

Countermeasures and Risk Mitigation Plans Introduction

Unit 6

1 OWASP Top Ten Mobile Controls

2 Security of the device

Android

iOS

BlackBerry

Windows Phone

3 *Mobile Device Management*

Functioning

Characteristics

Providers

Recommendations for each platform

4 Mitigation plans in mobile environments

5 Bring Your Own Device policies

6 Research exercises

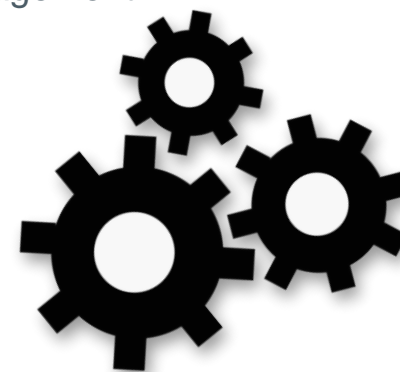


OWASP Top Ten Mobile Controls

◆◆◆ OWASP Top Ten Mobile Controls

Introduction

- The OWASP Top Ten Mobile Controls is a technical document developed by OWASP in collaboration with ENISA, the European Union Agency for Network, and Information Security.
- It specifies ten controls and design principles that should be used for the development of mobile applications:
 - C1: Identification and protection of sensitive data.
 - C2: Protection of authentication credentials.
 - C3: Data protection in transit.
 - C4: Implementation of authentication, authorisation, and session management.
 - C5: Use of secure APIs and back-end.
 - C6: Secure integration with third parties services.
 - C7: Consent to gather and handle data.
 - C8: Controls to prevent unauthorised access to paid-for services.
 - C9: Secure distribution.
 - C10: Secure use of the execution of dynamic code.



C1: Identification and Protection of Sensitive Data

Risks

- Due to the nature of mobiles, smartphones, and other mobile devices have a higher risk of loss or theft, what may lead to the loss and disclosure of sensitive data stored in the phone.

Controls

- During the design stage, the data that will be managed by the application should be classified according to sensibility (passwords, location, logs, etc.). For each category established for data, it would be necessary to design, implement, and verify specific controls.
- A security validation of the system's APIs that will handle sensitive data should be performed.
- The storage of sensitive data should be performed (whenever it is possible) in the back-end of the application.

C1: Identification and Protection of Sensitive Data

Controls

- For sensitive data that should be stored in the device, use the system's APIs for the protection/encryption of data (based on the lock code).
- The use of caches that store sensitive data should be avoided (including password) unless they are properly protected.
- Implement measures to restrict sensitive data depending on the context (bank passwords not accessible outside the dwelling).
- Do not store histories of data that may be sensitive beyond what is strictly required by the application.
- Always avoid the use of shared storage (SD card), when possible.

C1: Identification and Protection of Sensitive Data

Controls

- Carry out an active wipe of all the sensitive data that is not required for the execution of the application anymore.
- Consider the different stages that each sensitive data may go through and implement the necessary controls in each of them: collection, storage, caching, backup, and removal.
- Always use temporary unique identifiers that cannot be shared with any application of the device (avoid the use of serial numbers and other unique identifiers of the device).
- Include a specific remote wipe system for application data that do not depend on the one provided by the operative system.

C2: Protection of Authentication Credentials

Risks

- The theft of access credentials to a service would allow attackers to access such service's data; but, in addition, it may also provide information or access to other services by using the same user (use of the same credentials for various services).

Controls

- Substitute the storage of credentials (password) by authentication tokens, following standards, such as OAuth, that include a time limitation to be used and may be revoked from the back-end.
- Store the authentication tokens securely.
- Use encrypted channels (SSL) to transmit any credentials that will be sent to the back-end.
- Allow the modification of credentials from the mobile application itself (after a re-verification of the current ones).

C2: Protection of Authentication Credentials

Controls

- Authentication passwords and tokens should only be included in the backups if they are properly encrypted.
- Avoid the use of alternative authentication systems, unless it has been verified that they are able to provide enough entropy (amount of available passwords).
- Avoid the use of alternative authentication systems that are vulnerable to simple attacks, such as “smudge attacks”.
- Do not store any password or secret in the application binary.
- Check that no credentials are stored in the cache or filtered in logs, above all, in case of failure of the application.

C3: Data Protection in Transit

Risks

- The use of wireless connections may allow the interception and modification of data transmitted or received by a mobile application.

Controls

- Regardless the type of interface used (Wi-Fi, telephony, etc.), always assume that the provider's network is not secure.
- SSL connections should be used by default, with an appropriate security configuration (algorithms, key sizes, etc.).
- Use certificates signed by a reliable certificate authority.
- Do not send sensitive information via SMS, etc.
- Verify the certificate chain and, in case of error in the verification, do not allow information to be sent through the channel.
- Implement certificate pinning.

C4: Authentication, Authorisation, and Session Management

Risks

- Unauthorised users may reuse authentication token or stolen credentials to access sensitive data.

Controls

- Specify minimal requirements for passwords used by users within the application configuration.
- The back-end should require the authentication token to be sent in all the requests made to access sensitive resources or data.
- Use a source of randomness for the creation of authentication tokens, and thus, not to create predictable tokens.
- Whenever possible, include various authentication factors (SMS code, biometry, etc.).
- The authentication has to be associated with the user, not with the device.

C5: Use of Secure APIs and Back-end

Risks

- The use of insecure services or back-end renders useless all the protection measures included in the mobile application.

Controls

- Verify the possibility of the mobile application to send sensitive data unintentionally (location in a photograph's metadata).
- Regularly perform security analysis, penetration tests, definition of abuse cases and other practices of the secure SDLC for the back-end used by the application.
- Verify that the back-end stores the necessary logs to have a correct response against security incidents.
- Limit the number of request per second that a user/IP may make in order to limit the possibility of DoS attacks.

C6: Secure Integration with Third Parties Services

Risks

- Third parties' services used in an application may introduce new vulnerabilities in the application.

Controls

- Check the authenticity of third parties' libraries used (source of the code, maintenance, absence of Trojans, etc.).
- Maintain a list of all the third parties' libraries and services used in order to detect vulnerabilities or updates in the shortest period of time.
- Check that the libraries used do not have access to more information than what they are supposed to receive (advertisement libraries that access more data than what they should).

C7: Consent to Gather and Handle Data

Risks

- In the European Union, it is obligatory to obtain the consent of the user in order to collect or manage any personal information.

Controls

- Create a privacy policy covering the use of personal data and show it on all the occasions in which the users should take decisions regarding the use of their personal data.
- Consider any of the three following options to request the consent:
 - Installation or first execution.
 - First time that data are going to be gathered.
 - Via “opt-out” mechanisms in which the user is informed on the option by default and is given the possibility of deactivating it.

C7: Consent to Gather and Handle Data

Controls

- Verify the parts of the application in which personal data are gathered. It will not always be obvious since, for example: an identifier in the device that allows the user to obtain personal data should be considered as a personal data.
- Maintain a registry of how many times the user has provided consent for the handling of data. In addition, it is advisable to allow the user to revoke the consent through the same application (the way that OAuth provides it, for example).



C8: Access Controls for Paid-for Services

Risks

- The APIs used for the programmatic access to paid services may be abused by attackers or malicious software and lead to economical losses for the user.

Controls

- Maintain access logs to paid resources in a non-refutable format (receipt signed with a certificate) and provide users access to them.
- Protect such logs of unauthorised access or modification.
- Use mechanisms to detect anomalous use patterns and force the re-authentication of the user in such case.
- Use a white list to restrict the sending of information via SMS.
- Authenticate the access to all the paid resources' APIs.

C9: Secure Distribution

Risks

- Attackers may take advantage of the insecure distribution mechanisms of an application to provide “trojanised” versions of them.

Controls

- Distribute the applications through the official stores of the different platforms (they perform security verifications).
- The applications should be designed to be easily updated (database migration, taking into consideration the state of the application during the update process, etc.).
- Provide communication links and channels for users to be able to notify security issues in the application.

C10: Secure Use of the Execution of Dynamic Code

Risks

- The execution of dynamic code may give the opportunity to unreliable third parties to execute code in the application even if it has not been designed by the developers of the application.

Controls

- Minimise the use of interpreters during the use of the application (reflection in Java).
- Verify all the inputs and outputs of the application and limit data that are entered in the application via white lists.
- Verify the security of the application through the fuzzing of all its inputs.
- Isolate all the elements that may interpret code to be executed, to the least possible privileges



Security of the Device

Introduction

- Regardless the security characteristics provided by the operative systems, mobile devices face multiple threats:
 - Malware.
 - Dangerous behaviour by employees.
 - Wrongly programmed applications.
- Controls such as the ones included in the OWASP Top Ten Mobile Controls are useful to mitigate such threats. Such controls should be actively implemented in the development of applications.
- In the mobile environment, just like in desktop environments, it is possible to use a series of tools that allow users to improve the security controls provided by default by the operative system.
- Unlike the traditional desktop operative systems, the architecture of mobile operative systems limit the effect that a security tool may have on the operative system.
- Total access, just like in desktop systems, would allow malicious applications to control the system.

◆◆◆ Security of the Device

Introduction

- The device's security tools use specific APIs of the system that provide control over certain aspects of the operative system.
- On many occasions, the system requests the user's confirmation in order to allow the application to access the administration and security functionalities.
- Such authorisation may be made:
 - By the end user of the device.
 - By the department responsible for managing the devices of the organisation.
 - Through a specific management software that the device is connected to.
- Later in this section, the specific functioning of such security solutions will be described for each platform.





Antivirus

◆◆ Security of the Device

Antivirus

- Its scope is limited by the access that the operative system of the application provides.
- For example, on Android, antivirus softwares are able to inspect the content of SMS messages; however, on other platforms, such information is not accessible.
- In many cases, such privileges allow antivirus programmes to detect malicious behaviours, but they cannot execute the required controls to mitigate the threat automatically and thus, need the cooperation of the user.
- According to the operative system, they are able to:
 - Detect attempts of malware infection through the browser, application stores, messages, and other attack vectors.
 - Website's reputation services.
 - Detection of phishing or spam attempts.
 - Detect applications that include aggressive advertisement libraries.
- <https://youtu.be/OeBlfq84fwI>

Antivirus



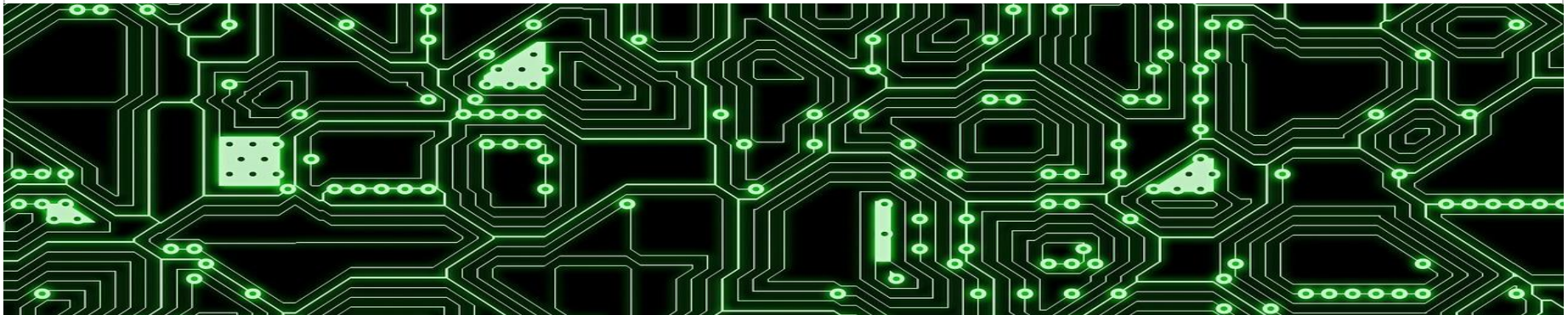
- Antivirus tools also collect information in devices, such as applications installed and other types of telemetry.
- This allows providers to transform the system in which the antivirus has been installed into an additional sensor of its network, for the early detection of new threats.
- In general, mobile antivirus softwares are provided for free with limited functionality.
- In addition, many providers of such products also offer additional services that sometimes require a paid subscription.
 - Location of the device via web.
 - Remote wipe of the device.
 - Backups.

Antivirus

- The detection of malicious behaviour is performed by following different complementary approaches:
 - Detection via signatures: malicious programmes' signatures are extracted and each file is compared with the signatures existing in the database. The signatures may include all kind of information, from files hashes, calls to API, code similarity, etc.
 - Detection of anomalies: the normal behaviour of the user and the used applications are modelled with a training process. If the system starts to behave out of the model, an alert is created.
 - Risk calculation: definition of some basic rules that all the applications should comply (use of permissions, access to personal data, etc.), and description of the risk that each of such operations implies. If an application exceed the limit, it is considered as potentially dangerous (even if it is not a malicious programme).
- Due to the restrictions existing in mobile operative systems, the detection via anomalies is not widely used.

Antivirus

- In an antivirus system, the period of time existing from the moment in which the software is created and deployed, to the detection and creation of new antivirus signatures is essential.
- Such time is known as window of vulnerability, since it is the period of time within which the antivirus systems based on signatures are not able to detect the threat.
- Systems based on anomalies and risk calculation, on the contrary, are able to detect such kind of threats, but only if they have been designed taking into consideration the aspects that the new malicious software takes advantage of.
- For this reason, some advanced attacks (targeted attacks) that use zero-day exploits may not be detected by such kind of systems.



Virtual Private Networks



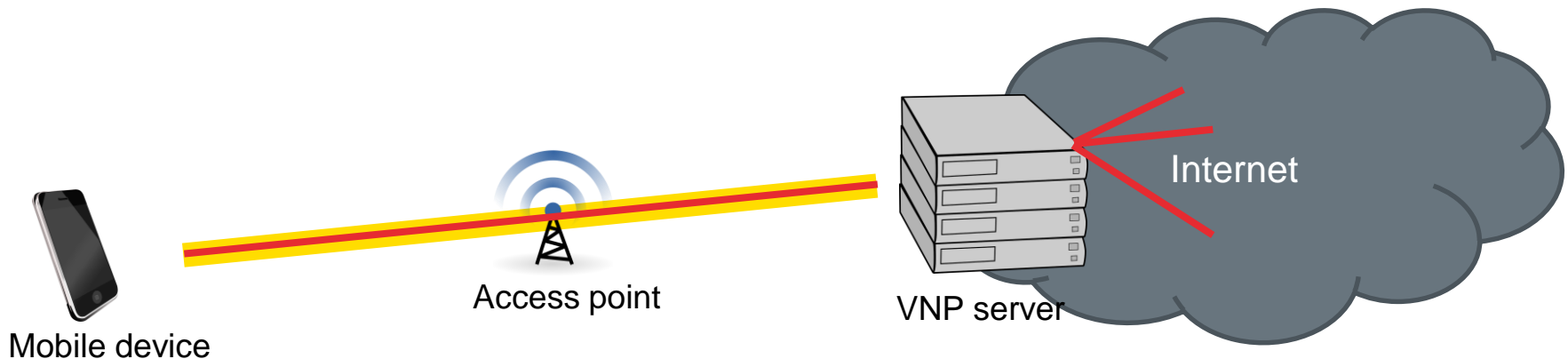
Virtual Private Networks (VPN)

- Operative systems include the option of creating connections to virtual private networks through the settings menus of the device.
- The parameters of such configurations are complex or varies over time, that is the reason why systems allow the configuration of VPNs via applications as described below:
 - The user runs the VPN management application (it may have been installed through an app store or included as part of the set of applications installed by the organisation).
 - The user's credentials should be entered in the application.
 - If the authentication is correct, the application downloads all the data for the configuration of the virtual private network in the device and requests the user its installation.
 - Depending on the operative system and permissions of the application, the user should confirm the new installed configuration.
 - The application uses the system's APIs to establish the connection to the configured VPN service.

◆◆ Security of the Device

Virtual Private Networks (VPN)

- When the mobile device is connected to the VPN network, all the (generally configurable) internet traffic is encrypted and sent to the VPN server.
- From the VPN server, each packet is sent to its final destination.
- For example, in the case of a connection, the SSL packet is encapsulated in the VPN protocol to the server and it is sent to its original destination from there.
- Thus, the device is connected to the internet from the VPN network and not from the original access point.





Content Blockers

Content Blocker

- A content blocker analyses the information exchanged in a website connection and eliminates those contents that are not allowed by the established policy before being showed by the browser.
- A content blocker may analyse HTML code, Javascript, flash objects, etc., according to the type of device and content blocker.
- Generally, they are used to block advertisements; however, they may be used to restrict connections to certain sites or to prevent the execution of certain contents in the user's browser.
- It is possible to implement them as own web browsers, or as applications that control the content shown by browsers that are already installed in the system.

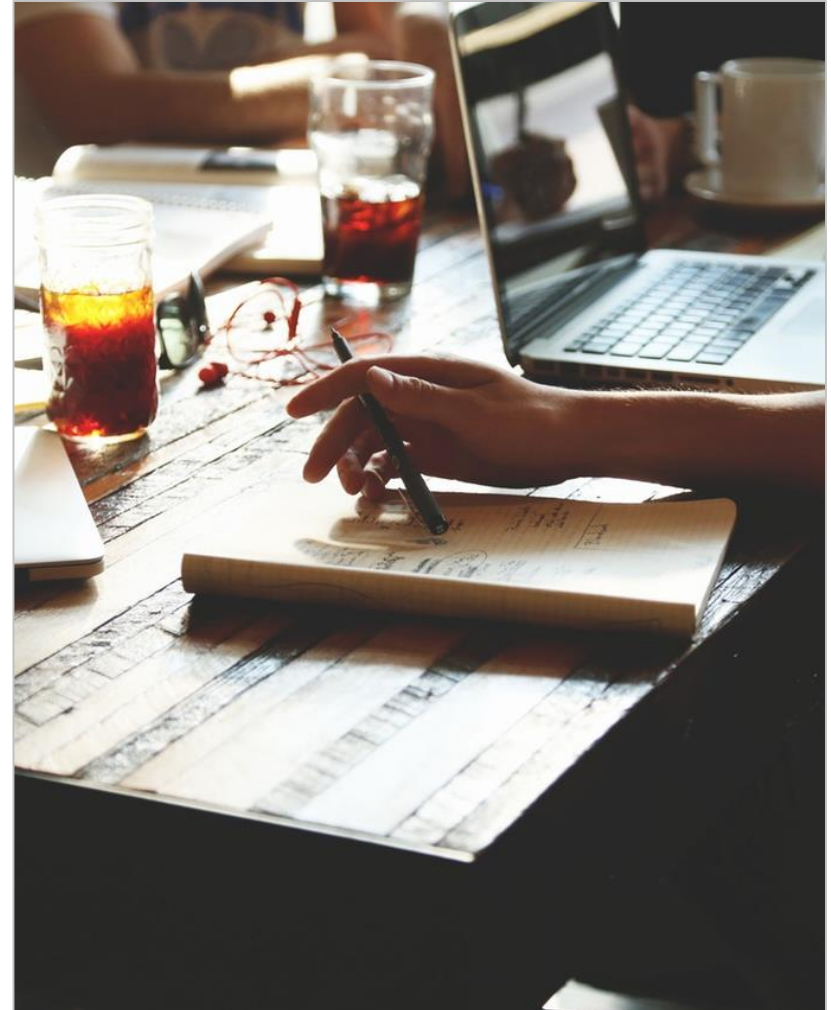
A tall, metal lattice tower, likely a telecommunications or radio tower, stands against a clear blue sky. The tower is covered in various antennas, dishes, and equipment. A semi-transparent dark grey rectangular box is centered over the middle of the tower, containing the text "Mobile Device Management" in white.

Mobile Device Management

◆◆◆ Security of the Device

MDM (Mobile Device Management)

- The device management systems (MDM) are used to control, at a high level of detail, the configuration and tasks that can be carried out with a mobile device.
- They are used in business environments in order to manage the mobile devices used by the employees to perform their functions
- There is a specific section within this unit in which the different characteristics and functionalities provided by MDM systems will be reviewed.



The image features the green Android robot character on the right side, set against a dark background with out-of-focus blue and orange light circles (bokeh). A semi-transparent grey rectangle is positioned in the center, containing the text.

Security of the Device on Android

◆◆◇ Security of the Device on Android

Introduction

- Android allows applications to use two main systems for the implementation of additional security measures on the device.
 - Permissions.
 - Device Administration API
- Furthermore, from version 4.2 of Android, devices with the Google Play application have the “Verify Apps” service activated by default.
- There is no an accurate public description of the functioning of Verify Apps, but it is known that:
 - It analyses both the static characteristics and the behaviour that applications have within the device in real time, whether they come from Google Play or not.
 - It enables the scanning of remotely activated devices, and the average time between devices scanings is one week.
 - Apart from being able to take decisions on the threat that an application may pose, it also sends telemetry to Google’s servers.

◆◆◇ Security of the Device on Android

Permissions

- Some of the permissions existing on Android, allow the implementation of specific security functionalities of the device as an antivirus.
- The main group of permissions that may be used by applications and the functionality that they provide from the point of view of security are explained below:
 - User accounts: they allow the remote wipe of the accounts of the device.
 - Location: it allows the user to locate the device in case of loss.
 - Calls: it allows users to block calls to special pricing numbers or to blocked contacts.
 - Internet and networks: it allows users to control networks that the device connects to, and limit access to networks that have not enough protection. It also allows the update of antivirus signatures.



◆◆◇ Security of the Device on Android

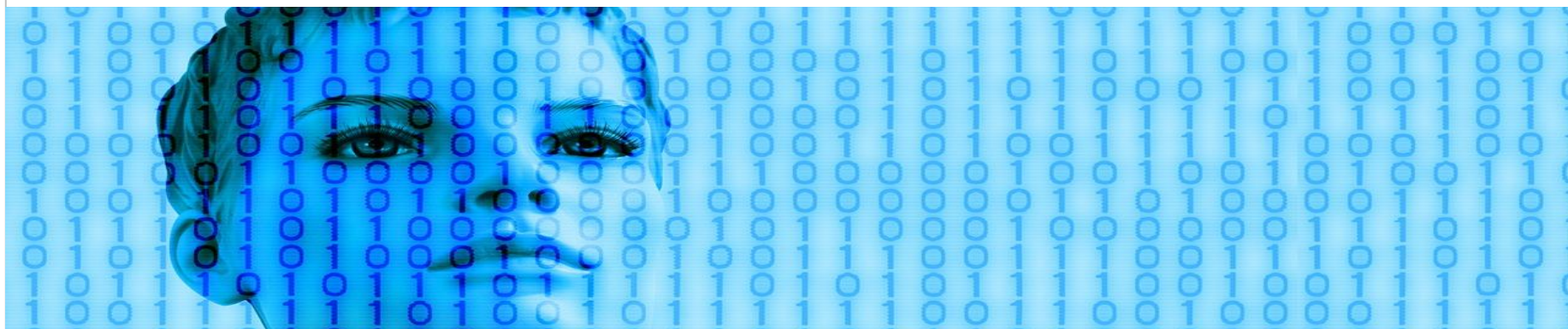
Permissions

- Personal and social network-related information: it enables the remote removal of information stored in calendars, email, and other personal information elements that require this group of permissions to access them.
- External storage: it allows users to analyse applications (code, resources, etc.) installed in the SD card. Due to the restrictions of the operative system, the applications installed in the internal memory cannot be analysed.
- History and bookmarks: they allow users to verify the origin and detect malicious websites that have been visited or are saved as bookmarks in the device.
- Management of applications: it allow users to list processes in execution, access the identifiers (package name) of each application and close applications considered as malicious.

◆◆ Security of the Device on Android

Permissions

- Camera: it allows users to take pictures in case of theft of the device.
- Draw on other applications: this permission makes it possible to show alert messages on the interface of any other application without needing the security tool to be in the foreground. This permission is used to show an alert if the user tries to open an application considered as malicious. It also allows, together with management of processes permissions, to block access to applications by drawing an interface above it (generally, to be unlocked via a password or code).
- Read logs: from Android 4.0, it is not available for third parties' applications. It enables access to logs in order to know what applications are being executed.



◆◆◇ Security of the Device on Android

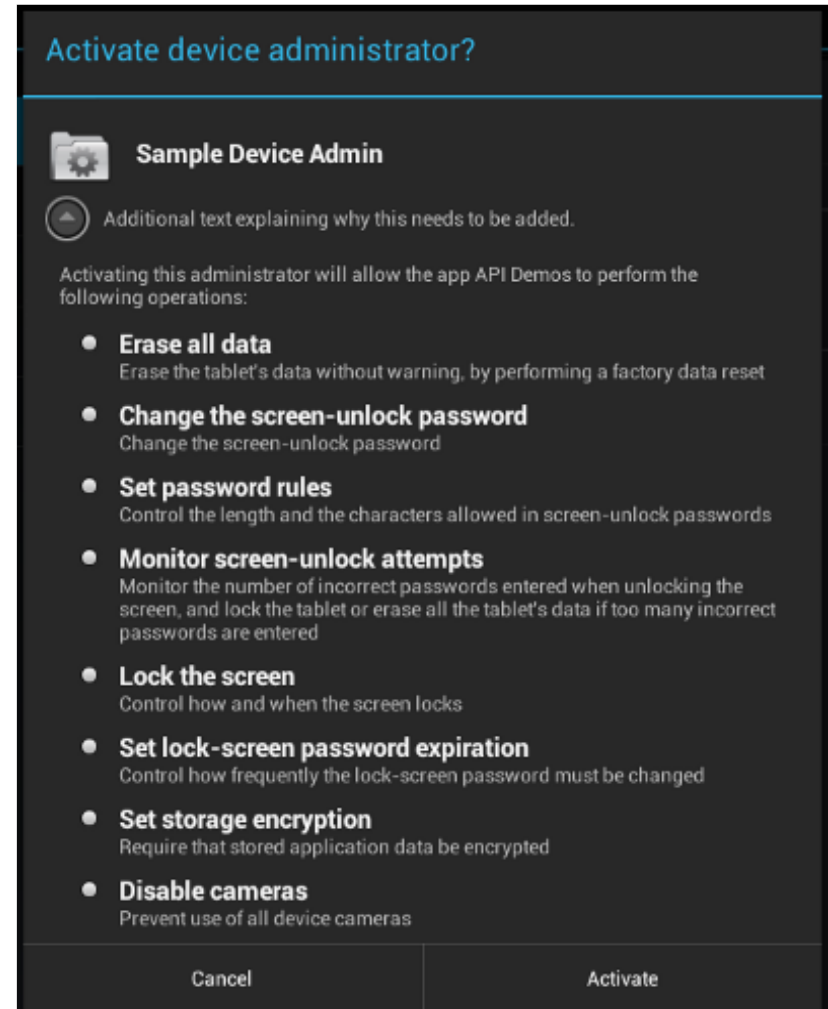
Device Administration

- The device administration API for Android (available from version 2.2) allows certain low-level characteristics to be managed by third parties' applications.
- This API is used by security applications of the device, but also by mobile device management (MDM) systems.
- The applications that use such API should:
 - Implement a Receiver that comes from `DeviceAdminReceiver`, able to capture intents with the action: `android.app.action.DEVICE_ADMIN_ENABLED`.
 - Add the `BIND_DEVICE_ADMIN` permission to the receiver to prevent it from being accessed by other applications.
 - Add the security policies to configure the created receiver. The security policies may be downloaded from the internet or be statically defined in the application.
 - Launch an intent with the `ACTION_ADD_DEVICE_ADMIN` action in order to use the administration functions.

◆◆◆ Security of the Device on Android

Device Administration

- In order to use the administration APIs of the device, the user of the device should explicitly confirm the access to the device administration functions.
- The management application should use an `ACTION_ADD_DEVICE_ADMIN` intent to request such permission. Then, a screen as the one shown here is displayed.



Device Administration

- Among other things, the Device Administration API allows users to:
 - Manage passwords:
 - Oblige users to establish a password in the device.
 - Establish minimal characteristics for passwords used in the device.
 - Establish a maximum number of failed attempts for the device wipe.
 - Limit the use of old passwords.
 - Define the period of time that the device may be inactive before blocking the screen with code.
 - Remotely perform the device wipe.
 - Deactivate the device's camera.
 - Activate the encryption of the device.
- In the following section, focused on Mobile Device Management, such types of policies will be reviewed.

Security of the Device on iOS



◆◆◇ Security of the Device on iOS

Introduction

- On iOS, it is forbidden by default to access the main resources of the system and no application may access them.
- It makes impossible the creation of applications that provide additional security characteristics within the device.
- For example, an antivirus application has no place within the iOS environment, since it cannot access the applications installed or being executed in the device.
- The security characteristics provided to third parties' applications on iOS are focused on three main points.
 - Creation of web browsers with content analysis via web visits.
 - Contents blocking on Safari.
 - Configuration profiles.

◆◆◇ Security of the Device on iOS

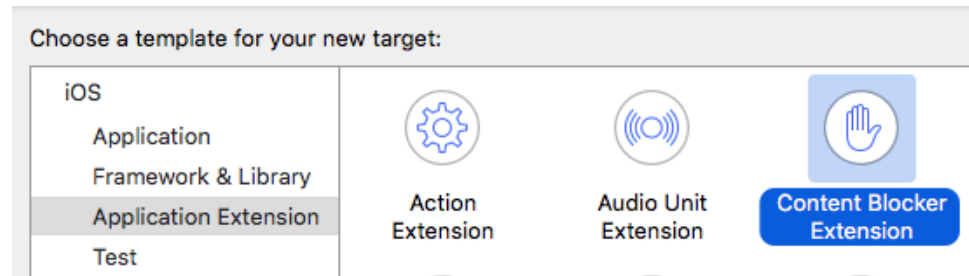
Secure Web Browsers

- To date, most security providers of the device have only provided web browsers that analyse the content that the user navigates through.
- To this end, a web browser is built through the use of web views provided by the operative system, above all via UIWebView and WKWebView.
- This way, the user obtains additional security services:
 - Verification that the accessed web page is not part of a phishing campaign and does not provide dangerous content.
 - Deactivation of elements of the web page, such as cookies to track the user, aggressive advertisements or dangerous Javascript code.
- The inspection of content is performed through the method that such views provide for the execution of Javascript.
 - *evaluateJavascript* for WKWebView.
 - *stringByEvaluatingJavaScriptFromString* for UIWebView.

◆◆◆ Security of the Device on iOS

Content Blockers

- Content blockers on iOS are created as an extension of the application, since they live and are executed as an different application from the main one:



- Once it is created, a new extension is created in Xcode including the following files (h and m files correspond to the Objective-C version):



◆◆◆ Security of the Device on iOS

Content Blockers

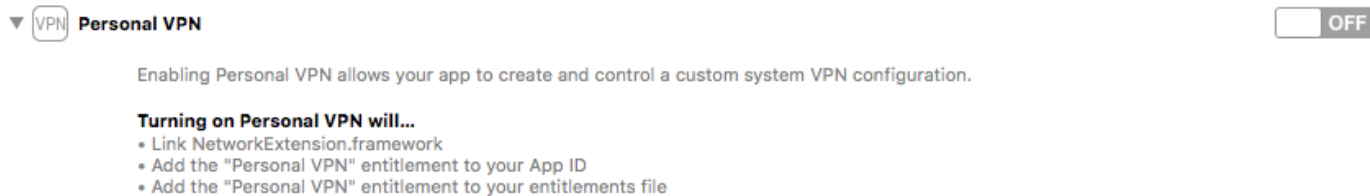
- **BlockerList.json:** it includes a set of rules in json format about contents to block. The rules enable the content blocking by using rules based on the URL, types of resources (tags, CSS, images, etc.), and regular expressions. The allowed actions when a rule is executed are: blocking all the content, blocking the site's cookies, or applying a specific CSS configuration not to show a part of the content.
- **ActionRequestHandler:** it is the code responsible for loading the blockerList.json file every time that the extension is activated. It may be used to update the block list of the device.
- **Info.plist:** it includes the configuration of the extension.




◆◆◆ Security of the Device on iOS

Configuration Profiles

- The configuration profiles are XML files that allow users to configure various properties of the system:
 - Restrictions in the characteristics of a device (camera, applications, etc.).
 - Wi-Fi and VPN connections.
 - Configuration of mail accounts, LDAP, and Exchange.
 - Credentials and passwords.
- In the case of the creation of VPN networks via applications, apart from the user accepting the configuration profile, it is also necessary that the application includes the ability to configure VPN connections.



- Options provided by the configuration profiles will be studied in deep in the section focused on MDM.



Security of the Device on BlackBerry

◆◆◇ Security of the Device on BlackBerry

Introduction

- Since BlackBerry is focused on security, the security options are generally implemented through MDM and not via third parties' applications.
- The permission system of BlackBerry, just like the one on iOS, highly limits the security functions that may be executed by applications external to the operative system.
- Given the possibility of executing Android applications, many of the options provided for the creation of security applications on Android, based on permissions are also available for BlackBerry
- From BlackBerry 10, all the applications installed on the device go through a security system called BlackBerry Guardian.
- The options available on Android for devices management are not available on BlackBerry, since they implement their own Mobile Device Management system.

Security on BlackBerry

- BlackBerry Guardian works in a similar way to Verify Apps by Google.
- The system combines three elements:
 - Automatic systems for static analysis.
 - Manual analysis of applications.
 - The apps reputation service provided by Tren Micro.
- Furthermore, BlackBerry Guardian analyses whether applications inform properly on how to access personal data of the user. If such information is not available and verifiable, the application is not accepted in the BlackBerry World market.
- Android applications are also analysed and verified by this system, both if they come from the Amazon app store or from other sources.

A black and white photograph of a Windows Phone lying on a textured surface. A pair of headphones is plugged into the phone and lies to its left. The phone's screen displays a music player application. At the top, the word "korektor" is visible. Below it is a search bar containing the text "niska". The main part of the screen shows a frequency spectrum analyzer with a grid of horizontal bars. The x-axis is labeled with values: -12, 57, 280, 690, 1300, 2200, 3600, and 6200. The y-axis is labeled with "niska" at the bottom and "wysoka" at the top. At the bottom of the screen is the Windows Phone navigation bar, featuring a back arrow, the Windows logo, and a search icon.

Security of the Device on Windows Phone

◆◆◇ Security of the Device on Windows Phone

Introduction

- Similarly to iOS and BlackBerry, Windows Phone's architecture highly limits the security functions that may be executed by external applications to the operative system.
- Similar to what happens on iOS, Windows 10 allows users to configure different security elements via Provisioning Packages that enable the configuration of the following elements among other ones:
 - Applications installed.
 - Subscription to MDM services.
 - Restrictions in the characteristics of the device (camera, applications, etc.).
 - Wi-Fi and VPN connections.
 - Configuration of the home menu.
 - Credentials and passwords.

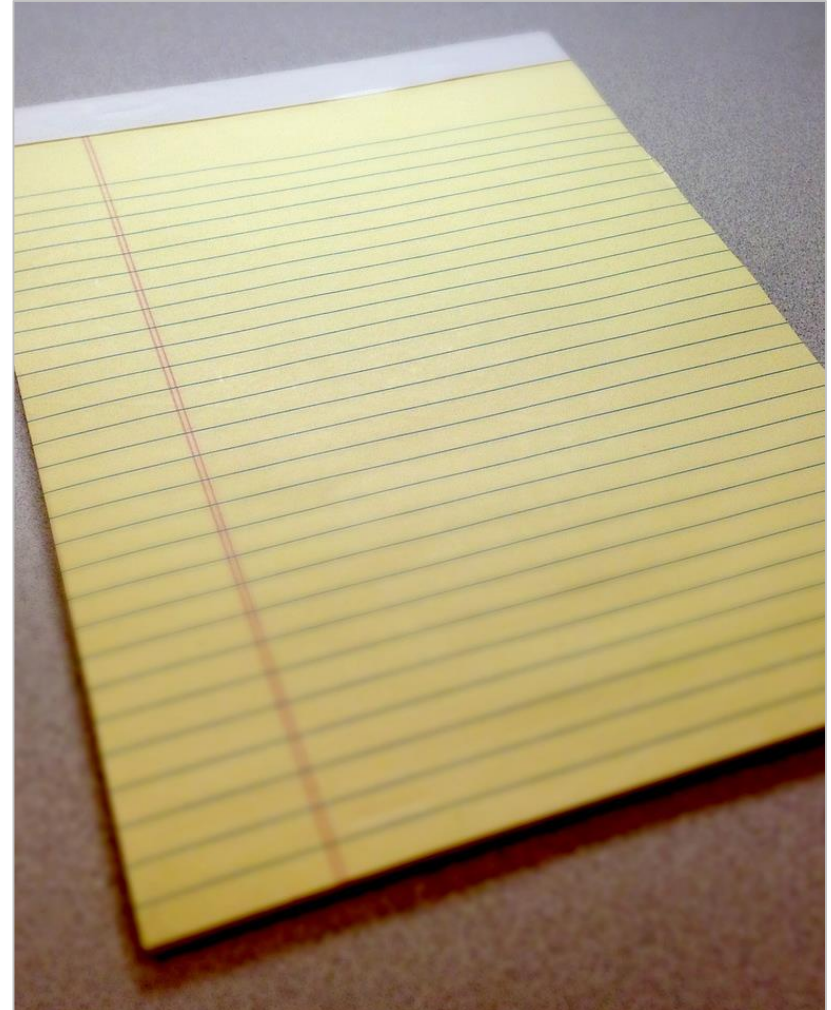
Instructions for the Forum

- Using the knowledge obtained within this section, students should use the forum to discuss the limits of security tools of the device that have been reviewed in this section.
- The main objective of this activity is to compare these kind of tools that are available in mobile devices with the same technologies in the context of desktop environments.
- In order to encourage the debate, we propose the following activities:
 - Analyse the specific functionality of the security applications available in each of the existing app markets.
 - In case of having a device, install the applications to verify their functionality.
 - Compare the most common functionalities provided by the different applications in each platform.

◆◆◆ Security of the Device

Instructions for the Forum

- In addition, the following questions are proposed to be discussed in the forum:
 - What resources does Android provide in order to protect the system against malicious applications that are executed from the internal storage?
 - What if such application is installed in the SD card?
 - Is there any API that provides a functionality similar to antivirus systems on iOS?
 - What if the device is jailbroken?
 - Taking into consideration limitations existing nowadays, is there any method to implement a firewall-based system in any of the mobile platforms existing?





Mobile Device Management

Introduction

- Mobile Device Management systems are responsible for administration, management, configuration, and inventory of mobile devices used in a business environment.
- MDM systems are aimed at optimising the use of mobile devices within an organisation, without compromising the information that is managed or its infrastructure.
- MDM solutions base their functionalities on the support that mobile platforms provide for the use of devices in a business context.
- During the initial versions of mobile operative systems, the management of devices for business environments is not a priority, but it is now included in most available mobile platforms.

◆◆◆ Mobile Device Management

Types of solutions

- There are different types of solutions in the context of mobile device management.
 - **Mobile Device Management:** it allows users to manage and configure security policies at application level. Solutions provide own applications already prepared to manage or use specific SDK in order to integrate the application in the management system.
 - **Mobile Identity:** it allows the use of mobile devices as a tool to verify the user's identity in the access the organisation's services.
 - **Mobile Device Management:** it enables the manage of information related to the organisation from the mobile device. Such tools provide access, after the correct authentication to documents of the organisation, restricting actions that can be performed with them from the device.

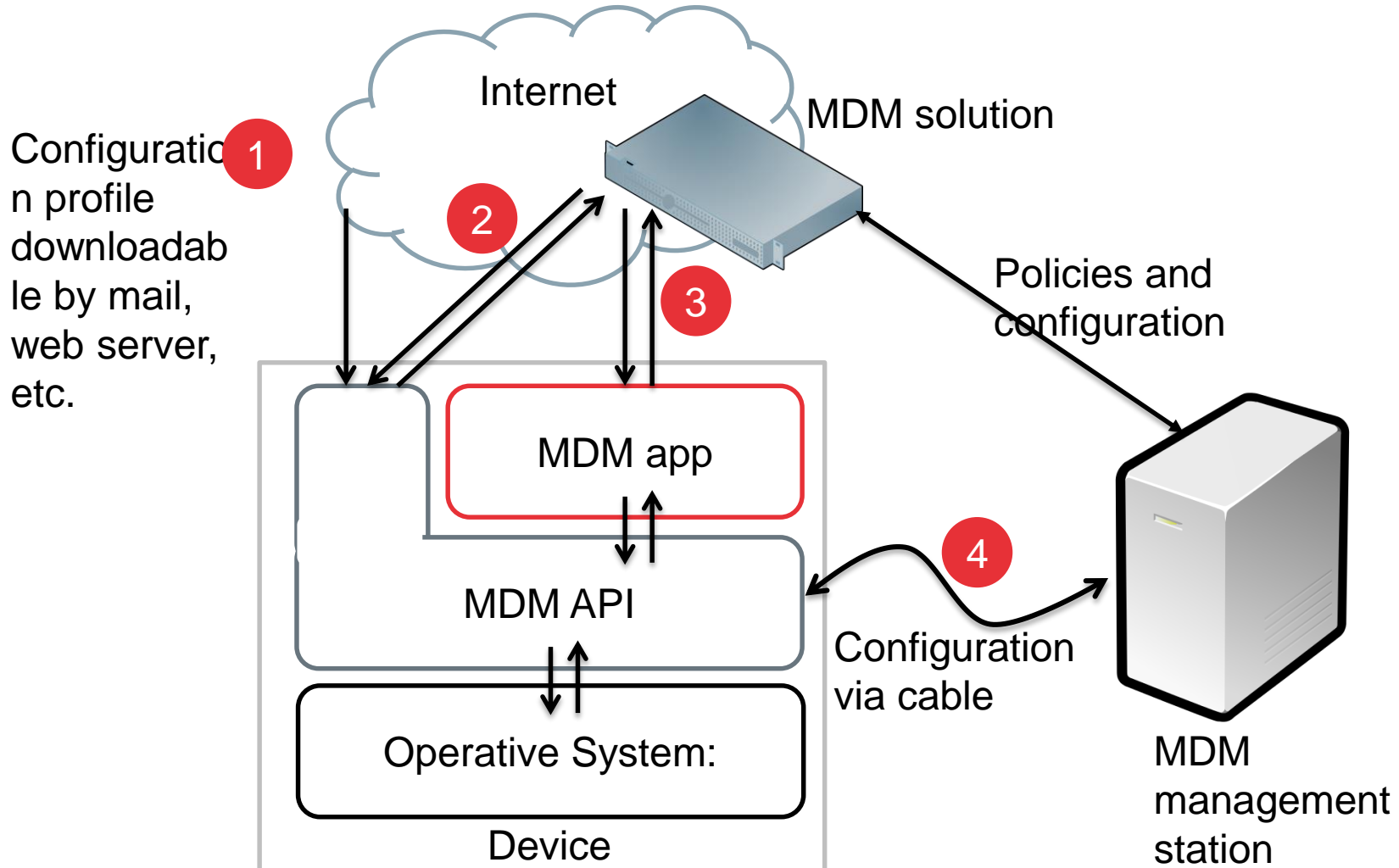




Functioning

◆◆◆ Mobile Device Management

Functioning



Functioning

- The operative system provides a series of MDM APIs that enable the configuration of different security aspects of the mobile device.
- The MDM APIs may be accessed through 4 main methods (circles of the last figure):
 1. By downloading configuration files (profiles) via an application of the system.
 2. Through a connection to an MDM solution that communicates with the device's MDM API directly.
 3. By using a specific application responsible for managing the connection with the MDM solution and communicates with the MDM API from the device.
 4. Through the connection of the device to a computer with an MDM solution for the configuration of devices through a wired connection.
- Next, the possible options are described more in deep.

Download of Files

- The configuration of devices through files is available on iOS (via configuration profiles) and Windows systems (via provisioning packages).
- The configurable options in each platform through such profiles are different:
 - For iOS.
 - For Windows.
- Configuration files may be signed to allow the identification of its origin. In the case of Windows, if the file has been signed by a “Trusted Provisioner”, it may be installed without the consent of the user.
- The use of such kind of profiles may create attack vectors, since malicious applications and webs may trick the user to install configuration profiles that make the device vulnerable against certain attackers.

Direct Connection with the MDM Server

- Mobile operative systems provide specific protocols for the connection with MDM servers.
- The protocols depend on each operative system; therefore, third parties' solutions should integrate each of them separately.
- In order to configure the MDM server in the device, there are three possibilities.
 - Use configuration files that the MDM server configures in the device. The file may be downloaded from a URL or opened from a mail application.
 - Use a wired connection and a programme for the configuration of the specific MDM section of the device.
 - Compare the pre-configured devices through a programme provided by a manufacturer or provider. An example of such system is the programme provided by Apple.
- Such type of deployment is allowed on Windows Phone, iOS, and BlackBerry devices.

◆◆◆ Mobile Device Management

Use of a Management Application

- Such type of solution is quite similar to the one that connects directly with the servers of the MDM solution; however, in this case, an application installed in the device is used and such device is intermediate between the server and the MDM API.
- The mail clients that allow the configuration of Exchange accounts are an example of such kind of applications.
 - Apart from access to mail accounts and calendars, the Exchange accounts allow to establish a series of security policy in a device.
 - Once the Exchange account has been configured, the policies that have been established in the Exchange server will be transmitted to the device.
 - This functionality is included in [Windows Phone](#), [Android](#), [iOS](#), and [Blackberry](#) devices; however, not all the policies are supported by all the devices.
- On Android, the MDM management should always be made through an application that uses the Device Administration API.

Wired Connection

- Wired connections allow users to create and transfer configuration profiles to devices to be managed.
- Such type of approach is viable for environments in which a relatively small number of devices have to be managed, but it is not able to manage great collections of devices efficiently.
- For example, [Apple Device Configurator](#) allows the configuration and management of iOS devices. The requirement of a wired connection make the configuration of great amounts of devices impractical. In order to configure a great number of devices, it is necessary to use third parties' solutions or the one provided by Apple ([Profile Manager](#)).
- Such type of solutions does not allow users to obtain information at runtime on the use of the device or the compliance with the policies installed.

A close-up photograph of a person's hand holding a silver smartphone. The person is wearing a dark grey or black suit jacket. The background is blurred, showing a light-colored wall and a white door frame. A semi-transparent grey rectangular box is overlaid on the image, containing the word 'Characteristics' in white, bold, sans-serif font.

Characteristics

Configuration Options

- MDM solutions allow the management of the following aspects, among other characteristics:
 - Authentication.
 - Inventory.
 - Definition and management of security policies.
 - Hardware restrictions.
 - Management of system and third parties' applications.
 - Management of the device's configuration.
 - Violations of the security policy.
- The specific functionalities depend on the MDM solution used and the operative system of the mobile device.
- Next, such functionalities will be described.



Authentication

- MDM solutions allow the installation of credentials in mobile devices, to be used when accessing services of the organisation.
- In general, credentials are installed in the device via certificates that are remotely or locally installed (through cables) in the device.
- The certificates may be used for:
 - Authentication on SSL servers when connecting to web pages.
 - Authentication on mail servers.
 - Authentication on corporate Wi-Fi networks or VPN servers.
 - Signature, verification, and encryption of email messages via S/MIME.
- The certificates remotely emitted may be obtained through the SCEP protocol.

Authentication

- This protocol is supported by iOS and BlackBerry by default. On Android, it is possible to add the support via third parties' applications, such as [BES12](#) by BlackBerry.
- The SCEP server may be configured through the MDM solution itself or a downloadable configuration profile.
- The certificate obtaining process varies according to the implementation and the certificate to use, but, in general, it is performed as follows:
 - The user obtains credentials from the organisation for the request of certificates through an out-of-band channel. The credentials (a pre-shared key) are configured in the SCEP server.
 - The client creates a certificate request and sends it to the SCEP server, including the pre-shared key.
 - The administrator reviews the request and whether credentials coincide with the ones stored by the organisation, the certificate corresponding to the request is created and sent back to the device.

Authentication

- The SCEP protocol may be vulnerable to attacks. Any attacker with access to the pre-shared key will be able to make requests on behalf of the user.
- Therefore, it is necessary to use a secure channel for the transmission of the request.
- In general, it is advisable that request to the SCEP server is made from the infrastructure of the organisation itself.
- Windows mobile 10 enables the integration of mobile devices for the authentication in work stations via MDM policies. This way, apart from the access password, the work station should be connected to the employee's mobile phone via Bluetooth, in order to verify the credentials and unlock the device.

Inventory

- The abilities of an MDM to perform inventories provide a general vision of mobile devices managed by an organisation.
- Most MDM solutions enable the organisation of mobile devices into groups. The groups may be used to represent departments or roles within the organisation.
- This enables a more efficient management of all the devices associated to a department.
- MDM solutions collect information on the device via two main mechanisms:
 - MDM API: it allows users to obtain information directly from the device.
 - Applications: through permissions obtained, they allow users to obtain information on other elements that are not accessible through the MDM API
- According to the operative system, the information elements will be collected via one or another mechanism.

Inventory

- In general, it is possible to access the following information of each device:
 - Basic information: including the name, IMEI, and serial number of the device.
 - Hardware: detailed description of the existing hardware on the device and its state (empty space, etc.).
 - Operative System: version of the operative system installed.
 - Network information: telephony network used, MAC address of the Wi-Fi and Bluetooth connections, roaming configuration, and phone number.
 - Location: depending on the solution, last known location or history of location.
 - Policy: it specifies the security policy of the device and whether it is being complied or not.
 - Software: applications installed on the device together with their version and size.
 - History: a history of events related to the device.

Definition and Management of Security Policies

- Regarding MDM, a security policy is a set of rules that define the configuration and state in which the organisation's mobile devices should be in order to maintain minimal security levels.
- The security policies allow users to reduce risks associated to the management of mobile devices and to ensure the conformity with security standards and regulations.
- Policies defined in the MDM service may be applied to:
 - All the devices controlled by the MDM solution.
 - All the devices included in a group.
 - A device in particular.
- In MDM, the policies may be sent to the devices:
 - Over-the-air: the device receives the security policies through a direct update of the MDM server.
 - Via cable: the mobile device is connected via cable to a work station that includes the MDM management tool.

Hardware Restrictions

- MDM solutions allow users to deactivate and restrict the use of certain hardware elements of the device:
 - Restriction in the use of the camera: in some solutions, it can be configured so that it cannot be used according to the context of the device (Wi-Fi network connected, GPS position, etc.).
 - Forbid screenshots.
 - Deactivate the device's biometric systems.
 - Deactivate the option to update the registration data of the device's biometric system .
 - Deactivate Bluetooth, NFC, Wi-Fi, or any other network interface available.
 - Deactivate the option of using SD cards.



Management of the Device's Configuration

- MDM solutions allow the modification or forcing of the following aspects of the device's configuration.
- The configuration of the lock code of the device, in addition to:
 - Making compulsory the configuration of a lock code.
 - The complexity of the lock code used (simple, alphanumeric values, complex, minimal length, etc.).
 - The expiration of the lock code.
 - The time before the automatic lock of the device.
 - The possibility of reusing lock codes.
 - Maximum number of attempts before the complete device wipe.
 - Time between failed attempts.
- The configuration of an obligatory HTTP proxy server.
- White and black lists of URLs that the device may connect to.
- The use of disk encryption and its configuration.

Management of the Device's Configuration

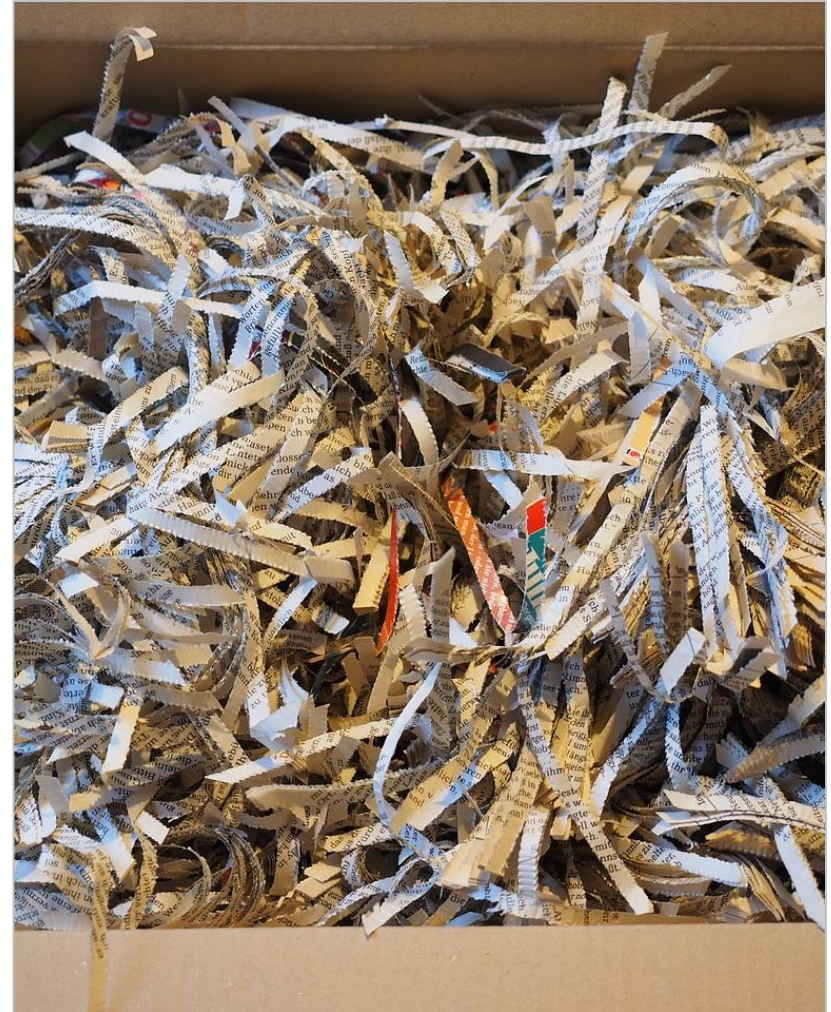
- Connection parameters of the device:
 - Wi-Fi authorised networks, including credentials for the connection and the option of connecting automatically.
 - Allowed Bluetooth devices.
 - VPN networks including access credentials and applications that should use them by default.
- Configuration of the SCEP service to obtain certificates.
- Email accounts, calendars, LDAP, CardDav...
- Restriction and configuration of specific characteristics of the operative system, such as backups, voice dictation, payment means, etc.
- Installation of root certificates: such certificates can be used to accept other certificates, and may, for example inspect the content of SSL connections.
- Avoid the modification of security options of the device through the use its menus.

Management of Applications

- MDM solutions allow different ways of management of applications installed in the mobile device:
 - Limiting the access to applications installed by default in the operative system, such as the web browse, application stores, or other applications of the system.
 - Defining white and black lists of applications to be installed or forbidden in the device.
- Some MDM solutions enable the deployment of specific application stores for devices of the organisation.
- Such specific stores may include applications developed by the organisation itself and a selection of applications of the official stores.
- MDM solutions that include such characteristics also allow the remote installation of applications in the device.

Violations of the Security Policy

- According to the MDM solution, there are various actions that may be carried out if one of the devices stops complying with any of the assigned policies. Such actions may be included within the policy itself to be automatically executed:
 - Notify the administrator with an alert message in the MDM administration console.
 - Send a message to the mobile device specifying the steps that the user should take to configure the device according to the policy.
 - Prevent the execution of certain applications or the access to certain services of the organisation, such as the email.
 - Remove the organisation's applications of the device or even the whole device.



A close-up photograph of a chessboard. In the center, a black king piece stands upright. To its left and right, several white pieces are lying on their sides, indicating they have been captured or are out of play. The chessboard has a black and white checkered pattern. The background is a blurred blue and white striped pattern, possibly a flag. A semi-transparent grey rectangle is overlaid on the center of the image, containing the word "Providers" in white text.

Providers

MDM Platform

- Nowadays, there is a great offer of MDM solutions.
- Among the solutions developed by the device developer companies, we can find the following:
 - Apple provides [Device Configurator](#) that requires wired connection, and [Profile Manager](#) that allows users to send policies via Internet. Both are limited to iOS devices.
 - Microsoft provides a solution called [Enterprise Mobility Suite](#) that enables the configuration of Android, iOS, and Windows Phone devices. In addition, it allows the integration of desktop and laptop Windows systems.
 - BlackBerry has BlackBerry Enterprise Server 12 ([BES12](#)) that enables the MDM configuration of Android, iOS, Windows Phone, and BlackBerry devices.
 - Google does not provide any self-included solution for the management of devices; it only provides services included through the [Android for Work](#) platform in order to be used by third parties' in the management of applications and devices.

Other MDMs

Third parties' MDMs



Regarding third parties' solutions, it is important to highlight the following ones, qualified in the “Magic Quadrant” by Gartner in 2015 as “visionaries” and “leaders”.

AirWatch: <http://www.air-watch.com>, product owned by VMWare.

MobileIron: <https://www.mobileiron.com>

Citrix XenMobile: <https://www.citrix.com/products/xenmobile/overview.html>

IBM MaaS360: <http://www-03.ibm.com/security/mobile/maas360.html>

Good Work: <https://www1.good.com/applications/good-work/>, recently acquired by BlackBerry.





Recommendations

◆◆◆ Recommendations

Good Practices

- Due to the convergence of the characteristics provided by most MDM platforms and solutions, it is possible to unify all the recommendations for the secure configuration of mobile devices in the context of an organisation.
- Variations in the different security policies will be specified in many cases by the organisation's needs.
- Next, we will describe a series of minimal security recommendations that should be included in all the security policies, regardless the operative system of the device.



◆◆◆ Recommendations

Good Practices

- Require lock codes in all the devices by default:
 - In order to increase the complexity of dictionary attacks, they should include, at least, a digit, an upper and a lower case letter, and a punctuation mark.
 - Minimal length of 8 characters.
 - Passwords should be changed every 6 months without the possibility of reusing the last ones.
- Use only devices that enable the activation of disk encryption by default (Android).
- Eliminate the functions of the operative system that will not be used:
 - Deactivate Siri, iCloud, AirDrop, and other functionalities on iOS.
 - Deactivate Google Now, NFC connections, and Bluetooth on Android devices.
 - Deactivate or limit the use of the camera and block screenshots.

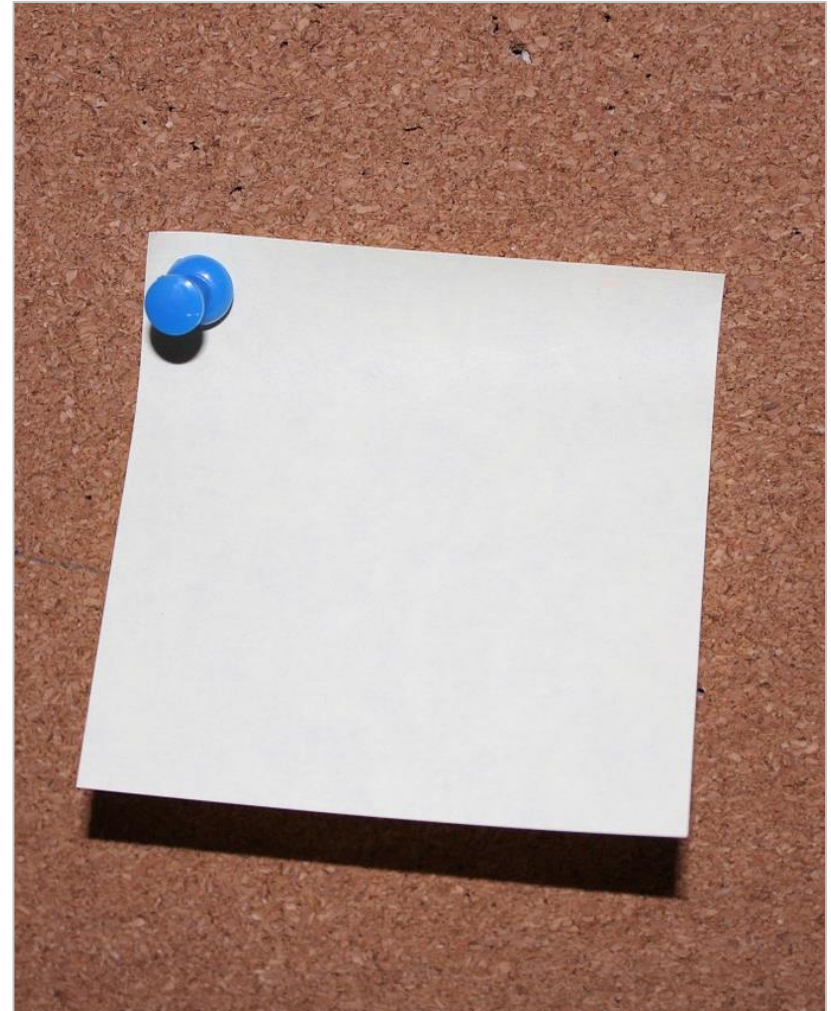
Good Practices

- Eliminate the access to official application stores and only allow the installation of applications via Push services of the MDM solution, and the creation of a specific application store for the organisation
- Use the profile synchronisation on the internet (Over The Air) to update the credentials and configuration for accessing Wi-Fi, VPN networks, and other credentials of the system's applications.
- Establish a set of actions that are automatically executed in case of failure in the monitoring of security policies:
 - Always notify the user when there is a violation of the security policy.
 - In case that the policy is considered critical, perform a device wipe.

◆◆◆ Instructions for the Forum

Tasks

- Once the main characteristics provided by the MDM solutions and some of their providers have been studied, we suggest students to use the forum of the unit to:
 - Identify risks that may be mitigated through the use of MDM technology.
 - Identify other recommendations of MDM policies that may be useful on specific environments.
 - Compare in deep the capacities existing in different MDM solutions for the same mobile operative system.
 - Compare, for example, the management characteristics of iOS devices existing in the MDM solutions studied in this unit.
 - Investigate the existence of other MDM solutions that have not been mentioned in this unit.



The background is a dark, almost black, surface with a grainy, textured appearance. A horizontal band of a medium blue color stretches across the middle of the image. Overlaid on this blue band is the text "Mitigation Plans in Mobile Environments" in a white, sans-serif font. The text is centered and split into two lines. The overall aesthetic is technical and professional.

Mitigation Plans in Mobile Environments

◆◆◆ Mitigation Plans in Mobile Environments

Introduction

- As explained in the previous unit, risk mitigation plans are aimed at reducing risks and costs related to a security incident.
- In case that the infrastructure of the organisation has mobile devices, it is necessary to establish a series of action plans for the security incidents in which such devices may be involved.
- Among the security incidents that may affect a mobile device, we can find:
 - Loss of a device.
 - Rooting of a device.
 - Disconnection of the MDM solution of the device.
- The security incidents are described below, as well as a summary of the policies and actions that, implemented in a response plan, allow the minimisation of risks that may be created.

◆◆◆ Loss of the Device

Incident

- In this context, the description of the incident is quite simple.
- Such type of incident may occur in two different ways:
 - The user of the device forgets the device and is unconscious of such loss after a period of time. The disappearance is notified when the user is conscious of it and tries to recover the device then. From the functional point of view, such context is similar to a theft, when the user is unconscious of it.
 - The device is stolen and the user is conscious of the theft (for example, a robbery). In such case, the user notifies the loss of the device, a short period of time after the incident.
- In both cases, the activation of the incident is performed due to the notification of the user having lost the device.

Preventive Measures

- The following measures, allow the reduction of risks against an incident of loss of device.
 - Regular performance of backups on the organisation's servers or the ones provided by the MDM solution.
 - Activation of the encryption options of the device.
 - Establishment of the shortest possible period of auto-block.
 - Password options:
 - The password should have a minimal complexity, including upper and lower case letters, digits, numbers, and punctuation marks.
 - At the tenth attempt when entering the lock code, the device should be automatically formatted.
 - Forbid the modification of configuration parameters of the device through its configuration menus.

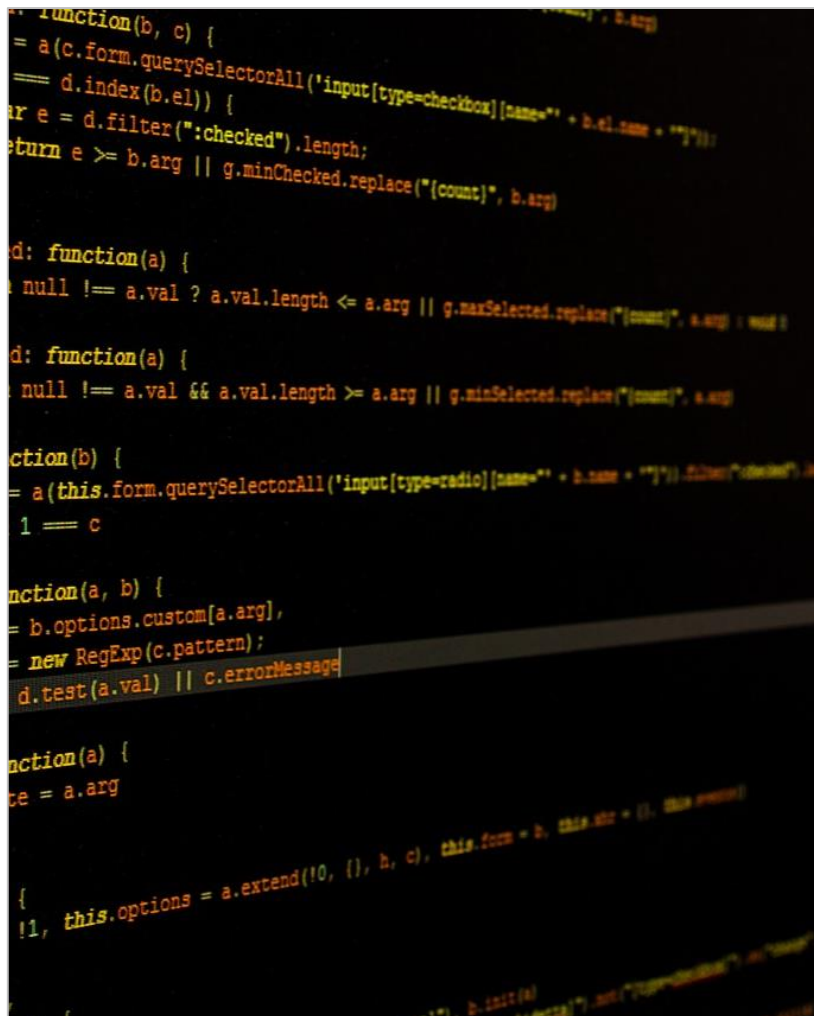
◆◆◆ Loss of the Device

Measures in Case of Incident

- In case that an employee notifies the loss of a device, the procedure to follow is explained below:
 - Use the MDM solution to locate the device and try to contact with the person that has found it via messages or its phone number. The following actions may be performed during this stage:
 - Locate the GPS position of the device.
 - Take pictures using the device's camera.
 - Send messages or make calls to the phone number corresponding to the device.
 - If there is a response and the person that found the device (if it was not stolen) agrees to give the device back → Agree on a place of delivery.
 - Process to block the device until the delivery.
 - Once the device has been recovered, it is important to verify whether it has been manipulated during the period of time that it was lost.
 - If there is no answer in 10 minutes, block and wipe the device completely.

◆◆◆ Rooting

Incident



```
function(b, c) {
  = a(c.form.querySelectorAll('input[type=checkbox][name="' + b.el.name + "']"));
  == d.index(b.el)) {
    ar e = d.filter(":checked").length;
    return e >= b.arg || g.minChecked.replace("{count}", b.arg)
  }

d: function(a) {
  a null != a.val ? a.val.length <= a.arg || g.maxSelected.replace("{count}", a.arg) : void 0

d: function(a) {
  a null != a.val && a.val.length >= a.arg || g.minSelected.replace("{count}", a.arg)

function(b) {
  = a(this.form.querySelectorAll('input[type=radio][name="' + b.name + "']").filter(":checked"));
  1 == c

function(a, b) {
  = b.options.custom[a.arg],
  = new RegExp(c.pattern);
  d.test(a.val) || c.errorMessage

function(a) {
  ce = a.arg

{
  !1, this.options = a.extend(!0, {}, b, c), this.form = b, this.elr = {}, this.elr = {}
}
```

- The user tries to perform the root or jailbreak of the device without the consent of the organisation.
- Such type of incident generally requires the execution of an exploit that is used to execute a process with administrator permissions on the device.
- Once the administrator permissions have been obtained, the rooting kit generally installs a set of utilities and tools that are required to install unsigned applications with administrator permissions.
 - In the case of iOS, generally, it can be installed via Cydia.
 - In the case of Android, it can be generally installed with SuperSU.

Preventive Measures

- In order to avoid the execution of the rooting exploit via third parties' applications, the following actions will be required:
 - Forbid the installation of applications from unauthorised sources.
 - Eliminate the applications store of the device.
 - Only allow the installation of applications that are included in the list of allowed applications.
- In addition, the MDM solution should include options to detect the rooting or jailbreak via two different methods:
 - Detection of common tools in environments with jailbreak/rooting such as Cydia or SuperSU.
 - Detection of specific characteristics of rooted devices:
 - System file permissions.
 - Existence of the required certificates to execute updates.
 - Verify the permissions of the user responsible for executing processes.
 - Try to request permissions to the administrator.

Measures in Case of Incident

- In case that an attempt of rooting or jailbroken is detected, the security of all data existing in the device may be compromised.
- Processes with administrator permissions may deactivate the MDM solution; therefore, the user may lose control over the system if we do not act quickly.
- Thus, when such procedure is detected, it is important to perform a device wipe.
- In addition, it is possible to notify the user the reason for the device wipe, via an email.

◆◆◆ Disconnection of the MDM Solution

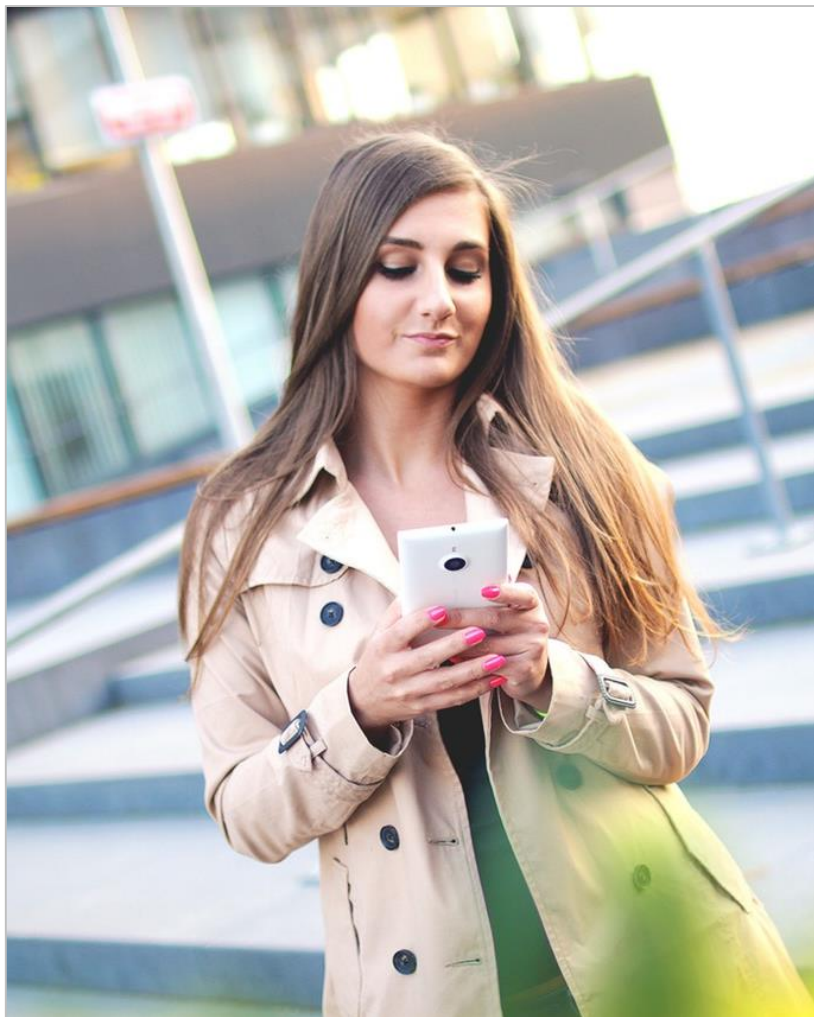
Incident



- The user disconnects the device from the MDM solution.
- Some MDM solutions allow the user to deactivate the connection with the MDM solution.
- Such type of behaviour is allowed in most devices that belong to a user, but they become part of the organisation's infrastructure via a Bring Your Own Device (BYOD) policy.

◆◆◆ Disconnection of the MDM Solution

Preventive Measures



- In order to avoid such kind of incident, it is important to use a security policy to restrict the possibility of making changes in the configuration of the device through its menus.
- Such devices that are not owned by the organisation cannot restrict that option.

◆◆◆ Disconnection of the MDM Solution

Measures in Case of Incident

- In case that an employee wishes to disconnect a device from the MDM solution.
 - If the operative system allows it, send a confirmation message to the user and warn him/her on the consequences of the procedure to perform.
 - If the user decides to deactivate the MDM solution, the process below should be followed:
 - The user should be sent a mail pointing the moment and the disconnected device.
 - An alert is created in the MDM management system.
 - All the applications and policies established in the device via the MDM service will be removed, including:
 - Applications of the organisation.
 - Credentials and configuration to access the organisation's networks.
 - Root certificates installed by the MDM solution.

A close-up, shallow depth-of-field photograph of a person's hands. The left hand holds a silver smartphone, with the thumb positioned over the screen. The right hand holds a white disposable coffee cup with a black lid. The background is blurred, showing warm, bokeh light spots. A semi-transparent blue rectangular box is overlaid across the middle of the image, containing white text.

Bring Your Own Device Policies

◆◆◆ Bring Your Own Device

Introduction

- Bring Your Own Device policies allow employees of an organisation to use their own devices for the performance of tasks related to the organisation without compromising its security.
- BYOD differs from other models in which the employee uses a device that belongs to the organisation to perform business tasks.
- The implementation of BYOD policies allows to reduce costs in the acquisition of devices and to increase the satisfaction of the employee, since they only have to use one device.
- The challenge when defining BYOD policies lies in the shared management of the device:
 - The users should be able to manage their personal information and applications without posing risks for data of the organisation.
 - The organisation should be able to manage its information and applications without interfering in the user's applications.

◆◆◆ Bring Your Own Device

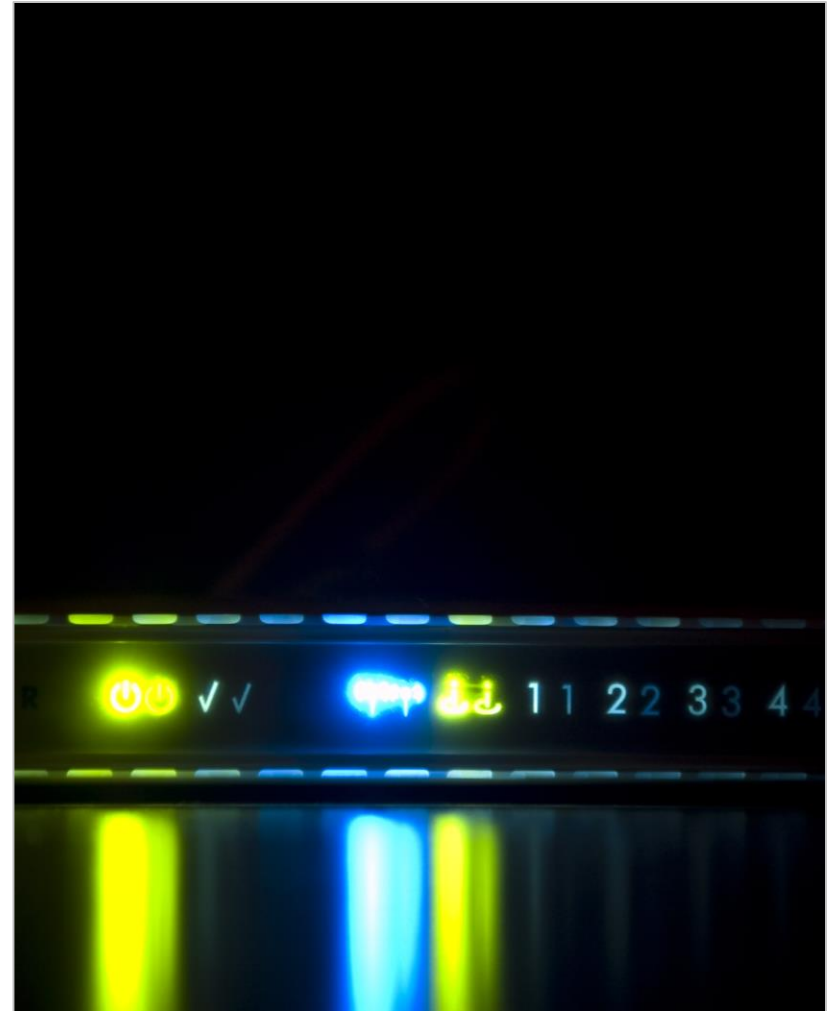
BYOD and MDM solutions

- In general, all the MDM solutions allow the management of devices via specific measures of BYOD.
- To this end, the solutions distinguish between two types of devices:
 - Belonging to the organisation: it includes devices that are managed by the organisation during their all life cycle. The company controls such devices all the time.
 - Belonging to the employee: it includes devices managed by the employee, but are used to perform tasks related to the organisation. The period of time that they are part of the organisation is limited.
- Due to the nature of the devices themselves, the policies that may be applied in each case are different.
 - The company may force the remote wipe of a device belonging to the company, but it cannot do that with an employee's device.
 - However, the company may force an employee to configure an access password with a minimal of complexity to unlock the device

◆◆◆ Bring Your Own Device

BYOD in Mobile Operative Systems

- Mobile operative systems provide a set of specific characteristics aimed at being used in BYOD environments.
- In many cases, the configuration options and policies available for BYOD policies are a subset of policies available for the devices belonging to the organisation.
- The success of the implementation of each operative system in a BYOD environment depends on the ability to balance security of data related to the organisation and the control by the user.
- The main characteristics of the operative system regarding their use in BYOD environments will be presented later.



Containers

- Due to Android's philosophy it enables the communication between applications in different ways such as Intents and Content Providers.
- Such type of philosophy directly disagrees with the separation requirements needed in BYOD policies; therefore, it is necessary to use additional mechanisms to adapt the system to the BYOD.
- Since Android is an open source operative system, the different providers may implement their own system.
- Until date, the two main alternatives are Samsung Knox and Android for Work, both are based on the creation of containers to separate the business and the personal environments.

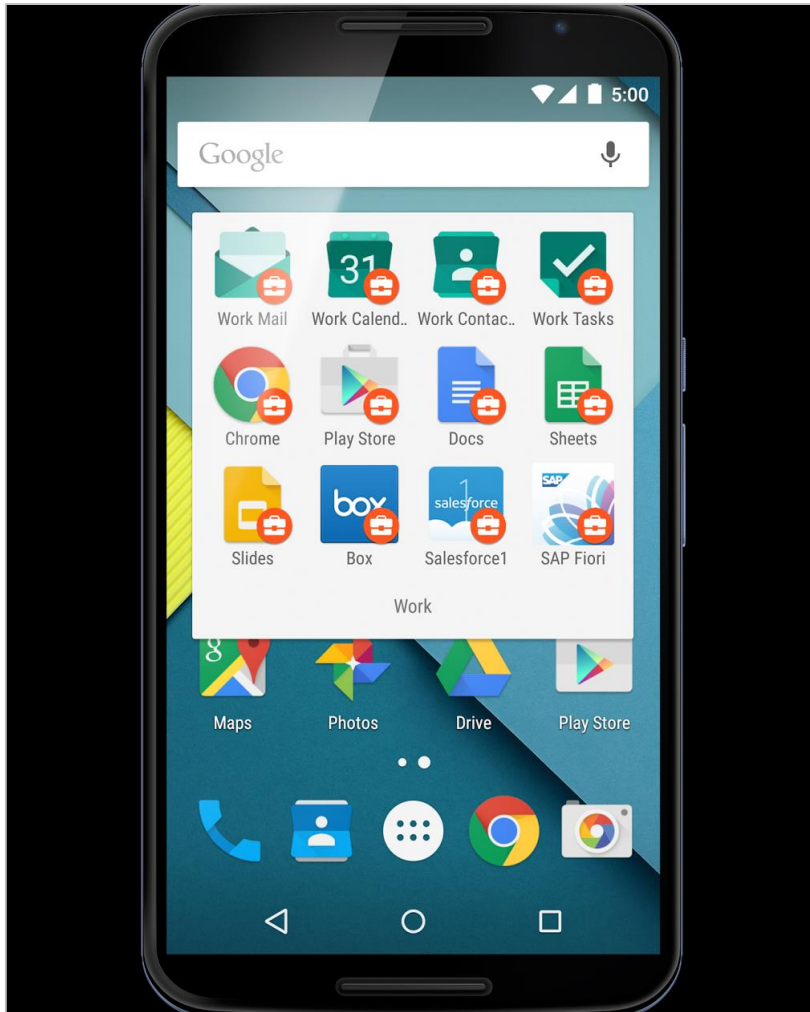
Android for Work

- Android for work is available in all Android versions provided by Google from version 5.0.
- Android for Work uses the concept of user implemented in Android 4.2.
- On Android, each user has an own space for data, a specific configuration of the device and a user interface that enables the switch of users. Android allows the execution of applications for a user while the other user's applications are in the background.
- Android defines of two types of users:
 - Main user: it is the first user added to the device. It has total control over it and is always in execution, at least, in the background.
 - Secondary user: any user added after the main one. They may have their own work space and is isolated from the rest of users, but its elimination does not affect the rest. Such users may have a specific configuration for the device.

Android for Work

- In order to implement BYOD, Android for Work creates a secondary user called “Work Profile” that enables the separation of data of the organisation and the user.
- In order to improve the workflow, the Work Profile is associated to the main user of the device, so that the notifications and other details are displayed in the home screen.
- Android for Work uses a specific Device Administrator for the “Work Profile”, called “Profile owner”. It enables the definition of specific security policies and configuration for the work space of the device that does not affect the rest of policies of the phone.
- Android forbids by default the sending of Intents from a user to another, even though it is possible to define exceptions in the Personal sense → Work.
- If the owner of the device wants to disconnect from the organisation, it is necessary to eliminate the secondary user and thus, eliminate all the information of the organisation in that space.

Android for Work



- Apart from the separation of work environments, Android for Work enables:
 - Automatic deployment of applications to the user's work environment.
 - Restriction in applications that may be installed in the user's work environment.
 - Implementation of encryption by default and use of TPM, hardware in the work container.
 - Creation of specific VPN networks for each application.
 - Managing of the configuration of applications installed in the work environment.
 - The use of a set of manageable applications specifically developed by Google that may coexist with similar applications for personal use: Chrome, calendar, email, tasks, PDF reader, etc.

Containers

- The original architecture of iOS limits the possible communication between applications within the system to a limited set of interactions.
- iOS provides the possibility of managing each of such interactions on BYOD environments, eliminating, thus, the need for separated containers.
 - Restriction of the use of AirDrop or devices it may communicate with.
 - Deactivation of screenshots and screen recording.
 - Management of applications that the device may install.
 - Management and limitation of configurable accounts.
 - Management and configuration of functionalities such as “Open in”, “Share”, and “Edit” that allow users to open documents on other applications.
 - Management of restriction and configuration of “Document Providers” that provide access to storage services on the cloud.
 - Management of installable keyboards and widgets.
 - VPN connections by application in order to separate data transmitted.

Configuration

- For a device to be managed by BYOD policies on iOS, the owner of the device should confirm (“opt-in”) the entrance of the device within the BYOD policy:
 - Through the acceptance of a configuration profile.
 - Through the configuration of an Exchange account with policies.
- Once managed by the organisation, the device may receive through the internet:
 - Updates of the system’s policies and configuration.
 - Applications, extensions of applications, books, and updates of the organisation.
 - Accounts to access resources of the application.
 - Request for the specific removal of applications.
- The device is also able to access services such as Wi-Fi, email and calendars that the organisation provides.

Disconnection

- On iOS, the user has always control over the adhesion of the device to the BYOD policies of the organisation.
- The user may, at any moment, decide to uninstall the configuration profile or deactivate the Exchange account to take the device out of the organisation's control.
- In such case, all the applications, accounts, etc. that have been configured through the configuration profile are eliminated.
- The use of Exchange accounts should be performed with extreme caution. One of the policies provided by Exchange is the option to perform a remote wipe of the device.
- Such type of policies may be activated, for example, when the employee leaves the organisation.
- When the contractual relationship has ended, it is advisable to eliminate both the exchange account and the configuration profile of the device.

Registration

- Windows 10 differs the belonging of the devices according to the account configured for the main user:
 - If the main user's account is a normal Microsoft account, it is considered as a personal device.
 - If it is an Azure Active Directory account, the device is considered as a corporate one and may be totally managed.
- In order to register a personal device, the user should perform a registration process ("opt-in").
- To this end, the user registers the corporate identity (Azure Active Directory account) in the MDM solution through the device.
- According to [Microsoft](#), the management functionalities for personal devices may be limited in the future.

Controls

- The MDM solution may implement the following controls on a personal registered device:
 - Creation of email accounts.
 - Passwords and configuration of the automatic lock.
 - Restrictions of the device's hardware.
 - Remote installation of certificates.
 - Connection to Wi-Fi and telephony networks.
 - Configuration of proxies and VPN.
 - Configuration of functionalities of the system (Cortana, Copy and paste, screen recording and screenshots, etc.).
 - Activation of the device's encryption and restriction or encryption of SD cards.
 - Remote installation of applications.
- MDM systems that include a personal device cannot control Microsoft accounts used by the device.

Disconnection



- On personal devices, the user may disconnect from the MDM solution at any time.
- Windows 10 allows the disconnection of personal devices without needing to perform a complete wiping of the system.
- Specifically, the disconnection without complete wiping eliminates the following information of the device:
 - Corporate mail accounts.
 - Certificates issued by the MDM solution.
 - Connection profiles to Wi-Fi and telephony networks.
 - Applications installed through the MDM solution.
 - All the data that the applications installed through the MDM solution have created.

BlackBerry Balance

- BlackBerry allows the implementation of BYOD policies through the BlackBerry Balance service.
- BlackBerry Balance enables the creation of a specific space for the work space.
- The work space is completely isolated from the personal space of the device, except for the presentation of notifications that is performed in the same place for the commodity of the user.
- The applications from the work space cannot communicate through any mean with the applications from the personal space.
- The use of BlackBerry Balance requires an MDM solution in which the device should be registered.
- The registry should be performed by an administrator through the console of the MDM solution, but the final user should confirm it.
- Once registered, the work space is automatically created.

◆◆◆ BYOD on BlackBerry

Applications

- On a device with BlackBerry Balance, the personal space is used by default for:
 - Applications downloaded from the BlackBerry application store (including the ones compatible with Android).
 - Phone and SMS messages.
- The following applications only exist in the work space:
 - BlackBerry Enterprise IM, BlackBerry Work Drives, specific application store for the work space by BlackBerry.
- The following applications exist in both work spaces and show shared information of both spaces:
 - Calendar, contacts, BlackBerry Hub, (notifications), reminders...
- The following applications exist on both spaces but access to the information corresponding to the space in which the are being executed:
 - Maps, Files, Documents on the Go, Browser, Camera, Adobe Reader...

Controls

- BlackBerry Balance allows users to implement the following controls:
 - Configuration of the password to access the device.
 - Configuration of an additional password to access the work space.
 - Configuration of the different applications existing in the work space.
 - Restriction of the clipboard from the work space to the personal space (it is not allowed in the opposite direction).
 - Applications available on the specific store of the work space.
 - Hardware, device, and applications restrictions while the device is at the work space.
- If the device detects that any security policy is not being complied, the work space is quarantined.
- No data of the work place, nor data shared with applications of the system may be accessed in quarantine.
- Data of the work space may be removed while it is quarantined.

Transition between the Personal and the Work Space

- The transition between the personal and the work space may be performed in two different ways:
 - From the home screen through a contextual menu that appears when sliding down the upper part of the screen.
 - From any application that allows the use of data in both spaces. In such case, it is necessary to change the space from the options of the application. The change of space from an application implies the execution of a copy of the application, but only with access to the selected space. At no moment there is a process with access to both spaces.
- By default, the work and personal spaces have the same aspect, therefore, it is advisable to configure different wallpapers for each space.

Elimination of the Work Space

- On BlackBerry, in order to disconnect a personal device from the control of the organisation, it is only necessary to eliminate the work space from the device.
- This action may be performed through the settings menu of the device itself.
- The elimination of the work space implies the elimination of all the applications and data stored in the work space.
- It does not affect applications that may also be used in the personal space, even though they will not allow the option of having access to their version on the work space.
- According to the configuration of the MDM solution, the connection to BlackBerry Balance allows the administrator to perform a complete wipe of the device.
- In order to avoid the wiping of the personal space of the device, if the user is using a personal device, it is advisable to eliminate the work space in case of termination of the employment relationship



Research Exercise

◆◆◇ Research Exercise

Statement

- In this exercise the student should conduct a research and write the results obtained on the subject's forum, in order to discuss them with the rest of students.
 - The exercise implies the development of a policy regarding the use of corporate and personal mobile devices in a fictitious organisation.
 - The rest of statements are divided into two sections:
 - Contexts: this section of the statement describes different types of fictitious organisations that may need the development of a policy of such type. The student should select one of the contexts to carry out the exercise. The student may develop a new context. In such case, the description of the context should precede the policy developed.
 - Aspects to mention: this section describes the following aspects that should be taken into consideration in the development of the security policy. The student may also add aspects as desired, apart from the ones mentioned in the statement.

◆◆◇ Research Exercise

Context - Hospital

- A system that uses mobile devices to improve the functioning of communications employee-employee and employee-patient is going to be implemented within the hospital.
- The hospital decides to adopt a system for the management of medical information that stores information of the patients in a central server and enables access via different clients, including a mobile application. The hospital aims at implementing an appointment service that enables the integration in the employees' calendars, as well as a consultation via an specific application. The employees of the hospital will also have an internal messaging application in order to receive notifications created by the patient monitor equipment.
- The hospital has 300 employees that are likely to use some of the system's functionalities.
- The hospital is structured into departments and one of them is specifically focused on computer services.

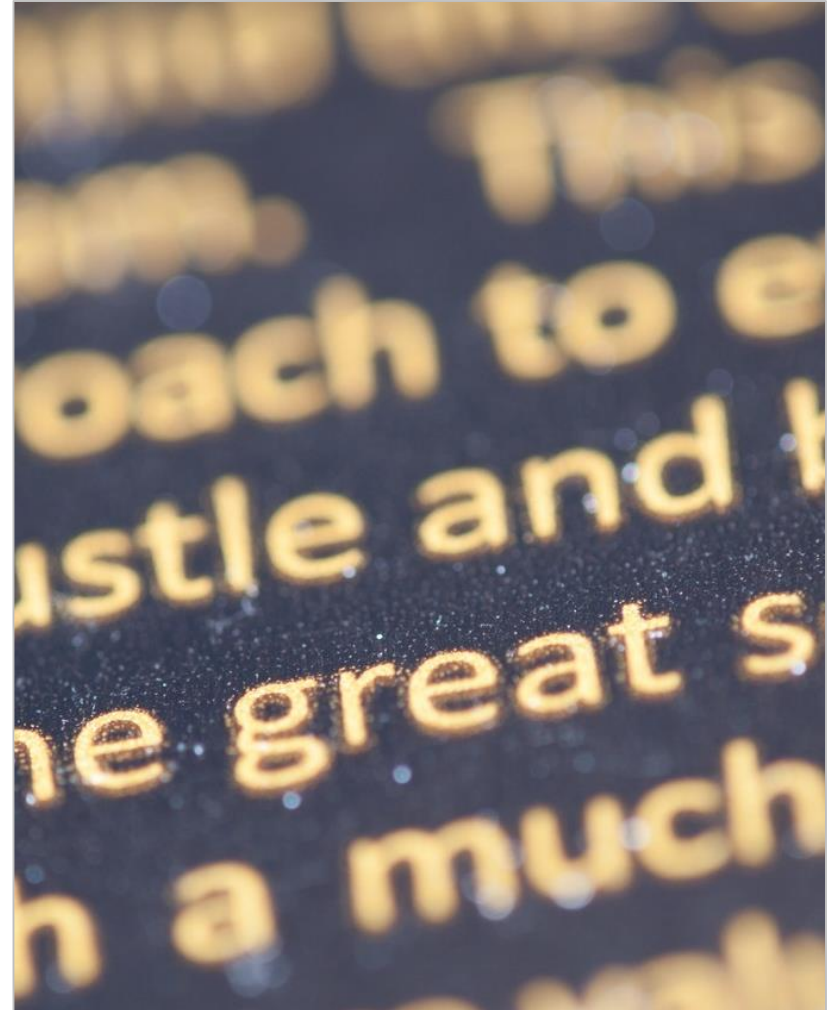
Contexts - University

- The university wants to implement a system that uses mobile devices to improve the communication between the teaching staff and the students.
- The aim is to deploy a system that allows students to access specific applications developed by the university in order to improve the teaching method.
- Professors will be able to load contents to the applications via desktop tools.
- The university also wants to provide a direct messaging system between students and professors that enables the creation of groups according to subjects, the request for tutorials, etc.
- The professors will be able to enter the marks through their mobile devices by using a specific application that is only available for employees of the university.

◆◆◆ Research Exercise

Contexts - University

- The professors should be able to access their email account through the mobile device, even if they are not at the campus.
- The professors' email account may include sensitive information regarding marks or personal data of the students.
- The university has 1,000 employees that are considered as professors, and 15,000 students.
- The university is organised into different faculties. Each faculty has departments that the professors are assigned to.



◆◆◆ Research Exercise

Context – Software Development Company

- The aim is to control the use of mobile devices used in a software development company.
- Currently, the mobile devices are used to:
 - Verify the functioning of mobile applications during the development process.
 - Establish communications between employees of the company through the corporate email and instant messaging.
 - Access source code files and other data stored by the company in a dedicated server controlled by it.
- The company has 50 employees in different departments. Two of them are in charge of computer equipment management.

◆◆◆ Research Exercise

Context – Event Planning Company

- An event planning company uses a set of mobile devices in order to validate tickets for certain types of events.
- The devices require a mobile application to manage tickets during the event.
- Such devices use the telephone network in order to send and receive data from the validation server during the event.
- In case of overload or lack of coverage, the devices should be able to use a specific Wi-Fi connection for the transmission of data.
- The devices enable the acquisition of tickets at that moment, through a credit card reader that is connected via Bluetooth.
- The company has 300 employees and 100 devices to be used during the events.

Aspects to Consider

- In order to develop the security policy, the following tasks should be performed:
 - Analyse the risk that the use of mobile devices may pose in the different described contexts.
 - Study the different types of current MDM solutions deployment and providers, and select the type that fits better the considerations of the specific context.
 - Design the procedure to connect and disconnect the devices from the organisation; both if the devices belong to the organisation and to the employees.
 - Specify the security policies for each roles or groups of the context (in case there are any).
 - Specify actions to carry out in order to mitigate the main risks in the event of detecting the violation of any security policy.

Security Policies

- In order to define the security policies, the following aspects should be taken into consideration:
 - Types of devices accepted by the policy.
 - Functionalities and controls that prevent the leakage of data.
 - Monitoring capability and search of devices according to different parameters.
 - Separation of the personal and corporate spaces.
 - Distribution of applications through business application stores.
 - Possibility of creation of VNP connections and configuration in the network access.
 - Restrictions of the device's capabilities according to the context.

A hand holding a pen is writing on a notebook. In the foreground, a black calculator is placed on the notebook. A semi-transparent blue rectangle is overlaid on the image, containing the text "Assessment test".

Assessment test

Thank you for your
attention

