Work in progress

This is an early draft of a chapter of a book on the foundations of cryptographic authentication being coauthored by Francisco Corella, Sukhi Chuhan and Veronica Wojnas. Please send comments to the authors.

1. Introduction

Digital transformation is predicated on the general availability of cryptographic authentication with credentials carried in mobile phones. But general availability has not been reached yet, and a multiplicity of efforts to reach it fast has resulted in a confusing, fractured and unstable technological landscape that makes if difficult for technology strategists and implementors to make sound decisions, especially in the government sector. The goal of this book is to clear the confusion by explaining the foundations of cryptographic authentication and how the variety of approaches to cryptographic authentication have evolved and are evolving from those foundations.

The following brief history of cryptographic authentication can serve as a guide to the chapters that most directly contribute to this goal.

As we explain in Section 4.1, cryptographic authentication on the internet goes back to SSL client certificates. It was a simple and elegant solution, applicable both to returning-user authentication and authentication with a third party credential. But it was difficult to use and failed to be widely deployed, because it was a transport-layer rather than an application-layer solution.

The failure of SSL certificates led to two different non-cryptographic authentication solutions, username and password for returning user authentication, and federated identity for third party authentication.

Returning-user and third-party authentication have evolved back to cryptographic authentication by different routes, and a common authentication solution for both authentication use cases remains to be found.

Returning-user authentication had to change as hackers became adept at exploiting the severe vulnerabilities of passwords. Two-factor authentication was introduced and heavily marketed until the Evilginx attack defined in Section 4.3 rendered it ineffective. Then the

FIDO Alliance introduced a cryptographic authentication solution based on a key-pair credential, that evolved from UAF to U2F, FIDO2 and Passkeys, as described in Chapter 10.

Federated identity depended on returning-user authentication for authentication of the user to the identity provider, so that was one motivation for moving away from it. But there was also another reason: the identity provider controls the identity by which the user is known on the internet, and there were only a few commonly used identity providers, each controlling the identities of a large percentage of internet users.

Concern with this control led to the concept of decentralized identifiers, described in detail in Chapter 14, and self-sovereign identity, SSI, described in Section 15.4. Decentralized identifiers needed to be bound to claims, and verifiable credentials, the subject of Chapter 15, where used for that purpose.

A practical problem with SSI and decentralized identifiers is that, if people are allowed to choose their own identifiers, two people may choose the same identifier. If that happens, a method is needed to decide who has chosen it first. As explained in Section 14.1, blockchains and distributed ledgers provided such a method, until random bit generation with high enough entropy provided a better solution.

So verifiable credentials seemed to be an alternative to the X.509 public key certificates used as SSL client certificates. But there are two difficulties. First, there is a conflict between self-sovereignty and user privacy, because using the same identifier in all credentials enables tracking by all transactions. Version 2.0 of the verifiable credentials data model warns that "Identifiers of any kind increase correlatability" and says that it is permissible to omit the identifier of the subject of a verifiable credential "when privacy is a vital consideration"; but when is privacy not a vital consideration? Second, as discussed in Chapter 15, verifiable credentials were not intended for authentication and provide no means of proving possession of the credential by the subject.

These difficulties are a motivation for returning to traditional cryptographic credentials, which are discussed in Chapter 3, including full disclosure public key certificates in Section 3.2, selective disclosure public key certificates in Section 3.3 and anonymous credentials in Section 3.5.

But digital transformation specifically requires credentials carried in mobile phones. The ISO/IEC mobile driver's license (mDL), discussed in Chapter 14, promised to be a big step in that direction as ISO/IEC 18013-7 specifies the use of the mDL for online authentication.

But it only supports authentication to a relying party that is accessed from the mobile device that carries the credential, as stated in NOTE 1 of Section B.1.1: “Cross-device flows are prone to engagement relay attacks which is the reason cross-device flow is not included in this document.” This defeats the overall purpose of providing online authentication, because most websites won’t implement an authentication method that only works in mobile devices.

In Section 12.4 we describe a possible way of providing cross-device authentication with a credential stored in a web browser. In that solution, the browser is a credential wallet, just like browsers were (and still are) credential wallets for SSL certificates. But it is an application layer solution rather than a transport layer solution, thus eliminating the obstacle that prevented widespread deployment of SSL certificates.

References

[1] Vial, Gregory (2019). "Understanding digital transformation: A review and a research agenda". The Journal of Strategic Information Systems. 28 (2): 118–144.