Kim Nguyen

Authentification and Identification – Taking the User into Account

Username/Password is still the prevailing authentication mechanism for internet based services – but it is not secure! We show how new authentication and identification mechanisms focused on usability and security can change this.

1 Introduction

Security breaches in the context of web based services and networks are everywhere, ranging from stolen passwords to the hijacking of complete digital identities. The heartbleet phenomena has shown that even existing protocol frameworks can be used for password exploitations, that even cannot be detected by standard systems.

From a technological perspective, hardware based (two factor) authentication is a good answer to many of these challenges, however one has to concede that a broad acceptance for these mechanisms is clearly missing outside certain small closed user groups.

We argue, that this is not due to the lack of technical functionality, but rather due to the lacking user acceptance.

The game can only be won when a concept can be found in which user acceptance, security, privacy and easy integration can be combined.

We aim at introducing such a new concept in this article[1].

2 IT technology - past and present

From the perspective of today, the availability of IT technology and services can hardly be compared to that of twenty years, ago, maybe even not with that of five years ago.

Today's smartphones, and in fact it is quite hard NOT to receive such a phone with a new mobile contract, are using greater ressources of memory, processing capabilities and support a multitude of interfaces of various types and thus exceed typical PCs as in use only a few years ago.

Furthermore new mobile devices are always connected with the internet, while ten years ago internet connectivity has to be implemented manually via the landline. But even more striking than all these technological dimensions is the focus on usability and applications that sets new benchmarks that need to be met by all the connected technologies as well. For the first time in the history of large scale distribution of IT technology, the user can focus on the application itself - and not the underlying technologies.

The comprehensive usage of smartphones and tablets as a universal channel to perform transactions of various sorts is in many situations already reality, and will certainly become even more dominating for coming generations of users. (even accepting the fact that PCs will still be existing and in use). It is therefore clear that mobile devices of various sorts have already established themselves as a primary digital communication channel and hence as the prevalent key to services of different types.

The user experience that comes along with these new types of mobile devices, i.e. the complete focus on usability and intuitive handling, also has impact on the way how to implement and integrate mechanisms providing more security for the mentioned various services and applications, especially when these security mechanisms rely on hardware token or such like. Token based authentication will only prevail, when a deep integration of these mechanisms in the underlying operating system or applications is guaranteed. Formerly common ways of integration (implying and including installation of additional software components and of reader devices) will no longer be acceptable to users that have been growing up within a application focussed IT world.

Do we need additional security mechanisms at all? This is certainly the cases, and especially so in the case of mobile devices, where most or all applications typically are secured only by username/password, a mechanism that neither has the required strength (especially if the user chooses to use same passwords over different applications) nor can be secured by the service providers in the appropriate way (every day brings us new indications of thousands and in some cases even millions of stolen passwords). Given the omnipresence of mobile devices in various application scenarios, it is on the other hand clear that more security is needed in order to secure at least critical services (either having a „financial" dimensions, i.e. online banking or payment, or having an „identity related" dimension, i.e. takeover of an identity in a social network).

The new application focussed world of IT users is opportunity as well as challenge for the providers of security tokens and

1 The author would like to thank Frank Byszio (Bundesdruckerei GmbH) for intensive and fruitful discussions on the topics discussed in this article.

Dr. Kim Nguyen

Chief Scientist Security,
Bundesdruckerei GmbH
Managing Director, D-Trust GmbH

E-Mail: Kim.Nguyen@bdr.de

technology: only if these will be compatible both technologically as well with respect to the user experience will they experience a larger acceptance.

3 Our technology - your problem

The offering of companies in the security business is still largely dominated by making available software modules (e.g. antivirus or encryption software) hardware (e.g. firewalls or other appliances) mostly in conjunction with associated tokens (chipcards or other form factors).

Todays offering is therefore still dominated by „technology" and not by „function/application". In this model the potential customer is requested to understand the problem he wants to solve and therefore to purchase the required technology building blocks to deal with this problem using the aforementioned providers.

Therefore in this scenario the providers wants to be seen and understood as provider of technology and not solutions. Furthermore in this context the user is in the end his own solution provider that builds the solution for his specific problem on the basis of the technology building blocks purchased.

However considering the fact that the dramatic increase of mobile usage is mostly based on operating systems like iOS and Android, which are totally focussed on Applications/Apps/solutions, the user here does not have the need to assemble different elements and combine them into one specific configuration. Hence, the main difference with respect to the previous situation, complete functionality and not only technologies are provided.

Considering the acceptance of token-based mechanisms this means in turns:

Not the functionality itself is of importance, but the integration of the token into a larger application context is where the user can experience a significant difference. Technologywise this implies especially that the integration should be both seamless as well as requiring only the absolute minimum of unser interaction. This especially implies that components should be provided either in pre-existing components of the operating system or should be provided server based. Furthermore existing interfacing technologies should be preferred as compared to additional interfaces that are being provided especially by additional hardware components.

The approach of the FIDO (Fast IDentity Online) Alliance, which will be introduced in the next section, follows this approach closely.

4 The FIDO approach

The FIDO Alliance is a non-profit organization nominally formed in July 2012 to address the lack of interoperability among strong authentication devices as well as the problems users face with creating and remembering multiple usernames and passwords. The FIDO Alliance aims at changing the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. This new standard for security devices and browser plugins will allow any website or cloud application to interface with a broad variety of existing and future FIDO-enabled devices that the user has for online security. FIDO has gained a remarkable momentum over the last twelve months.

The FIDO falls in two main categories to address a wide range of use cases and deployment scenarios. FIDO protocols are based on public key cryptography and are strongly resistant to phishing.

▸ **Passwordless user experience:**

The passwordless FIDO experience is supported by the Universal Authentication Framework (UAF) protocol. In this experience, the user registers their device to the online service by selecting a local authentication mechanism such as swiping a finger, looking at the camera, speaking into the mic, entering a PIN, etc. The UAF protocol allows the service to select which mechanisms are presented to the user.

Once registered, the user simply repeats the local authentication action whenever they need to authenticate to the service. The user no longer needs to enter their password when authenticating from that device. UAF also allows experiences that combine multiple authentication mechanisms such as fingerprint + PIN. For details refer to [1, FIDO UAF Architectural Overview].

▸ **Second Factor User experience:**

The second factor FIDO experience is supported by the Universal Second Factor (U2F) protocol. This experience allows online services to augment the security of their existing password infrastructure by adding a strong second factor to user login. The user logs in with a username and password as before. The service can also prompt the user to present a second factor device at any time it chooses. The strong second factor allows the service to simplify its passwords (e.g. 4–digit PIN) without compromising security.

During registration and authentication, the user presents the second factor by simply pressing a button on a USB device or tapping over NFC. The user can use their FIDO U2F device across all online services that support the protocol leveraging built–in support in web browsers.

The core ideas driving FIDO are (1) ease of use, (2) privacy and security, and (3) standardization. For implementing authentication beyond a password (and perhaps an OTP), companies have traditionally been faced with an entire stack of proprietary clients and protocols.

FIDO changes this by standardizing the client and protocol layers. This ignites a thriving ecosystem of client authentication methods such as biometrics, PINs and second–factors that can be used with a variety of online services in an interoperable manner. For details refer to [1, FIDO U2F Architectural Overview].

▸ **Online Crypto Protocol Standardization:**

FIDO standardizes the authentication protocol used between the client and the online service. The protocol is based on standard public key cryptography — the client registers a public key with the online service at initial setup. Later, when authenticating, the service verifies that the client owns the private key by asking it to sign a challenge. The protocol is designed to ensure user privacy and security in the current day state of the internet.

▸ **Client Standardization for Local Authentication:**

FIDO standards define a common interface at the client for the local authentication method that the user exercises. The client can be pre–installed on the operating system or web browser. Different authentication methods such as secure PIN, biometrics (face, voice, iris, fingerprint recognition, etc.) and second–factor devices can be "plugged in" via this standardized interface into the client.

5 FIDO and beyond - the role of identity based mechanisms

As described in the previous section the FIDO approach focuses mainly on the topic of authentication in two ways, namely u2f (strengthening a primarily username/password based infrastructures) and uaf (replacing password with various authentication possibilities).

For those use cases, where the authentication should also include a token based identification complementing the authentication, typically a Certification Authority (CA) comes into play.

Technically speaking we are referring here to certificate based mechanisms relying mostly on the definitions of the X.509 standard. However we would like to point out here that the main role of a CA lies in fact far beyond these technical considerations, the CA is in fact an institution that provides trustworthy services, amongst which the most prominent is that of reliable ID verification.

This is typically a new point in the discussion of the main properties of a CA, as these discussion mostly focus on technical matters, i.e. how is the certificate produced, how ist he key material handled, how are technical specifications adhered to. As any PKI based authentication mechanism relies on all these matters for its successfull technical completion, all this points are well worth considering, however the core of a „Trust service provider" needs a much broader discussion.

The certificate a CA issues is on the ohe hand a digital object, that can be used in various technical contexts. However, such a digital object may be produced by almost anyone technically versatile enough to set up the appropriate software and generate his own CA. Technically these certificates do not differ at all from those that are issued by a professional CA, so what is in fact the difference?

▸ **The paramount difference is a deeply non-technical one:**
The certificate is much more than the digital object representing the certificate, it ist he manifestation of a process which in its core takes a conventional identity (e.g. an identity related to a person on the basis of an ID document) and transform this identity into another one – a derived identitfy - that is more suitable for usage in the relevant application context (e.g. a X.509 based certificate, a SAML token etc.).

Thus, the trust provided in the manifestation of a certificate etc. is mainly based not on technical issues but on the trustworthiness of the underlying processes, the high quality of the provided ID data as well as on the possibility for third parties to verify the integrity of the provided identity (based typically on technologies like OCSP, ldap etc.)

Only on the basis of such a trusted identification and verification ecosystem can a token integration into applications guarantee the provisioning of trustworthy and verifiable identities.

Different applications and the related transactions will require different levels of trustworthiness, as they typically will have different economic impact and intrinsic value. Hence also different trust levels should be used to reflect this observation in the context of token based authentication and identification within the mentioned identification and verification ecosystem. This is in fact something quite well known as we use such a layered approach to identification and authentication in everyday life: Different identification is needed when buying a house as opposed to entering the gym for the daily workout (to name two rather contrasting use cases), and when transferring authentication and identification from the "analogue" to the digital world, this is something that user expect to recognize in the new technologies as well.

But not only the process of identification and verification is of interest, this holds also for the process of the delivery of the derived identity to the user.

While in the "classical" world, the delivery is mostly restricted to providing the certificate on a suitable physical carrier (i.e. card or another physical token), in the new application- and integration scenarios different ways of delivery come to mind.
This especially refers to the fact, that the user already possesses a physical token, that can be used for authentication purposes (e.g. u2f or uaf enabled), but would like to add identity based mechanisms to the functionality of the token.

In this case, a purely digital post-issuance scenario is attractive, in which the process of verification of an identity was already performed successfully (as the user is already known via his user account), or can be performed instantaneous using his ID or eID documents (preferably on the basis of mobile devices, like smartphones).

This is already reality for the German eID card using the sign-me system operated by Bundesdruckerei GmbH and D-Trust as trust service provider (see [2]), which can be used both as a means of identification as well as a carrier for a qualified certificate – in both cases fully digital and without the necessity for the user to handle paperbased documents at all.

The future lies clearly within the integration of various identification ways (resulting in different assurance levels as discussed above), preferably based on mobile usage, as well as new post-issuance scenarios, especially using token that are already well established with the user, for example from u2f or uaf authentication scenarios.

6 Conclusion

Summarizing, the future of hardware based authentication will rely on the following facts:

- Gaining user acceptance by deep and easy integration of hardware and software into applications
- Accepting the fact that authentication and identification will need to rely on a layered approach using different assurance levels ranging from simple token based recognition up to identification on the highest level
- Providing means to "upgrade" the functionality as needed in the moment of the interaction with an appropriate service

The combination of the existing trust service provider portfolio with new token functionality and token integration offers a unique opportunity to provide strong authentication and/or identification where and when need arises.

References

[1] https://fidoalliance.org/specifications/download
[2] https://www.bundesdruckerei.de/en/798-sign-me