Guidance

End User Devices Security Guidance: Enterprise considerations

Updated 06 January 2015

Contents

This section discusses some of the wider considerations an enterprise might wish to resolve when deploying end user devices. The considerations given here are common to several of the end user device platforms discussed in this documentation.

1. Private APN

A private Access Point Name (APN), which can be obtained from most mobile operators, is a service which can be used to capture all 3G/4G mobile data leaving a device, and route the traffic back to an IP endpoint at a corporate network. There are several benefits to using a private APN with mobile cellular devices:

- External corporate infrastructure (e.g. VPN gateway) is exposed only to provisioned devices, and not to the whole Internet
- Devices whose VPN allows split tunnelling, or do not offer an always-on VPN can be forced to traverse the corporate network regardless of the VPN deficiencies
- The device itself is protected from attacks from other users on the cellular network as only other devices on the APN can route traffic to that device
- Low-level malware such as rootkits which can bypass the VPN enforcement cannot bypass the APN and so will be easier to detect with corporate monitoring services

We recommend that the following platforms are deployed using a private APN in their architecture:

- Android
- Apple iOS (when not using the always-on IKEv2 VPN in iOS 8+)
- BlackBerry 10: EMM-Corporate
- Windows Phone 8 and 8.1
- Windows 8 RT

Note that the benefits of an APN are negated if devices connect to an insecure Wi-Fi network. For the above devices, connection to non-enterprise Wi-Fi networks is strongly discouraged.

To deploy a private APN:

1. Procure and provision an APN from a mobile operator; you will need a fixed IPsec connection or leased line between the carrier and your enterprise network.
2. Obtain SIM cards from the mobile operator that are exclusively provisioned to use the procured APN for their mobile data connection.
3. For devices which use an APN to enhance their security, users should be reminded not to change their SIM card.

2. Wi-Fi

In general, devices which support Wi-Fi can be used securely on any non-hostile Wi-Fi network which allows the VPN traffic to transit the network. However, there are risks associated to using Wi-Fi which must be considered and accepted before its use is permitted.

Many public hotspots redirect web traffic to a ‘captive portal’ page at first connection. User interaction (agreeing to terms and conditions, or entering a passcode) is required before an internet connection is allowed. Captive portals require devices to browse to a website outside of the VPN connection; during this time devices can be targeted for attack by the network itself, or by hostile users on that network. Configuring current devices to enable this type of connection requires a mechanism to disable or circumvent the VPN, increasing the risk of compromise of data in transit. Allowing captive portal interactions is not recommended where users are not trusted to manage their own connections appropriately.

Many devices expose a rich set of services when connected over Wi-Fi, and risk owners of deployments which use Wi-Fi should be content that the increased attack surface of these devices is within the bounds of acceptability. For example, some devices may expose synchronisation services over Wi-Fi to allow media and data to be synchronised, or devices may present a screen sharing service which allows the contents of the device’s screen to be shared with networked peripherals. The services may also be accessible locally when the VPN is connected, effectively causing a split tunnel. These attack surfaces should be considered on a device-by-device basis and only permitted where the risk is acceptable.

It should be noted that the use of Wi-Fi in deployments where a private APN is also used would negate the benefits of using the APN. The purpose of the private APN is to provide enforced routing from the carrier

network to the enterprise network for devices where the VPN does not guarantee full secure enterprise routing, or there is no VPN. In these cases, using Wi-Fi means that the enforced routing is essentially bypassed, and there is an increased reliance on the VPN to protect data-in-transit.

One final consideration for some organisations using Wi-Fi is that devices with Wi-Fi enabled may expose identifiable information from their transmissions. For example, many devices with Wi-Fi attempt to speed up initial connection times by actively searching for previously-connected networks. In searching for these networks, they transmit an identifier of that network which can be detected using publicly available tools by local attackers. This information may be used to identify members of staff (by looking for devices looking for the enterprise's Wi-Fi network), or to target those devices for attack (by spoofing the infrastructure of that network).

For further guidance around the use of Wi-Fi within Government Networks, eligible organisations connected to GSi can see IA Architectural Pattern 12 - Enterprise Wi-Fi Networks.

3. Device management

Device management products are used to remotely administer, configure and audit end user devices. They will typically comprise:

- a client component that manages the configuration of the device (which may be built into the operating system)
- a server component that issues commands to enrolled devices, and provides the administrator with an interface to control device policies

Client and server components do not necessarily have to be supplied by the same vendor. In the context of mobile platforms, these services are generally referred to as Mobile Device Management (MDM) products.

When deciding how to implement device management on end user devices, there are several key considerations.

3.1 Product features and policies supported

Ensure that the selected MDM product can enforce the security policies that are recommended in the per-product security guidance. The range of capabilities varies between different devices, so check that the MDM product can support all the platforms used.

3.2 Product security

MDM products are attractive targets for attackers; if they are able to compromise the MDM server they will be able to perform remote administration and password resets on all enrolled devices. Compounding this, MDM servers are often placed in internet-accessible locations within the corporate network, directly exposing them to external attackers. Consequently, the reliability, robustness and security practices of the MDM product are extremely important.

When choosing an MDM product, consider the product's development lifecycle and your resultant confidence in the security of the product. Is there a good track record of fixing security issues? Are security incident

management procedures in place to handle future problems? MDM products can be independently evaluated and certified to Foundation Grade, and details of such products can be found in the CPA certified products list.

3.3 On-premise or cloud deployment

Many MDM product vendors offer hosted versions of their product. Using cloud-based MDM products may decrease costs, but can increase risk. For example, other users of cloud services may be able to more easily attack or degrade the management service for your devices. If you're considering using cloud-based MDM services, read the Cloud Security Guidance for information on managing the risks associated with using public cloud services.

4. Device interfaces

Some devices allow administrators to exert control over their external interfaces - such as Bluetooth and NFC - which either prevents them from functioning, or restricts their functionality to a subset (such as restricting what the interface can be used to connect to).

Using these controls can help to reduce the overall attack surface of a device, and prevent information disclosure from the device (such as by removing the ability of the user to share information directly). The impact on the usability of the device can, however, be significant, and so administrators are urged to carefully consider the necessity of applying such controls.

It is strongly recommended that the use of these interfaces should be limited to non-sensitive information, and that information which an organisation wishes to protect should not be transmitted over these protocols. For example the use of Bluetooth headsets for non-sensitive voice communications presents a lower risk to data than the use of Bluetooth keyboards connected to the device would. In the latter case, sensitive typed data is transmitted over an unassured protocol.

5. Browsers

Many organisations deploying this guidance will want to access internal and external web services using a web browser. There are many web browsers available for most platforms, so it is important to consider the risks associated to each type of browser, and to balance that with the functionality provided by the browser which helps to perform business functions.

Modern browsers are feature-rich interfaces to enable users to be highly productive with their time online, but these features often have an impact to the security of the device and its data when used. For example:

- Browsers may cache previously-viewed web pages on disk. This places a reliance on the device to protect that information at rest. Whilst platforms with full volume encryption would normally encrypt the browser cache, platforms with file-based encryption may not, and sensitive information from web pages may be written unencrypted to disk.
- Browsers may cache credentials by offering a save password facility. Similar to the cache above, organisations should ensure that they are content with how this information is protected on the device, or disable any information caching functionality.

- Browsers may permit the concurrent browsing of Internet and intranet web pages in separate tabs. This may mean that the browser process is processing untrusted code and sensitive data at the same time, and the browser is required to enforce separation between the two domains. This presents a large and rich attack surface to the tab running untrusted code and the browser must therefore be robust to attacks from that code.
- Browsers may allow plugins to be installed. Typically these plugins run with the same permissions as the browser itself, so plugins must be fully audited and trusted before their use is permitted.
- Browser vendors regularly release updates to add features and fix security issues. As the attack surface of browsers is very large, and the chances of encountering malicious code is high, these security updates must be installed regularly and quickly following their release.

Ultimately, devices used for web browsing should use a modern, regularly-updated, and well-supported product which takes advantage of the native security features of the underlying platform. Further guidance on the use of web browsers can be found at https://gov.uk/cesg/browser-guidance.

6. Anti-virus and anti-malware protection

Security recommendation 7 notes the importance of reducing the risk from malicious software and content based attacks. On a number of platforms this is achieved by using anti-virus or anti-malware software which will usually be purchased from a third-party, but several platforms will meet this requirement through other mechanisms.

When deciding if a third-party component is necessary, consideration should be given to the issue of preventing malicious code from executing on the platform in the round. The extent to which application whitelisting is available and configured on the platform will be a significant factor, as will the ability to ensure incoming content is always routed through enterprise defences. The use of software restriction policies (or other security controls) native to the platform will also be a factor in deciding whether anti-malware or anti-virus products are necessary.

If selecting a third-party product, we recommend you:

- consider the management tools available. Specifically consider whether configuration policies can be centrally managed, and whether software and signature updates can be automatically rolled out across the device estate
- consider the audit tools available to the enterprise. Events from the product should be captured into a central location where they can be prioritised and investigated as part of an incident response plan
- consider whether the product provides heuristic and/or signature-based scanning
- consider the usability impact of the product on the platform (battery life, performance, etc)

Finally, many products now expect to be able to communicate with online services provided by the vendor in order to gain access to better analysis capabilities. You will need to consider whether these communications are able to transit via the enterprise and whether sensitive data could leak through these channels.

7. Security updates

Manufacturers will regularly release security updates and patches for their products. These updates should be applied regularly to ensure that devices are not compromised by known security issues.

For larger patches or feature releases, the security impact of any new features not yet described in this guidance should be considered before their use.

8. Revisit attacks

Device tampering and ‘revisit’ attacks is a common risk across all of the devices. Malicious functionality can be inserted into a device by an attacker who has physical access to it - such as a small form-factor hardware keylogger, or replacement of the whole device with a compromised equivalent.

These can be very hard to spot, and can be concealed within many different device types, allowing access to sensitive information. This threat can be mitigated through maintaining physical security around the device, but ultimately remains a threat from attackers who may be able to briefly physically acquire devices.

9. User guidance

It is recommended that guidance is given to all remote and mobile users on how to keep information on their devices safe and secure. This will need to be tailored to the particular device(s) being used, and matched to the local business procedures and activities. Some advice to users is common across all types of device, and this is provided here as a suggestion.

9.1 General advice

- Some of the settings on your device have been configured by your system administrator to help keep the information on it secure. Changing or circumventing these settings could put information at risk. If you are unsure about any of the settings, or what to do in particular situations, please contact your IT helpdesk.
- This device is valuable and so it is attractive to thieves. Take sensible precautions to prevent its loss or theft - but don’t put yourself at risk. Don’t leave the device unattended in an insecure location (e.g. outside of your house or office) - lock it away if possible, or keep it on your person.
- If your device is lost or stolen contact your IT helpdesk immediately to report this. You won’t be in trouble - it is better to report such a loss as quickly as you can. The faster you get in contact, the better - there is more that can be done to prevent information being accessed.
- When you are using your device be aware of who might be able to see your screen, and consider if applicable using a screen privacy protector. Devices which have ‘touch screens’ are particularly easy for bystanders to see what you are typing - even passwords.

9.2 Physical connections

- You should only use the specific device(s) that your organisation has approved; this includes all of the

peripherals that come with the device(s).

- Your device should only ever be recharged with trusted power adapters and cables.
- Don’t physically connect your official device to any computer without the approval of your IT helpdesk, this includes USB, HDMI, Firewire etc.
- Any ability to bridge connections using your device (e.g. internet connection sharing) must not be used unless specifically approved by your IT administration.

9.3 Passwords

- Whatever the reason, you must never disclose your password to anyone (including IT support staff, your manager, or a colleague), either in person, by phone, or by email or text message.
- It is acceptable to write your password down, but it must be stored securely - and never with the device itself. For example, if you write your password down, seal it into an envelope, and then store it according to its sensitivity (e.g. kept in a secure, locked, cabinet). Under no circumstances should you ever carry this copy of the password with your device.

9.4 Overseas use

- In general, it is acceptable for you to take and use your official device overseas, provided that your organisation has approved this.
- As highlighted above, you must extra vigilant and take extra care to ensure that no one overlooks you when you are accessing official information, and must take all possible precautions to prevent the theft of your device.

9.5 If things go wrong

When something goes wrong, or you suspect your device or its data may be compromised, it is important to take action promptly.

- If you have any reason to suspect that someone else knows your password then it must be changed immediately - either on the device itself or by contacting your IT helpdesk.
- If you forget the password for your device you should contact your IT helpdesk, who will confirm your identity before a password reset can take place.
- If your device stops functioning as normal, and/or experiences a significant decrease in performance or battery life, contact your IT helpdesk for further advice.
- If you are experiencing problems with the device, you must never give your device to anyone else (e.g. a commercial repairer) to try to fix; always contact your IT helpdesk.
- If you think someone may have tampered with your device (such as accessing the inside of it, or removing / replacing parts of it), stop using it immediately, turn it off, and contact your IT helpdesk for assistance.

10. Other information

10.1 Resources

The following CPNI Mobile Devices guidance documents provide more information on securing mobile devices.

http://www.cpni.gov.uk/documents/publications/non-cpni_pubs/2013-02-22-mobile_devices-executive_briefing_paper.pdf

http://www.cpni.gov.uk/documents/publications/non-cpni_pubs/2013-02-22-mobile_devices_guide_for_implementers.pdf

http://www.cpni.gov.uk/documents/publications/non-cpni_pubs/2013-02-22-mobile_devides_guide_for_managers.pdf

Legal information