Exploring a Low-Cost Hardware Reverse Engineering Approach: A Use Case Experiment*

André Waltoft-Olsen[1,2,3][0000−0003−3016−7824], Phillip Johnson[2][0009−0002−0700−3063], Lasse Øverlier[1][0000−0002−7640−8446], and Geir Olav Dyrkolbotn[1]

[1] Norwegian Institute of Science and Technology, Gjøvik, Norway
{andrejw,lasse.overlier,geir.dyrkolbotn}@ntnu.no
[2] Colorado State University, Fort Collins, Colorado, USA
{ajwo,phillip.johnson}@colostate.edu
[3] Statnett SF, Oslo, Norway

Abstract. This research delves into Hardware Reverse Engineering, specifically focusing on hardware manipulation. It leverages the Supply Chain attack vector and conducts a practical experiment to manipulate sensor trustworthiness. Results demonstrate that identifying weaknesses and exploiting hardware vulnerabilities can be achieved without costly reverse-engineering platforms. The study further benefits novices venturing into Hardware Reverse Engineering research by advocating a low-cost approach using open-access knowledge.

Keywords: Hardware Reverse Engineering · Low-Cost · Novice-friendly Tools.

1 Introduction

Transitioning to renewable energy necessitates a more intelligent energy system known as the Smart Grid. This system integrates physical infrastructure with digital technology to enhance efficiency, reliability, sustainability, and adaptability, requiring a high degree of automation [8]. Transducers like the ICEBOX Load Sensor play a crucial role in automation by collecting real-world data, such as line sag data, to optimize conductor ampacity and improve energy security.

Supply chain attacks leveraging hardware manipulations are strategically designed to achieve specific goals for the attacker [2]. These attacks generally occur through two methods: Seeding during manufacturing, embedding the attack from

* This work was Supported by The Norwegian Research Council, Statnett SF, and the U.S. National Science Foundation under Grant No. 1822118 and 2226232, the member partners of the NSF IUCRC Center for Cyber Security Analytics and Automation – Statnett, AMI, NewPush, Cyber Risk Research, NIST and ARL – the State of Colorado (grant #SB 18-086) and the authors' institutions. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation, or other organizations and agencies.

the outset, and post-manufacturing interdiction, involving secret alteration and re-packaging of finished devices [5,9]. Hardware manipulations within smart devices like the ICEBOX Load Sensor can grant attackers persistent access and are challenging to detect [4].

1.1 Motivation

Security in grid infrastructures focuses on network, software, and physical aspects, often overlooking hardware security. Hardware threats involving physical device manipulation pose distinct challenges. Addressing these challenges requires Hardware Reverse Engineering expertise, blending software and hardware knowledge with skill in using electronic testing equipment. Unfortunately, the complexities of such expertise often result in inadequate attention to smart device hardware security.

1.2 Research Questions

We focus on Hardware Reverse Engineering (HRE) at the Printed Circuit Board (PCB) level within the use case of the ICEBOX Load Sensor.

1. How can accessible tools, techniques, and educational resources suitable for novices be utilized for HRE, enabling individuals with limited HRE knowledge to analyze and understand the inner workings of smart devices?
2. How can an attack strategy leverage a low-cost HRE approach to identify hardware weaknesses, enabling attacks to manipulate device trustworthiness?

1.3 Contribution

We address the high cost and knowledge barriers associated with HRE. We employ a low-cost HRE approach that utilizes tools, techniques, and educational resources suitable for novices. Our attack centers on manipulating the ICEBOX Load Sensor to undermine its trustworthiness. We also provide a detailed account of our approach, intending to share our insights so others can leverage our work. Furthermore, we conducted a modest assessment to gauge the potential consequences of our attack in real-world scenarios.

1.4 Layout

The rest of the paper is as follows: Section 2 reviews prior work. Section 3 outlines our low-cost infrastructure, reverse engineering of the target ICEBOX Load Sensor, and the execution of our manipulation attack. In Section 4, we analyze our findings and results. Finally, Section 5 concludes with a summary and future work prospects.

2 Background

Efforts are underway to enhance the security of electronic supply chains. Omitola et al. [10] note that Apple employs a strategy of selective partnership with manufacturers to tighten control and oversight over iPhone components. However, despite stringent surveillance, vulnerabilities emerge from interactions with secondary suppliers and during maintenance phases, largely due to outsourced activities, making potential security breaches harder to identify and mitigate.

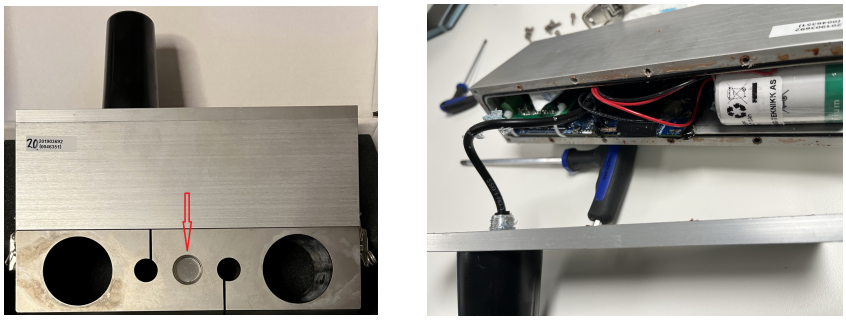
Additional efforts are improving methods and approaches to assess device hardware security. Sharma et al. [12] introduce a systematic approach to assess hardware security for smart IoT devices. They propose a comprehensive framework consisting of two distinct testing levels, namely the device and PCB levels, designed to facilitate a thorough analysis of black-box devices. At the device level, the focus is on evaluating various aspects of the device. This encompasses examining its overall functionality, the resilience of its enclosure against tampering, potential side-channel interactions, and the management of its battery resources. On the other hand, the PCB level delves into the intricacies of tamper protection mechanisms employed for individual components on the device's PCB. It also scrutinizes the functionality and security measures associated with these PCB components. A holistic view of the device emerges by meticulously investigating both levels, enabling researchers to uncover undiscovered vulnerabilities and comprehensively understand its security landscape. It's important to note that the research doesn't provide practical use-case experiments to illustrate their systematic approach to evaluating hardware security. Instead, their framework is intended to be implemented by "IoT manufacturers, hardware security testing labs, and research and educational organizations seeking to enhance their expertise, whether for teaching, training, or capacity-building initiatives." Additionally, it's worth mentioning that some of the methods discussed in the article require specialized knowledge and, in certain instances, expensive equipment. Therefore, cost-effectiveness and low-cost approaches remain challenging for risk owners seeking to improve the hardware security of their critical infrastructure.

Attackers rely on reverse engineering expertise in a black box scenario to manipulate hardware [1, 7, 13]. However, HRE is a multifaceted field that demands a diverse skill set. Carina et al. delve into this complexity and provide case studies on netlist HRE [3, 15]. Specifically, experience and domain knowledge are advantageous for HRE analysis, posing challenges for newcomers. Moreover, there seems to be a lack of educational courses to facilitate entry into HRE for motivated individuals [14].

Our use-case experiment with the ICEBOX Load Sensor involves leveraging a Supply Chain attack, wherein an attacker gains physical access to the device during shipment, installation, maintenance, or as an insider. Given the need for tailored hardware manipulation, HRE is employed to devise a low-cost approach for our attack.

Figure 1 illustrates the ICEBOX Load Sensor comprising two main sections. The lower casing houses the Wheatstone bridge (indicated by the Red Arrow in Figure 1a) and mounting holes for sensor installation. The upper section accom-

modates internal components such as the custom-made Nordic Semiconductor nRF9160 development PCB kit (DK), an additional amplifier PCB card (amp-PCB), and two batteries for power. The antenna is fixed on top. The ICEBOX Load Sensor utilizes a Wheatstone bridge circuit [6] to assess physical loads induced by compression or tension accurately. When tension or compression is applied to the transmission line, it affects the sensor's physical structure. The Wheatstone bridge translates the physical load into a voltage signal. The sensor's internal digital logic converts the analog signal into a digital representation before transmitting it to a remote gateway using the MQTT protocol[4].



(a) Fully assembled (b) Disassembled

Fig. 1: The ICEBOX Load Sensor

3 Approach

To address our research questions, we investigated whether manipulating Wheatstone bridge voltage levels impacts the quality of data transmitted by the ICEBOX Load Sensor. Our approach is depicted in Figure 2.

3.1 Literature Study

Table 1 show the keywords employed in our literature exploration. Our searches concentrated on Hardware Reverse Engineering, attacks, hacking, vulnerabilities, and errors relevant to IoT sensors. Moreover, we integrated power-related terminology into our search parameters, such as "Wheatstone bridge," "load cell," and "strain gauge," to ensure alignment with our specific use case and enhance the breadth of our investigation.

[4] https://mqtt.org/

1. Literature study and documentation analysis. Table 1 lists the phrases we used to search the literature relevant to our use-case experiment.
2. Experimental Setup. Lab equipment and cloud environment to read the sensor data.
3. Reverse Engineering. Encompassing an understanding of the Sensor's operational principles, including analyzing electrical signal levels.
4. Vulnerability Discovery and Analysis: finding potential vulnerabilities within the sensor's design and evaluating how they can be exploited.
5. Attack Strategy: we employ our findings to craft an attack compromising the trustworthiness of the sensor.

Fig. 2: Steps in our HRE Use Case Approach

Table 1: Search Terms

reverse engineering	attack	fault injection
hardware	hacking	false data
hardware reverse engineering	error	power bus
sensor error	vulnerability	power glitch
sensor	iot	power spike
sensor hacking	wheatstone bridge	sensor glitch
sensor attack	strain gauge	power rail
sensor vulnerability	load cell	point of failure

3.2 Experimental Setup

The lab setup is illustrated in Figure 3, where we operated in a general-purpose room without specialized electrical engineering provisions. We obtained low-cost tools as required, as listed in Figure 4. Figures 1b and 3 reveal the internal logic of the ICEBOX Load Sensor, elaborated further in Figure 5.

As previously mentioned, the ICEBOX Load Sensor transmits the processed signal from the Wheatstone bridge to a remote gateway or cloud infrastructure. In our experiment, we established a data collection system on AWS, connecting it to AWS IoT. A sample DK application was deployed to facilitate message transmission to AWS IoT. Additionally, we configured a DynamoDB database to store incoming messages, including the processed Wheatstone bridge signal, and established message routing rules to transfer messages from AWS IoT to our designated database.

Due to the ICEBOX Load Sensor's 20-tonne rating, we selected a load cell with a range of 0 to 1kg and a 1mV/V output rate, in contrast to the original sensor's 2mV/V output rate. To mimic the internal logic of the ICEBOX Load Sensor, we employed the original amp-PCB, an nRF9160 development kit, the 1kg load cell, and the RIGOL DP832 to power the setup. Common items specified in Table 2 were utilized to apply load.

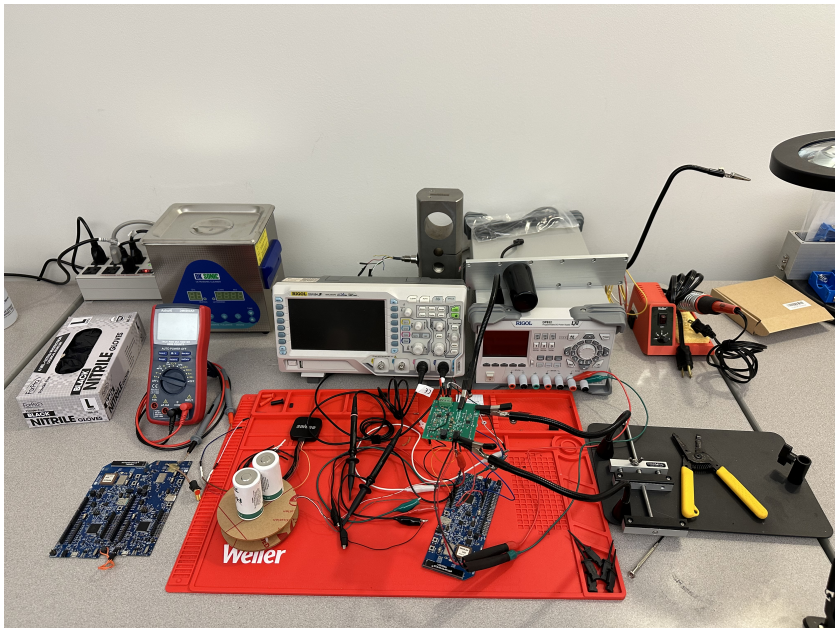


Fig. 3: A low-cost lab setup

1. Weller soldering iron.
2. RIGOL DS1054Z oscilloscope, an entry-level scope with a 50MHz bandwidth and four channels.
3. AstroAI True RMS 6000 multimeter.
4. RIGOL DP832 Triple output 195-watt power supply.
5. DK Sonic Ultra Sonic Cleaner.
6. 1kg Load Sensor with an output of 1mV/V.
7. iPhone 14 Pro.

Fig. 4: Lab tools: Shown in Figure 3. The iPhone was used to capture the image

a) Nordic Semiconductor nRF9160 development kit (DK). Blue color.
b) An amplifier-PCB (Amp-PCB). Green color.
c) Two LSH 20 batteries. White and green color.

Fig. 5: Internal Logic of the ICEBOX Load Sensor

Table 2: Common Item Weights

Description	**Weight**
1 LSH20 Battery	100g
2 LSH20 Batteries	200g
140W Apple Charger Block	340g
1 LSH20 + 140W Apple Charging Block	440g
Power Bank	567g
1 LSH20 + Power Bank	667g
2 LSH20 + Power Bank	767g
140W Apple Charger Block + Power Bank	907g
140W Apple Charger Block + Power Bank + LSH20	1007g

3.3 Reverse Engineering and Analysis

We started reverse engineering by photographing the internal logic. Before imaging, we cleaned the two PCBs with an entry-level ultrasonic cleaner, overcoming challenges posed by protective silicone residue. High-resolution images were captured with the iPhone 14 Pro to assist in identifying circuit pathways and Surface Mounted Device (SMD) components, facilitating the compilation of a Bill Of Materials (BoM) for the ICEBOX amp-PCB. Continuity testing with the multimeter yielded Figure 6, illustrating the amp-PCB's electrical flow and detailing important Integrated Circuits (IC) listed in Figure 7. Figure 8 shows the connection between the amp-PCB and the DK. The operation of the ICEBOX Load Sensor is described in Figure 9.

The two 3.6V batteries are connected to the amp-PCB as depicted in Figure 6. VDD_nRF represents the 3.6V battery voltage supply (VSUPPLY) for the DK, while VDD is the main supply (1.8V) for the remaining circuitry on the DK. The DK's GPIO (General Purpose In Out) pins interface with the amp-PCB. Once the internal logic is powered on, it initiates a 4-second signal transmission via pin P0.17 on the DK to p0.17 on the amp-PCB. Following this, it sends an approximately 30 ms signal, capturing measurements every 4 seconds thereafter.

On the amp-PCB, VDD voltage (1.8V) travels through the Blue wire from p0.17 into IC1. When triggered by pin p0.17, IC1 activates the Orange power bus, which provides excitation voltage to the Wheatstone bridge and power to IC2. The Wheatstone bridge returns a positive (Green) and a negative (White) signal, with a maximum output of 1 mV/V, fed into IC2. IC2 utilizes the power from the Orange power bus to amplify this signal. Following amplification by IC2, the signal proceeds to pin p0.14 (Yellow) and then to pin P0.14 on the DK, ultimately entering its ADC for conversion to a digital value.

In our experimental setup, ICs 5-8 were removed from the PCB to enable testing beyond the device's standard operating voltage range. These diodes prevent reverse current from reaching the batteries and limit the forward current flow to protect the PCB electronics.

We refer to the original nRF9160 DK in the ICEBOX Load Sensor as the "Live Board" (LB). The LB came pre-configured, posing challenges for data

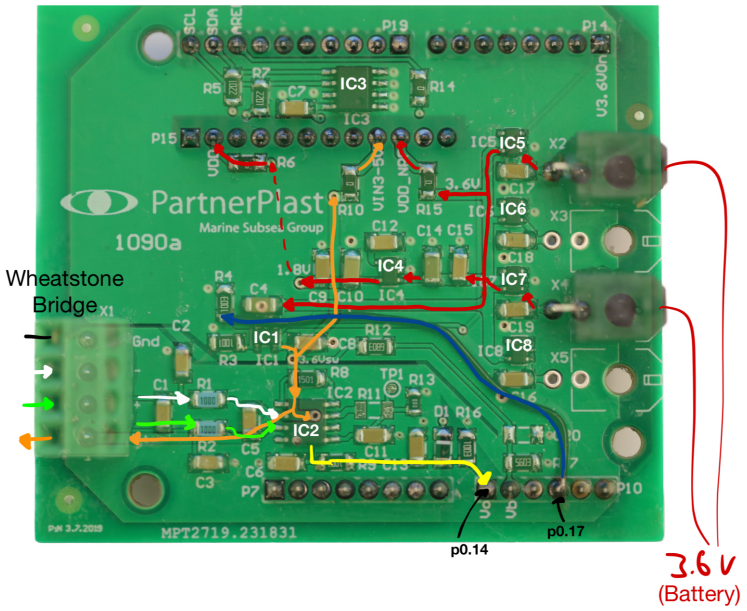


Fig. 6: Electrical flow amp-PCB

1) IC1: a Load Switch responsible for powering the Orange powerbus.
2) IC2: amplifies the Wheatstone bridge's output voltage signal (Green/White).
3) IC4: a voltage regulator that reduces the voltage level to 1.8V.
4) IC5-8: diodes to protect the batteries by preventing backcurrent.

Fig. 7: Important IC's

extraction. To overcome this, we replicated the LB's application onto a new DK. A key function of the LB is to convert analog voltage signals from the amp-PCB into digital values. Consequently, we configured our DK's ADC to match the LB's settings. Information on the memory locations for the configuration of the internal ADC was provided in the Nordic Semiconductor documentation. Using the nrfjprog tool[5], we interfaced with the DK to read the memory at specified locations, revealing the LB ADC configuration, as shown in Figure 10.

3.4 Attack Strategy

Given that the DK's ADC relies indirectly on the analog input from the Wheatstone bridge for conversion to digital format, we anticipated that ma-

[5] https://www.nordicsemi.com/Products/Development-tools/nrf-command-line-tools/download

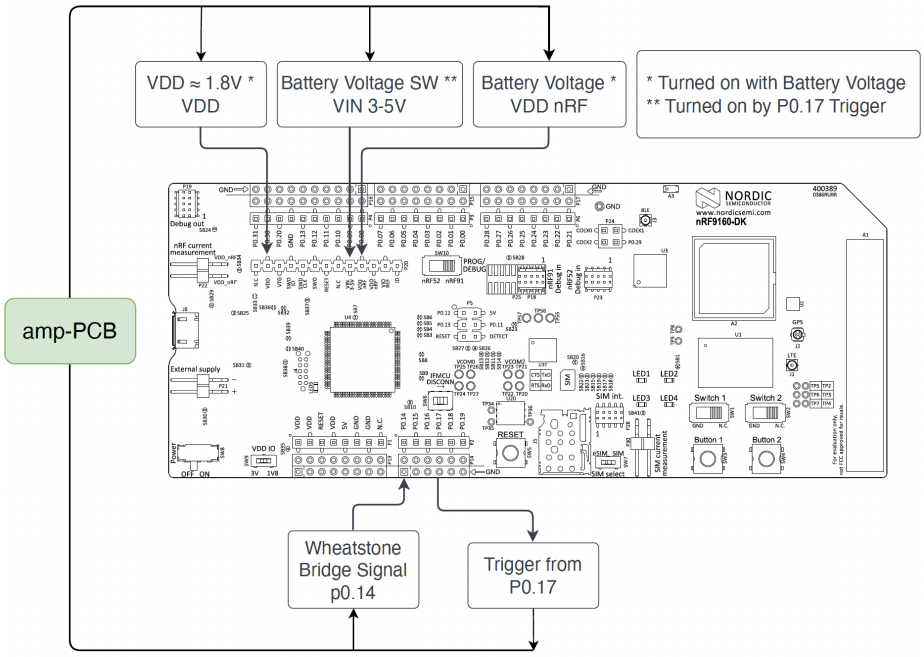


Fig. 8: Pin connection amp-PCB and nRF9160 DK

1) The two LSH 20 batteries supply the operational voltage to the amplifier-PCB. The amplifier-PCB is connected to the DK.
↓
2) The amplifier-PCB powers the Wheatstone bridge, which generates a voltage signal in return.
↓
3) The amplifier-PCB receives and amplifies the Wheatstone bridge voltage signal and then passes it to the DK.
↓
4) The DK processes the voltage signal to a digital representation. A nRF Successive Approximation Analog-to-Digital Converter (ADC) hosted on the DK within a 9160 System in Package (SiP) converts the analog voltage signal into a digital representation.
↓
5) The digital value is passed to the antenna interface and sent to a remote Gateway or cloud infrastructure.

Fig. 9: The ICEBOX Load Sensor Operation

nipulating the Wheatstone bridge return signal (Green and White in Figure 6) would result in inaccurate sensor data being sent to our AWS setup.

- Resolution: 14 (bits).
- Gain: 1/4 (of P0.14).
- Reference: VDD_GPIO/4.
- Acquisition Time: 20 microseconds.
- Differential: Off.
- Burst: On, Oversample (over256x).

Fig. 10: LB ADC Configuration

Our attack strategy involved adjusting the system's operating voltage level. However, the batteries lacked a direct means of adjusting the supplied power level and would quickly drain. By utilizing the Rigol DP832 Triple power supply, we could indirectly inject various manipulated voltage levels into the Wheatstone bridge. Notably, the system would not boot below 3.04V, prompting us to conduct tests from 3.1V to 3.9V in increments of 0.1V. For each weight-voltage combination, we took five measurements, totaling four weights, to validate successful voltage manipulation. Additionally, to assess the impact of our attacks, we tested ten weights over 5 minutes to sample an average value per weight-voltage combination for the ADC output values.

4 Results and Discussion

4.1 Analysis of Our Results

We utilized ADC data to generate lines of best fit for ADC output at various weights and battery voltages. Figure 11 displays the average values and lines of best fit for 3.1V (Black), 3.6V (Red), and 3.9V (Yellow). Comparing the 3.6V line with the other lines reveals that manipulating voltage results in ADC values representing a different load. Increasing the voltage raises the ADC value, indicating a higher load, while decreasing it yields the opposite effect. Our findings suggest an average 3% change in ADC output and weight for every 0.1V deviation from the standard voltage using our 1kg 1mV/V load cell.

Scaling our attacks to match the Wheatstone bridge in the ICEBOX Load Sensor, we calculate a 6% change instead of 3% for every 0.1V change. This doubling is due to the 2mV/V output compared to the 1mV/V of our 1kg max load cell. At the lowest battery voltage of 3.1V, we would observe a 30% decrease in the Wheatstone bridge signal, resulting in a reported load 30% lower than the actual load. Conversely, at 3.9V, we would see an 18% increase in signal and perceived load.

4.2 Analysis of Our Low-cost Approach

Figure 2 laid out five steps for our low-cost use case experiment. However, expertise to accomplish and complete each step sequentially is achieved through

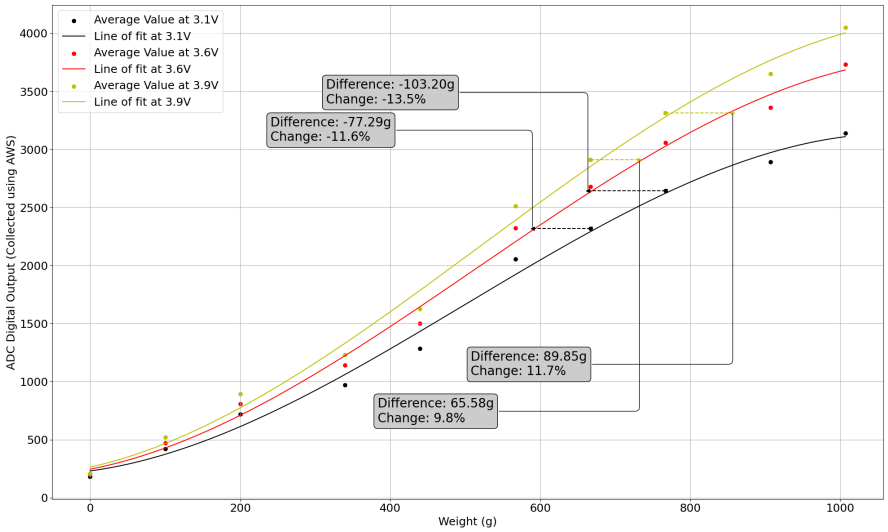


Fig. 11: Voltage manipulation results in a load increase/decrease

practice and experience [11]. For novices, adhering strictly to a step-by-step process may be challenging. For example, doubts about measurement data may arise, prompting questions about tool functionality. Tool inexperience may create uncertainty, leading to revisiting previous steps. Nonetheless, this reiterative process is rewarded by know-how expertise. Proficiency in tools instills confidence in measurements. Tool proficiency can be enhanced through proper training and practice. While commercial training courses can be costly, free online resources like Hackaday[6] and EEVblog[7] offer free access to easy-to-understand tutorials as well as expert advice.

Collaboration with peers significantly enhances problem-solving. For example, the print on SMD components doesn't always provide clear identification. In such cases, the expertise of an electrical design engineer can prove invaluable in deciphering their purpose by analyzing surrounding components. Moreover, developer forums like the Nordic Semiconductor Devzone[8] serve as interactive knowledge hubs, offering advice and guiding individuals to other valuable sources of information and learning. HRE is an exploratory process significantly enhanced by active discussion, whether conducted online, in a group setting, or both. For group collaboration, having access to a whiteboard and the object under scrutiny facilitates alignment and discussion to plan the next steps in the HRE process. Through collaborative efforts, the group collectively learns from each other, enhancing individual expertise and know-how in HRE.

[6] https://hackaday.com/
[7] https://www.eevblog.com/
[8] https://devzone.nordicsemi.com/

In summary, our Approach in Figure 2 is an iterative process that leverages collaboration to develop HRE expertise. It provides an initial framework, allowing to iterate through steps 1-4 as necessary before advancing to step 5. For example, this might entail 1) reviewing additional documentation, 2) enhancing lab equipment functionality, and 3) conducting reverse engineering and testing, leading to analysis and a deeper understanding of the object under scrutiny.

4.3 Shortcomings and Limitations

In our experiment, we opted for an affordable 1kg load cell for our manipulation attacks due to practical constraints. The ICEBOX Load Sensor's 20-tonne rating made it impractical for precise load applications. However, we acknowledge that the Wheatstone bridge quality in the 1kg load cell may not match the accuracy of the more expensive Wheatstone bridge found in the ICEBOX Load Sensor.

Although we had access to the RIGOL DS1054Z oscilloscope, we chose to use the multimeter for measuring analog signal levels in our experiment. We found this method to be faster, especially considering our difficulties in accurately capturing sub-mV levels with the oscilloscope, which has a 1mV per vertical division setting. Additionally, user errors may have contributed to our challenges in obtaining accurate captures. We could have utilized specialized probe tips and tailored grounding commonly employed in professional electrical engineering workshops to improve our setup. However, these options were not feasible for our low-cost approach. It's worth noting that the analog voltage level measurements were primarily used to verify our voltage manipulations. Using the multimeter did not affect the digital measurements recorded in AWS.

The AMIP ICs malfunctioned during testing despite our voltage manipulations being within their 1.5V to 5.5V operating range. The increased voltage overextended the forward Current limit, rendering the AMIP ICs inoperable. The output Current per channel from the RIGOL DP832 power supply can be limited if configured correctly. However, our low-cost experiment only had one specimen of the amp-PCB, and to address the malfunctioning AMIPs, we removed them and soldered a bridge between the voltage input and output pads on the silk print. We acknowledge the AMIP ICs may serve as a protective mechanism, possibly making our battery voltage manipulation attack irrelevant. However, attackers could exploit this by intentionally removing the AMIP for battery voltage manipulation or adding resistors to limit increased Current draw due to the increased operational voltage.

The ICEBOX Load Sensor allows remote monitoring of battery voltage. Thus, our voltage manipulation, which involves increasing operational battery voltage, could easily be detected. Our reverse engineering indicates that battery level measurement is sampled through pin P0.15 on the DK, receiving voltage from the amp-PCB pin V_b, placed to the right of p0.14, and enabled by IC1, as shown in Figure 6. Nevertheless, an attacker could evade detection by inserting a voltage regulator between IC1 and pin V_b.

5 Conclusion and Future Work

In conclusion, our research successfully leveraged a low-cost HRE approach to identify hardware weaknesses, culminating in an attack strategy to manipulate the device's trustworthiness. It also detailed how novice-friendly tools, techniques, and educational resources can be utilized to gain insight into a black box scenario. Apart from our iPhone, our entire laboratory setup costs less than one thousand US dollars, showcasing the effectiveness of low-cost approaches in uncovering vulnerabilities. This underscores that Hardware Reverse Engineering experiments are feasible without substantial financial investment, opening accessibility to a broader audience.

In future work, we aim to enhance our approach by experimenting with additional use cases to generalize our findings. Furthermore, we can explore the different categories of HRE that can be employed based on the toolset. Additionally, investigating the limitations of the various low-cost approaches will be valuable.

Acknowledgements

We want to thank Professor Indrajit Ray and Professor Indrakshi Ray for their valuable guidance and support throughout this research project. We also thank Colorado State University for providing the lab facilities necessary for this endeavor.

References

1. Bhunia, S.: The hardware trojan war. https://doi.org/10.1007/978-3-319-68511-3
2. Adee, S.: The hunt for the kill switch **45**(5), 34–39. https://doi.org/10.1109/MSPEC.2008.4505310
3. Becker, S., Wiesen, C., Albartus, N., Rummel, N., Paar, C.: An exploratory study of hardware reverse engineering — technical and cognitive processes. pp. 285–300. https://www.usenix.org/conference/soups2020/presentation/becker
4. Bhunia, S., Hsiao, M.S., Banga, M., Narasimhan, S.: Hardware trojan attacks: Threat analysis and countermeasures **102**(8), 1229–1247. https://doi.org/10.1109/jproc.2014.2334493, publisher: Institute of Electrical and Electronics Engineers (IEEE)
5. Harrison, J., Asadizanjani, N., Tehranipoor, M.: On malicious implants in PCBs throughout the supply chain **79**, 12–22. https://doi.org/10.1016/j.vlsi.2021.03.002, publisher: Elsevier BV
6. Horowitz, P.: The art of electronics. Cambridge University Press, third edition edn.
7. Huang, A.B.: Hacking the Xbox: An Introduction to Reverse Engineering. No Starch Press
8. International Energy Agency, I.: Electricity 2024 - analysis and forecast to 2026 https://iea.blob.core.windows.net/assets/6b2fd954-2017-408e-bf08-952fdd62118a/Electricity2024-Analysisandforecastto2026.pdf

9. Mehta, D., Lu, H., Paradis, O.P., M. S., M.A., Rahman, M.T., Iskander, Y., Chawla, P., Woodard, D.L., Tehranipoor, M., Asadizanjani, N.: The big hack explained: Detection and prevention of PCB supply chain implants **16**(4), 42:1–42:25. https://doi.org/10.1145/3401980
10. Omitola, T., Wills, G.: Towards mapping the security challenges of the internet of things (IoT) supply chain **126**, 441–450. https://doi.org/10.1016/j.procs.2018.07.278
11. Rekoff, M.G.: On reverse engineering **SMC-15**(2), 244–252. https://doi.org/10.1109/TSMC.1985.6313354
12. Sharma, A., Dyrkolbotn, G.O., Øverlier, L., Waltoft-Olsen, A.J., Franke, K., Katsikas, S.: A state-of-the-art reverse engineering approach for combating hardware security vulnerabilities at the system and PCB level in IoT devices. In: 2022 IEEE Physical Assurance and Inspection of Electronics (PAINE). pp. 1–7. https://doi.org/10.1109/PAINE56030.2022.10014884
13. Vosatka, J.: Introduction to hardware trojans. In: Bhunia, S., Tehranipoor, M.M. (eds.) The Hardware Trojan War: Attacks, Myths, and Defenses, pp. 15–51. Springer International Publishing. https://doi.org/10.1007/978-3-319-68511-3_2
14. Wiesen, C., Becker, S., Fyrbiak, M., Albartus, N., Elson, M., Rummel, N., Paar, C.: Teaching hardware reverse engineering: Educational guidelines and practical insights. In: 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE). pp. 438–445. https://doi.org/10.1109/TALE.2018.8615270
15. Wiesen, C., Becker, S., Walendy, R., Paar, C., Rummel, N.: The anatomy of hardware reverse engineering: An exploration of human factors during problem solving . https://doi.org/10.1145/3577198