The Choice of a Second Authentication Factor

Mark Sitkowski
Design Simulation Systems Ltd

Unless you've been in a Tibetan monastery for the last decade, or so, you will know that two-factor authentication comprises the submission of

- Something you know
- Something you have, or are

in response to an authentication challenge.

The first factor is usually a password or, in the case of devices such as ATM's, a PIN code. The second factor – again, taking the ATM, as an example - would be the card you swipe.

Since the advent of online shopping, online banking and other online services, the use of a card as the second factor has proved to be largely impractical for such applications, due to the fact that most computers don't have a card entry device.

Taking advantage of the fact that almost everyone has a mobile phone, most banks have adopted the practice of sending a one-time code as an SMS message, to the client's mobile phone, for entry into the challenge form, together with the password.

However, technology moves on, phones become smart and, now, very many people use the actual mobile phone to login to the online services, which makes the arrival of an SMS message rather inconvenient, when the client is in the middle of filling in the challenge form.

Since the mobile phone is already connected to the authentication service, why not use it (or any other device, for that matter) as the actual second factor?

There are many ways to achieve this, but this article will refer specifically to the method used by the DSS Enterprise Identity-as-a-Service system, described in detail in
www.designsim.com.au/DSS_Enterprise_Manual.pdf
The device has several characteristics which, when combined together, enable the creation of a signature which is unique to that particular device.
Specifically:

- The hardware device type, (as in Android, iPhone, Dell laptop, IBM 370 etc)
- The device version number.
- The CPU type and version
- The CPU clock rate
- The operating system used by the device, and its version
- The type and version of the device's graphics adapter
- The browser type used by the client, and its version number (as in Firefox, Opera, Safari etc)

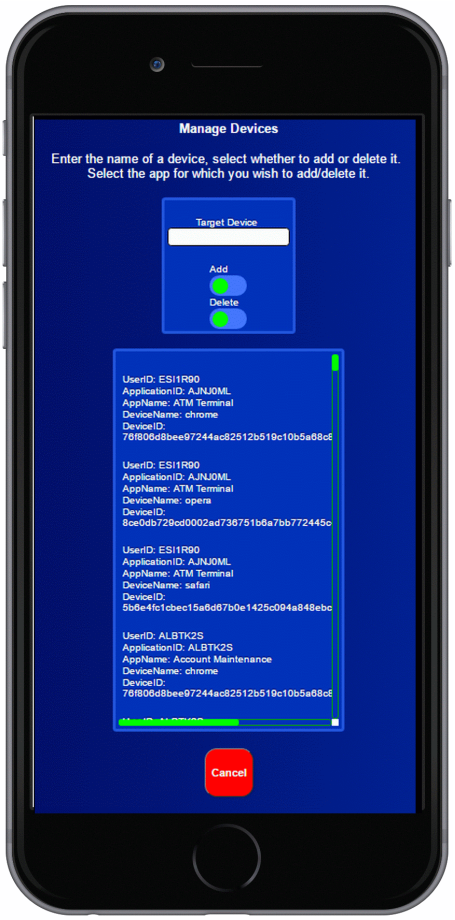
These factors are derived without any action on the part of the user, the use of cookies, the installation of client software on the device, nor of explicitly querying the device.

Summing the effect of all of these factors gives a signature which is so unique, that the need for an additional password becomes questionable. The only factor mitigating against its omission, is the fact that the risk associated with the loss or theft of the device is unacceptable.

In the interests of client privacy, and to make the signature impossible to fake by synthesis, the individual factors cannot be derived from the signature, which is automatically recalculated with each connection. This makes for a totally friction-free login experience from the user's perspective.

Having thus calculated the signature, DSS Enterprise further calculates the SHA256 hash of the signature as a DeviceID, and compares it against that previously registered against any application to which the user is registered.

When a client account is initiated, or the user is first registered to a new application, the device which the user proposes to use to access a given application is unknown, so it is set to a wildcard entry, as a kind of 'booking'.
The first time that the user successfully logs in to the application using his password, the wildcard is replaced with the DeviceID of the device being used, and all subsequent logins to that application must be made using that specific device.



In the light of the sensitivity of the signature to such events as operating system upgrades and browser updates, it makes sense to register several devices against every application (as may be seen above) and, if a major browser update causes the signature to change, to use an alternative device/browser to register the new version of the browser in question.

In practice, it is only certain changes to the browser or operating system which make the signature change and, if the user has not booked a new device, the system manager can do so on his behalf.