



ITU Kaleidoscope 2015
Trust in the Information Society

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

Emin Huseynov
emin@huseynov.com

Jean-Marc Seigneur
seigneurj@gmail.com

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

Barcelona, Spain
9-11 December 2015

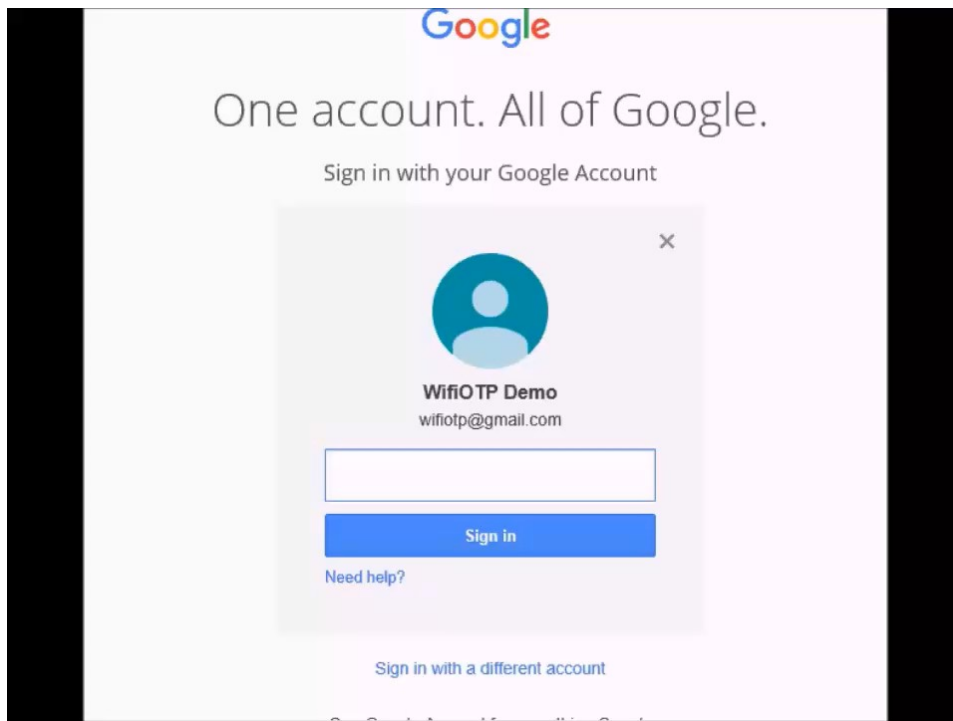
Agenda

- 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

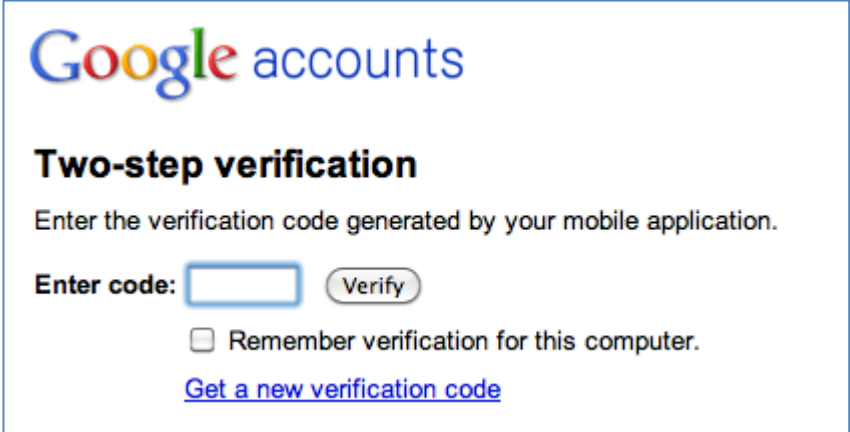
Classic two-factor authentication

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



The screenshot shows the Google accounts two-step verification interface. At the top, the Google logo is followed by the word "accounts". Below this, the heading "Two-step verification" is displayed. The instruction "Enter the verification code generated by your mobile application." is shown. The "Enter code:" label is followed by a text input field and a "Verify" button. Below the input field, there is a checkbox labeled "Remember verification for this computer." and a link that says "Get a new verification code".

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

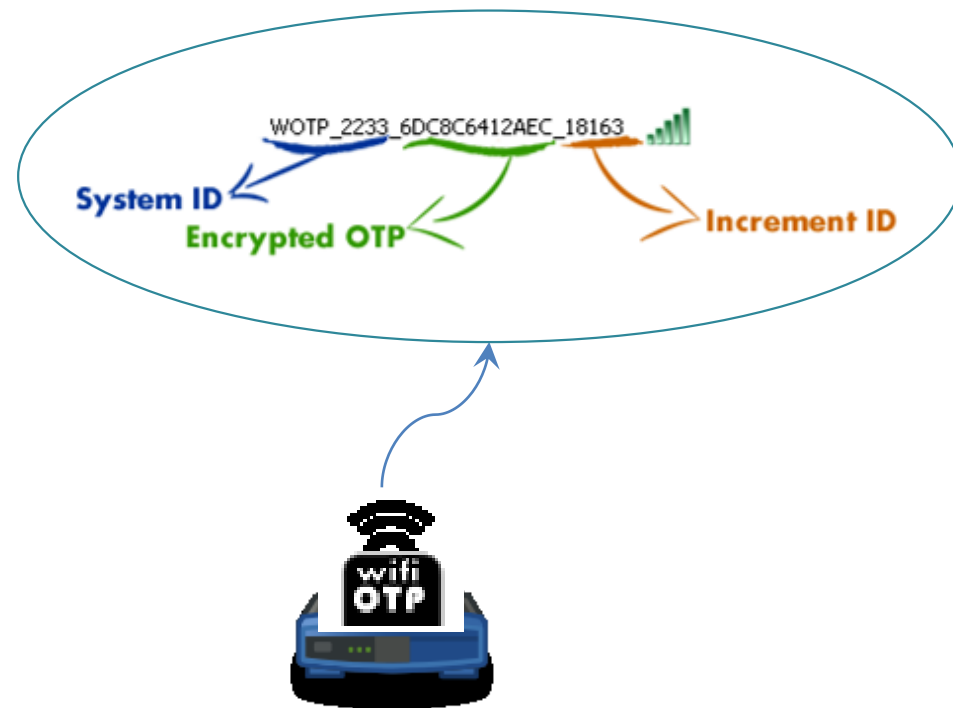
BLE Based

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

WifiOTP

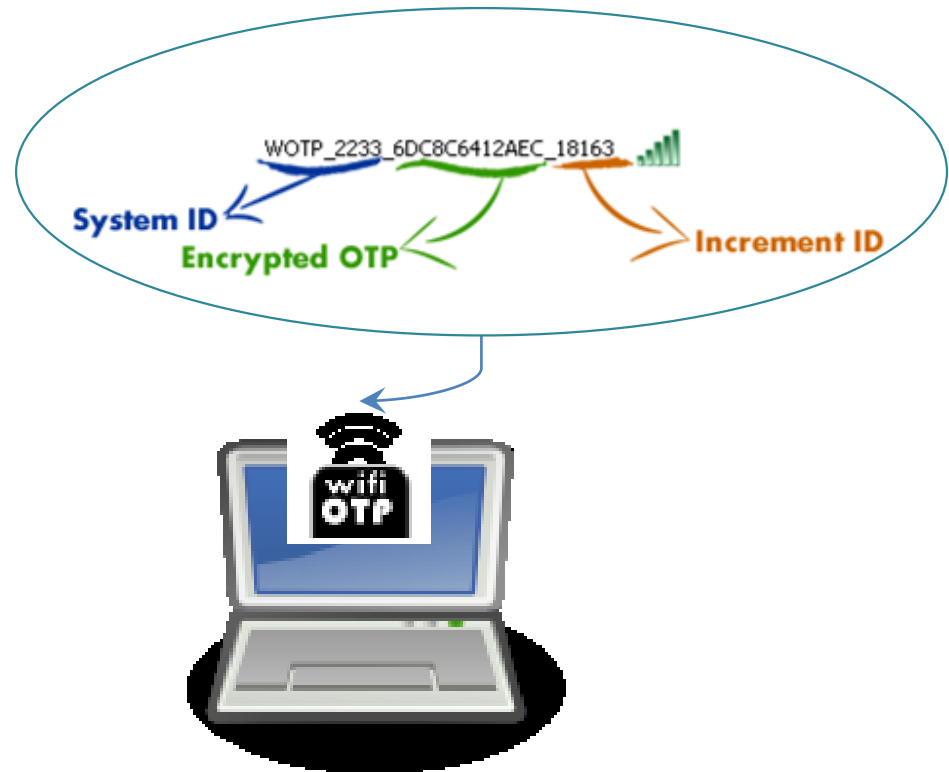
As can be guessed from the name, the idea is to use Wifi SSID broadcasts to transfer OTPs

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



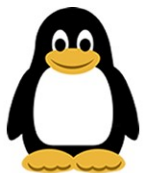
WifiOTP

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



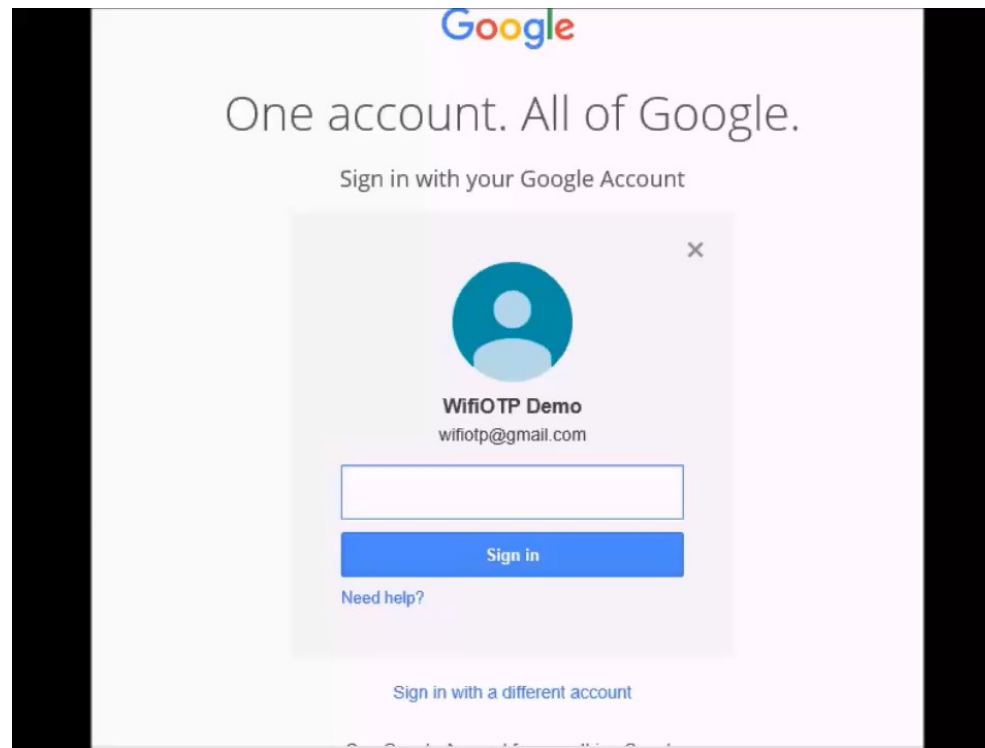
WifiOTP - Implementation

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



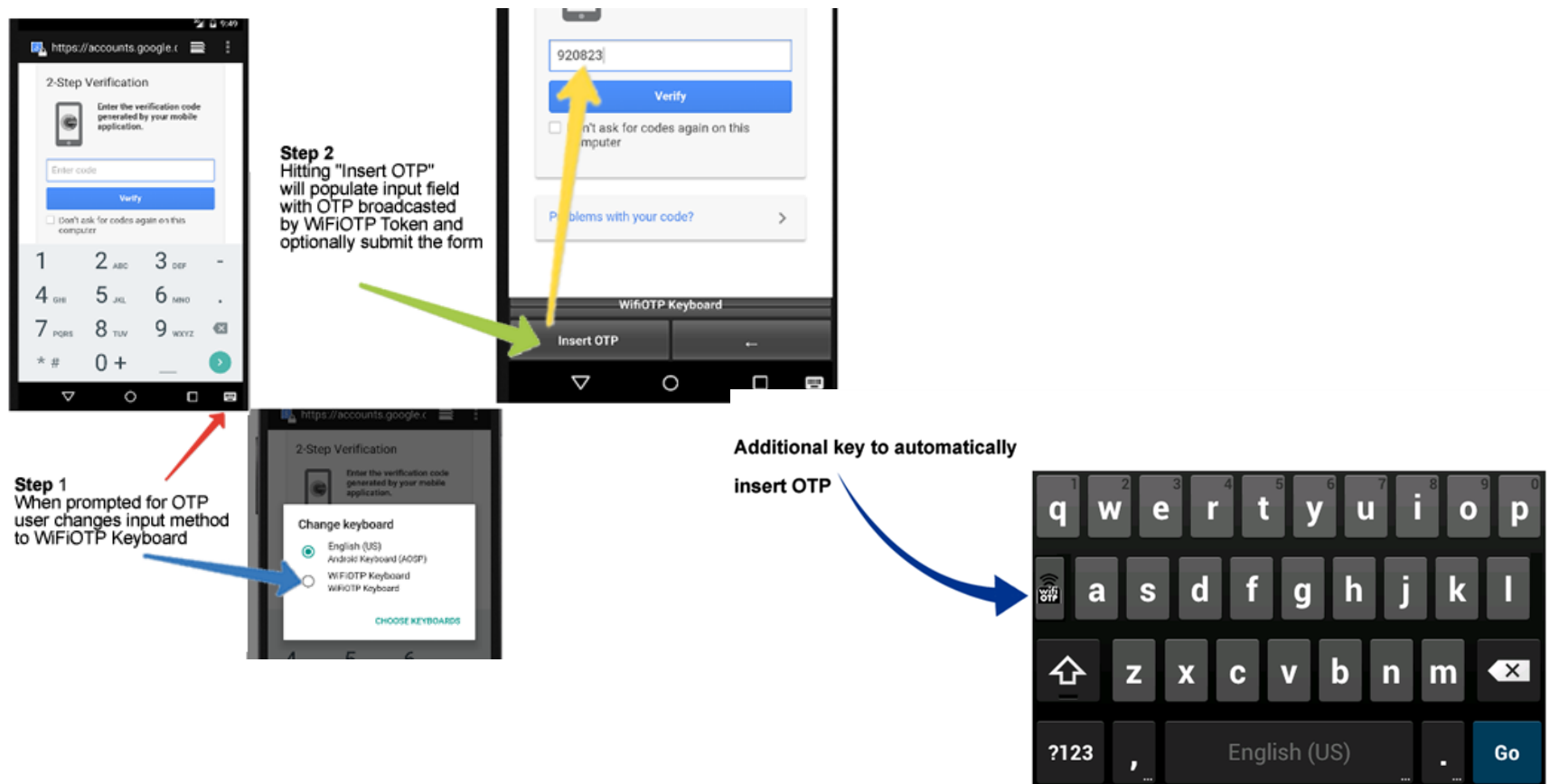
WifiOTP - Implementation

WifiOTP Demo – Windows 8



WifiOTP - Implementation

WifiOTP – Android keyboard



References & copyrights

- [0] M'Raihi, D., Machani, S., Pei, M., and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm", RFC 6238, DOI 10.17487/RFC6238, May 2011, <<http://www.rfc-editor.org/info/rfc6238>>.
 - [1] Thanasis Petsas, Giorgos Tsirantonakis, Elias Athanasopoulos, and Sotiris Ioannidis. 2015. Two-factor authentication: is the world ready?: quantifying 2FA adoption. In Proceedings of the Eighth European Workshop on System Security (EuroSec '15). ACM, New York, NY, USA, Article 4, 7 pages. DOI=<http://dx.doi.org/10.1145/2751323.2751327>
 - [2] Duo Security,. 'Mobile Authentication App For Smartphones'. N.p., 2015. Web. 18 Nov. 2015.
 - [3] Karapanos, Nikolaos, et al. "Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound." arXiv preprint arXiv:1503.03790 (2015).
 - [4] Authy, "Authy | The Future," 22 04 2015. [Online]. Available: <https://www.authy.com/thefuture#bluetooth>
- ❑ Some images used in this presentation have been obtained from publicly available websites and belong to Authy, DuoSecurity, OATH and others.