WifiOTP : Pervasive Two-Factor Authentication Using Wi-Fi SSID Broadcasts

Emin Huseynov
emin@huseynov.com

Jean-Marc Seigneur
seigneuj@gmail.com

CUI, ISS & Medi@LAB, Faculté des Sciences de la Société
University of Geneva

Barcelona, Spain
9-11 December 2015
Agenda

• Introduction
• OTP Related Work and their Shortcomings
• The design of our solution: WiFiOTP
• Prototypes
• Conclusion
Two-factor authentication

- Two Factor Authentication requires a user to have access to a physical token or a mobile phone in addition to providing a password.

- While there are quite a few solutions for two-factor authentication, the de-facto standard nowadays is TOTP
Classic two-factor authentication

Authentication steps
• User enters the first factor (username & password)
• When requested to enter OTP, user launches the mobile app
• User looks up the OTP on the mobile app
• User types the OTP using the keyboard
Classic two-factor authentication

User resistance
If two-factor authentication is optional, users prefer not to enable it

Only around 6% of Google accounts have two-factor authentication enabled *

* [1] Petsas et al.2015
Improving two-factor authentication usability & summary

- Duo Security [2]
- Sound Proof [3]
- Authy Bluetooth[4]
- Other concepts announced

**Classic 2FA**
Hardware tokens or mobile OTP applications require users to manually type the generated OTPs using their keyboards

**Push notifications based**
Require active data connection and cannot be used as a drop-in replacement of the existing solutions

**BLE Based**
Limited mobile device support (Bluetooth 4.0) and inconvenience of using the clipboard. There is one production system available for Mac desktops only.
WifiOTP

As can be guessed from the name, the idea is to use Wifi SSID broadcasts to transfer OTPs.

OTPs are generated with TOTP algorithm on a special device, WifiOTP Token, and broadcasted as a part of SSID in encrypted format.
WifiOTP

A special software, WifiOTP client, scans the broadcasted SSIDs, finds and decrypts the OTP generated by WifiOTP token.
WifiOTP - Implementation

WifiOTP can be implemented on any hardware equipped with a wireless network adapter.
WifiOTP - Implementation

WifiOTP Demo – Windows 8
WifiOTP - Implementation

WifiOTP – Android keyboard

Step 2: Hitting "Insert OTP" will populate input field with OTP broadcasted by WiFiOTP Token and optionally submit the form.

Step 1: When prompted for OTP, user changes input method to WiFiOTP Keyboard.

Additional key to automatically insert OTP.
References & copyrights


- Some images used in this presentation have been obtained from publicly available websites and belong to Authy, DuoSecurity, OATH and others.