

## Mobile Security

**"Security is not so much about what you, the user, can do with your phone - security is about what *other* people can do with it... that you might prefer they didn't!"** PENRILLIAN'S CHARLES WEIR ON MOBILE SECURITY

There's no such thing as a typical phone project. If anything, the opposite is true at Penrillian - it's the sheer diversity of what our customer's need that keeps us on our toes!

But a lot of projects that come our way have one thing in common: they are less about what *users* want to do with their phones, than what *other people* want to do with them - that users might prefer they didn't. In other words, they're about security.

It's easy to see why security matters. Phones are communications devices; our personal communications are very personal, and our business communications are sensitive. We want and expect privacy. Increasingly our phones are other things too; platforms for making payments and managing our money online, for example. We want and expect those transactions to be secure.

And yet phones are doubly vulnerable. As comms devices they are exposed to the public network where communications can be tapped or intercepted, and because they are small, portable, and visible - we take them everywhere, we use them everywhere - they are easily lost, or worse, stolen.

On any platform, security can be divided into three main problems. The first is channel security, ensuring that Alice can talk to Bob without risk of someone listening in. This is the problem that encryption solves, and modern techniques (like Public Key Encryption) are pretty good at it. Which is just as well, since every online shopping cart and bank account depends on it.

The second problem is authentication. Encryption secures the channel, but not the endpoints. To secure the endpoints you need to authenticate them, so that Alice can be sure she really is talking to Bob, and Bob

can be sure this really is Alice. Certificates solve this problem but are tricky to get right.



The third problem is malware, or worrying about what comes onto the device. Malware aimed at phones is on the rise, driven by exploding market growth for Smartphone's and apps. On mobile, the classic attack vector for viruses and spy apps is an incoming SMS link to a malicious app (Trojan Horse) that the user is invited to download. You can't stop the user receiving the SMS, but you can scan to detect the Trojan.

But phone security is not just about what happens over the air interface or on the phone itself. Much easier than hacking your phone is stealing it. When your phone is lost or stolen, everything is compromised; not just the phone or your music or apps - for which you have paid good money - but your data and your privacy too. The only really secure defense against loss or theft is to remotely locate and lock or wipe the phone itself. And that requires deep hooks not just into the phone OS, but into the mobile network too.

Penrillian has worked with clients on all aspects of phone security. The following are just a few of our recent projects:

- We worked with KoolSpan to bring TrustChip encrypted voice technology to Symbian smartphones. Koolspan's 'Trust Chips' memory cards fit in the phone, making security easy to deploy.
- We have worked with 2Ergo on an encrypted SMS solution for mobile apps. They provide channel security and authentication for secure banking, ticketing and payments.
- We worked with BlackBelt to create their BlackBelt AntiTheft solution for Android. It can locate a lost or stolen phone, report if the SIM card is changed, and remotely lock or even wipe a phone using SMS.

If you need to design and implement a secure solution as part of your mobile app or service, we can help.

Whether on the phone or on the back-end, and whatever the platform, we specialise in getting the job done, quickly and expertly.

[Contact us](#), and let us exceed your expectations!