MWR INFOSECURITY

CPNI
Centre for the Protection of National Infrastructure

Mobile Devices

Guide for Implementers

February 2013

Introduction

Modern working practices have seen radical changes in just a few short years. Today, business is increasingly likely to be mobile – conducted using devices that might not have existed even five years ago. As such, new and exciting ways of working have evolved very rapidly; and while this can bring many benefits to a business, there are also new risks that need to be appropriately managed.

This document is a guide for implementers: people who will be deciding the specific policies and controls that their organisation will use to secure its assets while opening up new ways of working. Also available from CPNI and MWR are two further white papers aimed at management and executive levels.

This implementers' document is designed to help you navigate the complexities of designing a robust mobile devices strategy. It covers the background to mobile working, the areas you need to consider when designing a strategy, and some of the controls you might want to implement. Also included are recommendations for further reading and case studies from MWR's experience that demonstrate some of the less obvious aspects of mobile device security. However, this document does not contain a set of rules or tick-boxes, such as 'on iPhones, set encryption to X algorithm with this setting'.

As you will see from the document, each organisation will require a different set of policies, which must be carefully considered and understood to gain maximum benefit while reducing risk to acceptable levels. With mobile device policies, as with suits, one size sadly does not fit all. If the budget is available, a bespoke one will undoubtedly offer the best fit.

MWR would like to acknowledge the help and support of CPNI in producing this Mobile Devices document and the accompanying products.

Contents

Blink and You Missed It

The speed at which mobile devices have spread has been breathtaking. Three years ago, in 2010, the iPad had not yet been released but today it is a common sight in all aspects of life. Meanwhile, many of the reasons for mobile devices becoming so popular in personal life are equally valid in the business world. Modern businesses are harnessing the power and popularity of these devices to help them work more effectively internally, and also to interact with customers in new and better ways.

Medical staff, for example, record patient details and view test results on tablets, while many airlines now offer iPads on flights instead of seat-back entertainment – and banks often allow customers to conduct their business from foyer-based tablets instead of waiting for a cashier. Exciting as the many business examples of mobile device use might be, all come with risks that differ in their severity (and often nature) from risks that organisations have been managing for decades. It is simply not possible to manage those risks by applying the old risk models to the new technologies.

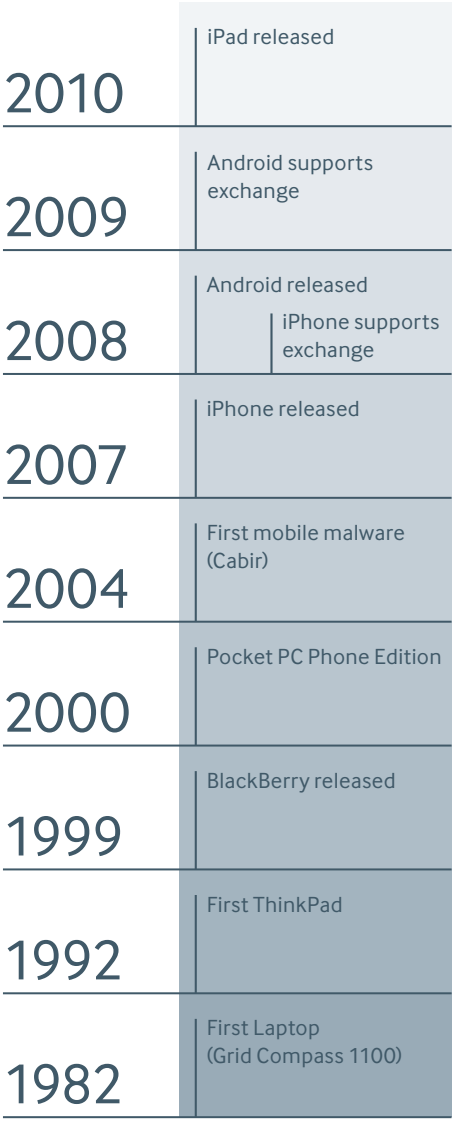
However, there are many reasons why an organisation might seek to introduce a mobile devices policy. A common motivator, and one that is likely to be responsible for the examples given above, is 'top down' – in other words, senior management levels within an organisation have perhaps identified business opportunities that require the use of mobile devices, or maybe they just want to support modern ways of working. Alternatively, the motivator could be 'bottom up', where employees are pressuring IT staff and management to be allowed to use their beloved personal gadgets for work purposes. Employees are increasingly likely to be communicating and conducting their lives on their own mobile devices and it is natural for them to want to extend that flexibility to their work. Users now find themselves emailing friends from the bus rather than having to sit in front of a desktop, and they might wonder why they can't have similar flexibility at work. Crucially, research and experience indicate that where users are not provided with that flexibility, they simply create it for themselves – introducing potentially serious risks of which their employers are unaware.

As a result, organisations are starting to recognise the importance of constructing a mobile devices policy that enables them to understand and manage those risks. In so doing, they can become confident that these new ways of working will not lead to data breaches or other asset compromise. Furthermore, many organisations accept that the radical changes of the last few years are unlikely to suddenly stop; and by building a firm base now, it will be simpler to support future devices and ever-evolving styles of working.

The changes that a mobile devices policy must take into account are significant. First, the range of devices now used for work has hugely increased. Instead of just corporate-build desktops, employees are likely to be using laptops, portable storage such as USB drives, smartphones and tablets. All these devices have risk profiles that are different from desktops, not least because of their portability. USB drives are able to store huge amounts of data, possibly even the majority of an organisation's assets, in a small and readily losable form. Smartphones and tablets, despite offering much of the functionality of full computers, do not have the same control models or security controls as computers and attempting to apply a computer's security policies and procedures to such devices will not work. Even within each class of device, there is immense variety: Android phones have a different risk profile from iPhones and, to further complicate the matter, different versions of the same device can have different risk profiles.

There is also the changing pattern of device ownership and control models to consider. In the past, employees were issued with a hardened corporate desktop plus possibly a locked-down BlackBerry and, aside from occasional webmail, they would use those devices almost entirely for business purposes. Today, many organisations support BYOD (bring your own device), where employees can bring their personal devices and have access to work email or other functionality provisioned. The degree of hardening in BYOD can vary, with some organisations requiring the personal device to be wiped and re-provisioned as a corporate device, while others just enable email access on an otherwise unprotected device. Corporate-owned devices are increasingly used for personal purposes too.

Timeline of events



As people's lives are more widely conducted on the internet, a work laptop is highly likely to be used for social networking, online dating or entertainment, instead of purely for work purposes. As well as the technical and security implications of these shifting ownership models, there are also significant legal issues to be considered as the previously accepted divisions between work and personal data and devices no longer apply.

Working locations have also changed. Whereas, in the past, employees were likely to work from a location managed and secured by their employer, possibly with some form of internet portal-based home working, employees are now able to conduct business from almost any location. Before mobile working became possible, a sales person might have visited a potential client with brochures and forms, and then processed those forms back at an office. Now, however, they are likely to take a laptop and capture the information at the client's location, processing it and uploading it immediately by Wi-Fi or mobile internet connection. This introduces risk, as an organisation can no longer rely on its physical security measures to protect data. Devices that are carried and used in public or even hostile areas frequently contain sensitive data as well as credentials and access mechanisms to greater data stores.

Another challenge arises as people become increasingly IT literate. In the past, very few employees would have attempted to break restrictions placed on them – and, had they tried, they would probably have failed to do so. Now, however, employees are generally more able to bypass poor controls; and to seek advice via internet forums to help them bypass more advanced controls. Web searches for bypassing specific controls on mobile devices yield worryingly large numbers of results. Hence technical controls cannot be trusted in isolation. Instead, it is vital that employees are educated – and then trusted.

As such, a mobile devices policy can be challenging to construct and implement. However, it is crucial to have one in place, as mobile devices will in all likelihood be used in the organisation, regardless of official policies. If users are enabled and supported by the organisation, then the risk is known and manageable. In the absence of policies, that risk is still present, but unknown and unmanaged.

Different organisations take different approaches to implementing a mobile devices policy. While one organisation might choose to allow employees to use one of the top four smartphone platforms for emails, another might only want to allow the executive team to have iPads. It is entirely reasonable that an organisation could start with a small project, such as tablets for executives, and then slowly widen the policies to encompass the majority of employees and devices.

However, it is recommended that all organisations should at the very least seek to understand employees' real usage of mobile devices for business purposes, as only then can the process of accurately assessing risk begin. Experience shows that understanding and working with employees is a critical step in managing risk – while retaining the numerous benefits possible from the business use of mobile devices.

Examples of ownership models

	CORPORATE OWNED	EMPLOYEE OWNED
CORPORATE MANAGED	Typical locked down 'work phone' like a BlackBerry	Employee purchased but locked down through policy/MDM
NOT CORPORATE MANAGED	Organisation merely provides device	Employee provisions access to own device

Mobile Working Considerations

Changing Ownership and Usage Models

The Challenges

Changing patterns of device ownership and usage are among the most significant information security challenges to emerge in recent years.

In the past, employees were satisfied with a thin client or standard corporate desktop but recent years have spawned radical changes. Now, there is an increasing expectation that corporate machines can be used for personal online purposes, while there has also been the emergence of BYOD (bring your own device), where personal machines are used as primary work devices.

The use of corporate machines and identities for personal purposes substantially increases the attack surface area: employees are likely to visit a great many more websites, including sites with poor security. An example of how this practice can threaten corporate security is the all-too-common case of large, popular websites being hacked and passwords leaked. Indeed, when conducting penetration tests, testers will often use such public password dumps to identify corporate email accounts and passwords.

Another significant issue is that social networking websites can help an attacker to understand the social dynamics of a company and identify links. A recent presentation demonstrated that even experienced security professionals can be duped into adding a non-existent person as a friend, thereby providing valuable intelligence to an attacker[1].

Meanwhile, using personal devices for corporate work presents multiple challenges. One option (recommended by CESG for government departments[2]) is that if an employee wishes to use a personal device, it is wiped and provisioned/locked down to the same degree as a corporate-owned device. While this is the most secure approach, it is rarely acceptable to enterprise users as, depending on the degree of the hardening, they are likely to find themselves unable to use many of the features for which they originally purchased the device.

There are a number of threats that can arise as a result of mobile device use. The diagram below shows these threats and gives the ways in which those threats may occur.

Threats from corporate use of mobile devices

LOSS OF CORPORATE DATA

Physical Compromise of Device
- Device lost
- Device stolen
- Decommissioned device

Logical Compromise of Device
- Malicious app installed by user
- Compromise of user application
- Malware infects device
- Insecure corporate application enables access to data

User Action
- User stores data inappropriately
- User tricked into disclosing data as a result of social engineering

Communications Compromised
- Cleartext data intercepted in transit
- Encryption key disclosed allowing data decryption
- Insecure encrypted connection

Contamination of Device
- User accesses information beyond their privilege
- Personal and corporate data combined

TRUST RELATIONSHIP COMPROMISED

Compromised Device Used to Pivot into Secure Environment
- Wi-Fi credentials used
- Poorly secured VPN environment

SECURITY MODEL WEAKENED

Bypass of Security Controls
- User jailbreaks device
- User bypasses application level control (eg sends data to personal email account)
- User provisions own access

A more common approach is to leave the personal data present, while allowing a restricted degree of access to corporate resources on the same device. This carries significant risks, however, as a device over which the organisation has little control is still being used to access the organisation's assets.

The examples opposite illustrate how the goals of the user and the organisation can appear to be incompatible. Generally, an organisation wishes to restrict what a user can do in order to reduce security threats, while a user wants to be able to use their device freely. The problem is particularly difficult to solve when it comes to personally owned laptops, since an employee is almost certain to be an administrative user on their own laptop – and hence can easily circumvent any controls placed on it. What's more, an employee's personal laptop is significantly more likely to become infected with malware than a corporate machine, as there are fewer controls preventing infection – and users are likely to engage in a variety of riskier activities on their own device.

It is therefore recommended that personal laptops are not permitted to access corporate resources. However, if such an approach is not workable, there are some potential solutions that could enable an employee to use a personal laptop safely. These are discussed in the 'Data Segregation' section of this paper.

In contrast, personally owned smartphones and tablets can generally be supported more safely, as a user does not typically run as a root or administrative user. It is therefore possible to enforce controls that are harder to bypass – although, for the controls to be effective, the model requires a method of detecting and preventing 'jailbreaking'.

Jailbreaking (also known as rooting) removes many of the built-in protections of the operating system and sets the owner up as an administrative user on their smartphone or tablet, enabling them to bypass controls placed on the device. This is covered in more depth in the 'Jailbreaking' section.

A situation that sometimes results from an organisation's reticence to give its official support to the use of personal devices is that the devices are used unofficially, with the organisation's inadvertent support. As people become ever more IT literate, there are increasing instances in which employees provision their own access in lieu of corporate-sanctioned access, or bypass poorly implemented controls. A fairly extreme example was that of a high-level executive whose son installed a poorly protected wireless access point at his office to allow him to use his iPad, but a more commonly observed situation is where employees use externally accessible exchange servers, or webmail, to provision their poorly secured personal mobile devices with corporate email access.

Solutions

Technical controls that address mixed ownership/mixed use devices are improving rapidly, particularly for smartphones and tablets. A variety of controls are available, either built into operating systems or available as third-party software.

The key technical control is data segregation (see later section) as it allows the separation of personal and corporate data, even on one device. Another crucial technical control is asset management (see later section) as it allows an organisation to gain visibility of what devices are being used to access corporate resources and hence to apply some level of security. The third significant technical control is data loss prevention, or DLP, software (see later section), which prevents users from inappropriately exfiltrating data.

Spanning all these controls, however, is the need for a clear, coherent and encompassing policy or policies regarding mixed use devices. If an organisation decides to support mixed use devices, whether corporately or personally owned, policies are required to cover what can and can't be accessed – and on which devices and under what circumstances. Employees need to fully understand what they are allowed to do; and why these policies have been adopted.

An increasing problem is that while many useful technical measures exist, it might be deemed unacceptable to apply those controls to personal devices. For example, mobile device management could allow administrators to set the password requirements on a personal phone so that passwords must be at least 10 characters. However, an employee could well be unhappy at having to enter a 10-character password every time the phone is unlocked and might therefore attempt to remove the control, or set a weak password such as 'qwertyuiop'. A recent survey indicated that a significant proportion of employees will attempt to bypass controls they perceive to be unfair[3].

Incident response policies are particularly important. For example, if a malware infection is suspected on a corporate machine, there is often an established process to remove and investigate that machine. Policies are likewise required for a potentially infected personal device; plus it's also worth considering what would happen to that personal device if an employee were suspected of malicious or inappropriate activity.

Policies need to be communicated effectively to employees, as well as the risks to corporate assets should they not comply. Controls to support these policies should be effectively implemented – and monitored to detect attempted bypass. If it turns out to be impossible to construct a policy that both satisfies corporate requirements and is acceptable to employees, then it is strongly recommended that the behaviour in question is disallowed, and controls are put in place to restrict and detect access that is in breach of the policy. This might require heightened security for externally accessible resources or port-level security to prevent personal devices from being connected to the corporate network. However, it is essential that – while bypassing controls must be detected and addressed – a culture of amnesty should nevertheless be encouraged so that employees do not fear reporting security issues.

Mobile Working Considerations

Jailbreaking

The Challenges

Jailbreaking, also known as rooting, is the act of elevating privileges on a smartphone or tablet in order to bypass restrictions that have been placed there by the manufacturer. It can be thought of as the equivalent of a user exploiting security vulnerabilities on a laptop to become an administrator instead of a regular user. People jailbreak their devices in order to gain greater control or run software that has been prohibited by the manufacturer. For reasons of security and content protection, mobile devices impose restrictions on what applications can do, and users often seek to bypass these restrictions in order to allow new functionality. As such, there are thriving jailbreak communities, particularly for iPhones, iPads, and Android devices. These communities regularly release jailbreaks for new devices and some Android manufacturers even support rooting officially. Jailbreaking activities have now been developed to the point where a person with little technical knowledge is still able to jailbreak their device.

However, jailbroken devices can present a risk to corporate assets as key security controls will have been deactivated or circumvented. Specifically, the process of jailbreaking can allow rogue applications to access data which would otherwise be restricted. Also, the applications available to jailbroken devices are typically unvetted and hence there is a higher risk of malware than there would be through acquiring applications from an official store. A significant problem is that the user will have full, or close to full, control of the device – so it becomes possible to bypass many of the controls that have been placed there for the protection of the data. Finally, many exploit mitigation controls are also deactivated during the jailbreaking process, meaning a device is less well protected than it would otherwise be.

Solutions

It is strongly recommended that jailbroken devices are not allowed to access corporate resources and that employees are made clearly aware of this fact. (It is often possible to restore a jailbroken device to its original state, albeit with a return to restricted functionality.) Owing to the significantly increased risks presented by a jailbroken device, MWR believes it is worthwhile for an organisation to put all necessary effort into detecting such devices – and into preventing them from accessing corporate resources.

Many MDM solutions purport to detect jailbroken devices; however, the effectiveness of these solutions can vary and should not be relied upon. In one case, an MDM solution was found by MWR to be 'detecting' jailbreaks simply by looking for the presence of a file that is commonly created during the jailbreaking process. This proved trivial to bypass, resulting in the MDM solution reporting a non-jailbroken device. Before purchase, potential MDM solutions should be researched to determine how effective the jailbreak detection is.

Manufacturers are often well-motivated to prevent unauthorised jailbreaks. This is because the process can allow bypass of protections on such content as applications, music and videos. If a manufacturer were seen not to be preventing jailbreaks, they could well encounter difficulties in licensing content, as the safety of the content could not be guaranteed. Vulnerabilities that are being exploited for jailbreaking are rapidly patched on Apple devices and are often patched, although less rapidly, on Android devices. Hence a key defence in preventing jailbroken devices from accessing corporate resources is patching – and ensuring that all devices that access corporate resources are updated to the latest version.

Finally, users should be educated as to the risks of jailbreaking devices and why it is at odds with corporate security policies; not to mention their own security needs.

Technology Refresh and Disposal of Devices

The Challenges

At the end of their lifecycle, mobile devices such as laptops, USB drives and smartphones/tablets are generally replaced by newer devices. Thanks to the wear and tear that mobile devices suffer, and the rate at which newer devices with increased functionality are released, the lifecycle is typically quite short; and organisations need to ensure that corporate data is not exposed once a device has been decommissioned. There are numerous examples of devices thrown away or resold with sensitive information still stored on them. Motivated attackers might even attempt to collect decommissioned devices specifically to perform data recovery.

In the past, devices were frequently decommissioned by running disk wiping software that copied random data over the contents of the disk multiple times to prevent recovery of data. However, this approach does not translate to many mobile devices as they lack traditional magnetic disks. Flash memory (as used in smaller USB drives, smartphones/tablets, and some laptops) uses a process called 'wear levelling' to ensure the longevity of the memory by not repeatedly writing to the same region of the storage medium. This can frustrate efforts to securely erase data, as software is not able to specifically erase a given region – as is possible with a magnetic drive[4].

A different challenge arises when personal devices are used for corporate work. Such devices, particularly smartphones, could well be replaced as often as once a year and, depending on the usage permitted by the organisation, might contain important corporate information. Individuals rarely destroy their devices, not least because they have a monetary value. A further problem is that when upgrading, individuals will often allow shop staff access to the device to migrate data to the new device. Although no loss of corporate data has yet been reported as a result of this activity, there is plenty of evidence of shop staff abusing their position of trust in other ways.

Solutions

Where machines use traditional magnetic platter-based hard drives, it is still possible to thoroughly wipe them. Corporate policy should include a secure erasure process, regardless of whether the drives were encrypted, with a thoroughness appropriate to the sensitivity level of data they contain.

It is recommended that even if no sensitive data is thought to reside on the drive, it is wiped with at least three passes of random data. If drives are to be repurposed inside the organisation, they can be wiped and then redistributed. However, if they are not to be reused, MWR recommends that drives are physically destroyed.

As mentioned above, it is strongly advised that personally owned laptops are disallowed for work purposes due to the inherent risks. However, if an organisation does support such use, policies should be designed to cover an employee replacing their own laptop or leaving. The preferable option is that all personal data is copied to an external drive, the hard drive securely wiped and then the personal data replaced. At the very least, corporate data and all empty hard disk space should be erased with a secure tool – although this can still leave corporate data potentially exposed to a technically advanced attacker.

Flash-based storage such as USB sticks and smartphones/tablets should be wiped using an appropriate utility and physically destroyed if possible. For example, on many devices such as Apple iPhone and iPad, a factory wipe is available that instantly discards the encryption keys for the memory. There are no publicly reported successes in recovering data that has been wiped in this fashion, but it is not impossible that a very advanced attacker will, at some point, do so.

Employees should be instructed to contact IT support staff if they are upgrading their smartphone or tablet. Support personnel can then de-provision the current device and re-provision the new one. It might be wise for an organisation to collate a guide for migrating data so that employees do not have to rely on external help; and employees should be clearly instructed to securely wipe their device before disposal. Alternatively, the organisation could choose to provide a service for employees to use.

Mobile Working Considerations

Loss of Device

The Challenges

By their very nature, mobile devices are at high risk of being lost or stolen, with smartphones and tablets regularly targeted by thieves. A large organisation is almost certain to experience the loss or theft of corporately owned mobile devices on a fairly frequent basis, while personally owned equipment is arguably at even greater risk (since an employee will typically carry the device around at all times, including socially).

Should a device be stolen or lost, the assets contained within it may be compromised – not to mention the potential for unauthorised corporate access via the device. For example, an attacker might be able to identify a corporate Wi-Fi passphrase and gain further access via the network. Many examples of public data breaches are a result of the loss of a mobile device, typically a laptop or USB key. Perhaps surprisingly, however, there have been few publicly reported cases of data breaches arising from smartphone or tablet loss, which sits at odds with surveys indicating that the majority of companies have experienced the loss of such devices[5]. It might be that advanced attackers favour the theft of a smartphone or tablet (as the controls on the device are generally weaker than on a hardened laptop), but the act has been disguised as a common theft rather than a targeted attack.

Solutions

A crucial technical control to mitigate device loss or theft is encryption of data at rest (see later section on 'Encryption'). The importance of effective encryption cannot be overstated and organisations should not allow data to leave their premises on unencrypted devices. However, this can be a challenging policy to adopt as encryption is implemented in a huge variety of ways depending on the device in question.

Smartphones and tablets are particularly challenging: even subsequent versions of the same product can require encryption in different ways. Just one example is the original iPad, which can only be encrypted if it has had a factory reset since the release of iOS 4.0. As such, corporate policy needs to address specific devices, with encryption implementation and efficiency studied for each and every device the organisation wishes to support.

A further problem with encryption is that its effectiveness is tied to the password on the device. A weak password/passphrase means the encryption will be of little use. Yet insisting on a stronger password has its own challenges, since smartphone and tablet users will need to enter the password each time the device is unlocked. For a smartphone, and particularly a personally owned smartphone, this can be multiple times an hour, and a user could well object to having strong password requirements set on their device.

A possible way to allow weaker passwords is to apply settings that cause a device to be wiped/erased if the password is incorrectly entered multiple times. However, the adopted policy must be communicated effectively to users, or organisations run the risk of users intentionally choosing weak passwords that are easy to enter rapidly. Users should also be made aware of the risk of attackers observing the password being entered or being able to derive it from grease marks on the screen.

Meanwhile, employees need to be aware of the procedure for responding to the loss or theft of a device. Part of this procedure should be to immediately inform both the organisation's security staff and the police. Police tend to respond rapidly to the reported theft of mobile phones and tablets, particularly if a tracking mode has been enabled (see 'Remote Track and Wipe' section). This is because there is a narrow time window before an attacker can be expected to disable the tracking and so, in that window, the police have a high chance of apprehending the thief.

Security staff might wish to remotely wipe the device. This is only possible if the device still has internet connectivity and there could be significant legal issues if the device is personally owned. This is discussed more fully in the 'Remote Track and Wipe' section. If a personally owned device can be securely but selectively wiped, it is strongly recommended to do so at the earliest opportunity; and employees should be incentivised to rapidly report lost or stolen devices.

In addition, security staff will immediately want to prevent any access the device might have to networks, as well as to services such as email, to reduce the data exposed. Ideally, information held on the mobile device will already be recorded as part of an asset management process. In the event of theft or loss, the information held on the device can then be assessed to determine the need for any operational changes. For example, if it is likely that an email chain exists on the device that discusses security arrangements at a site, those arrangements might need to be changed or monitored in greater detail. As a component of cancelling access, staff could also choose to cancel the SIM card's access to the mobile network. However, this should only be done after remote wipe commands have been communicated.

Training

The Challenges

Technical controls have improved substantially in recent years. There are now many more options to help secure devices and prevent dangerous or malicious behaviour than existed even a few years ago. However, an emerging issue is the need to adopt a system that works for the individual employees and does not result in them attempting to bypass the controls.

This can be increasingly difficult for several reasons. First, people have generally become more highly skilled in technical matters and are hence able to bypass poorly implemented controls. They are often able to find both resources and tools on the internet to help them bypass controls. Recent research indicates that a significant proportion of employees will attempt to bypass controls that prevent them from using their devices in the manner they want to[6]. A common way to do this is to jailbreak devices, which removes many of the protections that the controls rely on to be effective. Employees who use personal devices for work purposes are more likely to become frustrated with what they see as overzealous controls, preventing them from interacting with the device in the way they want. This is particularly true for laptops, as the owner is likely to be the administrator on the device and so can bypass controls with ease.

A separate issue is that while it might be possible to apply a control to a device, it could well be inappropriate from a legal or human resources standpoint. An example of this is 'remote wipe'. By provisioning a personal device such as a smartphone or tablet with exchange access or a separate MDM solution, a corporate administrator gains the ability to wipe the device remotely. This is a sensible control for a corporately owned device as it allows an administrator to respond to the theft or loss of the device by removing corporate data. However, on a personal device it raises significant issues as the user's personal data will also be wiped. The user might not be aware that the device could be wiped and hence might be upset – or even litigious – should it happen. Alternatively, a user could be aware of this possible outcome and simply avoid telling security staff in the event of a loss or theft.

In short, for effective security it's important that employees not only work within the controls that have been imposed, but that they also adopt secure practices. By doing so, employees can help to significantly reduce the risk to corporate assets. Conversely, poor security practice can result in employees inadvertently putting corporate assets at risk, despite the presence of controls.

Solutions

Once policy has been decided, employee training is a key step in helping individuals to understand the controls that are in place – and, very importantly, the reasons for them. For example, if employees are allowed to access corporate data on their personal devices, but the decision has been made to require a long passphrase, it's helpful for the employee to understand that in allowing them to use their own device the organisation is taking a risk. This can be supported with real world examples. The employee is then less likely to attempt to bypass the long passphrase or set a weak passphrase. It should be made clear to the employee that if they are not comfortable with the security requirements, then they should not use their personal device for work purposes.

Employees should also be trained to understand and agree to all aspects of the policy, including those that might be seen as problematic if used – such as remote wiping. If the remote wiping of a lost device (for example) is part of the policy, employees need to be aware of what the result would be; and the training could perhaps include guidelines on how to minimise lost personal data should such a situation arise. In the case of all such potentially problematic controls, it is recommended that the organisation obtain a signed agreement from the employee at the outset. At this time, the reasons for the controls should be clearly explained and the employees advised that if they are not happy with the control, they might prefer not to use their personal device for work.

Employees should also receive training in secure practices. This training needs to be relevant to the employee's circumstances and working conditions, and the specific mobile devices used. Training should include: awareness of threats, appropriate password/passphrase choice, the dangers of jailbreaking, the dangers of installing untrusted software/apps, and the risks of non-trusted networks. In addition, training should cover the motivations for enabling new working methods and the benefits of those methods to both the user and the organisation.

Employee training should also cover the reporting of incidents, both proven and suspected. It is recommended that a culture of amnesty is adopted so that employees who have bypassed controls will not fear reporting incidents. Furthermore, organisations might wish to incentivise the reporting of incidents through social or financial rewards.

Mobile Working Considerations

Working from Untrusted Networks

The Challenges

Modern working is increasingly mobile. Whether working from home, in the field or while travelling, it is no longer the norm to access emails and make business-related calls solely from a corporate desktop in a physically secure building. Many companies issue staff with laptops or smartphones/tablets so that information can be captured, delivered and manipulated from any location, rather than having to return to the office before the data is processed.

To realise the full benefits of mobile working, it is necessary to allow the mobile devices to access both the internet and corporate resources. Typical connections used by mobile workers include home Wi-Fi, client/partner Wi-Fi, public Wi-Fi, and 3G/4G/mobile internet. This generally means using non-trusted network connections and hence potentially losing control of the data.

Working from non-trusted networks can introduce risk to the devices through several vectors. The most widely understood is the interception of data. As the network is not under the control of the organisation, fewer guarantees can be made that there is no malicious interception or modification of the data. A poorly protected network will be easier for an attacker to join and manipulate, or the network itself could be operated by an individual with malicious intent. As shown in the illustration, home Wi-Fi and well-protected client/partner Wi-Fi tend to be more resilient to such problems but it should be understood that advanced attackers might still be able to gain access to the networks.

Public Wi-Fi makes it particularly easy for an attacker to gain control over communications and should be treated with caution. Mobile internet such as that provided by 3G/4G dongles or tethering to a phone is generally safe from most attackers, as interception requires specialist hardware. However, more advanced attackers, such as those of nation states or particularly well-funded private groups, could gain access to such equipment and therefore be able to intercept calls and other communications from a targeted employee. Public demonstrations have been given that illustrate the potential for these types of attack[7].

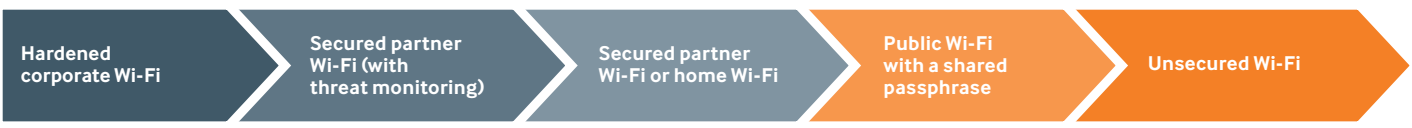
Many business communications, such as email, are likely to take place over an encrypted tunnel (secured with SSL), which makes it very difficult for an attacker to intercept. However, there are many communications of potential interest to an attacker that are not suitably protected. MWR has seen bespoke corporate applications that do not use encrypted links and so any data communicated on a compromised network could readily be intercepted or modified by an attacker.

Another risk is the use of public sites. Take a hypothetical situation in which a high-level employee is using a social network via an airport lounge's Wi-Fi. This connection is rarely well protected and so an attacker would be able to gain access to the employee's social network account. The attacker could then use that access to gain information about the structure of the organisation, identifying important people and routes to them. Alternatively, an opportunistic attacker might simply use this access for defamatory purposes.

Other risks that result from using unsecured networks include increasing the attack surface. In other words, by using an unsecured network the employee opens up a range of possible attacks that would not otherwise be viable. A common entry point onto a device is a browser vulnerability. An attacker with control over a network would be able to (for example) inject exploits into the browsing of the employee and gain persisting control of the device. This is true for both laptops and smartphone/tablet devices. One attack demonstrated by MWR is the compromise of an Android device through a browser vulnerability such that the device can then be used as an audio bug. Alternatively, by simply waiting until the device is connected to corporate Wi-Fi, the attacker can use it as a relay to gain access to the corporate network. As such, it is recommended that electronic devices are not taken into highly confidential meetings or, if they are, the device's batteries are removed.

Another risk resulting from mobile working is the breaking of the control model for corporate devices. Devices can be built to corporate specifications, yet used almost entirely in the field. As such, the devices are configured to receive group policy updates and operating system/third-party software patches from a corporate update server. However, as the devices are rarely used within the organisation's own premises and have tightly regulated access to corporate resources, they are unable to receive updates and will lack critical patches, allowing for trivial exploitation.

Risk of working from different networks



Solutions

Key technical controls that can help mitigate the risks of working via untrusted networks are VPNs, patching, exploit mitigation and antivirus (see relevant sections). However, in order to be effective, the controls must be supported by user education and policy.

Owing to the risks inherent in connecting to untrusted networks, it is recommended that corporate devices are prevented from doing so. This can normally be achieved through group policy in the case of laptops, and MDM solutions for smartphones and tablets. However, restriction of networks is not possible on all devices (notably iPhones and iPads) and so employee training is vital. There might be a requirement for employees to work from specific networks – such as their home, or while out and about. Possible solutions are either to provide all home-working employees with a wireless access point configured to corporate specifications, or to permit specific networks for specific devices. If the latter, it is recommended that employees are given a list of controls to apply to their home network such as passphrase complexity and encryption requirements.

If devices are left in a state where they can connect to arbitrary Wi-Fi, there is a risk that employees will connect to public or otherwise unsecured Wi-Fi. For employees who are required to work from multiple locations, a 3G or 4G mobile connection is recommended, as this is generally safer than allowing arbitrary Wi-Fi connections. A potential scenario to consider is that of employees travelling abroad, where 3G/4G access might be prohibitively expensive and hence there's a need to use internet access provided by a hotel. There is currently no ideal solution to this problem.

Where devices are allowed to connect to networks other than a corporate secured network, they should be provisioned with VPN access. This securely tunnels traffic back to the corporate network, allowing access to internal resources and also allowing for corporate security controls – such as network monitoring – to be applied. Where mobile internet (GPRS/3G/4G) is used, organisations would be wise to investigate obtaining a SIM-authenticated APN (access point name) from their mobile network operator. This acts as a further control by segregating the internet access of an organisation's mobile devices from other communications on the network. However, an APN should be used in tandem with a VPN, rather than in place of it.

Corporate devices used extensively in the field should be configured to remain updated. This could be achieved by using vendor-owned public update servers rather than corporate servers. Alternatively, corporate update servers could be provisioned within the network accessible via a VPN, so that devices can receive updates when connected via the VPN. Major software patches and important policy changes should be monitored to ensure that all relevant devices have received and applied the updates.

When it comes to personally owned devices, the challenge is different, as owners might find such restrictions unacceptable. Effective policies will therefore need to take into account the device, the assets accessible by the device and the usage requirements of the owner/user. It might prove necessary to restrict the access of the device to meet the user's requirements. A potential mitigating solution is to encourage the use of mobile internet (3G/4G) as opposed to public Wi-Fi. The organisation might need to provide its users with a portable Wi-Fi router/3G/4G modem or allow tethering to a smartphone. Users are also more likely to access public websites and services from a personally owned device and hence should be made aware of the risks of doing so from unsafe networks.

Mobile Working Considerations

Incident Management

The Challenges

Changes in the devices used for work purposes, along with changes in working styles, mean that current incident management resources and policies might be inappropriate or insufficient for many modern incidents.

In the past, incidents were likely to be related to breaches of corporate-owned devices on corporate-operated sites. However, with the prevalence of mobile devices and mobile working, many incidents will nowadays involve devices or resources that are not on enterprise-owned sites – and they could well occur outside normal working hours: an employee who has his phone stolen in the early hours of Sunday morning, for example, after a night out with friends.

There are several challenges facing modern incident response, not least of which is the sheer variety of devices that need to be supported. Not only are there different types of devices accessing company resources – including USB drives, laptops, smartphones and tablets – but there are different models and different versions of each device type. Each one could well require support staff to employ different tools and methods to manage an incident. For example, forensic recovery and analysis following the compromise of an iPhone requires different methodologies to a similar investigation of an Android device.

Yet another challenge is the changing model of device ownership. Previously, a device used to access corporate information would almost certainly be owned by the organisation, and hence could be taken from the employee, analysed, or remote wiped without issue. These days, however, organisations are frequently responding to incidents involving personally owned devices – and an employee might not be happy to have support staff perform forensic analysis of a device containing personal data, while remote wiping might also prove unacceptable. Finally, if the employee is suspected of wrongdoing, then investigation, monitoring, and response could all be impeded if the devices involved are personally owned.

As for incidents that occur outside working hours (such as the device stolen in the early hours of Sunday morning, described previously), employees might not have access to a phone or to the number to call to report the situation – and the support centre might not even be operational at that time. And yet when smartphones are stolen, there is often a relatively small time window before attackers disable any remote track/wipe functionality.

Solutions

It is important that organisations develop incident response procedures and policies that are tailored to specific devices. This will involve understanding what is forensically possible for each device and identifying the tools or vendors that will prove useful. Understanding which data or network resources a specific device has access to is also important, as is consideration of device specifics, such as not immediately disabling the device's SIM card (where present) without first communicating any necessary remote track and wipe commands.

Employees should receive training so that they understand the procedure following an incident. The training should cover different types of incidents and the employee's expected response in each case, and should also give the employee clear contact points for queries that do not fit within the defined incidents. Employees should not be discouraged from reporting incidents through fear of reprimand, even if the employee has intentionally bypassed controls.

Ownership is an important consideration in devising incident response policies. An organisation should have a robust and realistic understanding of the devices used to access corporate resources and their ownership. Response policies need to cater for both supported and 'unsupported' ownership models – in other words, when it becomes apparent that employees are using their own devices without official permission.

Where personally owned devices are used, employees need to understand what measures will be applied in the event of an incident. It could well be necessary to have employees sign additional contracts or disclaimers to cover specific eventualities. Some devices and management combinations allow selective wipe of corporate data and these might provide an acceptable solution for both the employee and the organisation. Owing to the legal difficulties of a company monitoring and analysing personally owned devices, however, it is recommended that employees are not permitted to use personally owned devices if they work in areas that are particularly prone to investigation – such as financial trading.

Incident response resources and policies should take into account the time and location of incidents. Ideally, an incident response centre or support desk would be available to employees 24 hours a day, 365 days a year. Employees need to be well aware of the contact details, or be able to obtain them very easily. This might involve an easy-to-remember number or simply having the number readily locatable on a public website or printed on the employee's ID card. As support centres are likely to be publicly discoverable, it is crucial that the centre is able to rapidly authenticate employees reporting incidents.

If it is not possible, or appropriate, to have a full-time response centre, employees should be made aware of the procedure to follow when the centre is unavailable. This might involve contacting an on-call employee or reporting the incident directly to the police.

Software Distribution

The Challenges

Installing third-party software on mobile devices is a primary requirement for many users, yet the way in which the software is distributed is changing, as devices evolve. The model used for desktop and laptop operating systems, i.e. downloading or otherwise obtaining software from a range of sources, has not been transferred to modern devices such as smartphones and tablets.

In order to preserve user experience by regulating the type of software accessible, mobile device manufacturers generally allow for third-party application installation through curated marketplaces. These marketplaces allow manufacturers to restrict the types of application available and to some extent reduce malware infection of devices. However, as the mechanisms for distributing software are dependent on the device manufacturer, the risks of malware vary depending on the device in question.

Apple controls a highly restricted application marketplace and simple installation of a binary is not possible on a non-jailbroken device. Applications are vetted by Apple prior to appearing in the marketplace (although there are indications that this is not a perfect process, as applications occasionally appear in the marketplace with functionality prevented by Apple). For corporate devices, Apple allows the creation of a corporate application marketplace.

Android devices, on the other hand, have access to a marketplace that is far more open. There is poor developer verification and little verification of applications, resulting in numerous incidences of malware in the marketplace. Android also permits the installation of programmes from other sources, such as downloads or transfer from a computer.

BlackBerry devices receive applications from a marketplace, but little is known of the effectiveness of any application verification. As with Android devices, BlackBerry devices can install applications that have been obtained from other sources. There have been isolated incidents of BlackBerry malware and these have all been from applications obtained through vectors other than the marketplace.

Windows Phone devices obtain applications from a marketplace only. Microsoft vets applications before releasing them, but there are no indications of how successful this process is.

The security of data on a device can also be affected by the permission models of the various applications. From iOS 6 onwards, for example, Apple devices have some enforceable permissions, such as preventing application access to tracking information, or contacts and photos. Prior to iOS 6, all applications on an iPhone could access contacts without the user's permission.

Android and Windows Phone applications declare the data and resources that they will access on installation, enabling users to make better judgements as to the applications to allow. BlackBerry devices present a user with the requested permissions of an application and allow changes to be made to those permissions.

Solutions

It is recommended that organisations with corporate-owned devices prevent the installation of third-party applications through MDM solutions and technical restrictions. However, many smartphones and tablets will be personally owned and the owner might not agree to have application marketplaces restricted. Organisations therefore need to calculate the risks from rogue applications, which will depend on the device in question.

Installing applications from sources other than the official marketplaces should be restricted regardless of device ownership. MDM solutions might be able to support blacklisting or whitelisting of mobile applications. Where users are allowed to access marketplaces and download applications, they will require training as to the risks of such behaviour and guidelines on best practice: specifically, only to install applications from well-known companies and to recognise unnecessary permissions requests.

All users should be prevented from installing smartphone and tablet applications obtained from sources other than official marketplaces, as there are no guarantees as to the legitimacy of the application.

Mobile Working Considerations

Creating Low-Impact, High-Value Data Views

The Challenges

There are benefits to allowing less secure devices, such as consumer smartphones and tablets, to access data. Such devices allow new methods of data entry or manipulation and can enable new working styles. For example, an employee waiting to meet a client can quickly review a proposal on a small mobile device rather than having to set up a laptop. However, as consumer mobile devices are less secure than hardened corporate machines, there can be increased risks to data. These risks can be reduced through technical controls and policy (although an inherent risk will still remain).

Solutions

Organisations can create views of data that are highly useful to the relevant staff, yet minimise exposure should a device or view be compromised. To do this, organisations need to work with staff to understand working patterns and which sets of data warrant this approach. For example, it might be useful to allow a salesperson to view open proposals. These data can then be collected into a view for the employee to consume safely. Views can be delivered over third-party applications or presented by a web application available over a VPN.

Another example is the presentation of data in a form that enables management staff to make decisions without seeing the data itself. For example, a company might decide that management staff can access a graph of changes in sales figures on their iPad, but not gain access to the actual sales data. The construction of such views is likely to require the production of bespoke applications, which can bring additional risks, but it might be considered worthwhile given the flexibility it affords decision-makers.

Technical Controls

There are a variety of technical controls that can be used to mitigate the risks that arise from the use of mobile devices; however, not all apply to all types of mobile device. The table below shows the different controls and the device types to which they apply.

Technical controls and the device types they apply to

CONTROL	LAPTOPS	PORTABLE STORAGE	SMARTPHONES AND TABLETS
Passwords	✓	✓	✓
Encryption	✓	✓	✓
VPNs	✓	X	✓
DLP	✓	✓	✓
Patching	✓	X	✓
Asset Management	✓	✓	✓
Remote Track and Wipe	✓	X	✓
Exploit Mitigation	✓	X	✓
Data Segregation	✓	✓	✓
Antivirus	✓	X	X

Passwords

Introduction

Passwords are a key control, as a weak password can enable the deactivation or the bypass of many other controls. For example, encryption is often implemented by protecting the decryption key with a passphrase. If the passphrase can be guessed or brute-forced, the encryption is of little use.

However, without appropriate education as to the importance of a strong password/passphrase, users will often choose weak passphrases. This typically results from a lack of understanding of the attacks possible ("I use a name no one would think of, plus a year") or a reluctance to remember and repeatedly enter a strong password.

There are two approaches to brute-forcing a password: online and offline. Online cracking is where passwords are cracked though the device itself, by querying an interface or API. An example would be to repeatedly enter a password into a lock screen interface. Offline cracking is where the passwords, stored as hashes, are retrieved from the device and then cracked on a different, specialised machine that will not impose the limitations that might exist on the device. As such, offline cracking is orders of magnitude more efficient than online cracking. For example, if the stored Windows password hashes are extracted, a standard laptop can attempt around 10 million potential passwords per second. In typical assessments of enterprise environments, around 70% of employee passwords are found to be crackable. Another significant risk, particularly with simpler passphrases and devices where the passphrase has to be regularly entered, is someone observing the passphrase being used.

Employees need to be made aware of the risks of weak passwords and, importantly, what constitutes a weak passphrase. The length and range of character types used in the password should be emphasised, as well as its resistance to guessing and dictionary attacks. Guidelines provided by NIST[8] offer a good general resource on the subject of passwords.

Technical Controls

Employees should also be educated as to the importance of adopting different passwords for different systems, so that a compromise of one would not result in a compromise of all. Also important to understand is the use of password managers to store passwords, particularly for public websites, so that should a website be breached and passwords publicly released, it will not result in passwords used for other systems being exposed. Technical controls can be used to enforce password complexity and length requirements and this is highly recommended. However, without training, employees might still choose a weak password such as 'Password1!' which will probably pass most technical controls, yet still be highly guessable.

Two-factor authentication is a mechanism to improve authentication processes. Employees use a second identification mechanism in addition to the passphrase to prove their identity. This can be token-based, or biometric – such as a fingerprint or retina scan. Organisations can choose to use two-factor authentication mechanisms to improve systems security, or use it in combination with reduced password length and complexity to allow for better usability while preserving a similar degree of security. Where possible to implement, two-factor authentication is recommended.

Laptops

Laptop passwords can be long and complex without adversely affecting users, as laptops typically have full keyboards, allowing easy entry of the passphrase. Where full disk encryption has been configured to use a password (see later section on 'Encryption') it is recommended that the password is at least 16 characters and complex, as it is not entered regularly, yet is a key defence against data loss following device theft[9]. The primary login password for the operating system should be similarly long – and different from that chosen for the full disk encryption.

It is possible to use two-factor authentication systems for laptops, including fingerprint scanners, smart cards, USB tokens and code-generating tokens. If a company intends to implement such a system, it is recommended that the various options are thoroughly researched as there are residual security risks with each. As such, it is not recommended that any of the above identifiers are used in place of a password but are instead used to complement the password. A particular issue to be addressed by training is that smart cards or other physical, token-based authentication should not be stored near the laptop itself. This significantly increases the risk that an attacker may obtain access to data, particularly if no password, or a weak password, is set.

Portable Storage

Encrypted USB drives can be considered as similar to laptops when it comes to password requirements, as they will be accessed through computers with full operating systems. As there is a higher risk of losing a USB drive than a laptop, however, it is recommended that a longer passphrase (greater than 20 characters) is required. The vast majority of USB drives will be software encrypted and hence, as the key will be stored on the device itself, are potential targets for offline cracking.

Smartphones and Tablets

It can be particularly challenging to ensure that users select secure passwords for smartphones and tablets. These mobile devices are used frequently, throughout the day, with users regularly checking information in brief spurts rather than engaging in extended work periods as they would with a laptop. Smartphones and tablets also regularly lack hardware keyboards, and instead require passphrases to be entered via an on-screen keyboard. It is therefore harder to encourage users to choose a suitably secure password and a greater level of user education is needed to ensure they understand the risks.

Without such education, a user is likely to choose a password that is quick and easy to enter, multiple times a day, using a non-optimal input mechanism. As with other devices, suitable passwords will be alphanumeric and of a reasonable length – as illustrated in the accompanying table, which shows the typical times taken to crack passwords on Apple devices. Furthermore, usage of PINs (numeric-only passwords) can expose these devices to extra risk, beyond the mere lack of complexity, as they commonly display a keyboard that differs from the main system keyboard for such PINs. This makes it easier to distinguish grease marks resulting from password entry. Users should also be made aware of such threats as the presence of untrusted observers when entering their password.

Some smartphone and tablet manufacturers include a non-password-based unlock mechanism such as a picture password for Windows 8 and Android's grid unlock feature. These are not recommended as acceptable authentication mechanisms, as they generally offer less resistance to cracking than an alphanumeric password with mixed case and special characters. Another important weakness is that unlock patterns are far easier to observe when being entered, or to derive from on-screen smudges, than a full password.

Currently, very few smartphones and tablets support two-factor authentication mechanisms. As such, adopting such a feature would require the purchase of very specific devices, which is unlikely to be practical.

Key Points:

- Crucial control
- Length and complexity requirements should be enforced
- Education crucial in preventing weak passwords

Time required to crack iOS passwords

CHARACTER SET	CHARACTER SET SIZE	PASSCODE LENGTH	APPROX. TIME TO EXHAUST
0 – 9	10	4	15 mins
		6	22 hours
		8	90 days
A – Z, a – z, 0 – 9	62	6	144 years
		7	9,000 years
		8	500,000 years
		10	2,100,000,000 years
A – Z, a – z, 0 – 9, symbols	~100	6	2,500 years
		7	250,000 years
		8	25,000,000 years
		10	25,000,000,000 years

Technical Controls

Encryption

Introduction

Encryption of data at rest protects long-term storage devices (such as hard disks) by using a 'key', without which it is next to impossible to extract usable data. This prevents an attacker from bypassing software-imposed controls and simply reading the data directly from the storage medium. Publicly reported losses of records from mobile devices almost entirely involve unencrypted devices. Encryption is therefore a crucial control and should not be overlooked.

Although encryption of storage media prevents an attacker from simply reading the data, if the device is turned on and logged in (in the case of a laptop) or unlocked (in the case of a smart device), the encryption offers little or no protection, as the operating system has access to the unencrypted files. The protection offered by encryption of storage media is therefore dependent on the state of the device obtained by the attacker.

An important factor with storage media encryption is that the key used to encrypt/decrypt data is typically long and complex and inappropriate to remember. To make encryption schemes more user-friendly, the actual key is protected, typically with a regular passphrase. If users are allowed to choose weak passphrases, it becomes much likelier that an attacker will be able to gain access to unencrypted data. There are other methods of storing and protecting the key that do not require passphrases, such as TPMs (Trusted Platform Modules) but, without a passphrase in combination with key storage on a TPM, an attacker would be able to boot the system, thereby exposing additional attack surface.

Commonly perceived downsides of storage media encryption include a negative impact on the user experience when a long passphrase is required each time the user boots; and that data recovery in the event of hardware failure can be impeded. However, it is possible to configure storage encryption to be largely transparent to users, and legitimate data recovery is also possible if the scheme is configured correctly. The importance of encrypting storage media on mobile devices cannot be overstated. Any concerns should be investigated and resolved, rather than allowing them to prevent the adoption of this important technical control.

A final question for organisations to ask themselves is the level of trust they place in the vendor of the encryption product, as should the key material (material used to generate the key) be known or become compromised, then the key itself might be derivable.

Laptops

Data stored unencrypted on a laptop hard drive can be at significant risk, as laptops are inherently portable and their hard drives are typically removable and easy to analyse on another computer. Encryption is therefore highly important.

Stored data is encrypted on a laptop in one of two ways: in either the hardware or software.

Hardware-encrypted disks manage the encryption and decryption of files on the disk itself and, as such, are typically faster than software implementations. However, such disks can be both expensive to purchase and difficult to source. Software-based encryption uses normal disks plus software that manages the encryption and decryption of the data. There are many companies offering software-based encryption solutions that cater for various needs and most enterprise-grade operating systems come with a solution built in. An added benefit of software-based encryption is that enterprise management is often available; however, access speed can be reduced compared with hardware disk encryption.

If a password is used to protect data, users are requested to enter it when the device boots. It is recommended that the passphrase/password is more than 16 characters long and non-predictable (see earlier section on 'Passwords'). Alternatively, laptops can be purchased with a Trusted Platform Module (TPM) which stores the keys securely. The disks do not then require a password on boot and will not be readable outside the laptop in which they belong. If a TPM is used, the device needs to have a secured OS and BIOS as an attacker could simply boot the laptop using a USB key and access the data that way. Finally, some solutions support token-based authentication such as smart cards or USB dongles. If these are chosen, staff need to be aware that they must not keep the token in the same bag/location as the laptop. It is recommended that multiple factors are required to unlock hard disk encryption. For example, usage of a TPM, supported by a strong password, is a highly desirable approach.

Encryption protects data at rest: in other words, data on the hard disk. Data in RAM is not protected and while the computer is running, there will be unencrypted data in the memory. Employees should be warned about the risks of sleep mode, as a laptop appears to be off but still has data in RAM and can wake to a state where the attacker will be able to interact with the operating system. Organisations might wish to consider disabling sleep mode through group policy, in favour of hibernation (state S4) where RAM is saved to disk and the computer powered off[10].

Portable Storage

USB storage and memory cards are both easy to lose and easy to analyse if found. What's more, an individual who finds a portable storage drive in the street is quite likely to plug it into their computer and examine it. There have been multiple high-profile data losses as a result of lost portable storage. Properly configured encryption is therefore crucial to prevent compromise of assets.

Some vendors offer 'secure' portable storage, although it is recommended that these devices are thoroughly researched prior to purchase as flaws in such products have often been reported[11]. To ensure that appropriate devices are chosen, it is advisable to seek verification of vendor claims by independent studies. Alternatively, restrict purchasing to devices that have been approved by schemes such as CAPS or FIPS, but be aware that a device could well use an encryption scheme approved by FIPS while the device itself might not be approved. In such cases, there is a risk that an attacker could bypass the encryption. Commonly, third-party software encryption products are used to protect removable storage, and packages that support full disk encryption will often also provide removable storage encryption.

Smartphones and Tablets

Although encryption is important for smartphones and tablets, there are some key differences that mean they need to be treated differently from laptops and removable storage. First, smartphones and tablets are commonly on, but in a locked state, and secondly, long-term storage is not normally removable as it is soldered onto the mainboard. These two factors mean it is unlikely that an attacker will attempt to access the storage media directly and will instead attempt to attack the device. Notable exceptions to this are smartphones and tablets that support removable storage such as SD cards, as these are trivial to remove and analyse and should be considered as portable storage.

Also, smartphones and tablets are typically locked down by the vendor and so third-party encryption software is less common than on other platforms, and in some cases simply not available. Instead, encryption of storage media is generally a feature of the mobile operating system itself and, as with all features, changes over versions. The effectiveness, or even the existence, of encryption is therefore entirely dependent on the device and OS version.

All major smartphones and tablet platforms (iOS, Android, BlackBerry, Windows Phone) offer storage encryption. However, in most cases encryption was only introduced in later versions and hence many devices are in circulation that do not support encryption.

There are also significant differences in how the various platforms implement encryption, and hence in the resulting implications for the security of data. For example, although iOS implements full storage encryption, the mechanism used means that if a bootrom exploit is available, an attacker without the password can obtain significant amounts of information, such as VPN/Wi-Fi credentials and contacts[12].

However, the mechanism used in iOS means that a device has to be unlocked before much of the critical information becomes available. Android (when encrypted) is not vulnerable to the bootrom issue, but all files are available at all times once the device has booted. Implementing encryption on smartphones and tablets therefore requires significant research into the chosen platform(s) to identify device-specific risks, and make informed decisions as to which devices to support. In a 'personal device' scenario such as BYOD, there might also be challenges in persuading users to accept encryption and use suitable passphrases.

Key Points:

- Crucial control
- Often dependent on good passphrase
- Many solutions exist
- Important differences between different classes of device

Availability of storage encryption on smartphone platforms

iOS	ANDROID	BLACKBERRY	WINDOWS PHONE
Later than 4.0	Later than 3.0	Yes	Later than 8

Technical Controls

VPNs

Introduction

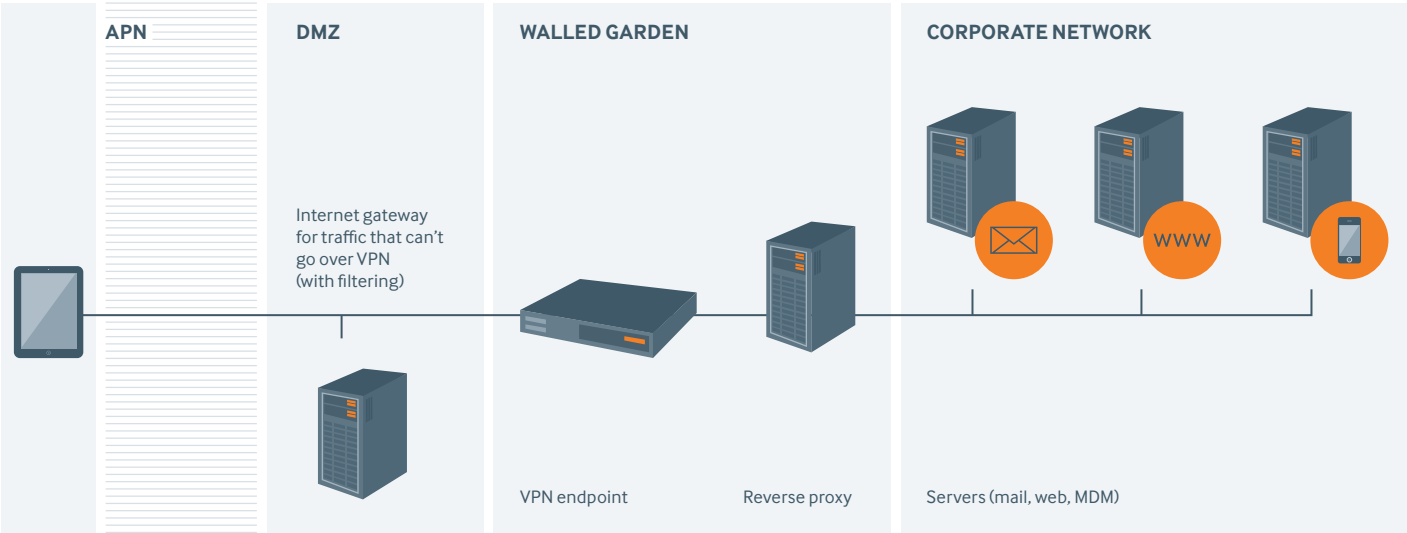
Virtual private networks (VPNs) are a technology allowing computers to establish trusted connections over untrusted communication channels. They are frequently used by mobile workers who are unable to guarantee a secure connection, yet might need to access the organisation's resources. If properly configured, a VPN prevents attackers intercepting and modifying traffic, while allowing approved access to internal resources. However, a VPN does not offer security if the attacker has a presence on the mobile device or the network to which it is connected. Poorly configured and secured VPNs can pose a risk, as they could expose sensitive assets and potentially give an attacker access to the organisation's internal network. There is also a distinction to be made between a true, secure, VPN and similar approaches that do not offer the same security. Mobile network APNs, for example, are recommended as part of a defence-in-depth approach to security, but should be used in combination with a VPN, rather than instead of it.

A range of technologies can be used to provide VPNs. A popular scheme is PPTP with authentication provided by MS-CHAPv2. Due to severe flaws recently reported in MS-CHAPv2, it is recommended that such VPNs are not used[13]. Another issue to be aware of is that of 'pre-tunnel-communications'. This is when a device is connected to a network and background services begin communicating before the VPN can be established. Depending on the nature of those communications, the result could be information leakage or an exposed attack surface. Truly hostile networks should therefore be avoided entirely and untrusted networks avoided where possible (see earlier section on 'Working from Untrusted Networks'). Ideally, always-on VPNs should be used, which ensure that all traffic is routed through a VPN. This is possible on many devices but not all.

VPN access is often controlled by certificates, passphrases or a combination of both. Wherever a passphrase is used it should be strong, and different from the main device login password, as it must be assumed that an attacker who has obtained a device could well be in a position to crack the stored login password. If a passphrase is not required, it could lead to a situation where an attacker with access to a VPN-enabled machine might be able to obtain access to the organisation's intranet. Conversely, if connecting to a VPN requires too much effort, a user might avoid doing so when not accessing what is perceived to be 'business critical' information. However, this could still result in an attacker having access to information that allows them to better understand their target.

It is also necessary to ensure that the design of the internal network minimises the risk to the internal network from the VPN. MWR has assessed networks where VPN access merely required a password and, once accepted, allowed total access to the organisation's internal network. When designing VPN infrastructure, it is highly advisable to use segregation so that VPN users only have access to the systems they require to conduct their business. A recommended approach is the so-called 'walled garden', as shown in the illustration, where a VPN connects a device to a purpose-designed network that is robustly segregated from the organisation's full network, only allowing certain connections to the required resources, preferably using technologies such as reverse proxies. Logging and alerting are also of paramount importance in ensuring that a VPN is not abused.

A model for secure mobile access to corporate resources



Laptops

Modern laptops come with native support for some VPN technologies. However, it is important to choose a VPN with the properties and features that fit your requirements and the technologies built into the operating system might not be appropriate. There is a healthy market in third-party VPN solutions and a list of those tested with Windows 7 can readily be found online[14]. An increasingly popular choice is DirectAccess, which is available in Windows 7 and 8 and is an 'always on' VPN-like solution. There are some important factors to bear in mind with DirectAccess, however: namely that earlier versions require IPv6 functionality in the organisation's network and that the solution only supports Windows 7 Enterprise and Ultimate editions that are joined to the domain. As such, DirectAccess is unlikely to be practical in a BYOD scenario and hence more traditional VPNs should be used for these cases, where they are currently permitted.

Smartphones and Tablets

Smartphones and tablets increasingly support VPN technologies. Android and Apple devices typically support a range of solutions out of the box, and include increasing support for two-factor authentication such as RSA one-time password generators. Third-party applications also exist in the respective marketplaces to add to the supported VPN technologies.

The 'pre-tunnel-communications' problem can be more significant on smartphones and tablets, however, as they often have services running in the background, such as social networking applications that will attempt to retrieve updates once a network connection is established. There is also a risk that a user might not enable the VPN for browsing a social networking site and only use it for work purposes. This could be problematic as, for example, contacts in a social network could very well be work contacts and such browsing could help an attacker learn about the structure of an organisation.

Android implemented a native always-on VPN option in Android 4.2 (Jelly Bean). Apple iOS does not do so explicitly, but from iOS version 6 onwards it is possible to set a master HTTP proxy. If this were set to a service only available over the VPN, and the VPN configured to connect on demand, a VPN would be established for all HTTP connections. It should be noted that this can be disabled or bypassed by the user and so users will require training as to the risks of doing so. BlackBerry devices can be configured to use a VPN and support always-on VPNs; however, Windows Phone devices do not have VPN capabilities.

A significant issue with smartphones and tablets is that they are more likely to be personally owned. In these circumstances, it may well be difficult to convince users to allow all their traffic to go through the corporate network. Policy should therefore take this into account and might require user education as to the risks of communicating at all on untrusted networks. One option might be the use of on-demand VPNs to cover all applications and communications requiring corporate access, while allowing the majority of network traffic to go through the public internet.

Key Points:

- Protects communications
- Allows controlled access to organisation's resources
- If configured poorly, can introduce risk to organisation's systems

Technical Controls

DLP

Introduction

There have been a number of high-profile incidents over the past few years where sensitive government and private corporate data has been leaked due to a lack of security controls on mobile devices.

Data loss prevention (DLP)[15] is a control designed to identify and prevent critical and sensitive data from 'leaving' or being 'leaked from' private confines. For a DLP programme to be effective, a number of processes, procedures, security and privacy controls need to be in place. One of the first processes is to determine the solution best suited to a particular scenario.

There are three main classes of data loss prevention solutions, depending on whether the DLP focuses on 'data at rest', 'data at the endpoint' or 'data in motion'.

'Data at rest' refers to data that resides in storage on file servers, workstations and databases. There are software solutions available that can discover and identify where confidential and sensitive data is stored on these systems.

'Data at the endpoint' refers to data that resides on laptops, mobile devices and external storage devices such as USB hard drives and DVDs. Typically, a software agent will be deployed to each device to monitor specific actions – such as copying, editing documents or sending emails with specific words or file types that might contain data of a sensitive nature.

'Data in motion' refers to data that traverses the network, both internally and externally, to determine any sensitive data being distributed to incorrect personnel/ departments or outside private confines.

While there are software solutions that aid DLP, they are likely to be more effective in limiting data leakage in some areas than others; and it is generally very difficult to control how data is handled once it leaves the confines of an organisation. If it is possible for data to be copied to a USB key or hard drive, emailed to an external account or uploaded to the cloud, then, inevitably, all control will be lost.

An effective DLP solution for mobile devices would therefore need to provide the following:

- Confidentiality of all corporate data while in storage
- Scanning and monitoring to check for clear-text storage of confidential data
- Monitoring for the distribution of confidential data internally and to third parties
- Suitable encryption of all corporate data sent and received on the device while in transit
- Monitoring for malicious applications or software that could leak confidential data

Laptops

There are many ways that data can leak from a laptop computer and the most effective DLP solution is a combination of technical security controls and user awareness.

Technical controls include a suitable level of encryption to protect data confidentiality while in storage (as specified in the earlier 'Encryption' section). Malware and antivirus software should be deployed to check for malicious software that could infect the system and disclose confidential data to external parties. A number of 'endpoint' security solutions in the form of a 'software agent' can be installed on the device to monitor inbound and outbound content to ensure that data is not unintentionally sent to unauthorised parties, or received from malicious parties. In addition, these solutions will monitor actions such as the copying of particular file types or files containing certain words to removable media, or sending them via email, for example.

Policies should also enforce the use of strong passwords at both encryption and operating system level, and ensure that users are aware of other risks that can lead to data leakage – such as leaving their laptops unlocked, or allowing confidential data to be visible in public areas.

Portable Storage

Portable storage devices are a prime candidate for data leakage or loss. The only real method of prevention is to ensure that all drives are using strong, full disk encryption approved by such schemes as CAPS or FIPS. Users should be made aware of the implications if confidential data is copied to these devices and misplaced. Policies should clearly state that confidential data is not to be copied to any removable media unless suitably encrypted with a strong passphrase. Users should also be made aware that even if the data on the portable storage device is encrypted, when copied onto or opened in another system, that system will contain the content of the files.

Some endpoint DLP software supports the restriction of USB drives on corporate laptops and workstations. This can be configured to prevent any USB drive from being connected, or it can allow a whitelisting approach where only corporate-owned devices can be connected.

Smartphones and Tablets

Advances in technology have meant that smartphones and tablets have almost the same capability as a laptop or notebook PC, but with greater accessibility and mobility. Additionally, with the popularity of the BYOD (bring your own device) schemes being implemented, the security of these devices are a high priority. DLP requirements have therefore changed and an effective solution needs to meet all three classifications: data at rest, data at the endpoint, and data in motion.

A number of solutions have been designed and developed specifically for smartphones and tablets. These include the use of a 'containerisation' approach that can completely separate corporate data from personal data (see later section on 'Data Segregation'). For example, all data associated with the corporate sandbox on the device, sent via email or downloaded via a secure browser, should only be accessible within the corporate sandbox and not by any other application on the device.

Some of these solutions are also said to provide encryption of all data transmitted between the corporate network and device, plus full encryption of corporate data while in storage on the device, as well as protection against mobile malware and agents – enabling secure email access.

Currently, however, no single solution appears to provide all the required protection and a number of obstacles might well be encountered when deploying effective DLP to smartphone or tablet devices. The mobile operating system often restricts what applications are allowed to do, and this can prevent the development of effective DLP endpoint agents. Therefore, solutions that offer DLP-like functionality often rely on the features provided by the mobile operating system itself.

A further risk for personally owned devices is the use of 'cloud' services. For example, Apple devices back up all emails and contacts to the Apple iCloud by default. If the device has been provisioned with corporate email access, this would result in corporate emails being uploaded to the Apple cloud – over which the organisation has no control. It is recommended that either all vendor clouds and back-up solutions are prevented by technical controls, or that emails and other data are accessed through trusted third-party applications, rather than the native clients.

USB access to devices can also be restricted by technical measures. BlackBerry and Apple devices from iOS6 onwards (in supervised mode) can prevent associations to arbitrary computers that could potentially be both an attack surface and a possible route for data extraction. Where possible and appropriate, this restriction is recommended.

Key Points:

- DLP solutions depend on where the data is stored or distributed
- No single solution is likely to address all key risks
- User training is as important as technical controls

Technical Controls

Patching

Introduction

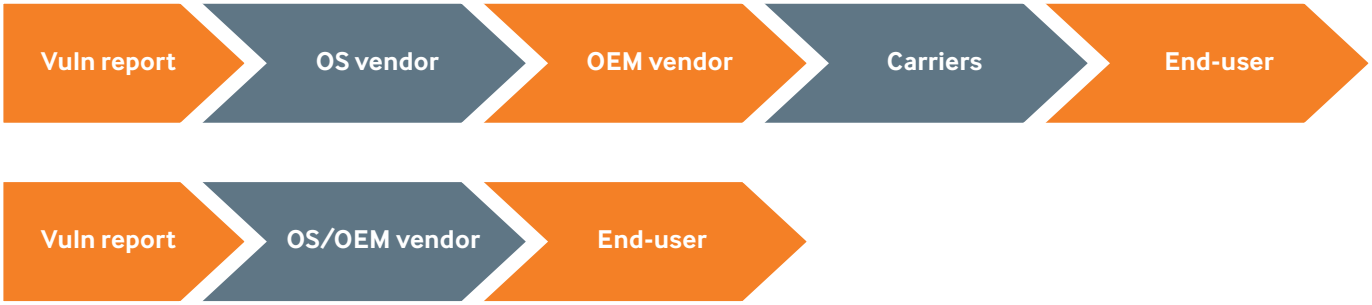
Patching is the process by which software flaws are fixed and features improved. Attackers and security professionals alike assess software for the presence of vulnerabilities. As software vendors become aware of vulnerabilities, they issue patches to correct the issues. However, the patches themselves are often analysed by hackers to identify the issues they address. This means that shortly after a patch has been released, exploits appear in the wild that target unpatched machines. It is therefore important to have a patching mechanism or policy that ensures that devices are updated soon after patches are made available. Patches, however, do not protect against unreported flaws: for protection against such threats, see the later section on 'Exploit Mitigation'.

Laptops

The attack surface for computers is shifting, with fewer vulnerabilities nowadays reported in operating system software and more vulnerabilities reported in third-party software. It's therefore important to ensure that patching mechanisms address the entire attack surface of the device. Operating system updates are typically handled by the operating system itself and it is recommended that automatic updates are enabled. If there are concerns that an update might cause critical software to stop working, then a corporate update server can be configured – but steps need to be taken to ensure that laptops used offsite are still able to update. MWR has encountered laptops that were configured to use a corporate update server, yet were used in the field and were therefore unable to update, leading to critical and exploitable vulnerabilities.

Third-party software updating can be hard to manage. On some operating systems it is possible to manage the updating centrally and, where possible, this is recommended. Endpoint protection systems can also provide details on currently installed versions, allowing administrators to track patch levels. This, too, is recommended. At the very least, auto-updating should be enabled where possible and users instructed as to its importance. Where users do not have administrative access to their laptops, policies should ensure that updates are still applied: MWR often encounters laptops that have outdated third-party software simply because the updating requires an administrator to log in. In BYOD scenarios, users should be educated as to the importance of updating, and current software versions should be checked by IT staff on a regular basis – or after critical updates. Key software to update includes Adobe Flash, Java and third-party browsers, as these are regularly targeted and a common vector by which attackers gain a foothold on a system.

Patching models for iOS and Android



Smartphones and Tablets

As with laptops, smartphones and tablets require patching as vulnerabilities are discovered. However, since apps are restricted in terms of what they can do, the significant attack surface is the operating system itself. As such, many attackers, security professionals and jailbreakers attempt to find security issues in mobile OSs. As an example, Apple's iOS 6 upgrade patched 197 security issues[16].

Different mobile platforms have different approaches to patching. These differences need to be considered when developing a mobile devices policy. Typically, Apple devices are regularly updated by users as security patches are released with feature updates, giving users motivation to patch. A flaw, however, is that some older devices are no longer supported and hence older iPhones and iPads will not be updated. It is recommended that devices not capable of running the latest version of iOS are not permitted to access corporate resources.

Android has a much-criticised patching model. Patches released for Android devices are typically specific to the model or sometimes even the model on a particular network operator. If a vulnerability is discovered in the core Android OS, it can mean waiting for both the device manufacturer and the network operator to release a patch – and in many cases this doesn't happen. As such, there are a significant number of Android devices with severely outdated versions of Android[17]. It is recommended that such devices are not allowed to access corporate resources. When significant issues are found in Android in the future, organisations should consider de-provisioning those devices that cannot be updated.

BlackBerry devices can be patched over the air or from a computer. However, few updates are released by BlackBerry and devices are often not updated by users. Windows Phone devices can be patched over the air, but patches are specific to the device and so not all devices receive updates at the same time. However, largely owing to the smaller market share, far fewer security issues are reported in BlackBerry and Windows Phone devices.

Key Points:

- Update operating system and third-party software
- Ensure hardening / policy doesn't prevent updating
- Deprovision devices not supported by updates

Technical Controls

Asset Management

Introduction

Asset management is the act of cataloguing and controlling devices (assets) that access corporate resources. Asset management is an important control in deciding policy and monitoring its implementation, as well as allowing an effective response to breaches or security issues. For example, if a serious issue were found in a particular mobile operating system, effective asset management would allow IT staff to quickly identify which employees' devices could be vulnerable and then restrict or remove access to corporate resources until a patch has been implemented. In the case of a lost device, effective asset management will allow details such as serial numbers to be quickly identified and passed to law enforcement, as well as providing security staff with information as to which resources the lost device has access to.

At its most basic level, asset management can take the form of a simple list of assets. This is favoured by many small organisations as they typically have few devices to manage and a list is therefore easily maintained. However, effective management across an enterprise can require dedicated software. Modern software typically includes other features to allow more active management of devices. This can include provisioning access to corporate resources, ensuring and monitoring compliance with security policy, reporting and metrics, and direct incident response functions such as remote wipe.

Laptops

Asset management is often included in endpoint security solutions, although ensuring compliance with security policy is typically achieved through Windows Group Policy – and then built upon by third-party software. As such, ensuring compliance can be more difficult on personally owned laptops where the employee's normal OS is used for accessing resources, as opposed to a virtualised desktop or live-booted desktop. This is because employees might not consent to having their personal machines adhere to the chosen group policy. Another significant issue is that an employee is expected to be an administrator on their personal laptop and could simply bypass group policy settings that they find restrictive. For this and other reasons, it is recommended that personal laptops are not used for corporate work unless combined with a live-booted desktop (see later section on 'Data Segregation').

Portable Storage

If an organisation has a policy restricting the use of non-corporate-owned USB drives, these drives should be listed and owners and usage tracked. However, to be effective, the policy needs to be combined with technical measures such as DLP software to restrict the USB drives that can be connected to a machine.

Smartphones and Tablets

Mobile device management (MDM) software is available from many competing vendors, each offering a range of features in addition to simple asset lists[18]. However, MDM software rarely adds controls to a smartphone or tablet operating system but simply provides convenient access to built-in controls on the device itself. The level of control that an MDM solution can offer is therefore dependent on the device, and occasionally the version and even the manufacturer of the device. For example, certain Samsung-manufactured Android devices have additional security controls implemented that MDM software can use[19]. Staff should be aware of these differences and ensure that policies take into account the differing levels of management that the organisation has over the various devices.

If personal smartphones and tablets are used for business purposes, it is recommended that they are managed using MDM software as this can ensure that policies are adhered to. To gain user acceptance, corporate policies might need to balance a user's desire for access and the organisation's desire for security. Research has indicated that users will attempt to bypass, or otherwise render ineffective, controls that they feel are overly restrictive[20]. Users should therefore be educated as to the reason for the restrictions and the implications of bypassing them. MDM software can often indicate whether a device has been jailbroken. Jailbreaking deactivates or bypasses many crucial security controls and it is therefore recommended that this is tracked and any jailbroken devices deprovisioned and prevented from accessing corporate resources (see earlier section on 'Jailbreaking').

Key Points:

- Important for defining policy and incident response
- Catalogue all devices used to access corporate data
- Different devices allow different levels of management

Remote Track and Wipe

Introduction

Remote track and wipe aims to mitigate the risk of device theft or loss. It works by having the device maintain or regularly establish a connection over the internet to check for updates. Should a device be stolen or lost, administrators can instruct the device to reveal its location or to wipe itself, thereby allowing recovery or preventing the attacker from gaining access to sensitive data. However, a significant issue with remote track and wipe is that it requires an internet connection.

The track and wipe function can be highly effective when it works. There are numerous cases of lost phones and laptops being recovered thanks to such a control, and police will generally respond quickly to lost phones with tracking enabled, as there is a short window of time during which the phones can be recovered (before the tracking is disabled).

However, a significant issue arises when remote wiping a personally owned device. Many configurations will allow a corporate administrator to wipe a personal device that has been enabled for BYOD usage. However, in many cases an administrator will need to wipe the entire device, meaning that personal data will also be lost in the process. A hypothetical but entirely possible scenario is the loss of an employee's phone that contains family photos not saved on any other device. An administrator might wish to wipe the device to ensure the safety of corporate data while an employee might prefer to wait in the hope that the device is recovered. Wiping the device could potentially present the organisation with legal issues. Policy and user education is therefore of paramount importance and organisations supporting personal devices are strongly advised to design a policy that takes remote wipe into account, and to ensure users are aware of its implications. Some devices or management solutions offer 'selective wipe' that only removes the corporate information. This is certainly worth investigating as it would allow an organisation to wipe corporate data while leaving personal data untouched.

A further issue affecting all vendor-managed remote tracking is that the vendor will have access to the employee's location. While this is unlikely to be a problem for most organisations, in some instances the information might be considered sensitive.

Laptops

There are a few remote tracking solutions available for laptops, including some that have agents at the hardware or BIOS level. However, laptops often lack mobile internet connectivity and therefore require Wi-Fi or a wired network connection. Hence a laptop that is stolen in an off or locked state (and is well secured) is less likely to be connected to a network, and so remote tracking is less effective than for smartphones and tablets with cellular connections. Some laptops do have internal cellular modems, however, and might be configurable for remote track and wipe commands.

Remote wipe of a laptop is also a less effective control than in smartphones and tablets as laptops typically have much greater storage capacities and wiping the entire drive can take hours. An attacker who becomes aware that a wipe is in process is likely to power down the device and analyse it statically.

Smartphones and Tablets

Most modern smartphone and tablet platforms have remote wiping and tracking built into the operating system. Remote tracking is generally only available to the actual user, typically through the vendor's online management service. An organisation would therefore have to work with the user to obtain the location of a lost device. As this feature often requires enabling, BYOD policies should require users to enable the feature before the device is allowed to access corporate resources.

Remote wiping is usually possible through both the vendor's online portal and an exchange or MDM connection. In the former case, the user would trigger the remote wipe, while the latter would be activated by a corporate administrator. Remote wiping of the device by an administrator is again subject to the issues raised above and could well be contentious, as a phone is often used as an individual's primary camera. Selective wiping is possible on some devices but this generally requires a compatible MDM solution. One example of selective wiping would be to instruct an Apple device to remove the profile that provisions email access, as this also causes email data to be deleted. An alternative solution is to use data segregation, so that all corporate data is accessed through a single application. By removing that application, all corporate data is then also removed.

As tablets do not always have a mobile internet connection, they can present a similar problem to that of laptops. Policy should therefore recognise that it might be technically more difficult to wipe or track a tablet unless it has its own mobile connection.

Key Points:

- Recommended control
- Requires network connectivity to lost device
- Legal problems with personally owned devices

Technical Controls

Exploit Mitigation

Introduction

Exploit mitigation technologies attempt to prevent exploitation of vulnerabilities. They typically achieve this by making the execution of unauthorised code difficult or impossible, while not affecting legitimate programmes. This is a significant challenge and, given enough time and skill, an attacker can often bypass these protections. However, these defences still serve to significantly raise the bar for people trying to exploit a vulnerability and as such are recommended controls.

Typically, exploit mitigation mechanisms are built into the operating system and, as with most features, improve and evolve with each version. However, in a few cases, enhanced protections are available for a given operating system that help to thwart an attacker. Often there is a price to pay in terms of extra administration, or the disabling of certain programmes, and as such it might be difficult to get buy-in from employees using personal devices.

Laptops

Exploit mitigation technologies in Windows have improved significantly, to the point where the latest versions of Windows are considered hard targets to exploit. However, improved protections are also available with the Enhanced Mitigation Experience Toolkit (EMET), a free toolkit from Microsoft. EMET adds protections to many recent versions of Windows, making exploitation even more difficult. EMET has to be configured to be compatible with the various programmes used on a device and hence might be inappropriate on a personal device.

Where organisations provide hardened laptops to employees rather than permitting personal devices, it is certainly worth investigating software restriction policies such as AppLocker. These allow administrators to control applications and their behaviours and thus help to prevent exploitation of vulnerabilities.

Availability of exploit mitigation technologies on iOS and Android

EXPLOIT MITIGATION	iOS	ANDROID
DEP	2.0	2.3
ASLR	4.3 (ineffective) 5.0 (effective)	4.0 (ineffective) 4.1 (effective)
Code signing	2.0	Self-signed certificates allowed

Smartphones and Tablets

Recent versions of smartphone and tablet operating systems have seen significant improvements in exploit mitigation technologies. Vendors are strongly motivated to implement and develop such technologies as not only can they help to protect users, they also make jailbreaking less likely – as jailbreaks rely on exploitation of security vulnerabilities.

Exploit mitigation technologies vary by device and also by version. The latest versions of Android, Apple and Microsoft devices all have similar protections. Windows Phone 8, iOS 6 and Android 4.1 all have key defences such as Data Execution Prevention, ASLR and application sandboxing (see accompanying table). BlackBerry, despite its reputation for good security, has few exploit mitigation preventions in its mobile operating system and therefore provides a potentially easier target for attack. It is recommended that only devices that are upgraded to the latest operating systems are allowed access to corporate resources.

Key Points:

- A feature of the operating system
- Jailbreaking reduces effectiveness
- Device-dependent features

Data Segregation

Introduction

Data segregation is an approach whereby personal and corporate data are separated, allowing different controls to be applied to each. Although this is less important on corporate-owned devices used only for corporate work, it can be extremely useful in other ownership scenarios such as personally owned devices used for corporate work. There are significant benefits to maintaining effective data segregation, including the potential effect on an employee's attitude to data, as clear segregation illustrates the level of care with which the employee should handle the data. However, the primary benefit is that strict and effective controls can be applied to corporate data and not to personal data. This allows the corporate data to be protected, while reducing inconvenience to the employee – which in itself can lead to improved policy compliance.

Data segregation can be challenging in practice as few operating systems support it in any robust fashion. As such, third-party software is often required to implement segregation and there are some weaknesses in many of the approaches. Initial set-up of effective separation can therefore be both costly and time-consuming but is highly recommended if personal devices are to be allowed for work use.

Once data segregation has been implemented, it must be maintained by ensuring that corporate and personal data remain separate. Typically, this requires data loss prevention software (see earlier section on 'DLP') to track and control corporate information. Numerous high-profile breaches have resulted from corporate information being stored with personal data such as emails forwarded to personal accounts. Training is therefore critical to ensure that employees are aware of the reasons for these controls and the risks that arise if they are circumvented. It is also recommended that employees are provided with a source of advice on moving or accessing data if the restrictions prove to be affecting their work – along with an appropriate contact to inform if a security issue should arise.

Laptops

Laptop operating systems do not currently offer suitable built-in options for data segregation. This can prove to be particularly problematic when a personal laptop is used for corporate work, since a personal laptop is at significantly greater risk of compromise than a hardened corporate laptop. This is especially true in the case of well-funded or motivated attackers targeting an organisation, as a personal laptop will expose a much larger attack surface area and is more likely to be used on home networks that lack monitoring and threat prevention.

Due to the lack of appropriate segregation options, an entirely separate operating system is recommended for corporate work. This is best delivered as an encrypted bootable USB drive. Currently, Windows 8 and various Linux distributions support delivery in such a manner. In this model, the employee boots the personal device using the USB drive and so no corporate data is written to their personal hard disk unless explicitly copied by the employee. DLP software would be needed to prevent such an act. In this way, a compromise of the employee's operating system will not lead to compromise of the corporate operating system. Alternatively, a corporate build can be installed to a separate partition on the employee's hard drive. However, this requires significantly more time and effort to implement – and offers weaker protection unless effective encryption is applied to the partition.

A further option for data segregation is the use of a virtual machine for corporate work. Virtual machine software and a copy of a corporate build is provided to the employee, who can then use it within their personal operating system. However, this approach is not recommended for organisations that are likely to be targeted by motivated or well-funded attackers, as compromise of the personal operating system can still result in compromise of the corporate resources. An attacker with complete control of the host (personal) operating system can inspect and modify memory and resources at will, and hence will be able to gain access to the corporate machine.

Allowing employees to use personal devices and then granting access to corporate resources through a remote desktop has similar risks to those of virtual machines. In other words, an attacker with control over the employee's device will be able to obtain and modify data.

Portable Storage

It is not recommended that personal USB drives are allowed for corporate purposes, as they make data segregation difficult and encourage poor practices. If organisations have sensitive resources that are likely to be targeted by more advanced attackers, it is recommended that personal USB drives are prevented through technical or physical measures – and only approved corporate drives allowed. If, however, the decision is taken to allow personal USB drives, then either the entire device should be encrypted or an encrypted container provided on the drive (see earlier section on 'Encryption').

Technical Controls

Smartphones and Tablets

Increasingly, mobile operating system vendors and third-party software vendors are implementing features to better support personally owned, mixed use devices. The challenge with smartphones and tablets is different from that of laptops, as the owner of a smartphone or tablet is not likely to be running as an administrative user on their device. (This is not true in the case of jailbroken devices and, as such, these should be forbidden from accessing corporate resources.)

A current approach is 'data containerisation', where corporate data is contained within a single app that can enforce protections from other apps and from the user or attackers. This is preferable to simply allowing a phone to access corporate email or other resources, as there can be other protections of segregation provided, such as forbidding copying and pasting. However, organisations should be aware that breakages of segregation can occur. For example, Apple devices save a screenshot whenever an app is minimised or the device rotated. These are not stored in an encrypted form and so a limited breach can arise if an attacker finds such an image containing sensitive data. Also, a user is often able to take screenshots to capture data (although this can be prevented on some devices through MDM policies).

Containers can be implemented in various ways, with different consequences for security. Many commercially available products are apps for smartphone and tablet operating systems that attempt to use features of the operating system to protect data, while others use more traditional controls such as encryption. However, some devices also offer enhanced data segregation. These include Samsung for Enterprise (SAFE) devices when managed by MDM solutions and the BlackBerry PlayBook. Containerisation that is implemented and enforced by the operating system is thought to be more robust than applications that manage the segregation on an operating system that isn't 'segregation-aware'.

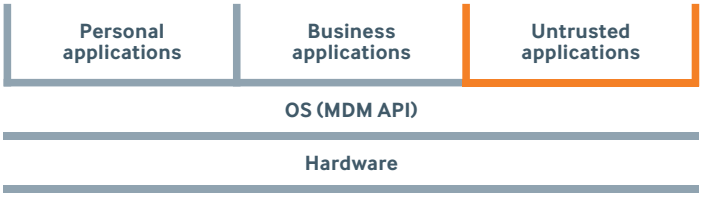
Virtualisation of mobile operating systems has been suggested as a solution. In other words, two separate operating systems could co-exist on a device, one for personal and one for corporate use. However, no such solution is commonly available and its implementation could be challenging. Hence mobile virtualisation is not expected to be a viable control in the near future.

Key Points:

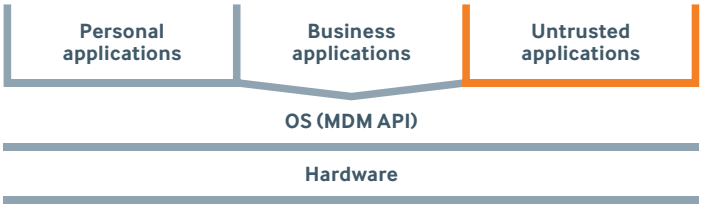
- Recommended control
- Can relieve legal/security issues with personal devices
- Can be difficult to implement well
- Segregation possibilities depend on the specific device

Models for data segregation from least secure to most secure

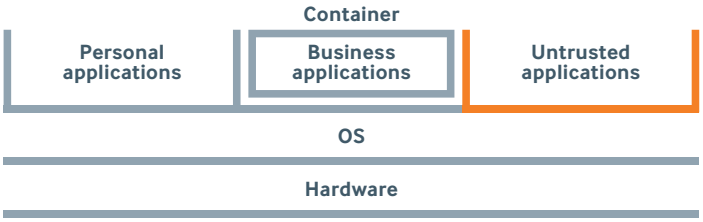
Untrusted applications installed on device alongside trusted ones



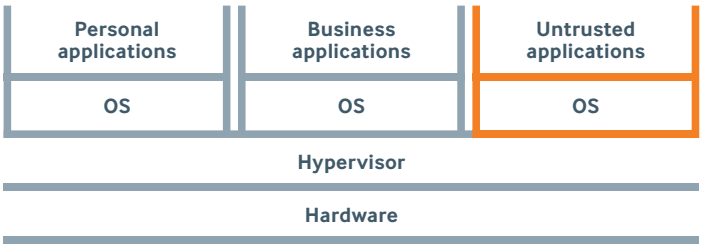
Business applications installed alongside untrusted ones but OS aware and can enforce separation



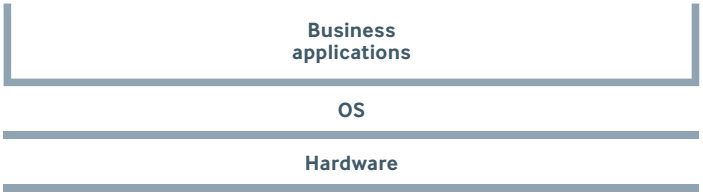
Business applications and data protected within a software container



Separate virtual OS for different types of data and applications



Only business/trusted applications allowed on device



Technical Controls

Antivirus

Introduction

Antivirus (AV) solutions aim to detect and remove malware from a system. As malware is detected and analysed by vendors, signatures are created to identify it. Antivirus solutions are helpful controls against common malware types, but the flaw is that a sample of malware has to be detected and analysed before it can be identified by an AV product. As such, AV does not offer good protection against targeted or more advanced threats but does offer good protection against mass spam or malware outbreaks, and is a useful control for laptops (see below). Portable storage can of course be a vector for malware but does not run AV products itself and so is not included in this section.

Laptops

A wide variety of AV products exist, with various distinguishing features and at a range of price points. Whichever product is chosen, it is recommended that, regardless of ownership, all laptops used for corporate work have AV installed as the majority of known malware targets Windows systems. Furthermore, since AV is dependent on updates to work effectively, policies should ensure that the AV is able to update. Occasionally, system-hardening attempts (if not done correctly) can prevent AV updating, so this is something that should be checked.

Smartphones and Tablets

Although several vendors offer AV solutions for smartphones and tablets, the effectiveness of the solutions is generally poorly regarded. For example, on the iPhone, iPad, and Windows Phone devices, the restrictions imposed by the operating system are too severe for an AV product to function properly unless the AV engine is built into the operating system. As such, AV on these devices is typically limited to scanning specific files rather than offering background, on-access scanning of files. There are also few, if any, reports of malware on the above platforms and it is not possible to obtain applications through methods other than the official marketplaces (see earlier section on 'Software Distribution').

Android is a different matter, however, as the operating system is more permissive. Malware has been found in the wild on Android, hence an AV product could potentially provide a useful function in the same way as it does on a laptop. From Android 4.2 onwards, an antivirus feature has been built into the operating system to scan apps that have been directly downloaded rather than obtained through the marketplace. However, owing to the security risks, it is recommended that the ability to obtain apps in such a way is restricted.

Key Points:

- Useful on laptops
- Not considered necessary on smartphones and tablets
- Only protects against known viruses

What Should I Do Now?

The key first step for any organisation is to assess how mobile devices are currently being used in the business. While this will involve a review of the current deployment of mobile devices and, where necessary, a re-appraisal of the associated policies, it is arguably more important to assess the unofficial usage of mobile devices.

This will require talking to employees, potentially with the guarantee of amnesty or anonymity, to assess the extent to which employees are using mobile devices. It might be possible to support such conversations with technical records: looking at devices enrolled in ActiveSync, for example, or at browser headers on network traffic. One organisation recently discovered that 5% of its employees had provisioned their own mobile devices by using an externally facing exchange server that did not restrict device enrolment. This presented a serious issue, as sensitive corporate data was now present on devices with no effective protections. Not only did this create inherent security issues, it also introduced regulatory and compliance issues.

Once the current usage has been understood, organisations can work to support employees safely. This will necessitate the construction of balanced policies supported by robust controls and will require an understanding of the differences between different devices. It is likely to result in analogue policies ('device X can access assets A and B, while device Y can only access A unless it is on the corporate Wi-Fi') rather than digital policies ('iPhone yes, Android no').

As devices change further, with controls added or improved, policies should be able to change as well. Policies, along with the processes for approving those policies, should be designed so that they can be modified and incrementally improved. If a control is added to a device, for example, it might not demand a complete re-assessment of security policy, but instead require only a minor tweak that can be implemented in a timescale of days.

IT departments will need to work with employees as business enablers. This will require the department to be ahead of the technology curve, aware of current and upcoming technologies, and actively considering ways to support those technologies. In this way, it will be the IT department leading the changes rather than those changes being driven by users. To fully – and safely – realise the benefits of modern devices and working styles, the IT department needs to be seen as a forward-thinking enabler, rather than a preventer.

Future Trends

The many changes that have come about in mobile working are unlikely to slow or stop. We can expect changes in working styles and the devices already in use, as well as the emergence of new devices and fresh working styles that are currently unimaginable. Come 2020, will corporate desktops exist at all? Will all business be conducted on some form of mobile device and what will those devices be running? It is hard to predict.

In the immediate future, however, some trends are predictable. Mobile devices such as smartphones and tablets are likely to become ever more popular and widespread. More business functionality will be possible on mobile devices as vendors and businesses alike find new ways to deliver and manipulate data. People are likely to become increasingly connected, with single devices used to manage the majority of their work and personal lives.

The devices themselves will mature, too. While security was not a selling point for early versions of smartphones and tablets, it is increasingly becoming both a standard requirement and, potentially, a unique selling point for the vendor. Looking ahead, smartphones and tablets are likely to catch up – and possibly surpass – 'full' operating systems in the range and efficacy of technical controls.

Mobile devices are almost certain to permeate ever wider areas of business. Whereas a year ago, perhaps, a high-level executive might have had a tablet, it is likely that smartphones and tablets will be seen in increasingly diverse areas of business – including high security areas. CESG's approval of Apple iOS 6 devices for the storage of 'Restricted' data can be seen as an important turning point for mobile devices.

Mobile operating systems, meanwhile, are also likely to improve their support for mixed use devices by providing robust data segregation and data loss prevention. RIM has demonstrated that its unique selling point in the next range of BlackBerry devices will be 'BlackBerry Balance', an architecture and assorted technologies that allow personal and corporate data to exist safely on the same device. It is probable that other vendors will begin to incorporate these ideas, too. One trend that extends beyond mixed use devices is that innovations will surely emerge from third-party vendors and niche players, who will in all probability come up with novel solutions to problems before major device vendors incorporate those ideas into factory products. This could be difficult for organisations to manage, as there is likely to be a range of unaccredited vendors offering tempting solutions. Assessing the claims of those solutions might prove time-consuming and costly.

It is conceivable that the idea of a corporate office with an internal network becomes outdated and is instead replaced by home working, mobile working, satellite sites and temporary office working. Networks would have to adapt to accommodate such a shift, as a single flat network cannot offer the controls and restrictions that would become necessary. Organisations might find in the near to intermediate future that a large number of their workforce are regularly connecting via a VPN rather than directly – and so security models will need to shift to take account of that. As many organisations currently operate a flat network, this could result in increased risk – or act as a motivator for organisations to divide their network into segments, requiring more management and hardware, yet allowing for greater control.

In short, it is probable that the mobile working business revolution will continue – and that there will be increasingly diverse options available to both individuals and organisations. This will mean increased complexity in managing the associated risks; but we can also expect to see the emergence of improved controls.

Summary

Mobile devices and modern working styles are revolutionising our personal lives and our business practices. However, they are also introducing complexity to security arrangements that were previously well understood. To ensure that assets are secure while supporting new ways of working requires significant attention on the part of the organisation, yet the potential benefits are numerous and substantial.

New policies are required; policies that demand a detailed understanding of the organisation, its employees, and the devices themselves. Crucially, it is vital to realise that many technical controls are ineffective or simply not present on some devices – and hence user training and acceptance of policy is critical in the protection of an organisation's assets. The many differences between classes of device, vendors of devices and even versions of devices must be taken into account.

Looking ahead, IT departments are likely to undergo a fundamental shift in perception. Instead of being seen as a department which prevents deviation from the rules, IT needs to become a department that helps users work safely – and in the manner they desire – through both technical controls and education.

Appendices

Case Studies

The following case studies help to demonstrate some of the less obvious aspects of mobile device security.

1. Unauthorised USB Drive

An organisation was designing and building a new network stack, the technical details of which were highly sensitive. Ensuring the protection of all information surrounding the network design was of the utmost importance. However, the organisation discovered that a third-party contractor had been using an unauthorised USB mass storage device to transfer plans for the new network between various systems – and a subsequent investigation identified that the device had also been connected to unauthorised computer systems both at the individual's home and at the contractor's office. This meant that the sensitive information was outside the remit of the organisation's corporate security controls and could have been compromised by malware, or copied to the hard disks of unauthorised computer systems.

In this scenario it was not possible to provide any level of assurance that the information had not been leaked or otherwise compromised as a result of the contractor's actions. To mitigate the potential impact of the incident, the network stack had to be redesigned, including changes to the technologies, architecture and addressing scheme at significant cost and delay to the project. The organisation in question had implemented technical controls over the use of USB devices in its equipment and had strict policies on the use of these devices to handle its data, but failings by a third party still resulted in a significant impact on security.

Ultimately, the failings in this situation were twofold. First, there were no mechanisms for the contractor to handle the data in a manner that enabled the secure completion of the project; and secondly, the individuals concerned had not been sufficiently educated about the risks of using unauthorised USB mass storage devices. Both these areas were subsequently addressed by the organisation to ensure that a similar incident could not occur in the future.

2. Home Working

An organisation wished to allow its employees to use corporate, hardened laptops from their homes. However, corporate policy required laptops to be prevented from connecting to arbitrary access points. A possible solution was to configure individual laptops with the owner's home Wi-Fi credentials but this would have required significant time and effort to implement and manage, as each employee's laptop would need to be configured individually. An alternative was the use of 3G/4G dongles to provide mobile internet. However, dongles can become expensive with increased data transfer and there was no guarantee that employees would live in an area with sufficient signal to support working.

The organisation therefore opted to provide those employees cleared for home working with a wireless access point that was connected by Ethernet cable to their home access point. The employees' laptops were then configured to connect to the home working access points, significantly reducing the support effort required, although there was an extra cost incurred for hardware.

3. Fooling the User

A recent penetration test of a secured enterprise environment required testers to migrate horizontally onto different machines, in order to locate an administrative user whose access could be commandeered to gain access to restricted assets. Common techniques (such as attempting to identify common passwords or operating system vulnerabilities) were unsuccessful. Testers were, however, able to use compromised email accounts to email administrative users with payloads targeting third-party client-side software such as Adobe pdf reader. This allowed compromise of an administrative user.

In the past, it was considerably more common to gain such access by exploiting core operating system vulnerabilities. The recent trend is for an attacker who wishes to gain a foothold on a machine to find more success with a client-side exploit – such as enticing the user to visit a malicious website or to open a malicious file. By combining these attacks with trust relationships, such as posting a link on a social network, the attacker will very often succeed.

4. Poorly Configured APN

When testing a smartphone, it was found that the device was configured to use a custom corporate APN in lieu of a VPN. This APN connected the smartphone to the internal network of the organisation, allowing access to internal resources such as email servers. Testers were able to gain access to the smartphone through exploiting a known issue in the operating system.

Once that was done, testers located the APN details, which were found to be a username and password. Testers then used a mobile connection configured to the same APN to connect to the corporate network. It was found that the APN connected directly to the core internal network of the organisation. Testers were then able to gain significant access to the internal network, including acquiring a 'domain admin' level account, by following standard internal penetration testing methodology. It was also found to be possible to use the tethering function on the phone to provide the same level of access to the internal network.

5. Small Fingers: Young Threat

A corporate executive used his iPad predominantly for business purposes, but would also use it at home for general internet access and communications. As such, the device would occasionally be left, in a locked state, around the executive's house. One day, the executive discovered that his iPad had been wiped and was reset to factory defaults, preventing him from working and erasing data that had not been backed up. Initially it was believed to have been wiped remotely; however, an investigation found that the device wipe was triggered by the executive's young child repeatedly entering an incorrect passphrase.

6. Incomplete Encryption

When performing a security assessment of a laptop and the data contained on it, it was found that the device was unencrypted. The laptop was sealed with security screws to frustrate attempts to remove the hardware but tools to remove the screws were found to be readily available. The drive was removed and analysed in a separate workstation. The hashed Windows passwords were extracted and cracked, as were stored domain credentials.

Client data was found to be stored by a bespoke application that used an encrypted file. However, analysis of the application yielded the password needed to decrypt the file. Significant amounts of cached private data were also found on the laptop by using a disk analysis tool that could identify recently deleted data. Browsing history identified addresses of corporate websites and the cracked credentials allowed access, giving testers a foothold on the corporate network. Wi-Fi credentials were also discovered and by visiting a site owned by the laptop user, it was found that the credentials were current and allowed access to the internal network.

This illustrates the dangers of only encrypting data that is considered confidential – as many items of information can prove useful to an attacker. Correctly configured, full disk encryption should be used for all devices that leave a secured office.

7. TPM but No Password

A 'stolen device' test revealed that the laptop in question was fully encrypted. However, the laptop had been configured to use a TPM for key storage, and no password was required to boot the drive.

The drive was removed and analysed and, although initial attempts to extract data were unsuccessful, the operating system was poorly secured and hence testers were able to boot the device to get the Windows login screen. Another laptop was then connected to the target laptop by FireWire cable, and DMA (direct memory access) was used to gain access to the operating system, bypassing the login screen. All the stored data was then successfully extracted.

This demonstrates the importance of locking down all aspects of a laptop. Even if the FireWire port had been disabled, testers would still have been able to use the PCI-E port to insert a FireWire card and conduct the attack that way. Although unsuccessful in this case, previous tests have used a poorly secured BIOS and boot process to simply boot to a 'live CD' Linux environment – and hence gain access to the stored data. As such, where a TPM is used to hold key material, a password should also be configured.

Further Reading

Top 20 Critical Controls – CPNI
Explores many of the critical technical controls for security. Some apply more than others to mobile working but highly useful as a framework for security planning
http://mwr.to/critical-controls

MWR Mobile Working White Paper
Previous work exploring some of the risks surrounding mobile devices
Available from MWR

Apple iOS Security Overview
An excellent overview of the security features of the iOS platform
http://images.apple.com/ipad/business/docs/iOS_Security_May12.pdf

CESG Security Procedures for iOS 6
In-depth guide to recommended controls and policies for iOS 6 devices
Unclassified – available from CESG

Trail of Bits iOS 4 Security Evaluation
Study of iOS 4, although much of it is still relevant today
http://www.trailofbits.com/resources/ios4_security_evaluation_paper.pdf

Google's Android Security Overview
Explores the security features of Android
http://source.android.com/tech/security/

NIST Password Management Guide
Good advice on password choice and complexity requirements
http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

Ponemon Institute Global Study on Mobility Risks
Survey-based study investigating security attitudes around mobile devices
http://www.websense.com/content/ponemon-institute-research-report-2012.aspx

Breach Watch (UK) and Privacy Rights Clearinghouse Breach Record (US)
Two sites collating known data breaches. Useful as case studies to understand how breaches can come about
http://breachwatch.com/
http://www.privacyrights.org/data-breach

Glossary

APN	Access Point Name – Segregated data on a mobile phone network
ASLR	Address Space Layout Randomisation – Randomises memory layout to prevent exploits from using existing code to bypass protections such as DEP
BIOS	Basic Input/Output System – System that manages the initial boot of a PC
BYOD	Bring Your Own Device – Use of a personal device as a business device
CESG	Communications-Electronics Security Group – Government information assurance department
CPNI	Centre for the Protection of National Infrastructure
DEP	Data Execution Prevention – Prevents code inserted into memory by an exploit from executing
DLP	Data Loss Prevention
DMA	Direct Memory Access – Technology allowing devices (or attackers posing as devices) to read and write to system memory
GPRS /3G/4G	General Packet Radio Service / Third Generation / Fourth Generation – Mobile phone data system
iOS	Operating System that runs on iPhones and iPads
MDM	Mobile Device Management – Software to allow management of mobile assets
NIST	National Institute of Standards and Technology – US standards organisation
OS	Operating System
TPM	Trusted Platform Module – Holds cryptographic keys securely
VPN	Virtual Private Network

References

[1] **'Getting in Bed with Robin Sage' by Thomas Ryan**
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf

[2] **CESG – IA Notice 2012/07 BYOD**

[3] **Websense/Poneman Institute, Global Study on Mobility Risks (2012)**
http://www.websense.com/content/ponemon-institute-research-report-2012.aspx

[4] **Reliably Erasing Data From Flash-Based Solid State Drives – USENIX**
https://db.usenix.org/events/fast11/tech/full_papers/Wei.pdf

[5] **Websense/Poneman Institute, Global Study on Mobility Risks (2012)**
http://www.websense.com/content/ponemon-institute-research-report-2012.aspx

[6] **Websense/Poneman Institute, Global Study on Mobility Risks (2012)**
http://www.websense.com/content/ponemon-institute-research-report-2012.aspx

[7] **BlackHat 2010 Lecture Notes – Attacking phone privacy**
http://media.blackhat.com/bh-us-10/whitepapers/Nohl/BlackHat-USA-2010-Nohl-Attacking.Phone.Privacy-wp.pdf
BBC news story – Call to check on mobile network security
http://www.bbc.co.uk/news/technology-10731612

[8] **NIST Guide to Enterprise Password Management**
http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

[9] **'Of passwords and people' – Komanduri et al**
http://dx.doi.org/10.1145/1978942.1979321

[10] **System Power States (Windows)**
http://msdn.microsoft.com/en-gb/library/windows/desktop/aa373229(v=vs.85).aspx

[11] **Cryptographically Secure? SySS Cracks a USB Flash Drive**
https://www.syss.de/fileadmin/ressources/040_veroeffentlichungen/dokumente/SySS_Cracks_SanDisk_USB_Flash_Drive.pdf
Dark Reading news story – Secure USB Flaw Exposed
http://www.darkreading.com/security/news/222200174/secure-usb-flaw-exposed.html

[12] **Trail of Bits – Apple iOS 4 Security Evaluation**
http://www.trailofbits.com/resources/ios4_security_evaluation_paper.pdf

[13] **CloudCracker Blog – Divide and Conquer: Cracking MS-CHAPv2 with a 100% success rate**
https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/

[14] **Windows Server – VPN Client Compatibility with Windows 7 and Windows Server 2008 R2**
http://technet.microsoft.com/en-us/library/dd787668(WS.10).aspx

[15] **A general guide by Gartner on various vendors can be found at**
http://www.gartner.com/technology/streamReprintPDF.do?id=1-16XRYHD&ct=110810&st=sb

[16] **Apple – About the security content of iOS 6**
http://support.apple.com/kb/HT5503

[17] **The Duo Bulletin – Early Results from X-Ray: Over 50% of Android Devices are Vulnerable**
https://blog.duosecurity.com/2012/09/early-results-from-x-ray-over-50-of-android-devices-are-vulnerable/

[18] **Gartner – Magic Quadrant for Mobile Device Management Software**
http://www.sap.com/campaigns/2011_04_mobility/assets/GartnerReport_MDM_MQ_April2011.pdf

[19] **Samsung – Samsung for Enterprise**
http://www.samsung.com/us/article/samsung-for-enterprise

[20] **Websense/Poneman Institute, Global Study on Mobility Risks (2012)**
http://www.websense.com/content/ponemon-institute-research-report-2012.aspx

Contributors:

David Chismon

Tassi Carter

Martyn Ruks

Henry Hoggard

MWR InfoSecurity
Churchill Plaza, Churchill Way
Basingstoke RG21 7GP

T: +44 (0)1256 300920
F: +44 (0)1256 811227

MWR InfoSecurity (South Africa)
11 Autumn Street, Rivonia
Gauteng, 2128, South Africa

T: +27 (0)10 100 3157
F: +27 (0)10 100 3160

www.mwrinfosecurity.com
labs.mwrinfosecurity.com

Follow us on Twitter:
@mwrinfosecurity
@mwrlabs