Wanna TEMPEST your computer?

Florian Barbarin, Maxime Gagliardini and Guillaume Squillaci

TLS-SEC

March 12, 2018

Table of contents

"Projet long" context

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 form an air-gapped computer
- "Tutorial" : guide the challenger step-by-step
- Main idea : follow how we succeed to reproduce a part of the paper

Air-gapped networks

Air-gapped networks

Electromagnetic emanations

Emanations

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

TEMPEST

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

Challenge context

Goal
Get a password stored on the air-gapped computer

Problem
Air-gapped computer $\implies$ no possibility to gain access and/or exfiltrate data via network

Solution
Use electromagnetic emanations to create a covert channel and exfiltrate data

Technical environment

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

Table of contents

Test

test

- test

Table of contents

Test

test

- test

Table of contents

The Malware

Idea

- Same skeleton than the Transmission section
- 1bit/s to reduce error rate

What is transmitted ?

- The message : a file in argument
- End of File
- A pattern to localize the message : 11111111
- All of this in an infinite loop

The Reception

In GNU Radio

- Start the malware before the acquisition to avoid a bug in the first bit transmitted
- Wait around 2 minutes

Conversion of the GRC file into our flag

- Localize a first pattern
- Extract bytes from this pattern until the next one
- Convert extracted bytes into ASCII and print it

The Reception

```c
void extract_msg(FILE * fic, char * msg, char * pattern)
{
  char chaine[TAILLE_MAX],
       tmp1[TAILLE_MAX],
       *tmp2,
       tmp3[TAILLE_MAX]="",
       *tmp4,
       bin[TAILLE_MAX]="";

  while (fgets(chaine, TAILLE_MAX, fic) != NULL)
  {
    memset (tmp1, 0, sizeof (tmp1));
    strncpy(tmp1, chaine+10, 55);
    rem_space(tmp1);
    strcat(bin, tmp1);
  }
  tmp2 = strstr(bin, pattern);
  strcpy(tmp3, tmp2+strlen(pattern));
  tmp4 = strstr(tmp3, pattern);
  strncpy(msg, tmp3, tmp4-tmp3);
}
```

Table of contents

Conclusion

Researchers work

- Better equipment
- Signal processing optimization
- Reception until 30m

Limits

- Very limited flow rate to prevent error
- Can be improve with a frequency modulation (attack USBee)

Countermeasures

- Faraday cage
- Zonal approach
- Antivirus