. The challenge/response exchange is zero knowledge, so the U2F credential cannot be tapped by malware, i.e. the identity can no longer be stolen by malware sitting on the end device (though a single login may still be stolen by malware).

The U2F token is usually realized as an USB stick. Of course there is a problem in case the end device for the login does not have an USB socket (most important example: smartphones) or in case it is not allowed to connect the stick to the end device. For this reason some U2F USB sticks were already extended by NFC connectivity. A formal U2F interface for contactless connection (NFC, Bluetooth) was published in June 2015 [2].

But even a U2F token having USB, NFC and Bluetooth (Bluetooth Low Energy BLE) connectivity may not find a hardware port on the end device on which the user wants to log in. We present a solution for this situation.

Every end device for a login has a screen. So in any given case the portal is able to show a 2D-code on its login page containing the authentication challenge. This 2D-code is scanned by the smartphone of the user. The smartphone forwards the challenge to the U2F token (via NFC or BLE) and the response received from the U2F token is forwarded by the smartphone to the portal server via smartphone Internet. The portal server checks the response and - in the positive case - redirects (via standard web techniques) the screen on the end device to an automatically opened account for the user.

This suggested procedure represents a solution for a login on any end device via smartphone and U2F token. It consists of many steps in the background but note that the user has not to do much.

A requirement for the method is that the smartphone and the U2F token have a connectivity method (Mini-USB, NFC, BLE) in common. BLE seems to be the universal solution because basically all recent smartphones including the iOS devices do have it. The disadvantage of BLE as compared to NFC is that the U2F token needs a battery. This is especially critical (but solvable [3]) in case the U2F token is a smartcard - which seems to be the ideal form factor for a contactless 2nd factor.

The indirect login method via smartphone described above is already in discussion since 2006 [4]. One of the first implementations was the system eKaay [5] at the Univ. of Tübingen starting in 2009. The extension of the smartphone method by a hardware token outside the smartphone (like in the above suggested U2F version) was developed within the eKaay project [6], including an obtained patent.

REFERENCES

[1] https://fidoalliance.org/specifications/overview/