Whisper in the Wire:
Voice Command Injection Reloaded

Chaouki Kasmi & José Lopes Esteves
ANSSI, France

Hack In Paris - 30/06/2016
WHO WE ARE

Chaouki Kasmi and José Lopes Esteves

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

➢ Voice command interpreters

➢ Previous work: injection through headphones

➢ Back-door coupling: characterization

➢ Back-door coupling: exploitation

➢ Conclusion
Your phone hears...
VOICE COMMAND INTERPRETERS

Where?

Who?

What?

APIs
VOICE COMMAND INTERPRETERS

- Processing
  - OK GOOGLE
  - Voice recognition
  - Call Mom
  - <Cmd: Call Mom>

- Activation
  - Google
    - "Ok, google" version
  - Google
    - Regular version

Chaouki Kasmi & José Lopes Esteves
VOICE COMMAND INTERPRETERS

- **Authentication**
  - Depends on settings and OS
  - Voice recognition available
  - Pre-auth commands can be limited

- **E.g. Google settings**

  - **From any screen**: You can say "Ok Google" from any screen on your device if the screen is on or the device is charging.
  - **Always-on**: You can say "Ok Google" whether your screen is on or off on a Nexus 6, Nexus 9, or Samsung Note 4 device.
  - **Trusted voice**: When you say "Ok Google" from a secure lock screen and we're able to recognize the sound of your voice, you can ask Google to do things for you or visit sites without having to unlock your device manually.
VOICE COMMAND INTERPRETERS

- Personalize keyword
- Carefully choose available commands (esp. Pre-auth)
- Limit critical commands
- Voice recognition
- Enable feedbacks (sound, vibration…)
- Provide finer-grain settings to user

(a)flickr.com/photos/hikingartist
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][10], audible obfuscated commands [8]
- Remote and Silent Voice Command Injection by Smart IEMI [9]
Previous work on remote voice command injection

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

Hack In Paris 2015
PREVIOUS WORK – TECHNIQUE [9]

- Voice command injection with a radio signal by front-door coupling on headphones cables.
PREVIOUS WORK – IMPACT [9]

- Tracking
- Eavesdropping
- Cost abuse
- Reputation / Phishing
- Malicious app trigger/payload delivery
- Advanced compromising
**Limitations**

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

- Headphones required: considered as the main limitation.

- Distance between source and target limited by the minimal required field.

- Activation conditions of the voice interpreters and exploitation impact depend on the settings.
Is it possible to overcome these limitations?

Maybe, if we change our attack vector.
Analysis of back-door coupling mode to reach to the audio interface

Reaching the smartphones connected to the power network through the USB cable
EM waves propagation modes

<table>
<thead>
<tr>
<th>Radiated</th>
<th>Conducted</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="a" alt="Radiated" /></td>
<td><img src="b" alt="Conducted" /></td>
</tr>
</tbody>
</table>

(a)wikipedia.org  (b)teseq.com
ELECTROMAGNETIC WAVES II

- EM waves coupling modes

<table>
<thead>
<tr>
<th>Front-door antenna to antenna</th>
<th>Back-door antenna to cable</th>
</tr>
</thead>
</table>

(a) [Image of a front-door antenna connection](dailymail.co.uk)  
(b) [Image of a back-door antenna to cable](cdiscount.com)
BACK-DOOR COUPLING PATH

- Exemple of a target: Samsung Galaxy Nexus

Targeted point MIC IC

Point of entry USB connector

Charging port part on the PCB
BACK-DOOR COUPLING PATH

- Target
  - USB cable (A)

- Cable (A) connected to smartphones next to the smartphone microphone (B)

- Phenomenon (PCB teardown)
  - Isolation by-pass by parasitic coupling
  - A and B share the same Vcc and Gnd
BACK-DOOR COUPLING PATH

- Back-door coupling mode **exploitation**
  - Replace the antenna with an injection probe
  - Replace the antenna with a home-made coupler (PLC-like power circuit of PLC modems)
- Inject voice through conducted IEMI

![Injection probe (teseq.com)](image1)

![Home-made coupler](image2)

PLC: Power Line Communication

Chaouki Kasmi & José Lopes Esteves
Experiments for injection validation radiated case

Coupling frequencies = 80 - 100 MHz
Experiments for injection validation
radiated case

Wi-Fi

Faraday Cage

Audio streaming

AM – 80-108 MHz
SIGNAL INJECTION

➢ Experiments for injection validation conducted case

- Power network
- Wi-Fi
- Faraday Cage
- Audio streaming

Ex. Coupling frequency = 218 MHz
SIGNAL INJECTION

Experiments for injection validation conducted case

- Power network
- Malicious coupler / PLC
- Wi-Fi
- Audio streaming
- Faraday Cage

Ex. Coupling frequency = 218 MHz
TARGET CHARACTERIZATION

- Analysis of conducted interference bypassing the power charger of devices offline
  - Direct injection on devices under tests with a specific test fixture (common-mode injection P-N)

- Target with Wireless Mic
- Monitoring with VLC
- USB cable with data link
- USB cable without data link

Chaouki Kasmi & José Lopes Esteves
TARGET CHARACTERIZATION

USB cable without data link

USB cable with data link

AM modulation sweep: 0.01 – 20 kHz
fcw = 218 MHz
TARGET CHARACTERIZATION

- Analysis of conducted interference bypassing the power charger of devices online
Preliminary results

- Audio signal can be injected through the power network when:
  - Devices are charging through the LV network
  - Devices are charging through USB interfaces of a computer
  - Interpretable by voice command interfaces?

- Power injected
  - $< 500 \text{ mW}$!
  - Enough to get voice signal interpreted and command executed?
Exploitation of back-door coupling mode to inject voice commands

Controlling the smartphones connected to the power network through the USB cable
EXPLOITATION SCENARIOS

- Analysis of conducted interference by-passing the power charger of devices on-line

- Considered scenarios
  1. Charging through the power network
  2. Charging through the USB port of a computer connected to the LV network
  3. Direct injection through malicious USB charging device
SCENARIO I

➢ Charger on power network

(a) extremetal.com (b) phys.org (c) treehugger.com
SCENARIO I

- Target connected to the power network
  - With standard USB charger
- EM waves propagation path
  - Point of injection: the power network
  - By-pass transformers of the charger
  - By-pass high-pass filters of the charger
- Audio
  - Quality have to be high enough to be processed
SCENARIO I

- Demo
SCENARIO II

- Charging through USB on a computer connected to the power network

(a)makeuseof.com  (b)istockphoto.com
SCENARIO II

- Target connected to a computer’s USB port
- EM waves propagation path
  - Point of injection: the power network
  - By-pass transformers of the computer
  - By-pass high-pass filters of the computer
- Audio
  - Quality high enough to be processed
- Computer and peripherals should not be disturbed if possible
SCENARIO II

- Demo
SCENARIO II

Demo
SCENARIO III

➢ Custom malicious charging device
SCENARIO III

- Less propagation and filtering issues
- Phone model/brand can sometimes be determined by cable shape (Apple)
- Try different frequencies until feedback of keyword recognition

Demo:
- Injection in the USB cable, behind the charger
RESULTS

- Successful voice command injection
  - Target charging directly from the power network
  - Target charging through a computer
  - Audio signal processed by remote servers
  - Command executed by the target

- Computer still running

- No real impact of the type of USB cables
  - Charge only / charge + data
  - Some minor differences (Spectral analysis)
LIMITATIONS

- Power network
  - Topology
  - Devices connected

- Chargers
  - Frequency response
  - Filtering and signal degradation

- Target phone
  - PCB characteristics
    - Unexpected coupling interface with some devices…
  - Audio input sensitivity and filtering
Conclusion
CONCLUSION

- Longer distance to reach the targets
  - Power network is a good propagating structure for EM waves
  - Power emitted is less than the one required for the radiation case (< 500 mW)
- Source can have limited size
  - PLC-like transceiver
- No need for headphones
- Reachable targets: devices charging
CONCLUSION

- We proposed two remote voice command injection techniques:

<table>
<thead>
<tr>
<th></th>
<th>Radiated attack</th>
<th>Conducted attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coupling path</td>
<td>Front-door</td>
<td>Back-door</td>
</tr>
<tr>
<td>Propagation path</td>
<td>Air</td>
<td>Power lines</td>
</tr>
<tr>
<td>Pre-requisite</td>
<td>Headphones cable with microphone</td>
<td>USB cable</td>
</tr>
<tr>
<td>Required power</td>
<td>40W (2m) / 200W (5m)</td>
<td>0.5W (&gt;10m)</td>
</tr>
<tr>
<td>Source size</td>
<td>Backpack (SDR + CPU + amplifier + battery + antenna)</td>
<td>PLC coupler / Charger</td>
</tr>
<tr>
<td>Target type</td>
<td>Outdoor mobile</td>
<td>Indoor stationary</td>
</tr>
</tbody>
</table>

PLC: Power Line Communication
Both front-door and back-door coupling paths exploited
- Remote and silent voice command injection

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

Carefully choose voice command settings
CONCLUSION

Voice command interface is evolving:

- Default settings are more secure
- More activation options (opt-in for pwn)
- Voice recognition available
- Authentication/unlock mandatory for some privacy critical commands

But also:

- Increasing scope of possible actions
- Users get used to it and will slowly move away from security towards usability
- Voice recognition not mature
Appendix:

Reloaded Voice Command Injection
ON VOICE RECOGNITION

- Voice recognition on keyword for authentication is not mature yet
  - Only keyword analyzed
  - Command can be any voice
- Simple audio replay attack example:
  - Get voice samples from the victim
  - Forge a sample reconstructing the keyword
  - Play it to unlock the phone

- Demo
Thank You

We thank the manufacturers and the editors for their interesting feedback
REFERENCES


 QUESTIONS ?

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