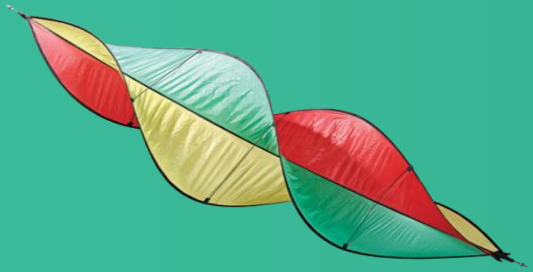
KU LEUVEN

TECHNOLOGIECAMPUS GENT



# Integrating Mobile Devices in Industrial Environments

Jan Vossaert
Jan.Vossaert@cs.kuleuven.be
MSEC

Veilige Industriële Netwerken
UG 28/04/2016

# Introduction

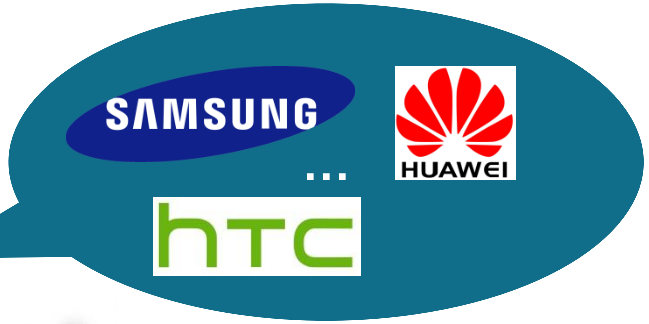
***Is the security of mobile devices adequate to be used in ICS environments?***

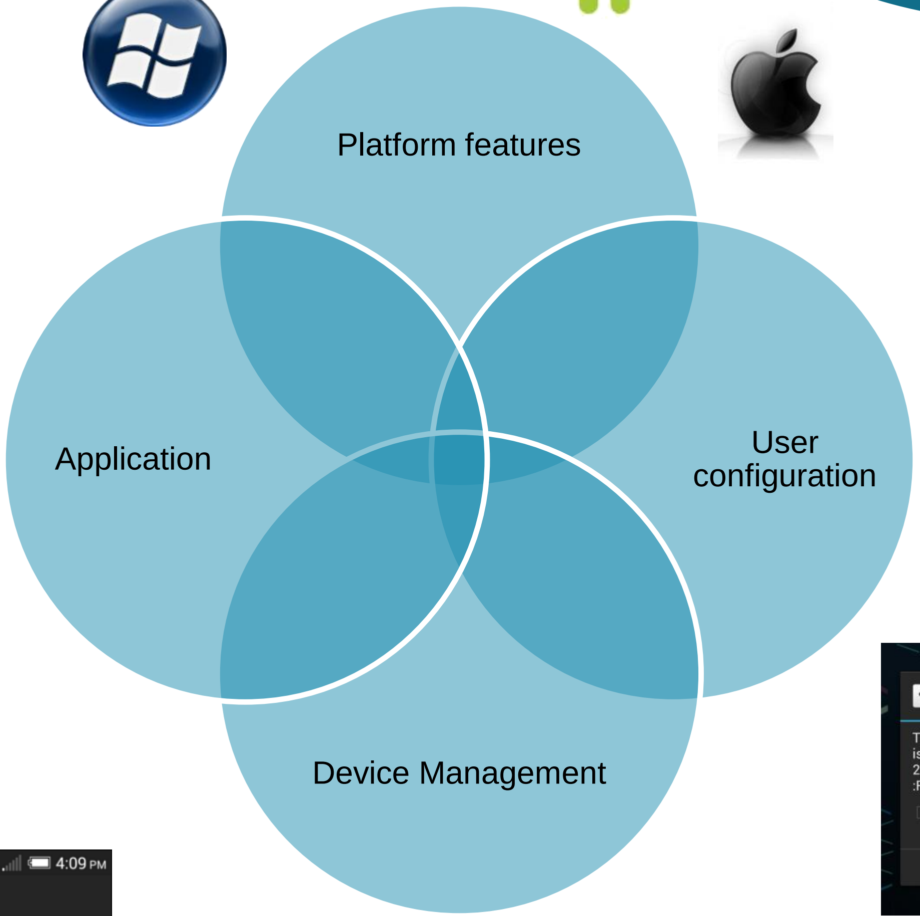
- This presentation:
  - Security features in mobile devices
  - Corporate security in mobile devices

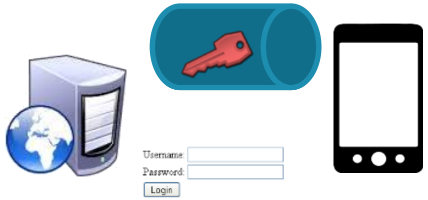
- Next GC:
  - Integration with production environments
    - Cloud
    - Mobile devices in the OT network
  - Overview existing solutions

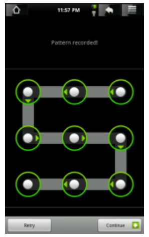
  - Focus on Apps

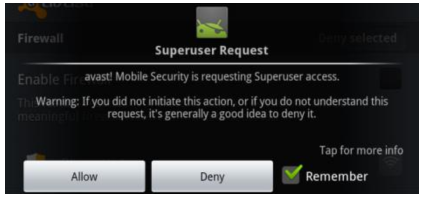
# Security in mobile platforms











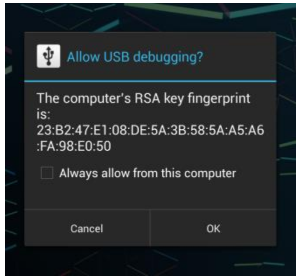
Superuser Request

avast! Mobile Security is requesting Superuser access.

Warning: If you did not initiate this action, or if you do not understand this request, it's generally a good idea to deny it.

Tap for more info

Allow | Deny | ☑ Remember

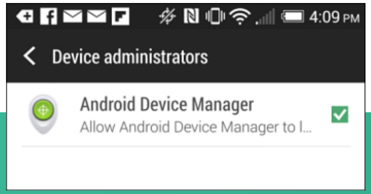


Allow USB debugging?

The computer's RSA key fingerprint is:
23:B2:47:E1:08:DE:5A:3B:58:5A:A5:A6:FA:98:E0:50

□ Always allow from this computer

Cancel | OK



4:09 PM

Device administrators

Android Device Manager
Allow Android Device Manager to l... ☑

Corporate policies complement user configuration

# Android and iOS

## Android

- Huge diversity
  - Broad price/quality range
  - Many different Android versions
  - Android internals!
  - Software update policy

## iOS

- Limited diversity

KU LEUVEN

# Android and iOS

### Android

- Huge diversity
- OS provider ≠ platform provider
    - Nexus range

### iOS

- Limited diversity
- OS provider = platform provider
    - Security philosophy from HW to App framework

# Android and iOS

**Android**

- Huge diversity
- OS provider ≠ platform provider
- Automated application verification

**iOS**

- Limited diversity
- OS provider = platform provider
- Strict/manual application vetting

# Android and iOS Security

- Out-of-box security in Android and iOS better than in desktop systems
  - Stronger threat model

- Average iOS device security > Average Android device security

- Security generally increases every platform version
  - Visible security enhancements (permission system, HD encryption…)
  - Under the hood security enhancements (ASLR, SELinux, verified boot…)

# Windows Phone

- Windows Phone is still quantité négligable
  - In terms of available apps
  - In terms of market share

- Why choose the Windows Phone platform
  - Main focus is dedicated industrial apps, not consumer apps
  - Integration with Windows platform/management
  - Development with .NET framework

# Security in Mobile Platforms

- Secure/verified boot
- Secure storage
- System updates
- Application security
- Mobile devices in a corporate environment

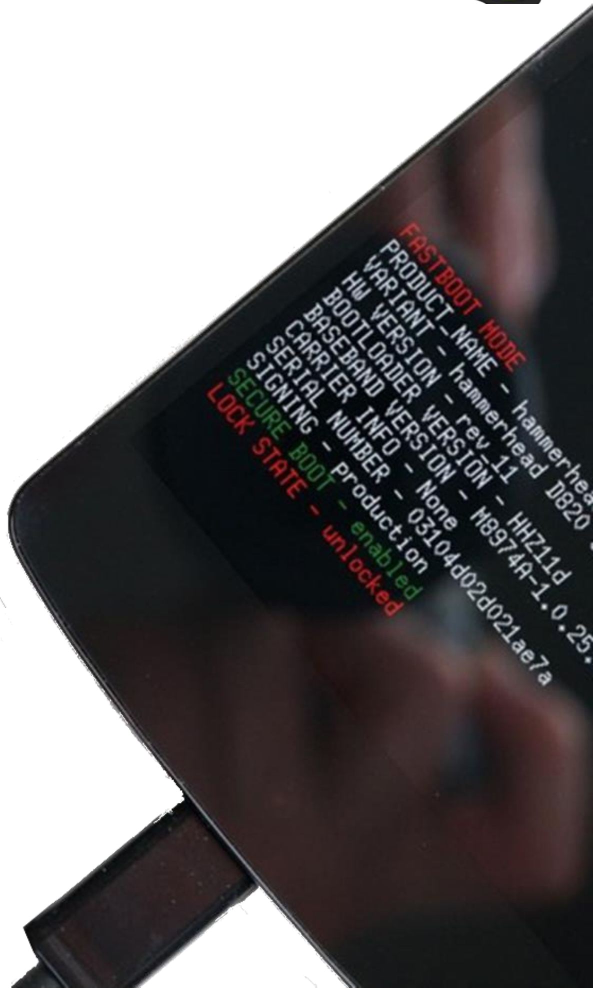
5(+)

# Secure/Verified Boot

- Bootloader
  - Software that starts when device boots
  - Responsible for starting Android

  - **Locked**: prevents flashing device with new ROMs
  - **Unlocked**: possible to flash custom ROMs

  - Unlocking capabilities depends on OEM
    - Samsung ships mostly unlockable
    - HTC supports official unlocking (voids warranty)
    - LG ships unlocked, but no default flashing support
    - Motorola tends to be locked tight (requires exploit)



```
FASTBOOT MODE
PRODUCT_NAME - hammerhea
VARIANT - hammerhead D820
HW VERSION - rev_11
BOOTLOADER VERSION - HHZ11d
BASEBAND VERSION - M8974A-1.0.25.
CARRIER INFO - None
SERIAL NUMBER - 03104d02d021ae7a
SIGNING - production
SECURE BOOT - enabled
LOCK STATE - unlocked
```

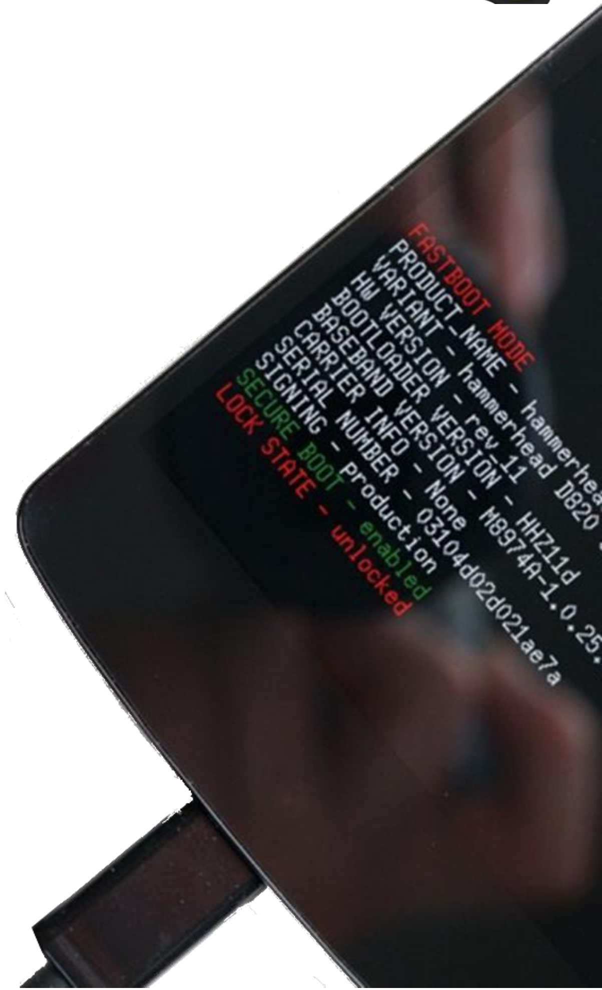
# Secure/Verified Boot

- Bootloader
  - Software that starts when device boots
  - Responsible for starting Android

  - **Locked**: prevents flashing device with new ROMs
  - **Unlocked**: possible to flash custom ROMs

  - Unlocking capabilities depends on OEM

  - Unlocking through OEM provided mechanisms wipes data
    - Privacy protection
    - Pre-full disk encryption era



```
FASTBOOT MODE
PRODUCT_NAME - hammerhea
VARIANT - hammerhead D820
HW VERSION - rev_11
BOOTLOADER VERSION - HHZ11d
BASEBAND VERSION - M8974A-1.0.25.
CARRIER INFO - None
SERIAL NUMBER - 03104d02d021ae7a
SIGNING - production
SECURE BOOT - enabled
LOCK STATE - unlocked
```

# Secure/Verified Boot

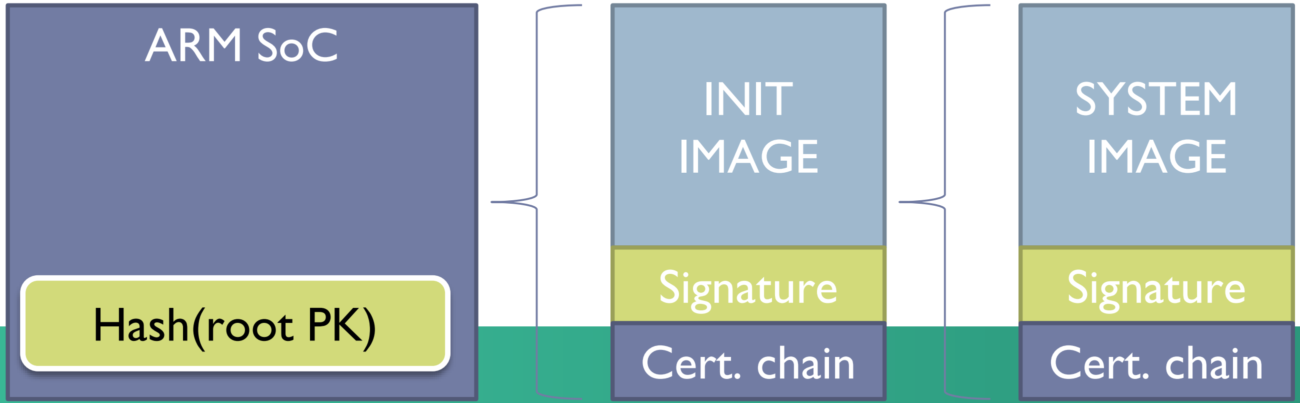
- Locked bootloader < verified boot

- Verified boot ensures the integrity of the device software starting from a **hardware root of trust** up to the system partition

# Secure/Verified Boot

- Locked bootloader < verified boot

- Verified boot ensures the integrity of the device software starting from a **hardware root of trust** up to the system partition
  - A public key is included on the boot partition, verified externally by the OEM
    - Used to verify the signature for that hash
    - Confirm the device's system partition is protected and unchanged
  - During boot, each stage verifies the integrity and authenticity of the next stage

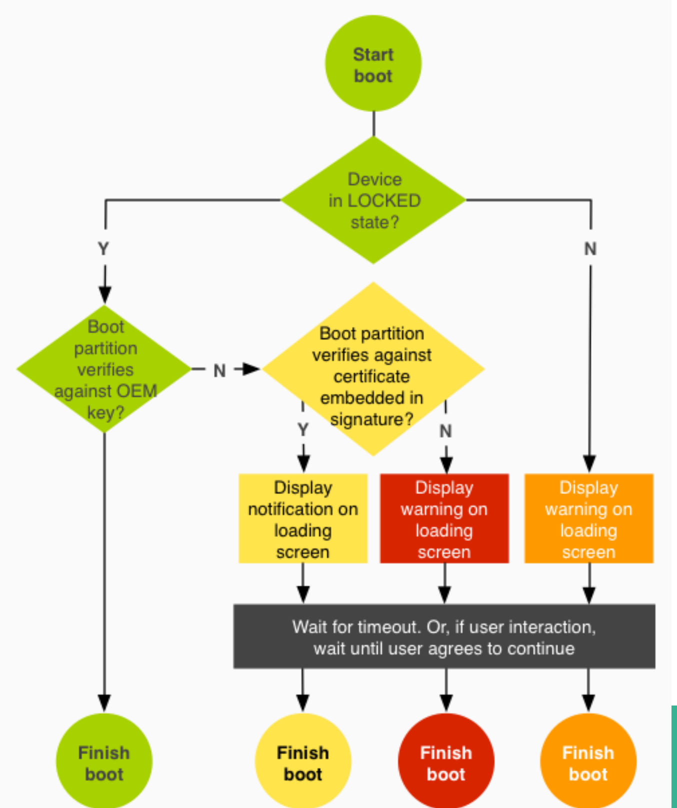


# Secure/Verified Boot

- Locked bootloader **<** verified boot
- Verified boot ensures the integrity of the device software starting from a **hardware root of trust** up to the system partition
- Implemented in Nexus range, other vendors?...
    - Mandatory as of Android 6.0 (Android Compatibility Definition)

# Secure/Verified Boot

- Warn users of unexpected changes to the software
  - Protection for against malicious system software
  - If verification fails, the user is notified and given an option to continue using the device at their own discretion



Start boot

Device in LOCKED state?

Y

N

Boot partition verifies against OEM key?

N

Boot partition verifies against certificate embedded in signature?

Y

N

Display notification on loading screen

Display warning on loading screen

Display warning on loading screen

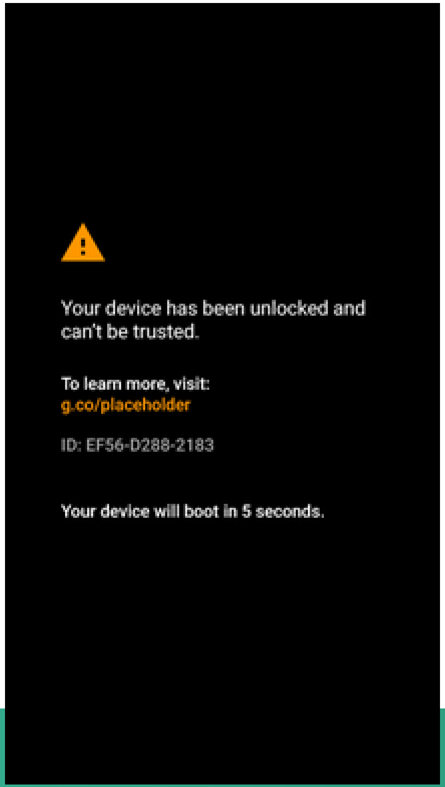
Wait for timeout. Or, if user interaction, wait until user agrees to continue

Finish boot

Finish boot

Finish boot

Finish boot

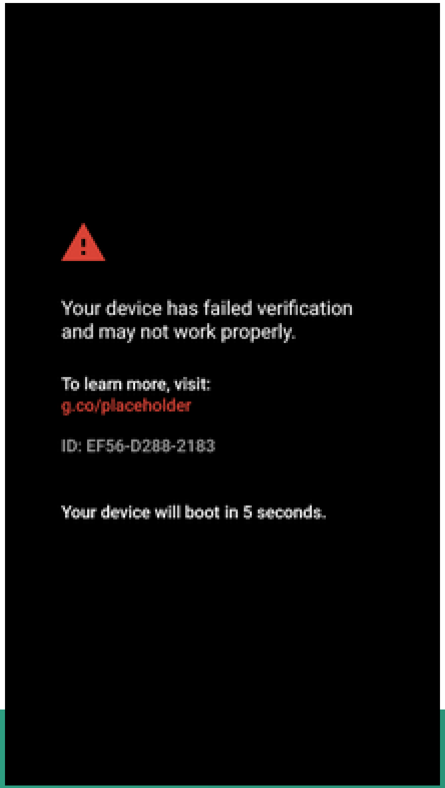


Your device has been unlocked and can't be trusted.

To learn more, visit:
g.co/placeholder

ID: EF56-D288-2183

Your device will boot in 5 seconds.

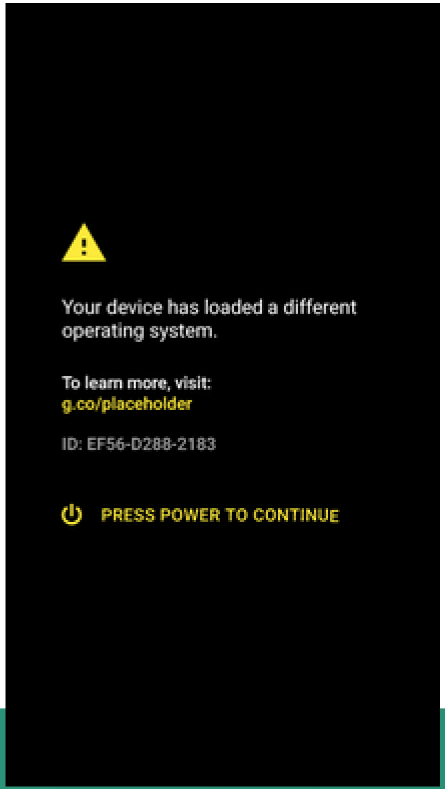


Your device has failed verification and may not work properly.

To learn more, visit:
g.co/placeholder

ID: EF56-D288-2183

Your device will boot in 5 seconds.



Your device has loaded a different operating system.

To learn more, visit:
g.co/placeholder

ID: EF56-D288-2183

⏻ PRESS POWER TO CONTINUE

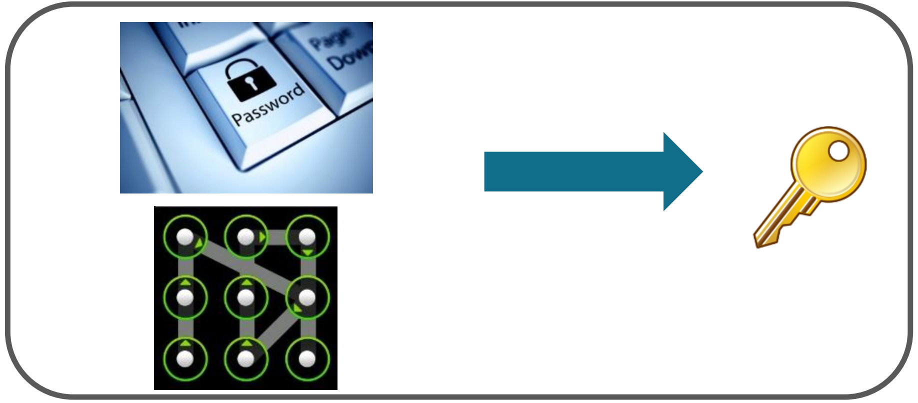
# Secure/Verified Boot

- Secure boot prevents booting custom ROMS (vs Android verified boot)
  - Only software signed by Apple can boot
    - Bootloader
    - Kernel
    - Kernel extensions
    - Baseband firmware

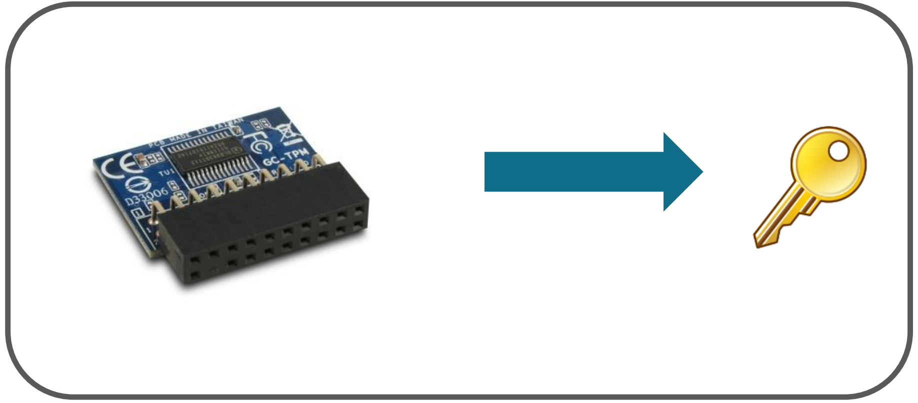
# Secure Storage

- Full disk encryption
  - Encryption key?

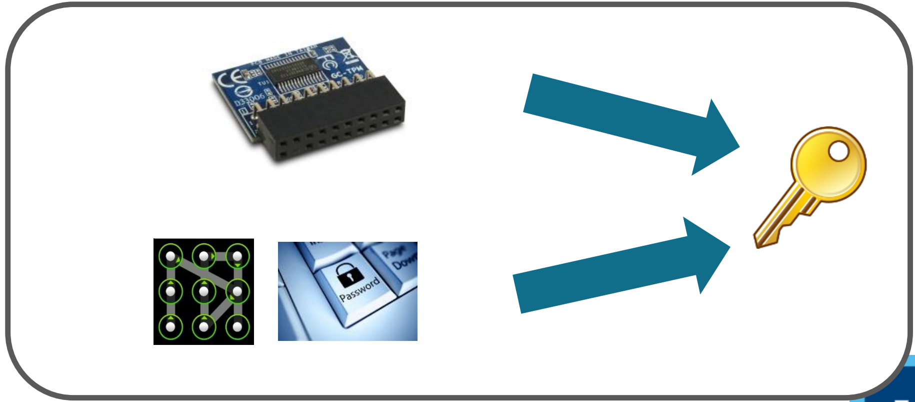
Key derivation function - KDF



Key derivation function - KDF



Key derivation function - KDF



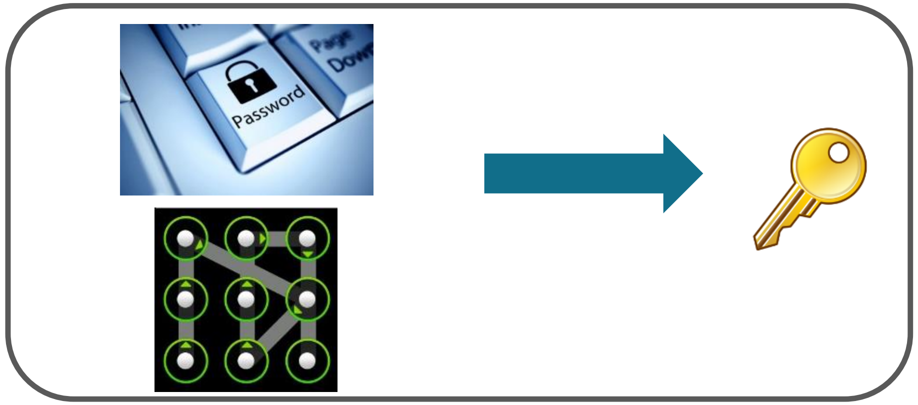
# Secure Storage

- Transparent to application (developer)
- Enabled by default (🤖 5)
- Based on **dm-crypt** in Linux kernel

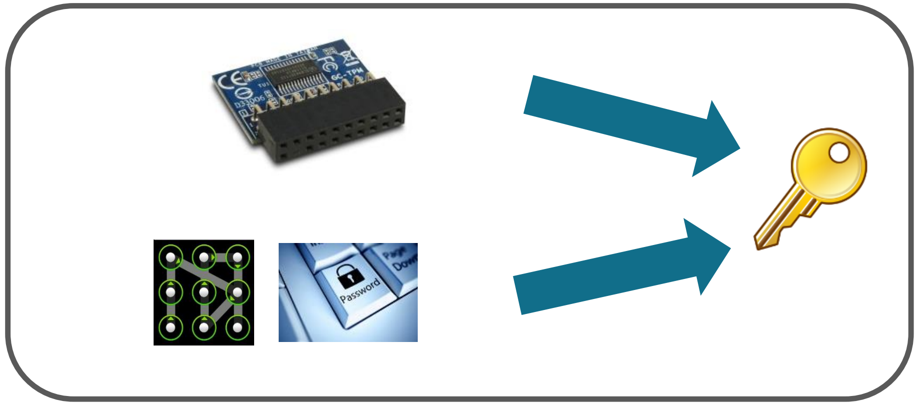
# Secure Storage

- Key derivation
  - Four kinds of encryption states
    - Default, PIN, password, pattern
  - Hardware-backing protection against off-device attacks
    - Hardware-backed encryption is currently *strongly recommended*
    - Planned to change to *required* in next API version

Key derivation function - KDF



Key derivation function - KDF

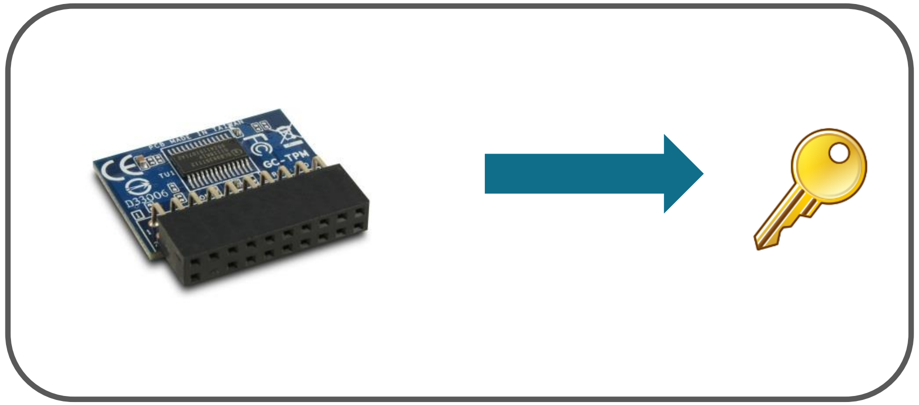


# Secure Storage

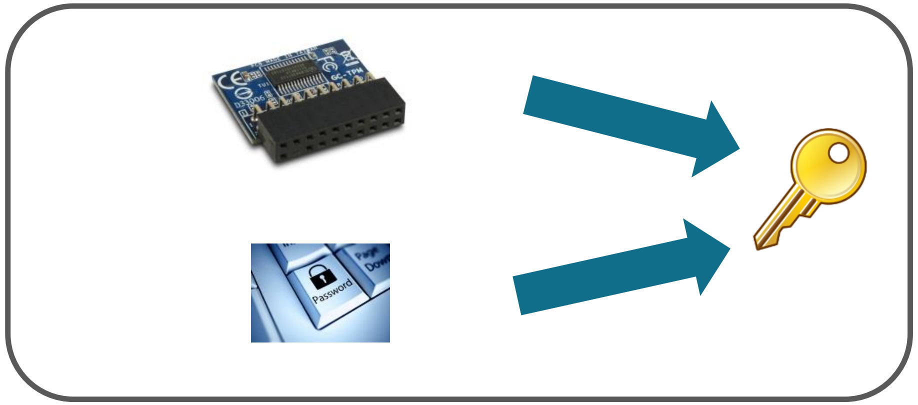
- Full disk encryption
  - Semi-transparent to application developer
    - Data protection classes!
  - Hardware-backed protection against off-device attacks

- Key derived from password/PIN

Key derivation function - KDF



Key derivation function - KDF

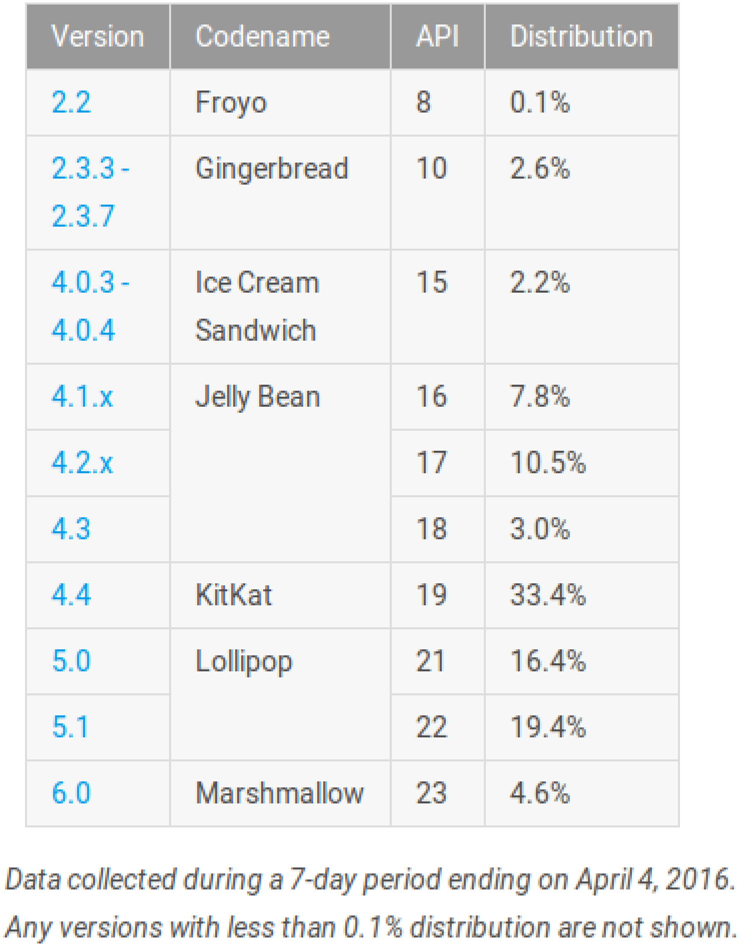


# System Updates

- Android update provisioning depends on three parties
  - Google (developer)
  - OEM (personalization phase 1)
  - Carrier (personalization phase 2)

- Short shelf-life of devices
  - Meaning short support/no updates by OEM/Carrier
  - Situation (very) slowly increasing with (some) OEMs
  - Nexus range gets updates from Google

- Resulting in millions of devices with known vulnerabilities



| Version | Codename | API | Distribution |
|---|---|---|---|
| 2.2 | Froyo | 8 | 0.1% |
| 2.3.3 - 2.3.7 | Gingerbread | 10 | 2.6% |
| 4.0.3 - 4.0.4 | Ice Cream Sandwich | 15 | 2.2% |
| 4.1.x | Jelly Bean | 16 | 7.8% |
| 4.2.x |  | 17 | 10.5% |
| 4.3 |  | 18 | 3.0% |
| 4.4 | KitKat | 19 | 33.4% |
| 5.0 | Lollipop | 21 | 16.4% |
| 5.1 |  | 22 | 19.4% |
| 6.0 | Marshmallow | 23 | 4.6% |

*Data collected during a 7-day period ending on April 4, 2016.*
*Any versions with less than 0.1% distribution are not shown.*

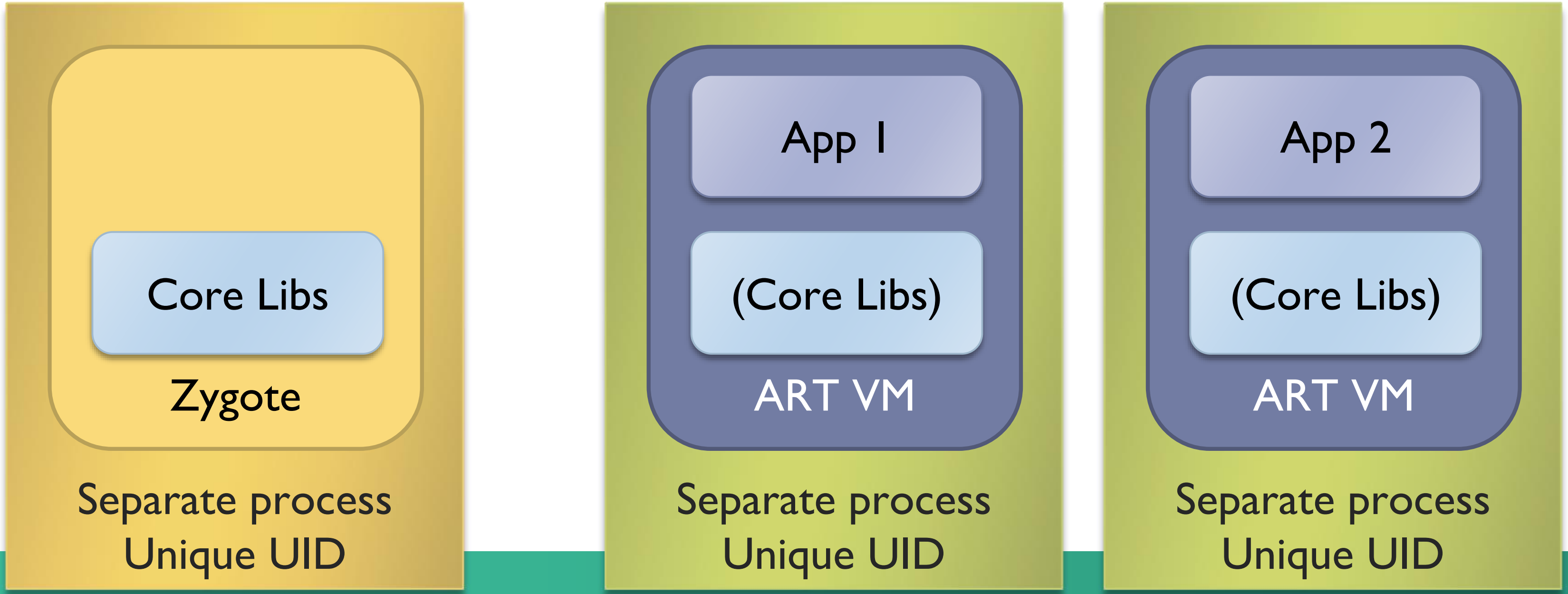
# System Updates

- iOS update provisioning sole responsibility of Apple

- Long-term support (for mobile devices ☺)
  - Depends on device

# Application Security

- Every Android App
  - Runs in its own process
  - Has its own ART VM instance
  - Is assigned a unique Linux user ID
  - Uses Linux file permissions linked to that user ID

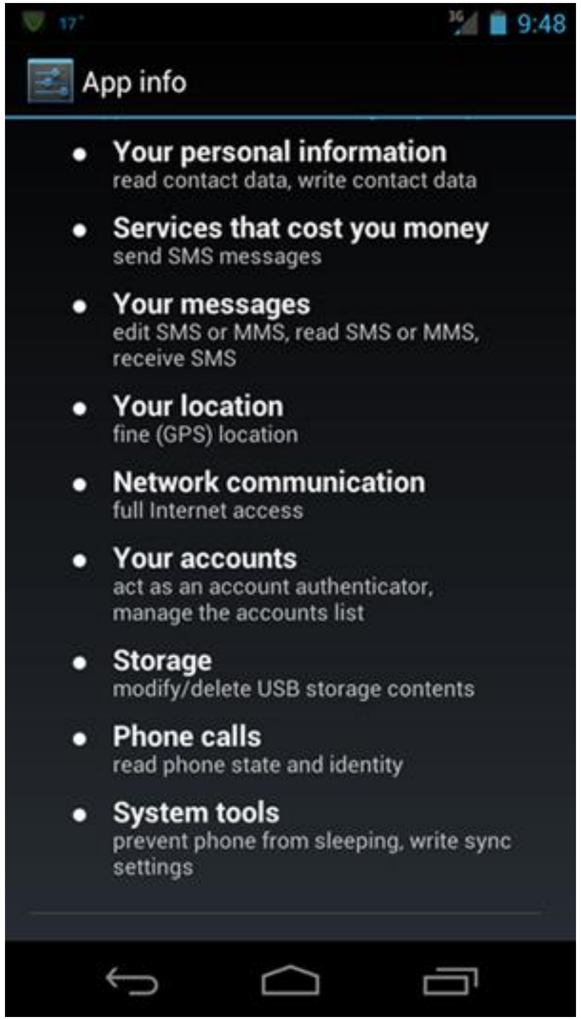


# Application Security

- Access to low-level resources (network, phone calls, SMS, etc.) is enforced through user and group permissions at kernel level
- Higher level permissions restricted by the Android Runtime

- App developers need to specify the required permissions

- 5(-): accept/deny all
- 6(+): users have the option of individually assigning permissions

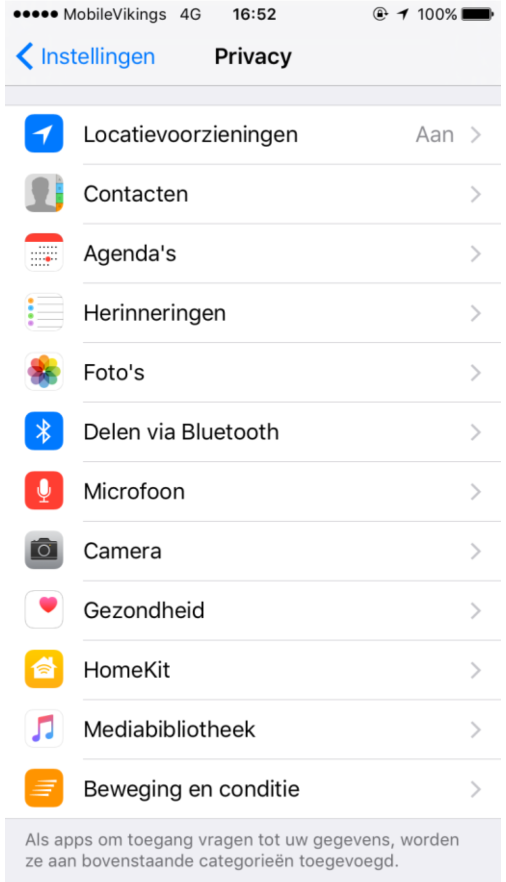


App info

- **Your personal information**
  read contact data, write contact data
- **Services that cost you money**
  send SMS messages
- **Your messages**
  edit SMS or MMS, read SMS or MMS, receive SMS
- **Your location**
  fine (GPS) location
- **Network communication**
  full Internet access
- **Your accounts**
  act as an account authenticator, manage the accounts list
- **Storage**
  modify/delete USB storage contents
- **Phone calls**
  read phone state and identity
- **System tools**
  prevent phone from sleeping, write sync settings

# Application Security

- Application vetting
  - Manual procedure
  - Verification of access to device resources (capabilities)
    - User is requested for specific entitlements at runtime
      - Location service
      - Notifications
    - Entitlements can be revoked by the user



●●●●● MobileVikings 4G 16:52 100%

< Instellingen Privacy

Locatievoorzieningen Aan >

Contacten >

Agenda's >

Herinneringen >

Foto's >

Delen via Bluetooth >

Microfoon >

Camera >

Gezondheid >

HomeKit >

Mediabibliotheek >

Beweging en conditie >

Als apps om toegang vragen tot uw gegevens, worden ze aan bovenstaande categorieën toegevoegd.

# Corporate Features

- Secure remote access via VPN

- Mobile device management

# Corporate Features

- Android supports network security using VPN (IPSec)
  - **Always-on** VPN
  - **Per User** VPN
  - **Per Profile** VPN
  - **Per Application** VPN

- OpenVPN requires VPN application

# Corporate Features

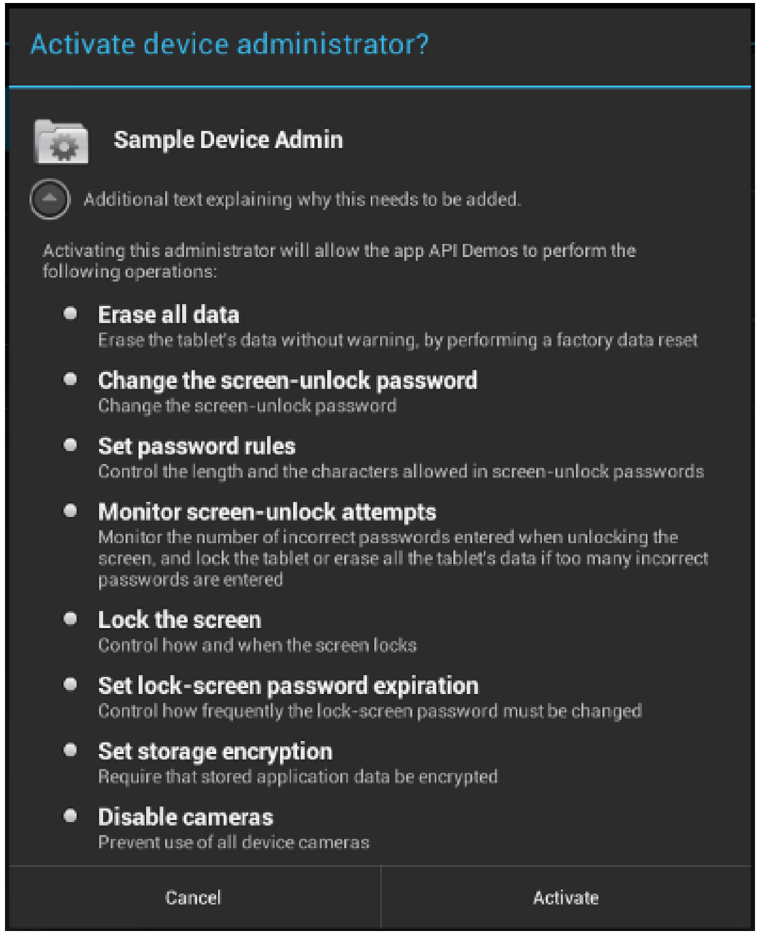
- Android support **Primary** and **Secondary** users
- **Primary user**
  - The first user added to a device
  - Can’t be removed, except by factory reset
  - Has special privileges and settings only set by that user
  - Always running even when other users are in the foreground
- **Secondary user**
  - Any user added to the device other than the Primary user
  - Can be removed by their own doing and by the Primary user
  - Can’t impact other users on a device

# Corporate Features

- Mobile device management
  - ○ Device administration API
    - 4(+)
  - ○ Android for Work
    - 6
    - 4.0 – 5.1.1 for Work compatibility application
    - Especially suited for mixed-use devices

# Corporate Features

- Device administration API
  - ○ Applications can request device admin privileges
  - ○ Policy specification
    - These policies could be hard-coded into the app
    - Dynamically fetch policies from a third-party server



Activate device administrator?

**Sample Device Admin**

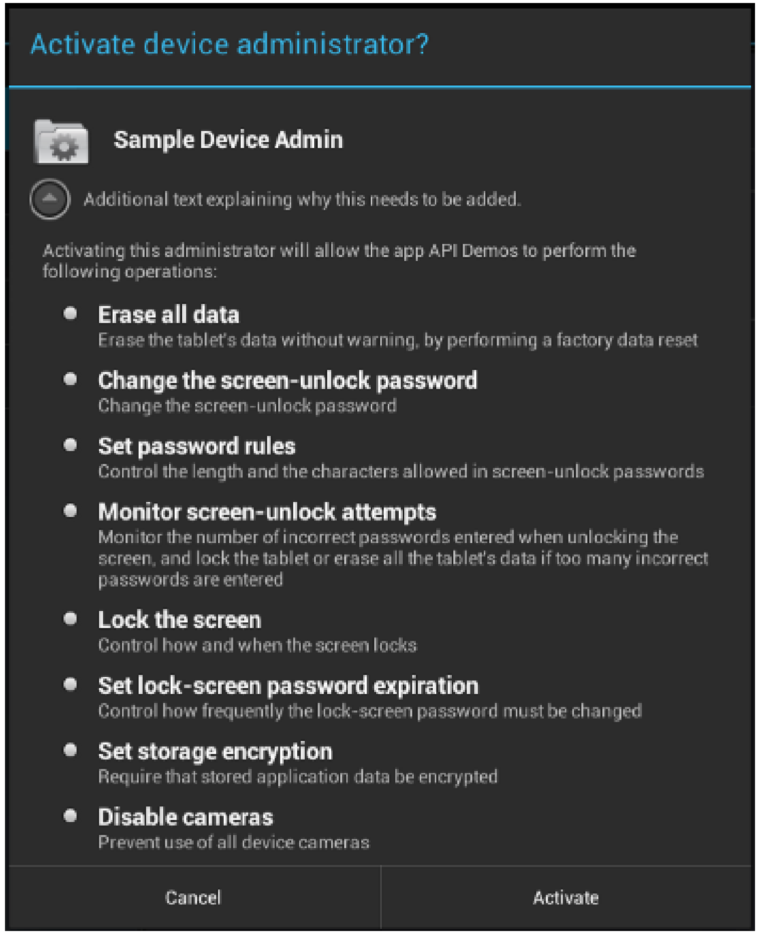
Additional text explaining why this needs to be added.

Activating this administrator will allow the app API Demos to perform the following operations:

- **Erase all data**
  Erase the tablet's data without warning, by performing a factory data reset
- **Change the screen-unlock password**
  Change the screen-unlock password
- **Set password rules**
  Control the length and the characters allowed in screen-unlock passwords
- **Monitor screen-unlock attempts**
  Monitor the number of incorrect passwords entered when unlocking the screen, and lock the tablet or erase all the tablet's data if too many incorrect passwords are entered
- **Lock the screen**
  Control how and when the screen locks
- **Set lock-screen password expiration**
  Control how frequently the lock-screen password must be changed
- **Set storage encryption**
  Require that stored application data be encrypted
- **Disable cameras**
  Prevent use of all device cameras

# Corporate Features

- Device administration API
  - Applications can request device admin privileges
  - Policy specification
  - Policy enforcement
    - If a user fails to comply with the policies it is up to the application to decide how to handle this
    - If a device contains multiple enabled admin applications, the strictest policy is enforced
    - If denied, no application benefits



Activate device administrator?

Sample Device Admin

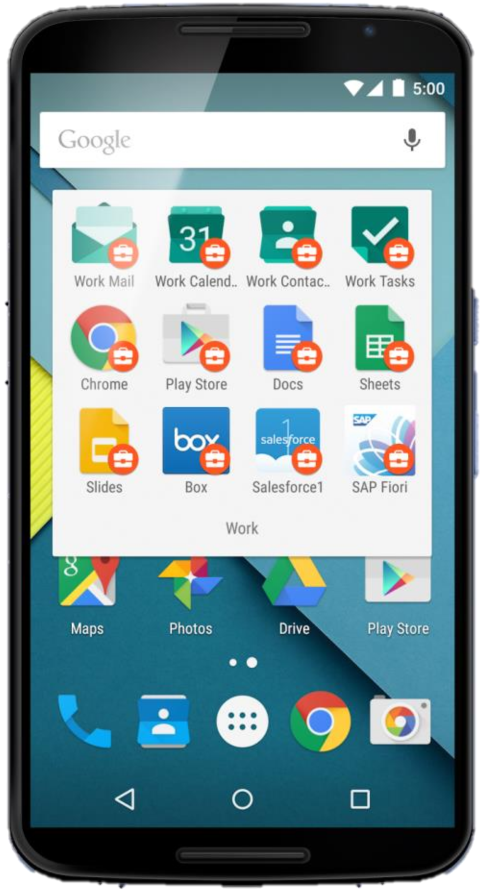
Additional text explaining why this needs to be added.

Activating this administrator will allow the app API Demos to perform the following operations:

- **Erase all data**
  Erase the tablet's data without warning, by performing a factory data reset
- **Change the screen-unlock password**
  Change the screen-unlock password
- **Set password rules**
  Control the length and the characters allowed in screen-unlock passwords
- **Monitor screen-unlock attempts**
  Monitor the number of incorrect passwords entered when unlocking the screen, and lock the tablet or erase all the tablet's data if too many incorrect passwords are entered
- **Lock the screen**
  Control how and when the screen locks
- **Set lock-screen password expiration**
  Control how frequently the lock-screen password must be changed
- **Set storage encryption**
  Require that stored application data be encrypted
- **Disable cameras**
  Prevent use of all device cameras

# Corporate Features

- Android for Work (🤖 6)
  - Program for supporting enterprise use of Android
    - Administrators control work profiles, which are kept separate from personal accounts, apps, and data
    - Allows organizations to manage the business data and applications they care about
    - Leave everything else on a device under the user’s control



KU LEUVEN

# Corporate Features

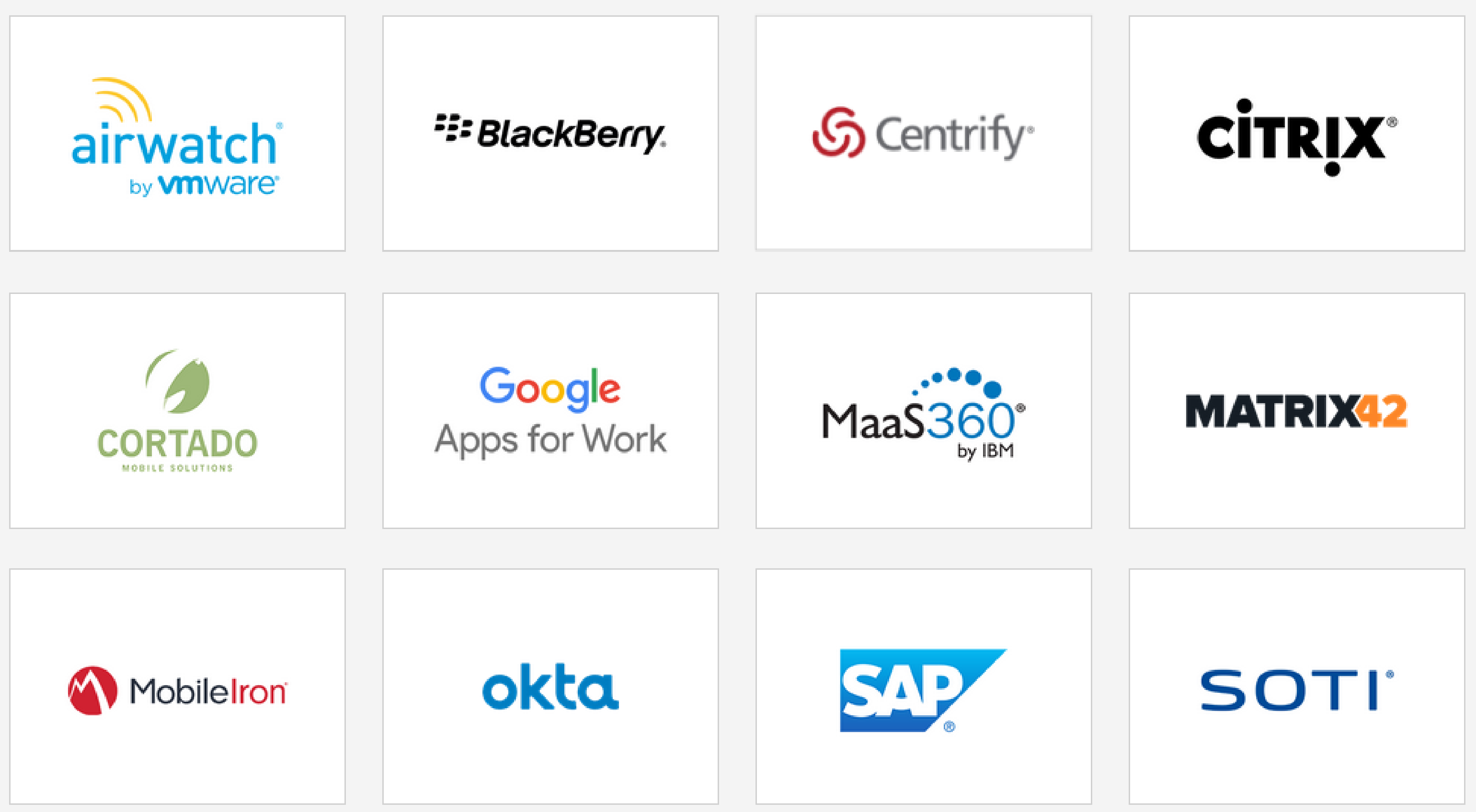
- Android for Work ( 5.0+)
  - Program for supporting enterprise use of Android
  - Android for Work benefits:
    - **Data security**: Business data is separated in a work profile and protected device-wide on work-managed devices. IT can apply data leakage prevention policies
    - **Apps security**: Work apps are deployed through Google Play for Work. IT can prevent installation of apps from unknown sources and apply app configurations
    - **Device security**: Android for Work devices are protected with disk encryption, lockscreen, remote attestation services, and hardware-backed keystore when available

# Corporate Features

- Android for Work (5.0+)
  - Program for supporting enterprise use of Android
  - Delete your work profile in Settings > Accounts > Remove work profile
    - Removal of all apps and data within the work profile
    - Only the device policy controller application and the Android device owner can delete the work profile and data
    - Only the device owner can delete the personal data and perform a factory data reset
  - If a device is owned by your company or organization and configured with a device owner, the device owner can also perform a factory reset

# Corporate Features

- Enterprise mobility management (EMM) solution
  - ○ [https://www.google.com/work/android/partners](https://www.google.com/work/android/partners)



| | | | |
|---|---|---|---|
| airwatch by vmware | BlackBerry | Centrify | CITRIX |
| CORTADO MOBILE SOLUTIONS | Google Apps for Work | MaaS360 by IBM | MATRIX42 |
| MobileIron | okta | SAP | SOTI |

# Corporate Features

- iOS supports network security using VPN (IPSec)
  - IPSec
  - OpenVPN
  - Cisco IPSec
  - …
- Granularity
  - VPN on-demand
  - Per app VPN
  - Always-on VPN

# Corporate Features

- Configuration profiles can be loaded on iOS devices
  - ○ Passcode management
    - Minimum length
    - Maximum passcode age
    - Allow Touch ID
    - …
  - ○ Device restrictions
    - Allow app installs
    - Allow iCloud backup
    - Allow in-app purchases
    - …
  - ○ Configuration management
    - Wi-Fi settings
    - VPN settings
    - Mail server settings
    - LDAP directory service settings
    - Credentials and keys
    - …
  - ○ Enroll devices with MDM server

# Corporate Features

- Mobile device management
  - Allows corporate resources and data to be managed in a way that is secure
  - Enforce settings, monitor corporate compliance, and remove corporate data and apps
  - Leave personal data and apps on each user’s device intact

# Corporate Features

- Mobile device management
  - Managed apps
    - Can be removed remotely by an MDM server or when users remove their own devices from MDM
    - Removing the app also removes the data associated with the app

# Corporate Features

- Mobile device management
  - Managed apps
  - Open In
    - Protects corporate data by controlling which apps and accounts are used to open documents and attachments.
    - Admins can configure a list of apps available in the sharing panel to keep work documents in corporate apps
    - Prevent personal documents from being opened in managed apps.
    - Also applies to third-party document providers and third-party keyboard apps

# Corporate Features

- Mobile device management
    - Managed apps
    - Open In
    - App configuration
        - App developers can identify app settings that can be enabled when installed as a managed app
        - These configuration settings can be installed before or after the managed app is installed

# Corporate Features

- Mobile device management
  - Managed apps
  - Open In
  - App configuration
  - Prevent backup
    - Prevents managed apps from backing up data to iCloud or iTunes
    - Prevents managed app data from being recovered if the app is removed via MDM, but is later reinstalled by the user

# Conclusion

- Future work
  - More information on mobile device management?
  - Existing applications/product for integrating mobile in ICS
  - Other things related to this topic?

- Related projects
  - www.msec.be/secureapps
  - www.msec.be/crossmos