Not Built On Sand - How Modern Authentication Complements Federation

Dr. Rolf Lindemann, Nok Nok Labs, Inc.

Nok Nok Labs, Inc.
4151 Middlefield Road
Palo Alto, California 94303, USA
rolf@noknok.com

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 Fast Identity Online (FIDO) Alliance has been founded to define an open, interoperable set of mechanisms that reduce the reliance on passwords.

We explain how secure hardware in conjunction with a generic protocol can help overcoming today's authentication challenges and how this protocol can be used as a solid basis for federation.

Motivation

Passwords don't work: In 2007, the average user had 25 accounts, used 6.5 passwords and performed logins 8 times a day [FlHe07]. Today, things are much worse. An analysis of 6 million accounts showed that 10,000 common passwords would have access to 98.8% of the accounts [Trus10]. This basically means that only 1.2% 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 [CSA10], 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." [CSA10]. 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 [Pone13].

Several proposals to replace passwords have been made. A good analysis can be found in [BHOS12].

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.

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.

Not all users are equal. A recent survey shows that more than two thirds of the participants in the study prefer authentication without sharing personal information, approx. 50% would accept use of a multi-purpose identity credential and 23% in the US and 40% in Germany would accept biometrics based authentication [Pone13].

The one authentication method satisfying all needs seems to be out of reach.

The FIDO Approach

We propose to (a) separate the user authentication methods from the authentication protocol and let an entity called FIDO Authenticator glue both together, and (b) to define an attestation method in order to attest the identity of the FIDO Authenticator to the relying party. Given this information, the relying party is able to infer the related assurance level (e.g. as defined in [BDN+13]). The assurance level can be fed into internal risk management systems. The relying party can then add implicit authentication methods as needed.

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 without requiring specific support in the FIDO Server and hence avoiding "silos" of authentication. Successful user authentication unlocks the relying party specific cryptographic authentication key.

The FIDO Protocol

The FIDO protocol supports the functions Discovery, Registration, Authentication and Transaction Confirmation.

The discovery enables relying parties to explore user authentication methods supported by the user's computer and hence handle heterogeneous client environments. The relying party can specify a policy for selecting FIDO Authenticators best suited for the specific purpose.
As part of the registration operation, the FIDO Authenticator generates a key pair specific to the relying party. The relying party binds the public key to a specific entity. This might be an existing user identity already present in the relying party's system or it

might be a user identity to be created. Using a dedicated key for each relying party enhances the user's privacy as two relying parties cannot link transactions to the same user. Storing only the public key at the relyiung party makes the FIDO protocol resililient to leaks from other verifiers.

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 [ECB12]. 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 approve 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 session.

This leads to the following reference architecture:

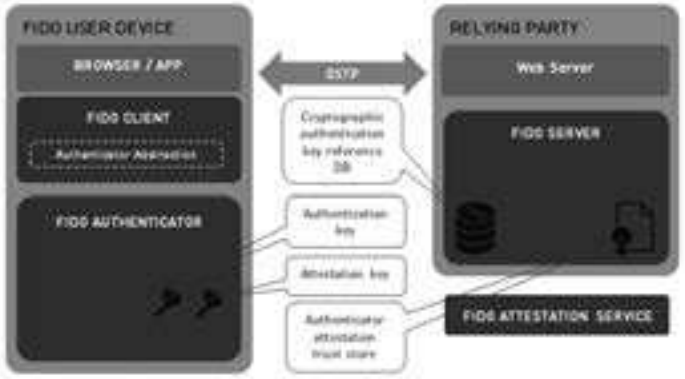

Fig. 1. FIDO Reference Architecture

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 and hence avoid additional costs, e.g. Microphones (→ Speaker Recognition), Cameras (→ Face Recognition), Fingerprint Sensors, or behavioral biometrics [ObSa].

Attestation

The relying party is interested in estimating the risk of a transaction. This risk depends on the assurance level of the authentication (and other factors). 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, 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 [Will06] methods try to estimate (b). Authenticator attestation provides a cryptographic proof of the FIDO Authenticator being used to the relying party, addressing (a). Trusted platform modules already support the concept of (pure) attestation [TCG08].

The FIDO Authenticator maintaines cryptographic authentication keys and performs the user authentication. The attestation provides a cryptographic proof of the Authenticator model to the relying party and hence allows the relying party to infer the assurance level from it.

FIDO and Federation

From a user's perspective, Federated Identity Management is a method that allows accessing privileged information across autonomous security domains after authenticating once. From an organization's perspective, it also "… allows organizations like enterprises and service providers to securely exchange user information across partners, suppliers and customers." [LaMo12]. InCommon is one example of successful real-world federation systems. SAML and OpenID Connect are examples for popular federation standards.

Federated Identity Management systems expect the user to authenticate to an Identity Provider (IdP). This user authentication method is relevant to the IdP, but not directly in the scope of current federation standards. Most IdPs still use password based authentication.

FIDO addresses this "first mile" authentication of the user to the IdP while leaving the user vetting up to it. FIDO protocol makes reliable information about the authentication assurance level available to the IdP ($\rightarrow$ attestation). Some of the federation standards[1] already support sharing this knowledge with the service provider. This enables IdPs to support heterogeneous authentication methods and it enables service providers to make informed decisions about the transaction risk.

References

[BDN+13] 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., "Electronic Authentication Guideline," National Institute of Standards and

[1] E.g. OpenID Provider Authentication Policy Extensions v1.0.

Technology (NIST), 2013.

[BHOS12] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano, "The Quest to Replace Passwords - A Framework for Comparative Evaluation of Web Authentication Schemes," in *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, 2012.

[Burn13] M. Burnett, "More Top Worst Passwords," 20 June 2011. [Online]. Available: http://xato.net/passwords/more-top-worst-passwords/. [Accessed 3 April 2013].

[CSA10] Cloud Security Alliance, "Top Threats to Cloud Computing, v1.0," 2010.

[ECB12] European Central Bank, "Recommendations for the Security of Internet Payments," Frankfurt am Main, 2012.

[FlHe07] D. Florêncio and C. Herley, Microsoft Research, "A Large-Scale Study of Web Password Habits," Redmond, 2007.

[LaMo12] S. Landau and T. Moore, "Economic tussles in federated identity management," 1 October 2012. [Online]. Available: http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/4254/3340. [Accessed 7 February 2013].

[ObSa] M. S. Obaidat and B. Sadoun, "Keystroke Dynamics Based Authentication," in *Biometrics. Personal Identification in Networked Society*, Kluwer Academic Publishers, pp. 213-229.

[Ping10] Ping Identity, "The Primer: Nuts and Bolts of Federated Identity Management," 2010.

[Pone13] Ponemon Institute LLC, "Moving Beyond Passwords: Consumer Attitudes on Online Authentcation - A Study of US, UK and German Consumers," 2013.

[TCG08] Trusted Computing Group, "Trusted Platform Module (TPM) Summary," 2008.

[Trus10] Trusteer, Inc., "Reused Login Credentials," New York, 2010.

[Will06] Gregory D. Williamson, GE Money – America's, "Enhanced Authentication In Online Banking," *Journal of Economic Crime Management,* pp. Fall 2006, Volume 4, Issue 2, 2006.