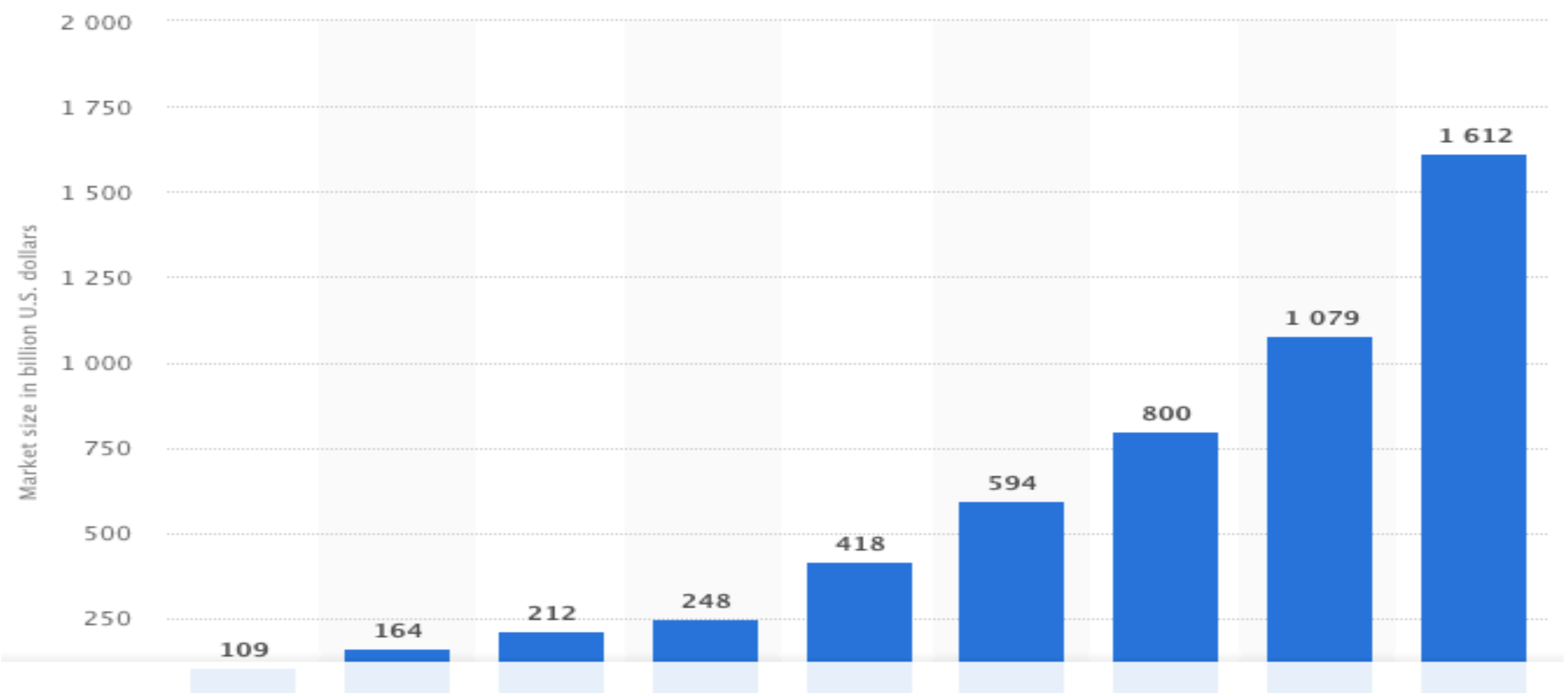
ETU "LETI"
SAINT PETERSBURG ELECTROTECHNICAL UNIVERSITY

Exploring Vulnerabilities of Pet Wearables to Side-Channel Attacks

Dr. Alla Levina

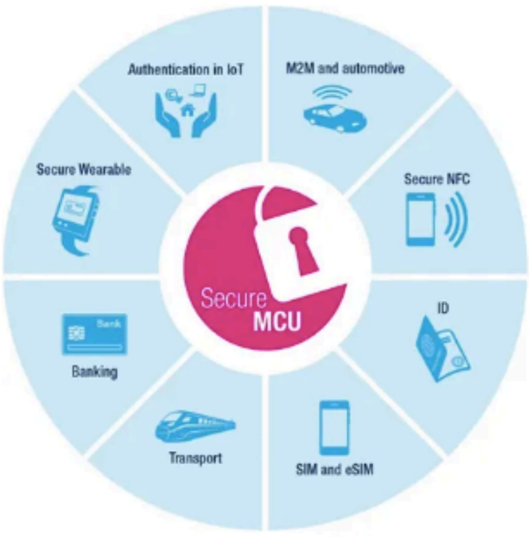
IoT

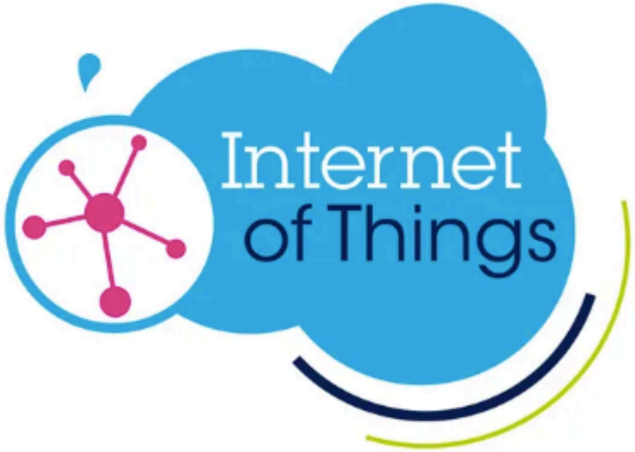
Size of the Internet of Things (IoT) market worldwide from 2017 to 2025 (in billion U.S. dollars)



IoT

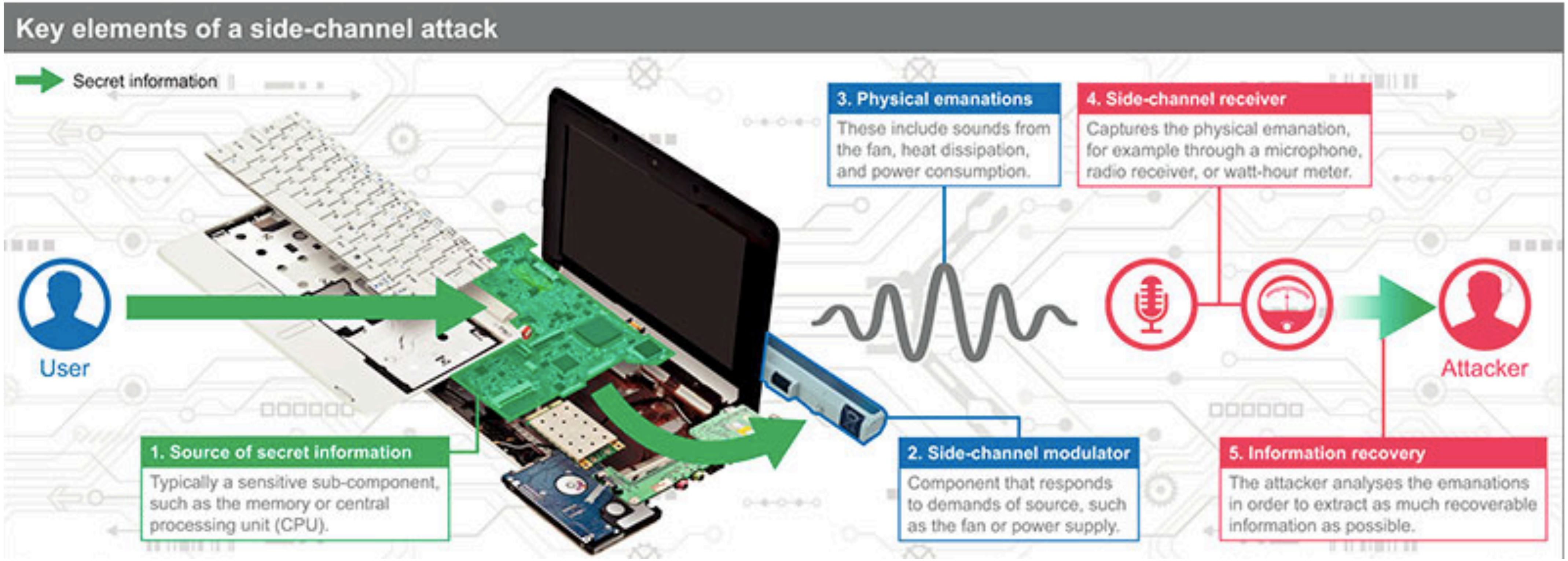
July 29, 2018





Side- Channel Attacks

Introduced in 1996 «Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems» by Paul Kocher.



Key elements of a side-channel attack

3. Physical emanations

These include sounds from the fan, heat dissipation, and power consumption.

4. Side-channel receiver

Captures the physical emanation, for example through a microphone, radio receiver, or watt-hour meter.

1. Source of secret information

Typically a sensitive sub-component, such as the memory or central processing unit (CPU).

2. Side-channel modulator

Component that responds to demands of source, such as the fan or power supply.

5. Information recovery

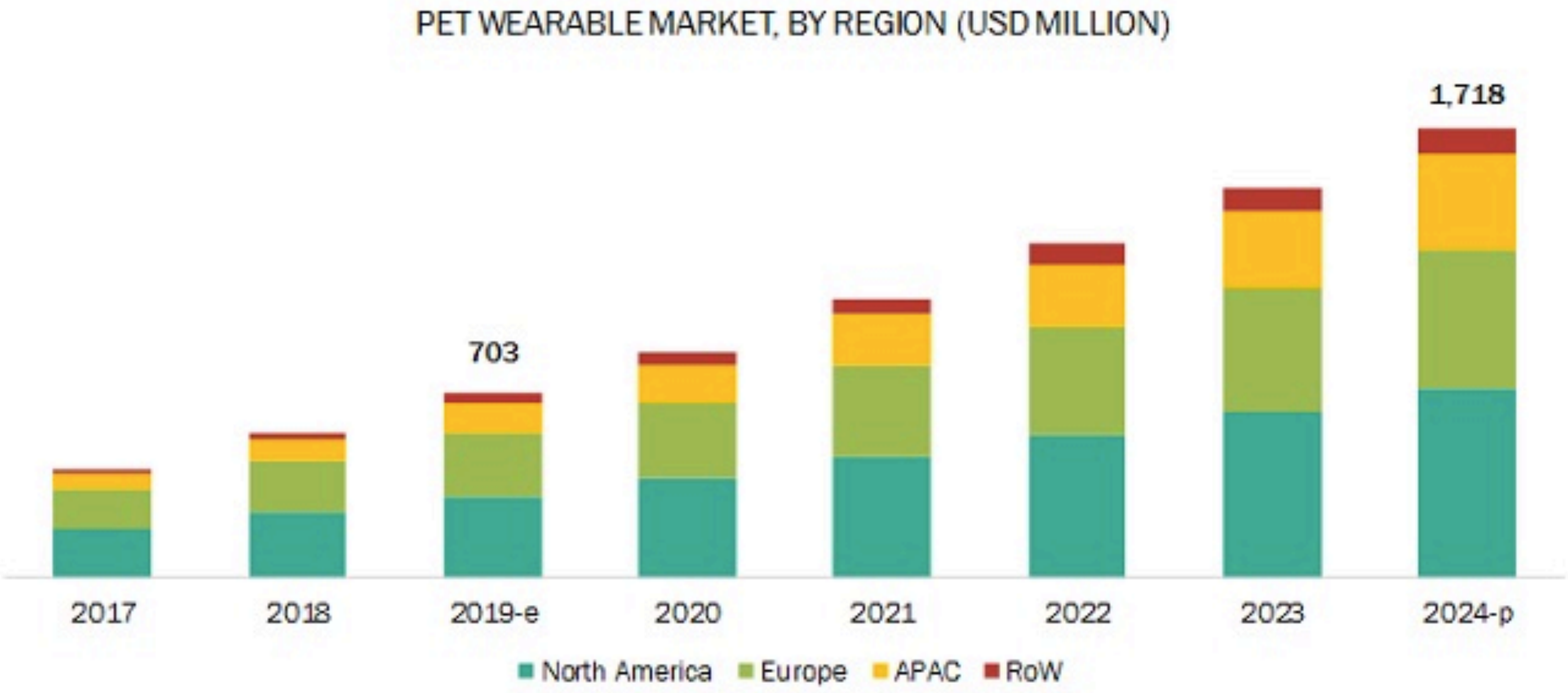
The attacker analyses the emanations in order to extract as much recoverable information as possible.

Side- Channel Attacks

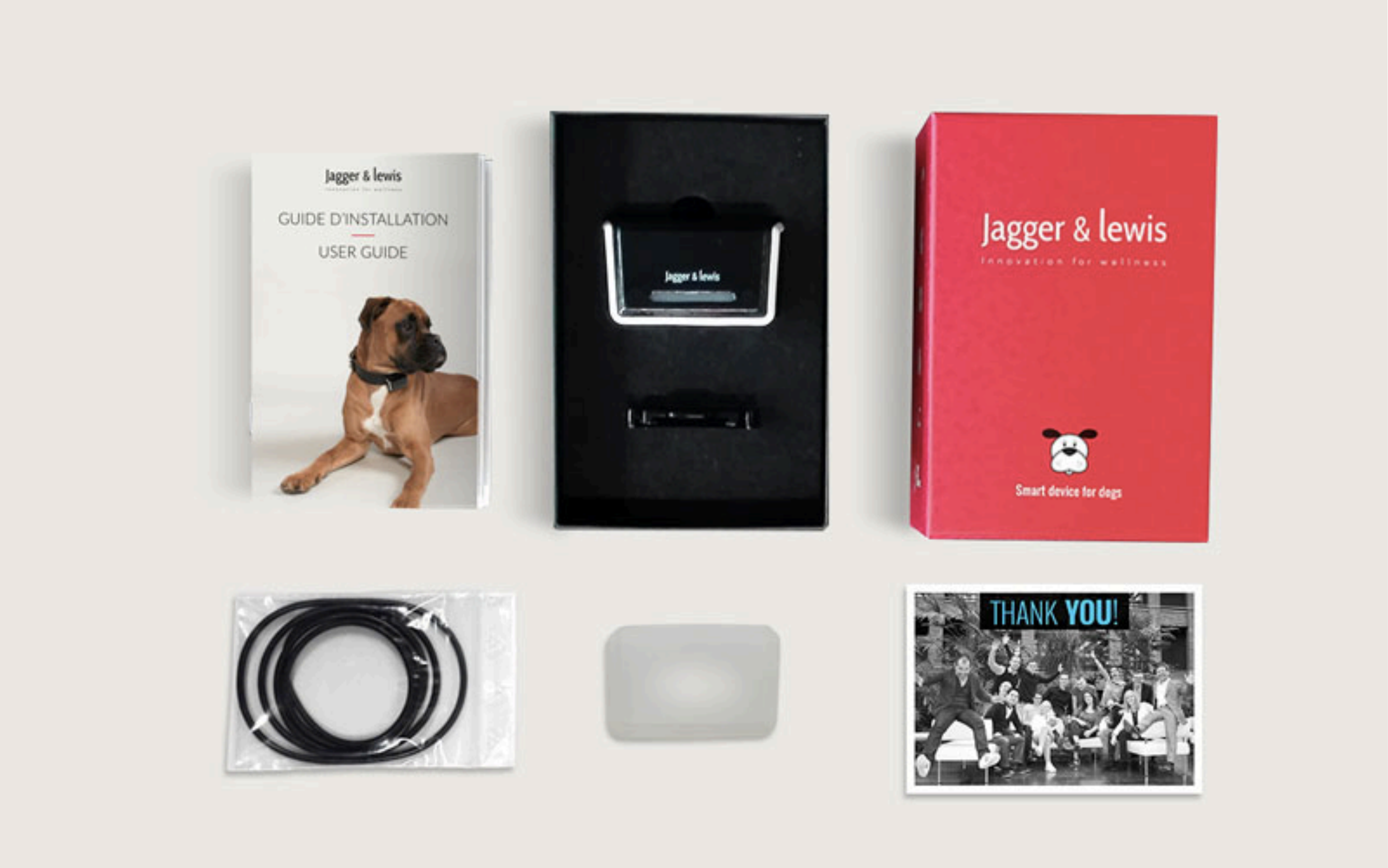
General classes of side channel attack include:

- Cache attack — attacks based on attacker's ability to monitor cache accesses made by the victim in a shared physical system as in virtualized environment or a type of cloud service.
- Timing attack — attacks based on measuring how much time various computations take to perform.
- Power-monitoring attack — attacks that make use of varying power consumption by the hardware during computation.
- ***Electromagnetic attack — attacks based on leaked electromagnetic radiation, which can directly provide plaintexts and other information. Such measurements can be used to infer cryptographic keys using techniques equivalent to those in power analysis or can be used in non-cryptographic attacks.***
- Acoustic cryptanalysis — attacks that exploit sound produced during a computation (rather like power analysis).
- Differential fault analysis — in which secrets are discovered by introducing faults in a computation.

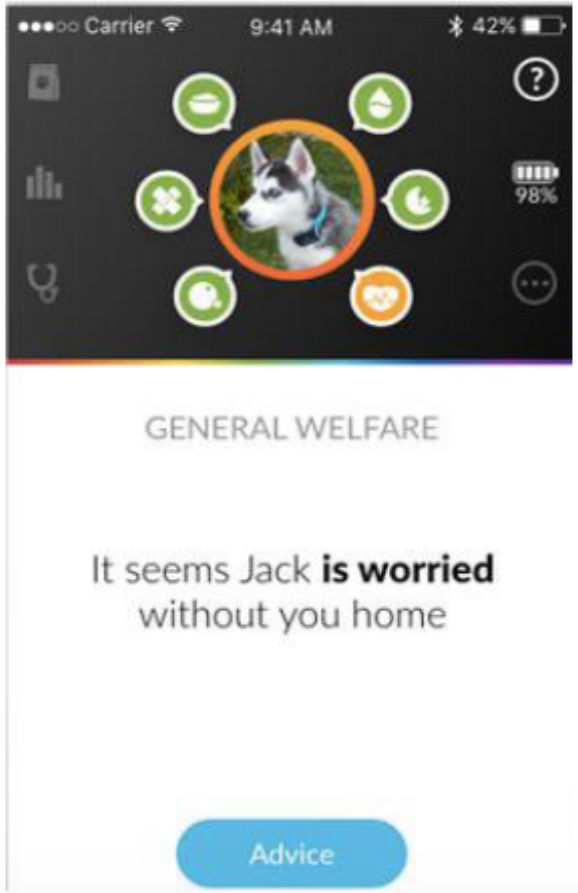
Side-Channel Attacks on Pet Wearable



Side-Channel Attacks on Pet Wearable

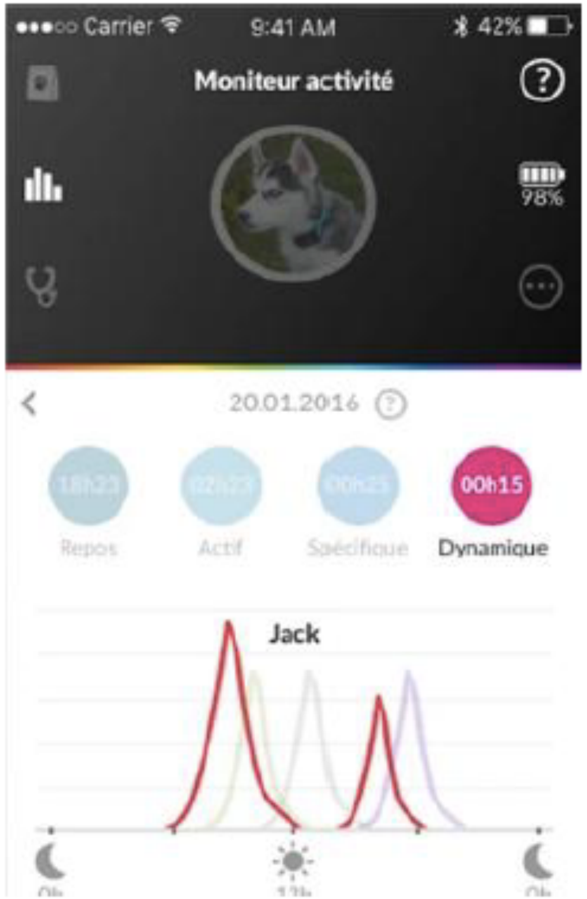


Side-Channel Attacks on Pet Wearable

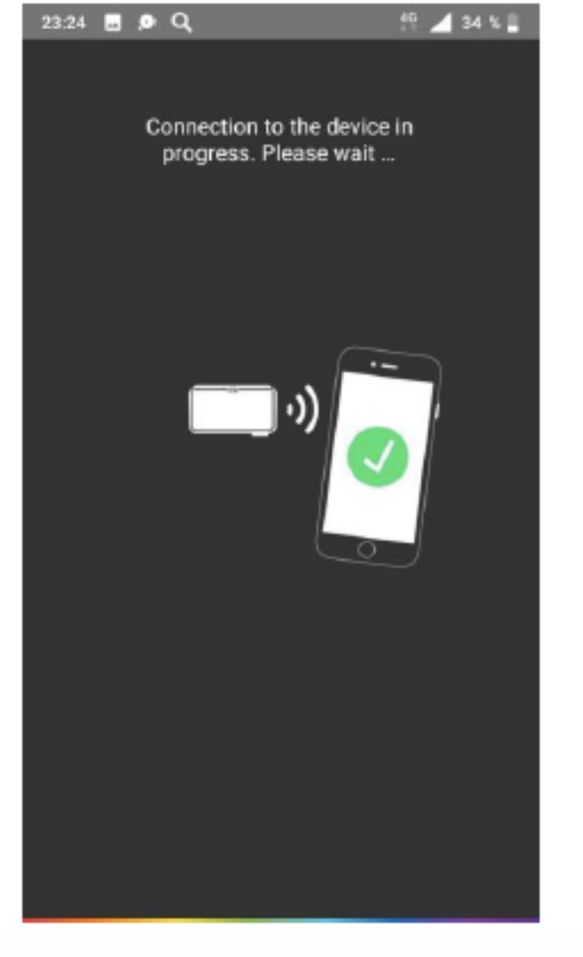


GENERAL WELFARE

It seems Jack **is worried** without you home

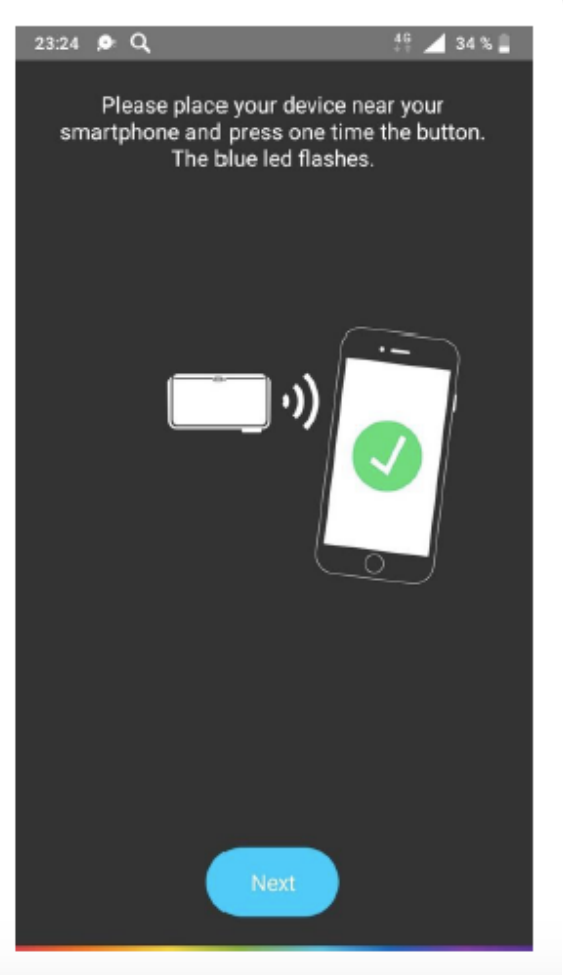


Side-Channel Attacks on Pet Wearable



23:24 34 %

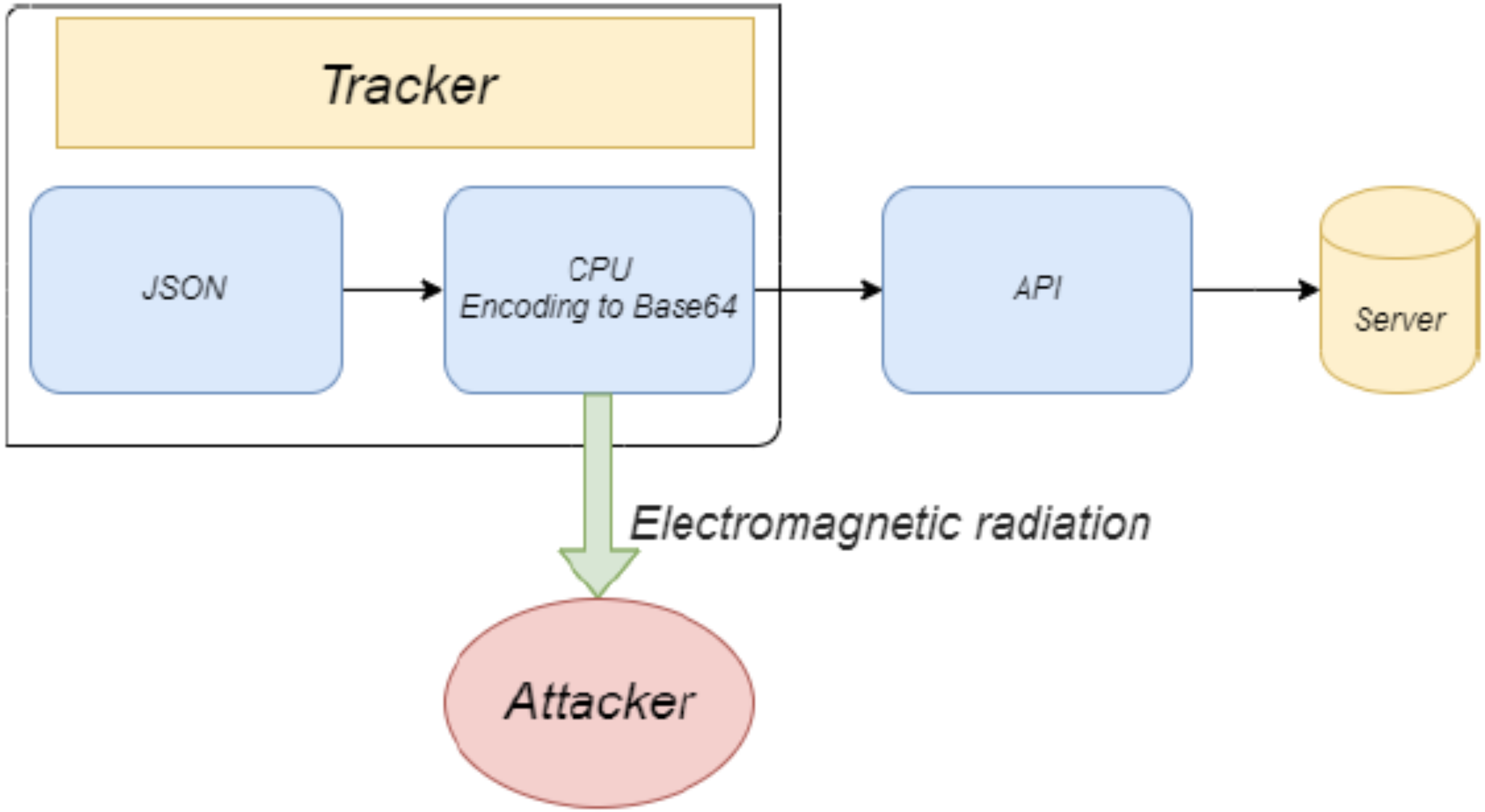
Connection to the device in progress. Please wait ...



23:24 34 %

Please place your device near your smartphone and press one time the button. The blue led flashes.

Side-Channel Attacks on Pet Wearable

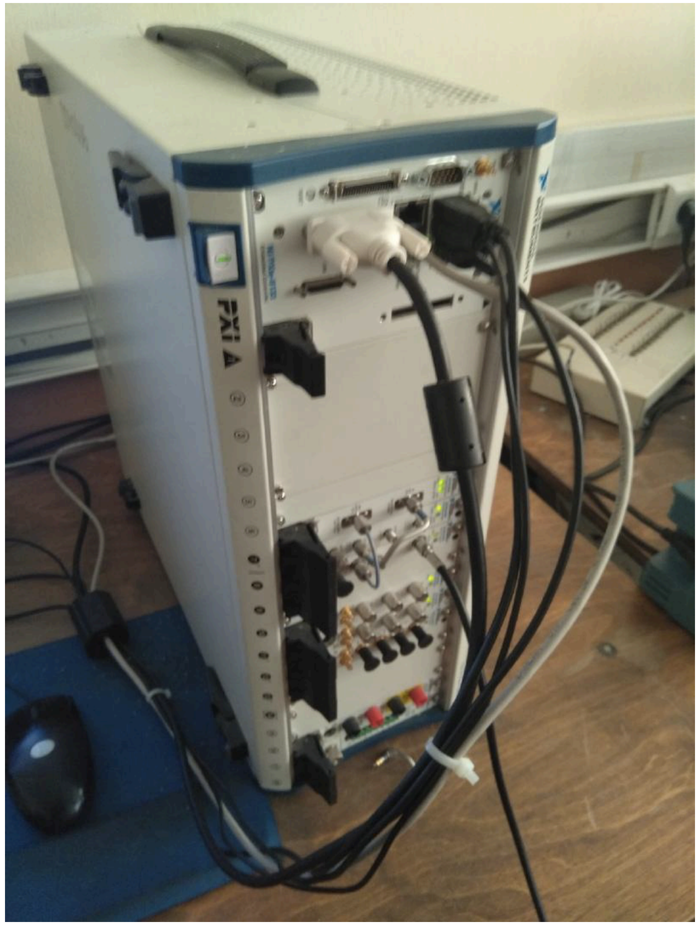


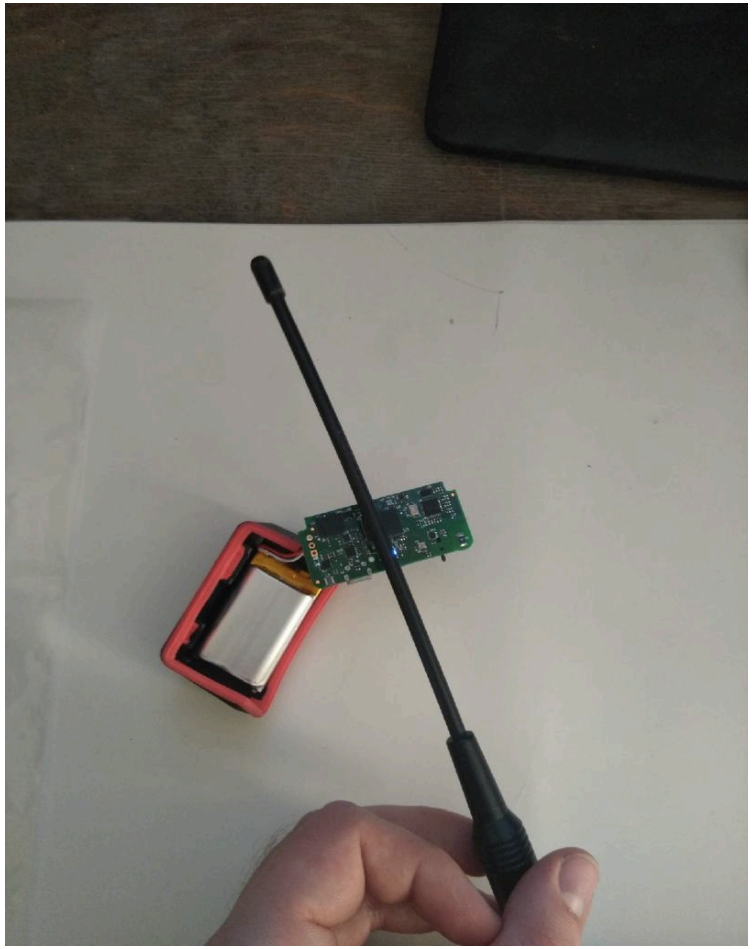
Side-Channel Attacks on Pet Wearable

The following equipment was used for the attack:

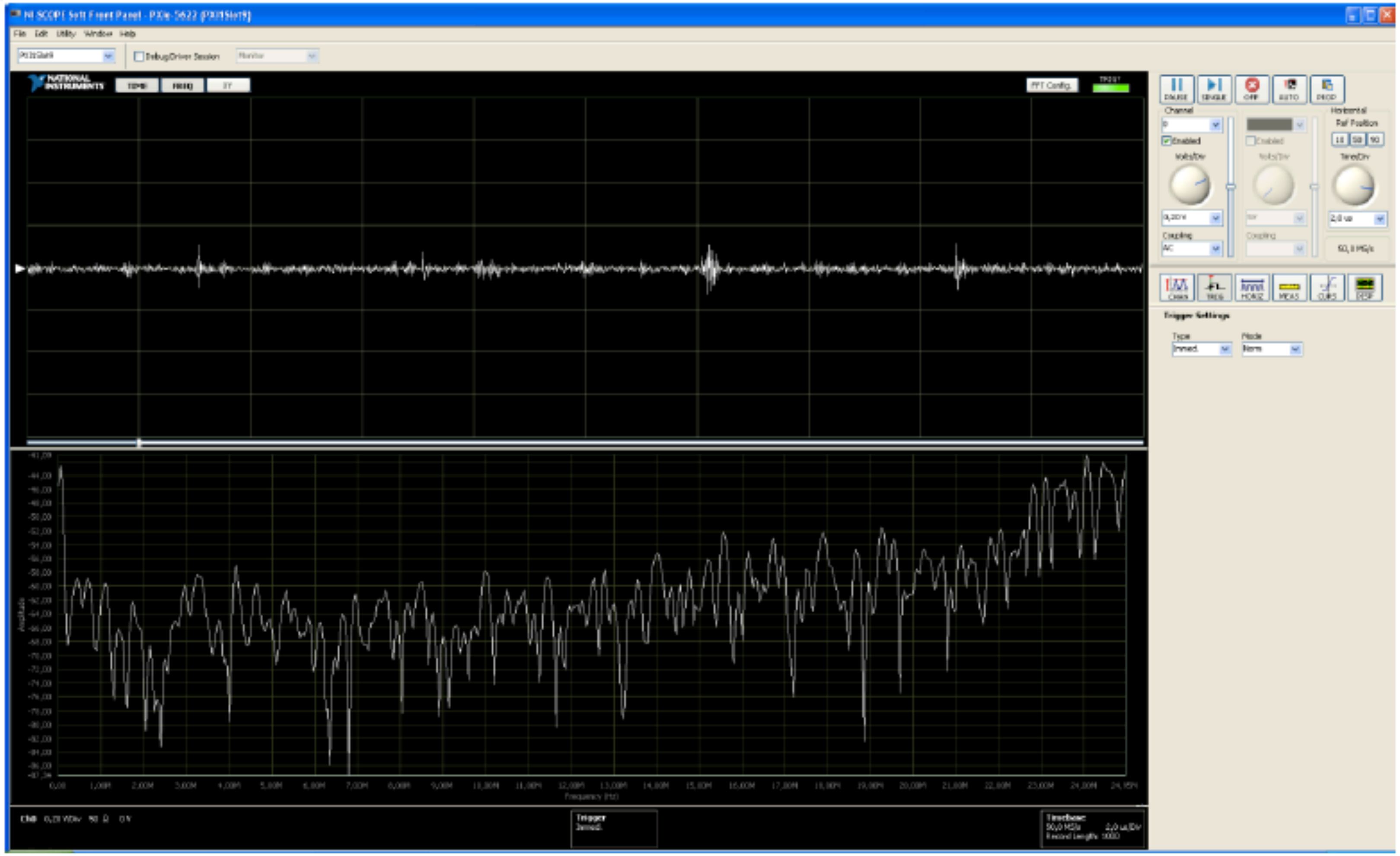
- digital oscilloscope from National Instruments PXI-5114(Sample clock set to 250 MS/s, Bandwidth, 125 MHz)
- an antenna with which the measurements of electromagnetic fields from the device (probe) were made
- software "RFSA - Soft Front Panel"

Side-Channel Attacks on Pet Wearable





Side-Channel Attacks on Pet Wearable



NI-SCOPE Soft Front Panel - PXIe-5622 (PXI1Slot9)

Volts/Div: 0,20 V

Coupling: AC

Time/Div: 2,0 us

50,0 MS/s

Trigger Settings

Type: Immed.

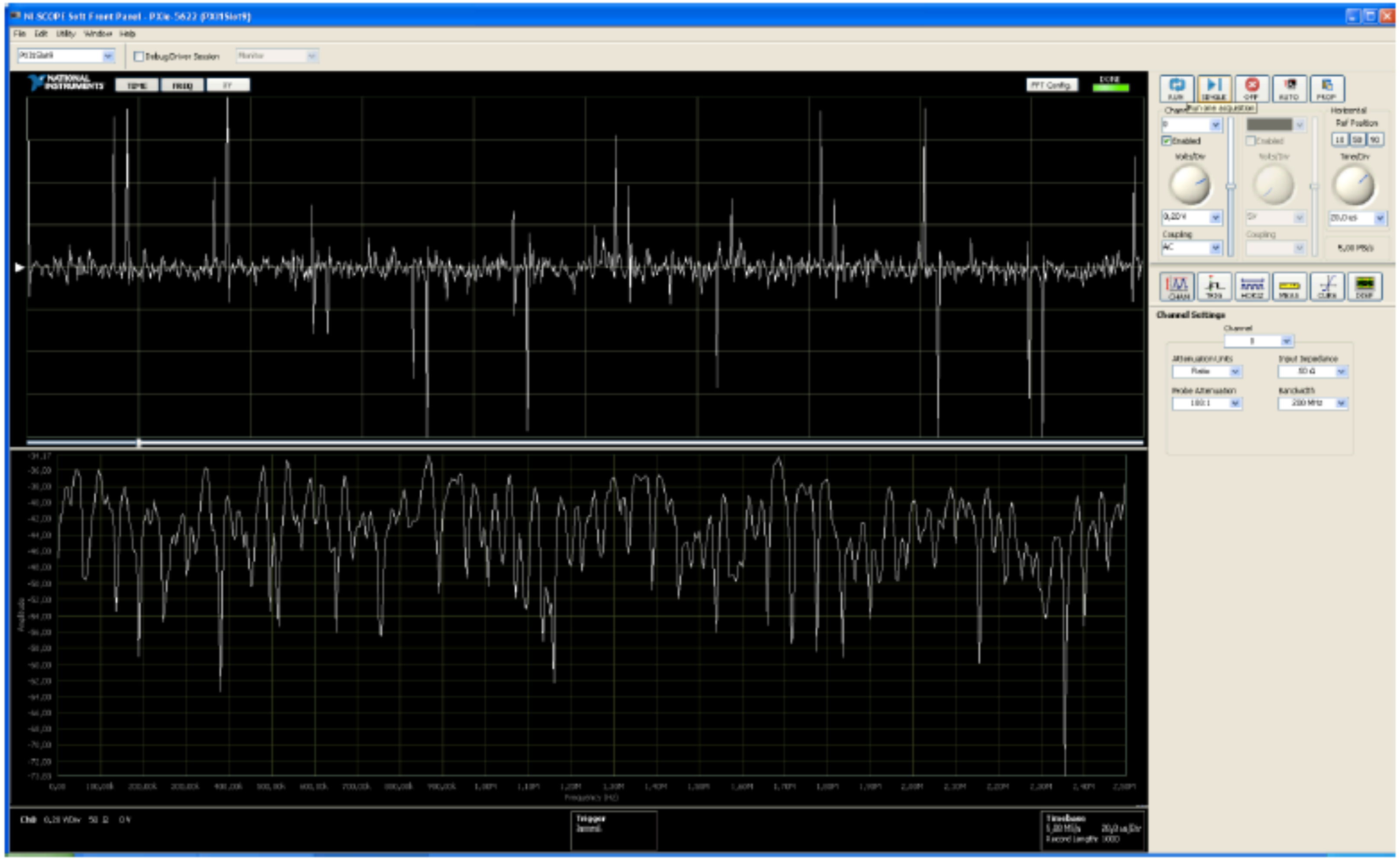
Mode: Norm

Ch0 0,20 V/Div 50 Ω 0 V

Trigger
Immed.

Timebase
50,0 MS/s 2,0 us/Div
Record Length: 1000

Side-Channel Attacks on Pet Wearable



NI-SCOPE Soft Front Panel - PXIe-5622 (PXI1Slot9)

□ Debug/Driver Session

Channel: 0 ☑ Enabled

Volts/Div: 0,20 V

Coupling: AC

Horizontal

Time/Div: 20,0 us

5,00 MS/s

Channel Settings

Channel: 0

Attenuation Units: Ratio

Input Impedance: 50 Ω

Probe Attenuation: 100:1

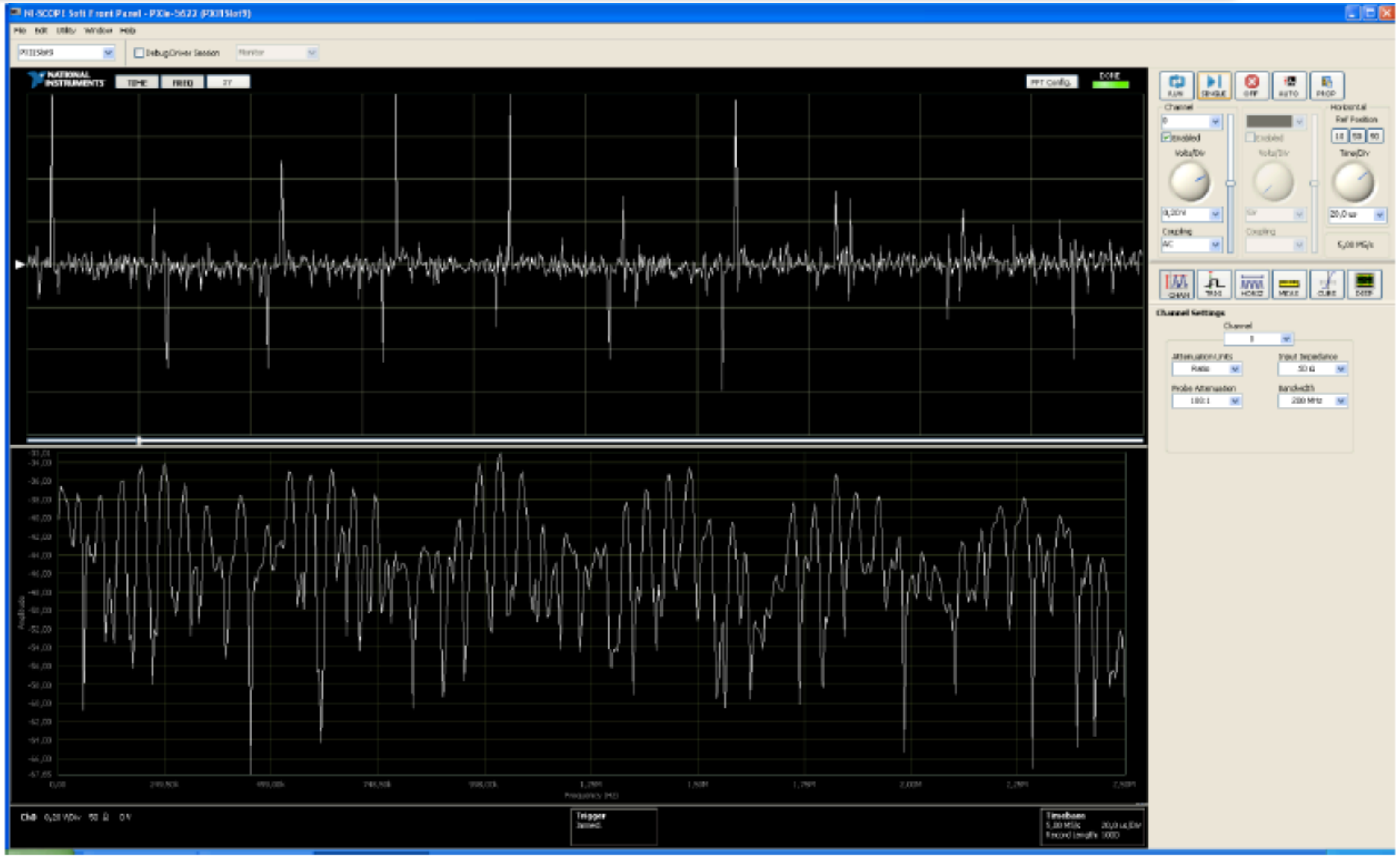
Bandwidth: 200 MHz

Ch0 0,20 V/Div 50 Ω 0 V

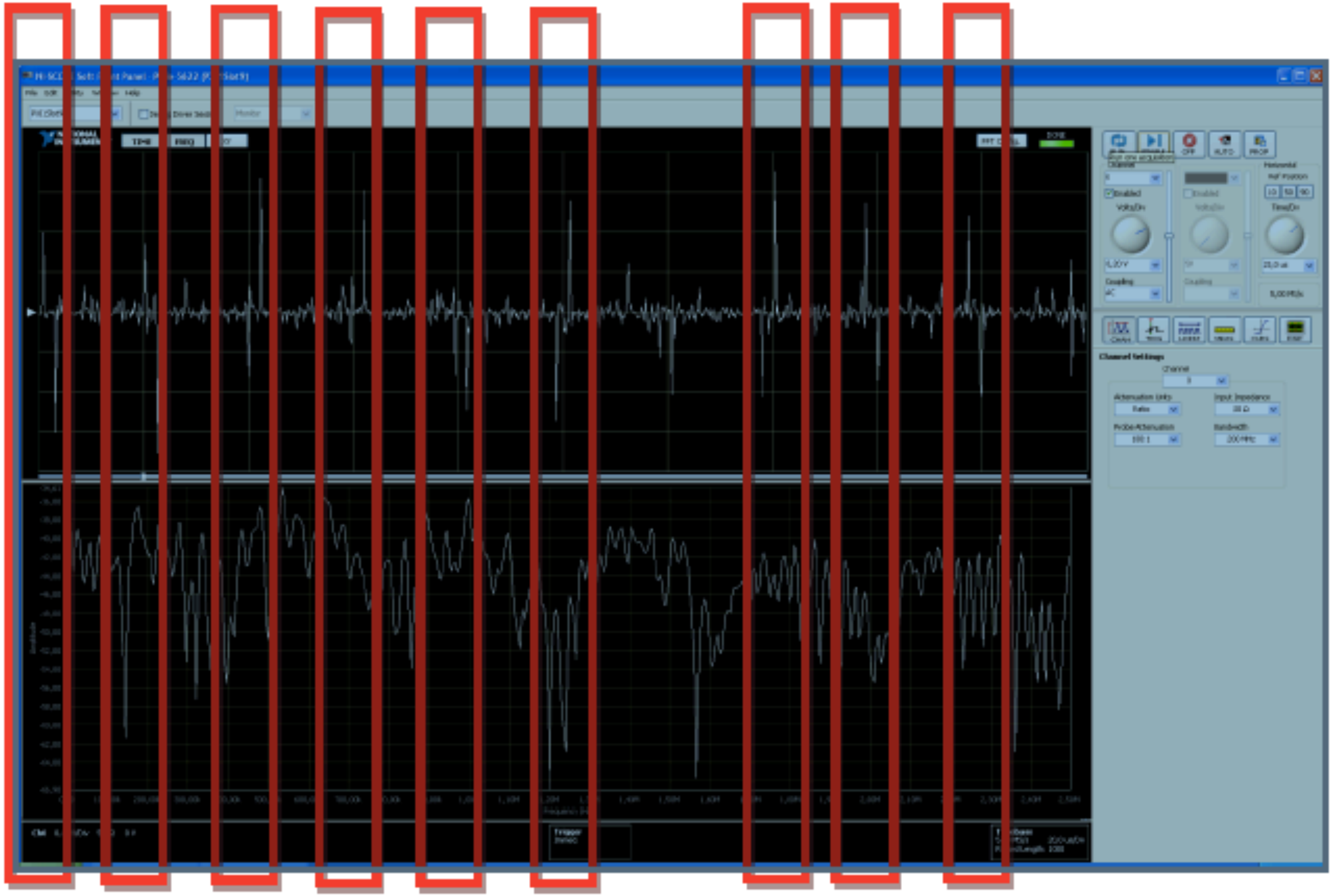
Trigger: Immed.

Timebase: 5,00 MS/s 20,0 us/Div Record Length: 1000

Side-Channel Attacks on Pet Wearable



Side-Channel Attacks on Pet Wearable



Channel

☑ Enabled

Volts/Div 1,20 V

Coupling AC

Horizontal

Ref Position 10 50 90

Time/Div 20,0 us

5,00 MS/s

Channel Settings

Channel 0

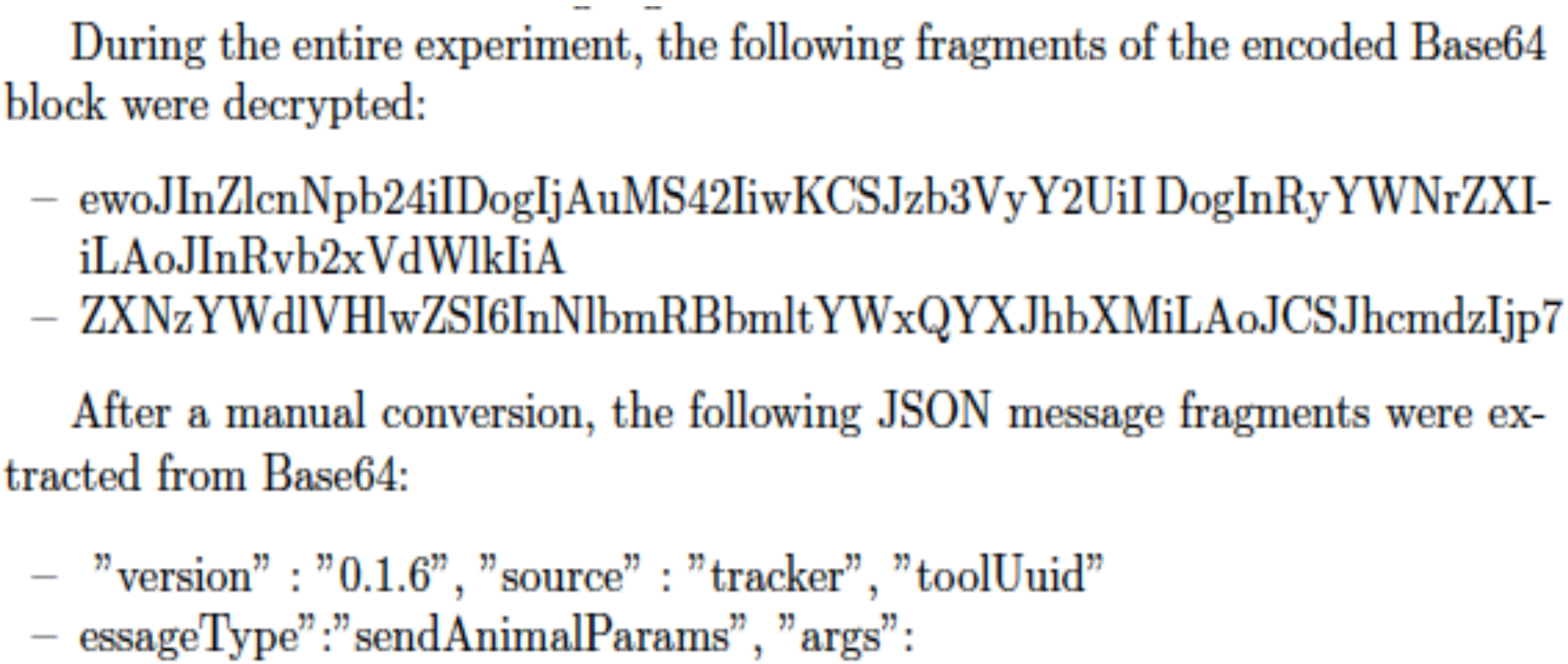
Attenuation Units Ratio

Input Impedance 50 Ω

Probe Attenuation 100:1

Bandwidth 200 MHz

Side-Channel Attacks on Pet Wearable



During the entire experiment, the following fragments of the encoded Base64 block were decrypted:

- ewoJInZlcnNpb24iIDogIjAuMS42IiwKCSJzb3VyY2UiI DogInRyYWNrZXIiLAoJInRvb2xVdWlkIiA
- ZXNzYWdlVHlwZSI6InNlbmRBbmltYWxQYXJhbXMiLAoJCSJhcmdzIjp7

After a manual conversion, the following JSON message fragments were extracted from Base64:

- "version" : "0.1.6", "source" : "tracker", "toolUuid"
- essageType":"sendAnimalParams", "args":

Thank you for your attention!