Implications of Physical Attacks on Single Chip Motes

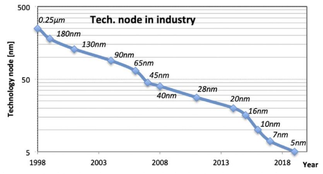
Sara Faour, Mališa Vučinić, Paul Mühlethaler

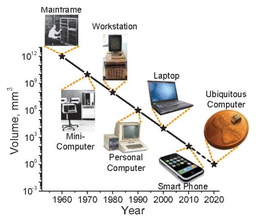
Implications of Physical Attacks on Single Chip Motes

FAOUR Sara VUČINIĆ Mališa MUHLETHALER Paul

Background: Single Chip Motes

The advancement of the fabrication technology in the last few decades enabled decreasing the size of integrated circuits (ICs) and even eliminating the need for the assembly of individual components on a printed circuit board (PCB).





Development of technology nodes in industry (example from one factory) [1]

1997 - Smart Dust Vision [2]

A complete system can be integrated into **1 mm3 mote** !!

- Sensing
- Computation
- Communication

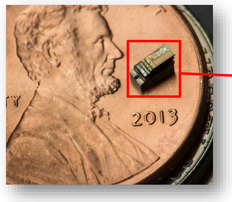
No crystal!

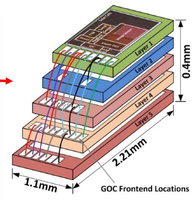
No PCB!

2012 - Michigan Micro Mote (M3) [3]

- Two ARM Cortex-M0 processors
- 3 kB retentive SRAM
- 16 kB non-retentive SRAM
- 335 kHz system clock
- Near-field radio
- Optical bootloader
- Power management
- Fabricated in three different technologies
- Includes five stacked IC dies

1 mm³

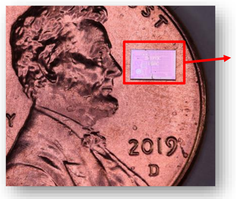


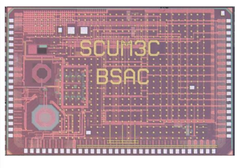


2019 – Single Chip µicro Mote (SCµM) [4]

- ARM Cortex-M0 processor
- 64 kB each of program and data SRAM
- 20 MHz system clock
- IEEE802.15.4 and BLE compatible radio
- Optical bootloader
- Fabricated using single technology
- Single die
- External antenna and power supply (not fully integrated yet)

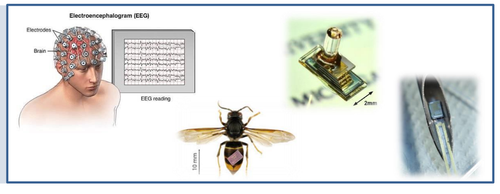
2·3·0.3 mm³



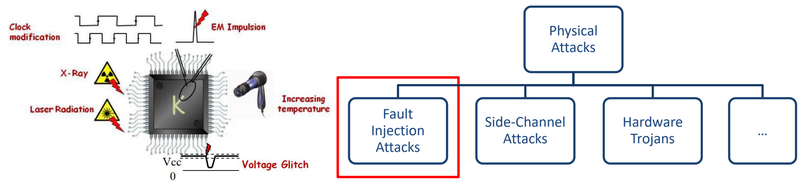


Applications

- Wireless EEG electrodes
- Tracking insects
- Imaging system
- Injectable computer
- Actuation of microrobots

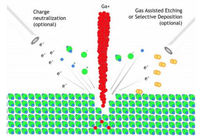


Physical Fault Injections Attacks (FIAs)



Ion-based Fault Injection

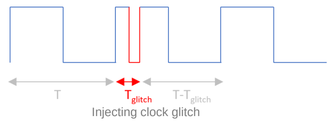
- Two types: Focused ion beams (FIB) or heavy-ion microbeams (HIM)
- Using liquid metal ion sources (gallium, gold)
- High-resolution imaging and precision milling at the micro/nanoscale
- Very expensive (+100,000$), but available as service for low-cost
- Invasive and destructive



FIB technology

Clock Glitching

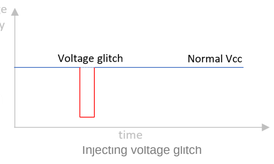
- Manipulating the system clock signal
- Requiring access to clock line, without any special or expensive tools
- Causing instruction misses and data misreads
- Low cost and risk of damage



Injecting clock glitch

Voltage Glitching

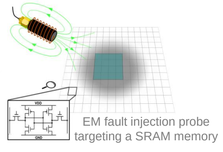
- Manipulating the supply voltage
- Requiring access to clock and power supply lines
- Causing delays in the setup of logic gates, corruption in memory contents, disruption in microprocessor
- Low cost and risk of damage



Injecting voltage glitch

Electromagnetic Fault Injection (EMFI)

- Injecting strong electromagnetic disturbances near the device
- Requiring near-field injection probe connected to an EM pulse generator
- Causing data perturbation in CPU registers, caches, external memory...
- Moderate cost and risk of damage



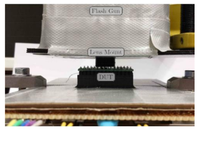
EM fault injection probe targeting a SRAM memory

Heating Attacks

- Altering the ambient temperature
- Can be done using a simple setup: light bulb and thermometer
- Causing bit errors in DRAM memory
- Causing read/write threshold mismatches in non-volatile memory
- Low cost and risk of damage

Optical Fault Injection

- Exposure to high energy light source
- Requiring UV lamp or camera flash with magnification lens, laser, or nanofocused X-ray beam
- Allowing to probe and change memory content, target registers and skip instructions



Implications of FIAs on Single Chip Motes [5]

Technique	Invasiveness		Precision (space)		Precision (time)		Technical skill		Cost	
Clock glitch	non-invasive	invasive	low	complete	high	high	moderate	very high	low	very high
Underfeeding*	non-invasive	invasive	high	complete	none	none	low	very high	low	very high
Voltage spike*	non-invasive	invasive	low	complete	moderate	moderate	moderate	very high	low	very high
EM pulse	non-invasive	non-invasive	moderate	moderate	moderate	moderate	moderate	moderate	moderate	moderate
Heat*	non-invasive	non-invasive	low	low	none	none	low	low	low	low
Light radiation	semi-invasive	semi-invasive	low	low	low	low	moderate	moderate	low	low
Light pulse	semi-invasive	semi-invasive	moderate	moderate	moderate	moderate	moderate	moderate	moderate	moderate
Laser beam	semi-invasive	semi-invasive	high	high	high	high	high	high	high	high
FIB	invasive	invasive	complete	complete	very high	very high	very high	very high	very high	very high
HIM	invasive	invasive	complete	complete	very high	very high	high	high	very high	very high

EM: Electromagnetic, FIB: Focused ion beam, HIM: Heavy-ion micro-beam.
* Internal oscillators of single chip motes are less stable than crystal oscillators when the supply voltage or the temperature change.

Table 1: Summary of FIAs on board-based systems and single chip motes according to our work. Gray color highlights the differing criteria

Clock and voltage glitching attacks are easier to perform on PCB systems

- Traces scale: To perform these attacks, we need to access the clock or the power-supply line trace. On a PCB system, these printed traces can be seen using naked eye. However, on a single chip mote, the traces are at a micro scale, since on-chip voltage regulators and internal oscillators are used.
- Required equipment: Accessing the traces on a PCB requires a simple equipment. However, on a single chip mote, the attacker needs to be able to create tiny channels or access points on the chip surface through which a probing wire can be attached or connected. This setup involves a much more advanced, expensive and spatially precise tool, known as FIB.

The exposure to Electromagnetic, optical and ion-based injections have about the same level of threat regardless if the target is a single chip mote or a PCB system

- Fabrication process: The process used to fabricate a chip plays an important role in making this kind of attack successful or not. The more advanced (smaller) the process is, the less the spatial resolution of the attack is, regardless if it is a PCB-based system or a single chip mote.

Single chip motes can be easily affected by any variations in the ambient temperature

- Temperature sensitivity: It is one of the main characteristics of single chip motes. Any variation in the ambient temperature will affect the frequency of the internal crystal-free oscillators if no calibration algorithm is implemented. Hence, heating attacks can present a higher level of threat.
- Risk of damage: Board-based systems are exposed to the risk of damage in earlier stages of heating compared to single chip motes. The reason is simple: a CMOS die has a much higher maximum temperature (approx 350 ◦C) than PCBs.

Ongoing Research

- Studying the implications of other physical attacks on single chip motes, including side-channel attacks and hardware trojans.
- Adopting security solutions that are more resistant to physical attacks, i.e. Physical Unclonable Functions (PUFs). Also, customizing these solutions to respect single chip mote constraints.

References

[1] Demaria, N. "The impact of microelectronics on high energy physics innovation: the role of 65 nm CMOS technology on new generation particle detectors." Frontiers in Physics 9 (2021): 629028.
[2] Warneke, B., Last, M., Liebowitz, B., & Pister, K. S. (2001). Smart dust: Communicating with a cubic-millimeter computer. Computer, 34(1), 44-51.
[3] Lee, Yoonmyung, et al. "A modular 1 mm3 die-stacked sensing platform with low power I2C inter-die communication and multi-modal energy harvesting." IEEE Journal of Solid-State Circuits 48.1 (2012): 229-243.
[4] Maksimovic, Filip, et al. "A crystal-free single-chip micro mote with integrated 802.15. 4 compatible transceiver, sub-mw ble compatible beacon transmitter, and cortex m0." 2019 Symposium on VLSI Circuits. IEEE, 2019.
[5] Faour, S., Vučinić, M., Maksimovic, F., Burnett, D., Muhlethaler, P., Watteyne, T., & Pister, K. (2023, October). Implications of Physical Fault Injections on Single Chip Motes. In IEEE World Forum on Internet of Things.