Banrisul

Position Paper submitted to the W3C Workshop on "Authentication, Hardware Tokens and Beyond"

nascent Technology Consultants

Beyond Online Authentication

- an e-banking and e-government perspective -

Sean Michael Wykes – CTO – Nascent Technology Consultants
sean.wykes [at] nascent.com.br

Statement of Interest

The author has been closely involved with the design and integration of secure authentication technologies for web environments during the last 12 years, in the financial, corporate and government application domains, and wishes to state his interest in participating in the workshop both on behalf of Banrisul S.A.* – the state bank of *Rio Grande do Sul*, Brazil – and Nascent Technology Consultants**.

Given the existence of entire categories of malware, banking Trojans for example, specifically designed for attacking online authentication mechanisms, the practical experience that financial institutions such as Banrisul S.A. have acquired in the detection and prevention of such menaces, including the commissioning and implementation of specific countermeasures within their authentication services, should prove to be of relevance to the workshop.

Introduction

A W3C initiative that enables the integration of strong authentication mechanisms within web applications will be a vitally important step towards a more-secure web. Naturally, this initiative and any resultant API or framework should aim to carefully balance flexibility, usability and the underlying security principals so as to ensure both adequate security levels and successful adoption rates.

Looking beyond strong authentication, however, there are a number of important use-cases from the financial and governmental domains that extrapolate the requirements for online authentication into the realm of digital-signatures. These use-cases include the provision of transaction-oriented signatures of the "e-banking", "e-government" and "e-business" type, as well as generalized digital-signatures for web-documents and files.

Experience has shown that while such use-cases share many of the same characteristics and issues as secure online authentication, they often demand additional functionality and enhanced security mechanisms. In this respect, in order for a W3C standard for strong web authentication to be effective, its scope should ideally contemplate some of these more advanced use cases.

Real World Use Cases

The following section briefly presents a number of use cases, in real-world web-applications and application domains.

E-Banking Application: Banrisul S.A.

Banrisul S.A. has issued nearly 5 million multi-application smart-cards to its current account customers. In addition to debit and credit applications, these cards are widely used for online authentication and digital-signature functions, as a result of their support for public-key cryptography, in conjunction with bank-issued PKI certificates.

Banrisul's browser-based e-Banking portal delegates to a Java-applet for authentication and signature functions. Such functions range from low-level smart-card reader accesses to trusted user interactions such as PIN entry and transaction confirmation. Security policies are in place

that enforce 100% of all payment or fund-transfer transactions to be digitally-signed, resulting in the bank having successfully reached and maintained ZERO fraud levels on all internet channels for the past four years or so. Additional countermeasures have also been incorporated into the Java-applet to protect against diverse forms of malicious software, including mutual-authentication as a defense mechanism against Man-in-the-Browser-style attacks, in which live JavaScript is compromised.

Online Corporate Authentication: Banrisul S.A.

Approximately 15,000 Banrisul employees and sub-contractors are equipped with a corporate smart-card for network login, authentication and digital-signature purposes. Significant numbers of intranet- and extranet-based web-applications have been designed for mandatory use of secure authentication, and additionally, a number of workflow applications require digital signatures for accountability during privileged administrative processes.

E-Government: Brazilian PKI Scheme

"ICP-Brasil" is the Brazilian government-regulated PKI Scheme, based on smart-cards and other cryptographic tokens for secure key storage. These cards are widely used for secure authentication and digital-signatures through a range of applications at both Federal and State levels. Through government mandates, innumerous areas of government are rapidly being transitioned towards fully online and paperless operation, including taxation, invoicing, public pensions and even the legal system, where paperless petitions and secure online access for barristers is becoming the norm.

For authentication purposes, the hardware cryptographic token is used in conjunction with TLS client authentication methods, thus requiring local installation and configuration of platform-specific components. When digital signature functionality is needed by a web-application, additional browser plug-ins and components are required, many of which are based on Java applets for the signature and presentation layers.

Lessons Learned

Many factors influence the success and security properties of an authentication and signature framework. The following issues would appear to be of fundamental importance in the context of strong web authentication.

Usability and user comprehension

Overall security is a result of both usability and secure technology. User authentication inevitably involves human interactions, and the average user must be able to easily understand why authentication is being requested and for what purpose or in which context, in order to be able to make a rapid decision as to whether to authenticate or not.

Trusted and Unforgeable Authentication Interface

Given the widespread incidence of malware and phishing, one of the most critical aspects for secure authentication is the provision of an easily-identifiable but simple to comprehend trusted interface – a trusted-path. In an authentication context, the user should be able to unmistakably recognize that he/she is securely authenticating via the browser user-agent, and is not being phished or otherwise. This unforgeability must of course apply to any visible information related to the site and authentication context, such as authenticated domain and web-application names.

For web-applications that require digital-signature functions, a trusted interface should ideally be able to accurately represent whatever transaction or document is about to be signed by the user, based on the WYSIWYS principle – *What You See Is What You Sign*.

Cross-browser, cross-platform and cross-device compatibility

To achieve large-scale acceptability, a secure authentication token should be readily usable across a wide-range of different platforms and devices. The wide diversity that exists between browsers, operating systems and device connectivity options has historically been one of the major stumbling blocks that has prevented the widespread adoption of hardware authentication tokens.

Many existing authentication solutions depend on installable components: "Cryptographic Service Providers" such as Microsoft CAPI or PKCS#11 libraries, custom browser-specific extensions or Java-applets. In addition to the platform and browser-specific nature of many of these components, evidence suggests that some, if not all, of these solutions may present significant security risks, in part due to the need for direct access to device and operating systems functions. As a result of this, cross-browser support for such components is gradually becoming more and more restrictive, through the use of software sandboxing technologies or due to removal of support for low-level native APIs such as NPAPI.

At the same time, existing smart-card-based solutions are being heavily impacted by the restricted and non-standard support for smart-card readers on mobile devices, although the increasing integration of embedded secure-elements (smart-card-like components) may offset this in the medium term.

Easy and Secure Integration into web-applications

Even the most secure technological solution is worthless if it cannot be easily and effectively integrated into web and mobile applications. Recent approaches to authentication, such as FIDO, look to increase compatibility by standardizing the higher-level protocols and framework APIs, abstracting away lower-level details in a similar way to existing cryptographic-token standards such as PKCS#11 and Microsoft CAPI are able to abstract details of the token hardware. Although specific client-side plugins will still be required, FIDO includes a discovery mechanism that aims to facilitate application integration with different authentication solutions and options.

Security Considerations

Experience with e-Banking applications leads us to understand that an authentication API which targets integration with web-applications should be designed to ensure that Phishing Attacks, Man-in-the-Middle / Relay Attacks and, perhaps most importantly, sophisticated attacks such as Man in the Browser, can be prevented. A Man-in-the-Browser attack is characterized by a partial compromise of the browser environment itself, either through injection of malicious JavaScript, or via the action of a malicious plug-in.

In an ideal world, an authentication API should provide a means of blocking "forged" accesses, thus preventing spoofing of authentication sessions by malicious JavaScript. Giving that code-signing techniques are either not applicable to JavaScript, and/or not widely supported, this turns out to be a somewhat difficult task.

One alternative may involves the use of mutual authentication protocols, in which cryptographic authentication of the server is an integral part of the user-authentication process, being an obligatory prerequisite for user-authentication to take place.

As a contrived example in a digital-signature application context, the data or document to be signed by the user could first be digitally-signed by the server, such that a user-signature would only be generated after successful validation of the server's signature by the client software, or preferable, by the hardware token.

Conclusions

Although FIDO can be considered an emerging standard, being still somewhat immature and relatively untested in large-scale rollouts, it has been designed to address and offer adequate solutions to many of the major problems encountered with secure authentication systems. One of the big questions for this workshop appears not to be if any future W3C standard should allow use of FIDO client APIs and devices, but whether other existing standards (PKCS#11, OpenSC, CryptoAPI, ISO7816) or even alternative and proprietary solutions should be supported, and how?

On the other hand, the increasingly restricted support available for native browser plug-ins may potentially lead to the exclusion of significant numbers of applications from use of web technologies and browser environments, if alternative and secure methods of performing digital-signatures are not found. FIDO currently does not offer support for general digital signatures, functionality that we hope to have demonstrated to be fundamentally important in a range of specific application domains.

How can these deficiencies be addressed by the W3C initiative? Should W3C include support for such functionality in a future specification, could the FIDO alliance assume responsibility for this, or shall the integration problems continue to be addressed via separate, non-standard and often isolated initiatives?

About Banrisul S.A.*

Banrisul S.A. is the State Bank of *Rio Grande do Sul* in Brazil. Founded in 1928, it is present in more than 500 cities and reaches more than 80% of the state's population. A true technology pioneer, Banrisul's multi-application smart-card project has consistently pushed the boundaries in the Latin American region, having gained international recognition, including best project and innovation awards from diverse organizations such as the Smart Card Alliance, MasterCard and the Cartes Congress.

About Nascent**

Since 2001*, Nascent Technology Consultants* has been actively involved in the design, development and rollout of web-based authentication systems for banking, corporate and e-government applications in Brazil and Latin America, including a number of smart-card based cryptographic tokens, client-side middleware and browser plugins, as well as host-side authentication and validation components.