

Wanna TEMPEST your computer?

Florian Barbarin, Maxime Gagliardini and Guillaume Squillaci

TLS-SEC

March 12, 2018



TLS-SEC

Toulouse
Hacking
Convention

Table of contents

Introduction

Transmitter

Receiver

Data exfiltration

Conclusion

"Project long" background

THC 2018 Challenge

- Prepare tutorial challenge
- Work based on *GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies* (24th USENIX Security Symposium)
- "Challenge" : data exfiltration from an air-gapped computer
- "Tutorial" : guide the challenger step-by-step
- Idea : follow how we succeed to reproduce a part of the paper

Electromagnetic emanations

Emanations

- Each electronic device has emanations
- Could be electronical, acoustical, mecanical or electromagnetical
- We focused on electromagnetic emanations

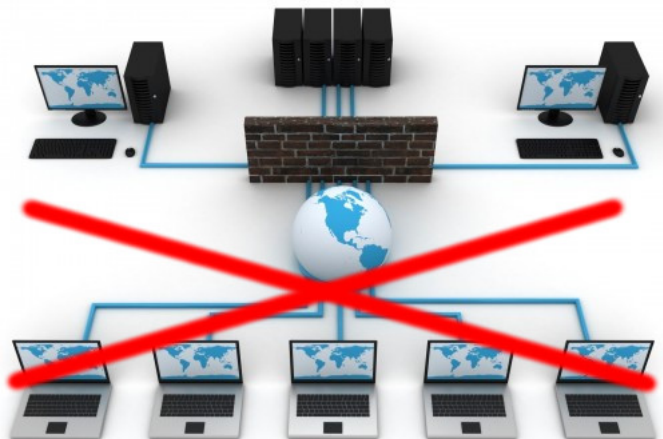
TEMPEST

- Name given by NSA for standards protecting against electromagnetic emanations
- Context : EMSEC, surbpart of COMSEC

Air-gapped networks



Air-gapped networks



Data exfiltration

Devices

- 1 air-gapped computer (attacked computer)
- 1 standard computer (attacker's computer)

Tools

- Spectrum analyzer
- Software-defined radio : USRP/RTL-SDR
- Antennas
- Softwares : URH/GNURadio

Goal

Transfer a password from the air-gapped computer to the attacker's computer creating a covert channel.

Table of contents

Introduction

Transmitter

Receiver

Data exfiltration

Conclusion

Test

test

- test

Table of contents

Introduction

Transmitter

Receiver

Data exfiltration

Conclusion

Test

test

- test

Table of contents

Introduction

Transmitter

Receiver

Data exfiltration

Conclusion

Test

test

- test

Table of contents

Introduction

Transmitter

Receiver

Data exfiltration

Conclusion

Test

test

- test