

February 2021, Athens, Greece

# Non-conformal malware attacks on smartphones

8<sup>th</sup> Information Security  
conference



**Professor DIMITRIS GRITZALIS**  
**Director, MSc Programme in Information Systems Security**  
**Athens University of Economics & Business, Greece**

# The Malware World: Exciting & Dangerous

A STUDY SHOWED  
5 OUT OF 10  
MALWARE  
INSTANCES  
WERE WORMS  
SPREAD BY USB  
REMOVABLE DRIVES  
IN 2014.

## TYPES OF MOBILE MALWARE

MCAFFEE FOUND  
THAT 8% OF  
MOBILE DEVICES  
ARE INFECTED;  
387  
NEW THREATS  
EVERY MINUTE.

### ADWARE

Spyware that collects information about the user to relay to a third party for purchasing patterns. Usually disguised as a legitimate app.

### PHISHING

Websites that are set up to entice users to enter, then steal credentials and personal information.

### BOTS

Applications that can run in background undetected. Can be quite sophisticated and adaptable. May have capability to contact botmasters to execute commands.



### SPYWARE

Monitors, logs, and shares information with remote servers on personal activity – text messages, emails, phone calls, voice recordings, contact lists, location, pictures, status, etc. Six of the top 20 mobile malware of 2014 were spyware.

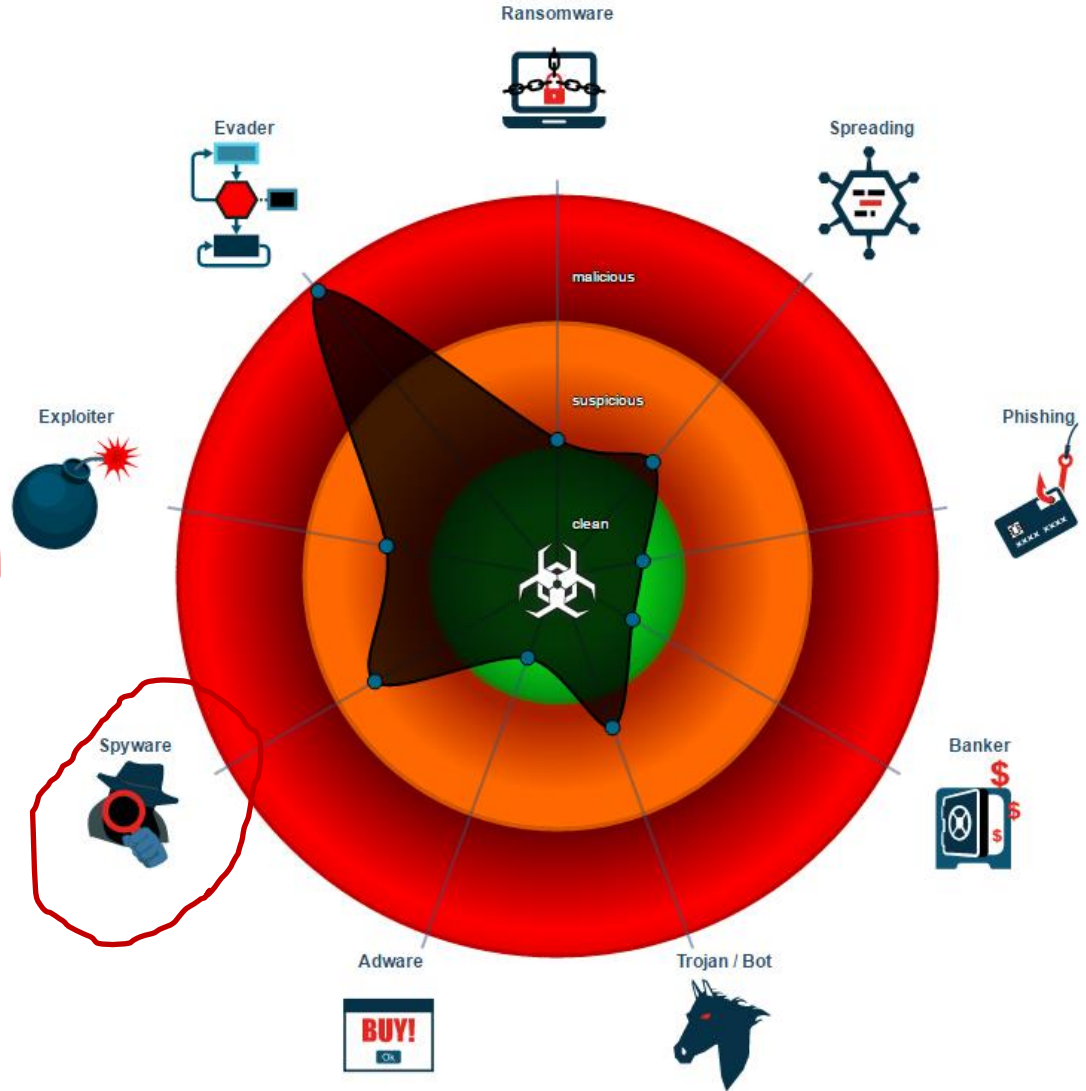
### TROJANS

Varying effects that can be mildly annoying or completely destructive. Usually are hidden and attached to applications that seem harmless. Ransomware is typically a member of this family of mobile malware. Can be quite sophisticated and adaptable.



LEARN MORE AT  
CHARGEDEFENSE.COM

SOURCES: McAfee Labs Threats Report, February 2015  
Microsoft Security Intelligence Report Volume 17, January - June 2014



# Malware & Smartphones: A risky co-existence

## CYBERSECURITY THREATS

RANK AS BIGGEST CHALLENGE IN 2017: IEEE SURVEY

Online security threats will be the biggest challenge for Chief Information Officers (CIOs) and Chief Technology Officers (CTOs) this year (45 percent), followed by the speed of technological change (18 percent) and regulation or compliance (11 percent), according to an IEEE survey of 300 U.S., U.K. and India CIOs and CTOs.

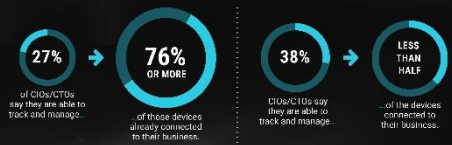


### DEVICE OVERLOAD

The global Internet of Things (IoT) market and installed base of connected devices – smartphones, tablets, sensors, printers, vehicles and more – is expected to increase dramatically to 30.7 billion devices in 2020, all potentially vulnerable to cyberattacks.



Today, there are already so many devices connected to businesses that:



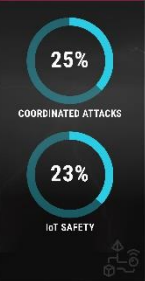
### TOP CYBERSECURITY THREATS

Workers are increasingly mobile, driving the growth of portable primary work devices. As such, among the top two concerns of CIOs and CTOs are cloud vulnerability and security issues related to employees bringing their own devices to work.

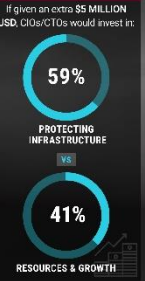


Other concerns include IoT security and mobile device vulnerability.

### MAJOR CONCERNS



### CONSIDERATIONS



### PREPARATIONS



### HACKING FOR GOOD

Whether highlighting flaws in order to improve security as a "white hat" hacker, teaching children to code, or through hackathons that unite coders and designers to expose problems before a public software release.

A STRONG MAJORITY OF CIOs AND CTOs BELIEVE HACKING CAN BE USED IN A POSITIVE WAY



To learn about cybersecurity vulnerabilities and advances, visit [transmitter.ieee.org/ieee-cyber-security](http://transmitter.ieee.org/ieee-cyber-security)



## A MOBILE MENACE: TRENDS IN MOBILE THREATS

### THE REALITIES

**2.5X** A USER IS 2.5 TIMES AS LIKELY TO DOWNLOAD AN APP WITH ANDROID MALWARE NOW COMPARED TO THE BEGINNING OF THE YEAR.

IN JUST THE FIRST HALF OF 2017, THE NUMBER OF UNIQUE ANDROID APPS WITH MALWARE WENT FROM 80 TO 400.



**10S OF THOUSANDS** MALWARE DETECTIONS PER MONTH

**THOUSANDS** MALWARE DETECTIONS PER DAY

### PHISHING FOR USERS

**3 IN 10** PEOPLE ARE LIKELY TO CLICK ON AN UNSAFE LINK ON THEIR MOBILE DEVICE.

### CATEGORY BREAKDOWN OF UNSAFE LINKS OPENED BY MOBILE USERS



**3 X** PEOPLE ARE 3 TIMES MORE LIKELY TO SUCCEED TO A PHISHING ATTACK FROM THEIR PHONE THAN ON A DESKTOP COMPUTER.

### TOP TYPES OF APPS THAT HAVE BEEN BUNDLED WITH MALWARE



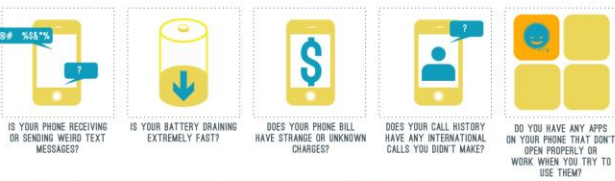
### TOP THREE ANDROID THREATS



WHAT CAN HAPPEN IF A USER DOWNLOADS AN APP WITH THIS MALWARE?



### HOW TO TELL IF YOUR PHONE MIGHT BE INFECTED WITH MALWARE



SOURCES: mylookout.com; Trustlook.com



## CYBER SECURITY

### Top 5 cyber threats

#### 1 Malware

Software specifically designed to gain access to a device or damage it without the owner knowing

#### Top malware families by type:



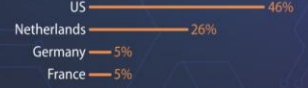
**92%** of detected malware infections came through compromised email

Increasingly targets IoT (Internet of Things) devices

#### 2 Web-based attacks

All available techniques regarding redirection of web browsers to malicious web sites

#### Top four source countries:



Incidents involving Content Management Systems (CMS) are increasing

#### 3 Web application/injection attacks

Feeding vulnerable servers and/or mobile apps with malicious inputs with the objective of injecting malicious code

**51%** - SQL injection is the most common attack

Often linked to major data breaches worldwide

#### 4 Phishing

Attempt to steal/intercept user names, passwords and financial credentials by combining spoofed emails and counterfeit web sites

#### Responsible for more than:



Phishing attacks on mobile devices have grown by an average of **85%** year-over-year since 2011

#### 5 DDoS

(Distributed) Denial of Services targets businesses and organisations by making system or networks unavailable to its intended users

**59%** of attacks take place in China

**55%** of attacks last less than 90 minutes

Source: European Union Agency for Network and Information Security (2019)



# A new\* non-conformal malware attack

## An Android-focused paradigm

Dropping malware modules to multiple Android smartphones, over the air and from a distance, using a sound medium\*\*.



\* Based on: G. Stergiopoulos, D. Gritzalis, A. Anagnostopoulou, E. Vasilellis, "Dropping malware through sound injection: A comparative analysis on Android operating systems", November 2020 (submitted).

\*\* Similar to **Shazam**'s audio fingerprinting.

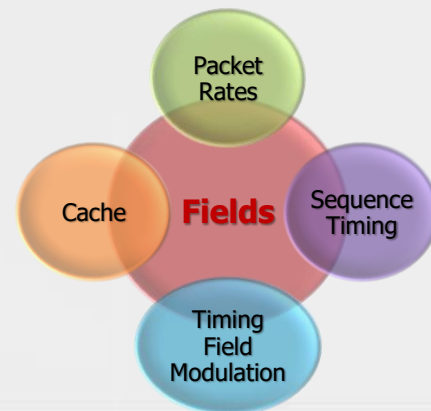
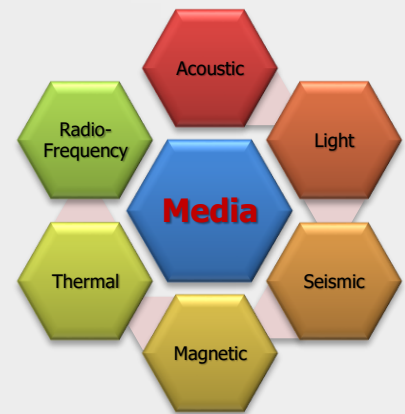
# Trojan Droppers & Covert Channels

## Trojan Dropper

- Carrier or delivery vehicle for the **payload** to be dropped.
- **Open a way** for attack (download and install core malicious modules).
- Among the top **worst malware** threats (especially for **Android**).
- Network channels are hardened to avoid droppers delivering their payloads (paving the way for **alternative routes of infiltration**).

## Covert Channel

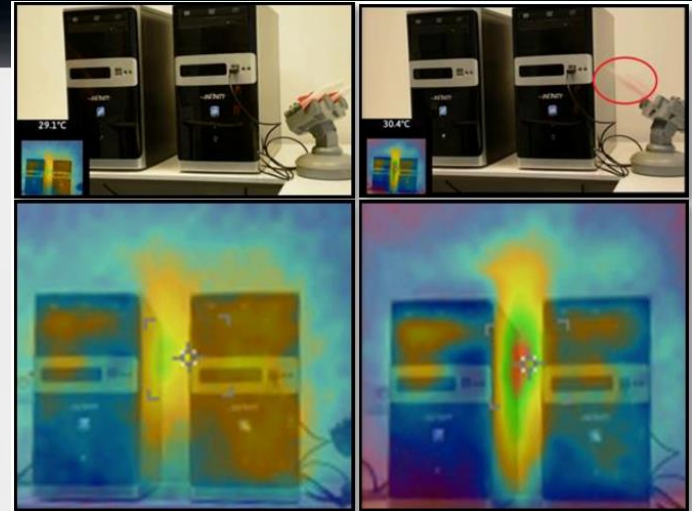
- Mechanism **not designed** for communication.
- Can be abused to transfer information objects between processes **not supposed** to communicate.
- Form the basis of **nonconformal** attacks, by utilizing different **Fields** and exploit various **Media**.



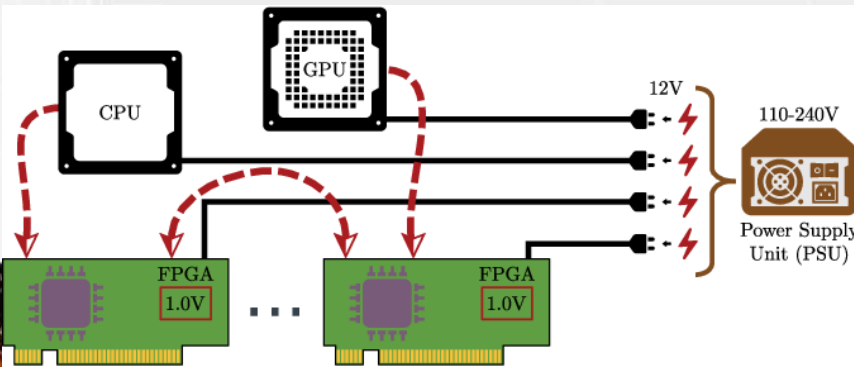
# The Non-conformal Attack Space: Examples



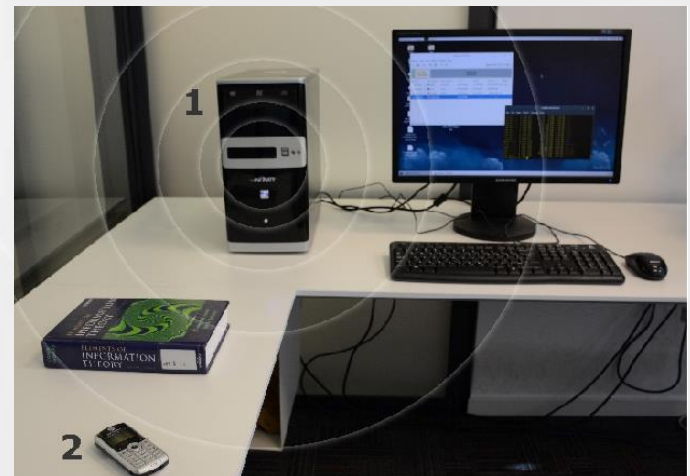
**AirHopper (2014):** Data exfiltration from air-gapped computers over FM frequencies.



**BitWhisper (2015):** Covert signaling between air-gapped computers using thermal manipulations.



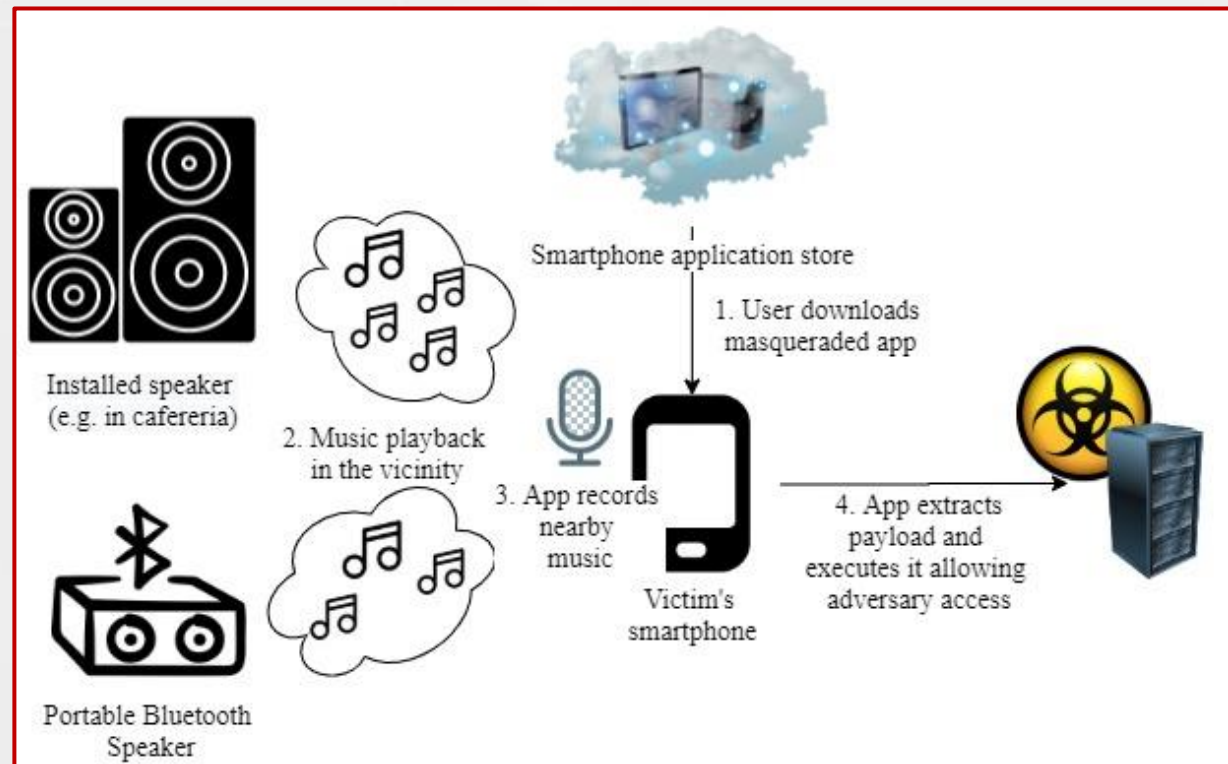
**C<sup>3</sup>APSULE (2020):** Data leakage across FPGA via voltage-dependent channels.



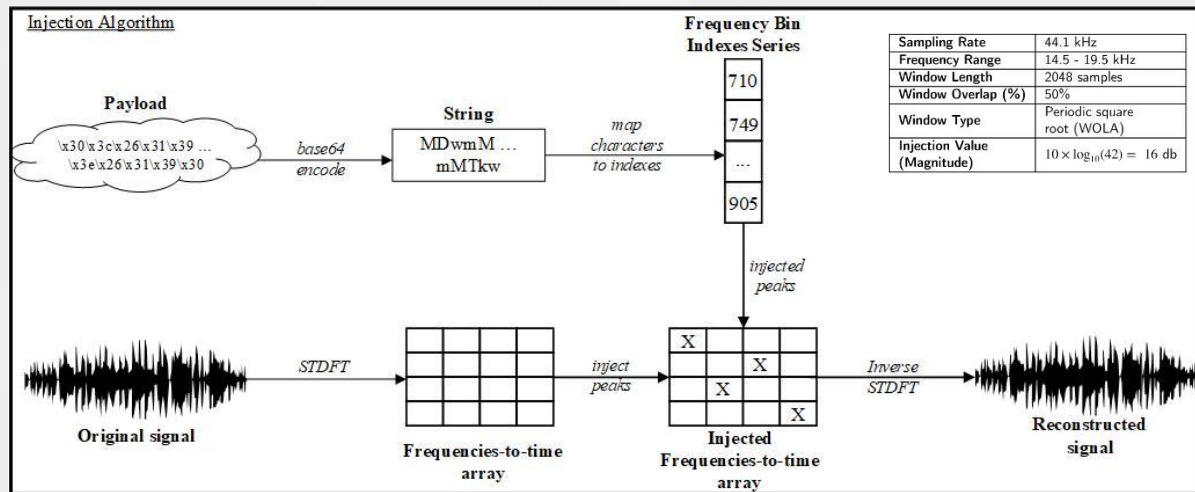
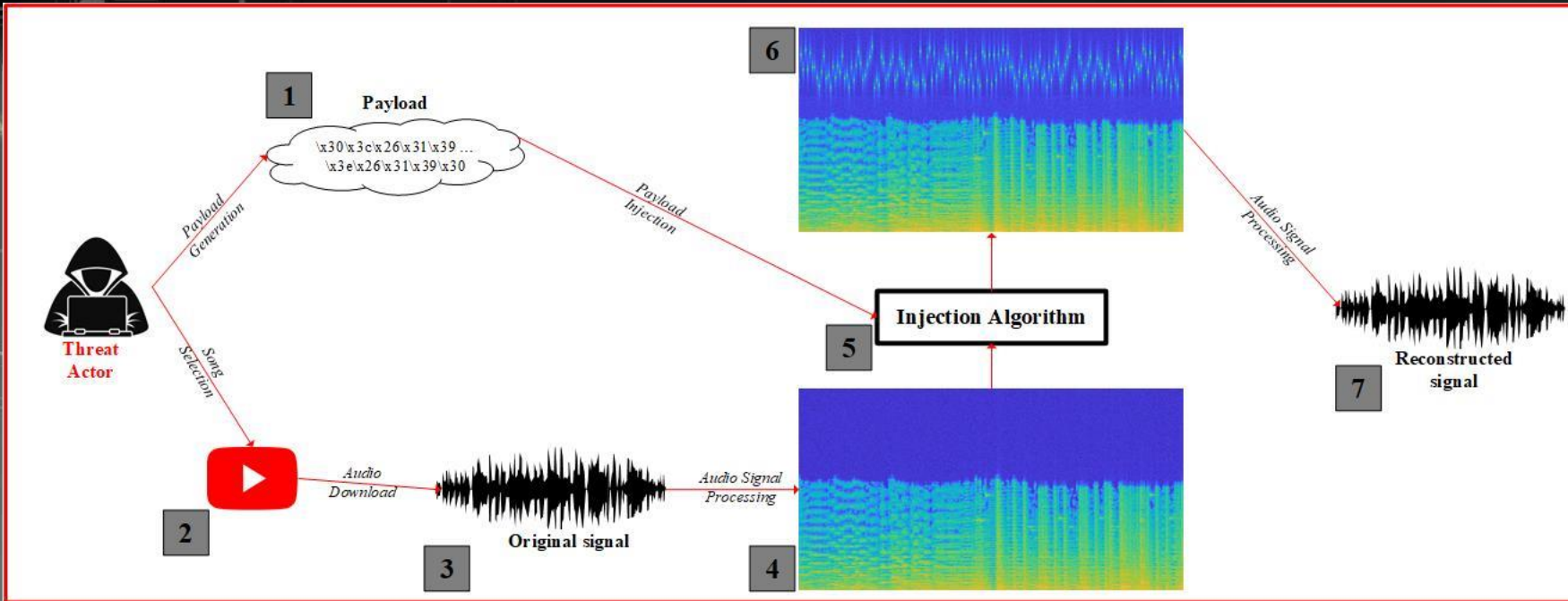
**GSMem (2015):** Data exfiltration from air-gapped computers over cellular frequencies.

# Dropping Malware through Sound Injection

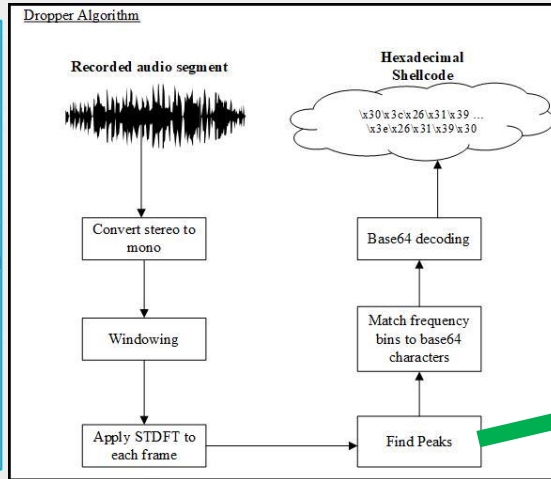
- ✓ A malware is **concealed** within music's inaudible frequencies.
- ✓ A dropper software masquerades as a **smartphone application** needing microphone access.
- ✓ Injected music is **played back** near the smartphone with a **dropper app installed**.
- ✓ Attacker **takes control** of an Android device and **acts maliciously** using Meterpreter commands (**take photo, display running process, search for a file, record sound, etc.**).



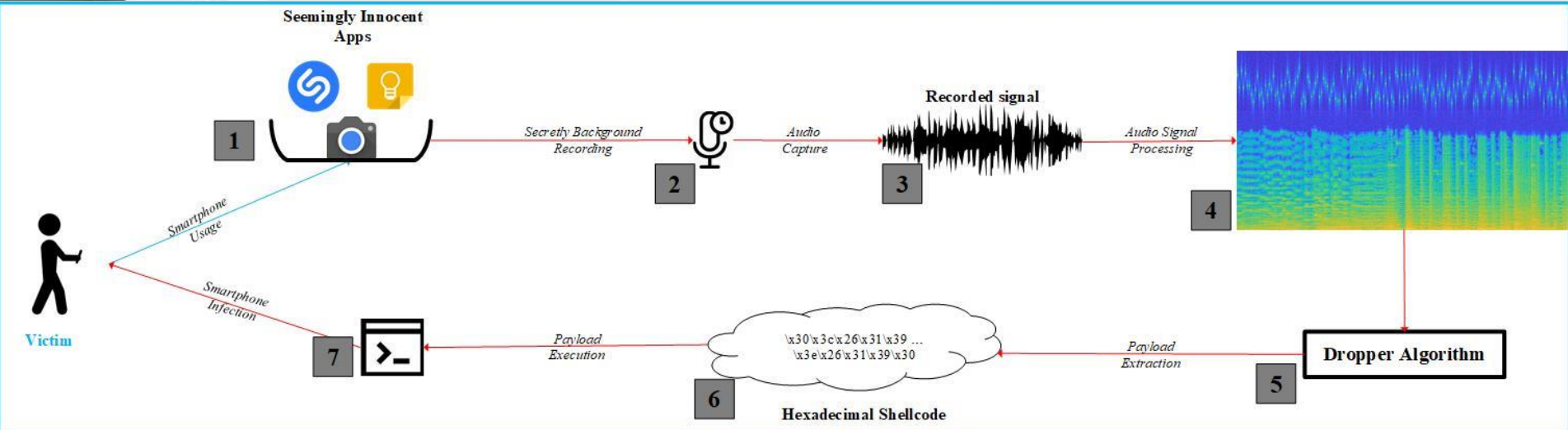
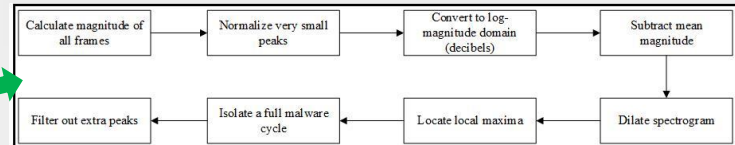
# Attack Anatomy: Malware Injection Process



# Attack Anatomy: Malware Dropping Process



Sampling Rate	44.1 kHz
Frequency Range	14.5 - 19.5 kHz
Window Length	2048 samples
Window Overlap (%)	50%
Window Type	Periodic square root (WOLA)
Injection Value (Magnitude)	$10 \times \log_{10}(42) = 16 \text{ db}$

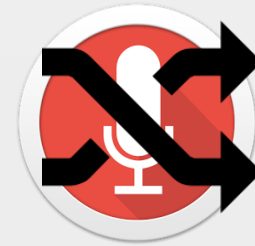


# Attack Evaluation: Experiments



Injection of a 65-byte Meterpreter reverse TCP payload to 22 songs

- Variety of music genres/languages (*e.g, rock, pop, folk, English, Greek, etc.*)

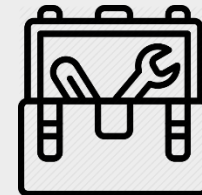


Random recordings on each song



Recording duration: 20 sec

- 2 x payload's length - first symbol



Equipment

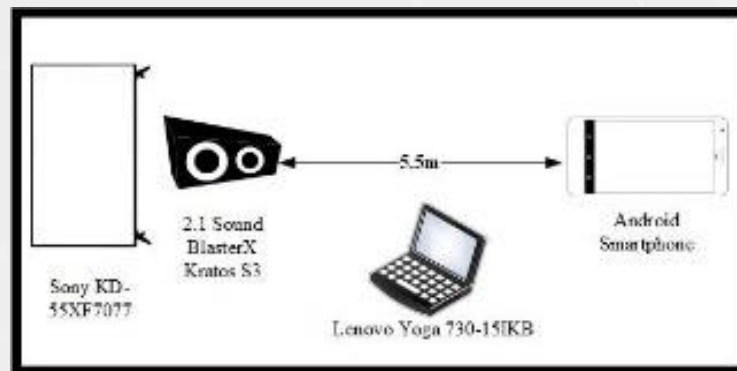
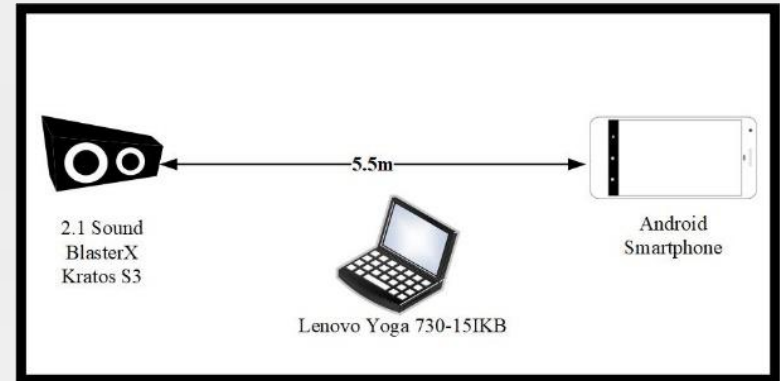
- Inexpensive non-professional off-the-shelf speakers
- 3 different smartphone manufacturers
- Various versions of Android OS



# Attack Evaluation: Environment & Settings

## Quiet Environments

- Only ambient music being played-back
- Speaker Volume: 4-26 DBm
- Recording Distance: 0.5-10 m



## Noisy Environments

- Random background noise through a smart TV or/and people chatter
- TV Volume: 4.4-44 DBm
- Recording Distance: 0.5-10 m



# Attack Evaluation: Performance Analysis

Comparative analysis of **Smartphones** (average performance)

Distance	Huawei P30 Pro <i>(brand new)</i>		Xiaomi Redmi Note 4 <i>(moderately used)</i>		Samsung A6+ <i>(heavily used)</i>	
	Quiet Environment	Noisy Environment	Quiet Environment	Noisy Environment	Quiet Environment	Noisy Environment
≤2.5m	100%	97%	95%	94%	95%	94%
≤6.5m	88%	84%	86%	80%	79%	76%
≤10.5m	75%	69%	75%	65%	61%	57%

Comparative analysis of **Environments** (average performance)

Distance	Quiet Environments		Noisy Environments	
	Minimum Success Rate	Maximum Success Rate	Minimum Success Rate	Maximum Success Rate
≤2.5m	91%	100%	91%	100%
≤6.5m	72%	82%	69%	77%
≤10.5m	55%	82%	49%	73%

**Best performance:** 82.8% quiet places, 78.1% noisy ones.



# Indicative Countermeasures



## Audio Source Level

- **High-peak compression and modulation** of sound-based channel frequencies.
- **Filtering and compression** of audio files to distort any existing ultrasonic frequencies as they pass through the amplifier.

## Smartphone Device Level

- Programmers: Not use **unnecessary background** activities in application.
- Users: **Decide** about permissions for sensor access when installing an application.
- Manufacturers: **Set microphone sensitivity <15kHz**, to avoid capturing inaudible frequencies.

## The Risks Behind the Apps

### Malicious Behaviors

- Accesses device management and restricted security APIs unnecessarily
- Accesses or requests Super User permissions
- Exploits operating system or zero-day vulnerabilities
- Roots or jailbreaks device
- Steals login credentials
- Communicates with known malicious IP addresses and domains

### Moderate Risk Behaviors

May be a risk if performed by apps from unknown or untrusted sources

- Reads and Sends emails
- Reads and Sends SMS messages
- Reads and sends GPS information

### Dangerous Behaviors

- Uploads user information without permission or without notifying user
  - Upload address book without notifying user
  - Reads SMS messages and sends them off the device
  - Reads emails and sends them off the device
  - Reads browser history and sends it off the device
- Includes SSL vulnerabilities that enable communications to be intercepted
- No privacy policy or refers to an invalid privacy policy
- Installs boot-time startup item



# Overview and conclusions

A new\* **non-conformal malware** attack on **Android** smartphones:

## Scope:

- An **over-the-air payload dropping/injection** attack on smartphones, non corrupting the original audio signal.

## Viability affected by:

- **Hardware:** (i) microphone quality/sensitivity of different manufacturers, (ii) poor device handling, (iii) extended mobile use.
- **Surrounding:** (i) poor acoustics, (ii) type of background noise, (iii) low speaker's DB volume.

## Environment:

- Duration: A **20 sec recording** is needed for Meterpreter payloads.
- Effective distance: **4-5 m** away from the music source.

\* Based on: G. Stergiopoulos, D. Gritzalis, A. Anagnostopoulou, E. Vasilellis, "Dropping malware through sound injection: A comparative analysis on Android operating systems", November 2020 (submitted).



## References

1. Carrara, B., Adams, C., “On acoustic covert channels between air-gapped systems”, in *International Symposium on Foundations and Practice of Security*, pp. 3-16, Springer, 2014.
2. Deshotels, L., “Inaudible sound as a covert channel in mobile devices”, in *8<sup>th</sup> USENIX Workshop on Offensive Technologies*, 2014.
3. Iliadis, J., Gritzalis, D., Spinellis, D., Preneel, B., Katsikas, S., “Evaluating certificate status information mechanisms”, in *7<sup>th</sup> ACM Computer and Communications Security Conference*, pp. 1-9, ACM Press, 2000.
4. Goodin, D., “Meet “badBIOS,” the mysterious Mac and PC malware that jumps airgaps”, *ars technica*, Vol. 31, No. 10, 2013.
5. Guri, M., Monitz, M., Mirski, Y., Elovici, Y., “Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations”, in *28<sup>th</sup> IEEE Computer Security Foundations Symposium*, pp. 276-289, IEEE, 2015.
6. Guri, M., Kachlon, A., Hasson, O., Kedma, G., Mirsky, Y., Elovici, Y., “GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies”, in *24<sup>th</sup> USENIX Security Symposium*, pp. 849-864, 2015.
7. MalwareBytes Labs, Trojan.dropper. <https://blog.malwarebytes.com/detections/trojan-dropper/>
8. Mylonas, A., Dritsas, S., Tsoumas, B., Gritzalis, D., “Smartphone security evaluation: The malware attack case”, in *International Conference on Security and Cryptography*, pp. 25-36, IEEE, 2011.
9. Mylonas, A., Gritzalis, D., Tsoumas, B., Apostolopoulos, T., “A qualitative metrics vector for the awareness of smartphone security users”, in *International Conference on Trust, Privacy and Security in Digital Business*, pp. 173-184, Springer, 2013.
10. Mylonas, A., Kastania, A., Gritzalis, D., “Delegate the smartphone user? Security awareness in smartphone platforms”, *Computers & Security*, Vol. 34, pp. 47-66, 2013.
11. Mylonas, A., Meletiadiis, V., Mitrou, L., Gritzalis, D., “Smartphone sensor data as digital evidence”, *Computers & Security*, Vol. 38, pp. 51-75, 2013.
12. Mylonas, A., Theoharidou, M., Gritzalis, D., “Assessing privacy risks in android: A user-centric approach”, in *International Workshop on Risk Assessment and Risk-driven Testing*, pp. 21-37, Springer, 2013.
13. Rasmussen, K., Giechaskiel, I., Szefer, J., “CAPSULE: Cross-FPGA covert-channel attacks through power supply unit leakage”, in *IEEE Symposium on Security and Privacy*, Vol. 1, USA, 2020.
14. Theoharidou, M., Kandias, M., Gritzalis, D., “Securing transportation-critical infrastructures: Trends and perspectives”, *7<sup>th</sup> IEEE Conference on Global Security, Safety and Sustainability*, pp. 171-178, Springer, 2012.
15. Wang, A., “An industrial strength audio search algorithm”, *Ismir*, pp. 7-13, 2003.