



openHPI – Internet Security Privacy: Smartphones

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

Smartphones are constantly with us

Smartphones have become our **inseparable companion**.
They store and generate **huge amounts of personal data**

- calls
- SMS
- contacts
- emails
- **usage statistics** for everything the smartphone does
- **movement data:**
 - GPS, WLAN positioning, GSM location by cellular network
- **activity data:**
 - step counters that (currently work in almost any smartphone using the acceleration sensor)
- ... and lots of other **personal data:**
 - photos, videos, etc.

Risk: Online Synchronization (1/2)

Smartphones often perform data synchronization over the Internet, e.g.,

- iPhones with iCloud, Android with Google account

All user settings, applications and application data are also stored online

Online account allows access to other devices

- **Advantage:**

- ☐ data is also safe when a local backup is lost, and can be restored from anywhere in the event of loss or damage

- **Disadvantage:**

- ☐ storage of data on the Internet carries the risk of theft
- ☐ attacker can install and delete applications, recover and destroy data, unlock phone, etc.

Risk: Online Synchronization (2/2)

By the way, access to the

- Apple App Store
- Google Play Store

in order to install applications, is - without an online account – technically very complicated or not possible at all

Risk: Online Synchronization

An Attack Example (1/3)

Attack on Mat Honan, author at Wired.com:

Attackers using stolen Apple ID deleted all data on Mat's MacBook, iPhone, iPad, and also his online backups

- Attackers wanted to take over Mat's Twitter account
- Twitter account contained information about personal website
- Using the "whois" service, attackers found out Mat's postal address and private Gmail address
 - "Whois" allows the retrieval of stored data from domain owners (here: from Mat's personal website)
- By means of the Gmail account's password recovery, an attacker found the email address of the Apple ID
 - Gmail: "We sent an email to [m****n@me.com](#) " → Attacker discovered full address...

Risk: Online Synchronization

An Attack Example (2/3)

Attack on Mat Honan, author at Wired.com:

Attackers using stolen Apple ID deleted all data on his MacBook, iPhone, iPad and also his online backups

The attacker now knew name, postal address, private Gmail address, and email for the Apple ID

- Attacker contacted Amazon and associates a new credit card with Mat's account at Amazon
- Attacker contacted Amazon again, got the password restored (possible by knowing the previously added credit card number)
- Attacker found the last four digits of a genuine Mat Honan credit card on the Amazon account

Risk: Online Synchronization An Attack Example (3/3)

Attack on Mat Honan, author at Wired.com:

Attackers using stolen Apple ID deleted all data on his MacBook, iPhone, iPad and online backups

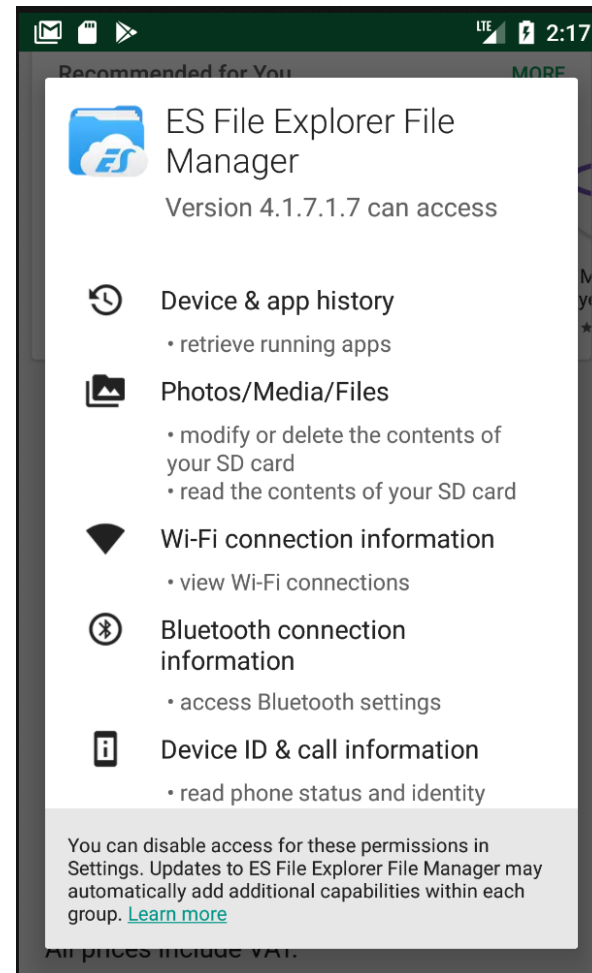
The attacker now knew name, postal address, private Gmail address, email for the Apple ID and last four digits of the credit card number

- Attacker contacted AppleCare and got access to the Apple ID (by knowing the name, address, email address, and last four digits of the credit card number)
- With the aid of Apple ID and access to Apple's mail account, the attacker reset the Gmail password (and then also the Twitter password) and deleted all data from the iPhone, iPad and MacBook ...

Risk: Apps – Applications

In addition to the online synchronization of the smartphone, each application can synchronize the data with its own server

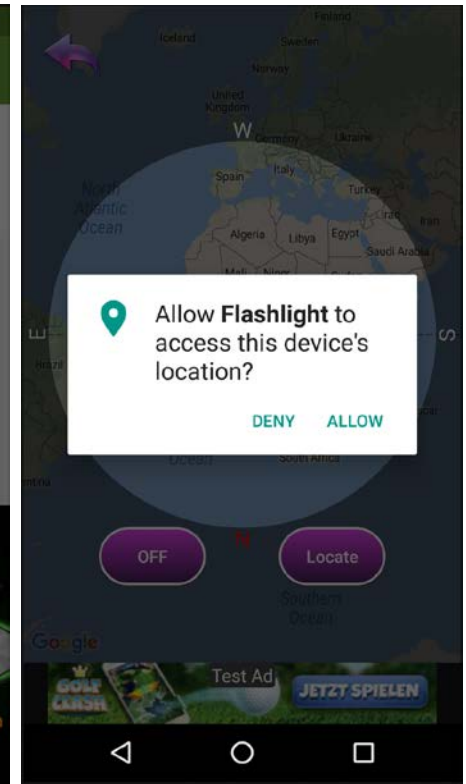
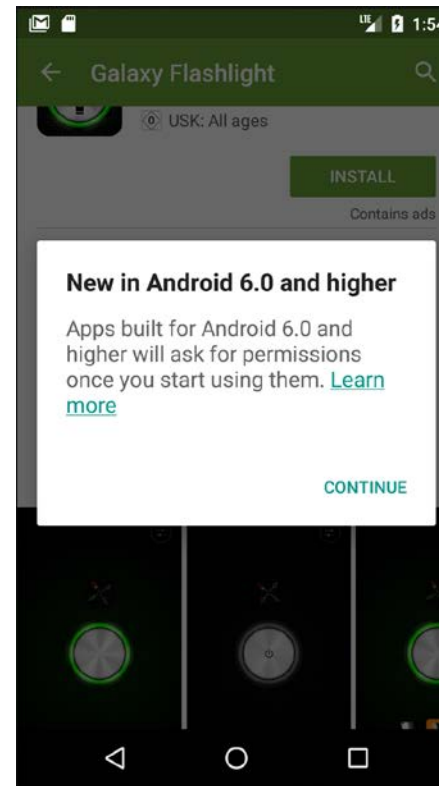
- Each app has different Data Protection Policy
- Apps can, for example, also access user data from other applications, GPS, or camera, depending on **authorizations**
- **Android:** Possible required authorizations can be displayed during the installation of the application



Authorizations for Applications

Example: Flashlight app may require access to camera and **location information**

- **Android:** Blocking individual authorizations is again possible with Android since version 6.0
 - privacy guard on LineageOS still can have more options
- **Apple iOS:** Allows blocking of the authorizations in the settings



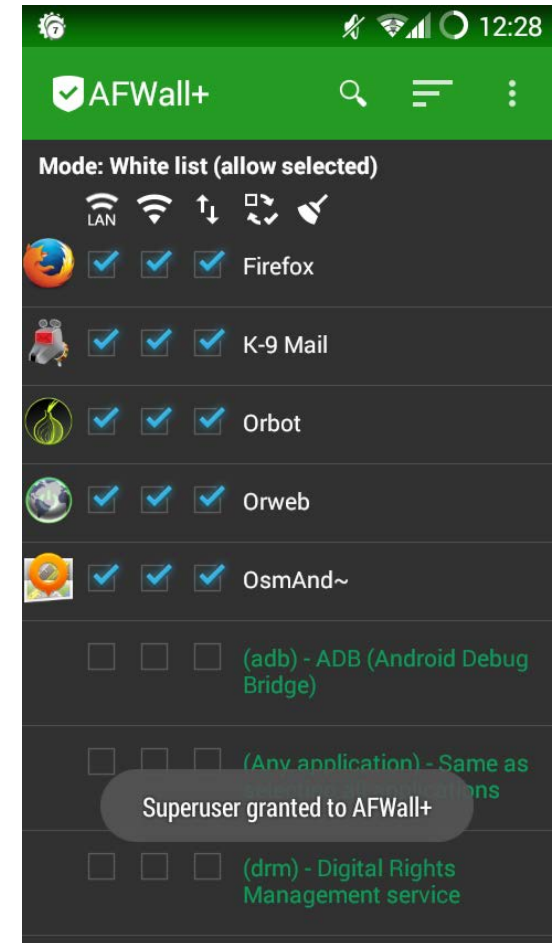
Authorizations for Applications: Internet Access

Application authorizations only control access to data

Internet access should actually be separately controllable for individual applications, e.g., by using a firewall

But:

- Not possible with standard tools of smartphones
- AFWall+ on Android
 - requires „root“ access
- Firewall IP for iOS
 - only available after „jailbreak“



Unavoidable for Users (1/2)

Monitoring by the manufacturer and backdoors, e.g.,

- **2011:** All location data of the iPhone was saved in the “consolidated.db” and sent to Apple
- **2014:** Developers of "Replicant" (free Android distribution) claim that all Samsung Galaxy smartphones have a backdoor in the modem software (with access to the file system)
- **2016:** Xiaomi can remotely install apps on customer's devices
- **2017:** OnePlus2 sending fine grained usage statistics of application usage and user's behavior to the cloud

Unavoidable for Users (2/2)

Mobile tracking by cellular network and **data retention**

- Cellular network must be able to determine the current cell of a cell phone, e.g., to be able to connect calls
- Telecommunication providers in most European countries were obliged to store traffic data and connection data for specific time periods