Security in Mobile Devices

IV. Székelyföldi IT Konferencia
October 14th 2016

Zoltán Damó

iOS Developer

Space Observer

Available in the App Store

RedRock Tech

Developers Meetup - Sepsiszentgyörgy

21 October, 18:00

Abstract

- Threats from user's point of view
- Threats from developer point of view
- Detection and prevention

User

Open Doors

- Physical access
- Rooting/Jailbreak

Rogue Chargers

- Looks as a regular charger, even charges the phone
- Installs malware

WiFi

- Public WiFi can be snooped, rerouted
- Copy cat AP, same name as a trusted AP but open

Bluetooth

- Security Mode #1, no encryption at all, no pairing
- Ultimate trust in paired devices
- Unsecured serial stacks

Software

- Permissions, be a skeptic
- Don’t visit dubious sites, browsers are vulnerable
- Don’t use apps from outside of the store
- Install security updates
- Disable Dev mode

Developer

Handling Sensitive Information

- Don’t store clear text, use hashes
- Use secure hash, md5 bad m’kay
- Use salted hash
- Use native secure storage
- Don’t store sensitive data at all. oAuth
- Use 3rd party payment provider
- Assume all devices are compromised
- Don’t log or cache sensitive data

Secure Communication

- Use secure protocols.
  HTTPS is the new HTTP
- Don’t implement your own crypto
- Don’t hash a hash

Don’t Be a Tool

- Bad publicity if your app is the culprit
- Secure your app. Don’t be the backdoor. Example using unsafe C functions gets, strcpy etc
- Don’t request permissions to services you don’t need (yet)
- Sanitise user input

Protection

- System update
- Turn off unused services NFC, Bluetooth, GPS
- Antivirus
- Firewall
- Be a skeptic, use common sense

Detection

- Sudden drop in battery life
- Device overheats for no reason
- Suspicious network activity
- Suspicious speed degradation

Summary

- Don’t lose phone, don’t trust every peripheral
- Update OS
- Secure communication
- Secure user data
- Don’t implement your own crypto
- Be a skeptic

Q&A