The Evolution of Authentication

The Role of Secure Hardware in Overcoming Authentication Challenges

Dr. Rolf Lindemann, FIDO Alliance

rolf@noknok.com
4151 Middlefield Road
Palo Alto
California 94303
USA

Abstract. Even after 40 years of IT innovations, passwords are still the most widely used authentication method. They are inherently insecure. Neither users nor service providers handle passwords appropriately. On the other hand more than 1 billion Trusted Platform Modules (TPMs) and more than 150 million secure elements have been shipped; microphones and cameras are integrated in most smart phones and fingerprint sensors and Trusted Execution Environments (TEEs) are on the rise. There are better ways for authentication than passwords or One-Time-Passwords (OTPs).

The FIDO Alliance has been founded to define an open, interoperable set of mechanisms that reduce the reliance on passwords. Secure hardware is important to achieve high assurance levels.

We explain how secure hardware in conjunction with a generic protocol can help overcoming today's authentication challenges.

Keywords: Authentication, Cloud, Security, Biometrics, Secure Hardware

1 Motivation

Passwords don't work: In 2007, the average user had 25 accounts, used 6.5 passwords and performed logins 8 times a day. (Dinei Florêncio and Cormac Herley, Microsoft Research, 2007). Today, things are much worse. An analysis of 6 million accounts showed that 10,000 common passwords would have access to 99.8% of the accounts (Burnett, 2011). This basically means that only 0.2% of the users chose strong passwords. Even when looking at passwords for banking accounts only, it can be found that 73% of users shared their online banking password with at least one *non-financial* site (Trusteer, Inc., 2010), which means that when the non-banking site gets hacked, the banking account is threatened.

"Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks." (Cloud Security Alliance, 2010).

The password problem seems to be an important issue to solve: “Account and service hijacking, usually with stolen credentials, remains a top threat” (Cloud Security Alliance, 2010). It’s not only about security. According to a recent study, more than 45% of the online transactions fail “Very Frequently” or “Frequently” due to authentication problems (Ponemon Institute LLC, 2013).

Several proposals to replace passwords have been made. A good analysis can be found in (Joseph Bonneau, 2012).

Silos of Authentication: Current alternative technologies require their respective proprietary server technology. The current authentication architecture therefore consists of silos comprising the authentication method, the related client implementation and the related server technology.

Innovative authentication methods proposed by the research community are not widely deployed, as in addition to the client implementation the complete server software needs to be implemented and deployed. Instead of having a competition for better user authentication methods, authentication companies are faced with a battle for the best server technology.

Heterogeneous Authentication Needs: Authentication is used for electronically initiating high value money transactions and for accessing the personal purchase history in an online bookshop. The security needs are different.

Users might authenticate using standalone PCs, tablets or smart phones. The employer might control some devices; others might be controlled by the user (David A. Willis, Gartner, 2013). Increased adoption of mobile devices and the BYOD trend lead to an increasingly heterogeneous authentication landscape. The one authentication method satisfying all needs seems to be out of reach.

Trustworthy Client Environment: Client side malware could capture and disclose passwords or OTPs. It could alter transactions to be confirmed after being displayed or it could misuse authenticated communication channels to perform unintended actions. Authentication – even with username and password – needs at least one trustworthy component at the client side.

2 Related Work

A survey of (basic) authentication protocols can be found in (Jacob, 1997). The principle of hardware attestation is mentioned in (Benjie Chen and Robert Morris; MIT Laboratory for Computer Science, 2003) and it has been implemented and widely deployed by Trusted Platform Modules (TPMs).

As well as research into specific user authentication methods, the research community has tried to standardize authentication. The following standards are related:

- PKC#15, achieving smart card profile interoperability by introducing a meta card profile;

- PKCS#11 (RSA Laboratories, 2009), achieving cryptographic token interoperability by providing a unified API;
- GSS-API (RFC 1508, RFC 2078, RFC 2743, Kitten working group), generic security service API. Achieving interoperability by allowing applications to use a shared module, i.e. effectively reducing the number of implementations;
- ISO/IEC 24727 is a set of programming interfaces for interactions between integrated circuit cards and external applications to include generic services for multi-sector use.

The aspect of supporting a variety of authentication methods for network access authentication is approached by the Extensible Authentication Protocol (EAP, RFC 3748). This protocol is designed for situations in which IP layer connectivity may not be available. "Use of EAP for other purposes, such as bulk data transport, is NOT RECOMMENDED" (B. Aboba, Microsoft; L. Blunk, Merit Network, Inc.; J. Vollbrecht, Vollbrecht Consulting LLC; J. Carlson, Sun; H. Levkowetz, ipUnplugged, 2004).

The Initiative for Open Authentication (OATH) is an industry-wide collaboration to develop an open reference architecture by leveraging existing open standards for the universal adoption of strong authentication (see www.openauthentication.org). Besides the OATH Reference Architecture (Initiative for Open Authentication (OATH), 2007), this initiative has published standards documents regarding an HMAC-Based OTP Algorithm (RFC 4226), Time-based One-time password Algorithm (RFC 6238), OATH Challenge/Response Algorithm (RFC 6287), and two provisioning standards (Portable Symmetric Key Container RFC 6030 and Dynamic Symmetric Key Provisioning Protocol RFC 6063).

In the case that a user has authenticated to the first relying party (typically called Identity Provider, IdP), this authentication can be federated to other relying parties (→ Federation). Popular federation protocols are SAML, OpenID, and OpenID Connect. Related to these federation protocols is the web authorization protocol OAuth. An initial authentication (of the resource owner in this case) is leveraged here as well.

The FIDO protocol is concerned with authenticating the user to the first relying party ("first-mile authentication"); federation is about leveraging this "first-mile authentication" to other relying parties ("second mile authentication").

3 FIDO Approach

We propose to (a) separate the user authentication method from the authentication protocol and (b) to define an attestation method in order to proof the FIDO Authenticator type to the relying party. Given this information, the relying party is able to infer the related assurance level (e.g. as defined in (William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk; Computer Security Division, Information Technology Laboratory and Sabari Gupta, Emad A. Nabbus; Electrosoft Services, Inc., 2013). The assurance level can be fed into internal risk management systems. The relying party can then add implicit authentication methods as needed.

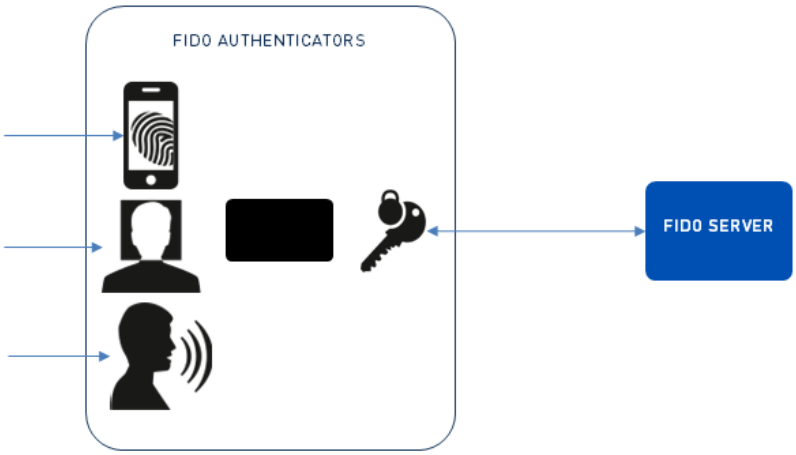


Fig. 1. Mapping Arbitrary User Authentication to Cryptographic Authentication

In the FIDO approach, standardized challenge response based cryptographic authentication schemes are used between the FIDO Authenticator (controlled by the user) and the FIDO Server (controlled by the relying party). The FIDO Authenticator can implement any user authentication method, but it has to cryptographically attest itself to the relying party. The security relevant functions are centralized into the FIDO Authenticator.

3.1 FIDO Protocol

Starting from this challenge response based authentication scheme, the FIDO protocol is defined. It is called Online Secure Transaction Protocol (OSTP), and supports the following functionality:

1. Discovery
2. Registration
3. Authentication
4. Transaction Confirmation

The discovery enables relying parties to understand the user authentication methods (more specifically the FIDO Authenticators) supported by the FIDO User Device. The relying party can specify a policy for selecting FIDO Authenticators best suited for the specific purpose.

The Registration operation binds the FIDO Authenticator to a specific entity. This might be an existing user identity already present in the system or it might be a user identity to be created.

The Authentication operation supports single or multiple FIDO Authenticators to be involved. Each FIDO Authenticator might be implemented to represent either simple or strong authentication / two factor authentication (European Central Bank,

2012) (FFIEC, 2005). The Authentication operation is used to establish an authenticated channel between the Browser / App and the relying party Web Server.

The Transaction Confirmation allows the user to see and authenticate a particular well-defined transaction to the relying party. It is more secure as it doesn't rely on a Web Browser / App to not misuse an authenticated channel.

This leads to the following reference architecture:

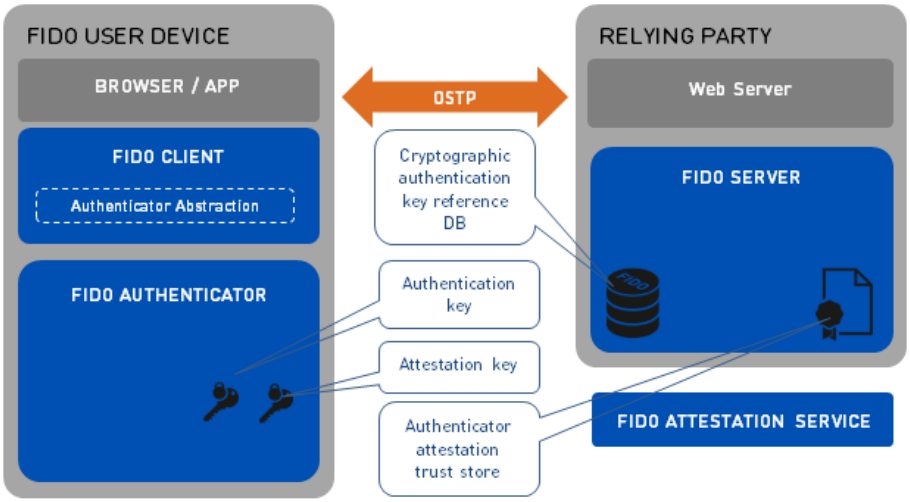


Fig. 2. FIDO Building Blocks

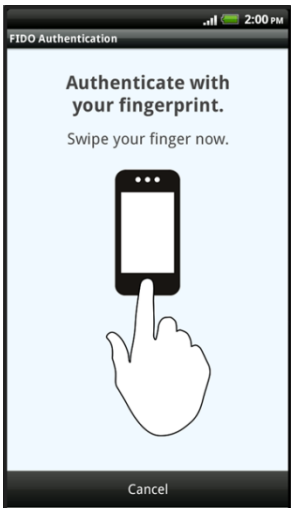
The FIDO Authenticator is a concept. It might be implemented as a software component running on the FIDO User Device, it might be implemented as a dedicated hardware token (e.g. smart card or USB crypto device), it might be implemented as software leveraging cryptographic capabilities of TPMs or Secure Elements or it might even be implemented as software running inside a Trusted Execution Environment.

The User Authentication method could leverage any hardware support available on the FIDO User Device, e.g. Microphones (→ Speaker Recognition), Cameras (→ Face Recognition), Fingerprint Sensors, or behavioral biometrics, see (M. S. Obaidat) (BehavioSec, 2009).

3.2 User Experience

The user experience is mainly dominated by the user authentication method. For example, entering strong passwords on a smart phone leads to bad user experience (Florian Schaub, Ruben Deyhle, Michael Weber; Institute of Media Informatics, Ulm University, 89069 Ulm, Germany, 2012). Bad user experience might lead to poor security as many users opt for convenience rather than security (Confident Technologies, 2011).

FIDO Authenticators could implement any user authentication method. Such methods can be optimized for particular use cases and for the devices they are running on. In some situations, the user authentication method should be non-intrusive, so continuous authentication (Koichiro Niinuma, Fujitsi Laboratories, Kawasaki, Japan; Anil K. Jain, Department of Computer Science & Engineering, Michigan State University, East Lansing, MI, USA, 2009) (Martha E. Crosby and Custis S. Ikehara; University of Hawaii/Manoa (USA), 2004) could be an option. In other situations a more precise user authentication method might be desirable, so the use of fingerprints or dedicated hardware tokens (such as smart cards) might be more suitable.



Due to the separation of user authentication method and authentication protocol, the change of the user method doesn't have any impact on the authentication server – as long as the assurance level is acceptable in the given context.

3.3 Attestation

Passwords, OTPs and other bearer tokens (M. Jones, Microsoft; D. Hardt, Independent, 2012) can be submitted by legitimate users or phishing servers. For the risk of a transaction, this makes a significant difference.

The relying party is typically interested in estimating the risk of a transaction. This risk depends on the transaction volume and on the assurance level of the authentication. The assurance level depends on (a) the authentication method and (b) the certainty that the legitimate user controls the relevant portions of the client device. In the case of Transaction Confirmation (see above), this could be limited to the FIDO Authenticator. In the case of Authentication it will also include the Browser / App or User Agent in general. Risk based authentication (Gregory D. Williamson, GE Money – America's, 2006) methods try to estimate (b). Authenticator attestation provides a cryptographic proof of the FIDO Authenticator being used to the relying party.

Using hardware attestation is not new, e.g. see (Vivek Haldar, Deepak Chandra, and Michael Franz; Department of Computer Science, University of California, 2004). In Public Key Infrastructures (PKIs), the hardware verification is typically being performed by the Certificate Authority before issuing the user certificate. The device policy is typically included into the user certificate as Certificate Policy OID (e.g. "id-fpki-certpcy-pivi-hardware" in the case of Federal Bridge CA, see (Federal Public Key Infrastructure Policy Authority, 2011)). User registration/identification and hardware attestation are combined into a single certificate. Relying parties verify such certificate policies included in the user certificate when validating the user certificates.

In non-PKI environments, hardware attestation and user registration/identification have to be separated. Trusted platform modules already support the concept of (pure) attestation (Trusted Computing Group, 2008) (Bare, 2006).

4 The Need for Secure Hardware

As previously mentioned, authentication requires at least one trustworthy client side component. In the case of FIDO this is the FIDO Authenticator. The security relevant functions are centralized into it. The most important security functions are:

1. Securely maintaining the attestation key and only using it for attesting newly generated authentication keys.
2. Securely maintaining the cryptographic authentication keys and
   (a) Enforcing proper user authentication before unlocking the authentication key for authentications and
   (b) Restricting its usage to cryptographic operations on defined clear-text message structures.

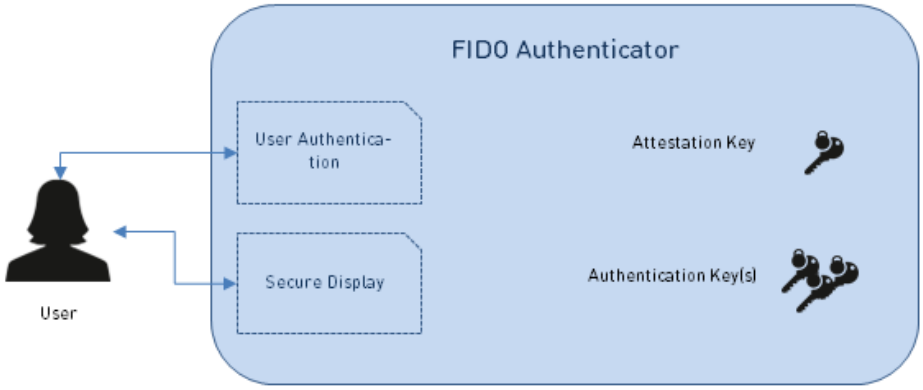


Fig. 3. Logical FIDO Authenticator Architecture

Use of secure hardware will significantly improve overall assurance level.

Existing secure hardware platforms include Smart Cards (ISO/IEC, 2004), TPMs (Trusted Computing Group, 2013), Secure Elements (GlobalPlatform, 2012), and TEEs (ARM Limited, 2009).

Some secure hardware can be accessed through standardized APIs e.g. PKCS#11 (RSA Laboratories, 2009), or Microsoft Crypto API Next Generation (Microsoft). Such APIs allow secure generation and storage of (authentication) keys (e.g. RSA keys). However, as the concept of attestation is missing by those APIs, there is no way for a relying party to be sure that a key has been generated by a specific secure hardware. Software generated keys would look the same.

Other secure hardware, e.g. ISO7816 compliant smart cards, or TPMs either support the concept of attestation by default (TPMs) or can be initialized to support that

concept (e.g. by using secure messaging). For Java Cards (Oracle), applets can be implemented to provide the security related functions of an Authenticator, i.e. Attestation, Authentication and PIN based user authentication.

Implementing all aspects of the FIDO Authenticator (i.e. User Authentication, Secure Display, Authentication and Attestation) in a TEE *and* storing the keys in a Secure Element exclusively accessible by a FIDO Authenticator Trustlet would lead to the highest assurance level.

References

ARM Limited. (2009). *ARM Security Technology - Building a Secure System using TrustZone Technology.*

B. Aboba, Microsoft; L. Blunk, Merit Network, Inc.; J. Vollbrecht, Vollbrecht Consulting LLC; J. Carlson, Sun; H. Levkowetz, ipUnplugged. (2004). *Extensible Authentication Protocol (EAP), RFC3748.* Network Working Group, The Internet Society.

Bare, C. (2006). *Attestation and Trusted Computing.*

BehavioSec. (2009). *Measuring FAR/FRR/EER in Continuous Authentication.* Stockholm, Sweden.

Benjie Chen and Robert Morris; MIT Laboratory for Computer Science. (2003). Certifying Program Execution with Secure Processors. *USENIX HotOS Workshop.*

Burnett, M. (2011, June 20). *More Top Worst Passwords.* Retrieved April 3, 2013, from Xato.net: http://xato.net/passwords/more-top-worst-passwords/

Cloud Security Alliance. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing v2.1.

Cloud Security Alliance. (2010). Top Threats to Cloud Computing, v1.0.

Confident Technologies. (2011). *Mobile (In)Security - A Survey of Security Habits on Smartphones and Tablets.*

David A. Willis, Gartner. (2013). *Bring Your Own Device: The Facts and the Future.* Gartner.

Dinei Florêncio and Cormac Herley, Microsoft Research. (2007). *A Large-Scale Study of Web Password Habits.* Redmond.

Elbert, K. N. (2013). *Understanding Consumers' Visual Attention Patterns Online: An Eye Tracking Analysis of Web Trust Seal Effects On Visual Attention and Choice.*

European Central Bank. (2012, April). Recommendations for the Security of Internet Payments. Frankfurt am Main, Germany.

Federal Public Key Infrastructure Policy Authority. (2011). *United States Federal PKI - X.509 Certification Practice Statement (CPS) for the Federal Public Key Infrastructure (FPKI).*

FFIEC. (2005, October 12). Supplement to Authentication in an Internet Banking Environment. Arlington, VA, USA.

Florian Schaub, Ruben Deyhle, Michael Weber; Institute of Media Informatics, Ulm University, 89069 Ulm, Germany. (2012). *Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms.* Ulm, Germany.

GlobalPlatform. (2012). *Secure Element Access Control.*

Gregory D. Williamson, GE Money – America's. (2006). Enhanced Authentication In Online Banking. *Journal of Economic Crime Management*, pp. Fall 2006, Volume 4, Issue 2.

Initiative for Open Authentication (OATH). (2007). *OATH Reference Architecture, Release 2.0.*

ISO/IEC. (2004). *ISO/IEC 7816-8 Commands for security operations.*

Jacob, J. C. (1997). *A Survey of Authentication Protocol Literature: Version 1.0.*

John C. McCarthy with Christopher Mines, Pascal Matzke, Yahor Darashkevich; Forrester Research. (2011, March). Mobile App Internet Recasts The Software And Services Landscape – A BT Futures Report. (F. Research, Ed.)

Joseph Bonneau, C. H. (2012). The Quest to Replace Passwords - A Framework for Comparative Evaluation of Web Authentication Schemes. *Proceedings of IEEE Symposium on Security and Privacy.* Oakland.

Koichiro Niinuma, Fujitsi Laboratories, Kawasaki, Japan; Anil K. Jain, Department of Computer Science & Engineering, Michigan State University, East Lansing, MI, USA. (2009). *Continuous User Authentication Using Temporal Information.*

KPMG. (2011). 2011 KPMG Mobile Payments Outlook.

Leicher, A., Schmidt, A.U., Shah, Y. and Cha, I. (2011). Trusted computing enhanced user authentication with OpenID and trustworthy user interface. *Int. J. Internet Technology and Secured Transactions, Vol.3*(No.4), pp. 331 - 353.

M. Jones, Microsoft; D. Hardt, Independent. (2012). *The OAuth 2.0 AuthorizationFramework: Bearer Token Usage (RFC6750).* Internet Engineering Task Force (IETF).

M. S. Obaidat, B. S. (n.d.). Keystroke Dynamics Based Authentication. In R. B. A. Jain, *Biometrics. Personal Identification in Networked Society* (pp. 213-229). Kluwer Academic Publishers.

Martha E. Crosby and Custis S. Ikehara; University of Hawaii/Manoa (USA). (2004). *Continuous identity authentication using multimodal physiological sensors.*

Microsoft. (n.d.). *Cryptography API: Next Generation.* Retrieved May 3, 2013, from Windows Dev Center - Desktop: http://msdn.microsoft.com/en-us/library/windows/desktop/aa376210%28v=vs.85%29.aspx

Oracle. (n.d.). *Java Card Technology.* Retrieved May 3, 2013, from Oracle: http://www.oracle.com/technetwork/java/javacard/overview/index-jsp-140503.html

Ponemon Institute LLC. (2013). *Moving Beyond Passwords: Consumer Attitudes on Online Authentcation - A Study of US, UK and German Consumers.*

RSA Laboratories. (2009, July 10). PKCS#11 Base Functionality v2.30: Cryptoki - Draft 4. USA.

Sally Hudson, IDC. (2011, June). Worldwide Identity and Access Management Market 2011-2015 Forecast. (IDC, Ed.) Framingham, MA, USA.

Sascha Rehbock and Ray Hunt, Computer Science and Software Engineering University of Canterbury. (2008). *Trustworthy Clients: Architectural Approaches for Extending TNC to Web-Based Environments.* Christchurch, New Zealand.

Sharon A. Mertz, Chad Eschinger, Tom Eid, Yanna Dharmasthira, Chris Pang, Laurie F. Wurster, Tsuyoshi Ebina, Hai Hong Swinehart; Gartner. (2011, September). Forecast: Software as a Service, All Regions, 2010-2015. (Gartner, Ed.)

Stefan Ried, Ph.D.; Holger Kisker with Pascal Matzke, Andrew Bartels, Miroslaw Lisserman; Forrester Research. (2011, April). Sizing The Cloud - A BT Futures Report.

Stuart E. Schechter, MIT Lincoln Laboratoy; Rachna Dhamija, Hardvard University & Commerce Net; Andy Ozment, MIT Loncoln Laboratory & Univeristy of Cambridge; Ian Fischer, Harvard University. (2007). *The Emperor's New Security Indicators.*

Trusted Computing Group. (2008). *Trusted Platform Module (TPM) Summary.*

Trusted Computing Group. (2013). *Trusted Platform Module Library - Part 1 Archutecture.*

Trusteer, Inc. (2010, February 2). Reused Login Credentials. *Security Advisory, February 2, 2010*. New York, NY, USA. Retrieved from http://landing2.trusteer.com/sites/default/files/cross-logins-advisory.pdf

Václav Matyáš and Zdneněk Říha, Faculty of Informatics, Masaryk University Brno, Czech Republic. (2002). *Biometric Authentication - Security and Usability.*

Vivek Haldar, Deepak Chandra, and Michael Franz; Department of Computer Science, University of California. (2004). *Semantic Remote Attestation - A Virtual Machine directed approach to Trusted Computing.* Irvine, CA, USA.

William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk; Computer Security Division, Information Technology Laboratory and Sabari Gupta, Emad A. Nabbus; Electrosoft Services, Inc. (2013, February). Electronic Authentication Guideline. *Draft NIST Special Publication 800-63-2*. National Institute of Standards and Technology (NIST).