Radio-Frequency Retroreflector Attacks:

Multi-trojan scenario and attacks through a disordered media

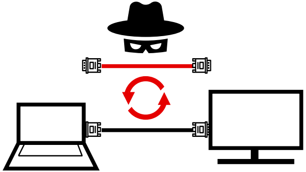
GRANIER Pierre & SARRAZIN François {firstname.lastname}@univ-rennes.fr

Our problematic :

An attacker swaps a cable to later monitor it remotely.
The cable is swapped following an :

Attack scenario :

- Evil maid attack
- Supply chain attack

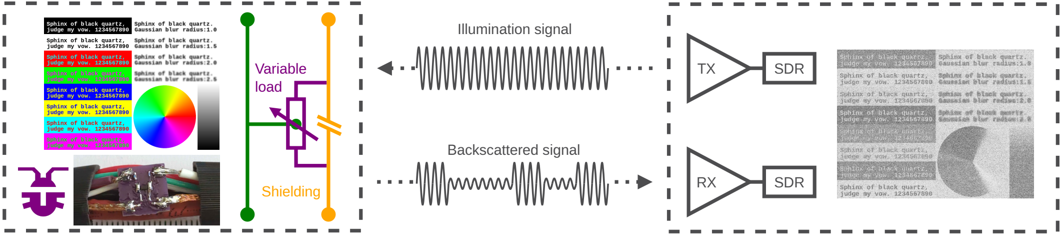


The modified cable does not emit anything, yet, the attacker can monitor it. How !?

Monochrome VGA RFRA

Secret data changes the state of a retroreflector variable load.

Retroreflector states modulate the backscattered illumination signal.

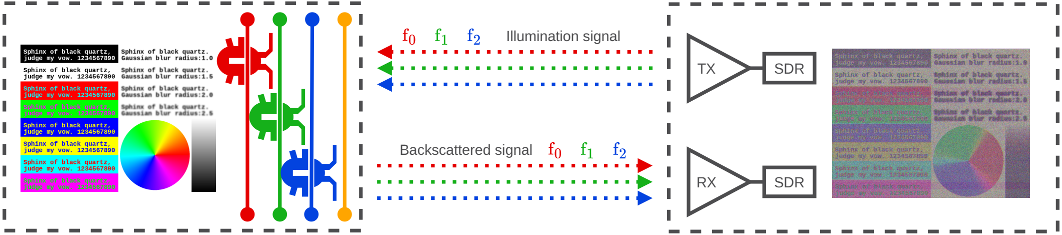

Sphinx of black quartz, judge my vow. 1234567890
Sphinx of black quartz. Gaussian blur radius:1.0
Sphinx of black quartz. Gaussian blur radius:1.5
Sphinx of black quartz. Gaussian blur radius:2.0
Sphinx of black quartz. Gaussian blur radius:2.5
Variable load
Shielding
Illumination signal
Backscattered signal
TX
SDR
RX
SDR

At a few meters we can recover data, but only the color probed by the implant.

(Demonstration running after the presentations.)

RGB VGA RFRA

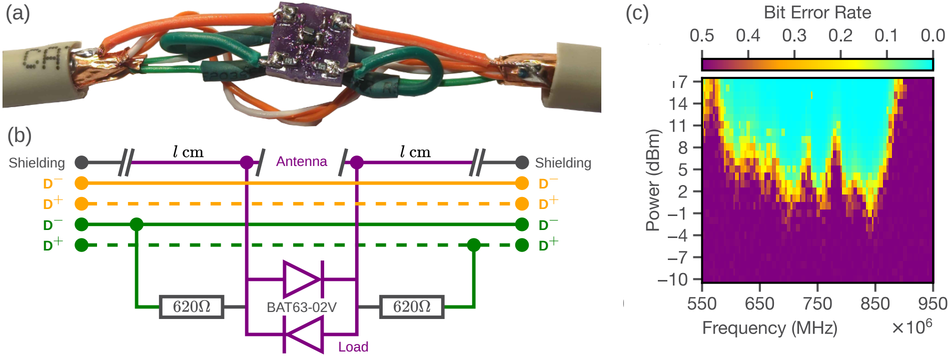
The previous methodology can be adapted to allow interrogation of multiple implants.


Sphinx of black quartz, judge my vow. 1234567890
Sphinx of black quartz. Gaussian blur radius:1.0
Sphinx of black quartz. Gaussian blur radius:1.5
Sphinx of black quartz. Gaussian blur radius:2.0
Sphinx of black quartz. Gaussian blur radius:2.5
f_0 f_1 f_2
Illumination signal
Backscattered signal
f_0 f_1 f_2
TX
SDR
RX
SDR

To discriminate between implant we used the phase difference due to them being not co-located. (More details in our poster)

100BASE-TX RFRA

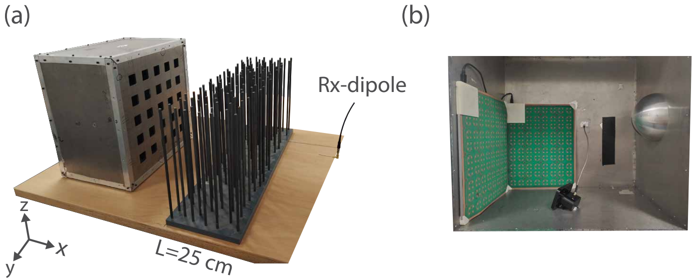
We also made a PoC for ethernet 100BASE-TX (125 Mbit/s).



Measurements made at a distance of 4 m in an anechoic chamber.

Attacks through a disordered media

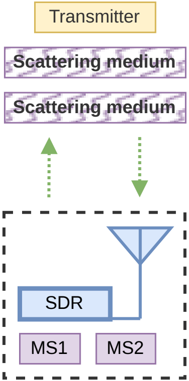
Focalization using a cavity containing two metasurfaces.



The metasurfaces create an array of 152 programmable pixels, each configuration shaping the wavefront coming out of the cavity.

Attacks through a disordered media - Focalization

Compared to a simple horn antenna we get around 15 dB when focalizing on transmitter behind 50 cm of disordered media.



Transmitter

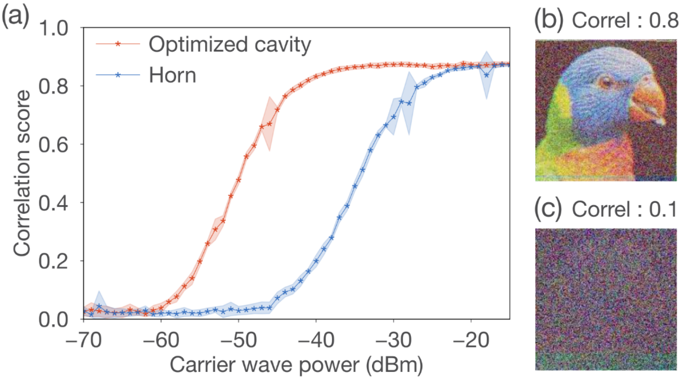
Scattering medium

Scattering medium

SDR

MS1

MS2


(a)
Optimized cavity
Horn
Correlation score
Carrier wave power (dBm)
(b) Correl : 0.8
(c) Correl : 0.1