ANDROID-(IN)-SECURITY

SECURITY AND PRIVACY (FOR ANDROID USERS) WHAT CAN BE DONE?

Talk at DefCamp Bucharest · November 28, 2014

Dr. Ralf C. Staudemeyer · @n0airc0n
Herbert Braun · @wortwart · mailto

---

woerter.de/android/

PART I: THE PROBLEM

YOUR SMARTPHONE KNOWS EVERYTHING (ABOUT YOU)

→ but wasn't built as a data safe anyway

in the light of the NSA revelations … a really bad idea!

PART I: THE PROBLEM

ARE CRYPTOPHONES A SOLUTION?

Maybe … for politicians, managers and criminals

Can I get better privacy with my standard Android device?

Even more maybe …

PART I: THE PROBLEM

CRYPTOPHONES VS. LEAKPHONES

- very expensive (over 2000 Euros or costly subscriptions)
- possibly not compatible with each other
- key question → who do you trust?
  countries, companies, politicians
  to trust individuals and your feeling might be the best advice :-(

PART II: FIXING THE HOLES

OUR TODO LIST

1. Baseband security and firmware
2. Android OS
3. Permission management
4. Data encryption
5. Communication tools
6. Search and browsing
7. Apps, updates and wipe

PART II: FIXING THE HOLES

1. BASEBAND SECURITY AND FIRMWARE

GSM is broken by design:

- traceable identifiers (IMSI, IMAI)
- compromised base-stations
- silent SMS
- insecure channel encryption

PART II: FIXING THE HOLES

1. BASEBAND SECURITY AND FIRMWARE

You know there's a hidden OS on your device?
… and heaps of other buggy, non-free firmwares

- Baseband OS
  → remote access to sensors and memory
- WLAN
- Bluetooth
- NFC
- Campera

Better retire 2G, skip non-free firmwares, and start monitoring baseband activity (AIMSICD).

PART II: FIXING THE HOLES

2. HARDENING ANDROID OS

Disable access to:

- Location
- Text and voice input
- Backup and restore
- Device name
- …

PART II: FIXING THE HOLES

3. PERMISSION MANAGEMENT

Android's app permissions management is a mess

- unclear prior to installation
- excessive requests are common practice
- descriptions are unclear
- revoke not provisioned
- …

PART II: FIXING THE HOLES

3. PERMISSION MANAGEMENT

Android's app permissions management is a mess
→ guess what: it got worse since V4.8.19

- updated permissions do not require user approval
- network access is permitted by default
- silent update

AppOps, xprivacy mod and CM's Privacy Guard 2.0 can restore control

PART II: FIXING THE HOLES

4. FILE SYSTEM AND FILE ENCRYPTION

Great: We can encrypt the file system using dm-crypt! But …

- encryption is limited to the /data folder
- unlock PIN/password is the passphrase
- decide between security and usability

Setting a strong password is possible
(but requires root)

PART II: FIXING THE HOLES

5. COMMUNICATION TOOLS: THE PHONE

- Forget GSM –
  use VoIP with TLS/[S|Z]RTP (whenever feasible)
- but serious connectivity and encryption issues
- any trustworthy service providers out there?
  OSTEL/OSTN might be a route to take
  video chat? … it is worked on

PART II: FIXING THE HOLES

5. COMMUNICATION TOOLS: PIM, MAIL AND MESSAGING

- build your own cloud
  to handle personal data
- GPG/PGP and OTR are your friends
- P2P might save us (WebRTC)

OwnCloud, DavDroid, K9 Mail/AGP and ChatSecure are options

PART II: FIXING THE HOLES

6. SECURE SEARCH AND BROWSING: SEARCH

Google tries to be your personal assistant
→ incompatible in terms of privacy
skip that!

Get TOR into place!
Access DuckDuckGo via Hidden Service?
(https://3g2upl4pq6kufc4m.onion)
try DuckDuckGo Search & Stories

PART II: FIXING THE HOLES

6. SECURE SEARCH AND BROWSING: BROWSERS

Firefox is a good trade-off between privacy and usability – but a stock browser is traceable

→ you'll need a few addons.

- HTTPS Everywhere
- Phony
- Privacy Badger
- CleanQuit
- Self-Destructing Cookies
- noscript

… and get TOR in place using Orbot + orWall.

PART II: FIXING THE HOLES

7. APPS, UPDATES AND WIPE: PRE-INSTALLED APPS

Google's bundled apps leak all your data

- Play Store -> Fdroid
- AOSP -> Hacker or Anysoft Keyboard
- Google Maps -> OSMAnd~
- YouTube -> Download YouTube app
- PIM and storage -> ownCloud + DavDroid
- Access Google Apps with GApps

It is a nightmare – get rid of them!

Open Source alternatives are all on Fdroid

PART II: FIXING THE HOLES

7. APPS, UPDATES AND WIPE: UPDATES AND WIPE

- Ancient Androids are everywhere
- Auto-updates for apps are good
  → but more control is better
- Ensure remote wipe?
  … intheclear might work for you

PART III: WRAP-UP

WHAT CAN I DO?

Your Android device has more holes than a Swiss cheese.

there's reason to despair, but do something anyway!

- Install CyanogenMod (or better Replicant)
- Check out our guide with recommended settings on woerter.de/android/droidcon/
- Replace Google apps
- Communicate encrypted by default
- Tell us if we're wrong or if you have a good idea!
  @n0airc0n · @wortwart