You don’t hear me but your phone’s voice interface does

José Lopes Esteves & Chaouki Kasmi

Hack In Paris - 18/06/2015

WHO WE ARE

José Lopes Esteves and Chaouki Kasmi

- ANSSI-FNISA / Wireless Security Lab
- Electromagnetic threats on information systems
- RF communications security
- Embedded systems
- Signal processing

AGENDA

- Voice command interpreters
- Voice and command injection
- Attack scenarios
- Countermeasures
- Conclusion

Voice Command Interpreters

Your phone hears…

VOICE COMMAND INTERPRETERS

- Definition
- Commands scope
- Activation conditions
- Process description
- Security

DEFINITION

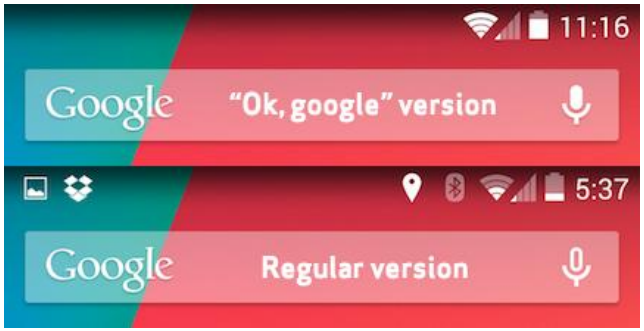
- Hands-free UI
- More and more deployed
- Smartphones, smartwatches, IoT, cars, desktop OS, browsers, apps…
- Apple: Siri, VoiceControl
- Microsoft: Speech, Cortana
- Google: Google Voice Search
- 3rd party apps (e.g. Samsung S-Voice)

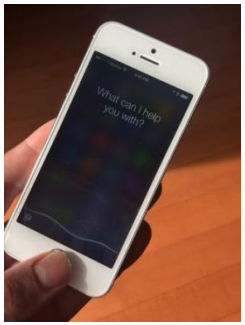
COMMANDS SCOPE

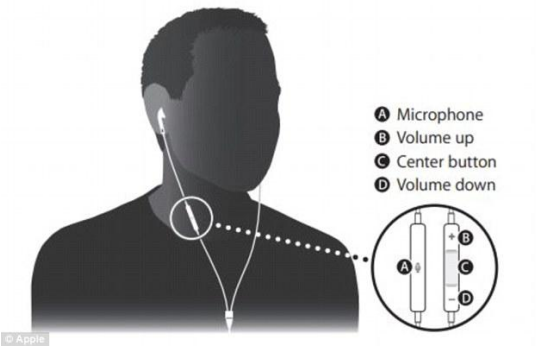
- Telephony: calls, SMS…
- Internet: browsing, emails, social networking, web searches, maps…
- Local: launching/using apps, changing settings, creating notes, alarms, calendar entries…

ACTIVATION CONDITIONS

- Always on: keyword (*OK Google*, *Hey Siri*)
- Via soft button: in specific applications
- Via hard button: on phone or on headset remote

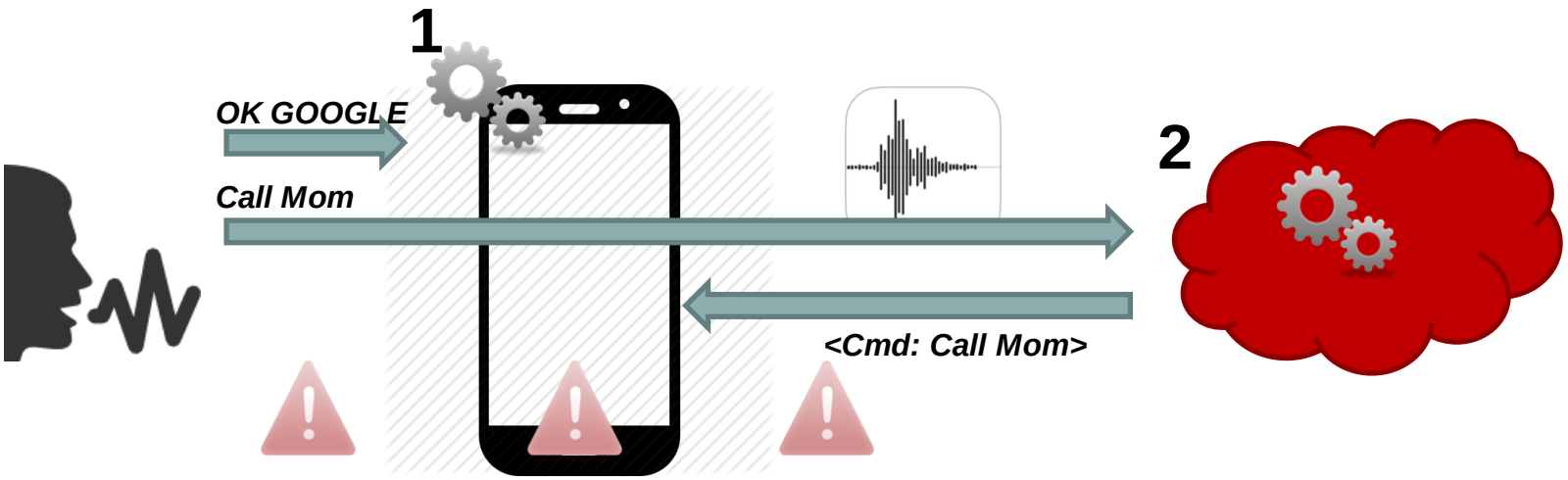






PROCESS

- Local: keyword detection, limited actions
- Remote: voice processing and command recognition



SECURITY

- Pre-auth actions (limited but still…): auth bypass [1]
- Cloud based: malicious server responses [2]
- Voice processing: privacy [3], biometric data
- Local attacks: malicious app voice sending commands by audio front-end [4]

SECURITY

- Pre-auth actions (limited but still…): auth bypass [1]
- Cloud based: malicious server responses [2]
- Voice processing: privacy [3], biometric data
- Local attacks: malicious app voice sending commands by audio front-end [4]
- Today: Remote and Silent Voice Command Injection by Smart IEMI

Voice and Command Injection

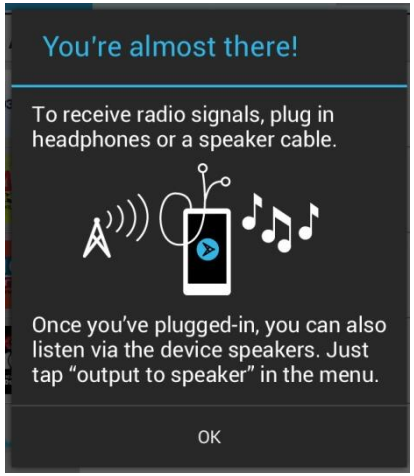
But you don’t hear anything…

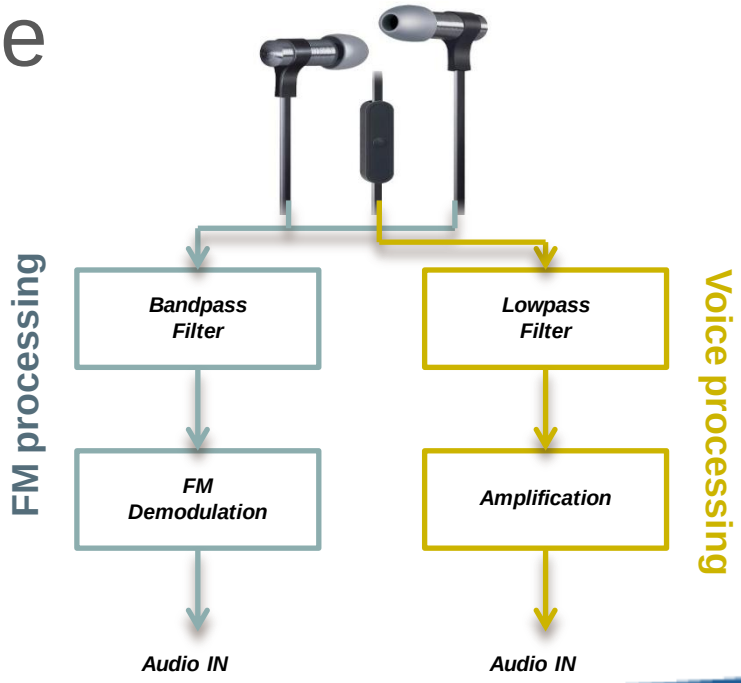
VOICE COMMAND INJECTION

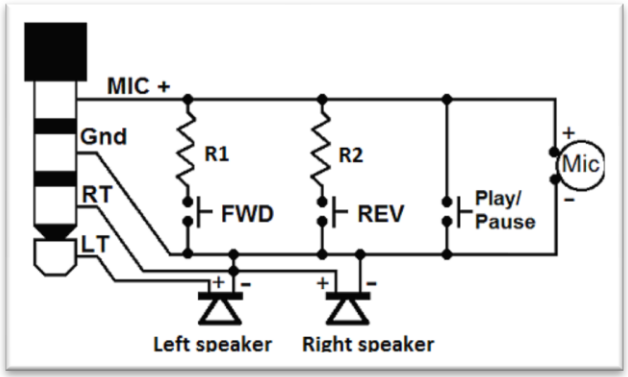
- Smartphones, headsets, FM
- Transmission principle and field to line coupling
- Experimental setup
- Results

SMARTPHONES, HEADSETS, FM

- Some smartphones are FM radio capable
- Use headphones cables as an antenna
- Remote buttons change the signal on the MIC cable





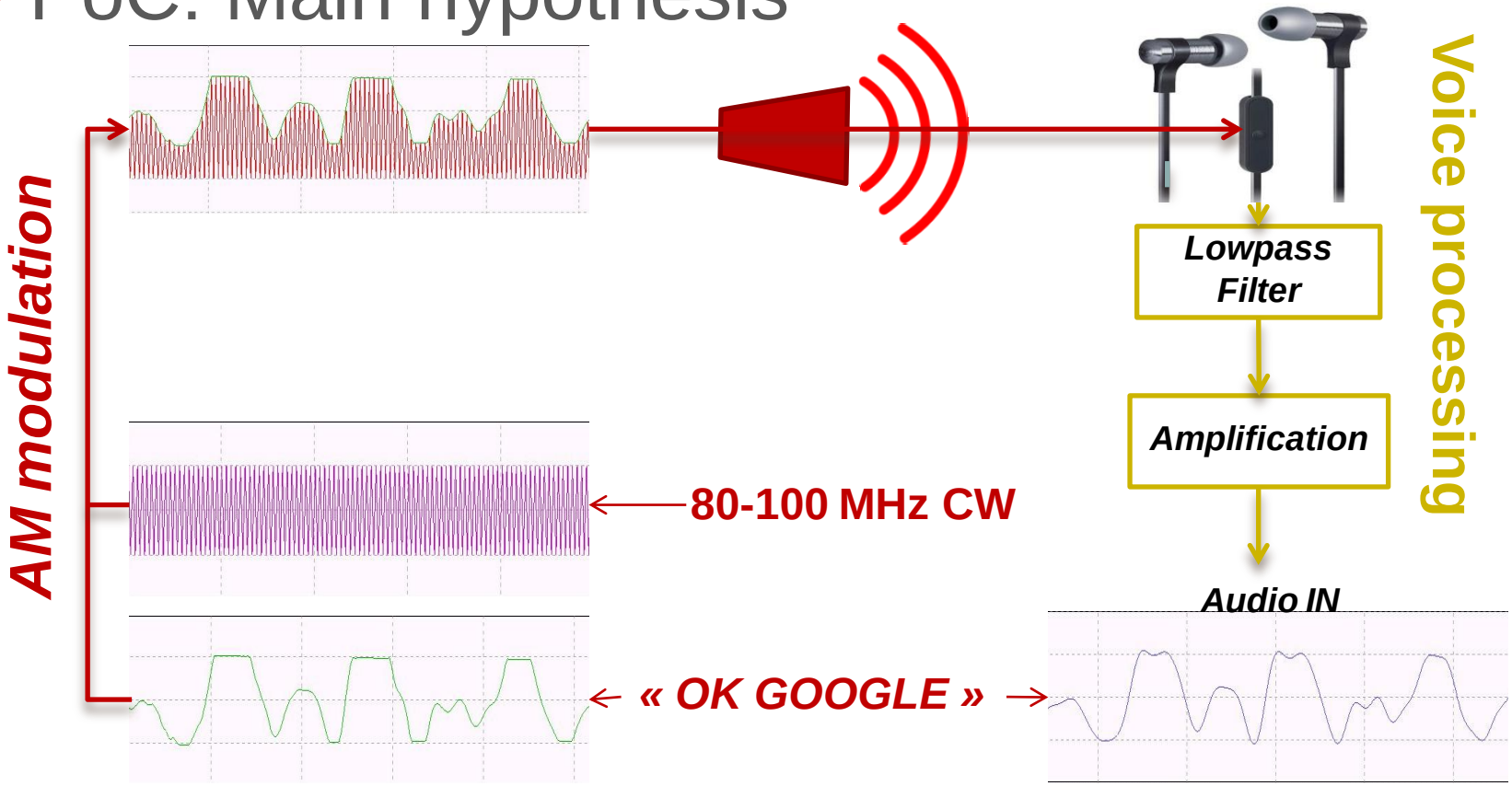


SMARTPHONES, HEADSETS, FM

- Some smartphones are FM radio capable
- Use headphones cables as an antenna
- Remote buttons change the signal on the MIC cable
- Headphones are good [80MHz-108MHz] coupling interfaces
- Maybe we can inject a signal interpreted as sound by abusing the low-pass filter with a VHF AM signal

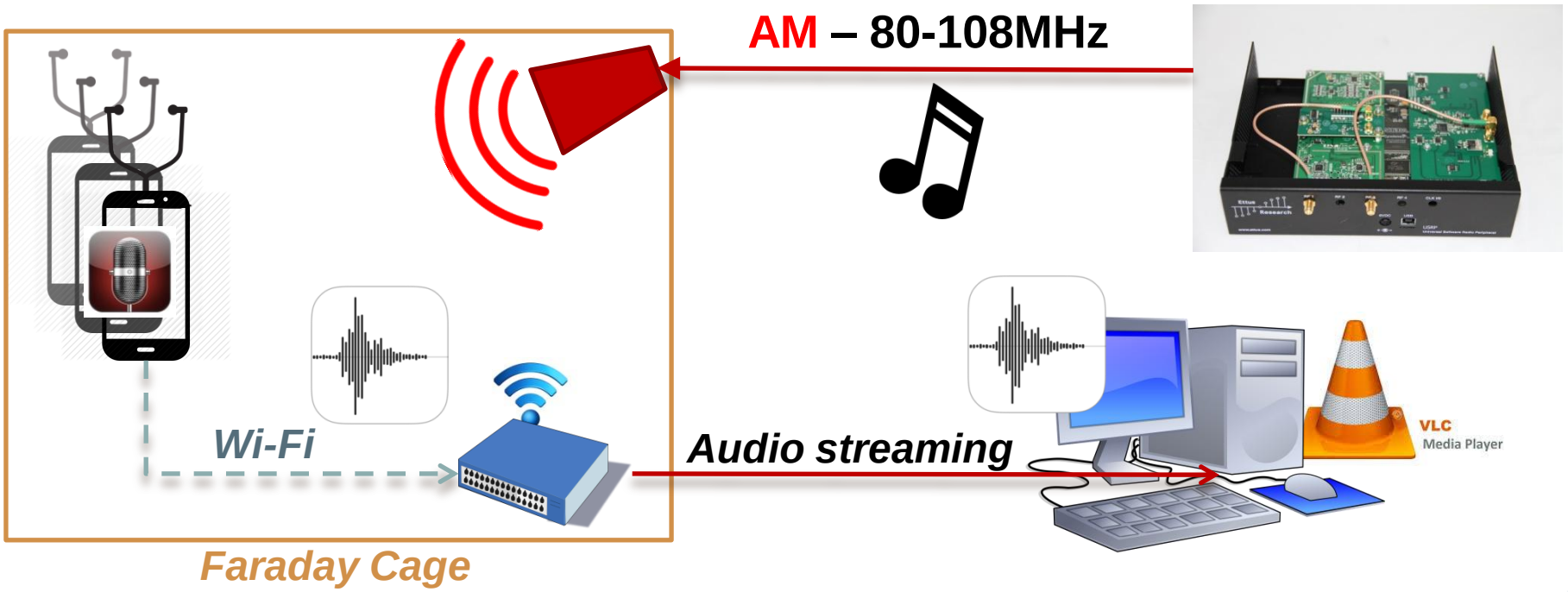
SMARTPHONES, HEADSETS, FM

- PoC: Main hypothesis



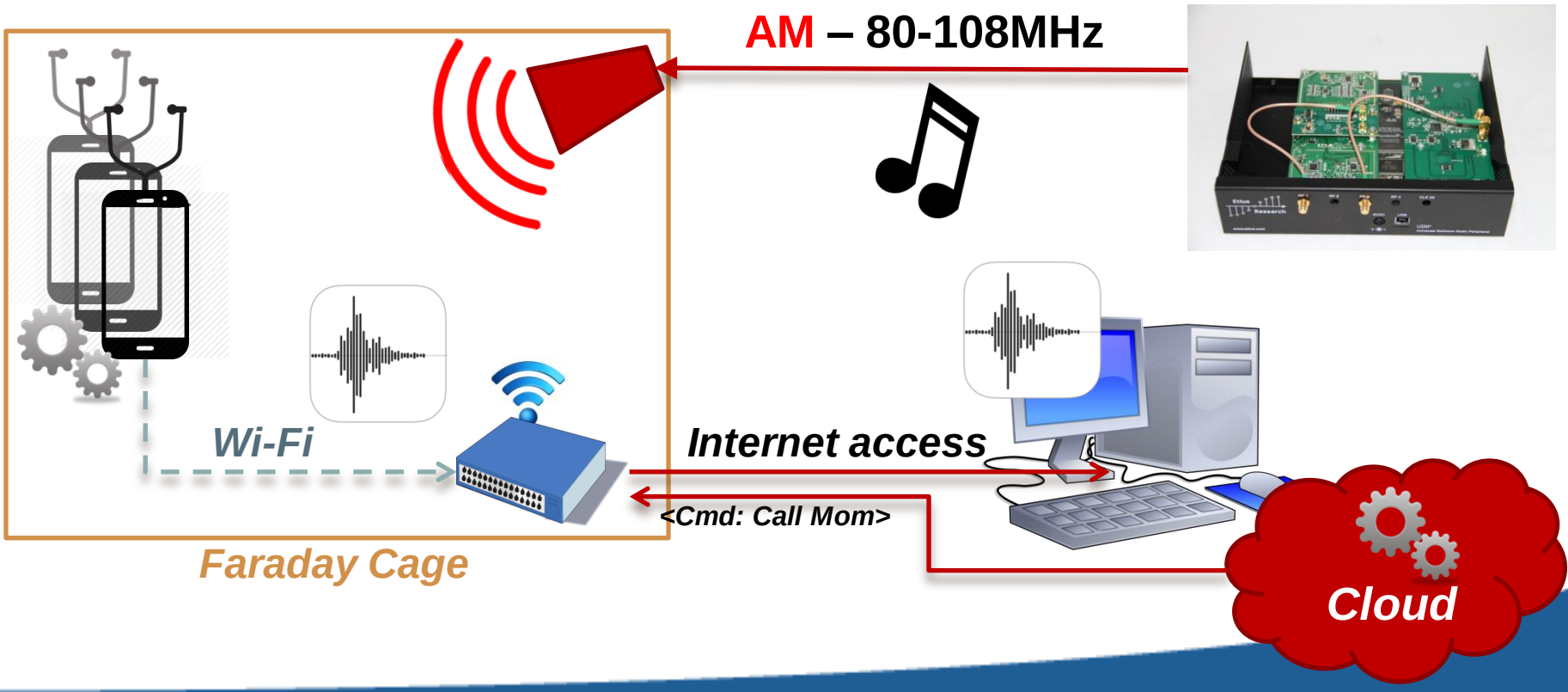
EXPERIMENTAL SETUP

- PoC: injecting music



EXPERIMENTAL SETUP

- PoC: injecting commands ?

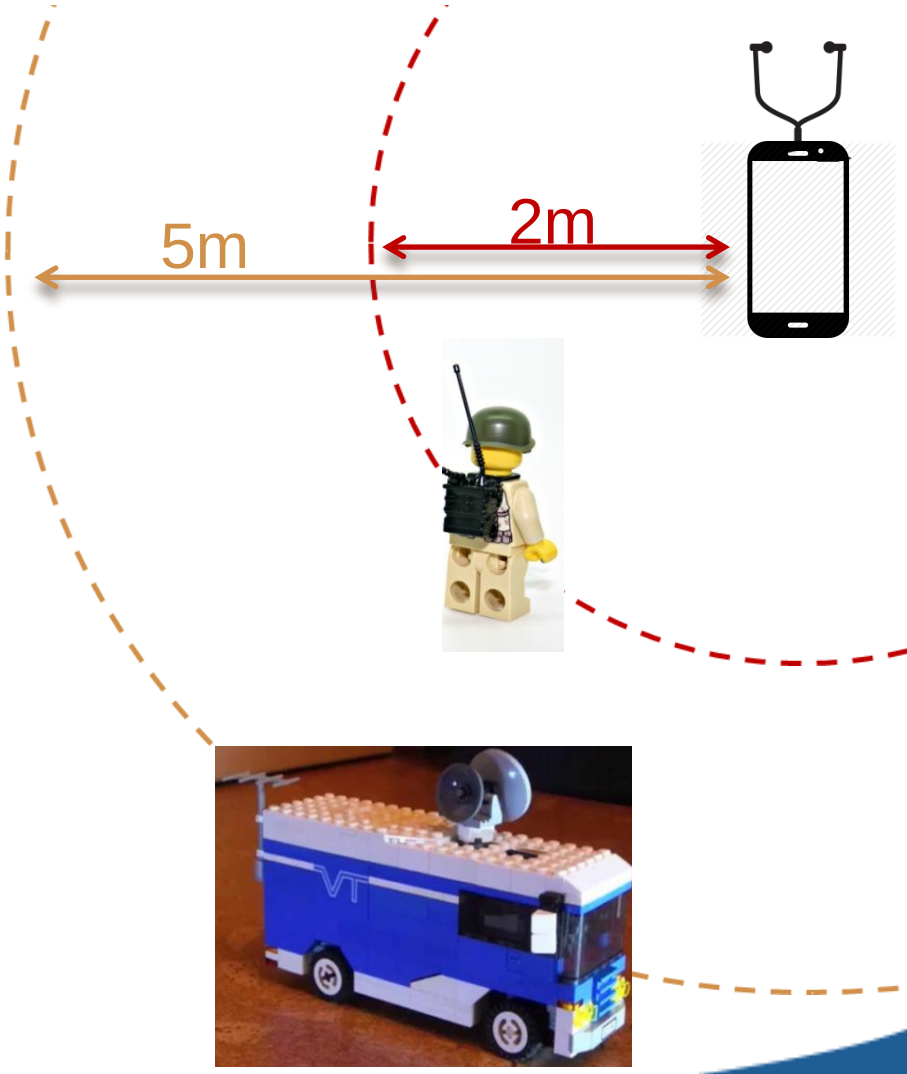


RESULTS

- Activation (if needed):
  - CW (80-108MHz), Frequency modulated signal
- Exploitation:
  - CW (80-108MHz), Amplitude modulated CW by audio voice commands
- Electric field level/range:
  - 28V/m at 100MHz (< than the human safety limit)

RESULTS

- Limitations
  - Antenna size (~30cm)
  - Emitted power
- E-field level/range
  - 28V/m at 100MHz
- Power level/range
  - 40W/2m, 200W/5m



Attack scenarios

…Silent and Remote Command Injection

ATTACK SCENARIOS

- Tracking
- Eavesdropping
- Cost abuse
- Reputation / Phishing
- Malicious app trigger
- Advanced compromising

ATTACK SCENARIOS

- Tracking
  - Activate wireless interfaces (Wi-Fi, BT)
  - Capture advertising packets (Probe Requests)
  - Use MAC addresses to identify
  - Use presence of packets to locate
  - Use Wi-Fi SSIDs to identify known locations
- **Demo: S-Voice bluetooth (de)activation**

Payload: Hi Galaxy – Bluetooth

ATTACK SCENARIOS

- Eavesdropping
  - Place a call to a monitoring phone's number
  - Simply listen to the target's sound environment
- **Demo: placing a call**

Payload: Call « Mon Compte » (« My account »)

ATTACK SCENARIOS

- Cost abuse
  - Massive attack in a crowded place
  - Place a call or a SMS to a paid service
  - Browse to some URL with ads
- **Demo: web browsing**

Payload: OK Google – Go to www.ssi.gouv.fr

ATTACK SCENARIOS

- Reputation / Phishing
  - Create malicious content (embarrassing, phishing)
  - Send by SMS, email
  - Or publish to social media
  - Web/search history poisoning

ATTACK SCENARIOS

- Malicious app trigger
  - Launch an already installed malicious application
  - Use voice input to trigger a payload
  - Launch a critical application (e.g. Sesame)
- **Demo: launching an application**

Payload: OK Google – Open Gmail

ATTACK SCENARIOS

- Advanced compromising
  - Use voice command injection as a way to extend the attack surface (Interface activation, web browsing…)
  - Exploit vulnerabilities to compromise the device
  - Ex: silent application install via a malicious web page [5], local priviledge escalation…
  - Ex: wireless interface reset, capture initial exchange, exploit protocol weaknesses, rogue AP [6], launch an application…

Countermeasures

Restrict, Detect and Alert

COUNTERMEASURES

- For
  - Users
  - Manufacturers/editors
- To
  - Reduce attack surface
  - Limit impact
  - Increase attacker level
  - Detect the attack

USERS

- Unplug headphones when not used
- Use mic-less headphones
- Only enable voice command when needed
- Personalize keyword
- Carefully select commands available (especially pre-auth)
- Enable as many feedbacks as possible (sound, vibration…)

EDITORS

- Limit critical commands available
- Reduce audio front-end sensitivity
- Voice recognition
- Provide finer-grain settings to users
- Detect abnormal EM activity with built-in sensors [7]

Conclusion

CONCLUSION

- **Voice command interface IS critical and shall be correctly secured**
- Users: use it wisely
- Editors: allow users to use it wisely and implement secure defaults
- Researchers: take a look at it, it is a critical and complex command input interface

CONCLUSION

- **Smart IEMI can be an efficient attack vector against information systems**
- Not limited to DoS
- More and more affordable (SDR…)
- Take it into account for risk analysis

References

REFERENCES

[1] N. Gonzalez, *Siri exploited again – how to bypass the lock screen in iOS 8*, ios.wonderhowto.com, 2014

[2] Applidium, *Cracking Siri*, GitHub, 2011

[3] W. Wei, *Apple admits Siri voice data is being shared with third parties*, www.hackernews.com, 2015

[4] W. Diao et al., *Your Voice Assistant is Mine: How to Abuse Speakers to Steal Information and Control Your Ph*one. SPSM 2014

[5] A. Moulu, *Abusing Samsung KNOX to remotely install a malicious application*, Quarkslab, 2014

[6] G. Wilkinson, *The machines that betrayed their masters*, BH Mobile Security Summit, 2015

[7] C. Kasmi, J. Lopes Esteves, *Automated analysis of the effects induced by radio-frequency pulses on embedded systems for EMC safety*, AT-RASC, URSI, 2015

IMAGE CREDITS

dailymail.co.uk, jimmymacsupport.com, scene7.com, wonderhowto.com, eroelectronic.net, dryicons.com, webniraj.com, shopify.com, icon100.com, icon8.com, tagstation.com, wikipedia.org

Thank You

QUESTIONS ?

- Jose Lopes Esteves, jose.lopes-esteves@ssi.gouv.fr
- Chaouki Kasmi, chaouki.kasmi@ssi.gouv.fr