Smartphone Architecture & Security

Laurent Simon
Connected Devices SIG
January 13
Content

1. Smartphone Architecture
2. Android Permission Model
3. Stakeholders & Business Model
4. Current Mobile Malware
5. Current Approaches and Future Trends
Smartphone Architecture
Phone Evolution: "just"phones

• place/receive calls

• contact edition/viewing

• simple built-in functionalities: alarm
Phone Evolution: feature phones

• GSM stack

• user interface

• built-in applications on baseband CPU
  > accessible via serial port/usb
  > communication thru AT commands
  > carrier-locking/IMEI
Phone Evolution: smart phones

- different processors for GSM stack and applications
- baseband / OS users interact with: android, iOS, WP, BB
- baseband CPU / application CPU
- AT commands replaced by proprietary protocols
- hardware connection: USB/SPI/shared mem
- baseband: perfect for spyware / security thru obscurity
Android and its permission model
Permissions

• mapped to functionalities on phone (API) > ex: internet / sms-read

• permission review by user at installation time

• no change possible after installation

• all-or-nothing = install or not
Permissions

THIS APPLICATION HAS ACCESS TO THE FOLLOWING:

YOUR ACCOUNTS
CREATE ACCOUNTS AND SET PASSWORDS
Allows the app to use the account authenticator capabilities of the AccountManager, including creating accounts and getting and setting their passwords.

ADD OR REMOVE ACCOUNTS
Allows the app to perform operations like adding and removing accounts, and deleting their password.

HARDWARE CONTROLS
TAKE PICTURES AND VIDEOS
Allows the app to take pictures and videos with the camera. This permission allows the app to use the camera at any time without your confirmation.

YOUR LOCATION
APPROXIMATE LOCATION (NETWORK-BASED)
Allows the app to get your approximate location. This location is derived by location services using network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the
Allows the app to get your approximate location. This location is derived by location services using network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine approximately where you are.

**PRECISE LOCATION (GPS AND NETWORK-BASED)**

Allows the app to get your precise location using the Global Positioning System (GPS) or network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine where you are, and may consume additional battery power.

**NETWORK COMMUNICATION**

**FULL NETWORK ACCESS**

Allows the app to create network sockets and use custom network protocols. The browser and other applications provide means to send data to the internet, so this permission is not required to send data to the internet.

**YOUR PERSONAL INFORMATION**

**READ YOUR CONTACTS**

Allows the app to read data about your contacts stored on your tablet, including the frequency with which you've called, emailed, or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge. Allows the app to read data about your contacts stored on your phone, including the frequency with which you've called, emailed, or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge.

**MODIFY YOUR CONTACTS**

Allows the app to modify the data about your contacts stored on your tablet, including the frequency with which you've called, emailed, or communicated in other ways with specific contacts. This permission allows apps to delete contact data. Allows the app to modify the data about your contacts stored on your phone, including the frequency with which you've called, emailed, or communicated in other ways with specific contacts. This permission allows apps to delete contact data.

**PHONE CALLS**

**READ PHONE STATUS AND IDENTITY**

Allows the app to access the phone features of the device. This permission allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call.

**STORAGE**

**MODIFY OR DELETE THE CONTENTS OF YOUR USB STORAGE**

Allows the app to modify or delete the contents of your USB storage. If the app does this, it may access your personal photos, documents, and other files on your device. Apps may use this to determine approximately where you are.
Permissions: flaws (1)

• not mapped to use-cases: IMPOSSIBLE for anyone to spot a malicious app

• all-or-nothing: users prefer non-secure service to no service at all

• permission review has poor design (in terms of security)
Permissions: flaws (2)

• users do not know what they are and/or how to use them
  > known fact
  > poor design

• fun, vdo, social network vs security
  > distraction effect: Real Hustle
  > selective attention: Invisible gorilla
Permissions: why??

• Google focus on user experience because it sells, security does not

• ecosystem: appeal to developers
Stakeholders & Business Model
Stakeholders: complexity

• SIM + baseband: carrier (NFC payments)

• "smart" OS: carrier / OS provider / manufacturer
  > built-in services: Gmail, Search
  > customization layer (default apps) added by carrier and manufacturers

• apps: developers and other companies
Business Model: misaligned incentive

• carrier / manufacturers
  > no loyalty, buy every 2 years
  > no incentive for customer service
  so no upgrade: 50%

• developers make money thru ads
  > incentive for more permission
  > privacy concerns / information leakage
Current Malware
Installation Methods

• repackaged apps (free/paid). 86% of malware. revenue thru ads / copyright problem / clickbot

• dynamic load of code: java/WebView/native. for code evasion (plankton and AnswerBot)

• drive-by-download in apps, QR/NFC codes, (mobile) web browser (city centers)
Payload Content (1)

• early root exploits: 33%

• remotely controllable (sms/server: 90%)

• premium SMS/subscribe premium services

• calls (possible but not found)
Payload Content (2)

• incoming SMS / defeats bank 2-factor auth
  > SpitMo and ZeusMitmo
  > 36M euros stolen in 2012

• private data theft:
  > IMEI: reflash baseband
  > SMS, contacts: spearphishing
  > user account: sold on black market
Payload Content (3)

• notification abuse

• touch-jacking/overwrite screen

• phishing via Inbox folder SMS
Payload Content (4)

• Abuse of onboard sensors for spyware: GPS tracking, video, audio, temperature

• Side channel attacks:
  > Infer sex of user via accelerometer
  > Infer PIN via accelerometer
  > Infer PIN via video reflection
  > 3D imaging thru camera
Future Trends
Future trends

• cloud / Trusted Execution Environment (TEE)
• # sensors increase
  > smell sensor at CES 13
• Internet of Things: smartphone-centric
  > oven running android at CES 13
  > metawatch / pebble
  > card SDK
  > control lighting at home
  > linux riffle, etc
Summary

• complex multi-stakeholder ecosystem

• more intimate info than desktop computers

• large number of built-in hardware/sensors

• android: a broken permission model?
Thank you!

Laurent Simon
lmrs2@cl.cam.ac.uk