Offline Personal Authenticating Device applied in Hospitals and E-banking - OffPAD
Denis Migdal, Christian Johansen, Audun Jøsang

To cite this version:

HAL Id: hal-01589876
https://hal.archives-ouvertes.fr/hal-01589876
Submitted on 19 Sep 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License
**Motivation**

The concept of Lucidman (Local User-Centric Identity Management) is an approach to providing scalable, secure and user friendly identity and authentication functionalities. In this context we demonstrate the OffPAD as a trusted device to support different forms of authentication.

OffPAD aims to strengthen authentication assurance, improves usability, minimizes trust requirements, and has the advantage that trusted online interaction can be achieved even in the presence of malware infection of client platforms.

A video for this demo is available online.

---

**OffPAD device**

- microUSB
- secure element
- fingerprint
- NFC
- flash memory
- e-Ink screen

Prototype OffPAD version 1.

---

**Features**

- **Portability**: OffPAD is designed as a phone cover connected to its host with a standard micro-USB interface. This makes the OffPAD a portable object, but not a second electronic object in the user’s pocket.
- **Biometrics**: Unlocking the OffPAD is currently done through fingerprint biometrics.
- **Usability**: OffPAD is intended to increase security assurance with minimal interference with the normal tasks of the user, yet automate some of the authentication and identity management related tasks.
- **Anywhere security**: OffPAD allows to achieve trusted online interactions even on malware infected client platforms like the Android OS.

---

**Hardware and Firmware specifications**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description / Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td>STM32F401 ARM Cortex-M4 32-bit, 105 DMIPS, 256KB Flash, 64KB RAM</td>
</tr>
<tr>
<td>Secure display</td>
<td>e-Ink 2.5 inches</td>
</tr>
<tr>
<td>NFC transceiver</td>
<td>NFC 1002A2EV, NFC Forum Certified</td>
</tr>
<tr>
<td>Secure element</td>
<td>Java Card / Global Platform compliance, ST33FIMPEST Micro</td>
</tr>
<tr>
<td>microUSB interface</td>
<td>USB OTG 2.0 (High speed)</td>
</tr>
<tr>
<td>Fingerprint sensor</td>
<td>Touch Fingerprint Sensor, Pixel matrix 192x192 @502 dpi</td>
</tr>
<tr>
<td>3 states switch</td>
<td>Mechanical switch: On / Off / Maintenance</td>
</tr>
<tr>
<td>Flash memory</td>
<td>16GB for private/secure storage</td>
</tr>
</tbody>
</table>

---

**Assumptions**

- We assume that the sensors integrated in the OffPAD are secure.
- OffPAD still makes use of the host phone for other sensors, like camera, thus a malware on the phone can communicate false information to the OffPAD.
- OffPAD also asks the host phone for the heavier computations, e.g., for OCR. However, all these inputs from the phone are considered in our scenarios as untrusted.
- The OffPAD is a trusted device, i.e. assumed to function as intended and to be adequately protected against relevant attacks. OffPAD jacket is designed to withstand physical or software tempering.
- OffPAD is considered offline, meaning that communications follow controlled formats, during short and restricted time periods, not involving wireless broadband capabilities.
- Being offline eliminates exposure to Internet threats. Thus we assume that attackers are unable to exploit bugs in OffPAD’s firmware and applications.

---

**Demonstrators**

Data-US: Authentication of user Data by the Service provider, based on OCR (Optical Character Recognition), alternatively displayed on the OffPAD e-Ink screen.

SU: Server authentication by the User, based on petname systems managed by the OffPAD.

Auto-login: Contextual automatic login/off based on indoor location of the OffPAD, using Sonitor’s system.

Multi-login: Automatic access to a resource conditioned on multiple users authenticated at once, also using TellU Smarttracker system.

**Strong auth**: Strong authentication required for accessing sensitive information or tasks, using biometric fingerprint authentication of the user by the OffPAD.

---

**Acknowledgements**

We thank all OffPAD project members who have either put effort into parts of this demo or have contributed with great ideas or discussions, particularly to:

- Leonard Dallot, Laurent Miraflaie, and Guillaume Cornet (TaoTag, manufacturer of secure mobile hardware),
- Knut E Hass and Steen Morka (TellU, providing IoT platform and services),
- Marius P Haugen (U Oslo),
- Christophe Rosenberger and Estelle Cherrier (ENS Caen GREYC lab),
- Amir Taberkdini (Sonitor, manufacturer of indoor locating solutions),
- Petter Tøgersdal (Vail+, managing coordinator).

---

**Links**

- Detailed Technical Report
- Video
- offpad.org

---

**Presenters**

- Denis Migdal: denis.migdal@ensicaen.fr
- Marius P. Haugen (U.Oslo), cristinli.luo.no University of Oslo
- Audun Jøsang: audun.josang@mnm.uio.no University of Oslo
Sequence of messages/actions for data authentication:

1. User types the transaction data in a browser window on the client computer.
2. User activates the OffPAD to take a snapshot of the browser window.
3. Snapshot is taken from the text displayed in the browser window on the untrusted client.
4. The OCR (or QR code) function recovers the transaction data from the snapshot.
5. MAC generation with the transaction data and the user-password as input.
6. OffPAD sends MAC to client computer.
7. Client computer sends transaction data together with MAC to server.
8. Server verifies that the MAC corresponds to the received transaction data.

Petnames systems for Cognitive authentication

Zooco’s triangle for Petname Models.

Bryce “Zoooc” Wilcox-O’Hearn described in 2005 three fundamental desirable properties of names:

- Global (like DOIs or URLs);
- Unique (collision-free within a domain);
- Memorable (or human-meaningful).

Zooco explains with supporting evidence why no name space can have all three properties!

**The Petname Model** consists of two name spaces:

- One of global and unique names (pointers);
- One of memorable and unique names (pet-names);
- Mapping a name space of pointers to individual name spaces of petnames, which thereby combines all three desirable properties.

HTTP Extended DAA (XDAA)

HTTP Digest Access Authentication (HTTP DAA, RFC 7616) is an user authentication protocol:

1. client sends a query (HTTP GET);
2. server responds with a Challenge (HTTP 401);
3. client prompts for username and password;
4. client computes the Response;
5. client sends a new query, with the Response;
6. server answers the query (HTTP 200).

Response = \text{hash}(HA1 : Challenge : HA2) = \text{Hash} (\text{GET} : \text{uri})

Klevjer, Varmened, & Jøsang extend HTTP DAA:

- challenge forwarded to the OffPAD;
- password generated from user biometric;
- \text{HA1} can be precomputed and stored on the OffPAD.

Mutual authentication using Petnames and XDAA

Sequence of messages/actions for user and server authentication ceremony:

1. User initiates connection with Bank's server through the client/browser (which is not trusted).
2. Server sends HTTP XDAA challenge to client, along with the Bank's ID in a certificate (maybe using DNSSEC).
3. Challenge and BankID are forwarded by browser to OffPAD.
4. OffPAD presents user authentication request to user.
5. Server certificate is forwarded to OffPAD.
6. Server certificate is validated (syntactic server authentication).
7. Server certificate/BankID is mapped to petname.
8. Petname is presented to user.
10. User approves authentication request.
11. OffPAD computes response to challenge from server.
12. Response is sent from OffPAD to client.
13. Client forwards response to server.

Automatic login-logoff and Multi-login

Paring and Take in use:

- Nurse takes OffPAD in use at beginning of shift by authenticating through biometric fingerprint.
- Device loads user profile and registers to TellU.
- Nurse pairs location TAG to OffPAD device.
- Pairing information sent to TellU system.
- Now the TAG tracked by the Sonitor system is known to TellU as being attached to the User that activated the respective OffPAD.

Multiple users Access Control:

- Both Nurse and Patient are in front of a Terminal. TellU system triggers an access control event.
- Sensitive operations or information, e.g. signing a receipt, or ending a task.

Context based Access Control:

- Indoor location of Objects (Nurse/Patient/Doc-
tor) tracked in real-time by the Sonitor system.
- When Nurse approaches a Terminal the TellU decision system is notified and a login event is triggered through the Hospital system.
- When Nurse walks away, the TellU system is notified by Sonitor, and triggers a logoff event.
- Continuous biometric authentication methods can ensure that OffPAD is in User’s possession.

Strong authentication:

- Context authentication may be not good enough for some sensitive operations or information, e.g. signing a receipt, or ending a task.
- Hospital systems may require the Nurse to authenticate through the OffPAD using biometric fingerprint before allowing access.

**eHospital Infrastructure**

**Automatic login-logoff and Multi-login**

**Context based Access Control**

**Strong authentication**