



Today's Mobile Threat Landscape

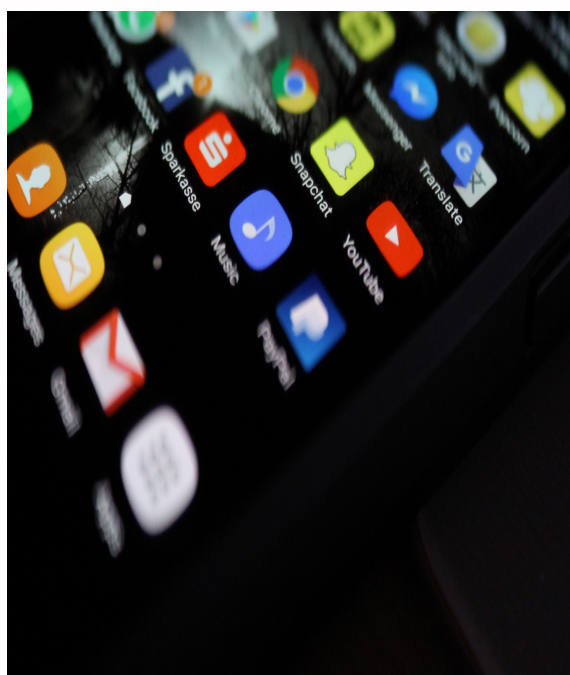
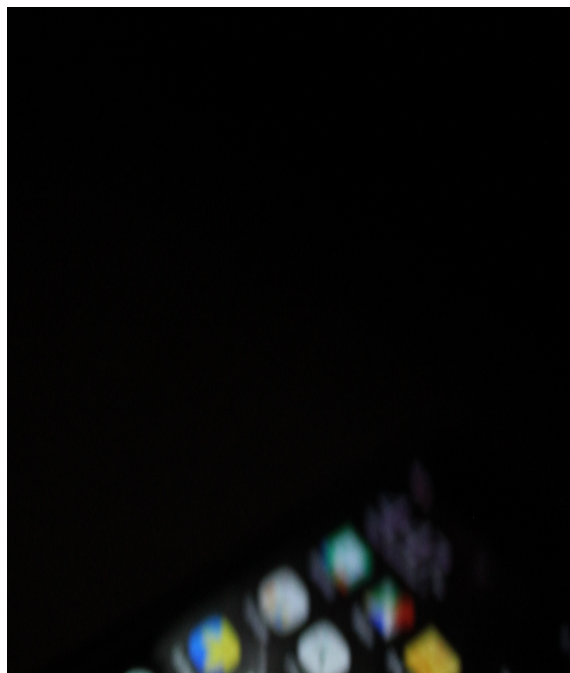
Real People, Compromised Devices,
Insecure Infrastructure

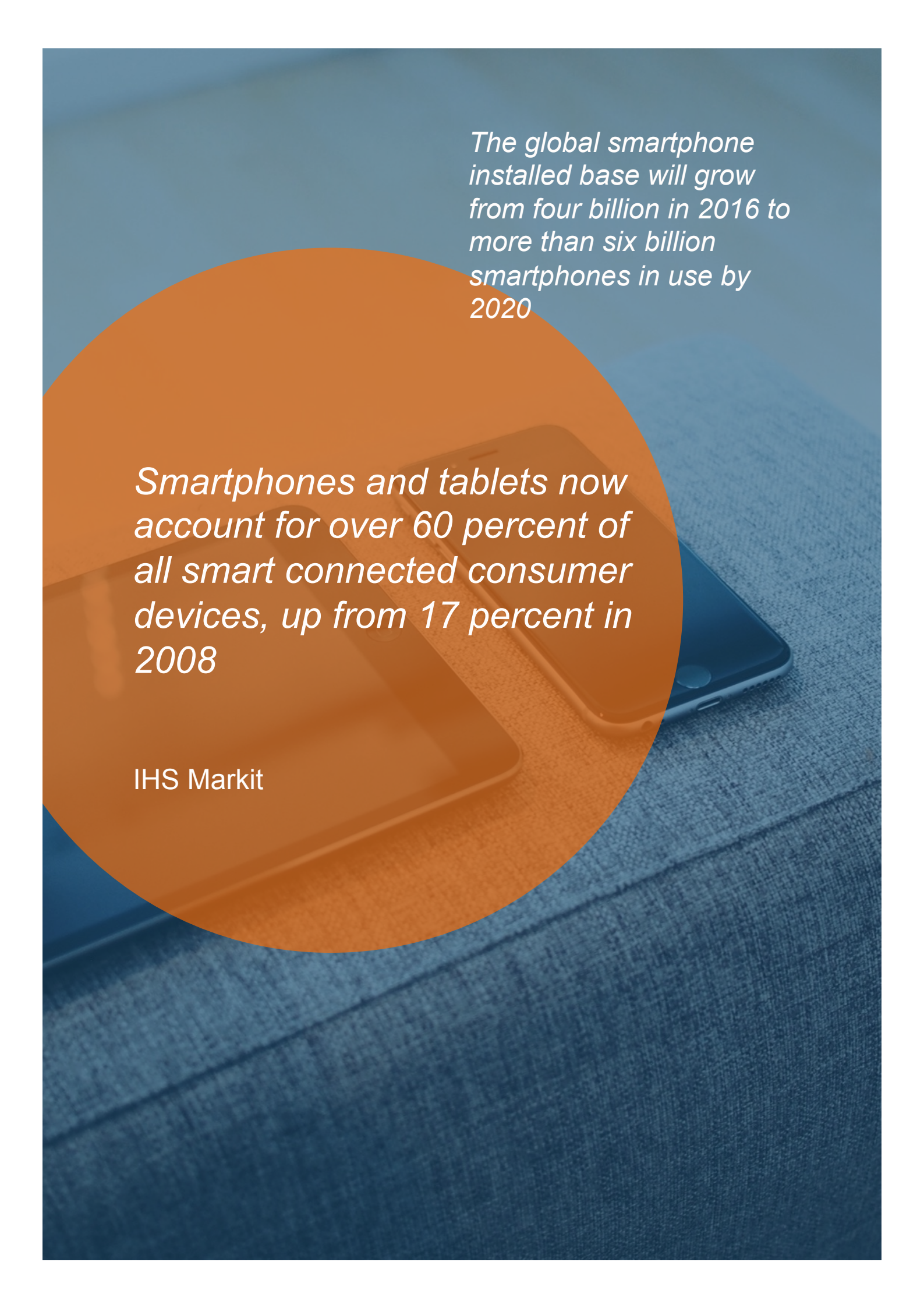
Mission Critical Mobile

Unusually for such a world changing event we can pinpoint the exact moment when the smartphone revolution began. It was at 9:47am Pacific Standard Time on 9 January 2007 that Steve Jobs unveiled the iPhone. To industry veterans such as Nokia or Blackberry the fact that it didn't have 3G radio meant that it wasn't really a smartphone at all.

But for Apple fanboys it was the moment they had long been waiting for. Today it's clear that the product launched that day profoundly altered the very fabric of day-to-day life in a thousand ways. It's created Uber and countless other parts of the 'on-demand economy.' It has played a critical role in political revolutions (the Arab Spring and Hong Kong's pro-democracy movement) and revolutionized dating (think Tinder). It's accelerated the pace of business and created the 24 hour news cycle. Unquestionably, because of the smartphone, we have become the first generation in human history to live 24x7 always-on, always connected lives.

The impact on our work experience has been no less profound. It started with email: how did we ever survive without our inbox at our fingertips. It extended to the full range of digital workplace tools including calendaring, conferencing and file sharing. Now it is being used to re-shape the way business is conducted from kiosk based banking, to on-site invoicing, to on-demand logistics. Today we live in the era of mission critical mobile.





*The global smartphone
installed base will grow
from four billion in 2016 to
more than six billion
smartphones in use by
2020*

*Smartphones and tablets now
account for over 60 percent of
all smart connected consumer
devices, up from 17 percent in
2008*

IHS Markit

Mobile Security in Perspective

Today, as more and more critical functions migrate to mobile it seems timely to take stock of where we stand as an industry and to provide guidance on the critical threats and vulnerabilities which we face today.

In the ten years since the launch of the iPhone we have learned much about ensuring the integrity and confidentiality of information stored and processed on mobile devices. Apple and Google have made much progress in making iOS and Android appropriate for use in enterprise environments. It's clear that the architecture of both the Android and iOS operating systems have helped them avoid many of the security issues which have plagued Windows. Application segregation, in particular, has made it far more difficult for malware to successfully exploit mobile devices.

This is because each separate piece of software ('app') operates independently and access to data belonging to another app is highly restricted. In addition apps do not have the kind of administrator privileges which would allow unfettered access to device data and functions. Instead end-users act as administrators of their own devices and are responsible for deciding whether apps have access to specific types of data (e.g. contacts, photos) or functions (camera, location services).

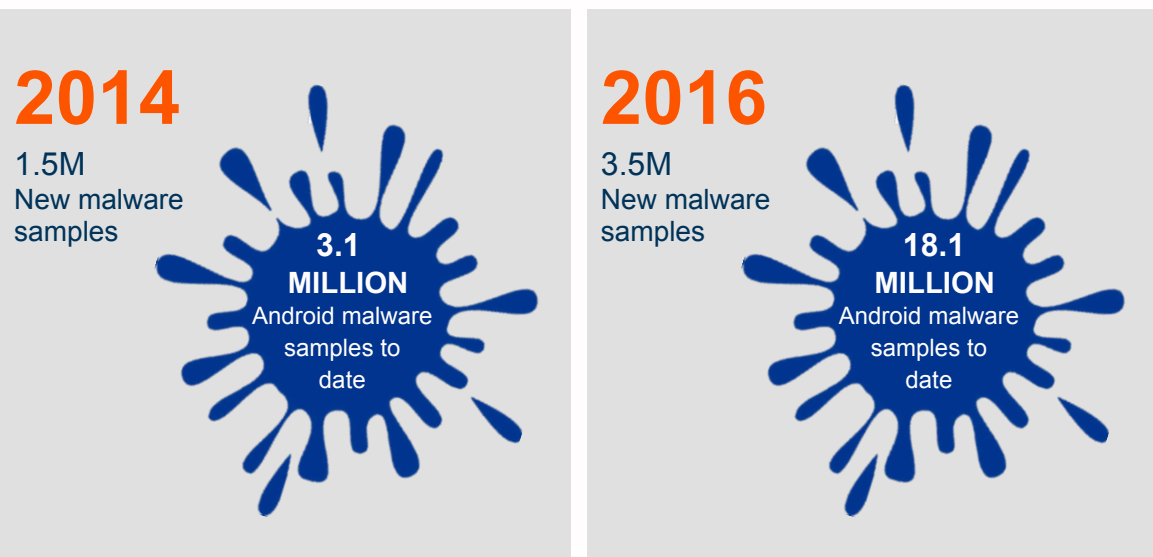
While such end-user control can be a double-edged sword, Enterprise Mobility Management (EMM) systems can compensate for this. In these circumstances more stringent controls can be imposed and an end-user's ability to inadvertently compromise a device can be reduced.

Both Apple and Google have shown themselves committed to addressing security issues in a timely fashion. Apple in particular is in the enviable position of having circa 90% of its devices on the last OS version.



Mobile Security in Perspective

The app store software distribution model is another major security enhancement. In Apple's case software can only ever (except in limited edge case circumstances such as enterprise distribution) be downloaded to an iOS phone via the App Store. Apps submitted to the App Store are subject to stringent vetting. Malicious apps which do make their way through the process are quickly removed once identified. While Android has also adopted the app store distribution model is continues to allow non Play Store downloads. In addition, Android is inherently more open and as a result the opportunities to introduce malicious code are greater. As a result Android suffers from a non trivial rate of malware infection.



source: AV-Test

Mobile's Unique Challenges

Widespread adoption of EMM, the OS design and the app store distribution model undoubtedly help make mobile devices safer. Nonetheless it would be complacent not to recognize that there are elements inherent to enterprise mobility that pose challenges from an information security perspective.

We group them into three broad areas: human factors, device factors and infrastructure factors

Human factors

Mobile devices are used in a much more informal way than the typical dedicated work device. For one thing they might not be a corporate device at all but rather an employee owned phone which is authorized to access corporate data. Devices are mixed used - they're often as likely to be used to keep the kids occupied on a long journey as to polish your latest killer PowerPoint deck.

On mobile, work and personal life blend and bleed - one moment your WhatApping your pals about Friday night, the next your clarifying thorny issues in a critical contract.

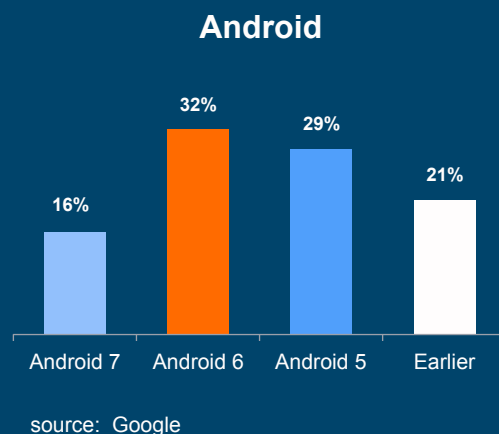
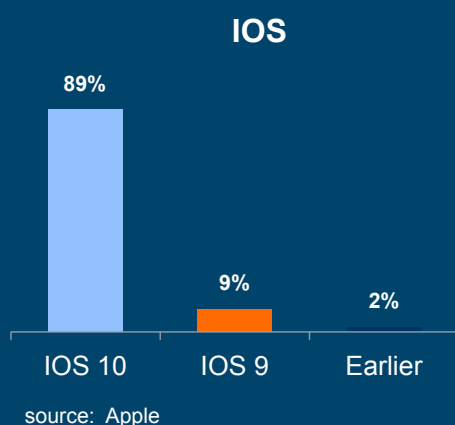
All of this and more means that the locked down, corporate-mandated (and protected) environment which was the norm in the desktop world has broken down. As a result one of the biggest challenges every information security and enterprise mobility professional faces is striking a balance between security, privacy and usability that works for your end-users.



Mobile's unique challenges

Device Factors

Two device related factors in particular present challenges for information security. The first is well understood: the device software update process. When a new release becomes available the enterprise is reliant on some combination of end users, mobile operators and device manufacturers to ensure that the software is updated on the phone. As a result you may have to tolerate a position where a device is running with a known vulnerability for which a patch is available.



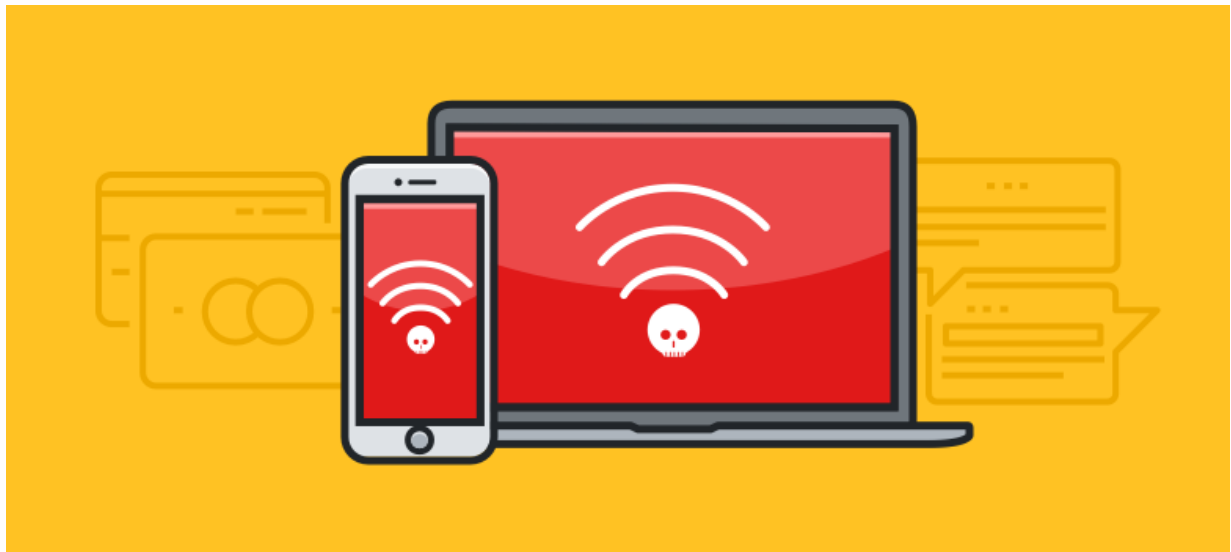
The second information security issue with mobile is less well understood: enterprises have little or no visibility of how the device is behaving. As a result it is impossible for an enterprise to assess whether a device is to be trusted. When a new threat is identified enterprises are unable to search for IOC's (indicators of compromise). This is because mobile device management is limited to controlling the settings on a device and is blind to activity. What's more, because the device is usually outside the corporate environment, network-based monitoring tools are ineffective.

Mobile's unique challenges

Infrastructure Factors

The third set of factors that make mobile devices different relate to the networks to which they connect. Cellular networks benefit from built in security features which make it relatively difficult to intercept over the air communications. In most parts of the world cellular connectivity is provided by large, regulated entities who invest heavily in maintaining the integrity of their networks.

In contrast Wi-Fi networks are wide open to attack. Traffic between the device and the wireless access point can be intercepted and the wireless access point itself can be compromised or faked. The providers of public Wi-Fi networks at hotels, coffee shops and airports rarely have the expertise or incentive to ensure the integrity of the data they handle.



In the light of all this what could possibly go wrong?

The rest of this whitepaper outlines what real world experience has shown to be the key mobile security threats which enterprises with a mature EMM program need to consider and lays out actions which should be taken to address them. We deal with threats in three groups - user compromise, device compromise and infrastructure compromise and explain how to protect, detect and respond to these threats.

Social Engineering

According to Verizon's Data Breach Report

90%
**of all data breaches
involve social
engineering.**

Mobile has become an environment in which there are rich pickings for the cybercriminal intent on using such tactics to steal sensitive data.

The mobile device is particularly vulnerable both because of the way in which it is used (mix of personal, business, informal and 24x7) and the absence of the protections that enterprise information security professionals take for granted.

This second point is often under-appreciated. Corporates have invested heavily in firewalls, network and end-point security solutions to improve the security stance of traditional desktop and mobile computers. In the vast majority of cases mobile devices are not protected in the same way.

Take web filtering. Most enterprises have a web filter on their corporate network which prevents employees visiting sites which host malware and filters out other undesirable content. But when a device is off the corporate network no such protection applies.





Hackers hide cyberattacks in social media posts

The New York Times

Social Engineering



Phishing is a great example of how mobile opens up gaps in the traditional cyber security architecture. There are typically two layers of protection against phishing attacks. In the first instance, there is a mail filter which blocks suspicious email before its delivered to the employee. A second layer of protection is offered by the corporate web gateway which will block access to malicious links contained in the email.



Contrast this with the situation where the phishing takes place over SMS. As SMS goes nowhere near your mail server, a phishing SMS will not be stopped by your mail filter. What's more, the mobile device is highly likely to be on a public network. As a result if an employee clicks on the link in the SMS they will bypass your web gateway.



Mobile phishing can take place not just over SMS but over messaging apps like Facebook Messenger and WhatsApp. Links can be distributed over social media services like Snapchat, Facebook and Instagram but also over professional networks like LinkedIn. Employees can be tricked into revealing login credentials, installing rogue profiles on iOS or downloading malware to Android devices.



The Android app distribution model represents a particular problem. By changing a single device setting, apps from outside the Play Store can be downloaded to any Android device. Malware infection rates for such 'sideloaded' apps are high relative to 'official' apps downloaded from the Play Store. Social engineering tactics are often used to encourage users to sideload. Users might want to access a free stream for a sporting event or download a pirated game. By promising free 'goodies' the cybercriminal can easily entice careless users into installing malware which steals data, monitors communications and captures credentials.

Social Engineering

Countermeasures

As in all things cyber a layered approach is key. Monitoring device settings with EMM and including mobile risks within broader cybersecurity employee training programs are table stakes. Beyond this there are also specific technical countermeasures which are both powerful, feasible and can be delivered without compromising user experience.

Specifically your users need to be protected with a web filtering solution which is made for mobile. Made for mobile implies a number of things. Firstly, the web filtering solution must work 'off-net', i.e. when your users are on the cellular network or public Wi-Fi. Secondly, the solution must work across both apps and standard browsers. A web filter which requires the installation of a special browser is not a solution which will work in practice as people today expect the convenience of the native browsers on iOS and Android. Thirdly it should avoid the need to route traffic through a proxy or gateway as this will introduce unacceptable latency and user privacy issues.

Even with the best protection you need to prepare for previously unknown threats. Recognizing this, it is essential that you have a way of detecting which users have been breached when intelligence about a new threat becomes available. This is where the lack of visibility of mobile device activity becomes a glaring weakness in organizations ability to properly implement security for mobile devices. Imagine knowing that a spear phishing attack has been attempted on your key executives and being unable to quickly identify the victims.

Corrata's Mobile Threat Defense solution incorporates a made for mobile web filter and logging of device and networking metadata to facilitate investigation of attacks.

Your Apple ID account has been locked due to unauthorised login attempts. Please login here and verify your information

bit.ly



Final Notification

Your Apple ID is due to expire today. Prevent this by confirming your Apple ID at <http://update-apple.uk>

Apple Inc

Device compromise

How can my mobile device be compromised:

let me count the ways. Devices can be jailbroken, known vulnerabilities can remain unpatched, malware can be installed, developer mode enabled, legitimate apps subverted with a rogue SDK.....the list goes on.

Device compromise



SIDELOADED APP

Malicious App downloaded from unofficial app store



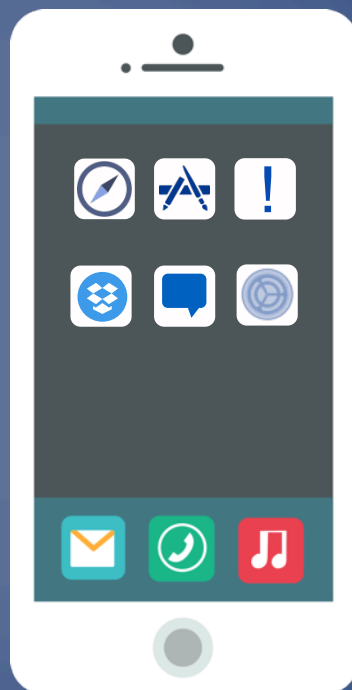
MALICIOUS SDK

Malicious SDK embedded in otherwise benign app



Wi-Fi

Malicious code installed via Wi-Fi subsystem



PHYSICAL CONNECTION

Malicious code infection via cable connection to compromised device



APP STORE DOWNLOAD

Malicious app not identified in review process



MMS

Malicious code installed through vulnerability in MMS



BLUETOOTH

Malicious code installation exploiting vulnerability in Bluetooth radio subsystem

Device Compromise

Jailbreaking

Lets first talk about jailbreaking.

By this we mean the deliberate attempt to get root access to a phone in order to do things which would otherwise not be possible.

For example, an end-user might want to install an app which is not available from the App Store or to replace the version of the operating system provided by the manufacturer with another one.

Of course when we say end-user we don't necessarily mean the 'owner' of the device. An end-user could be someone who has managed to get their hands' on someone else's device and wants to subvert it in some way.

Once a phone is jailbroken, for whatever reason, from a security perspective, all bets are off. It becomes impossible to rely in any way on the operating system's security model.

A device which has been compromised to this extent should not be given access to sensitive corporate data or systems. Knowing whether or not a device has been jailbroken is critical. Mobile Device Management systems are designed to detect jailbroken or rooted devices but shouldn't be relied on exclusively.

Device behavior should also be monitored to detect anomalous activity which might indicate that a device has been compromised .



Device Compromise

Vulnerabilities

Vulnerabilities are flaws in the security system of the underlying device. By attacking these vulnerabilities hackers are able to get the device to do things which would otherwise not be possible without the consent and knowledge of the user.

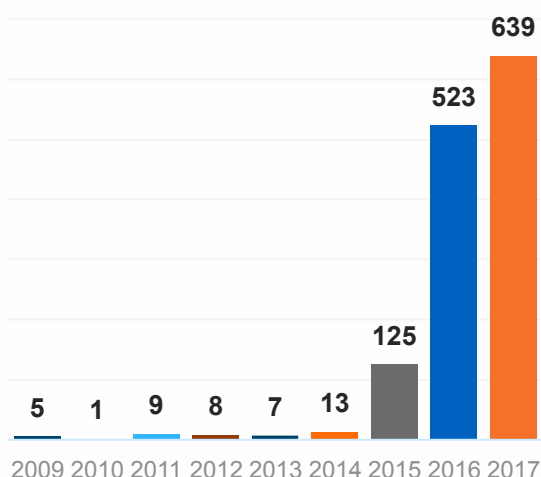
A vulnerability can be exploited to do a wide range of potentially harmful things. At one end of the spectrum a vulnerability may enable an app to show unwanted ads. At the other end of the risk spectrum a vulnerability could be used to remotely record audio from your phone's mic.

Hundred's of vulnerabilities are discovered each year. These can be in any part of the phone - the operating system, the firmware or hardware subsystems such as Bluetooth or Wi-Fi radio. Software vulnerabilities once discovered, are generally addressed quickly by Google or Apple through their regular software update cycles.

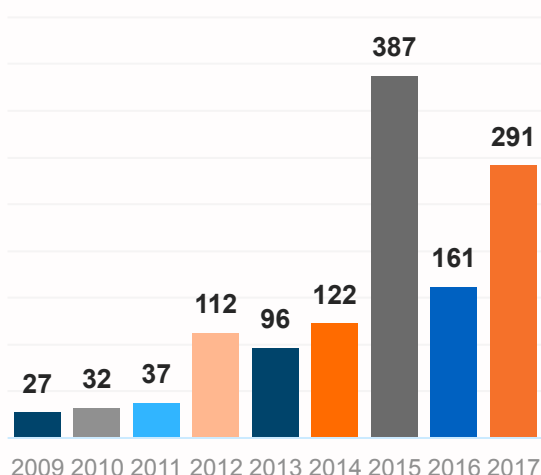
However getting these security updates installed on devices requires action by up to three actors: the end-user (who must agree to install the update) and in the case of Android devices, the manufacturers as well as the mobile carrier.

The reality is that at any point in time there will be large numbers of devices which have not been protected against known vulnerabilities. In addition, there are always as yet undisclosed vulnerabilities (zero days) which cybercriminals will seek to exploit

Android Vulnerabilities by Year



iOS Vulnerabilities by Year



Device Compromise

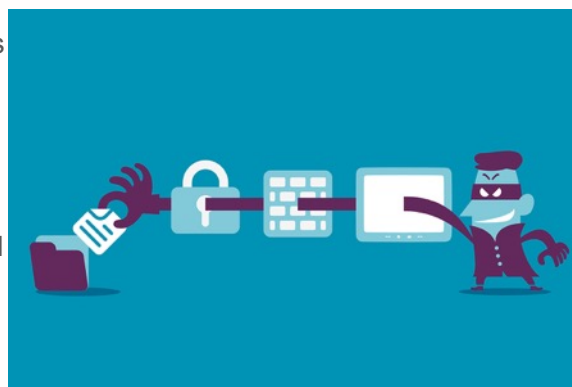
Malware

The most obvious way to exploit these vulnerabilities is with malware. In the case of iOS, the app distribution model offers considerable protection against malicious software. Apple has been very effective at excluding malicious software from the App Store. Getting an app on to a non-jailbroken device other than through the App Store is confined to a small number of circumscribed use cases e.g. via enterprise distribution or app testing software.

However, as demonstrated by XcodeGhost, there are always chinks even in the best defended fortress. XcodeGhost refers to a modified version of the iOS Xcode development environment. Apps developed with XcodeGhost were compromised in a way which was not identified by the App Store review process and resulted in a not insignificant rate of infection. Other malware such as AceDeceiver and Wirelurker has shown that it's possible to infect an iOS device when physically connected to a compromised Mac or PC. Finally, malicious profiles are also a problem.

Pegasus, the most powerful yet disclosed iOS breach, managed to completely bypass Apple's mechanisms for preventing malicious software installation. It exploited a trio of vulnerabilities known as Trident to perform a jailbreak on an end-user device without the end-user's knowledge. Installation was through an MMS message sent to the target device. Once the embedded link was clicked the process of infection commenced. Apple has since patched these vulnerabilities but Pegasus was a powerful demonstration that complacency about iOS and malware is ill advised.

The more open nature of Android means that there is a non trivial level of malware on Android devices. Malicious software has on multiple occasions passed Play Store approval. In addition large numbers of legitimate apps have been infected with dangerous code through the incorporation of compromised SDKs. Google's anti-virus program 'Verify Apps' means that known malware can quickly be identified on devices but, without user action, malicious apps are not automatically removed.



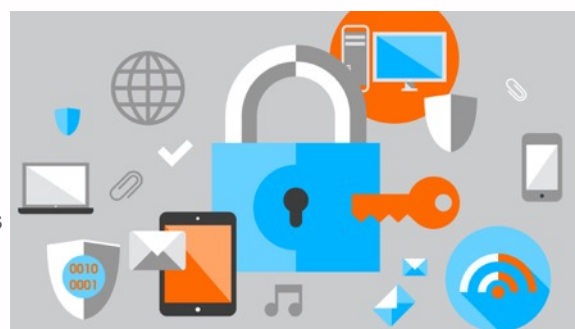
Device Compromise

Countermeasures

The key to protecting against device compromise is continuous monitoring of device security health. This means monitoring configurations and behavior. EMM solutions will generally include the ability to monitor the basic security configuration settings. In many cases it will be possible to use EMM to enforce device configuration policies.

A Mobile Threat Defense (MTD) solution like Corrata's will also ensure that a broader range of relevant settings are monitored. An MTD solution can check whether end-users have impaired device health by changing settings which will leave the device vulnerable. For example turning on USB debugging, allowing sideloading of apps or enabling developer mode. Worse still, end-users can undermine some inherent protections by disabling Google's Play Protect or Apple's Fraudulent Website Warning.

However, it's essential that in addition to monitoring configuration, you also monitor device behavior. The most dangerous threats will be designed to by-pass the standard device level and EMM enforced controls. The only way of detecting them is through continuous monitoring of device behavior. Your mobile threat defense solution must incorporate the ability to capture what's happening on the device in a timely way. With good data and the right analytics, an advanced mobile threat defense solution like Corrata will help protect against even the most sophisticated attacks.



Infrastructure compromise

Wi-Fi's security problems are a combination of the nature of the technology and the business model associated with public Wi-Fi networks.

Wi-Fi is provided for free at a wide range of locations by organizations in hospitality, travel, education, entertainment and public services. Unlike mobile operators whose business is based on charging for their connectivity, Wi-Fi is generally provided as a complement to core business. Wi-Fi at hotels, coffee shops and other places is often administered by staff without strong IT skills or security knowledge. Systems can easily be misconfigured, lack the latest security patches and will often use domestic rather than enterprise grade equipment. Access points are rarely in physically secure locations which make it trivial for an attacker to compromise the device with malicious software. Public Wi-Fi networks are rarely monitored for threats or suspicious activity. Free Wi-Fi is provided by people whose main objective is to have a sign saying 'free Wi-Fi' to draw business and not by people concerned with the security of your data!

Rogue or fake access points are another source of risk to your data when you're browsing online. It's trivial to quickly setup a laptop as an access point in a hotel lobby and then 'entice' devices to connect. Once traffic is captured in this way there are multiple techniques for stealing data, even data that is encrypted.

It's important to understand that even if you are using a public Wi-Fi connection which is password protected your online activities are still vulnerable. If the network is public then hackers can access the

network too. It is always better to assume any public Wi-Fi network is a high-risk place to go online and that your traffic will be exposed to sniffing (i.e. potentially monitored by unauthorized third parties who you don't want to see your data). Strong Wi-Fi encryption helps (though even WPA2 has been shown to be vulnerable) but there are plenty of other security gaps that can be exploited by hackers.



Infrastructure compromise

Three easy steps to make your company and staff's data more secure:

Make sure all corporate apps use encrypted communications.

A hastily launched or upgraded app developed internally or by a third party on behalf of your company may not use encryption at all times. You can use a product like Corrata to monitor unencrypted communications from wireless devices. This will help to identify potential security issues.

Encryption remains the bedrock of keeping your data secure but the second line of defense is using networks whose integrity you can rely on.

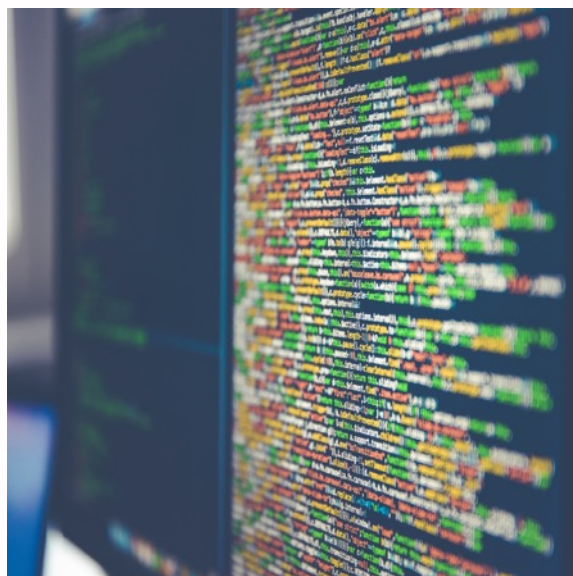
Use cellular data whenever possible for work related communications.

The big advantage of cellular radio networks over Wi-Fi is that all traffic over the radio interface is encrypted. In addition, it is very difficult to fool a device into connecting to rogue infrastructure. While in the past roaming data cost and network speed would have been a concern, however, this is less of an issue now as costs have fallen and 3G or 4G is readily available.

Typically business use is relatively low bandwidth, particularly when compared to non-business use like video streaming for social media and entertainment apps.

Alert users to the distinction between trusted and untrusted wireless networks.

Trusted networks include the corporate WLAN, the cellular network and, generally, staff's home Wi-Fi. Everything else should be considered as untrusted and not suitable for business use. Employees need to be aware that their privacy and security, and that of their employer, are compromised when they use these networks outside the safe zone.



Conclusion

We have entered the era of mission critical mobile. Mobile devices are supporting more and more key enterprise processes and data. For information security professionals this requires a keen focus on a range of familiar and unfamiliar threats and a thorough understanding of the strengths and weaknesses of the mobile platforms. This whitepaper has sought to provide a starting point for considering these issues in the specific circumstances of your organization. It provides a framework for reviewing mobile threats in terms of people, devices and infrastructure. It makes clear that there is no room for complacency.

The last ten years has shown that there are multiple paths through which this new computing platform can be compromised. The good news is that a new class of security solution - Mobile Threat Defense - is emerging. The best Mobile Threat Defense solutions have been designed from the ground up to address mobile specific challenges rather than re-purposing the endpoint protection technologies of the past. These solutions successfully balance the sometimes competing priorities of security, user experience and privacy and complement existing investments in EMM. To learn more about Corrata's Mobile Threat Defense solution visit www.corrata.com

