

Revealing the Secrets of Radio-Enabled Embedded Systems

On extraction of raw information from any on-board signal through RF

Erez Danieli¹, Menachem Goldzweig¹, Moshe Avital² and Itamar Levi¹

¹ Bar-Ilan University BIU, Ramat-Gan, Israel

² Rafael, Israel

Abstract. In this work we are interested in evaluating the possibility of extracting information from radio-enabled embedded-systems from a long distance. That is, our focus is capturing information from sources in the micrometer to tens of centimeters scale, such as intra- or inter- device busses, board-level routing traces etc. Moreover, we focus on distances in the range of millimeters to tens of centimeters from the (on-chip or on-board) embedded-system Tx Antenna to the signal source.

Side-channels denotes presence of information in illegitimate channels. Side-channel analysis (SCA) attacks typically require statistical analysis and many leakage traces, focusing on micrometer level signals (sources) which emanate direct Near-Field information up to centimeters-level distances. In the same context (Near-Field and micrometer-level) simple power analysis (SPA) like attacks typically extract either direct raw information from one or few leakages or utilize statistical analysis on various samples from the same trace, similarly to horizontal attacks. Lately, radio-enabled systems were shown to emanate to a large distance (Far-Field), information from micrometer level sources, such as CPU processing, through the RF Tx Antenna: so far, SCA-like statistical analysis were shown. On the other hand, various reports exist on direct information eavesdropping/ sniffing or data exfiltration, emanated from centimeter to tens of centimeters scale sources, e.g., SATA, USB, Power-lines, Serial interface, Air-Gap systems, Screens and even optical fibers. All these elements are typically being used as a source and a direct Tx Antenna (huge, several to tens of centimeters) of the sensitive information. These antennas typically transmit information to short distances and the decay is very steep (proportional to r^{-2} - r^{-3} depending on various factors and models). To the best of our knowledge, we report here for the first time an alarming security challenge: any signal in the embedded system, from serial ports, DMA-controlled memory-access, JTAG and SPI interfaces, on-board signals with galvanic connection to the Tx Antenna-chip and *on-board signals without galvanic connection to the Tx Antenna-chip itself, all leak direct information up to tens of centimeters from source to the Tx Antenna*. This alarming situation induce signal-integrity implications within the embedded system, and significant implications relating to device-isolation and user-isolation, it may also affect standards and specifications for e.g., electromagnetic compatibility (EMC), on-board signal shielding, electromagnetic and RF interference (EMI, RFI), cross-talk, and generally design-for-manufacturing (DFM) guidelines for both intra-IC and PCB board. We demonstrate such direct readout of signals with commercial and low-cost equipment indicating how problematic the situation is. The existence of such leakage is demonstrated both over an ultra-low-cost platform such as the nRF52832(nRF) embedded-system and on a more advanced ESP32-c3-devkitc-02 board which is far more widespread in ISM radio applications and meets certification like FCC and CE (as compared to the nRF device). We have constructed an experiment to demonstrate leakage scenarios from (1) on- and (2) off-chip, on-board or (3) signals without galvanic connection to the RF front-end chip, showing the severity of the leakage,

repetitively and systematic nature of the phenomena over various devices. We further demonstrate how sophisticated adversaries can build a code-injection Gadget which can carry sensitive-data and modulate it to be best extracted by the RF-channel. The main observation we push forward is that unless concrete interference and isolation standards appear with security metrics in mind, which are significantly different than ones needed for communication, it would be hard to prevent such leakages.

Keywords: Code Injection · FLASH · JTAG · Leakage modulation · Memory · NFC · Radio Transceivers · RF · Side-channel attacks · SCA · Sniffing · Spectral modulation · SPI · Serial · Spectrum

1 Introduction

Background and scope: Digital communication takes a major part in our modern way of life. Sky rocketing volumes of transmitted information only increase in this data-era, and techniques to store and process this information secretly are becoming more and more complex. In addition, radiating devices which embed antennas and enable wireless connections between devices, such as WiFi, Bluetooth, LORA, NFC, Zigbee and various other small antennas which exist locally on-board, are massively deployed and used to communicate diverse data types with various modulations. Another clear reality derived by needs and technological road-maps, is that many manufacturers develop small and cheap System on a Chip, SoC devices, containing digital, analog and Radio-Frequency, RF, parts on the same die (i.e., mixed-signal device), and embed antennas in tiny embedded-systems. For example, a chip featuring a (digital) microcontroller as well as the (analog) radio such as WiFi, and other *close-integration* technologies on the same package, e.g., Multi Chip Modules, MCM, System In a Package, SiP, or board [Tai00, ABC⁺17].

Massive deployment of communicating devices open a hatch to various threats, and perhaps the more alarming class are wireless devices transmitting locally amplified signals. Side-Channel Attacks are powerful attacks against implementations of cryptographic algorithms at present, breaking conventional cryptanalysis security-bounds and are quite easy to mount. Passive e.g., electromagnetic, EM, optic and acoustic SCAs were previously demonstrated and are quite alarming as they do not require galvanic connections. SCAs are in nature statistical attacks due to low signal-to-noise (SNR) ratio, which deems for repeated measurements as signals are very small and statistical tools are needed to average out noise components. Traditional Statistical-SCAs, SSCAs (or DPA in the jargon) typically target intra-device processing of information and targets micro-to-millimeter source-dimensions scale (local cache, CPU, register-file etc.). EM-SSCAs sources typically radiate Near-Field (NF) emanation [LMPT15, HMH⁺12, SBO⁺15] owing to the dimensions of the targets/sources. Simple Power Analysis, SPA, attacks work with larger signals and better SNR conditions, providing the ability to directly readout or correlate processed values. Non-invasive EM attacks (SPA or SSCA), are quite complex to implement in a noisy environment, since usually the emissions of low-power devices are very weak.

Recent advances on mixed-signal devices, used in widespread wireless communication protocols (e.g., WiFi, Bluetooth), demonstrated that it is possible to utilize the leakage of a cryptographic algorithm which is amplified and then transmitted by the antenna [CPM⁺18, CFS20, WWD20]. These attacks are very powerful and they have given attention to challenges with leakage from radiating-devices (antenna enabled) which broadcast amplified Far-Field (FF) emanation. However, to date and to the best of our knowledge, only statistical attacks were shown requiring repeated measurements, only small micro-millimeter target signals (sources) were considered which emanate small energy, thus requiring repeated measurements and statistics. Furthermore, the targets chosen were on-die with the Tx Antenna meaning maximum several millimeters distances from sources to antenna.

In this paper, we present a much wider scope of the leakage in transmission of mixed-signal devices and systems, emanated from various elements of the embedded-system into

Table 1: Radio/spectrum based covert or side-channels, where color-code from white to yellow, through orange up to red indicates severity.

	Source Dimensions (scale)	Source-to-Tx Distance (scale)	Tx-to-Rx range (& potential)
CPU on die [CPM ⁺ 18]	μm	mm	>10 m
Coupling to Fiber [HPWW22]	cm to m	m	> 100 m
USB, PS/2, from Cable [KHF19, VP09, ALWS17, VP09]	0	cm	cm to m
SATA Cable [Gur22]	cm to m	0	<m
Screens [HHM ⁺ 14]	cm	0	<10 m
Acoustic vibrations, human movement [WWZZ15, ZLAA ⁺ 18]	m	0	m
<i>This work:</i>	μm to cm	μm to tens of cm	m scale (>10 m)

the receiver Antenna, mainly focusing on direct readout or no statistics/averaging.

Prior art and jargon on the topic does not always refer to the issue as ‘an SCA attack’, for some examples: information sniffing [CFWX20, LJL⁺16], eavesdropping [SLKS18], information exfiltration [LGG⁺21] covert-channels [MSBK16], spoofing [LMRZ16], snooping [MTGJ21] and out-of-band signals [CA16, AKM17]. All of which are definitions and jargon used in various reports which have a clear connection to this research. For example, out-of-band signal injection attacks are aimed at exploiting sensor/actuator hardware imperfections which leaks unintentional information upon injection. In the context of this paper we are interested in broadening the scope and collectively group them all together, the reason is that they all relate in some application space to NF and FF injected or natural (inherent) side-channels. We are interested mainly in direct (side-channel) readout of raw information, without massive statistics or large volume of repeated measurements. I.e., with similarity to SPA or single/few-traces attacks. We refer to the source dimension as the physical element size of the information carrying source. The Tx distance as the physical distance between diverse modules or *sources* inside and outside the chip and the RF Tx module. The Rx distance is defined as the distance between the Tx antenna and the receiver FF Rx antenna. Existing reports on > 5 cm EM attacks typically focus on huge antennas such as: SATA [Gur22] as illustrated in the bottom-right of Fig. 1 and listed in Table 1, USB or PS/2 cables [KHF19, VP09, ALWS17, VP09] as illustrated in the bottom-center of Fig. 1 and listed in Table 1, Screens [HHM⁺14] as illustrated in the middle-right of Fig. 1 and listed in Table 1, or Optical-fibers [HPWW22] as illustrated in Fig. 1 on the right and listed in Table 1 and even Power-lines [GZBE19]. These are all used as both (tens-of-centimeters to meter scale) sources and Tx antennas which emanate to rather short distances (up to 1 meter). In this work, we focus on FF radio Tx Antennas radiation which amplify and broadcast information to rather huge distances, similarly to [CPM⁺18, CFS20, WWD20]. However, with direct readout in mind, we target the *entire embedded system* and show SCA on: (1) any signal in the embedded system carried on an internal-bus, from serial ports to memory-access, JTAG and even SPI connected Flash (2) on-board signals with galvanic connection to the Tx Antenna-chip, and (3) on-board signals **without** galvanic connection to the Tx antenna-chip itself, *leaking direct information up to tens of centimeters from source to the Tx Antenna, anywhere on the embedded system board*.

1.1 Our Contribution

This paper covers an *in-depth* side-channel evaluation of RF signals within closely integrate embedded systems. We list here the main contributions of the paper:

1. **Embedded-System Perspective:** as illustrated in Fig. 1, in this work we show RF module interference related to three distances defined as {source dimension,

Review on Advances of EM – radiation based attacks

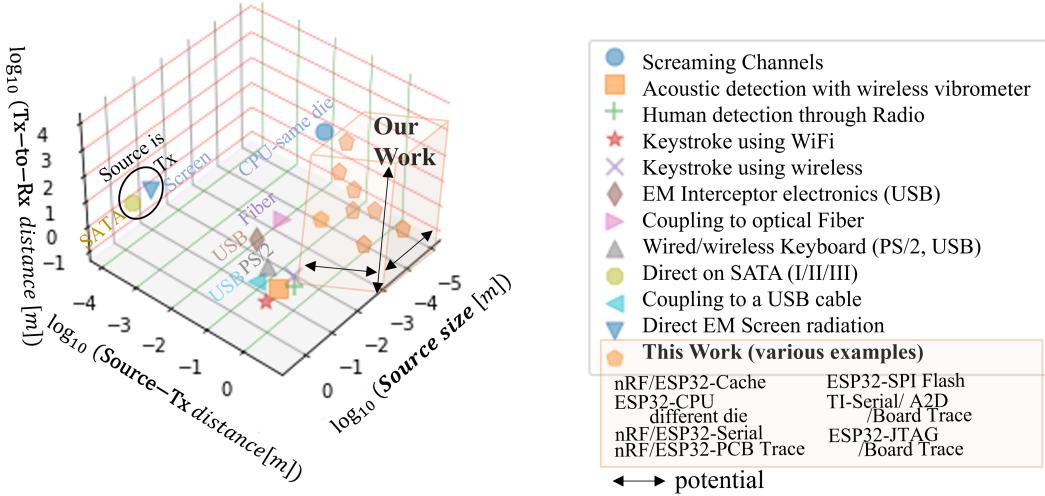


Figure 1: An overview of RF-based SCA as a function of source to Tx and Rx distances, and dimensions of source signal. In this work we evaluate smaller sources in dimensions and larger source-to-Tx distances.

Rx distance, and TX distance}. We demonstrate various cases with leakages along these axis with many unexplored regions leaking unintentionally RF information as compared to prior-art.

2. **Direct Readout of Ports (e.g., a serial port):** we showcase direct readout of on-board UART serial ports and (e.g.,) SPI-enabled Flash and JTAG communication. *Leading to the natural question of why encrypting the data if it is already exposed?*
3. **Direct Readout of Memory Accesses:** we demonstrate direct leakage of memory/cache accesses which can enable (close to) one-shot leakage of raw memory processed data.
4. **Experimental Root-Cause First Steps:** With the goal of providing a clear demonstration that the root-cause is not only a “bad device” or bad design methodology we have set out an experiment to demonstrate an evidence from various devices, and to show also that not necessarily a galvanic connection is needed between the source to the Tx antenna device.
5. **Extending Available Experimental Data:** although none of the previously reported experiments were demonstrated with our focus on the nRF device platform, some prior results were shown on this platform [CPM⁺18]. Our goal was to extend the available body-of-knowledge and experimentation with other higher-end device. For example on a more widespread ESP32 and CC2642 devices.
6. **The Threat of an RF-optimized Code-Injection Gadget for Data Exfiltration:** we further demonstrate how a sophisticated adversary can build a code-injection Gadget which can carry sensitive-data and modulate it to be best extracted by the RF-channel (such as PWM, AM, and FM modulations).
7. **RF²:** we show how isolation is problematic, e.g., when a communication channel such as NFC, designed for small distance communication <5 centimeter, is leaking, amplified and then transmitted to far-field (>100 m) over Bluetooth. *Arousing a discussion on standards and required testing.*

Table 2: Experimental overview. $\{\checkmark, \times, -\}$ denotes leakage shown in this paper, no-evidence and not-tested, respectively.

Device	Enc(CPU)	JTAG	SERIAL	NFC	FLASH	MEM (Cache)
Nordic nRF	\checkmark	\checkmark	\checkmark	\checkmark	-	\checkmark
ESP32	\times	\checkmark	\checkmark	-	\checkmark	\checkmark
TICC2642	-	\checkmark	-	-	-	-

The main observation we push forward is that unless direct isolation, or well defined RF termination and integrity mechanisms of all such components exist in the system, it would be hard to prevent such leakages. However, we also highlight that standard tools (i.e., from RF and communication) would not necessarily suffice or be optimal as they typically do not quantify information leakage, they capture signals-integrity which does not imply our security objectives, highlighting the needs this paper put forward.

Paper organization. The manuscript begins with a short discussion on implications and impact of threats as discussed in this paper. Then we follow with elaborating on technical details needed on equipment, setups, and evaluation in Sub-section 1.3. In Section 2 we first give a general formulation and discussion of leakage into far-field antennas, possible reasons for the phenomena etc. It is followed in Section 3 by an instrumental and inherent discussion and experimentation relating to leakages on-board and close to the device, even with no physical contact, leaking into the RF circuitry. Section 4 demonstrates possible direct readout of serial-interface through RF emanation, escalating to RAM readouts in Section 5. In Section 6 we show how a sophisticated adversary can orchestrate a code-injection gadget, to leak any sensitive variable efficiently by RF modulation. Sections 7 and 8 discuss JTAG and SPI-flash Far-field and Near-field leakages, and in Section 9 we show how NFC antennas are broadcast by the RF circuitry to a far distance, outside the conventional model. In Section 10 we conclude the paper, extent and open questions.

1.2 Impact and Implications

In this work we demonstrate that physical, architectural or structural boundaries between sensitive and non-sensitive data (if present), are quite breachable with radio-enabled devices. This potentially leads to numerous challenges:

- Signal-integrity, cross-talk and device-isolation implications within the embedded system, on-die or on-board.
- Significant implications relating to security architecture, user-isolation and privileges
- Trade and commerce implications relating to restrictions on radiating and communicating devices

These all have potential to affects standards and specifications, EMC of devices and production methodologies.

High-frequency signals can radiate electromagnetic interference (EMI) if care is not taken with how they are routed on the circuit board and inside SoC's. Not only can the length and configuration of the traces¹ be a problem, but trace and *via*-stubs can act as an antenna as well, and move the interference to another trace on the board or SoC. Another source of EMI is the signal return path, which optimally should be on an adjacent reference plane. If the return path is blocked in any way, the signal will radiate even more as it seeks a path back to its source. High-speed signals on traces that are too close together may inadvertently couple with one signal overpowering the other. Such crosstalks can result in the victim signal mimicking the characteristics of the aggressor signal and not performing the task they were intended to do. Not only is this a problem with traces

¹Note that we assume the reader distinguishes from the context between an SCA leakage *trace* signal and a physical metal-connection routing a.k.a a *trace* in the jargon.

that are side-by-side, but also with traces that are routed in parallel on adjacent layers of the board. This type of crosstalk is known as broadside coupling and is why most circuit board designs alternate horizontal and vertical routing directions on adjacent layers. Traces routed without the proper attention to their impedance value will suffer changes to those values in different board areas depending on various conditions. To properly route, impedance controlled sensitive traces requires a specific layer configuration, trace width, and clearance. *Specifications to prevent such interactions, standards and guidelines exist but they mainly touch reliability/ integrity challenges.* Any device will require a range of testing to make sure it is not producing any EM emission that exceeds the limits set by any Federal Communications Commission (FCC) rule and requirement. Every manufacturer requires the testing and certification of devices to ensure they meet EMC standards. To pass these tests and get certified, companies need to run EMI tests and EMC, *part of these tests measure or quantify the emission of the unit under test (UUT), but not the emission and interference between the UUT blocks.* These standards do not comply or were not characterized to joint embedded-systems-and-chips coupling information within the system, and in practice existing tool-sets and design-flows anyway struggle to comply with such specs in design-phases owing sometimes to lack-of models and intellectual-property (IP) issues relating (e.g.,) third-party IPs.

For example, for IoT devices that work in the industrial, scientific and medical (ISM) band, the 2.4-2.5 Ghz is legitimate, so the peripheral block leakage frequency that interfere with the RF section and up-conversion to the ISM band will pass the EMI test. Part of these standards require RF shields, but these shields are for the EMI, in the (e.g.,) nRF device case, the JTAG signal goes through a legitimate path that passes to the ISM antenna. In our case, the problem is not the EMI from the UUT outside, but inside the UUT topology. Such standards concentrate on the emission of the device UUT, for example near field magnetic wave. The clock frequency of the nRF device can meet the FCC standards, but still it can be modulated to the RF section and jump to the ISM region. To eliminate such problems, many guidelines exist (e.g., providing attenuation specs in dB, minimizing trace length, keep high-speed components close, especially in mixed signal designs, use good grounding practices, isolate inputs, high sensitivity inputs may even require a separate routing layer, using bypass capacitors to reduce noise around DC components). *However, these guidelines were not evaluated per se for security interest but for signal-fidelity, reliability, performance and signal-integrity. As long as a “leakage” signal does not induce interference and reduces the communicated signal such standards can as well disregard it.* Another aspect is that providers are not obliged in the hard sense to comply with such recommendations, these are only recommendations for reliability and meeting (e.g.,) specs such as timing, which can just be relaxed in many cases.

On the other hand, security specifications are not up-to-date to account for tiny radiating embedded-systems. For example looking on the TEMPEST initiative: from the 1950's, the National Security Agency (NSA) engaged in the TEMPEST program to layout definitions and guidelines for securing un-encrypted and encrypted data signals, several following reports culminated with the latest TEMPEST01-02 [TEM, NSA82] and some published in partial (with blank texts) such as the NACSIM 5000, NACSEM 5112 and NSTISSI no. 7000 TEMPEST². The purpose was to set testing methodologies and guidelines so as to evaluate the risk of electromagnetic emanations of computers and digital equipment. In the scope of this work, it is clear that any such aim should be re-adjusted and well fine-tuned to the current state-of-the-art (i.e. advanced IoT SoCs) and technological advance of embedded systems. Such specs (to the best of the existing literature we know of) suffer from a lack of clear separation of intra-UUT and inter-UUT. Furthermore, not only test-ability, validation and evaluation methodologies updates are required but also concrete chip- to PCB- level design guidelines and specification for information security.

²<http://www.cryptome.org>.

As to enhance the understanding and implication of what demonstrated in this paper we briefly elaborate here on possible threats relating to the signals we have intercepted: the type of information which flows through Joint Test Action Group interface (JTAG) ranges from test-patterns and diagnosis but also boot-firmware, device's bitstreams, protocols between modules which are not enabled through some other network connected ports, and system registers configuration and setup. Other ports we have exposed such as Serial interfaces may carry unencrypted information, keys firmware boot and updates. SPI-flash ports in turn communicate un/encrypted firmware, keys and boot program. Near-field communication (NFC) carries banking/ through-air payment and is not designed to communicate to far-field and multiple devices such information in a broad sense. We believe it is also possible to eavesdrop OTP devices being read, Fuses readout storing unlock keys etc.

1.3 Technical Details

Setup and equipment: The experimental setups for the nRF, ESP and TI mixed-signal devices are categorized to transmitter and receiver parts. At the transmitter part, each device was initialized to a specific configuration which included parameters such as central RF frequency, and communication protocol. The nRF and the TI devices were set to a center frequency of 2.4GHz, and to a BLE-5 protocol. The ESP device was set to a center frequency of 2.4GHz, and to a WiFi protocol. At the receiver part, an Omni-directional antenna with 0dB gain was connected to a Software Defined Radio (SDR) RSA-306B. This SDR is centered to the leakage frequency (dependent on the tested peripheral), with a hundreds of KHz Bandwidth. The SDR records i-q data stream for a later information leakage analysis.

The leakage frequency of the nRF and the TI devices were set to 2.528GHz (the second harmonic of the CPU clock), and 2.56GHz for the ESP device. Several distances between the devices and the receiver antenna up to 20m were examined. For short distanced up to 1m, omni-directional antenna with 0dB gain is sufficient, whereas for longer distances above 1m a compensation is required which includes a directional antenna with high gain and Low Noise Amplifier (LNA). On the receiving side, we use an antenna with a gain of 24 dB (TP-Link TL-ANT2424B) and two low noise amplifiers with a gain of 20 dB (Minicircuits ZEL 1724 LNA), followed by a DC Block to stop any direct current components after the amplifiers.

Leakage From Building block devices: In sections below we describe diverse lab experiments performed on mixed-signal device and embedded-systems of close integration (which includes a digital MCU including its' many peripherals and RF parts). The purpose of these experiments is to analyze the information leaking unintentionally from digital components via (seemingly) independent RF transmissions. In general, this kind of mixed-signal device consists of different parts such as CPU, memories, peripherals, RF etc. (as illustrated in Fig. 2a), all implemented on the same silicon, but separated physically. Alternatively interactions between close devices on the same PCB board are shown with the RF transmission (as illustrated in Fig. 2b). Next we show that despite of the physical design partitioning, some dependency does exist between the digital parts and the RF part. This dependency leads to information leakage of internal digital processing through the RF transmissions. This leakage can be in the spectrum during the BT/WiFi operation (or other transmitting/radiating protocols). For example, common RF devices focus in frequency band between 2.4GHz and 2.6GHz, the ISM band (between 2.4GHz and 2.5GHz) can be distinguished clearly when the Bluetooth is operating. However, the 2.5GHz-2.6GHz band can contain additional information as well as is shown below; specifically, we show how the 2.562GHz frequency, which carries peripheral modules packets information ready to read-out easily.

Board-level evaluation and interactions with the overall setup: The examined RF mixed-signal devices included the Nordic nRF, ESP32 and TICC2642, In Fig. 2a, presented from right to left respectively: The target device and some chosen sub-modules with an RF transceiver onboard. said device is mounted on a Target board which might include numerous other component devices with possible sensitive *data* saved on and/or interacted with. those devices leak data to the target device using the target board electric circuits. Neighboring galvanically isolated circuits can even leak sensitive data to the target device using induction. This has been shown in an experiment where a short wire circuit was placed nearby the target board, the signal could be seen in RF. The vulnerable data signal was magnified through the target's radio transceiver to reach the attacker's spectrum analyzer on a much greater range. shown in Fig. 2c includes the various mentioned targets, different types of RX antennas, connected to Spectrum Analyzer or SDR, sampling the RF measurements. Data analysis as well as devices configurations are made by a computer. Additional setups for information leakage from on-board traces includes contact experiment (refers to the tested device PCB), and no-contact experiment (refers to a different PCB), as illustrated in Fig. 2b. The no-contact lab experimental setup is shown in Fig. 2d. On leakage from the periphery through traces on the board, there are two main experiments. The first experiment contains the transmission of logic signals with a power of 3.3 volts on traces of different lengths (1, 5, 10, 20 cm) on the pcb being tested (nRF), at the same time the nRF chip is with a radio on and BLE is on, in addition the spectrum analyzer searches for the logic signal contain the logic data in a frequency range of 2.48-2.6GHz. The second experiment contains the transmission of logic signals within a different pcb (that pcb performs logical operations and does not transmit radio signals) at the same time the nRF chip is in radio mode on and BLE is on, in addition the spectrum analyzer searches for the logic signal contain the logic data in a frequency range of 2.48-2.6GHz. The results show that the nRF chip is a bouncer for the logic signals from the various experiments at a distance of up to tens of centimeters from the nRF chip as will be discussed below.

2 Far Field emanation - leakage into the antenna-loop, prior to amplifier/modulator or through shared-ground

In previous reports, that focus on leakage from an encryption processing by the CPU to the RF front-end [CPM⁺18] (which are embedded on the same die, as illustrated in Fig. 2a), the underlying assumption was that the leakage is modulated by the CPU clock signal. I.e., some sensitive signal $s(t)$ is multiplied by the clock signal, $c(t)$, to produce a modulated signal $m(t)$. Such that, the spectrum of this signal is the convolution $M(f) = S(f) \otimes C(f)$.

In our model we do not specifically focus on the clock signal as the modulating clock (or sub-carrier), nor we specifically focus on the CPU processed encryption as the leakage. In the scenarios evaluated below, the modulation carrier can originate from anywhere and any protocol in the embedded-system: e.g., the Baud-rate of the Serial interface, the JTAG protocol modulation, as well as possible other sources such as the NFC carrier, Flash connected SPI interface rate or the Cache memory access time etc. I.e., the locations in the spectral domain we need to “search” for leakage considerably vary among application/scenario. As an illustration in our system we evaluate leakage from any on board signal as indicated by red-highlighted signal-traces on the schematic PCB in Fig. 2b.

In any case, following the above mentioned modulation, the signal is additionally modulated by the RF circuitry, propagating to the amplifier and filter stages and finally the antenna, as illustrated in Fig. 3. The modulation circuitry modulates the signal over a carrier with frequency f_c producing the pre-amplification broadcast signal $s_{bc}(t)$:

$$s_{bc}(t) = \sum_{n=-\infty}^{\infty} a_n s(t) e^{i2\pi(nf_s+f_c)t} ; S_{bc}(f) = \sum_{n=-\infty}^{\infty} a_n S(f-nf_s-f_c) ; a_n = \frac{1}{2} \cdot sinc\left(\frac{n\pi}{2}\right) \quad (1)$$

For a duty-cycle of 1/2, perfect rectangular (ideal) clock, with $w_0 = 2\pi/T$ and amplitude of 1V.

Notably, there exist numerous mechanisms which can generate such coupling behaviour into the RF modulator as illustrated in Fig. 3 and listed below:

1. **Ground plane/supply V_{dd} coupling:** If PCB ground planes or perhaps a power-supply regulator are not well isolated from the Tx modulation circuitry, or from its modulator clock input f_c , any signal which passes and is not fully suppressed will be RF modulated. Admittedly, large planes such as ground PCB planes (if not

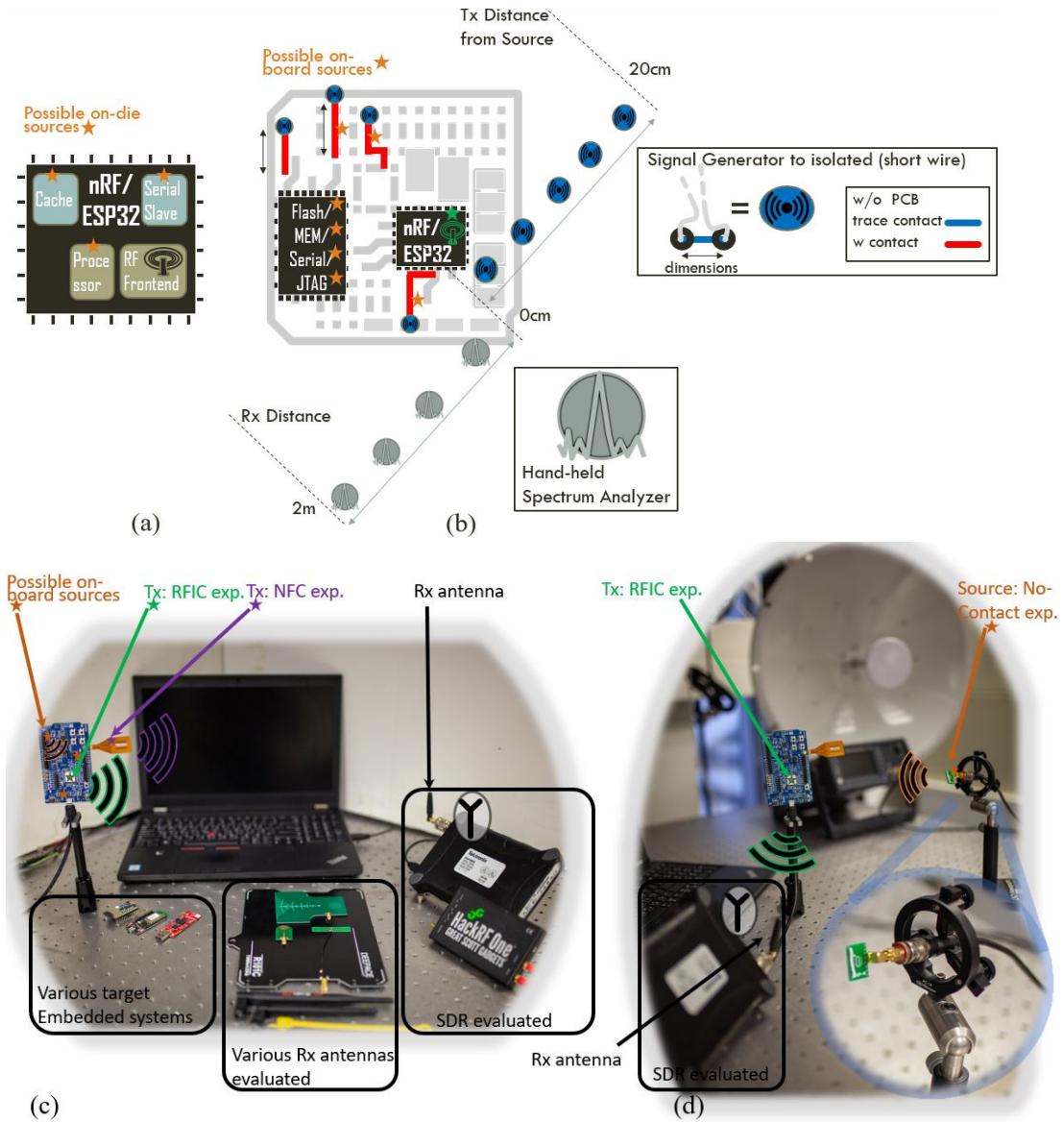


Figure 2: Embedded System Perspective and setups illustration

well guarded) are easy radiation target for near-field EM and even close-by layers carrying signals by capacitive connection.

2. ① **Silicon substrate coupling:** a grounded Silicon substrate is in most cases shared among modules or macros in an integrated-circuit (IC), if a sensitive signal couples to it, it will reach the RF modulator as well, if in the same IC. Furthermore, a say Flip-Chip with a not very strong (high impedance) grounded substrate might be an easy target.
3. ③ **Data Bus/wire coupling:** a high metal-layer data bus (e.g., Tx_{data}), if not well taken care of, can be a direct and additive entry point for RF modulation on-top of the normal transmitted data (not sensitive).
4. ④ **Clock coupling:** perhaps one of the most alarming coupling scenarios is into the modulated clock signal. Leaking or coupling to the clock source or generator circuitry can take place by many mechanisms and to many locations such as to a DCM, a PLL, to an external generator, a clock buffer or a clock tree.
5. ⑤ **Near Field coupling to (e.g.,) a coil:** filters in RF circuitry are typically composed of large passive elements such as coils, a passive near-field radiation can potentially leak into the filtering circuitry.

Depending on the source of the leakage and its whereabouts in the embedded system, some of these mechanisms require galvanic connection in order to couple and some does not. Clearly, the amplitude and the signal-to-noise ratio of the coupled leakage depends on many factors as well as on the noise-floor in the embedded system.

The question of the largest contributor to this phenomena is not simple to answer. However, our experimentation on several devices indicates that (1, 2 and 5) mechanisms, which can potentially leak without contact (passive), are evident in some devices. The situation is amplified in the non-passive scenarios (i.e., with galvanic connection) possibly by other mechanisms in the list.

3 Extracting Signals from an Embedded-System

In this section we show that in addition to the leakage of internal modules inside the chip (such as the peripherals), information of external elements outside the chip can be leaked and amplified by the RF module as well, and that generally signals significantly leak within the RF embedded system, that the challenge is systematic and the emanation variation among such systems is quite large. This indicates a lack of clear standard and specification, specifically for information security aspects.

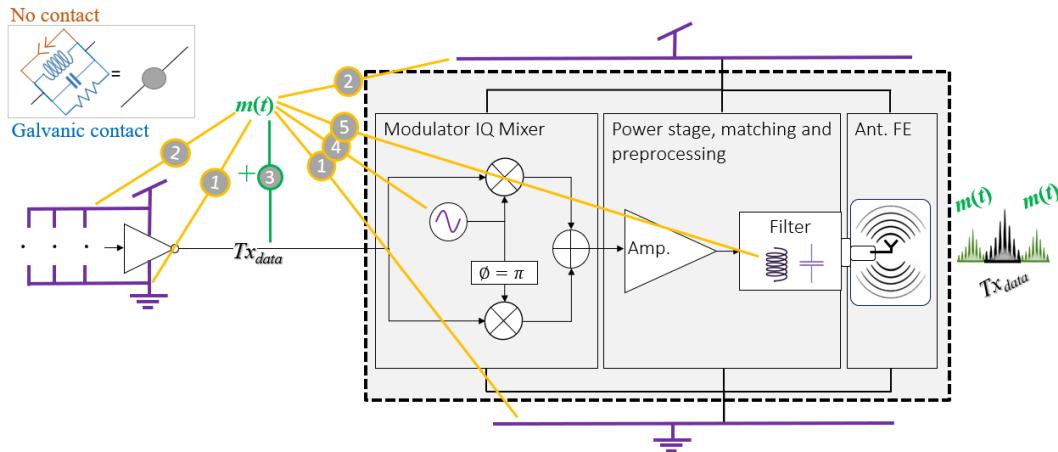


Figure 3: Open Questions

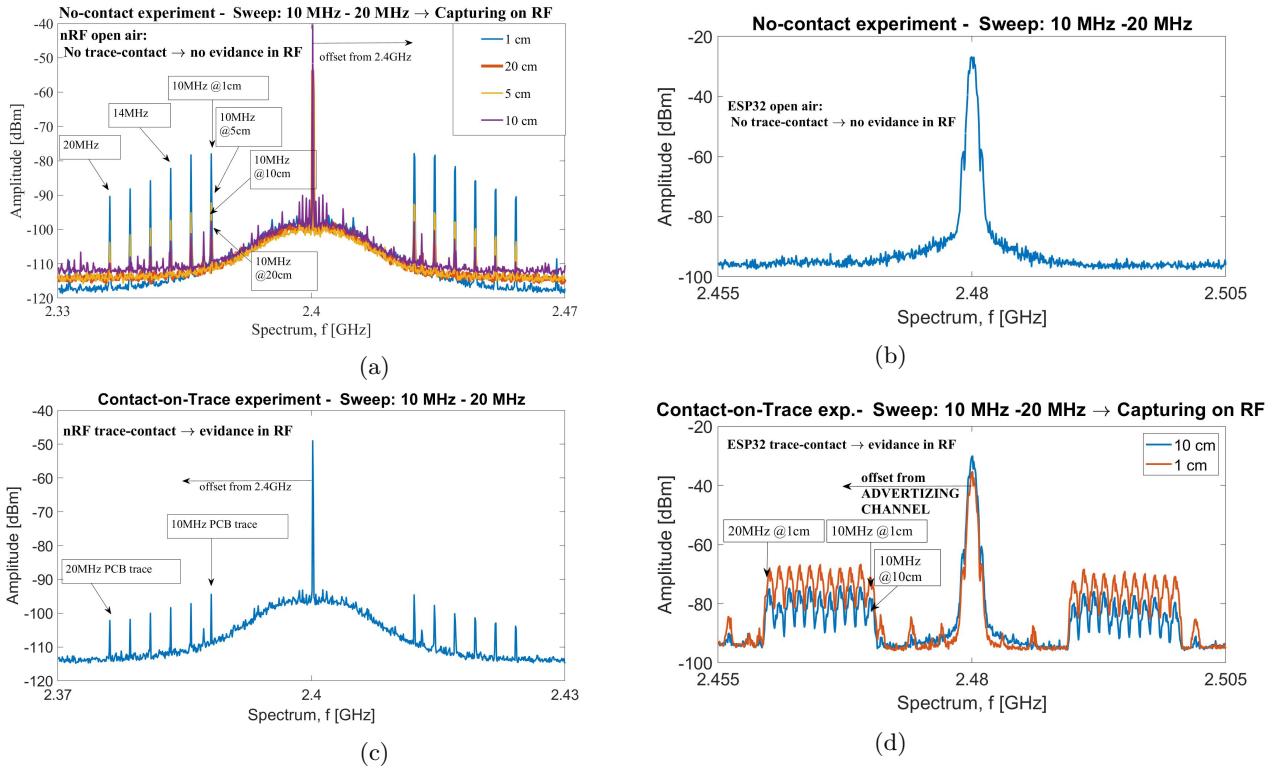


Figure 4: Experimental results in the spectrum domain: (a) **nRF** *airgap* antenna sweep up to 20 cm from Tx RF antenna modulator chip (b) **ESP32** *airgap* antenna sweep up to 20 cm from Tx RF antenna modulator chip (c) **nRF** Touch-on-PCB trace antenna leaking into the Tx RF antenna (d) **ESP32** Touch-on-PCB trace antenna leaking into the Tx RF antenna..

For the experiment outlined in this section we were interested in generating mock-up known signal patterns. For that purpose we have generated signals by a signal generator³ sweeping frequency, voltage, impedance ranges respectively of 10-20 MHz, 1.1-3.3V and 50Ohm. The generated signal was carried by an especially well isolated BNC cable (An RG-59 coaxial cable which is typically used for RF testing; the signal attenuation is 10db/100M in our test scenario of 100MHz range), placed further away from the embedded system (more than a meter), at the tip of the coax. cable a very short wire was extracted carrying the generated signal serving as a small antenna (Fig. 2d). It is important to note that the signal generator can only drive maximum currents of 200mA and works with maximum amplitude of 3.3V. We have evaluated two scenarios: (a) the antenna tip scanned in open-air (i.e., no galvanic contact) on top the embedded system in distances from 0 cm (right on-top of the RF Tx antenna chip) to 20 cm away from it. (b) the antenna tip was physically connected (galvanic connection) to traces on the PCB board (Fig. 2b) from distances of 20 cm when possible, i.e., when the PCB is large enough, through 10 and 5 cm to 1 cm access point on a trace from the Tx antenna chip.

Fig. 4 shows information leakage of an RF signal outside the chip (setup illustration in Fig. 2c), as a function of TX-distances. The RF signal in Fig. 4a is a communication signal transmitted through a wire in distances of 0, 10cm and 20cm. The RF signal in Fig. 4b is the same communication signal but physically connected to an arbitrary trace on the

³Picoscope oscilloscope series 5 signal-generator.

Device Scenario	nRF NORDIC	ESP32	
No-contact (airgap)	Evidence ✓	No evidence ✗	Conclusion 1: PCB traces leak to the antenna FE
PCB trace contact	Evidence ✓	Evidence ✓	
Conclusion 2: A systematic issue			

Figure 5: Conclusion of experimental evidence of leakage into the antenna RF FE.

PCB (setup illustration in Fig. 2d). The information leakage shown in Fig. 4c refers to an RF signal connected to a trace of a different PCB located next to the nRF. Notably, our coaxial cable holds an impedance of 75 Ohm, which actually implies that 1/3 of the energy is suppressed and in essence using a 50 Ohm such cable the illustrated leakage amplitudes below would in fact be larger.

Fig. 5 concludes the evidence this experiment provide:

- **Significant device dependence:** From the negative experimental results on ESP32 we can assume different devices might be more susceptible to leak on-PCB signals than others.
- **Real world implications:** A trivial example of a wire antenna which is nearby PCB traces shows how it can propagate separate signals to be amplified and leaked through RF module.
- **The issue is systematic:** The fact that even airgapped inducted EM fields are amplified in some devices shows the systematic security issues in embedded RF modules.

4 Direct Information Redout and De-modulation: Serial interface

In general, UART is an asynchronous serial communication module, which is commonly implemented in hardware devices, such as PC, SoC, embedded devices, etc. Particularly, the UART module acts as the interface between external devices and internal modules. The data contained in the UART transport is usually in a clear text and not encrypted, and therefore consists of a sensitive and significant information (e.g., firmware, configuration files, sensors data). This work exposes the vulnerability of the peripherals, and challenges the protection requirements along the design.

The first step of this experiment is the nRF configuration which allows a UART communication. The next step is the RF signal measurement using a far-field antenna and a spectrum analyzer, as described in Fig. 2b. The measurements are taken while specific data is transferred to the UART peripheral. The Bluetooth module is turned on. Note that the analysis for the data extraction is made on a region of interest. In case the CPU is involved, such as in UART operation, this region is related to the system clock and the RF carrier frequency of the transmitter. In case of the nRF, the clock is 64MHz, and the interesting frequency area is the frequency range that includes the RF carrier as well as the system clock harmonics (added to the carrier).

The spectrum of the Bluetooth activity is shown in Fig. 6c. It can be noticed that the left side of the spectrum describes the Bluetooth carrier. The right side describes the region of interest, where the information of digital parts in the chip are leaking. In addition to the Bluetooth activity, when the UART module is on, a quite different spectrum at the same region of interest is obtained, as shown in Fig. 6a. After having these insights, the purpose of the final step is attempting to extract the actual (digital) data transferred from the UART module from the RF samples. In order to achieve this, various data of different hamming weights has been sent through the UART, and the RF signal (in

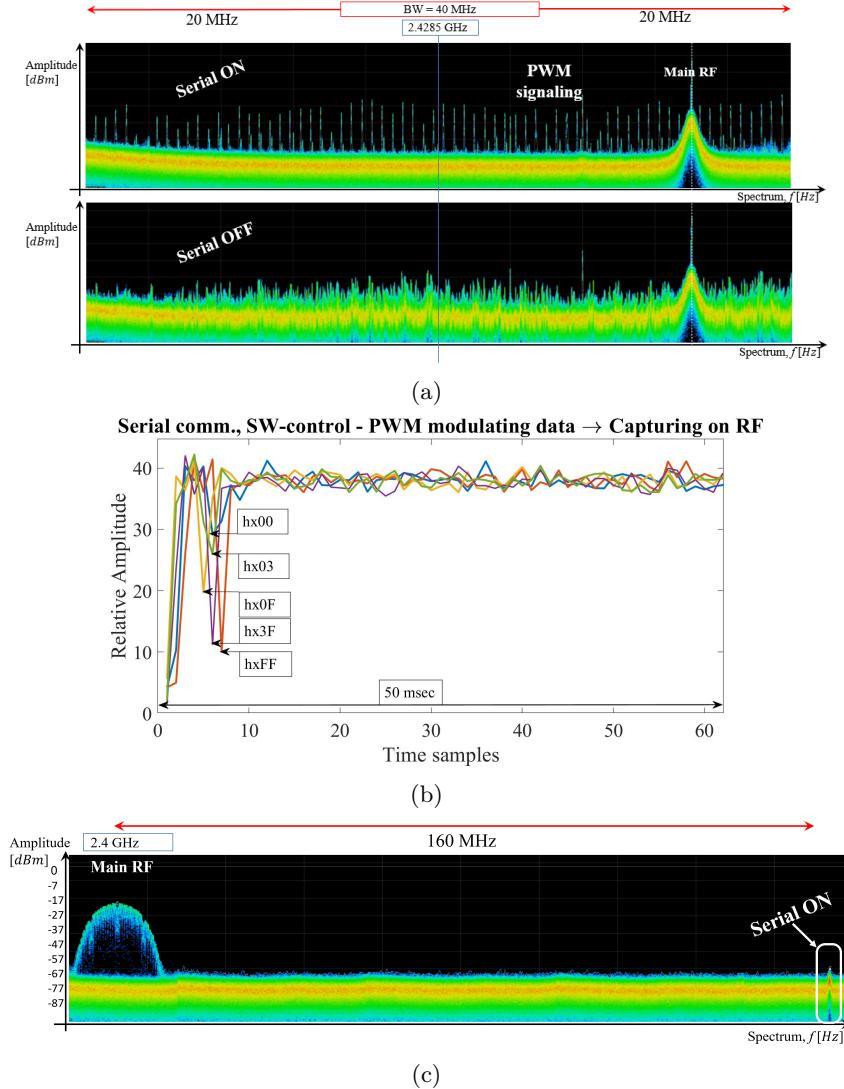


Figure 6: **nRF**: Experimental results in the spectrum/time domains: (a) SW controlled *Serial* communication being read in the Spectrum domain (b) Serial communication in the Time domain capturing different read data. **ESP32**: Experimental results in the spectrum domains: (c) SW controlled *Serial* communication being read in the Spectrum domain

the same region of interest) was sampled in time-domain. Fig. 6b shows five different time-domain signals for different hamming weight data values. The classification is very clear, where each hamming weight value correlates to a specific and different graph. In other words, a sensitive information about the UART data can be extracted without any additional statistics.

5 Direct Information readout and De-modulation: Memory

Random Access Memory (RAM) is used to store the most basic operational data on any SoC. RAM is where user sensitive information will be stored by any internal logical modules that require data storage. Most times no extra security measures are implemented as it is an integral internal memory that can be used freely and will be erased on power off.

The attack setup (illustrated in Fig. 7b) consists of the nRF connected to a PC which writes data bytes through UART. The nRF is configured to store data received by UART directly to RAM using the internal Direct Memory Access (DMA) module. Meanwhile The RSA306 spectrum analyzer is used to record activity caused by the UART writes stored to memory. The RF spectrum observed correlates to internal signal clock frequency and not the UART symbol frequency configuration.

In this experiment we kept in mind to have minimum chip activity besides the RAM. So we can isolate only emissions that are enacted by memory access. The Bluetooth is active And The CPU is in sleep mode when running the attack. The RAM is logically independent to both. The only parts that should react to the UART relate to the DMA-RAM memory bus. The data being received over UART in 1.152Bps must be converted at some point internally to parallel memory, this would happen in 64MHz domain (the internal system clock). The memory modulated signals we observed using the RSA306 can be seen in 2.4GHz+128MHz which is the second harmonic of the system clock. Common usage of Bluetooth enabled MCUs involve it being active in the background of onboard functionalities so in our setup it is turned on. The experiment shows that the data being accessed on RAM is leaking to the active Bluetooth antenna.

The results in Fig. 7a show the spectrum where we observed the activity in system

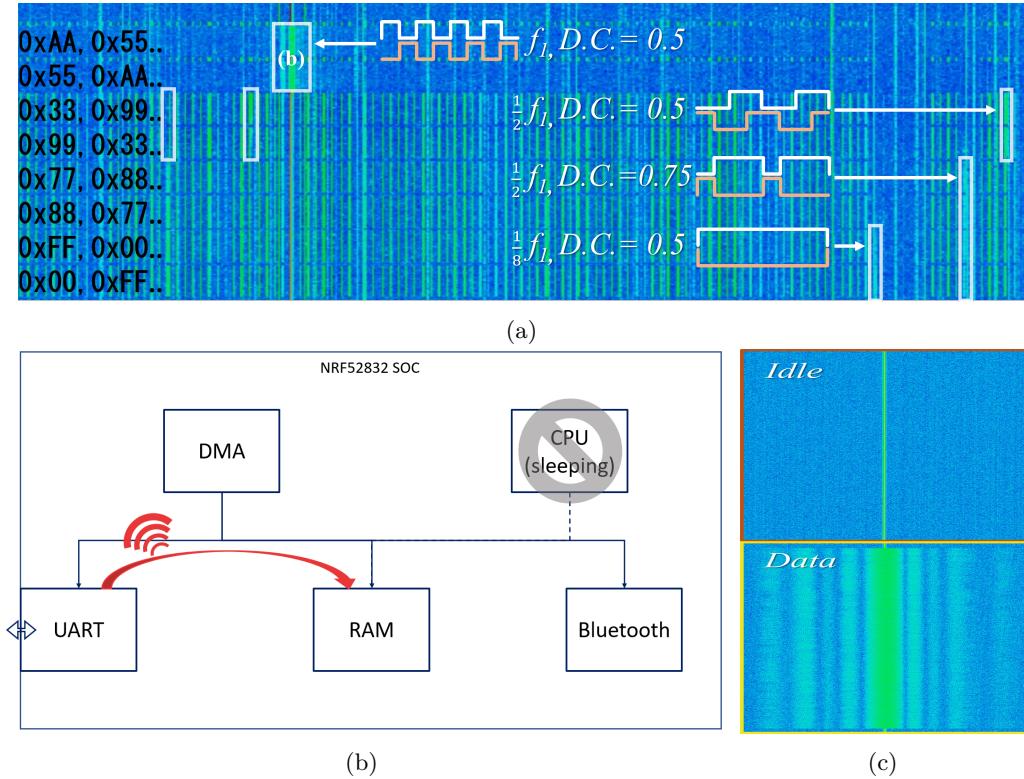


Figure 7: **nRF:** An example of The RF emissions reacting to Data written to the RAM buffer: (a) The spectrum around 2.56GHz were internal soc activity is observed. Indicated on the side of each section is the value of the looping data stream. Marked are frequencies which modulate according to specific values being written. (b) system configuration for direct memory R/W readouts: only serial and memory are activated by PC input, The Bluetooth is idling in the background and transmitting R/W EM disturbances. (c) Zoom-in view of signal with Values being written to memory (bottom) vs without (top).

clock domain. The Specific frequencies marked were modulating in reaction to specific data content being written into RAM. We have written to the chips UART the binary values 0xaa and 0x55 alternatively and out observed a frequency highlight and modulation. A focused view in 7c clearly shows an area where there is no special noise activity modulate in a repeating pattern in response to the repeated memory activity. Different values written were observed on different frequencies highlight. the values 0xaa, 0x33, 0x77 and 0xff00 Have been chosen to multiply the frequency toggling ones to zeroes. The hamming distance between the 2 different values written in a loop is also varied. The correlation between data being leaked and either the modulation and the specific frequency it is on, might not be intuitive to the naked eye. Dictating the frequency and modulation would be many factors and would need access to the inner implementation of the chips design to explain. The essence of the experiment is to show that even dealing with our attack target as a black-box we can still read the data consistently from the RF side-channel.

In conclusion of this section: different embedded systems might require more advanced equipment for better capture resolutions than are shown here. This would change according to internal workings transmission protocol and memory management architecture. More consistent results and usable data streams could then be achieved. But once studying a specific chip leaked data “signatures”, any resourceful attacker can scale the attack to snoop on any of said chip operational in the field.

6 Code Injection Gadget

An adversary might want to exfiltrate sensitive raw/encrypted data. We can consider a scenario where the adversary constantly monitors signals, or deliberately injects (e.g.,) malware/code/sniffing-mechanism into the device. We were interested in evaluating the special RF case and how to shape such a ‘Code Injection’ Gadget which will specifically modulate leakage in a way which is easily captured by the RF apparatus. I.e., input sensitive *Data* interacting or passing through gadget will be transmitted via this RF covert channel, and generate a side-channel signal which is easily de-modulated. Some modulated transmissions that an attacker might implement are PWM, FM, AM which are shown in Fig. 8b, 8c, 8d, respectively.

The field of malicious code injections is already well established and commonplace. But the implications of a covert outward communications channel to such an attack can be game changing in some target scenarios. An attacker might require the physical location of some device and with some triangulation achieve the location which the device itself might not have stream out, without interrupting the DUT conventional communication channels. Similarly, direct modulation of any raw sensitive data can be modulated transmitted and intercepted from the RF channel by such a gadget.

Assuming The attacker achieved malicious code execution on said device; If he requires FM, PWM transmissions of data he needs to modify the CPU’s flow to jump between distinct operating power draw levels. Once such measurable flow is isolated all the attacker needs is to jump to the high current state in a modulated timing using injected code such as in the loop based examples in Fig 8a. The generated RF output will be modulated and broadcast the hidden data the attacker requires. In figure Fig 8d it is shown that in some memory allocations we even observed analog signal variation in leaked transmission according to memory stored value, so with a specific values stored (in program memory in this case) and then reading those value sequentially by this AM modulation. A pseudo-code is provided in Fig 8a as well as abstract simplified algorithm in Algorithm 1. Various parameters exist here for the adversary \mathcal{A} to tailor the modulation, such as loops periodicity, duty-cycle and size utilized in memory.

The currently accepted methods to detect unauthorized RF transmissions assume they’re looking for known protocols over the standard frequencies. This attack has 3 advantages over current RF attacks:

RF Code injection Gadget:

Characteristics: Optimized for passive RF leakage exfiltration

```

Input: address or data
↓
FM_modulation(){
    data_FM[MEMSIZE]
    Loop:
    for i=1:MEMSIZE
        for j=1:data_FM[i]/2
            NOP//some CPU OP
        for j=1:data_FM[i]/2
            NOP}

    PWM_modulation(){
        data_PWM[MEMSIZE]
        Loop:
        for i=1:MEMSIZE
            for j=1:period*data_PWM[i]
                NOP//some CPU OP
            for j=1:period*(1-data_PWM[i])
                NOP}

    AM_modulation(){
        data_AM[MEMSIZE]
        Loop:
        for i=1:MEMSIZE
            for j=1:period //DATA is either case on
                //data_AM[i] or Hard-coded
                //in immediate values
                volatile int value=DATA
            for j=1:period
                volatile int value=0}

```

(a)

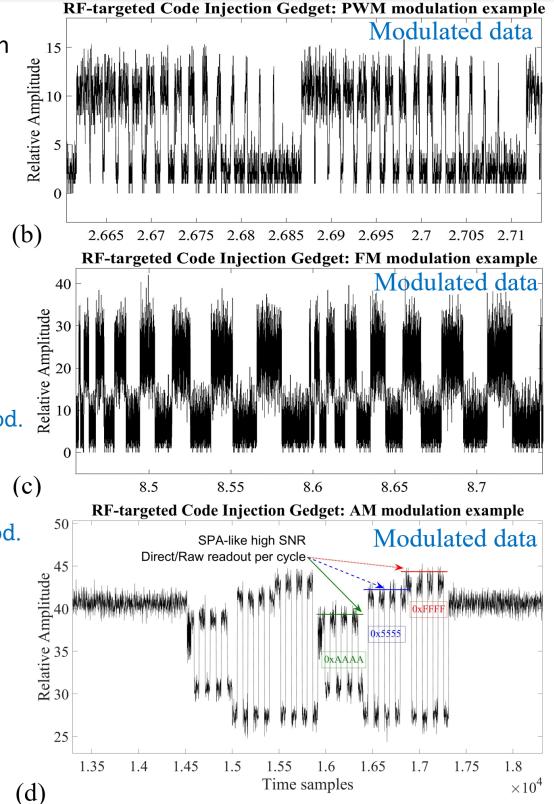
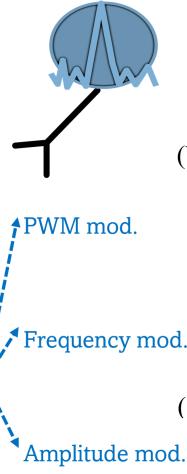


Figure 8: Code Injection Gadget - RF modulation

- **Power:** by modulating over an existing more powerful RF protocol we can achieve distance while keeping our own signal intensity low. unlike previous RF attacks which have to transmit with full power their own signal to achieve distance.
- **Frequency:** The modulated signal utilizes radio channels outside the expected RF spectrum and in a narrow bandwidth.
- **Protocol-level:** can transmit some unexpected protocols which aren't standard in the chosen RF band.

These aspects makes this attack extremely hard to detect and scan for without having previous knowledge of the attack implementation.

Algorithm 1 Simplified example: memory-cache procedure

- 1: **Pre-processing:** Store a series of (presumably secret) values in a memory address space.
- 2: **Pre-processing:** choose a subset of addresses (denote Add_{space}) to exfiltrate information from.
- 3: **Pre-processing:** define a volatile variable vector, $temp$, size of Add_{space} and set to all zeroes vector.
- 4: **RF encode:**
- 5: **Loop:** over all Add_{space} and perform reads to $temp$ elements.
- 6: **Launch Tx and Rx device.**
- 7: **Capture spectrum.**
- 8: **Filter and export time signal.**

7 Direct Information Readout and De-modulation: JTAG

JTAG (Joint Test Action Group) is a standard for testing and debugging integrated circuits (ICs) and printed circuit boards (PCBs). It uses a serial communication protocol to access the internal registers and test points of a device for the purpose of testing and debugging. With JTAG, you can perform a variety of tasks, such as program non-volatile memory such as flash memory or EEPROM on a device, direct access to the internal registers of a device, test the functionality of an IC or PCB, remotely troubleshoot and debug, Boundary-scan testing and more. When JTAG protocol leak from the device, an attacker is able to obtain various parameters, including the program memory, writing to various registers, and more.

The experiment we performed shows that the JTAG protocol leaks to the radio module, and this up-converted the JTAG protocol to a frequency of 2.4 GHz. As a result, the JTAG protocol was added to 2.4 GHz Bluetooth module. Fig. 9 shows an example of the

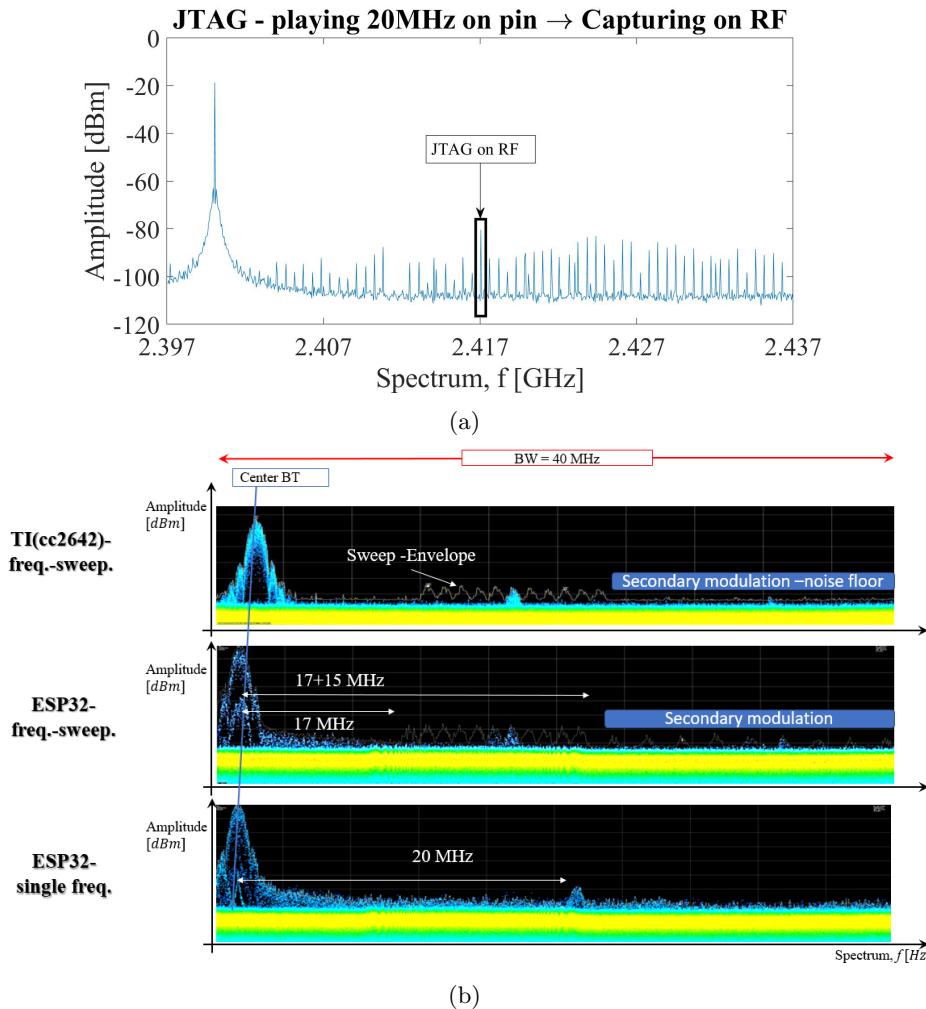


Figure 9: JTAG sniffing: (a) 20 MHz over JTAG pin appearing in RF channel in the Spectrum domain over the nRF device (b) spectrum domain: **Top**, TI(cc2642) device, signal sweeps 17-32 MHz **Middle**: ESP32 device **Bottom**: single 20 MHz signal on the JTAG pin over the ESP32 with 20 MHz.

TCK leg leakage of the JTAG protocol at different frequencies. Fig. 9a shows the leakage in the spectrum, along with the Bluetooth protocol. In order to see the signal in a better way, it was necessary to use a band pass filter with a bandwidth of 1MHz to isolate the signal from the Bluetooth protocol. Fig. 9b shows the leakage of the JTAG protocol TCK leg, on different devices (TI, ESP32), and at different frequencies (10 - 20 MHz). It can be concluded from this experiment that the JTAG protocol flows through the radio module out to the ISM band on various devices as illustrated within the figure.

8 SPI-Flash, ESP32 device

Non volatile flash memory devices are commonly used to store program data and are regularly mounted besides the actual device as it is much cheaper than fabricating the memory inside the SOC die. Specifically in our case the ESP32 has an external SPI controlled flash device to flash the program, this flash memory can be written via serial UART or the chip itself.

As we have demonstrated for (e.g.,) the UART and JTAG, digital traffic leaks through RF. We assumed the same could be said about the onboard SPI interface communicating with the critical Flash. So we configured the setup to verify it is so. Our setup, and different measurement scenarios evaluated such as near-field and far-field measurements, were focused to minimize previously shown leakages activity so we should isolate any emissions caused directly by the SPI interface itself.

Active modules in our setup consist of The CPU, WiFi, and SPI as illustrated in Fig. 11(a), like so:

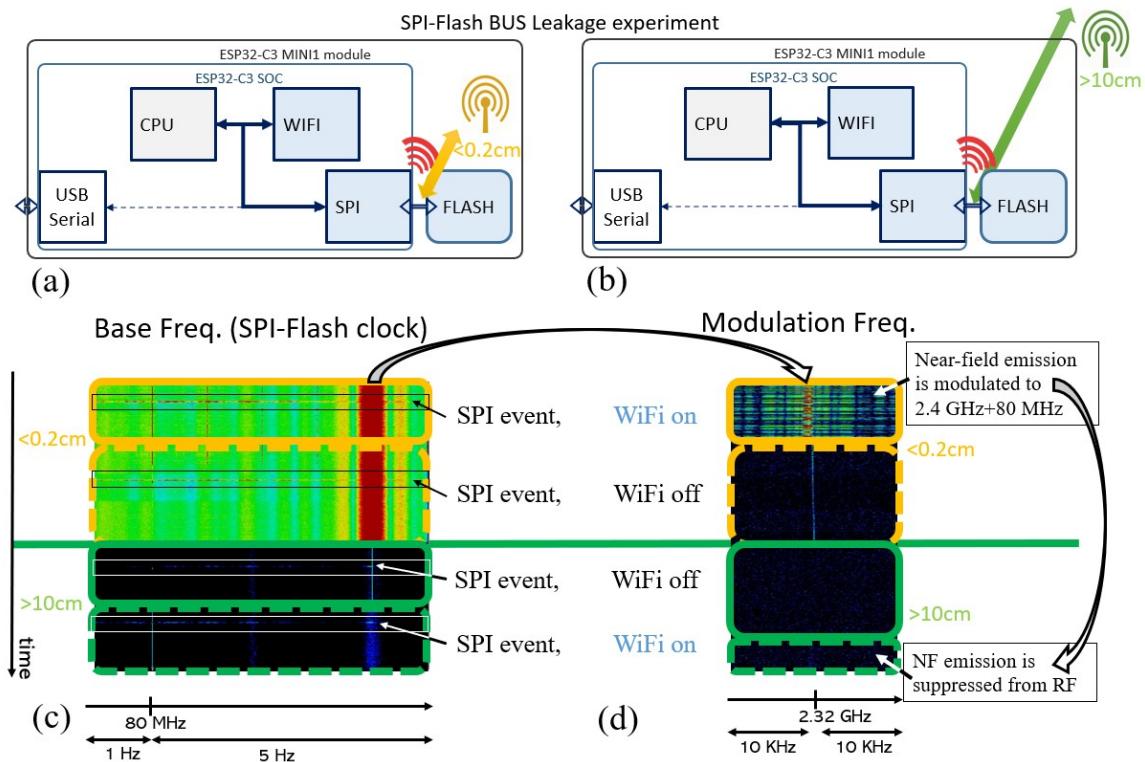


Figure 11: SPI Flash leakage: (a) NF measurement abstract setup (b) FF measurement abstract setup, and (c), (d) corresponding spectrum around the base frequency of 80MHz and 2.32GHz, respectively.

- The CPU activates the wifi and spi transactions Operated in 160MHz.
- As a result WiFi continuously transmits in 2.4GHz.
- The SPI interface controls a separate flash chip housed close under the RF shield with the main chip, Operated in 80MHz.

First, as illustrated in Fig. 11(a) we have performed a near-field (NF) measurement from practically zero distance directly above the RF shield housing the ESP32 and flash devices, And from a distance greater than 10cm away from the board as illustrated in Fig. 11(b). From Fig. 11(c) we can see the spectrogram where first (top) part of the spectrogram shows near-field emanation centered around 80MHz and SPI-Flash events are clearly identified as marked with black rectangles, **both when WiFi is enabled and disabled** indicating a clear NF Flash leakage which is a very alarming situation on its own indicating the need of non-natively supported NF leakage protection. In the bottom part of the spectrogram (10cm airgap) this information is vanished, though some weak transmission appears around the 80MHz of the SPI-Flash data packet which **modulates more when the WiFi is On**. Second, as shown in Fig. 11(d) around the modulation frequency which is $2.4\text{GHz}\pm80\text{MHz}$, clearly one can see the NF leakage was leaked to this modulated carrier when the antenna was placed in close proximity, but this is **visible only when the WiFi is On**, meaning some SPI protocol leaks to the RF modulator or surrounding circuitry. Taking both said mutual NF leakages into account (explicitly, the SPI signal leaks into Wifi frequency-range and the Wifi signal leaks into SPI frequency). Therefore, it is clear there is at least **some** EM relationship crossing the RF module isolation boundaries. However, when the antenna is taken further away we can see that no clear FF emanation exists when the WiFi is On, meaning **the leaked signal to the RF modulator does not pass amplification and is filtered-out/suppressed from RF**.

Clearly, we see an alarming situation: NF leakage and modulation of that leakage by TX logic. However, in this platform and with our setup/equipment we do not capture the information from afar. We leave this point to further investigations: perhaps better (less noisy) setup in a shielded room and better equipment will show otherwise, perhaps different devices will behave differently.

9 NFC leakage

Near Field Communication (NFC) is a set of communication protocols for communication between devices that are in close proximity to each other, typically no more than a few centimeters. NFC is based on radio frequency identification (RFID) technology and is used for a variety of applications, such as contactless payments, data exchange, and access control. NFC-enabled devices, such as smartphones, can be used to make payments at retail locations, transfer files and data between devices, and unlock doors or access restricted areas with a simple tap or wave. NFC is generally considered to be a secure form of communication, but there are some potential security risks to be aware of.

In some SoC device, the NFC protocol can leak to the Bluetooth radio transceiver, thus appearing at a higher frequency of the Bluetooth protocol (2.4GHz-13MHz) and be transmitted to long distances than was intended to (as illustrated in Fig.12a).

An experiment was performed when the signal of the NFC protocol was sampled at the same time the Bluetooth protocol was sampled. At the same time as the signal was sampled, we have activated the NFC protocol by bringing a mobile device closer to the nRF device. For capturing the NFC protocol, we used a Pico-scope 5 series and a NEAR FIELD antenna. The nRF device also include NFC antenna. For capturing the leakage in Bluetooth frequencies, we use an RSA 306b spectrum analyzer and a basic dipole antenna located a few meters from the NFC device, it is possible to move further away and increase the gain or a more directional antenna. In order to run the experiment, a code was written for the NFC device in order to create a connection with the NFC protocol at the same time as transmitting data on Bluetooth frequencies. The experimental process: After bringing

the mobile device close to the nRF, the flow of data from the mobile device to the nRF device is clearly seen by the scope (Fig. 12b), at the same time at frequency 2.4GHz-13MHz an envelope is visible identical to the NFC protocol envelope (Fig. 12c), it was found that even the NFC data flows to the Bluetooth frequencies (Fig. 12d). Conclusions: The NFC protocol located near the Bluetooth radio in the SoC component or close to it, leaks within high frequencies of the ISM protocols.

10 Conclusions, Extent and Open-Questions

In this paper, we present a much wider scope of the leakage in transmission of mixed-signal devices and systems, emanated from various elements of the embedded-system into the receiver Antenna, mainly focusing on direct readout or no statistics/averaging, as compared to prior-art.

We broadly report a phenomenon of information leakage from wireless and computing components within the system, on-board, and from the same IC chip. In addition, it can be concluded from this study that today's standard dealing with the subject of electromagnetic

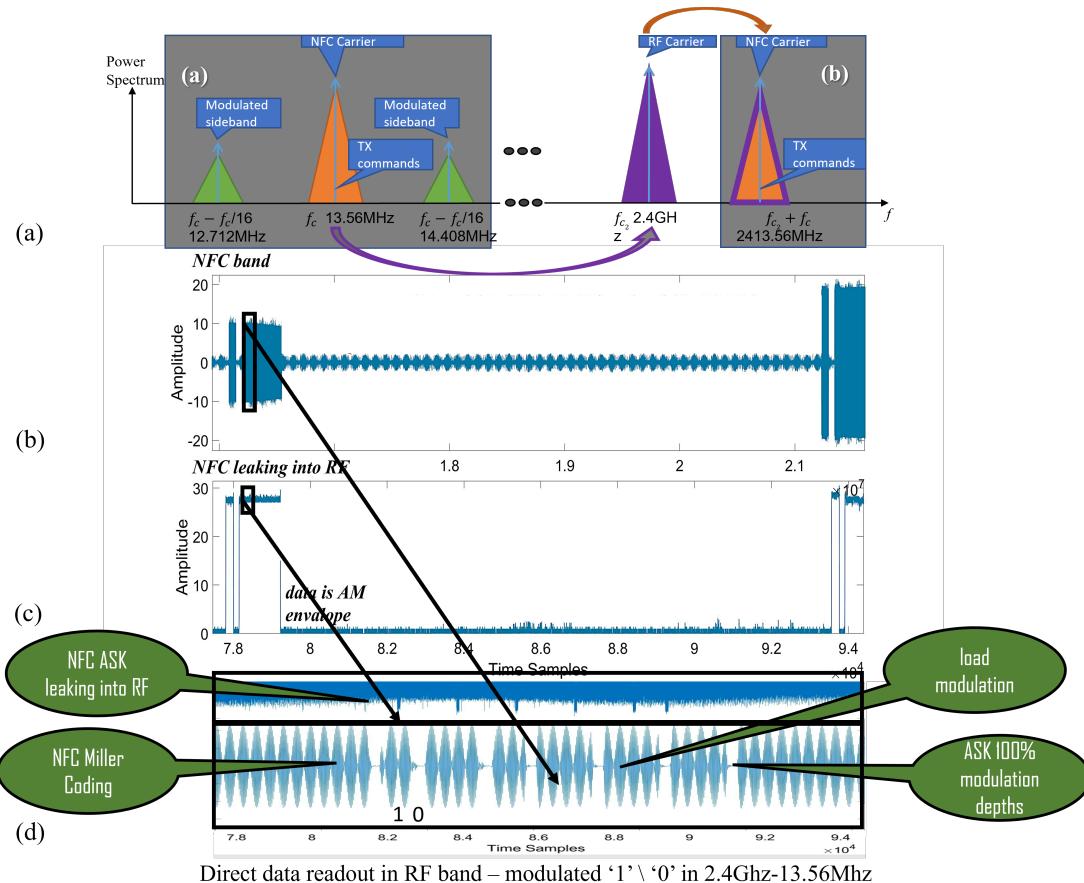


Figure 12: NFC protocol, designed to transmit for only few centimeters, leaks into far-field tens/hundreds meters: (a) abstract illustration of modulation and leakage into RF bands, (b) readout in the NFC domain 13MHz range in ASK modulation, (c) a direct equivalent sequence readout (the envelope for the NFC protocol and the data inside) in the RF 2.4GHz±13MHz range and, (d) example for the data leakage from the nRF communication the the 2.4GHz±13MHz range

interaction between modules (crosstalk) is not suitable for the world of information security, what is true for the correct/reliable operation of a circuit, is certainly not sufficient to set standards or goals for the world of information security, this phenomenon can be seen in a variety of components. Another conclusion from this study is that it is relatively simple to monitor sensitive information from various communications and peripherals in a system chip such as serial communications, JTAG, writing to memory, Flash devices or even other radiating protocols such as NFC, and more, as opposed to extracting encryption keys, in which case the leaking signal is much lower (smaller SNR). Therefore, a complex analysis is required and the information is not obtained directly from the emission.

Concretely, we show how on-board signals with galvanic connection to the Tx Antenna-chip and on-board signals without galvanic connection to the Tx Antenna-chip itself, all leak direct information up to tens of centimeters from source to the Tx Antenna. The extent of this alarming situation induces signal-integrity implications within the embedded system, and significant implications relating to device-isolation and user-isolation, it may also affect standards and specifications for e.g., electromagnetic compatibility (EMC), on-board signal shielding, electromagnetic and RF interference (EMI, RFI), cross-talk, and generally design-for-manufacturing (DFM) guidelines for both intra-IC and PCB board. We demonstrate such direct readout of signals with commercial and low-cost equipment indicating how problematic the situation is.

Among the many open questions we identify, our aim to start investigation which relates to: first, technological effects, such as less/more miniaturized embedded system such as multi-chip-module (MCM), Silicon-in-package (SiP) technologies, interposers and stacked-devices through VIAs or advanced substrates, and evaluation of security implications of an RF-system in such a scenario; and second, making a clear connection between communication and reliability metrics such as “communication”-SNR and dB signal degradation in (e.g.,) some band, say ISM and other metrics, and on the other hand cryptographic hardware security metrics, and trying to provide a starting-point answer to the challenge.

Acknowledgments. Itamar Levi was partially Funded by the Israel Innovation Authority (IIA), Bio-Chip Consortium Grant file No. 75696, Israel Ministry of Defense Directorate of Defense Research and Development (IMOD DDR&D), Research Grant 4441189902 and Israel Science Foundation (ISF) grant 2569/21.

References

- [ABC⁺17] Akhil Arunkumar, Evgeny Bolotin, Benjamin Cho, Ugljesa Milic, Eiman Ebrahimi, Oreste Villa, Aamer Jaleel, Carole-Jean Wu, and David Nellans. Mcm-gpu: Multi-chip-module gpus for continued performance scalability. *ACM SIGARCH Computer Architecture News*, 45(2):320–332, 2017.
- [AKM17] Angelos Antonopoulos, Christiana Kapatsori, and Yiorgos Makris. Security and trust in the analog/mixed-signal/rf domain: A survey and a perspective. In *2017 22nd IEEE European Test Symposium (ETS)*, pages 1–10. IEEE, 2017.
- [ALWS17] Kamran Ali, Alex X Liu, Wei Wang, and Muhammad Shahzad. Recognizing keystrokes using wifi devices. *IEEE Journal on Selected Areas in Communications*, 35(5):1175–1190, 2017.
- [CA16] Brent Carrara and Carlisle Adams. Out-of-band covert channels—a survey. *ACM Computing Surveys (CSUR)*, 49(2):1–36, 2016.
- [CFS20] Giovanni Camurati, Aurélien Francillon, and François-Xavier Standaert. Understanding screaming channels: From a detailed analysis to improved attacks.

- IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 358–401, 2020.
- [CFWX20] Minhao Cui, Yuda Feng, Qing Wang, and Jie Xiong. Sniffing visible light communication through walls. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, pages 1–14, 2020.
 - [CPM⁺18] Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. Screaming channels: When electromagnetic side channels meet radio transceivers. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 163–177, 2018.
 - [Gur22] Mordechai Guri. Satan: Air-gap exfiltration attack via radio signals from sata cables. In *2022 19th Annual International Conference on Privacy, Security & Trust (PST)*, pages 1–10. IEEE, 2022.
 - [GZBE19] Mordechai Guri, Boris Zadov, Dima Bykhovsky, and Yuval Elovici. Powerhammer: Exfiltrating data from air-gapped computers through power lines. *IEEE Transactions on Information Forensics and Security*, 15:1879–1890, 2019.
 - [HHM⁺14] Yuichi Hayashi, Naofumi Homma, Mamoru Miura, Takafumi Aoki, and Hideaki Sone. A threat for tablet pcs in public space: Remote visualization of screen images using em emanation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 954–965, 2014.
 - [HMH⁺12] Johann Heyszl, Dominik Merli, Benedikt Heinz, Fabrizio De Santis, and Georg Sigl. Strengths and limitations of high-resolution electromagnetic field measurements for side-channel analysis. In *International Conference on Smart Card Research and Advanced Applications*, pages 248–262. Springer, 2012.
 - [HPWW22] Haiqing Hao, Zhongwang Pang, Guan Wang, and Bo Wang. Indoor optical fiber eavesdropping approach and its avoidance. *arXiv preprint arXiv:2207.05267*, 2022.
 - [KFH19] Masahiro Kinugawa, Daisuke Fujimoto, and Yu-ichi Hayashi. Electromagnetic information extortion from electronic devices using interceptor and its countermeasure. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2019(4):62–90, 2019.
 - [LGG⁺21] Corentin Lavaud, Robin Gerzaguet, Matthieu Gautier, Olivier Berder, Erwan Nogues, and Stephane Molton. Whispering devices: A survey on how side-channels lead to compromised information. *Journal of Hardware and Systems Security*, 5(2):143–168, 2021.
 - [LJL⁺16] Marc Lichtman, Roger Piquerias Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, and Jeffrey H Reed. Lte/lte-a jamming, spoofing, and sniffing: threat assessment and mitigation. *IEEE Communications Magazine*, 54(4):54–61, 2016.
 - [LMPT15] Jake Longo, E De Mulder, Dan Page, and Michael Tunstall. Soc it to em: electromagnetic side-channel attacks on a complex system-on-chip. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 620–640. Springer, 2015.
 - [LMRZ16] Mina Labib, Vuk Marojevic, Jeffrey H Reed, and Amir I Zaghloul. How to enhance the immunity of lte systems against rf spoofing. In *2016 International Conference on Computing, Networking and Communications (ICNC)*, pages 1–5. IEEE, 2016.

- [MSBK16] Nikolay Matyunin, Jakub Szefer, Sebastian Biedermann, and Stefan Katzenbeisser. Covert channels using mobile device’s magnetic field sensors. In *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, pages 525–532. IEEE, 2016.
- [MTGJ21] Haoyu Ma, Jianwen Tian, Debin Gao, and Chunfu Jia. On the effectiveness of using graphics interrupt as a side channel for user behavior snooping. *IEEE Transactions on Dependable and Secure Computing*, 2021.
- [NSA82] NACSIM NSA. 5000: Tempest fundamentals. *National Security Agency, Partially declassified transcript: <http://cryptome.org/nacsim-5000.htm>*, 1982.
- [SBO⁺15] Daehyun Strobel, Florian Bache, David Oswald, Falk Schellenberg, and Christof Paar. Scandalee: a side-channel-based disassembler using local electromagnetic emanations. In *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 139–144. IEEE, 2015.
- [SLKS18] Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. Accuracy enhancement of electromagnetic side-channel attacks on computer monitors. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pages 1–9, 2018.
- [Tai00] King L Tai. System-in-package (sip): challenges and opportunities. In *Proceedings 2000. Design Automation Conference.(IEEE Cat. No. 00CH37106)*, pages 191–196. IEEE, 2000.
- [TEM] Tempest standards overview: <https://cryptome.org/2013/01/tempest-standards.pdf>.
- [VP09] Martin Vuagnoux and Sylvain Pasini. Compromising electromagnetic emanations of wired and wireless keyboards. In *USENIX security symposium*, volume 1, 2009.
- [WWD20] Ruize Wang, Huanyu Wang, and Elena Dubrova. Far field em side-channel attack on aes using deep learning. In *Proceedings of the 4th ACM Workshop on Attacks and Solutions in Hardware Security*, pages 35–44, 2020.
- [WWZZ15] Teng Wei, Shu Wang, Anfu Zhou, and Xinyu Zhang. Acoustic eavesdropping through wireless vibrometry. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, pages 130–141, 2015.
- [ZLAA⁺18] Mingmin Zhao, Tianhong Li, Mohammad Abu Alsheikh, Yonglong Tian, Hang Zhao, Antonio Torralba, and Dina Katabi. Through-wall human pose estimation using radio signals. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 7356–7365, 2018.