Smartphones in classified environments

Markku Korkiakoski
16.10.2018
Contents

• Paradigm change
• Commercial technology in special domain
• Top threats and mitigations
• Summary
Paradigm change

Enabling the broadband data for special mobile workforce
Handset is more integrated part of the network

Utilization of commercial technology

Wide range of new data applications
Many roles of the device

- Enables new digital services
- Creates flexibility to processes
- Enables real time communication
- Enhanced productivity

Enhanced reliability
Availabilty of information
Usability of devices and services
More efficient use of human resources

RELIABILITY
AVAILABILITY
USABILITY
ECONOMY
Consumer technology in special domains
COTS

System Verification
- Concept verification
- Accessory testing
- Env/Mech testing
- IOP testing
- IOT
- Field testing
- GSM
- WCDMA
- LTE
- BT/WLAN

Pre-Conformance
- Regulatory
  - FCC / IC
  - E911
  - HAC
- Type approval
  - PTCRB
  - CTIA
  - IEEE 1725 (Battery)
  - CTIA OTA
  - WiFi RF perf
- Certifications
  - USB
  - BQP
  - Wifi

Conformance
- Regulatory
  - FCC/IC/R&TTE
  - E911
  - HAC
  - SAR
  - Safety
- Type approval
  - PTCRB
  - CTIA
  - IEEE 1725 (Battery)
  - CTIA OTA
  - WiFi RF perf
- Certifications
  - USB
  - BQP
  - Wifi

Operator testing
- Lab entry criteria
- Regulatory grant
- Type approval done
- Operator pre-testing
- Operator lab testing
- Operator field testing

Change Management

Error Management

Time
eCOTS

System Verification
- Concept verification
- Accessory testing
- Env/Mech testing
- IOP testing
- IDT
- Field testing
- GSM
- WCDMA
- LTE
- BT/WLAN

Pre-Conformance
- Regulatory
- FCC / IC
- E911
- HAC
- Type approval
- PTCRB
- CTIA
- IEEE 1725 (Battery)
- WiFi RF perf
- Certifications
- USB
- BQP
- Wifi

Conformance
- Regulatory
- FCC/IC/R&TTE
- E911
- HAC
- SAR
- Safety
- Type approval
- PTCRB
- CTIA
- IEEE 1725 (Battery)
- CTIA OTA
- WiFi OTA
- WiFi RF perf
- Certifications
- USB
- BQP
- WiFi

Operator testing
- Lab entry criteria
- Regulatory grant
- Type approval done
- Operator pre-testing
- Operator lab testing
- Operator field testing

Additional approvals for targeted domain

Change Management

Error Management

Time
DEPLOYMENT

OS patch

Release

App patch

OS patch

Firmware upgrade

Sec patch

Firmware upgrade

Version Control

RELIABLE SERVICE

R&D

Testing

Approval

Release

App patch

Firmware upgrade

Sec patch

© Bittium 2018 | Public
Top threats and mitigation
# Top threats

<table>
<thead>
<tr>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclosure of information</td>
</tr>
<tr>
<td>An unauthorized use of the device</td>
</tr>
<tr>
<td>Unauthorized physical access into device memory</td>
</tr>
<tr>
<td>Get physical access to the device</td>
</tr>
<tr>
<td>Unauthorized remote access to a device</td>
</tr>
<tr>
<td>Social engineering attacks</td>
</tr>
<tr>
<td>Jailbreaking and rooting of devices</td>
</tr>
<tr>
<td>Denial of service attacks</td>
</tr>
</tbody>
</table>

Source: CCDCOE, Defending mobile devices for high level officials and decision-makers
Intrusions via remote access
Intrusions via remote access

**THREAT**

- Attacks from malicious applications e.g. installed from fraud applications store
- SW based Security vulnerabilities (e.g. in operating system)

**MITIGATION**

- Application permission firewall
- Secure, customized app store
- Secure over-the-air SW update possibility
- Possibility to enforce SW patches
- Up-to-date SW version
Intrusions via remote access

**THREAT**

- Cryptographic keys captured, modified or disclosed to unauthorized individuals
- Intercept IP data calls or messages

**MITIGATION**

- Off-device brute-force attack can be prevented through e.g. TPM utilization
- Kernel-level IPSEC VPN (e.g. Bittium SafeMove)
- Secure VoIP and messaging applications
Intrusions requiring physical access
Intrusions requiring physical access

**THREAT**
- Unauthorized, modified or invalid system SW is injected and booted e.g. via USB
- Attempt to steal data from the mobile device e.g. via USB, SD-card or memory

**MITIGATION**
- Secure Boot
- Integrity checks on both SW and HW
- HW-backed secure memory storage
- TPM-tied encryption
- Strong encryption in mass memory and SD-card
- Remote Device Management (DM) solution
Intrusions requiring physical access

**THREAT**

Attacks against the operating system e.g. replace OS components with own ones or inject malware via USB.

Attacks on the critical system HW components e.g. change or add own components, jump wirings etc.

**MITIGATION**

- Device boot and run-time integrity checks
- File system integrity check

- Tamper detection that destroys user data in case of detected user intrusion.
- Integrity check for HW
SUMMARY

- Solid security policy and framework for E2E solutions
  - How to introduce applications
  - How to introduce devices
- Device management in place
- Remote access for security
- Required security measures in the device

Device is part of overall IT infrastructure
Thank you!