Strong Authentication for Future Web Applications

Chris Williams
Leidos, Inc.
July 18, 2014

For W3C Identity in the Browser Workshop

Abstract

Leidos (formerly SAIC), has been using strong authentication within its enterprise for over a decade to protect Internet access to its resources and protect against advanced cyber threats. We have watched the US government attempt to adopt strong authentication, first through the HSPD-12 mandate for smart card badges for all employees and contractors, and later with the OMB 11-11 mandate for all new information systems to be enabled for HSPD-12 credentials for logical authentication. Yet, we have watched as adoption rates have remained low, implementation has been difficult, expensive, and seldom executed well, and the government has failed time and time again to realize the full business value of its investment.

Now, with the advent of mobile and cloud, we have a new opportunity to do authentication on the Internet well, and with more at stake than ever before. Leidos would like to ask that the W3C consider the full and complex use cases for strong authentication, and design present and future protocols to support those use cases in a manner that is straightforward and "secure by default".

Strong Authentication at Leidos

Leidos (formerly SAIC) was an early adopter of strong authentication technology going back to the late 1990s using one-time password tokens, and evolving to include smart cards, smart card badges, and most recently, hybrid token devices that combine the capabilities of smart cards and one-time-password tokens into a single device. In addition to these strong authentication capabilities, we use smart card logon to our computers, strong authentication for system administration accounts, and digital signature and encryption for documents and e-mail. All of this in an environment with over 23,000 employees, with over 50% of them using strong authentication, digital signature or encryption capabilities in some way or another on a daily basis. See figure below for a graphical representation of this roadmap.

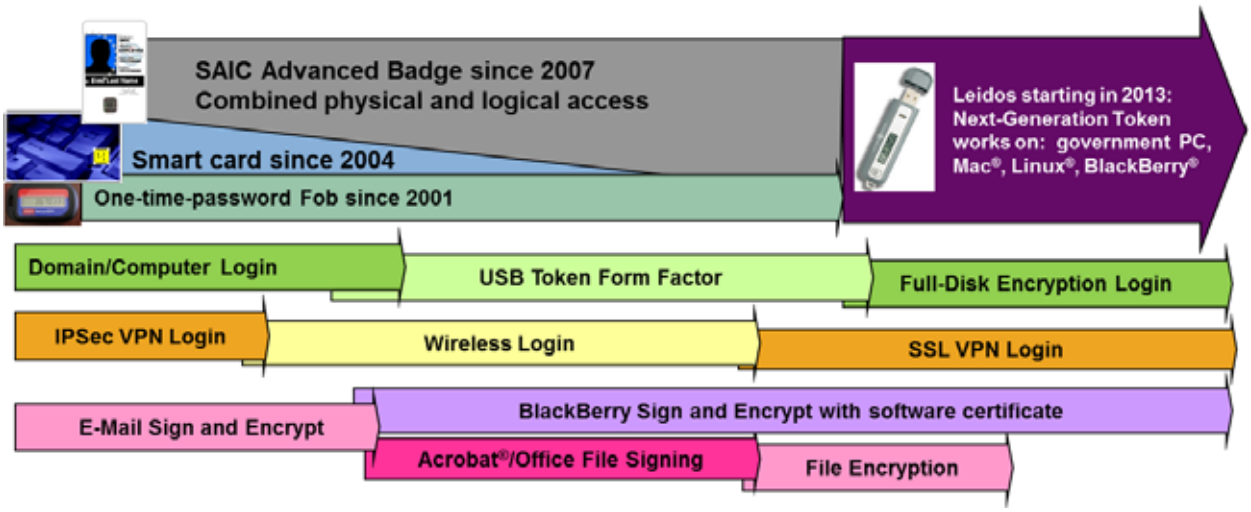

Figure 1: SAIC/Leidos strong authentication over ten years

Strong Authentication in the US Government

Strong authentication at the US Government goes back more than 15 years, to the Department of defense Common Access Card and various token technologies before that. While one can debate the philosophical merits endlessly, the fact is that the US government has committed seriously to smart card technology, through HSPD-12, FIPS-201, SP800-73, and OMB 11-11. Of course, the challenge with smart cards is the form factor and the fact that a reader of some type is required for a computing device to be able to read the card. This introduces the "challenge of the last inch" which is made significantly more difficult in a mobile environment. As they say, "there ain't no smart card reader on an iPad." Because of these facts, the US government has some challenges on its hands right now, and the answer to those challenges is a new idea called Derived Credentials.

Derived Credentials

The concept of derived credentials is very simple. Start with a high-grade credential that is trusted, and use that credential to authenticate and authorize the issuance of additional credentials that are in form factors, on platforms, or use interfaces that are more useful than the original high-grade credential. The policy for this is still under development, but the theory behind the concept is quite simple. Using derived credentials, the government is hoping to make strong authentication capabilities – and digital signature and encryption capabilities as well – available on the myriad of endpoint, mobile and BYOD devices that are out there, and enable them to interface with cloud services for the next decade. The key thing with the derived credential is the integration of the identity lifecycle so that the derived credentials and other devices can be managed according to the same lifecycle as the parent credential, and so that the entire credential issuance process has the required level of assurance.

Figure 2: Derived credentials concepts.

The Great Cryptography Evolution

At the same time that all of this is going on, we are in the middle of a tremendous transition with regard to cryptography on the Internet. As the Heartbleed debacle showed, even widespread cryptography implementations are subject to flaws and vulnerabilities, but what it failed to emphasize is the fact that a large percentage of Internet cryptography is inadequate to begin with. In particular, the following five transitions are all taking place right now:

1. SSL: SSL 3.0 to TLS 1.0, then 1.1, then 1.2
2. Digital Signature: MD5 to SHA-1 to SHA-256
3. Encryption: Triple-DES to AES
4. RSA Key size: 1024 bits to 2048 bits and larger
5. Asymmetric Algorithms: RSA to Elliptic Curve or alternatives

Mostly, what this transition shows us is that for strong authentication based on cryptography, constant change must be assumed. The "secure" cryptographic standard of yesterday is going to be the Achilles heel of tomorrow, and organizations and protocols need to be prepared for this change to continue and perhaps even accelerate in the future.

Implications for the W3C

What does all this mean for the W3C? It means that there is no "one-size-fits-all" for strong authentication. It means that the concepts and processes for "strong" authentication are going to get more complex – most likely much more complex – before they get simpler. It means that authentication protocols need to flexible and modular to accommodate a variety of technology plugins, and to allow users to authenticate with whatever strong authentication method they have at their fingertips at that moment. It means that the strong authentication method that you used five minutes ago may not be the one that you want to use now, and you need your web applications to be flexible enough to accommodate that reality.

Implications for Web Authentication

At SAIC/Leidos, we have found that one size does not fit all. At SAIC, we deployed a strong authentication web portal that supported up to eight different strong authentication technologies, all side-by-side:

Figure 3: SAIC Strong Authentication logon portal

We custom-developed this portal technology to meet our needs, but we really would like to see capabilities like this "out of the box", and fully integrated with federated authentication as well as legacy back-end authentication technologies. The fact is that authentication is terribly complex, involving large numbers of technologies and protocols, and we need to make this simpler across the board if we are going to make it simpler, cheaper, more secure and more robust for everyone.

Requirements for Web Authentication

Leidos would like to ask the W3C to ensure that future web authentication protocols are designed from the start to accommodate the following requirements:

1. "Pluggable" architecture for strong authentication, with no assumptions about how the authentication protocol is to be performed.
2. Integration with legacy protocols, such as LDAP and RADIUS, as well as future protocols such as SAML.
3. Enable the user to have the same authentication experience whether they are accessing a local application, one in the enterprise network, or one in the cloud.
4. Support for "step-up" authentication where the user can get basic capability with basic authentication, but then require additional authentication to gain greater privileges later on in the session.
5. Support for a variety of multi-factor authentication methods and allowing the user to select which method they want to use. Have this "user selection" capability built in to the protocol, rather than having to be built by the owner of the system.

6. Have the protocol enforce good security practice and security policies by default, but give system owners control to customize those policies where required.
7. Have the protocol ensure an intuitive experience for the user, regardless of their platform or form factor (PC, Mac, Linux, iOS, Android, desktop, tablet, mobile, etc.). Roll as much of the user experience into the standard as possible, so that the experience is consistent and secure. Don't trust system owners to "do this right". It's hard to do well.

Conclusion

We would like to thank the W3C for soliciting input on these difficult challenges. Strong authentication on the Internet is extremely difficult to do well, but in the age of mobile, BYOD and cloud, it has become more important than ever before. The technologies exist to do this well, but those technologies are difficult to deploy, difficult to use, unintuitive, and constantly changing. Leidos would like to ask that the W3C do what it can to solve these problems once, solve them reasonably well, and engineer those solutions in a way that they can benefit the full Internet community. A lot is at stake, and this is a tremendous opportunity for us all to help each other and the Internet become more secure and more successful for the decade to come.