



# openHPI – Internet Security Excursion: Android Security

**Prof. Dr. Christoph Meinel**  
Hasso Plattner Institute, Potsdam, Germany

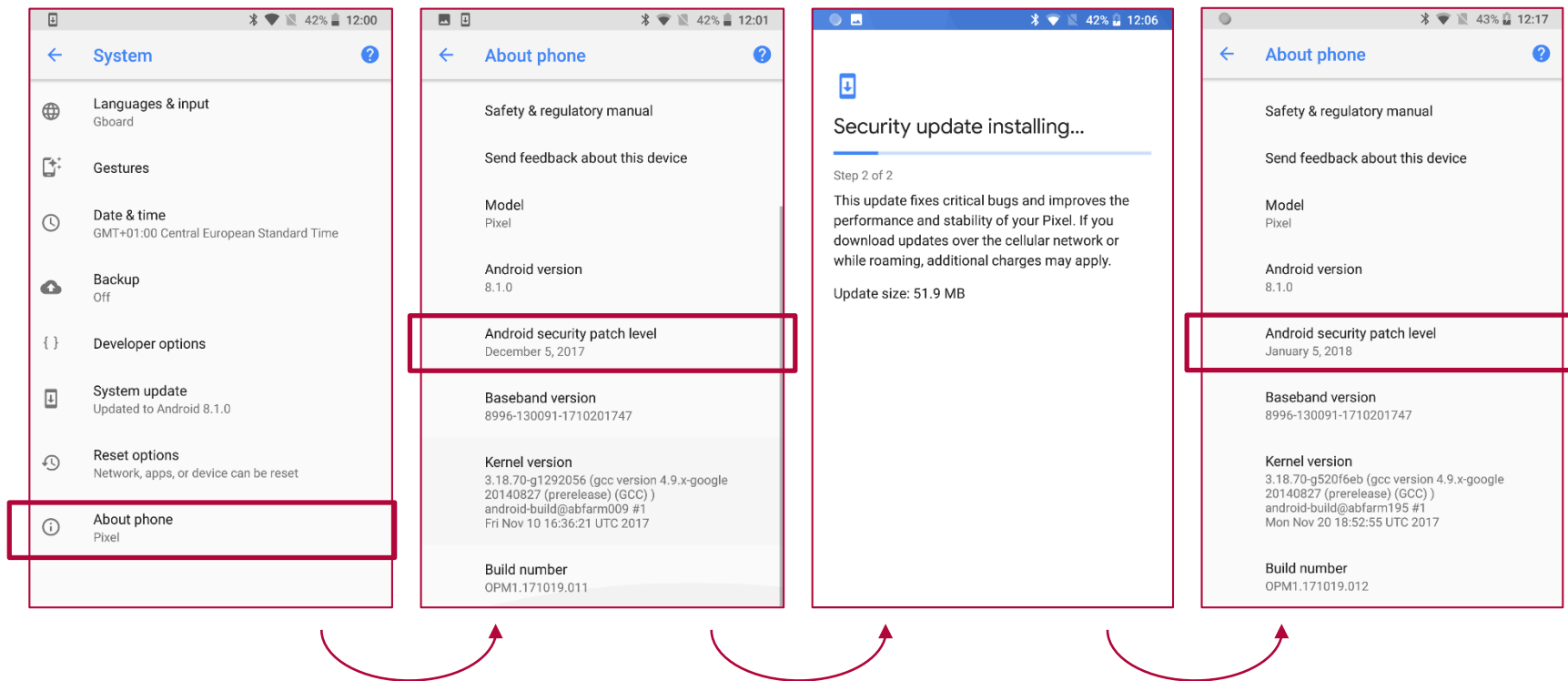
# Security: What is special about Android?

---

- Both Google and Apple issue monthly updates for Android and iOS, respectively
- As an average, Apple supports their phones for **4-5 years**
  - iPhone 5s released in September 2013, still supports the latest iOS version 11 with all security patches
- However, different from iPhone, Android-based phones are produced by many manufacturers
  - each manufacturer has its own customized Android-based firmware for phones
  - Android security patches from Google need to be integrated by each manufacturer independently
    - once the warranty (**1-2 years**) is expired, manufacturers are not interested in supporting old smartphone models,
    - there is no lifetime / service life defined by law

# How to check if your Android phone is up to date? (Google Pixel)

Settings → System → About Phone → Android Security Patch Level



# What to do if your Android phone is not supported anymore?

---

- Buy a new smartphone every 1-2 years
  - could still be cheaper than devices from Apple over time
  - however, it increases volumes of electronic waste
- Select a smartphone with having a longer service life or a longer specified update period by the manufacturer
- Select a smartphone with an Android version by Google, i.e., Google Pixel

# What to do if your Android phone is not supported anymore?

---

Regularly follow security news and check whether mitigation without a patch is possible

- **Example** for Stagefright vulnerability:

- disable auto-retrieval of MMS, install latest version of Firefox
- **do not use any apps other than Firefox, calls and SMS**

Check if an up-to-date version of LineageOS (alternative firmware for Android phones) is available for your smartphone

- **Requires rooting, but provides new security updates**

# Android: Root Access (1/3)

---

**"Smartphone rooting"** means hacking the smartphone to gain root or administrative rights on the smartphone

- Users are given administrative rights and can also pass these rights on to any application
- **Caution:** important security mechanism is broken
  - usually, only core components of the operating system have administrative rights
  - attackers can exploit vulnerabilities in an app with root access in order to get root privileges themselves, attacks may be more powerful
- Users with root privileges can still install non-critical apps that do not require root access

# Android: Root Access (2/3)

---

**Rooting** opens up many other possibilities:

- Installation of alternative versions of Android (“ROMS”)
  - earlier security updates, different user interfaces, more performance etc., e.g., LineageOS
- Better control of OS and hardware, e.g., CPU over- and underclocking in order to get better performance or longer battery life
  - **can lead to malfunction of the mobile phone**
- Better control of applications: It becomes possible to install or remove system components

## **Important:**

- If possible, only give root privileges to a few trustworthy apps to reduce the number of system components with root privileges as they can present possible targets for attacks!

# Android: Root Access (3/3)

---

## **Danger:**

- Process of rooting can damage device (“brick”)
- Warranty does not work as it is also possible to change hardware settings with root privileges, for example, increase the processor clock frequency. This can lead to overheating of the mobile phone
- Rooting is not a recommended option for users with no in-depth knowledge of these areas:
  - authorizations
  - AppStore (Google Play Market)
  - root privileges
  - ...

**Rooting is always at your own risk**