Smartphone Attack Vectors

LOGICAL ATTACKS

COMMUNICATION SERVICES
Even Smartphone services such as e-mail and ActiveSync are potential gateways for attacks via manipulated contents. Contrary to stationary PCs, services such as SMS, MMS or over-the-air-updates are not checked at a company’s perimeter and may hit vulnerable device interfaces unfiltered.

BASEBAND PROCESSOR
Home-brewed base stations are relatively inexpensive. Attackers can modify these devices to carry out attacks against the mobile radio interfaces. Often the goal is to obtain access to the user’s data. Reversal attacks from smartphones against the mobile service providers’ infrastructures are possible as well.

MULTIMEDIA PLAYER
In the past the complexity of processing compressed data streams (MP3, WAV, TIFF, PDF, etc.) has already been the cause for many vulnerabilities. This is an easily overlooked aspect when safeguarding business smartphones, because applications are not the only potential threats.

OPERATING SYSTEM
Besides the general weaknesses that already exist in operating system components, the reduced smartphone surface especially enables attacks against weaknesses of the graphic user interface, for example against the password screen. In addition, apps may circumvent runtime environment restrictions (sandbox) or abuse potential vulnerabilities.

3RD PARTY APPS
Beyond the danger of installing malware on the device, apps also present a threat due to their own inherent vulnerabilities. Past experience with many apps shows that the quality of their protective measures is insufficient, this may also entail that more than their own application data may be affected.

USERS
Often users become accomplices in an attack because they were deceived into carrying out security critical actions.

REMOTE MAINTENANCE
Disabled automatic updates or an insecure configuration may promote attacks just as much as insufficiently protected interfaces to the remote device management.

PHYSICAL ATTACKS

WIRELESS INTERFACES
When an attacker is located in the immediate vicinity of a device, manipulated data can be sent allowing vulnerabilities in radio communication (Bluetooth, NFC, WiFi, etc.) to be taken advantage of in order to obtain user data and passwords illegally.

MEMORY CARDS
Data on external storage media is frequently unprotected. An attacker may be able to read the data directly if a smartphone ends up in his hands. When an attacker is able to store manipulated data on the memory card, the smartphone’s vulnerabilities can be taken advantage of if a manipulated smartphone is hooked up to the company’s PC, the attackers may use it as a host for infections and attack the computer during synchronization and beyond that the overall enterprise network as well.

HARDWARE INTERFACES
An attacker may obtain access to data over memory buses and hardware interfaces (JTAG) or use them to circumvent the protection mechanisms of the user interface.

MEMORY
Manipulating flash memory contents or RAM disks often offers an option to remove protective mechanisms or directly read user data.

FIRMWARE
The firmware integrity represents the basis for many security functions. If a user is unaware that firmware has been manipulated (evil maid attack), the attacker may obtain complete remote control over the smartphone and its data.

USB
Many of the described physical attacks may be carried out by low level access over USB without opening the smartphone itself. Beyond that most smartphones have additional logical interfaces for modem functions and data access, which represent an additional gateway for attacks, for example during unsupervised recharging.

BIZZTRUST FOR ANDROID – TWO SMARTPHONES IN ONE
BizzTrust provides separate use areas on a smartphone, each of which can have its own data records and access authorizations. The device’s private applications (app) to run simultaneously, without limitations and independently from business applications. Moreover, extended remote maintenance protocols allow in the business use area to determine the device status, automatically implement software updates and integrate the device in full into the central event management infrastructure of the company. BizzTrust offers:

- Business data protection
- Unrestricted private use
- Secure communication within the company (anonymity)
- Remote management and updates
- Supports RODI strategy
- Automatic policy enforcement

YOUR SMARTPHONE GONE ASTRAY?
Smartphones are practical tools and have become indispensable for everyday business. Not caring about smartphone security means an immense risk. Financial loss may occur due to the abuse of premium services, for example by malware having been transmitted on unauthorized access to enterprise networks. Fraunhofer SIT supports companies and public authorities in their secure smartphone use. We offer independent security analyses and development support for the implementation of innovative solutions to device manufacturers and software providers. We offer:

- Security analyses (with or without certificate)
- Practical attack tests
- Develop and implement security concepts
- Safeguard mobile devices and resources
- Adapting to and determining secure configurations
- Innovative solutions

LOGICAL ATTACKS

BROWSER
In addition to the usual browser vulnerabilities (Web standards processing), smartphones offer further targets due to the interaction between browser and phone. For example, the user identity connected to the SIM card may be abused.

BASEBAND PROCESSOR
Home-brewed base stations are relatively inexpensive. Attackers can modify these devices to carry out attacks against the mobile radio interfaces. Often the goal is to obtain access to the user’s data. Reversal attacks from smartphones against the mobile service providers’ infrastructures are possible as well.

MULTIMEDIA PLAYER
In the past the complexity of processing compressed data streams (MP3, WAV, TIFF, PDF, etc.) has already been the cause for many vulnerabilities. This is an easily overlooked aspect when safeguarding business smartphones, because applications are not the only potential threats.

OPERATING SYSTEM
Besides the general weaknesses that already exist in operating system components, the reduced smartphone surface especially enables attacks against weaknesses of the graphic user interface, for example against the password screen. In addition, apps may circumvent runtime environment restrictions (sandbox) or abuse potential vulnerabilities.

3RD PARTY APPS
Beyond the danger of installing malware on the device, apps also present a threat due to their own inherent vulnerabilities. Past experience with many apps shows that the quality of their protective measures is insufficient, this may also entail that more than their own application data may be affected.

USERS
Often users become accomplices in an attack because they were deceived into carrying out security critical actions.

REMOTE MAINTENANCE
Disabled automatic updates or an insecure configuration may promote attacks just as much as insufficiently protected interfaces to the remote device management.

FIRMWARE
Even though the SIM card itself is highly secure, attackers may be able to manipulate the communication between the SIM card and the smartphone’s components (SIM toolkit) in order to circumvent restrictions and read critical IT security information and possibly change it.

HARDWARE INTERFACES
An attacker may obtain access to data over memory buses and hardware interfaces (JTAG) or use them to circumvent the protection mechanisms of the user interface.

MEMORY
Manipulating flash memory contents or RAM disks often offers an option to remove protective mechanisms or directly read user data.

USB
Many of the described physical attacks may be carried out by low level access over USB without opening the smartphone itself. Beyond that most smartphones have additional logical interfaces for modem functions and data access, which represent an additional gateway for attacks, for example during unsupervised recharging.

BIZZTRUST FOR ANDROID – TWO SMARTPHONES IN ONE
BizzTrust provides separate use areas on a smartphone, each of which can have its own data records and access authorizations. The device’s private applications (app) to run simultaneously, without limitations and independently from business applications. Moreover, extended remote maintenance protocols allow in the business use area to determine the device status, automatically implement software updates and integrate the device in full into the central event management infrastructure of the company. BizzTrust offers:

- Business data protection
- Unrestricted private use
- Secure communication within the company (anonymity)
- Remote management and updates
- Supports RODI strategy
- Automatic policy enforcement

YOUR SMARTPHONE GONE ASTRAY?
Smartphones are practical tools and have become indispensable for everyday business. Not caring about smartphone security means an immense risk. Financial loss may occur due to the abuse of premium services, for example by malware having been transmitted on unauthorized access to enterprise networks. Fraunhofer SIT supports companies and public authorities in their secure smartphone use. We offer independent security analyses and development support for the implementation of innovative solutions to device manufacturers and software providers. We offer:

- Security analyses (with or without certificate)
- Practical attack tests
- Develop and implement security concepts
- Safeguard mobile devices and resources
- Adapting to and determining secure configurations
- Innovative solutions