Assault and Battery: Evaluating the Security of Power Conversion Systems Against Electromagnetic Injection Attacks

Marcell Szakály
University of Oxford
United Kingdom
marcell.szakaly@cs.ox.ac.uk

Sebastian Köhler
University of Oxford
United Kingdom
sebastian.kohler@cs.ox.ac.uk

Martin Strohmeier
armasuisse
Switzerland
martin.strohmeier@ar.admin.ch

Ivan Martinovic
University of Oxford
United Kingdom
ivan.martinovic@cs.ox.ac.uk

***Abstract*—Many modern devices, including critical infrastructure, depend on the reliable operation of electrical power conversion systems. The small size and versatility of switched-mode power converters has led to their widespread use. While transformer-based systems passively convert voltage, switched-mode power converters have an actively controlled feedback loop that relies on accurate sensor measurements. Previous academic work has shown that many types of sensors are vulnerable to Intentional Electromagnetic Interference (IEMI) attacks, and it has been speculated that power converters are also susceptible.**

In this paper, we present the first detailed and practical evaluation of IEMI attacks against switched-mode power converters as a whole by manipulating the voltage and current sensors in their feedback loops. We develop a novel multi-frequency IEMI attack technique to effectively target devices with multiple sensors. We experimentally validate our theoretical predictions by analyzing multiple AC-DC and DC-DC converters, automotive-grade current sensors, dedicated battery chargers, and a real-world electric vehicle charger. Our attack is reliably effective at overcharging and permanently damaging Li-ion cells, and causing the EV charger to output 50 V more than it reports.

1. Introduction

Modern electronics are highly complex devices, often containing a mixture of analog, digital, sensing and actuation electronics, which require many different voltages. Additionally, modern renewable energy technologies increasingly require variable DC voltages, such as battery charging and Maximum Power Point Tracking in solar power. These requirements are driving the adoption of cheap and versatile switched-mode power converters. Switched-mode power supplies encompass a wide range of devices of different sizes and capabilities, including AC-DC and DC-DC converters, from small devices integrated into portable electronics, over EV charging, to grid scale conversion for long distance DC transmission lines.

Failure of a power converter renders the entire device unusable and may even cause permanent damage. Many electronic components are destroyed by applying too much voltage to their input, and lithium-based battery chemistries can catch fire as a result of overcharging [1]. Different laws regulate the transportation of batteries around the world, for example, ferries in Greece only allow EVs with batteries less than 40% charged [2] and passengers on airplanes can only carry batteries below a certain capacity [3]. In addition, there are outright bans on some products that have proven to be particularly dangerous, such as e-scooters on London's public transport [4], or the Samsung Galaxy Note 7 on most major airlines [5].

Switched-mode power supplies are actively regulated devices. This means that they monitor their output and adjust their operation to achieve the desired voltage or current. A large body of previous work has shown that various sensors are vulnerable to physical-layer attacks [6], [7], and it has been proposed that IEMI is effective against standalone voltage sensors [8].

To the best of our knowledge, no prior work has presented a detailed theoretical and experimental evaluation of IEMI attacks on power conversion systems and their feedback loops, instead only showing attacks against standalone voltage sensors and simulated evaluations [8], [9]. In this paper, we overcome these limitations and present the first evaluation of sensor attacks against various power conversion systems. Our proposed wireless attack uses Intentional Electromagnetic Interference (IEMI) and can be carried out using cheap off-the-shelf equipment, making the barrier to entry for an adversary low.

Contributions: We identify multiple differences between power converters and other targets for IEMI sensor attacks,

Published by IEEE in Proceedings of the 2024 Annual Computer Security Applications Conference (ACSAC). DOI 10.1109/ACSAC63791.2024.00033.

that raise the inherent barrier for entry. Nonetheless, we show that the attacks are still viable, with significant real-world impact. We present a detailed evaluation of IEMI attacks against power converters, examining the scope and scalability of the attack. We discuss the complexity of multiple sensors being involved in the CC-CV battery charging scheme, and develop a novel multi-frequency IEMI attack to address this challenge. We demonstrate our attack on a real EV charger, and use a COTS battery charger to overcharge and destroy several Li-ion batteries.

2. Related Work

Academic literature has presented several examples highlighting the importance of sensor reading integrity [6], [7], with attack signals ranging from acoustic waves [10], [11] over light [12], [13] to wired [14] and wireless RF signals. In particular, signal injection into analogue sensor systems using IEMI is a well documented attack vector, which has been demonstrated experimentally against a variety of systems. IEMI attacks have been used to inject intelligible signals into microphones [15], [16], cameras [17], [18] and even digital communications [19]. In addition, it has been shown that IEMI can inject DC offsets into systems such as temperature sensors [20], voltage and current sensors [8], and output driving signals [8], [21].

In the context of power electronics, a large body of work exists in the engineering and chemistry literature to study the safety properties of battery systems [1], [22], with the threat model assuming accidental malfunction instead of active attacks. In addition, researchers have studied the EV powertrain and charging against software based attacks [23], [24].

Three previous papers are closely related to this present work, as they study electromagnetic attacks on power converters. In [8], the authors demonstrated an attack against a standalone voltage and current sensor, taken from a power converter. In their experiments, they used an inductively coupled attack source, by placing a toroidal magnet around the voltage sensor wires, which is unable to scale towards a remote attack. They showed that both standalone sensors can be affected, with a $200\,\mathrm{mW}$ signal source at close proximity making the sensor measure $42\,\mathrm{V}$ instead of $21\,\mathrm{V}$. The paper only presents attacks against the standalone sensor, it does not actually raise the voltage. Our paper improves upon this work, by attacking sensors as they are also used inside unmodified COTS power converters, during operation, to study the real-world challenges of such an attack and the practical impact on the output. Furthermore, we use a radiating attack source, and present attacks from a distance.

In [25], the authors presented an end-to-end attack on solar inverters, using an electromagnet pulsed at $1\,\mathrm{Hz}$. Due to the use of a non-radiating transmitter and low frequency, this attack can not scale to a distance. Moreover, we focus on converters outputting DC power (AC-DC and DC-DC converters), not AC power (inverters), due to their different architecture and control schemes.

In [9], the authors studied by simulation the effect of low frequency ripple on boost converters. Their simulation results show that an attack affecting the voltage sensor measurement can affect the output voltage of the device. The low frequency attack leads to an increased ripple in the output, and can even lead to an increase in the output voltage.

Compared to established sensor attacks, we expect multiple challenges: Unlike sophisticated sensors designed to measure mV signals, sensors in power converters have to deal with large, many volt signals. Large filter capacitors are present to smooth voltages, and can absorb attack signals. Finally, devices incorporate multiple different sensors.

3. Threat Model

Goals: We assume an adversary whose goal is to wirelessly disrupt the proper functioning of a power supply using only intentional electromagnetic interference. The attack can cause a temporary denial of service by lowering the voltage or shutting down the system or, in a more serious case, cause permanent damage by increasing the voltage and current. Given the growing importance of battery systems in consumer electronics, electric vehicles, and photovoltaic systems, we assume that the attacker would be particularly interested in battery charging systems with the goal of causing permanent damage. The intent of such an attack can vary from denial of service to blackmail.

Capabilities: Given the low barrier of entry for IEMI attacks, we consider an adversary with the budget and knowledge of a motivated hobbyist. In addition, access to only commercial off-the-shelf (COTS) equipment is required. This includes a signal generator or software-defined radio capable of operating in the required frequency range, a suitable high-gain directional antenna, and, if necessary, a suitable RF amplifier to increase the range of the attack. In line with related work in the area of IEMI, we assume that the attacker has access to appropriate amplification needed to achieve the required distance from the target [19], [26].

Scenarios: We briefly discuss possible attack scenarios to illustrate how the attack can be used. The attacker must hide their EMI emitter close to the target device, but they do not need to personally remain present. Public targets such as photovoltaic installations, power infrastructure or EV chargers are often unattended, and can be approached at close proximity. Trash bags or cardboard boxes can be used as camouflage, as such items are often found in outdoor, urban environments. For indoor targets, the attacker must choose an appropriate disguise, or operate at an increased distance. Additionally, the attacker can place their device on the bottom of a table, inside a drawer or on the other side of a wall. The added material between target and attack device attenuate radio signals, however this is compensated by the proximity the attacker can achieve.

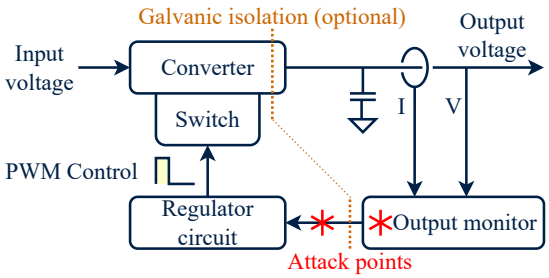


Figure 1: Diagram of a generic switched-mode converter, showing the 4 most important functional components, as well as the most vulnerable part of the circuit where we expect the attack signal to couple into.

4. Background

In this section, we present a brief technical overview of power converters and battery charging.

4.1. Power Converters

Power converters convert between AC and DC, or different voltage levels. The two simplest options are transformers (AC-AC) and rectifiers (AC-DC). While simple to make, they have limited capabilities [27].

Many modern applications demand small, light, high efficiency devices, able to handle fluctuating input voltages (e.g. those provided by a battery) with a variable output (such as needed for USB Power Delivery). Switched-mode power supplies meet all these requirements with a complex, actively regulated architecture, made possible by modern low cost semiconductors. They can produce a constant output voltage or current regardless of input fluctuations, and can be adjusted during runtime. The constant current feature is particularly important for battery charging, LED [28] and laser diode applications. They are thus widely used in AC-DC and DC-DC converters, in a wide range of applications.

Their operation relies on switching their input into a coil at a high frequency (often 10 to 100 kHz), transferring energy from the input to output in small packets. Many specific architectures exist, differing in arrangement of coils, capacitors, diodes and switches. The output is determined by the input voltage, the duty cycle of the switching, and potentially the load on the output. Active regulation monitors the output, derives a feedback signal that is fed into the controller, which adjusts the duty cycle of the system accordingly. By creating a feedback loop that adjusts the output based on the feedback signal, the system is able to maintain the output at a stable value, regardless of any changes. A generic schematic of a switched-mode power converter is shown in Figure 1.

For low cost devices, a single switched mode regulator IC incorporates all of these features, requiring minimal external components, while more complex devices have an array of dedicated ADC sensors, and digital control systems.

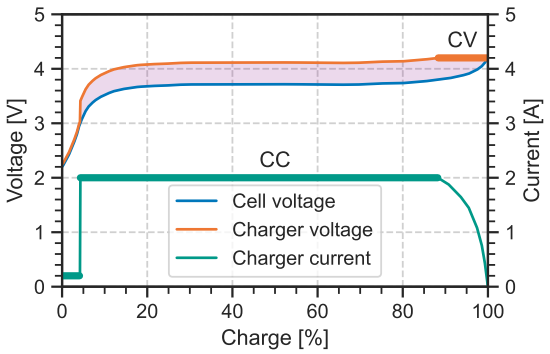


Figure 2: Approximate diagram of the charging phases for a Li-ion battery. The diagram shows the internal voltage of the cell, the external voltage (including the shaded voltage drop across its internal resistance), and the charging current. The bold sections show the limiting current and voltage during the CC and CV phases respectively.

4.2. Battery Charging

Batteries use chemical reactions to store energy. The electrical properties of a battery depend on the type of chemistry used, manufacturing specifics, and random process variations. Thus, correctly charging a battery requires appropriate circuits to generate the correct voltages and currents at all time.

Exceeding the maximum current of the battery can cause excessive heating, which leads to degradation and potentially damage. Exceeding the maximum voltage by even a small amount can cause breakdown of the internal structures, which causes permanent damage.

The battery can be modeled as a Thevenin equivalent circuit [29]: an ideal voltage source V_{cell} and an Equivalent Series Resistor (ESR) R_{ESR} in series. Charging the battery is done by connecting an external voltage V_{charger} larger than the internal cell voltage to the battery, this will cause current to flow into the battery given by:

$$I_{\text{charge}} = (V_{\text{charger}} - V_{\text{cell}})/R_{\text{ESR}} \quad (1)$$

The standard method for battery charging is the CC-CV scheme. In this, the current and voltage of the charger never exceed the current and voltage limits of the given battery. Early on in the charging process, the internal cell voltage is low, so the voltage of the charger is limited by the maximum current and internal resistance of the battery, called the Constant Current (CC) phase. As during the charging process the voltage of the battery slowly increases, so must the voltage of the charger in order to maintain the current at the maximum limit. Eventually, the voltage of the cell is so high that the charger would need to exceed the voltage limit for the given battery. At this point, the charger transitions into the Constant Voltage (CV) mode, where the voltage is no longer increased. After this, as the cell voltage increases further, the current slowly decreases. Chargers may

also include a pre-charge or regeneration phase [30], using a lower CC limit for deeply discharged batteries. The stages of charging are illustrated in Figure 2.

5. Attack Theory

In this section, we provide an overview of IEMI attacks, explain its application to power converters, and present our improvement to overcome the multiple sensors involved in the CC-CV scheme.

5.1. Attack Description

We propose an IEMI sensor attack, where a malicious RF signal is emitted to manipulate the measurements of the target. The wires inside the target act as unintentional antennas, receiving the attack signal. Since the attack signal is at a much higher frequency than legitimately occurring signals within the target, it has no direct effect on its behavior. However, previous work has shown that non-linear properties in the analog front end of sensor systems (amplifiers, ADCs, comparators) can demodulate high-frequency RF signals, converting them into a DC offset [31]. This effect is strongly frequency dependent, since the receiving "antenna" will be resonant at a certain frequency. This frequency depends on various factors, such as the length of the wire or PCB trace and the characteristics introduced by the non-linearity. We use this attack vector to modify the sensor readings of the voltage and current sensors that provide reference measurements for the feedback system in switched-mode converters.

Switched-mode converters rely on a feedback system for correct operation: the device measures its own output and compares it to a target value. For example, if the output is measured to be lower than it should be, the converter will increase the output voltage, thereby also increasing the measurement until the set value is reached. Our attack targets the integrity of the sensors used for this measurement. The goal of the adversary is to manipulate the sensor readings, so that the feedback regulator adjusts the output to a wrong and potentially harmful value. In other words, if the injected signal causes an offset between the real and measured value, the converter (falsely) corrects the output signal to ensure it matches the defined output value. The attacker can control the offset from the predefined value by varying the amplitude of the attack signal - a higher amplitude causes a larger DC offset and a more significant deviation from the predefined output voltage.

It is important to note that at each frequency, the attacker will only be able to induce either a positive or negative change in the sensor. Due to the feedback loop, if the attacker causes the sensor to measure more than the real value, they cause the feedback loop to lower the value, and vice versa. Thus, the high impact frequencies are those that lower the sensors value, thus increasing the output. Following the calculation in [20], we expect that at any given frequency, the impact of the attack is linear with the RF power.

5.2. Regulator Feedback

At its core, any feedback system takes in measurements of a system, compares them to a reference value, and then issues corrective actions. The corrective action causes the system to change, which changes the measurements, thus completing the feedback loop. In power converters, the measurement is related to the output voltage or current. The corrective action adjusts the pulse-width modulated duty cycle of switching, which then influences the output.

It is not always possible to measure the output directly: current sensors usually convert the current to a voltage, while high voltage systems need to decrease the voltage to a safe level. Additionally, converting the output before measurement allows the same IC to be configured to different output voltages via simple passive components. For example, an IC can be designed to keep its feedback pin at a precise voltage V_{ref}. If the output is connected to the feedback pin via a resistive divider that decreases the voltage to λV_{out}, the system will maintain V_{out} at V_{ref}/λ. Our proposed attack targets the measurement of the feedback pin, effectively shifting V_{ref}. Thus, under attack we get:

$$\Delta V_{\text{out}} = \Delta V_{\text{ref}}/\lambda \tag{2}$$

If converters only differ in their resistive divider values λ, and hence set output voltages V_{out}, we can conclude that the fractional impact of the attack is independent of the set output voltage:

$$\Delta V_{\text{out}}/V_{\text{out}} = \Delta V_{\text{ref}}/V_{\text{ref}} \tag{3}$$

5.3. Current Measurement Systems

Current limited (or Constant Current) power supplies are common for various applications. In essence, such a device seeks to output the maximum possible voltage, such that the voltage is less than the voltage limit, and the current is less than the current limit. If the output is, for example, short circuited, the voltage will be decreased to near zero, but a current equal to the current limit will still flow. Such devices are utilized extensively in laser diode and LED drivers [28], which are extremely sensitive to changes in their input voltage, and can best be controlled by limiting the current flowing through them. The CC-CV battery charging scheme (except for the regeneration phase) can also be performed simply using a current and voltage limited power supply, by setting the current limit to the desired CC charge current, and the voltage limit to the CV phase voltage.

In order to implement the current limit, the device must measure the output current. There are two primary ways to measure current: current shunt and magnetic fields. In the current shunt approach, the output current I is ran through a small resistor in series with the load, and the voltage difference across the resistor V_R is measured. The second method is to place a magnetic field sensor next to the wire and measure the current via its magnetic field.

Both of these methods are good targets for an attacker, since the current is first converted into small voltages, that will be heavily amplified.

5.4. Multi-Frequency Attack

To execute the CC-CV charging scheme, the device must contain sensors to measure both the voltage and current. If the attacker spoofs the current sensor, and increases the charge current, their attack will quickly hit the voltage limit. Similarly, spoofing the voltage sensor and overcharging the battery could lead to significant impact on its own, however the attack will be limited by the current limit. We thus develop a new way to achieve control of both sensors, by combining their respective EMI signals into a single transmission. Per our theory, each unintentional antenna will tune to different parts of the combined attack signal, thus achieving independent control of the two sensors.

Sensor may have vastly different effective frequencies, for example, below we show a system that needs a $1650\,\mathrm{MHz}$ and $855\,\mathrm{MHz}$ for its two sensors. It is thus not possible to use a low cost SDR to create the combined high bandwidth signal. To overcome this limitation, we use a passive power combiner device to merge two low bandwidth sources into a combined signal.

6. Susceptibility Evaluation

Our attack relies on unintentional antennae in the victim device receiving the attack signal, and demodulating it. As such, there are specific frequencies where the antenna and receiving circuit are resonant, and thus the attack signal is received at a high amplitude, while other frequencies are largely ignored. Furthermore, some frequencies may cause a positive offset in the sensor, whereas others may cause a negative offset.

6.1. Experimental Design

In this section, we seek to gain theoretical understanding of the attack, as well as explore the relevant parameters. We are interested in seeing how many devices are affected, how they respond to various frequencies, and how the attack is impacted by changes in the output load. These experiments are thus conducted in a lab setting, with low RF power and measurement instruments. In later sections we present high power experiments, as well as real world evaluation.

We set up each converter in realistic conditions connected to a power source and optionally a load. An antenna was placed next to the device, to irradiate it with an RF signal. The frequency of the signal varied across a wide range and the output voltage or current were recorded during the frequency sweep. A vulnerable device will be resonant to some attack frequencies, resulting in peaks in the output measurement around those specific frequencies. Multiple subsequent runs are performed, adjusting parameters such as the set output voltage or applied load, without changing the geometry or other parameters of the setup. An overview of the equipment is depicted in Figure 14 in the Appendix.

We used a Rhode & Schwartz SMC 100A or USRP N210 as our signal source, both emitting pure sine waves around a given frequency, with less than $20\,\mathrm{dBm}$ ($100\,\mathrm{mW}$).

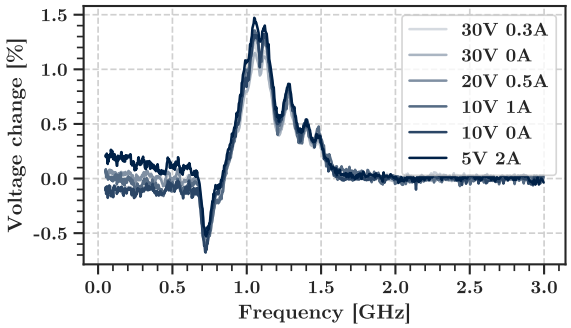


Figure 3: Frequency sweep results for DC-DC #1 at $80\,\mathrm{mW}$ attack power. Different lines represent different set output voltages and applied loads, however the relative change of the output voltage is always identical and peaks for an attack signal at around $1.1\,\mathrm{GHz}$.

Unless otherwise stated, to avoid affecting any of our measurement instruments, we used no additional amplification, and placed a VERT900 antenna next to the target. We investigated the $50\,\mathrm{MHz}$ to $3\,\mathrm{GHz}$ in most experiments, since it is easily accessible to potential attackers. High frequencies require expensive microwave components, while low frequencies require large antennas. In addition, our results did not suggest interesting behavior lying outside this range.

When testing devices under a load, we used the Rigol DL3021A DC load, which also measured the output voltage and current. The DC load can be programmed to act as a Constant Voltage (CV), Constant Current (CC) or Constant Resistor (CR) load, as appropriate for the given experiment. In addition, we use it as a battery simulator to allow testing battery chargers in a reproducible and safe way.

6.2. DC-DC Converters

DC-DC converters are used in many consumer products, where a single DC input is converted to appropriate levels for internal components, such as logic ICs, processors, or analog systems. To evaluate the security of common DC-DC converters, we tested various non-isolated, off-the-shelf DC-DC converter boards, available from commercial websites. These boards contain the same ICs and reference designs that is integrated into products.

A list of the converters tested and their relevant features can be found in Table 2 and seen in Figure 15. A benefit of these standalone devices is that they have adjustable resistors instead of fixed dividers, allowing us to test many different set output voltages, and compare them against the expected behavior.

6.2.1. Method. First, an output voltage was set by adjusting the resistor. Each device was powered by an input DC power source and connected to a Constant Resistor (CR) load at the output. To evaluate whether the load affects the attack, we also repeated the experiments without a load. An antenna

ID	Input	Output			Features	Topology	Main IC	Voltage sense	Current sense		
		Voltage		Current				Feedback	Shunt	Amp	Feedback
DC-DC #1	5.5 – 30 V	0.5 – 30 V	↕	< 3 A	CC	Single ended SEPIC	FP5139	Adjustable divider	25 mΩ	LM358	Adjustable reference
DC-DC #2	3 – 40 V	1.5 – 35 V	↓	< 3 A		Buck	LM2596	Adjustable divider	N/A		
DC-DC #3	5.5 – 30 V	0.5 – 30 V	↕	< 3 A	CC	Single ended SEPIC	FP5139	Adjustable divider	25 mΩ	LM358	Adjustable reference
DC-DC #4	5.5 – 30 V	1.25 – 30 V	↕	< 5 A		4-Switch Buck-boost	LTC1625	Adjustable divider	7 mΩ	LM321	Adjustable reference
DC-DC #5	8 – 36 V	1.25 – 32 V	↓	< 5 A	CC	Buck	XL4015E1	Adjustable divider	50 mΩ	LM358	Adjustable reference
DC-DC #6	10 – 40 V	1.2 – 36 V	↓	< 40 A	CC	2-Switch Buck	LM5116	Adjustable divider	4 mΩ	LM321	Adjustable reference

TABLE 1: Overview of the 6 different DC-DC converters we tested. ↑ indicates that the output voltage must be higher than input, ↓ means lower, and ↕ either. For CC capable devices, the method of current sensing, and current sense amplifier are provided.

ID	F [MHz]	Power [dBm]	Result	Independent of	
				Voltage	Current
#1	740	19	↓ 0.5%	✓	✓
	1080	19	↑ 1.4%	✓	✓
#2	1250	19	↑ ≈ 0.1%	✗	✗
#3	500	19	↓ 0.9%	✓	✓
	1200	19	↑ 0.8%	✓	✓
#4	None	19	N/A	N/A	N/A
#5	760	19	↑ ≈ 2%	✓	✗
#6	850	19	↑ 0.1%	✓	✓

TABLE 2: Results for the DC-DC converters, showing the direction and magnitude of peaks for each device.

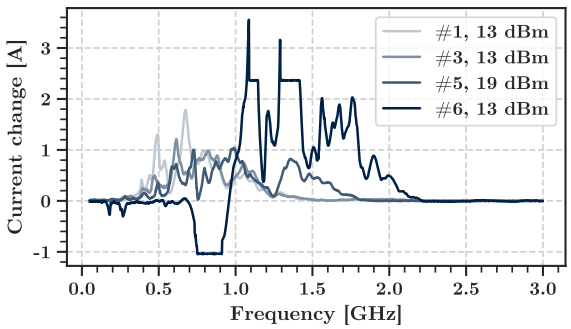


Figure 4: Frequency sweep results for the DC-DC converters set to 1 A CC mode, with a 7 V CV load applied. All devices are highly vulnerable to the attack, requiring us to decrease the attacker power to record meaningful curves.

was placed next to the converter, in close proximity to the regulator IC, and a frequency sweep was carried out with 19 dBm (80 mW) power, in the 50 MHz to 3 GHz range. For each converter, multiple output voltages and loads were tested, while the input voltage and geometry are kept constant. These experiments thus examined the frequency response as a function of the set output voltage, and eliminate variety due to any other parameters.

6.2.2. Results. Figure 3 shows the fractional change in output voltage for device #1 at various set outputs and loads. The plot confirms the expected behavior that fractional change is independent of the set output voltage and applied load, validating the theoretical expectation derived in Equation 3. We summarize further results in Table 2, and show the relevant plots in Appendix A.

Our results demonstrate that many typical DC-DC converters are vulnerable to IEMI attacks, with all vulnerable devices showing a stable impact, and constant resonant frequency regardless of output settings. For multiple devices we also show that the theoretical expectation holds, giving a constant fractional change regardless of setting or load.

The order of magnitude of the attack impact was around 1 %, with 19 dBm (80 mW) of power. We would like to emphasize that these results are only to investigate the existence of the effect, via precise measurements. Based on our conclusions here, we present high-power and high-impact attacks against a variety of devices in Section 7.1.

6.3. AC-DC Converters

Most devices receive their power from AC mains, through AC-DC converters. While the basics of the switched more architecture are shared, many details differ from DC-DC converters, for example due to their full galvanic isolation, and optical feedback system. To examine the security of these devices we tested three power bricks sold with commercial devices, designed to output 6, 12 and 19 V.

6.3.1. Method. We used the same test setup as Section 6.2. The devices were not connected to a load during these experiments, and no modifications were made to the housing of the converter, in order to ensure a realistic attack.

6.3.2. Results. For all three devices, our attack was able to lower the output voltage of the converter by up to 0.1 V at 19 dBm (80 mW). The frequency response curves are shown in Figure 17 in the Appendix. We investigate how using more power can allow this to easily be scaled in Section 7.1.

6.4. Constant Current Supply

Out of the 6 tested DC-DC converters in Table 1, 4 featured a stable constant current (CC) output capability. This means that the device will not exceed the current limit on its output, and is an essential part of the CC-CV battery charging scheme. As explained in 5.3, it is expected that the current sensor is significantly more sensitive than the voltage sensor, and we thus expect the impact of the attack to be higher in many cases.

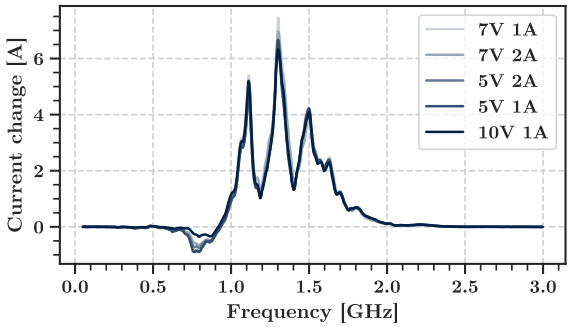


Figure 5: Frequency response of DC-DC #6 in constant current mode at various applied CV loads and current limits.

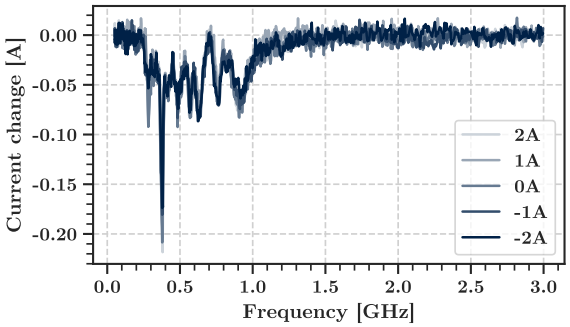


Figure 6: Frequency sweep results for the TLI4971 current sensor at various real currents.

6.4.1. Method. The devices were set to operate at 1 A constant current mode, and a CV load of 7 V was applied. The stable operating point of such a system is that the current flowing into the load is the current limit set on the supply, and the voltage is the CV value set on the load. The use of a CV load is representative of batteries and LEDs, two common systems which are driven by a constant current, since the voltage drop across them changes very little as a function of current.

6.4.2. Results. Figure 4 show the results, all 4 devices clearly exhibited an impact. For three devices (#1, #3, #6), the attack power had to be reduced to measure a useful frequency response curve, since the response was so powerful that the increased current risked damage to the converter, or overloaded the connected test equipment. The strongest response was seen for device #6, which can be explained by it having the smallest shunt resistor. This is advantageous when the device is rated for a high maximum current, to decrease wasted power, however greatly increases the capability of an attacker. The experiments showed a much larger change in current compared to the change in voltage experienced by the same devices during a CV attack, easily achieving multiples of the set current, and reaching the limits of the devices. Due to the importance of CC supplies in battery and LED systems, this attack demonstrates a significant vulnerability, which we investigate further in the scaling and real world section.

We also examined how the attack works at various loads. Since the devices used an adjustable reference scheme for current control, we expect the impact to be governed by Equation 2. We tested device #6, since it had the lowest ripple, and thus most stable operation. The results in Figure 5 clearly show that the absolute change in current is independent of the set CC limit or the applied CV load, in accordance with the theory.

6.5. Automotive Current Sensors

The previously examined CC drivers all relied on a shunt-based current sensor, with a separate discrete amplifier. In many industrial applications, small, tightly integrated, galvanically isolated or digital sensors will be used. We thus tested four different current sensors from reputable vendors, marketed for applications such as EV Supply Equipment, photovoltaic inverters, or other forms of power infrastructure. The selected devices include magnetic and shunt-based technologies as well as analog and digital outputs. Their key properties are summarized in Table 3.

6.5.1. Method. Specific constant currents are ran through the sensor, while an antenna is placed near it. Unlike previous attacks, we are not targeting the power supply itself, but instead only a standalone sensor. Thus, while previously we used un-attacked lab equipment to measure real changes in the output of a power supply under attack, in this experiment we measure the impact of the attack on a sensor, while the real current is supplied by un-attacked lab equipment, and does not change.

6.5.2. Results. Table 3 summarizes our findings, and we show the curves in Figure 6 and Appendix C. We saw success on 3 out of 4 targets, with a variety of behaviors. Notably, in previous experiments, an increase in the output voltage or current was the higher impact result, since this increased voltage can cause damage to the downstream devices. This is not the case for sensor attacks, where lowering the measurement is the significant result. This is because in a feedback loop, the lowered measurement causes the system to increase the current, leading to the more damaging attack outcome. By demonstrating a successful attack against automotive grade sensors, we demonstrate that much like low cost devices, these high quality sensors are also vulnerable to attack, and thus devices relying on them will also be vulnerable.

6.6. Battery Chargers

Battery chargers using the CC-CV scheme are just power converters with current and voltage limits. They often accommodate additional features, such as temperature detection, and digitally programmable operation. We chose two different chargers sold to recharge lithium batteries, the SkyRC e4 and C240 Duo. While the SkyRC e4 charger

Part number	Range	Method	Output	Sensitivity	F [MHz]	Power [dBm]	Result	Independent of Current
TLI4971-A025T5-U	$\pm 25\,\mathrm{A}$	Hall effect	Analog	$20.83\,\mathrm{mA/mV}$	380	19	$\downarrow 0.2\,\mathrm{A}$	✓
TMCS1100A4	$\pm 5.75\,\mathrm{A}$	Hall effect	Analog	$2.5\,\mathrm{mA/mV}$	380	19	$\downarrow \approx 50\,\mathrm{mA}$	✓
INA253A3	$\pm 6\,\mathrm{A}$	Shunt	Analog	$2.5\,\mathrm{mA/mV}$	None	N/A	N/A	N/A
INA260	$\pm 15\,\mathrm{A}$	Shunt, ADC	Digital	$1.25\,\mathrm{mA/LSB}$	340	19	$\uparrow 5\,\mathrm{mA}$	✓
					800	19	$\downarrow \approx 5\,\mathrm{mA}$	✗

TABLE 3: Summary of the automotive grade current sensors that we tested and their results.

only allowed the charging of two or more cells in series with 1, 2 or 3 A, the C240 was able to charge one or more cells with up to 10 A in 0.1 A steps. In both cases, multiple charger settings were tested, to determine how they effect the results.

6.6.1. Method - CC. We seek to attack both the current and voltage sensors of the devices. To attack the current sensors, we set various current limits on our charger and set our battery simulator to 3.5 V per cell. On the SkyRC we simulate a battery with 2 cells in series, while the C240 Duo we test both 1 and 2 cells. We perform a frequency sweep, and measure the current on the DC load.

6.6.2. Results - CC. We plot the response in Figures 19, 20 in the Appendix. On both chargers, we find frequencies where the current exceeds the current limit sent on the charger, and in all cases we find that the magnitude of the attack is independent of the set voltage or current of the charger. On the SkyRC e4, we observe a difference of 1 A, while on the C240 Duo we observe 0.1 A, both at 19 dBm of power.

6.6.3. Method - CV. To measure the impact on the CV phase, we connect a resistor in series with the CV load simulating our battery. Due to the voltage drop across the resistor, the charger becomes voltage limited. We now perform a frequency sweep, and observe the voltage at the charger.

6.6.4. Results - CV. The results from both chargers are shown in Figures 21 in the Appendix. We thus conclude that only the C240 Duo shows any impact above noise. In this case, we observe a difference of 0.06 V at 19 dBm, which means we expect the attack to scale to 1.2 V at 2 W, which we test later.

6.7. Multiple Frequencies

In previous experiments, we were only able to increase either the current or voltage limit at different attack frequencies. To achieve a more significant effect, we developed a method to attack both sensors simultaneously. Our hypothesis was that transmitting an attack signal composed of two signals at the respective frequencies of the voltage and current sensors would affect both sensors independently. To create this multi-frequency signal, we took two signal sources and combined them using the Mini Circuits ZN4PD1-63HP-S+ passive power splitter/combiner. As in previous experiments, the combined signal can be amplified and transmitted via an antenna. For these experiments, we used two USRP N210s as our signal sources, but we do not use any modulation feature. Hence, any cheap device that can produce a pure sine wave could have been used.

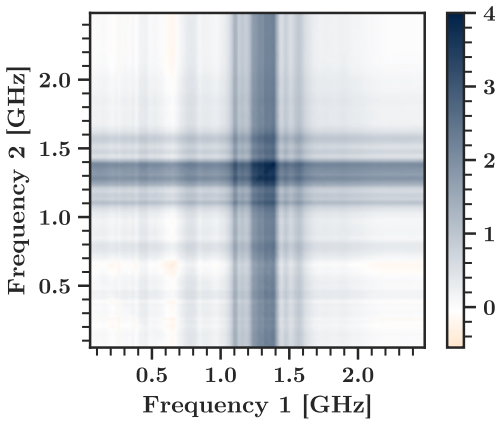


Figure 7: Frequency sweep of DC-DC #6 in CC mode with two different frequencies being transmitted simultaneously. The lack of any diagonal features shows that the two signals affect the sensor independently, there is no inter modulation.

6.7.1. Independence Study. We analyzed whether the attack signals can be treated completely independently, i.e., whether adding the two attack signals is the same as adding their respective effects. To do this, we utilized DC-DC #6 in CC mode, as it produced a very clean measurable impact even at low power. We varied the frequencies of both sources and measured every combination within the spectrum where the devices were susceptible to electromagnetic interference. Figure 7 shows the results of this experiment. The plot clearly shows that the attack is successful when either of the signal sources hits a resonant frequency. Furthermore, there are no visible diagonal features, which indicates that there is no mixing or non-linear interaction occurring between the two sources. With this result we can conclude that adding up attack signals will allow their effects to be added up.

6.7.2. Multi-Sensor Experiment. To evaluate the effectiveness of the attack against two sensors, we targeted the C240 Duo battery charger, which has susceptible current and voltage sensors. We added an amplifier to the combined signal, and transmitted the voltage and current sensor signals

Figure 8: The portable EV charger used in our experiments, as well as the placement of the attacking antenna. The attack is highly effective at 2 W power, despite the metal casing of the charger.

at 2 W each. We set up our battery simulator as a 5.1 V CV load and set the charger to charge a single cell battery at maximum 4.2 V, 1 A. Despite the simulated battery already exceeding the voltage limit, the charger started without issues and began charging. We measured 5.1 V, 1.4 A on the un-attacked DC load, while the charger displayed 4.18 V, 1 A. This confirms our hypothesis that a simultaneous attack on the voltage and current sensors is possible, resulting in the charger simultaneously exceeding the voltage and current limits.

6.8. Real-world EV Charger

To demonstrate our attack on a highly impactful target, we evaluated a DC Electric Vehicle (EV) charger, shown in Figure 8. To avoid causing damage to public infrastructure, we used a Setec SET450-20B 10kW CCS EV DC charger in a laboratory environment. In addition, due to the obvious safety risk, we replaced the EV with a dummy load that can safely accept the potentially erratic voltages from the charger, and used the pyPlc project [32] to perform the necessary communication with the charger, as well as to log data from the charger. We used an RF power of 2 W for our attack on an unmodified charger.

We discovered that the charger is vulnerable to both a current and voltage sensor attack. At 1310 MHz the charger increases the current from 2.2 to 2.25 A. However, at 620 MHz the charger reports a voltage of 115 V, while outputting 165 V. We thus demonstrated a significant difference of 50 V due to our attack.

7. Practicability Evaluation

In the previous section, we showed that a variety of devices produce a measurable impact at a short range and for small transmission power. In this section, we evaluate how the attack scales to higher powers as well as larger distances, and we investigate the repeatability of the attack.

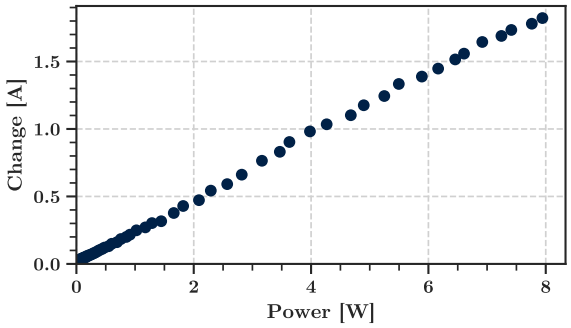


Figure 9: The impact of attacker power against the C240 Duo charger, confirming our theory of the linear trend. We also see that the attack impact reaches significant values well within a realistic power budget.

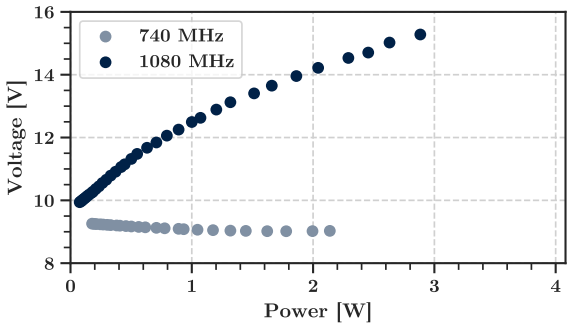


Figure 10: DC-DC #1, 10 V output, investigating a frequency corresponding to both a positive and negative change. The end of the traces corresponds to a full shutdown of the output.

7.1. Attacker Power Budget

We investigated how the attacker can extrapolate their low-power measurements to determine the power level required for a given impact. According to expectations from theory [20], the impact of the attack should scale linearly with the used RF power.

7.1.1. Method. We investigated multiple of the previous devices at their resonant frequency: the 6 V AC-DC power converter at 820 MHz, the C240 Duo in CC mode at 1.65 GHz, the SkyRC charger at 1.28 GHz and DC-DC #1 at both 740 MHz and 1080 MHz. For these experiments the signal was supplied by a USRP N210 connected to the Mini-Circuits ZHL-10W-202S+ 10 W power amplifier. Instead of sweeping the frequency, the frequency was fixed at a known resonant value for each device, and the output power of the RF source was swept. We connected an RF coupler between the amplifier and antenna, allowing us to measure the power level of the output signal going to the antenna during the experiments. This allowed us to make accurate measurements, regardless of the gain of our power amplifier.

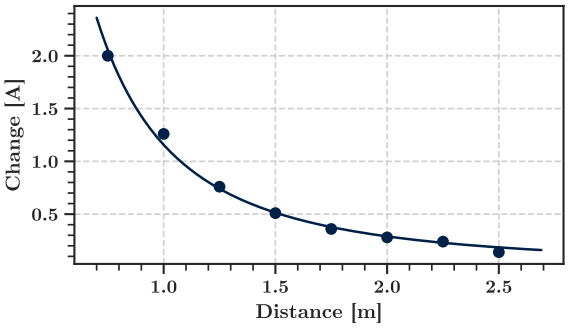


Figure 11: Impact of attack distance against the SkyRC e4 charger, confirming our theory that with increasing distance the effect diminished according to the inverse square law. Line shown is the best fit inverse square law to the points.

7.1.2. Results. We show two plots in Figure 9 and 10, and further plots for the tested devices in Appendix E. The plots validates our theoretical prediction, that the attack impact is linear as a function of RF output power, assuming everything else is kept constant. For some devices, we see that at higher power, the impact start deviation from the line, before the device shuts off entirely. In all cases, we show that with sufficient power, the attack can either be scaled to a significant change (at least 1 V or A), or achieve a full shutdown of the device.

7.2. Ranged Experiments

Theory predicts that the RF power density at the receiver is the only relevant metric to determine the success of the attack. This can be achieved by a nearby low powered attacker, or a distant high power attacker.

7.2.1. Method. We used the SkyRC e4 charger, as it demonstrated a larger attack response, thus making it easier to accurately measure the impact of distance. The charger was connected to the battery simulator, charging a simulated battery consisting of two cells totaling 7 V, with 1 A. We used the Mini-Circuits ZHL-10W-202S+ amplifier, outputting 37 dBm (5 W), connected to an RFSpace TSA600 directional antenna. We tested the attack at the known resonant frequency of 1290 MHz.

7.2.2. Results. We tested our attack from various distances, and plot our results in Figure 11, along with a best fit inverse square law. Our results show reasonable agreement, proving that our attack is coupled via far field EM radiation. We demonstrate a current increase of 1 A from 1 m. We conclude that even with our limited amplification, the attack can thus have a significant impact up to two meters away, which demonstrates a significant real-world threat.

7.3. Compact Attack Setup

We assembled a compact attack setup, shown in Figure 12, to show that the required equipment is portable and

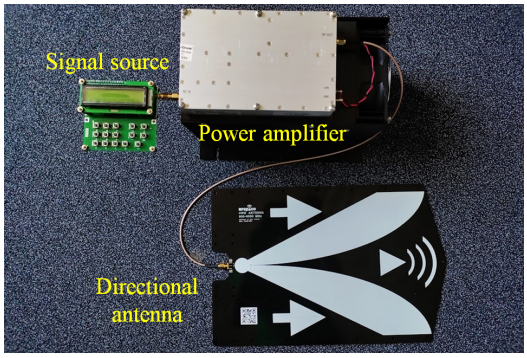


Figure 12: Portable attack setup showing the necessary components.

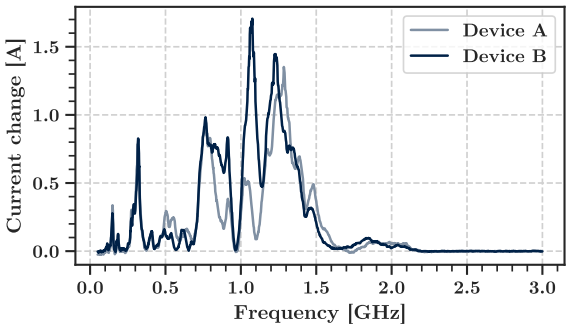


Figure 13: Frequency sweeps for two identical SkyRC chargers, showing largely identical behavior at most frequencies.

within the budget of motivated individuals. Since our attack only requires one or more unmodulated signals, a cheaply available tunable PLL source is sufficient, for example those based on the ADF4351 chip. While our setup used a wideband COTS power amplifier, the amateur radio community has demonstrated that a skilled attacker can construct power amplifiers cheaply, such as a 1.3 GHz, 600 W amplifier for US$710 [33]. For transmission, a cheap directional wideband PCB antenna can be used for an excellent balance of size and gain.

7.4. Repeatability

Like previous EMI work, we assume that an attacker can determine resonant frequencies, and prepare the attack, before exploiting it on other identical targets in the wild. However, due to manufacturing imperfections between devices it is unknown if this is true. We take two supposedly identical SkyRC chargers, and test them in the same environment. In addition, while swapping the devices between the experiments, we inevitably disturb the geometry of the setup. Regardless, we find that their resonance curves largely overlap, so an attacker should be able to reuse their initial measurements on new targets. We show this plot in Figure 13.

8. Battery Charging Attacks

In addition to lab-based evaluation of battery chargers, we seek to understand how real Lithium batteries react to the attack. There may be important differences between the battery simulator used in previous experiments, and a real battery. We also want to assess whether the increase in current and voltage caused by the attack is sufficient to permanently damage a battery. We thus tested 4 different "18650" lithium cells and a small pouch lithium battery, to evaluate their behavior during a charging attack.

8.1. Ethical and Safety Considerations

As described in Section 4.2, overcharging a battery can lead to safety-critical situations, such as fires and explosions. Safety was thus taken seriously. We placed the battery in a metal chamber, connected to the charger via a long cable. We separated both ourselves and the rest of the experimental hardware from the battery in case of an emergency. The battery was enclosed such that any chemical leakage could be safely contained and disposed of.

Examining the true state of the internal battery chemistry is difficult and internal protection mechanisms might have been destroyed during the experiments. Because chemical reactions can occur even after charging has stopped, we kept the batteries safely isolated for a days after the experiment.

8.2. Experiment Setup

The RF signal was provided by a USRP N210 and amplified by a Mini-Circuits ZHL-10W-202S+, which is capable of delivering up to $40\,\mathrm{dBm}$ ($10\,\mathrm{W}$) of power, but in our experiments it was limited to $33\,\mathrm{dBm}$ ($2\,\mathrm{W}$). The C240 Duo is a realistic target due to its granular voltage and current settings, as well as addition safety features such as optional temperature monitoring. The transmitting antenna was placed below the charger, and two $2.5\,\mathrm{m}$ long, $5\,\mathrm{mm}^2$ cross-section wires from the charger connected it to the battery. We did not connect any additional telemetry to the system, and could only rely on prior knowledge of the device, as well as the current and voltage visible on the chargers screen.

We tested 4 18650 cells, the TerraE INR_18650_30_E, Panasonic NCR18650BD, LG Chem INR 18650 M29, and an unbranded one sold in a rechargeable flashlight. In addition, we tested the Renata ICP402035 pouch battery.

8.3. Overcharging Experiment

When a Li-ion battery is overcharged, a non-reversible chemical reaction begins to produce CO2 in the cell [34]. The pressure build-up triggers the Circuit Interrupt Device (CID), which permanently disconnects the cell and prevents further charging [35]. A malfunctioning CID or excessive heating due to an overcurrent can also cause the cell to explode and possibly catch fire.

We set each battery to the manufacturer's recommended charge current (for the unbranded flashlight battery, we used $1\,\mathrm{A}$ based on measurements of the device) and started the charge process. When the batteries were almost fully charged (near the end of the CV phase), we activated the current and voltage attacks at the known resonant frequencies of the charger. We saw the voltage displayed on the charger drop by about $1.2\,\mathrm{V}$, and the charger re-entered the CC phase. While not visible on the charger, previous experience suggests that the current attack added an additional $0.5\,\mathrm{A}$ to the charge current.

All 4 18650 cells continued to charge, and the voltage measured by the charger increased. About 20 – $40\,\mathrm{minutes}$ after we initiated our attack on the nearly full batteries, we estimated that the cell voltage reached about 5 – $5.5\,\mathrm{V}$, and all 18650 batteries made a loud popping noise. For the three branded batteries, the charger immediately stopped and the battery showed no electrical characteristics, so we concluded that the CID was triggered, which permanently but safely disabled the battery. The unbranded battery, however, produced a much louder noise, emitted a liquid, and continued to charge while emitting smoke. Charging finally stopped when the charger detected that the battery voltage was high enough despite the attack. The pouch battery also reached a cell voltage of about $5.5\,\mathrm{V}$ and bulged slightly. There was no catastrophic damage, and it went through a normal discharge and recharge cycle. After the batteries were safe to approach, we found them all to be hot and waited for them to cool before moving them to safe storage.

9. Countermeasures

We enumerate a variety of countermeasures that increase the barrier for a successful attack significantly and discuss their practicality.

9.1. Voltage Protection System

The power input or battery module in a device can be equipped with a protection circuit. This circuit can be designed to monitor voltage and current and disconnect the device from the outside world if a problem is detected. In addition to protecting against attacks, this protection system also protects against legitimate power supply failures as well as user error, such as connecting the wrong power supply. Such systems are often partially present in real-world devices, particularly in brown-out detection, since a drop in input voltage occurs naturally when the device is disconnected from the power supply. Battery modules in mobile phones have an advanced circuit board that is responsible for monitoring the SoC and battery health, as well as protection elements. EV battery packs contain an advanced BMS that monitors all cell voltages and pack current, and high-current contact to physically disconnect the battery in an emergency. These systems are designed for emergency situations, so they may not fully mitigate damage and may be damaged with repeated use. In addition, these protection systems themselves rely on accurate measurements of voltage and

current, making them vulnerable to identical sensor injection attacks. As we have demonstrated, it is possible to attack multiple sensors in parallel, allowing an attacker to target both the power converter and the protection systems.

9.2. Shielding

A common countermeasure against EMI is to shield the circuit with a conductive metal layer. This attenuates RF signals and increases the attacker's required power budget. The effectiveness depends on the amount of shielding: a light mesh can attenuate some signals, but a thick copper shell offers superior performance. However, the end product must often be inexpensive, small, and lightweight, which limits the amount of shielding. In addition, input and output wires require holes in the shielding, allowing attack signals to couple to these wires and enter the device as conducted interference. Our experiments showed that despite the use of a metal case, our EV charger remained vulnerable to attack.

9.3. Filters

Given the relatively low frequency at which switching and feedback occur ($100\,\mathrm{kHz}$), low-pass filters can be used to block the high-frequency RF signals used by the attacker just before the input of the amplifier/regulator ICs. Such a filter is already built into many existing devices via small capacitors on the feedback line. Its main purpose is not to protect against RF attacks, but to reduce noise at the input and to improve the stability of the feedback loop. As our results show, the existing capacitors are not sufficient to prevent the attack. A major limitation is that low-pass filters become ineffective well above their rated cutoff, due to parasitic properties of the components used [36]. A filter that is effective over a wide frequency range requires expensive and high-quality RF components. Furthermore, the small section of wire connecting the filter to the input of the sensitive analog component, or the internals of the component itself, will still be vulnerable.

9.4. Attack Detection

As laid out, fully preventing IEMI attacks is difficult. Therefore, academic literature has proposed various approaches to instead detect attacks. The authors of [37], [38] have investigated ways in which systems can detect if they are under IEMI attack. This can, for example, be accomplished by transmitting and measuring two identical signals and looking at the difference [38], or by randomly connecting/disconnecting the legitimate input and checking if the disconnected measurement produces an expected "null" value [37]. Since the vulnerable logic components of a feedback system are often inside a tightly integrated chip, these countermeasures require the engineering of new semiconductor devices. In more software-based systems, where the feedback control is performed by a microcontroller, the designer should be able to integrate such schemes with few added external components.

9.5. Thermal Fuses

In many cases, the main damage is caused by an increased voltage leading to an increased current. This increased current is then dissipated as heat in a component, causing permanent structural damage. By fitting devices with an appropriate fuse, the damage caused by overcurrent can be mitigated. In contrast to sensor-based current monitoring systems, a simple heat-based fuse is not vulnerable to our attacks. Similarly, Polymeric Positive Temperature Coefficient (PPTC) [39] devices can be used as re-settable thermal fuses. The batteries tested included various forms of protection systems, such as the CIDs, and they also claimed to include PPTCs. While these may have been effective at preventing a violent explosion and combustion of the battery, they did not prevent our attack from permanently disabling them, allowing for an effective denial of service.

10. Conclusion

Our paper studied for the first time the real-world effects of IEMI attacks on DC power converters. Our findings show that the output sensing, active feedback-based nature of switched-mode power converters allows IEMI attacks to be successfully executed on a wide range of devices. We demonstrated a measurable attack against a variety of devices with only $19\,\mathrm{dBm}$ ($80\,\mathrm{mW}$), well within the budget of a motivated hobbyist, and show that we can achieve a significant impact from up to $2\,\mathrm{m}$ with $38.3\,\mathrm{dBm}$ ($6.7\,\mathrm{W}$), opening up the possibility for ranged attacks within a reasonable budget. We innovated on the state of the art IEMI attacks, by introducing a low-cost multi-frequency attack, capable of targeting multiple sensors simultaneously.

We evaluated our attack in realistic settings, causing permanent damage to multiple Li-ion batteries with about $33\,\mathrm{dBm}$ ($2\,\mathrm{W}$) of RF power. In addition, we successfully injected a $50\,\mathrm{V}$ difference between the voltage reported by an EV charger and the actual measured voltage. We conclude that IEMI attacks against power converters represent a significant risk with potentially dangerous real-world consequences, even within the budget of motivated hobbyists. Better funded adversaries using high power amplifiers and directional antennas can easily scale the attack to greater distances. We discuss a variety of countermeasures, highlighting prior academic work in attack detection and sensor authentication systems, and physical-layer defenses.

Acknowledgments

We would like to thank Orlando Summermatter and the testing group of armasuisse Science + Technology for their support during the experiments. Marcell was funded by the Engineering and Physical Sciences Research Council (EPSRC) and Sebastian was supported by the Royal Academy of Engineering and the Office of the Chief Science Adviser for National Security under the UK Intelligence Community Postdoctoral Research Fellowships programme.

References

[1] Y. Cui, Z. Yu, D. Shi, F. Yun, Y. Hu, X. Zhang, W. Hua, S. Gao, S. Fang, and Y. Fang, "Safety boundary analysis for lithium-ion batteries via overcharge-to-thermal runaway," in *2022 IEEE 5th International Electrical and Energy Conference (CIEEC)*, 2022, pp. 433–438.

[2] Nikana. Rules for transporting cars by ferry in Greece. [Online]. Available: https://nikana.gr/en/blog/6255/rules-for-transporting-cars-by-ferry-in-greece

[3] IATA. Passengers travelling with lithium batteries. [Online]. Available: https://www.iata.org/contentassets/6fea26dd84d24b26a7a1fd5788561d6e/passenger-lithium-battery.pdf

[4] TfL. (2021, 12) TfL announces safety ban of e-scooters on transport network. [Online]. Available: https://tfl.gov.uk/info-for/media/press-releases/2021/december/tfl-announces-safety-ban-of-e-scooters-on-transport-network

[5] "Samsung galaxy note 7 banned by more airlines over fire risk," Oct 2016. [Online]. Available: https://www.bbc.com/news/business-37674170

[6] C. Yan, H. Shin, C. Bolton, W. Xu, Y. Kim, and K. Fu, "SoK: A minimalist approach to formalizing analog sensor security," in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 233–248.

[7] I. Giechaskiel and K. Rasmussen, "Taxonomy and challenges of out-of-band signal injection attacks and defenses," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 645–670, 2020.

[8] G. Y. Dayanikli, R. R. Hatch, R. M. Gerdes, H. Wang, and R. Zane, "Electromagnetic sensor and actuator attacks on power converters for electric vehicles," in *2020 IEEE Security and Privacy Workshops (SPW)*, 2020, pp. 98–103.

[9] C. Attaianese, A. D. Pizzo, G. Brando, L. P. D. Noia, and A. Dannier, "Effects of electromagnetic inductive attack on the performance of a boost DC-DC converter," in *2022 IEEE International Conference on Metrology for Extended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE)*, 2022, pp. 254–259.

[10] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in *2017 IEEE European symposium on security and privacy (EuroS&P)*. IEEE, 2017, pp. 3–18.

[11] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking drones with intentional sound noise on gyroscopic sensors," in *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C.: USENIX Association, Aug. 2015, pp. 881–896. [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/son

[12] S. Köhler, G. Lovisotto, S. Birnbach, R. Baker, and I. Martinovic, "They see me rollin': Inherent vulnerability of the rolling shutter in cmos image sensors," in *Annual Computer Security Applications Conference*, 2021, pp. 399–413.

[13] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands: laser-based audio injection attacks on voice-controllable systems," in *Proceedings of the 29th USENIX Conference on Security Symposium*, 2020, pp. 2631–2648.

[14] Y. Jiang, X. Ji, K. Wang, C. Yan, R. Mitev, A.-R. Sadeghi, and W. Xu, "WIGHT: Wired ghost touch attack on capacitive touchscreens," in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 984–1001.

[15] Z. Xu, R. Hua, J. Juang, S. Xia, J. Fan, and C. Hwang, "Inaudible attack on smart speakers with intentional electromagnetic interference," *IEEE Transactions on Microwave Theory and Techniques*, vol. 69, no. 5, pp. 2642–2650, 2021.

[16] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating EMI signal injection attacks against analog sensors," in *2013 IEEE Symposium on Security and Privacy*, 2013, pp. 145–159.

[17] S. Köhler, R. Baker, and I. Martinovic, "Signal injection attacks against CCD image sensors," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, ser. ASIA CCS '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 294–308. [Online]. Available: https://doi.org/10.1145/3488932.3497771

[18] Q. Jiang, X. Ji, C. Yan, Z. Xie, H. Lou, and W. Xu, "GlitchHiker: Uncovering vulnerabilities of image signal transmission with IEMI," in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 7249–7266. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/jiang-qinhong

[19] G. Y. Dayanıklı, A. Z. Mohammed, R. Gerdes, and M. Mina, "Wireless manipulation of serial communication," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, ser. ASIA CCS '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 222–236. [Online]. Available: https://doi.org/10.1145/3488932.3517427

[20] Y. Tu, S. Rampazzi, B. Hao, A. Rodriguez, K. Fu, and X. Hei, "Trick or heat? manipulating critical temperature-based control systems using rectification attacks," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 2301–2315. [Online]. Available: https://doi.org/10.1145/3319535.3354195

[21] A. Z. Mohammed, A. Singh, G. Y. Dayanıklı, R. Gerdes, M. Mina, and M. Li, "Towards wireless spiking of smart locks," in *2022 IEEE Security and Privacy Workshops (SPW)*, 2022, pp. 251–257.

[22] M. Lelie, T. Braun, M. Knips, H. Nordmann, F. Ringbeck, H. Zappen, and D. U. Sauer, "Battery management system hardware concepts: An overview," *Applied Sciences*, vol. 8, no. 4, 2018. [Online]. Available: https://www.mdpi.com/2076-3417/8/4/534

[23] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4639–4657, 2021.

[24] S. Sripad, S. Kulandaivel, V. Pande, V. Sekar, and V. Viswanathan, "Vulnerabilities of electric vehicle battery packs to cyberattacks," 2017. [Online]. Available: https://arxiv.org/abs/1711.04822

[25] A. Barua and M. A. A. Faruque, "Hall spoofing: A non-invasive DoS attack on grid-tied solar inverter," in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, pp. 1273–1290. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/barua

[26] J. Jang, M. Cho, J. Kim, D. Kim, and Y. Kim, "Paralyzing drones via EMI signal injection on sensory communication channels," in *Network and Distributed System Security (NDSS) Symposium 2023*, 2023.

[27] P. Horowitz and W. Hill, *The art of electronics; 3rd ed.* Cambridge: Cambridge University Press, 2015.

[28] Maxim Integrated, *Why Drive White LEDs with Constant Current?*, Aug 2004, application Note 3256. [Online]. Available: https://www.analog.com/media/en/technical-documentation/tech-articles/why-drive-white-leds-with-constant-current.pdf

[29] R. R. Thakkar, "Electrical equivalent circuit models of lithium-ion battery," in *Management and Applications of Energy Storage Devices*, K. E. Okedu, Ed. Rijeka: IntechOpen, 2021, ch. 1. [Online]. Available: https://doi.org/10.5772/intechopen.99851

[30] D. Hamo, "Challenges in Li-ion charging," Aug 2003. [Online]. Available: https://www.electronicproducts.com/challenges-in-li-ion-charging/

[31] I. Giechaskiel, Y. Zhang, and K. B. Rasmussen, "A framework for evaluating security in the presence of signal injection attacks," in *Computer Security – ESORICS 2019*, K. Sako, S. Schneider, and P. Y. A. Ryan, Eds. Cham: Springer International Publishing, 2019, pp. 512–532.

[32] U. Hennig. CCS hacking: Electric car charging experiments with python and PLC network adaptors. [Online]. Available: https://github.com/uhi22/pyPLC

[33] W6PQL. (2023) Parts I can supply. [Online]. Available: https://www.w6pql.com/parts_i_can_provide.htm#23cm

[34] Battery University, *Charging Lithium-ion*, BU-409. [Online]. Available: https://batteryuniversity.com/article/bu-409-charging-lithium-ion

[35] ——, *Making Lithium-ion Safe*, bU-304b. [Online]. Available: https://batteryuniversity.com/article/bu-304b-making-lithium-ion-safe

[36] R. Hurley, "AND8245/D design considerations for ESD/EMI filters: II low pass filters for audio filter applications," 2007.

[37] Y. Zhang and K. Rasmussen, "Detection of electromagnetic interference attacks on sensor systems," in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 203–216.

[38] ——, "Detection of electromagnetic signal injection attacks on actuator systems," in *Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses*, ser. RAID '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 171–184. [Online]. Available: https://doi.org/10.1145/3545948.3545949

[39] Littelfuse Inc, *Use of Low Resistivity Surface Mount PPTC in Li-ion Polymer Battery Packs*, 2012, application Note. [Online]. Available: https://www.littelfuse.com/~/media/electronics_technical/application_notes/resettable_ptcs/littelfuse_use_of_low_resistivity_surface_mount_pptc_application_note.pdf

Artifacts

Our code for collecting data (requires the same instruments as used in the paper), the raw data files, and plotting code can be found at https://github.com/ssloxford/assault_and_battery.

Appendix

In this section we present the frequency response curves and additional plots for the devices that were not included in the main body of the text due to space constraints.

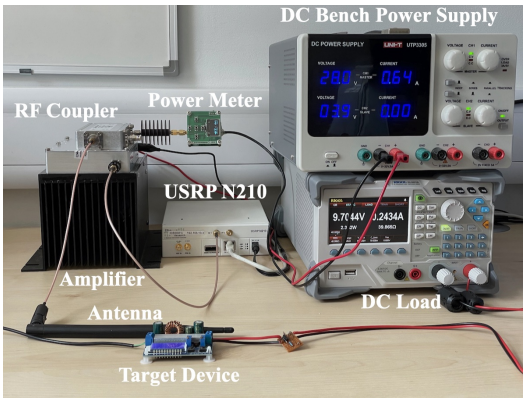


Figure 14: Overview of the equipment that we used for most of our experiments. In this case, the signal was generated by a USRP N210 and amplified by a Mini-Circuits ZHL-10W-202S+ that was connected to the DC bench power supply on the right. The device under test was connected to the DC load.

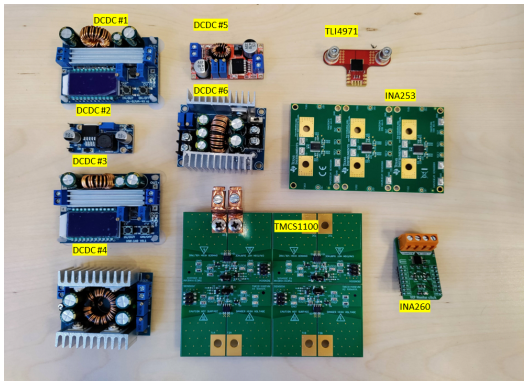
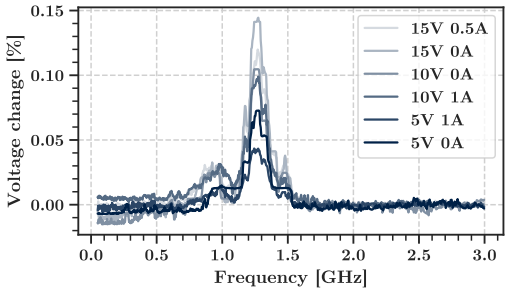
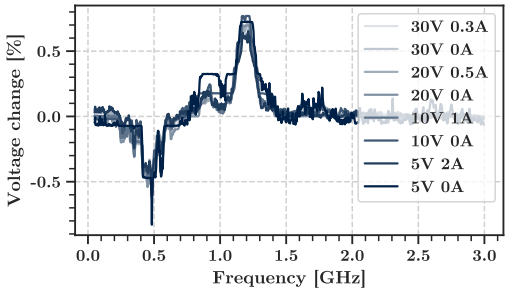


Figure 15: Overview of DC-DC converters and automotive current sensors evaluated in this paper.

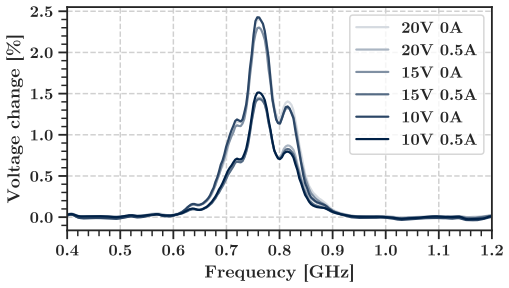
1. DC-DC converters



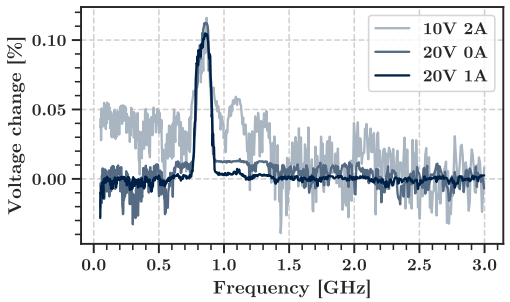
(a) Device DC-DC #2, 20 V input.



(b) Device DC-DC #3, 12 V input.



(c) Device DC-DC #5, 25 V input.



(d) Device DC-DC #6, 25 V input.

Figure 16: Relative change in the measured output voltage on the remaining prototyping boards. Different lines represent different set output voltages and applied loads.

2. AC-DC Converters

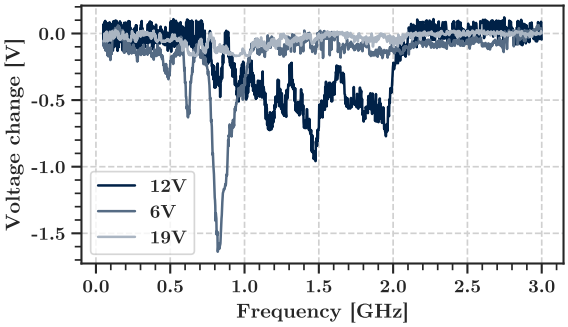
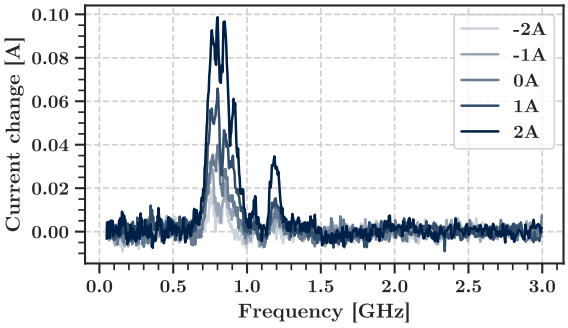
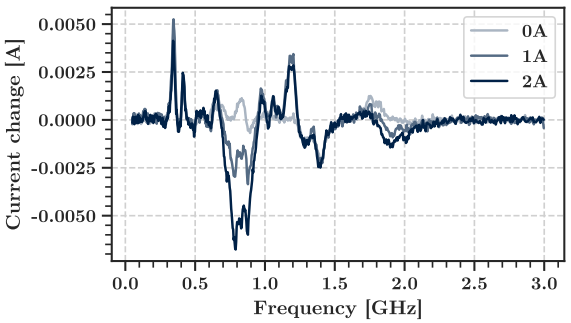


Figure 17: Frequency sweep results for three different AC-DC wall plugs, showing that all devices are susceptible and have a measurable response for 19 dBm attack power.

3. Current sensors



(a) Current sensor TMCS1100.



(b) Current sensor INA260.

Figure 18: Frequency sweep results for the various current sensors with an attack signal of 19 dBm (80 mW), at different actual current values. Some peaks exhibit a constant behavior, while others depend on the current.

4. Chargers

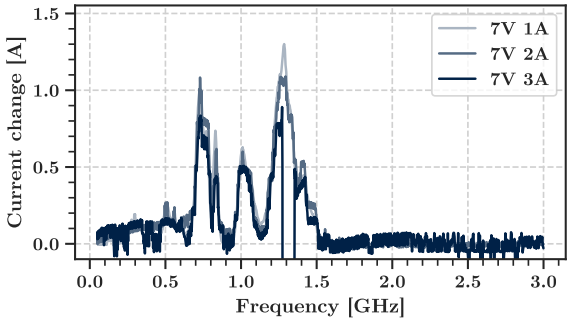


Figure 19: Frequency sweep results for the SkyRC e4 battery charger for three different current settings and an attack signal of 19 dBm. The injection causes a constant offset regardless of the charging current.

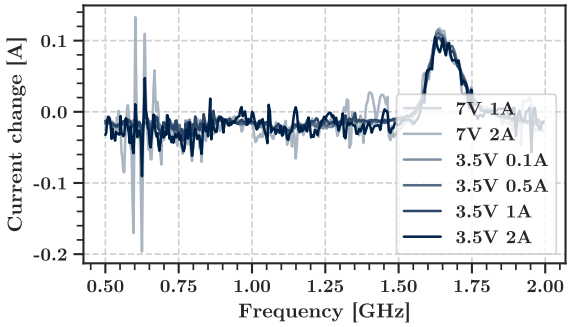


Figure 20: Frequency response of the C240 Duo in CC mode at various loads at 19 dBm

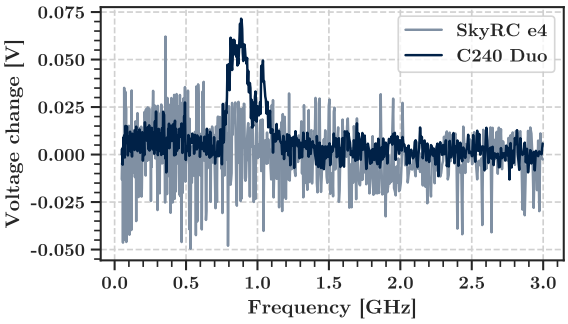


Figure 21: Frequency sweep results for the two chargers in the CV phase for 19 dBm of transmission power. Only the C240 is vulnerable in this frequency range.

5. Power

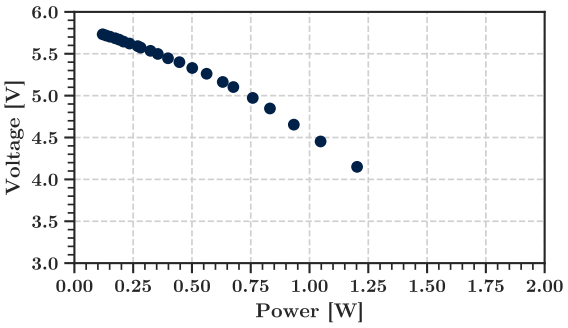


Figure 22: 6 V AC-DC converter, 820 MHz. The end of the trace corresponds to a full shutdown of the output.

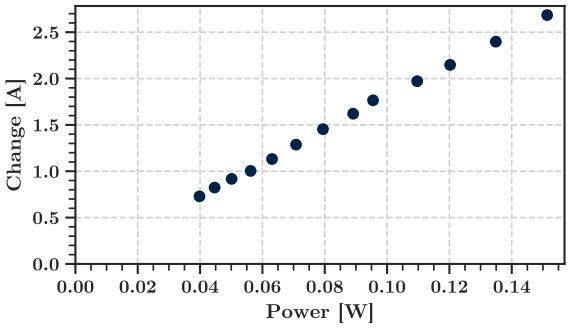


Figure 23: SkyRC charger, 1 A in CC mode, 1280 MHz. We stopped the attack once the charger passed its maximum rated current.