Etherify

Leak data from an air-gapped computer

Pierre AYOUB

May 01, 2023

Source

- Jacek Lipkowski, SQ5BPF, 2020
- `https://github.com/sq5bpf/etherify`

Goal

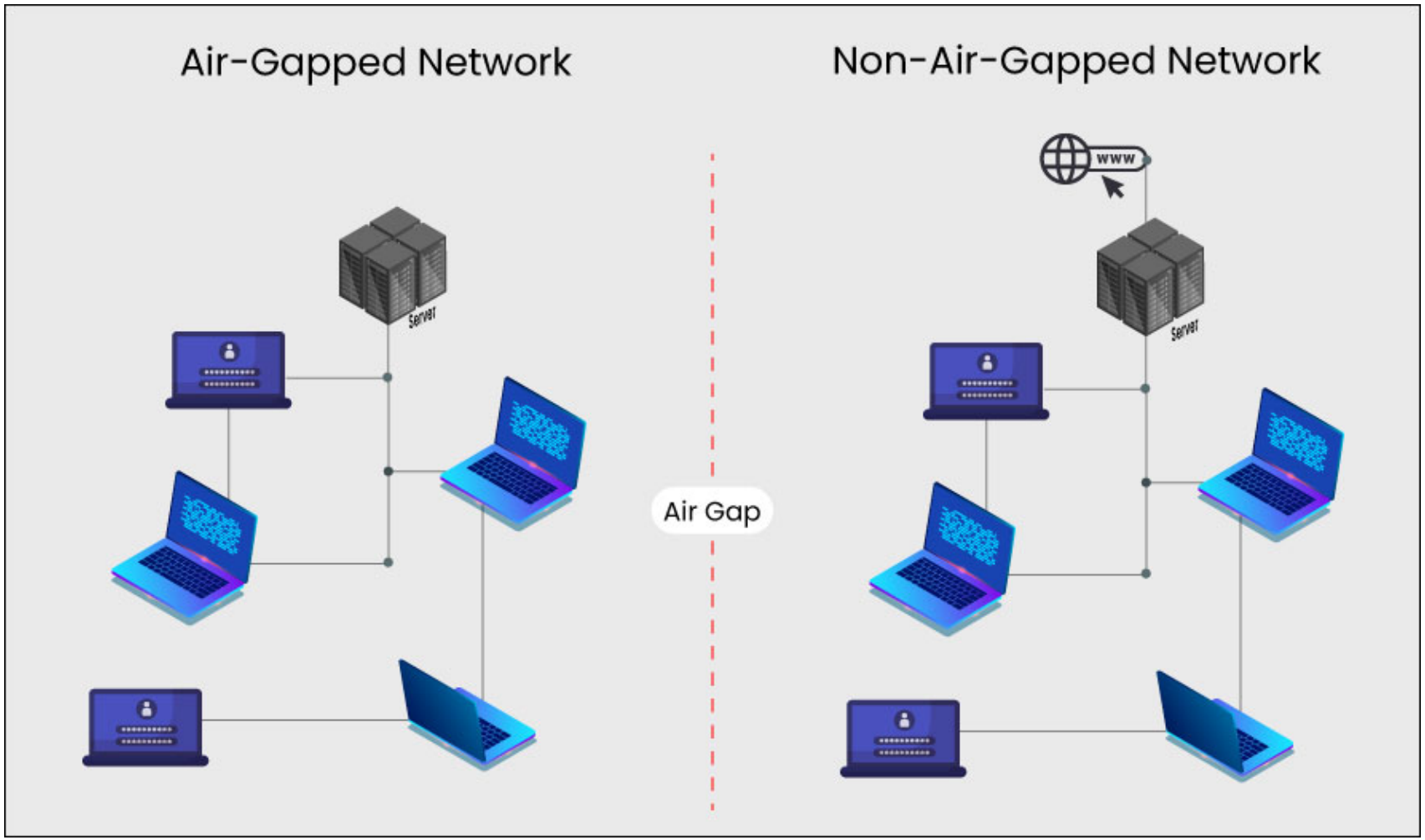

Figure: Illustration of an air-gapped network

Leak source

Ethernet cable

- 4 twisted pair lines

Leak source

Ethernet cable

- 4 twisted pair lines
- Carries conducted RF signals from 1 to 1000 MHz range

Leak source

Ethernet cable

- 4 twisted pair lines
- Carries conducted RF signals from 1 to 1000 MHz range
- Imperfections leads to radiated EM signals

Leak control

Software

- `ethtool` allows to change Ethernet mode.

Encoding

Ethernet modes:

10BASE-T Manchester Encoding, 10 MHz symbol rate
-> Space signal (logical 0).

Encoding

Ethernet modes:

10BASE-T Manchester Encoding, 10 MHz symbol rate
-> Space signal (logical 0).

100BASE-T 4B5B Encoding & NRZI, 125 MHz symbol rate
-> Mark signal (logical 1).

Encoding

Ethernet modes:

10BASE-T Manchester Encoding, 10 MHz symbol rate
-> Space signal (logical 0).

100BASE-T 4B5B Encoding & NRZI, 125 MHz symbol rate
-> Mark signal (logical 1).

- We can turn Ethernet modes to Morse code!

Encoding

Ethernet modes:

10BASE-T Manchester Encoding, 10 MHz symbol rate
-> Space signal (logical 0).

100BASE-T 4B5B Encoding & NRZI, 125 MHz symbol rate
-> Mark signal (logical 1).

- We can turn Ethernet modes to Morse code!
- No packets -> send an idle sequence
  -> we receive a constant signal!