Appareil Personnel et Hors-ligne d'Authentification - OffPAD

Denis Migdal, Christian Johansen, Audun Jøsang

Appareil personnel et hors-ligne d'authentification

OffPAD

Motivation

Lucidman est une approche fournissant des fonctionnalités d'identité et d'authentification sécurisées et ergonomiques.

Dans ce cadre, nous présentons l'OffPAD, un appareil sécurisé, supportant différentes formes d'authentifications.

L'approche Lucidman/OffPAD consiste à effectuer la gestion des identités et de l'authentification côté utilisateur au lieu de le faire côté serveur ou dans le cloud.

OffPAD vise à améliorer la sécurité et la maniabilité de l'authentification, et a l'avantage de permettre des interactions en ligne sécurisées quand bien même le client serait infecté par un virus.

L'OffPAD

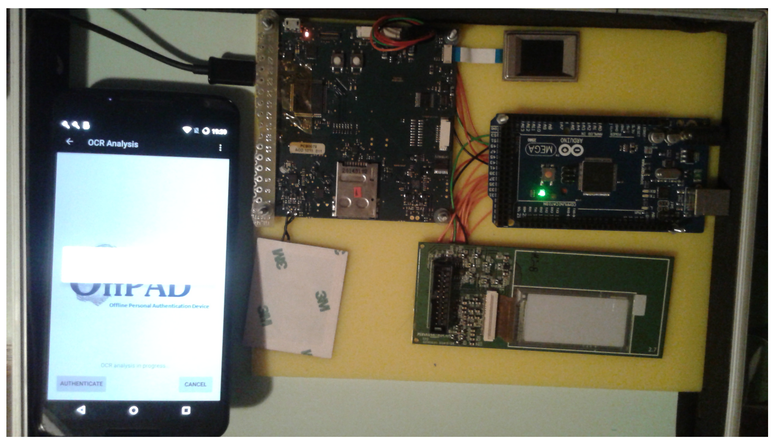


Figure 1: Prototype OffPAD version 1 .

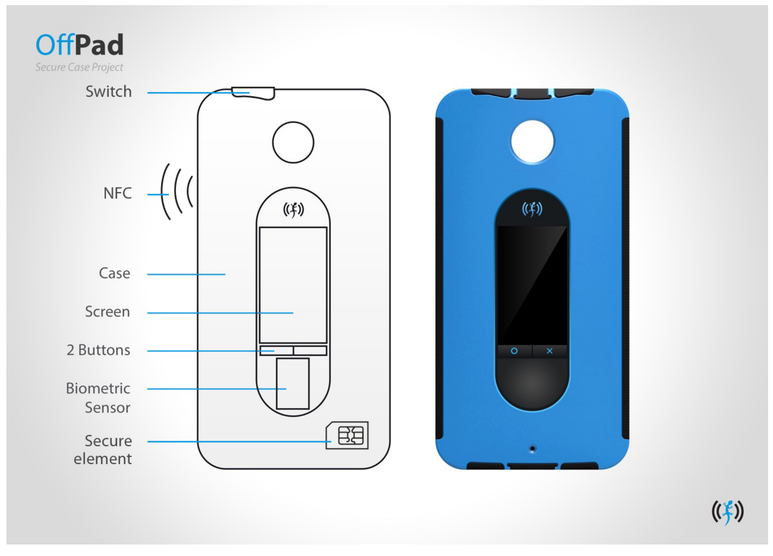


Figure 2: Coque de téléphone, OffPAD version 2 .

Fonctionnalités

Portabilité: L'OffPAD est un objet portable sans être un nouvel appareil porté par l'utilisateur.

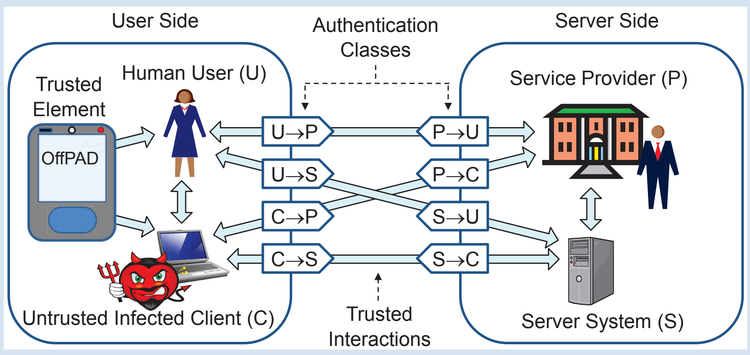
Biométrie: L'OffPAD est déverrouillé via les empreintes digitales de l'utilisateur.

Ergonomie: L'OffPAD est conçu de sorte à ne requérir qu'un minimum d'effort de la part de l'utilisateur.

Catégories et Types d'Authentification

Catégories d'Authentification

Dans le modèle client-serveur, les entités en jeu peuvent être des entités systèmes (client ou serveur) ou des entités cognitives/légales (humain ou organisation). Il est ainsi possible de distinguer plusieurs catégories d'authentifications (Authentication Classes).



Trois types d'authentification

Syntaxique : le plus simple, mais ne protège pas contre les imitations. MonSite.net copiant MonSite.com sera considéré valide tant qu'il possède un certificat (cadenas dans le navigateur) ;

Sémantique : inclue des vérifications supplémentaires dépendant d'une politique de sécurité. On peut alors vérifier si le nom du site est dans une liste noire ou est trop proche d'un site connu et de confiance ;

Cognitive : requiert que l'entité vérifiant le domaine dispose de capacités cognitives tel un humain ou une IA. L'authentification cognitive prévient efficacement les attaques par phishing, l'utilisateur reconnaissant le site et son nom.

Spécification du matériel

Matériel

- **Écran e-Ink ;**
- **LED multicolore ;**
- **Interface microUSB 2.0 ;**
- **NFC ;**
- **Capteur d'empreinte ;**
- **Mémoire flash.**

API.

- **Authentification de l'utilisateur ;**
- **Gestion des certificats ;**
- **Signature et vérification de signatures ;**
- **Afficher des informations sensibles ;**
- **Enrôlement biométrique de l'utilisateur.**

Démonstrations

- **Authentification des données :** le serveur vérifie que les données proviennent de l'utilisateur.
- **Authentification du serveur :** l'utilisateur attribue des surnoms aux sites visités (petnames).
- **Authentification de l'utilisateur :** le client transmet la demande d'authentification à l'OffPAD.
- **Auto-login :** Connexion automatique basée sur la position de l'OffPAD.
- **Multi-login :** plusieurs utilisateurs peuvent être connectés en même temps.
- **Auth. forte :** authentification via le capteur d'empreinte, en plus de sa position (Auto-login).

Remerciements

Nous remercions tous les membres du projet OffPAD qui ont travaillé sur des parties de cette démonstration ; particulièrement :
Leonard Dallot, Laurent Miralabe, et Guillume Cornet (TazTag, concepteur de téléphones sécurisés),
Knut E. Husa et Svere Morka (TellU, fournisseur de services et de platforme IOT),
Marius P. Haugen (U.Oslo),
Christophe Rosenberger et Estelle Cherrier (ENSI Caen GREYC lab),
Amir Taherkordi (Sonitor, concepteur de localisation d'intérieur).

Auteurs

Denis Migdal
denis.migdal
@ensicaen.fr
GREYC Lab

Christian Johansen
cristi
@ifi.uio.no
Université d'Oslo

Audun Jøsang
audun.josang
@mn.uio.no
Université d'Oslo

Cette démonstration sera présentée à la 23^{me} conférence ACM annuelle sur la sécurité informatique et des communications (CCS 2016), à Vienne.