Simon Cairns outlines the growing threat to mobile security and the increasing importance of phone encryption

WHY MOBILE SEC

Over the last few years we have seen the development of the smartphone and its capabilities within the bring-your-own-device (BYOD) world. Now most smartphones carry all of our data, both private and business, and increasingly include personal information including financial details and passwords.

Smartphones are never more than a few feet from us at any time and travel everywhere we go. Unfortunately, they are also the weakest link in any cyber attack and with the recent iOS breaches, given just some basic knowledge, it is now possible to crack almost any phone in a matter of seconds. As a result of this, espionage is now one of the fastest growing cyber crimes in the UK and set to explode in growth over the coming years.

Corporate secrets, business deals and information sent via tablet and smartphones are recorded and intercepted daily in the UK by thieves using jammers in the car park, outside your building and in public Wi-Fi areas. Setting up a Man In The Middle Attack (where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with one another) is now easier than ever and such actions can sit undetected on a network for more than a year until they are discovered. By this time the breach could be huge and the fines for phone providers are set to grow by 2018 with penalties to rise to 4 percent of Global Turnover. Add to this a loss of trust, reduction in share values and most of all loss of customers who will switch to a provider who can guarantee better security. It's a fact that 75 percent of people will not deal with a breached organisation.

Cyber crime against SMEs is rising at the rather alarming rate of 300 percent every month, while it's claimed that as many as 93 percent of SMEs have been breached in the last year alone and are not even aware of it. The fact that ransom-ware could be lying dormant on your company's system for weeks, months or even years before being discovered – or worse still – private data should be reason for concern. The average price for a data breach against SMEs currently stands at £64,000 and for larger companies this figure rises to a shocking £1.5 million, which in turn will rise with GDR coming into force in the next 16 months. Jammers too can be purchased online and used to disrupt 4G and 3G signals leaving your phone vulnerable.

It is estimated that as many as 75 percent of all business in the UK are currently completely unprepared for a potential cyber attack and many still have poor password security, weak authentication and very little in the way of phishing education or training.

Abroad is even worse and any business traveller can expect to have ALL of their conversations recorded, while SMS and browsing sessions risk being watched in many countries that are looking for competitive information.

So who is a target? C-level executives, business travellers, senior management, high net worth individuals, celebrities, financial traders, lawyers... The list is almost endless. The long and the short of it is that anyone who has information of value and that uses their smartphone to discuss sensitive information is at risk both at home and abroad.

Thankfully, the answer to gaining maximum protection is simple. Mobile and tablet encryption will provide the greatest protection for all calls, SMS and browsing sessions and will also encrypt any files that are sent from your mobile device back to your

©Getty Images

Not all apps are equal and some may have been produced by malicious developers purely to gain access to your personal data

CURITY MATTERS

home network. There are many solutions available on the market, however not all are equal. Many are downloadable applications which provide some security, but not total protection as they still run on the system's operating system and so can still be hacked or jail breaked.

Some solutions are proprietary and these are far more secure. However, they can be expensive and rely on the recipient of your call utilising the same software solution. This often leads to a two-phone scenario, which is far from ideal.

The rapid growth and vast adoption of smartphone usage poses a severe security threat to both enterprises and organisations. Organisations have never faced a greater risk of exposure to malicious attacks and the resulting leakage of their sensitive data, leading to potentially substantial commercial damages and the theft of users' personal data. The explosive rise in voice and data communication interceptions, malware and targeted Trojan attacks, information stealing applications and stolen mobile devices just highlight how fragile and vulnerable mobile devices have become. Organisations need to rethink their mobile security strategy in order to provide users with a robust security solution, which offers the optimal balance between ultimate freedom of use and seamless yet effective protection.

Basic communication is at risk of interception tactics such as rogue cellular towers that aim to function as alternative GSM base stations or Man In The Middle techniques used to invisibly sniff out Wi-Fi and GSM traffic, leaving organisations exposed to malicious voice, messaging and data-based communication interception threats. In addition, mobile network operators that have the ability to monitor, intercept and record the entire mobile communication stream, serve as an additional dimension of data leakage and communication interception threat.

Devices such as smartphones are vulnerable to various attack patterns. These include rogue applications with user-granted permissions that provide access to device data and resources, highly targeted Trojan attacks that are now commercially available and which operate undetected in the background as well as physical data extraction attacks that enable the access and extraction of any locally stored data.

Ultimately, though, the weakest mobile security link is the human factor. A mobile user will always choose convenience over data security. The main risk lies within the large amounts of user-generated data stored locally on the device. Solely relying on the education and training of users to prevent mobile security threats is an approach that's bound to lead

> **"Secure communications is key as is usability; the phone has to be both user friendly and capable of keeping everything secure from calls to SMS and data".**

WHY MOBILE SECURITY MATTERS

©Getty Images

There are a number of measures you can follow, but a high-end off-the-shelf smartphone is a good start

to failure. Mobile security needs to be seamless, avoid restrictions and adapt itself to defend against evolving threats without relying on an end user's involvement or actions. By providing maximum smartphone functionality together with seamless protection, it is possible to contain the 'second phone syndrome' – a scenario in which a secured but highly restricted smartphone is abandoned for a user-friendly yet non-secured smartphone alternative.

So what should we be looking for in our encryption solution? There are five key areas to consider. Firstly, an encryption layer protects data-in-motion as well as data-at-rest. It secures all forms of communication (voice, data, messaging) from interception of the communication channel (sniffing and MITM, passive and active) and it secures information locally stored on the device.

Secondly, a protection layer protects against device penetration techniques. It effectively battles various penetration vectors exploiting web sessions, Wi-Fi networks, Bluetooth communication, USB interfaces, application vulnerabilities, OS level vulnerabilities, *etc.* The protection layer blocks out the vast majority of Trojan horses and malware types.

Next you should consider a prevention layer, which prevents unauthorised and/or risky access to sensitive device resources and data, through a sophisticated and automated resource permission firewall. This grants permissions based on a calculated reputation score, risk assessment and the resources required for proper functionality.

A detection layer can be used to monitor and detect malicious code, app misbehaviour, surpassed risk level thresholds, data interception and extraction attacks. It is able to apply countermeasures that are based purely on the device's risk level and security posture. Finally, it is vital to ensure that whenever possible you use a secure device. This ideally needs to be a high-end off-the-shelf smartphone. You also require encrypted storage securing data at rest as well as protection against physical extraction of data. Finally, in a worse case scenario when your security is compromised you need the ability to carry out a remote wipe and remote device locking.

Secure communications is key as is usability; the phone has to be both user friendly and capable of keeping everything secure from calls to SMS and data. Anything less than this will result in a device that is fundamentally hackable and so will leave you with doubts and at risk in the future.

One last area that is frequently overlooked is that many users have additional apps on their phones and that many of these applications ask for and receive information by default. They also ask for and get permission to read SMS messages, read contacts and use camera and track location. Many of these applications have no need of these permissions and so we have to ask the question. Why have they built them in?

This is a real issue as the more applications on a given device makes the phone that many more times susceptible to misuse *etc.* If an app has been developed by a malicious developer – as seen recently in the iOS touch malware – the catastrophes could be never ending.

In conclusion, in the UK more than 32 councils have been fined in excess of £2m over the past few years for lack of security. Only last month, more than 30 legal firms were held to ransom for unknown amounts and medical data is the most valuable of them all. Sadly, once data is stolen, it is often resold dozens of times on the dark web and it is this issue that leads to the massive rise in phishing emails and more crime. Armed with the right protection you and your organisation should be equipped to ensure that you don't add to these statistics.

Simon Cairns has been working for 26 years in the security industry, selling to retail, banks and insurance companies. More recently, he has set up Orion, which provides new and innovative cyber solutions to all sizes of businesses