Use of SIM Card Authentication in the Open Web Platform

John Mattsson, Ericsson Research

Abstract. It's time to move "beyond passwords", not only for high-value environments such as the financial industry and government, but for all types of web applications. Most mobile devices already have a hardware token suitable for authentication, the SIM card. To not make use of that is a waste. This hardware-based authentication should also be available to web application developers interested in using secure and user-friendly authentication.

1. Introduction

The most commonly used client authentication method on the web today is HTML form-based authentication with the user entering username and password. The weaknesses with passwords are well known; they offer weak security and bad usability, especially on mobile devices. It's time to move "beyond passwords", not only for high-value environments such as the financial industry and government, but for all types of web applications.

Ways to enable more secure authentication include multi-factor authentication and the use of hardware tokens. Web applications may give the user a second password, a hardware token, or send a verification code to the user's mobile phone. None of these are very user friendly, and the last one fails to give two-factor authentication if the web application is accessed from a mobile phone.

The fact is that more and more browsing is done from a mobile browser instead of a desktop one. The number of mobile broadband subscriptions is currently over 2.3 billion and is predicted to rise to 7.6 billions by 2019 [1]. For most people in the world, the mobile browser is the only browser they have access to. Another fact is that most mobile devices (those using GSM, UMTS, and LTE) already have a hardware token suitable for authentication, the SIM card. To not make use of that is a waste. Even if many mobile apps are not pure web apps, a large portion of them is so called hybrid apps; apps built using web technologies and rendered by the device's browser engine, but delivered from an app store inside a native container.

3GPP has standardized GBA [2], enabling third-party web applications to reuse the SIM card for strong hardware based authentication, suitable for use-cases in high-value environments such as the financial industry. The use of GBA has been held back by lacking network and device support, but this is changing with the introduction of LTE (i.e. 4G) and VoLTE (Voice over LTE). As VoLTE makes use of GBA, there is increasing support of GBA in both mobile networks and devices. This strong and user-friendly hardware-based authentication should also be available to web applications.

The "SIM card" is a general reduced-size smart card that consists of CPU, ROM, RAM, EEPROM and I/O circuits, and the (U)SIM application is just one of many applications. The SIM card is also well suited for secure storage and processing of authentication applications such as national eID systems. Mobile PKIs where the private key is stored on the SIM cards has been deployed in many European countries [3]. The SIM card is also an important part of the World Bank's project 'Secure Electronic Identity for Africa'.

One benefits of using hardware-based authentication such as GBA is the significantly increased protection against key extraction, another is the improved user experience of the end user. The SIM card and GBA does not have to be the only authentication mechanism, they can also be used as a part of strong multi-factor authentication solutions. Many web applications are currently using the mobile phone (via text messages) as a second authentication mechanism, GBA is a better and more secure way of accomplishing that.

2. GBA Architecture

The SIM card enables strong hardware-based mutual authentication between the mobile phone and the operator. Generic Bootstrapping Architecture (GBA) [2] is a technology that enables third-party authentication and authorization providers to reuse this hardware-based authentication so that it can easily be used by web applications. There are two ways to implement GBA in a browser:

- HTTP Digest, where the browser performs the authentication via HTTP headers [4].
- JavaScript API, where the web application can request an authentication token [5].

In both cases the GBA functionality would be implemented in the SIM card/mobile chipset/operating system and the browser would only have to implement a few calls to fetch the authentication token. The JavaScript API alternative is the most flexible one, and the one most suitable for adoption in the Web Cryptography API.

GBA can easily be integrated into other authentication protocols such as OAuth and OpenID, see e.g. [6]. A high-level illustration of GBA is given in Figure 1. Web applications would use standard web technologies, only the auth provider needs to implement parts of the open 3GPP standards [2]. Larger web application providers could take the role of the auth provider and communicate directly with the operator.

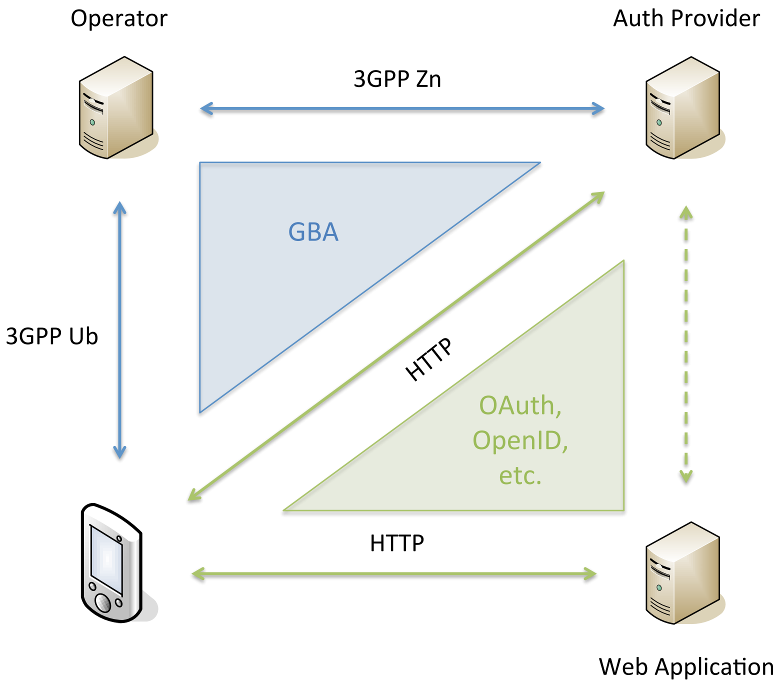

Figure 1: Architecture for SIM card authentication (GBA)

The Operator is only involved in the authentication and do not have access to any encrypted information sent between the Web Application and the browser.

3. Conclusions

It's time to move "beyond passwords", not only for high-value environments such as the financial industry and government, but for all types of web applications. To meet the demands from the industry sectors with high security demands as well as ordinary web developers, W3C should strive to make authentication part of the Open Web Platform, and enable interaction of various secure “beyond passwords” authentication systems with the Web Cryptography API and other Web APIs.

More and more browsing is done from mobile devices that already have a hardware token suitable for authentication. SIM card authentication can, not only provide strong hardware based authentication, it can also be used to provide a better seamless user experience. Authentication needs to be done in a secure, developer-friendly, and user-friendly way. As VoLTE makes use of GBA, there is increasing support of GBA in both mobile networks and devices. This hardware-based authentication should also be available to web application developers interested in using secure authentication.

References

[1] Ericsson, “Ericsson Mobility Report”, June 2014
http://www.ericsson.com/ericsson-mobility-report

[2] 3GPP TS 33.220 “Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)”
http://www.3gpp.org/DynaReport/33220.htm

[3] UL Transaction Security, “Electronic Identities in Europe”, 2013
http://www.ul-ts.com/downloads/whitepapers/finish/6-whitepapers/114-electronic-identities-in-europe

[4] 3GPP TS 33.222 “Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)”
http://www.3gpp.org/DynaReport/33222.htm

[5] 3GPP TR 33.823 “Security for usage of General Bootstrapping Architecture (GBA) with a User Equipment (UE) browser”
http://www.3gpp.org/DynaReport/33823.htm

[6] 3GPP TR 33.924 “Identity management and 3GPP security interworking; Identity management and Generic Authentication Architecture (GAA) interworking”
http://www.3gpp.org/DynaReport/33924.htm