

## The SIM and Mobile Security

*"A hardware token is always more reliable than a software token, because it requires physical access to compromise it, not just some clever code."*

**PENRILLIAN'S CHARLES WEIR ON MOBILE SECURITY**

In the last newsletter we talked about mobile security, and the three main problems it must address - channel security, authentication, and malware.

In the weeks since we published it, there has been a flurry of new reports about potential vulnerabilities in Android, alongside the latest stats for malware targeting the platform. The absolute numbers remain small, but year-on-year growth of 400% underlines the importance of taking mobile security seriously. Worth mentioning is the growth of multiple-vector threats - malware that targets phones using a combination of methods that can include SMS, MMS, email, web, and even voice - which suggests that the bad guys are becoming more sophisticated.

We also touched on privacy, the red thread that runs through all security-related topics. Recently the GSMA, the industry body for mobile operators, sparked debate with a call for comment on proposed new Privacy Design Guidelines.

It seems timely then to round off our thoughts on security and privacy topics by considering the special role that operators occupy in the mobile technology chain, and the privileged position it gives them as potential trusted security providers.

It's not exactly a law of the universe, but it's a universal law of digital security - when the software going gets tough, look to the hardware. As our headline quote above emphasises, a hardware token is always more reliable than a software token, because it requires physical access to compromise it, not just some clever code.



Hardware dongles that unlock a software licence, VPN key generator dongles, card readers that validate your smartcard to your online bank account - these are all examples of a hardware token being preferred as a more reliable authenticator than a software-only solution. In fact, a smartcard is itself a hardware token, and the move to chip and PIN is another example of the same principle.

Back to phones. You can fake many things, but it's hard to fake a SIM card, which is what makes it a reliable and secure token for authentication. Mostly we take the SIM for granted - for the non-technical, it just is their mobile number - but in fact the phone SIM is another example of a hardware authentication token, which is used to authenticate a user to the network.

It's more than that: in principle at least. It's a secure storage device with its own built-in processor, accessible from the phone itself (or from a PC in the case of a dongle). The SIM is capable of storing and running application-like software (think of SIM Toolkit), as well as dedicated decryption and encryption algorithms using encryption keys that are securely stored on the SIM.

### **So let's think about that. Want to protect your on-phone data?**

Easy; encrypt the files on your device, or encrypt the whole device file-store or database, using keys stored on the SIM.

### **What if you lose or forget your key?**

Easy; the operator can reset it remotely. This could solve the problem of what to do if you lose your phone or have it stolen; much simpler than trying to physically wipe the phone's storage using remote protocols, the network operator could simply withdraw the encryption key from the SIM, and lock the bad guys out of your phone instantly. Changing the SIM wouldn't help them, because it wouldn't have your keys - those would still be safe with the operator. And if you recover the phone, all your data is still there, you only need to restore the key to the SIM.

Of course this is a what-if scenario, but existing technologies already prove some of the concepts. For example, the SIM is already used as an authentication token to WiFi networks using EAP-SIM (Extensible Authentication Protocol). In principle, similar technologies could allow you to delegate the whole on-phone data security problem to your network operator - and give the operator a possible new market as a trusted security provider for any device capable of hosting a SIM, or just a dongle.

Mobile security, like any technology, will never be infallible. GSM encryption, for example, was very publicly cracked last year, although how much of a threat that poses outside the laboratory is debatable.

The more obvious issue is the one of trust: how much trust do you want to give your network operator? It's not so much a question of data access, as controlling access. Could the operator lock you out of your own data if instructed to do so by some third-party - or even when you forget to pay your bill?

To make the SIM a player in the wider security context, and not just a private authentication token for the network, would require additional operator infrastructure. That may be enough to ensure that it won't happen any time soon, because re-engineering infrastructure is always difficult.

But it's food for thought. And it underlines an important point, that operators are *the* privileged players in the mobile ecosystem. Device manufacturers are important, but operators really own the game; they can do things that no one else can.

Penrillian have worked with all of the UK's major operators, on a wide range of projects:

- For Orange, we developed [Your Orange](#), BlackBerry app to enable customers to manage their Orange accounts via their BlackBerry handsets
- For T-Mobile, we developed [My T-Mobile](#), an app that enables customers to view balances and itemised bills on their smartphones. We also developed network performance tools to sample actual customer network experience using standard handsets from T-Mobile's UK stores
- We developed the connection and configuration software for [Vodafone's Mobile Connect USB Modems](#), laptop dongles that enable 3G network access
- For a major UK network operator we developed 'plug and play' software to connect a user's laptop to the 3G network via their smartphone to enable easy mobile broadband

Whatever the problem you are trying to solve, Penrillian can help you too. Whether it's expertise to help you build the back-end of your mobile solution, or front-end skills to develop your mobile app or service, or skills at deploying across platforms and across networks, Penrillian can help. We specialise in getting the job done, quickly and expertly.