DEMO: OffPAD – Offline Personal Authenticating Device with Applications in Hospitals and e-Banking

Denis Migdal
Ecole Nationale Supérieure d'Ingénieurs de Caen
denis.migdal@ecole.ensicaen.fr

Christian Johansen
Department of Informatics, University of Oslo.
cristi@ifi.uio.no

Audun Jøsang
Department of Informatics, University of Oslo.
josang@ifi.uio.no

ABSTRACT

Identity and authentication solutions often lack usability and scalability, or do not provide high enough authentication assurance. 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 use of an OffPAD (Offline Personal Authentication Device) as a trusted device to support different forms of authentication. The Lucidman/OffPAD approach consists of locating the identity management and authentication functionalities on the user side instead of on the server side or in the cloud. This demo aims to show how OffPAD strengthens authentication assurance, improves usability, minimizes trust requirements, and has the advantage that trusted online interaction can be achieved even on malware infected client platforms. The trusted device OffPAD has been designed as a phone cover, therefore not requiring the user to carry an extra gadget. We focus on six demonstrators, three useful in e-banking and three in the hospital domain where nurses, doctors, or patients are authenticated and access is granted in various situations base on the OffPAD. A video with the same title is available online at www.offpad.org.

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: L. Dallot, L. Miralabe, and G. Cornet (TazTag, manufacturer of secure mobile hardware), K.E. Husa and S. Morka (TellU, providing IoT platform and services), M.P. Haugen (U.Oslo), C. Rosenberger and E. Cherrier (ENSI Caen GREYC lab), A. Taherkordi (Sonitor, manufacturer of indoor locating solutions).

1. MOTIVATION AND BACKGROUND

We demo the OffPAD concept, i.e., the hardware, a phone cover with secure elements, and software components. The concept of OffPAD has been put forward in [5], whereas the hardware prototype and software have been developed during the past two years part of the project called OffPAD.[1] Several use cases have been identified to show case the OffPAD in the domains of e-banking and hospitals.

One aim with OffPAD is to increase security assurance without reducing the usability, i.e., have minimal interference with the normal tasks of the user, yet automate some of the authentication related tasks. OffPAD can be seen as an identity management device, assuming an entity to have multiple identities simultaneously, similar to what ABAC and Attribute-Based Credentials advocate. OffPAD aims to improve on the traditional "silo model" where the identities are located on the server side, by managing identities locally under user's control only. However, an OffPAD maintains, besides user's credentials, also the credentials of service providers to be used in authenticating the service to the user. OffPAD also improves on the identity federation endeavours (e.g., Shibboleth, OpenId, FacebookConnect, FIDO) which are managed on servers or clouds, thus making them "network-centric" instead of "user-centric".

We take the distinction between a system entity (browser or server) and a legal/cognitive entity (person or organisation) thus multiplying the mutual authentication possibilities. We also consider authentication to be of three types: (i) *syntactic*, being the simplest, including X.800 certificates, which, e.g., does not prevent phishing attacks since the relying party is indifferent to the identity of the certificate owner; (ii) *semantic* authentication includes syntactic and moreover the verification by the relying entity that the remote entity has semantic characteristics that are compliant with a specific security policy; and (iii) *cognitive* being the richest, requiring the relying party to have cognitive reasoning power, such as in humans or advanced AI systems. Cognitive authentication effectively prevents phishing attacks as users recognise the server identity, spotting a malicious owner of a legitimate certificate accepted by the browser.

With OffPAD we are interested in cognitive authentications involving the human user.

The X.800 standard is concerned with authenticating the Client Computer to the Server (CS) and the other way around (SC) which take place at the network protocol layers and are typically transparent to the human user. However, for online services the User authentication to the Server (US) and the cognitive server authentication by the user (SU) are more relevant. The importance of these authentication classes emerges from the need for end-to-end security, i.e., between the human user (U) and the server system (S).

CCS'16 October 24-28, 2016, Vienna, Austria

ACM ISBN 978-1-4503-4139-4/16/10.
DOI: http://dx.doi.org/10.1145/2976749.2989033

[1]Funded by EUREKA and Eurostars, with nr. E!8324.

It is assumed that traditional server authentication with browser PKIX[2] server certificates and TLS provides SU authentication, however in reality it does not. This might seem surprising but is in fact easy to understand [3].

For example, phishing attacks normally start with spam emails that invite people to access a fake web site that tricks the user into providing user Id and password. In a syntactic sense the fake phishing website is correctly authenticated through TLS because the server certificate is validated by the browser. However, from a cognitive point of view this is not authentication because the website's identity is different from that intended by the user. The problem is due to the poor usability offered by current implementations of TLS [4] which does not facilitate cognition of identities.

Data origin authentication, according to the X.800 standard, is *"the corroboration that the source of data received is as claimed"*. Malware infection of client platforms opens up for attacks against data authentication that entity authentication cannot prevent. A typical example is online banking transactions with mutual entity authentication. Even when there is strong 2-factor user authentication, there is the possibility that a Trojan program changes the transaction details without the user's knowledge (commonly known as a *"web inject"* that can change the behaviour of the browser and modify input and output data arbitrarily). SpyEye, Zeus, IceIX, TDL, Hiloti, Carberp, are concrete examples of malware that enable such attacks. In this case the human user is assumed to be the origin, but the client modifies data input by the user before it is sent to the server system, thus breaching data origin authentication. For typical online transactions current solutions for user data origin authentication are either non-existent or inadequate because they assume the client system to be the origin of data.

The difference between entity authentication and data authentication makes it necessary to have specific security mechanisms to ensure data integrity in online transactions. The OffPAD enables data origin authentication with high assurance and usability, as explained below.

Related works are discussed in the journal paper [5] and the technical report [7] accompanying this abstract. Several authentication solutions that rely on an external device are present in the literature, including Pico by Stajano, MP-Auth by Mannan and van Oorschot, and Nebuchadnezzar by Singer and Laurie. However, these devices only support authentication of client-side entities to server-side parties, i.e. typically user authentication, in contrast to the OffPAD which also supports the authentication of server-side entities to client-side parties, as well as data authentication.

2. OFFPAD DEVICE DESCRIPTION

The OffPAD is a trusted device, i.e. assumed to function as intended and to be adequately protected against relevant attacks. The first OffPAD prototype is 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. Unlocking the OffPAD is currently done through fingerprint biometrics.

OffPAD is considered offline, meaning that communications follow controlled formats, during short and restricted time periods, not involving wireless broadband capabilities, i.e., we use only micro-USB or NFC communications.

[2]Public-Key Infrastructure based on X.509 certificates

Being offline eliminates exposure to Internet threats. Thus we assume that attackers are unable to exploit bugs in OffPAD's operating system and applications.

The first connection to the OffPAD requires Trust-On-First-Use (TOFU), also known as leap-of-faith. On first use, there is no cryptographic way to verify the connection between the device and the client platform, the trust must simply be based on the physically observed set-up.

A schematic view of OffPAD design is illustrated in Fig.1.

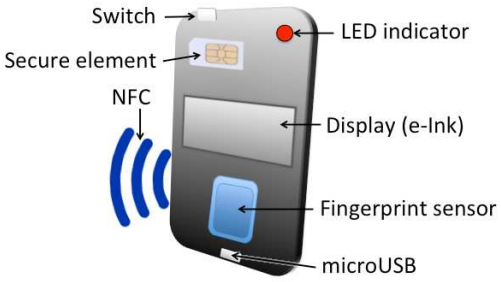

Figure 1: OffPAD v.1 design elements

OffPAD integrates the following hardware components: (i) *secure Javacard/Global platform* component for secure application execution and storage, (ii) *e-Ink screen* 2.5 inches, (iii) *multi-color LED* for simple information transmission, (iv) *NFC transceiver* and (v) *micro-USB* for communication with the client, (vi) *fingerprint sensor*, (vii) *4GB to 16GB flash memory*.

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 more heavy computations, e.g., for OCR. However, all these inputs from the phone are considered in our scenarios as untrusted.

The OffPAD firmware supports the following features:

User Authentication by performing a biometric authentication of the holder.

Manage certificates in OffPAD's certificate store to check signature, s.a. for authenticating service provider identities.

Sign and check signature using the OffPAD's holder private key unlocked after successful holder's authentication.

Show sensitive information using the e-Ink display or the multi-color LED.

Biometric user enrolment on the OffPAD according to the specified biometric modality.

3. OFFPAD DEMONSTRATORS

The following applications of OffPAD are demonstrated.

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 [2] managed by the OffPAD.

US: User authenticated by the service provider, based on an extended challenge-response protocol XDAA [6] between the client terminal and 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.

We demonstrate how the OffPAD enables mutual user-server entity authentication as well as data authentication. Each use case is illustrated with a ceremony [1] which is simply a protocol where relevant actions by users and the context environment are included. The intention of our solutions is to support trusted interaction even in the presence of malware infected client platforms. We illustrate here only the ceremony SU and motivate Auto-login for hospitals.

In order to support cognitive server authentication, the server domain name, received in the server certificate, is mapped to a user-defined petname representing the service provider. The server certificate is also validated in the traditional way, which provides syntactic server authentication.

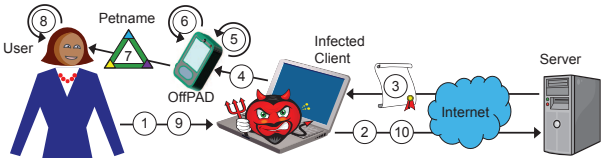

Figure 2: Server authentication by the User based on petname systems managed with the OffPAD

The actions/messages of the SU demonstrator are described at a high-level as: (1) User initiates secure TLS connection through client platform (2) Client platform contacts server (3) Server returns server certificate containing public key (4) Server certificate is forwarded to OffPAD (5) Server certificate is validated (syntactic server authentication) (6) Server certificate is mapped to petname (7) Petname is presented to user (8) User performs cognitive server authentication (9) User approves server authentication (10) TLS connection established between client and server

Hospitals are a hectic working environment where multiple users with diverse roles interact with hospital IT shared systems for various duties like patient records, routine information, or logging of medical tasks. However, patient information security and privacy must still be ensured throughout the daily work. This implies that the staff must log on to terminals and be authorised every time they interact with IT systems. This has been found very time consuming and distracts attention from primary tasks. The inadequacy of standard username/password process is due to the following observations: (i) clinical work happens in a fast pace while login causes focus shift; (ii) medical work is nomadic and with constant interruptions while login is fixed to one computer; (iii) medical work is collaborative using shared material while login is intended for single user activities.

The OffPAD demonstrators focus on continuous, context-aware, and usable authentication mechanisms to relieve the user from the burden of a frequent login/logoff process. We demonstrate a location-based authentication mechanism where the user will be automatically logged in to a terminal when she approaches the terminal, and logged off from it when she leaves the terminal.

4. DISCUSSIONS AND CONCLUSION

Various applications can be imagined using OffPAD [8]. We mention here a few other than the six demonstrated. The method for bank transaction can be used to sign medical prescriptions. The method for loading patient record can be used in other situations, e.g., when a nurse is allowed to make changes to a resource only under the supervision of a doctor (maybe a specialist). Auto-login can be used for easy moving of patients between rooms, where the entertaining system, like preferred TV channels, are immediately transferred to the new terminal based on the location. Petnames can be associated to any kinds of domain names for sensitive services, like tax office, preferred shops, etc, and the user can do cognitive authentication of these web-sites as well.

During the demo we also use a poster to describe the OffPAD graphically. The demo uses two laptops which need to sit at least 2 meters apart, along with indoor location equipment from the project partners TellU and Sonitor. Besides, the demo also uses a smart phone application, together with the OffPAD hardware phone cover attached to the phone.[3] The demo also uses the SmartTracker technology from the project partner TellU, which runs in the servers of TellU, therefore, Internet connection is needed.

5. REFERENCES

[1] C. Ellison. Ceremony Design and Analysis. Cryptology ePrint Archive, Report 2007/399, 2007.

[2] M. S. Ferdous and A. Jøsang. Entity Authentication & Trust Validation in PKI using Petname Systems. In Theory and Practice of Cryptography Solutions for Secure Information Systems (CRYPSIS), pages 302–334. IGI Global, 2013.

[3] A. Jøsang. Trust Extortion on the Internet. In 7th Workshop on Security and Trust Management (STM), pages 6–21. LNCS 7170, Springer, 2012.

[4] A. Jøsang, B. AlFayyadh, T. Grandison, M. AlZomai, and J. McNamara. Security Usability Principles for Vulnerability Analysis and Risk Assessment. In 23rd Annual Computer Security Applications Conference (ACSAC), pages 269–278. IEEE, 2007.

[5] A. Jøsang, C. Rosenberger, L. Miralabé, H. Klevjer, K. A. Varmedal, J. Daveau, K. E. Husa, and P. Taugbøl. Local user-centric identity management. Journal of Trust Management, 2(1):1–28, 2015.

[6] H. Klevjer, K. A. Varmedal, and A. Jøsang. Extended HTTP digest access authentication. In 3rd IFIP WG 11.6 Working Conference on Policies & Research in Identity Management (IFIP IDMAN), volume 396 of IFIP AICT, pages 83–96. Springer, 2013.

[7] D. Migdal, C. Johansen, and A. Jøsang. Offpad: Offline personal authenticating device – implementations and applications. Technical Report 454, U. Oslo, Aug. 2016. (http://heim.ifi.uio.no/~cristi/papers/TR454.pdf).

[8] K. A. Varmedal, H. Klevjer, J. Hovlandsvåg, A. Jøsang, J. Vincent, and L. Miralabé. OffPAD: Requirements and Usage. In Network and System Security (NSS), volume 7873 of LNCS, pages 80–93. Springer, 2013.

[3]The secure cover is a hardware prototype version 1, which does not have the proper dimensions. Unfortunately, the version 2 of the cover, with proper form factor, will appear only towards the end of the year.