ORAL CONCOURS 2014
ANGLAIS - LVI

Blackphone: can a mobile ever truly be hack-proof?

Encryption and security specialists Silent Circle has teamed up with Geeksphone, a joint project between security-conscious developers, entrepreneurs and ex-special forces operatives, to launch a new mobile phone that claims to give users back control of their data and lets them "determine what data they want to reveal, rather than be forced".
On the face of it, the Blackphone does exactly that. For $629 (£377), customers get a smartphone that includes one year's subscription to secure communication service Silent Circle and a virtual private network (VPN) for secure browsing, a "remote wipe" anti-theft feature, a firewall and a year's subscription to 5GB of secure cloud storage. It also has no sign-up process, no ecosystem like Android or iPhone has (although it runs a modified Android OS) and a Blackphone specific app-store that is on the way, although users can still download apps from the Google Play Store or third party apps unrelated to Google.

As 2014 smartphones go, it also has reasonably decent specifications.[...] But, perhaps the most interesting feature is the security manager app which lets you manage what data regular apps can harvest from your phone. During a demonstration of the security manage app, Blackphone's vice president of engineering David Purón pointed out that a simple barcode scanning app was accessing his contacts list. "There's no reason for it to do that, right?" he asked. "So all I need to do is press 'restrict' and it can no longer access my contacts - but the app will continue to work as normal."
While it's disquieting to think that single purpose apps like a barcode scanner are exploiting their access to data, it's the lack of public awareness that the Blackphone team are hoping to highlight when the device comes to market this summer.
Even with data restriction for apps and secure browsing, some companies can still build up a picture of the activity you generate on your phone. A perfect example is Polystar, a Swedish "network monitoring" company that measures internet traffic and sells the data to telecommunications companies. Polystar looks at how much bandwidth you're using and at what time of the day, and can tell that you're watching a couple episodes of House of Cards, or a cat do something hilarious on YouTube. You can never really escape someone looking over your virtual shoulder.

One of a new wave of hardware and software services claiming to offer enhanced security and privacy in the wake of the Edward Snowden revelations, early coverage of Blackphone described it as "NSA proof". The Blackphone team has since rowed backwards on that claim, acknowledging that any such claim is likely to be short-lived.
"Yes, of course you can protect yourself from spying agencies, that's true," said Purón. "But in this privacy and security industry, no one can say that something is 100% secure."[...] The NSA, or any other security agency that wanted to hack the phone, would attempt to exploit the one major security flaw that exists in the Blackphone – the phone's baseband.

A phone's baseband is essentially a black box that communicates with a cell tower and has low-level access to your GPS and microphone. The baseband is entrenched hardware in your phone, which has its own CPU and operating system and is entirely vulnerable to attacks. The Blackphone doesn't protect against this. Stephen Bonner from KPMG's information protection team also thinks that the phone's focus on privacy is another security flaw in itself. "By owning a Blackphone a user could become a target because it acts as a red flag to criminals by highlighting that there's something to hide. As the devices attract and house high value data, attackers will be inclined to break in," said Bonner. "Some of the threats these type of products aim to protect against aren't realistic for most users. They might be a cool gadget for wannabe James Bonds but business users need to worry a lot more about the applications on their device and the end-to-end protections they have in place."
The Blackphone team doesn't pretend to offer NSA-level security – few companies do – but wants to appeal to corporate users as well as individuals, exploiting concern over corporate espionage in "hostile environments", Bonner explains.

The Blackphone team argues that it isn't for people who wear tin foil hats and communicate entirely via tin-can telephone, and it might not be James Bond's go-to gadget. But it is for people who are unhappy with the everyday phenomenon of brazen and unchecked data mining.

The Guardian, 4th March 2014