JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

LOKI F0RG3: A comprehensive Survey of Hardware Pentesting Tools for IoT Security Assessment

H Sanjay
Dept. of Computer Science & Engineering (Cyber Security), Dayananda Sagar College of Engineering
Bengaluru, India

R Aswin
Dept. of Computer Science & Engineering (Cyber Security), Dayananda Sagar College of Engineering
Bengaluru, India

Ritisha Bhattacharjee
Dept. of Computer Science & Engineering (Cyber Security), Dayananda Sagar College of Engineering
Bengaluru, India

Riya Sinha
Dept. of Computer Science & Engineering (Cyber Security), Dayananda Sagar College of Engineering
Bengaluru, India

Padmavathi S
Dept. of Computer Science & Engineering (Cyber Security), Dayananda Sagar College of Engineering
Bengaluru, India

***Abstract*—**The exponential growth of Internet of Things (IoT) devices has created a rapidly expanding range of exploitable entry points for malicious actors, necessitating specialized hardware penetration testing tools for thorough evaluation of system resilience . The hardware pentesting tools available today are systematically analyzed in this survey, with an emphasis on small, multipurpose devices that are appropriate for assessing the security of the Internet of Things. Identifies significant deficiencies in protocol coverage, automation capabilities, and operational efficiency through the comprehensive analysis of existing tools including Flipper Zero, Proxmark3, and HackRF One . Our research shows that the tools we have now are very fragmented, and no one platform covers all the wireless protocols used in modern IoT deployments. Based on a 2.45 billion USD analysis of penetration testing market data and an evaluation of over 15 hardware platforms, this survey establishes a framework for next-generation integrated security assessment tools. The research contributes to hardware security methodology by quantifying automation gaps, where basic tools achieve only 30-85% automation across different testing categories, while custom solutions can reach 85-100% automation . One of the primary recommendations is the development of unified platforms that integrate Sub-GHz, RFID/NFC, WiFi, and Bluetooth capabilities in portable form factors specifically designed for field assessment operations.

Keywords*—*hardware penetration testing, wireless protocol analysis, RFID, NFC, IoT security, software-defined radio, and cybersecurity evaluation tools.

I. INTRODUCTION

The Internet of Things (IoT) ecosystem has expanded rapidly . In 2024, there were an estimated 18.8 billion connected devices around the world, and by 2030, there will be 40 billion [3] . This rapid growth has changed the cybersecurity landscape by adding many different types of attacks that go beyond what traditional network security measures can handle. Hardware penetration testing has now become a very important part of digital security which helps to find vulnerabilities in physical devices, protocols of wireless communication, and embedded systems that form the basis for current deployments of IoT.

Security evaluations have risen up quite significantly with the expansion of IoT devices across the areas or domains of smart cities, health care, automobiles and industrial automation. Security system vulnerabilities of IoT come via hardware by way of communications protocol implementation, wireless communication, and physical interfaces, for which specific test methods and tools are required, thus making it different from the formal network based weaknesses.

The current hardware penetration testing techniques have some ingrained weaknesses that make extensive security testing very difficult to be performed. Tool fragmentation has increased the complexity and cost of operations by a huge margin, since a multitude of different specialized tools are now required to address all the protocols. Besides being complex, the lack of support for a considerable degree of automation by existing platforms means a great deal of work must be performed manually, thus making it more difficult to scale up and opens the door to human errors as well.

This survey addresses these challenges by a structured investigation of available hardware pentesting tools and estimation of protocol coverage holes, combined with a deep analysis of the automatability status across various testing areas. Our key contributions are: (1) a comprehensive comparison of well-known hardware penetration testing tools; (2) quantitative estimate of protocol coverage fragmentation; (3) market analysis that shows the proof for CAGR 17.1% growth in the need for penetration testing; and (4) framework recommendations for the next generation of integrated security assessment tools.

II. BACKGROUND AND RELATED WORK

Table I: IoT Device Vulnerability Distribution

Device Type	Vulnerability %	Common Attack Vector
TV Sets	34	Unpatched firmware
Smart Plugs	18	Default credentials
Digital Video Recorders	13	Buffer overflow
Routers	12	Configuration flaws
IP Cameras	15	Authentication bypass
Smart Speakers	8	Voice command injection

A. IoT Security Landscape

The security threat environment of IoT has evolved very dramatically over the years with critical vulnerabilities to multiple device categories. Current research indicates that buffer overflow vulnerabilities constitute about 28.25% of the total IoT security vulnerabilities, followed by denial of service attacks at 27.20% [6]. With 34% in the Tv Sets device category; smart plugs and digital video recorders have 18% and 13%, respectively [6].

IoT security attacks average a financial loss of around $330,000 per attack and attacks on healthcare IoT devices have increased at a yearly rate of almost 123% [9]. Nearly 60% of IoT security attacks result from unpatched firmware, citing the ongoing challenge of managing security across disparate device ecosystems with different 13% security mechanisms and lifecycle management practices.

B. Hardware Pentesting Evolution

Basic protocol testing has been replaced with advanced multi-vector testing frameworks in hardware penetration testing methods. Conventional methods mainly responded to the network layer vulnerabilities whereas the contemporary IoT systems demand very aggressive wireless protocol testing, cryptographical methods, and physical security controls.

Software-defined radio technology advancements have totally changed hardware security analysis. It provides programmable, flexible platforms for supporting different wireless protocols. However, SDR-based solutions also tend to require enormous computational capability and technological expertness, which makes it difficult for them to be applied on run-of-the-mill security testing and field deployments.

C. Current Tool Limitations

Current hardware pentesting tools have three inherent shortcomings in that there is fragmentation in protocol coverage, automation features are highly restricted, and operations are complex. No single tool offers comprehensive coverage of all protocols in the entire IoT universe, hence security experts will have to carry on with multiple dedicated platforms and tools, which include steep learning curves, maintenance, and interoperability issues.

III. METHODOLOGY

This survey combines a systematic review of existing literature, practical or empirical analysis of hardware penetration testing tools and current market trends. It includes in-depth and critical assessment of peer-reviewed academic literature, analysis of technical software documentation, and a quantitative consideration of the capability of the tools in various different aspects.

A. Criteria for Tool Selection

The hardware penetration testing tools were chosen based on their market adoption, technical capabilities and their relevance to IoT device security assessments. Five major factors formed the basis of selection : 1) multi-protocol support abilities, 2) portability and capability for field operation, 3) open-source or commercial platforms, 4) active development and community backing, and 5) documented use in manufacturing and academic studies.

B. Evaluation Framework

Tool analysis was made using a formal structure for evaluation of technical specifications, protocol coverage, automation and other operational features. Quantitative measures mainly included frequency range coverage and transmission power capabilities while supporting modulation schemes and protocol compatibility matrices were also made sure to be recorded.

C. Data Sources

The basis of the data sources are peer reviewed scholarly journals with publications dated from the year 2020 to 2024 along with technical reports by manufacturers, market research studies by popular cybersecurity groups, and results of testing by security research institutions. Market Data has several insights from research entities which include popular ones like Markets and Markets, Straits Research, and Fortune Business Insights.

IV. CURRENT HARDWARE PENTESTING TOOLS ANALYSIS

A. Flipper Zero:

Flipper Zero represents a huge leap forward in the field of handheld hardware security testing due to its combination of multiple wireless interfaces in an elegantly small and user-friendly package. Based on the STM32WB55 microcontroller, the hardware comes with onboard Bluetooth Low Energy and a dedicated CC1101 transceiver, therefore supporting Sub-GHz frequencies between 300 MHz and 928 MHz with region-specific lockout [21][24].

Technical Specifications: It can support a host of protocols such as iButton/Dallas key analysis, NFC Type A/B, 125 kHz and 13.56 MHz RFID, Sub-GHz wireless protocols, and infrared communication. The device can operate up to approximately 168 hours with the provided 2000 mAh battery, and custom hardware integration is supported via GPIO interfaces.

Capabilities and Applications: Flipper Zero excels at keyless entry gadgets, remote-controlled garage doors, Smart Home device testing, and standard access control installations. It can be operated by security professionals with different technical proficiency because it has a user-friendly interface that reduces learning to a great extent compared to traditional hardware security devices.

Limitations: Although a multi-tool, Flipper Zero does have limitations that make it incapable of performing a complete IoT security scan. WiFi testing is important in current 802.11-based IoT devices, but the tool cannot accomplish that. High-end signal analysis is limited by processing, and while the Sub-GHz band is broad, it is not all frequency bands available on current wireless devices. Firmware restrictions also prevent it from performing real-time signal processing and full protocol examination, both of which are needed in sophisticated attack scenarios.

B. Proxmark3:

Proxmark3 platform is the gold standard for NFC and RFID security evaluation, offering unmatched accuracy and versatility for contactless communication testing. The tool utilizes a double-architecture framework consisting of an ARM7 microcontroller and an Xilinx Spartan-II FPGA for signal processing at high speed [22][25].

Architecture and Capabilities: The architecture of FPGA allows advanced signal analysis, user programmable protocol implementation, and real time demodulation / modulation on both the low-frequency band of 125 kHz and the high-frequency band of 13.56 MHz. Besides a number of proprietary RFID implementations, the product offers broad protocol coverage including ISO14443 and ISO15693 [22].

Advanced Features: Proxmark3 boasts of more enhanced features which include the capability to visualize signals, reverse engineer protocols along with emulation and cloning of cards. The scriptable interface allows for automated test scenarios and the large community-driven development has created specialized modules for new RFID technologies.

Constraints: The specialization in RFID/NFC technologies at the cost of general protocol support is the platform's drawback. Proxmark3 has no features for Sub-GHz communications, WiFi scanning or Bluetooth testing, and some other tools would be needed for thorough IoT security testing. High learning curve and computer connection requirement also reduce its appeal for field work.

Table II: Hardware Pentesting Tools Technical Specifications

Tool	Frequency Range	Architecture	Max TX Power	Protocols Supported	Price (USD)	Battery Life	Form Factor
Flipper Zero	300-928 MHz	STM32WB55 + CC1101	0 dBm	Sub-GHz, NFC, RFID, IR, iButton	169	168 hours	Portable handheld
Proxmark3	125 kHz, 13.56 MHz	ARM7 + FPGA	Field generation capable	LF/HF RFID only	300-500	USB powered	Desktop/Lab
HackRF One	1 MHz - 6 GHz	MAX2837/MAX5864	5-15 dBm (varies by freq)	Wide SDR support	300	USB powered	Desktop/Lab
RTL-SDR	24 MHz - 1.75 GHz	RTL2832U + R820T2	RX only	DVB-T-based protocols	25-50	USB powered	USB dongle

C. HackRF One:

The HackRF One provides software-defined radio capabilities covering an unprecedented frequency range from 1 MHz to 6 GHz enabling flexible protocol analysis and custom signal processing applications . The platform utilizes the MAX2837/MAX5864 transceiver architecture with USB 2.0 connectivity for computer-based operations [23][26].

Technical Specifications: It supports sample rates of up to 20 Msps with 8-bit resolution providing 20 MHz instantaneous bandwidth for signal analysis. The half-duplex architecture enables either transmission or reception, while the wide frequency coverage encompasses most wireless protocols used in IoT deployments [23] .

Applications and Flexibility: The Software Defined approach enables custom protocol development, spectrum analysis, or research applications requiring fine-grained frequency control which when integrated with a GNU Radio or other SDR framework, will provide the advanced user with a very capable signal processing platform.

Operational Limitations: High technical expertise and desktop connectivity are required to operate HackRF One, hence limiting its usefulness in field assessments. The half-duplex nature does not allow transmission and reception to take place simultaneously, while the lack of an integrated user interface makes it unsuitable for fast security testing. Heat production and power consumption during continuous operation are other operational limitations.

V. PROTOCOL COVERAGE ANALYSIS

The wide-ranging analysis of protocol coverage has shown large fragmentation among the existing hardware pentesting tools, each of which does not support the wide range of wireless technologies that are typically deployed in contemporary IoT environments.

Table III: Protocol Coverage Comparison Matrix

Protocol	Flipper Zero	Proxmark3	HackRF One	RTL-SDR
Sub-GHz (300-928 MHz)	Full	None	Full	Limited
LF RFID (125 kHz)	Full	Full	Full	Limited
HF RFID/NFC (13.56 MHz)	Full	Full	Full	Limited
WiFi (2.4/5 GHz)	None	None	Full	Limited
Bluetooth LE	Limited	None	Full	Limited
Infrared	Full	None	None	None
iButton/1-Wire	Full	None	None	None
GPIO Interface	Full	Limited	Limited	None

A. Sub-GHz Protocol Support

Sub-GHz frequency bands span from 300 to 928 MHz and are used primarily in IoT devices, such as smart home appliances, industrial sensors, and agricultural monitoring systems. Flipper Zero is capable of broad coverage within the frequency bands supported by it whereas HackRF One provides wider frequency coverage, although at the cost of advanced configuration. Proxmark3 has no functionality for Sub-GHz at all, which creates gaps in comprehensive security assessment workflows [21][33].

B. RFID and NFC Analysis

For many tasks, such as access control, asset tracking, and payment systems, low-frequency 125 kHz and high-frequency 13.56 MHz RFID technologies are still used. Of these, Proxmark3 proves to be the best in this domain by offering the best accuracy and protocol coverage, while Flipper Zero has basic functionality that is somewhat enough for a frequency burst. However, HackRF One can analyze those frequencies with ease but lacks all those features of specialized RFID processing [22][33].

C. WiFi and Bluetooth Assessment

Modern IoT devices are increasingly using WiFi protocols operating at 2.4 GHz & 5 GHz and Bluetooth Low Energy protocols for connectivity. Frequency coverage for these technologies is provided by HackRF One but requires external deployments for protocol-specific analysis.Neither Flipper Zero nor Proxmark3 has the capability for comprehensive WiFi assessment - a serious gap in the current set of offerings [24][26].

D. Coverage Gap Analysis

Quantitative analysis reveals that complete protocol coverage involves using several specialized tools which would result in considerable complexity and operational overhead. No platform currently supports the combination of Sub-GHz, RFID/NFC, WiFi, and Bluetooth protocols required by a complete IoT security assessment. This fragmentation demands significant expertise in many tool platforms and creates more chances of security gaps because of incomplete assessment coverage.

VI. AUTOMATION CAPABILITIES ASSESSMENT

Automation remains a crucial factor in scaling up hardware security assessments for very large-scale IoT deployments. Current analyses indicate large differences in terms of automation within various categories of testing and test tool capabilities.

A. Network Scanning and Device Enumeration

Basic network scanning utilities reach about 85% automation in discovery and enumeration of devices, whereas advanced ones are capable of going upwards to 95% automation. Custom made solutions can achieve near complete automation (100%) for network reconnaissance activities. Device enumeration also shows related close patterns, with basic tools achieving near 70% automation and advanced platforms reaching 90%.

Table IV: Automation Capabilities Assessment

Testing Category	Basic Tools (%)	Advanced Tools (%)	Custom Tools (%)
Network Scanning	85	95	100
Vulnerability Detection	45	75	95
Protocol Analysis	30	65	90
Signal Capture	60	85	95
Device Enumeration	70	90	95
Security Assessment	40	70	85

B. Vulnerability Detection and Assessment

Vulnerability detection is one of the most difficult automation classes, where simple tools only achieve about 45% automation because of the sophistication involved in vulnerability identification and validation. Advanced tools boost this to 75%, while customized solutions are able to achieve 95% automation using specialty detection algorithms and machine learning techniques.

C. Protocol Analysis Automation

Protocol analysis shows the lowest automation rates among all categories, with basic tools achieving only 30% automation for complex protocol reverse engineering tasks . Advanced tools improve this to 65%, while custom solutions can achieve 90% automation through specialized protocol parsers and analysis frameworks .

D. Signal Capture and Processing

Signal capture and processing activities show moderate automation potential, with basic tools achieving 60% automation for routine capture tasks . Advanced platforms improve this to 85%, while custom solutions achieve 95% automation through automated triggering, filtering and analysis capabilities .

VII. MARKET ANALYSIS AND TRENDS

A. Market Growth Trajectory

The global market for penetration testing is very strong, with growth expected from around $2.45 billion in 2023 to close to $11.37 billion by the end of the year 2033, at a CAGR of approximately 17.1%. This is attributed to increased awareness of the need for cybersecurity, coupled with regulatory demands that push organizations toward proactive security evaluation methods [2][5].

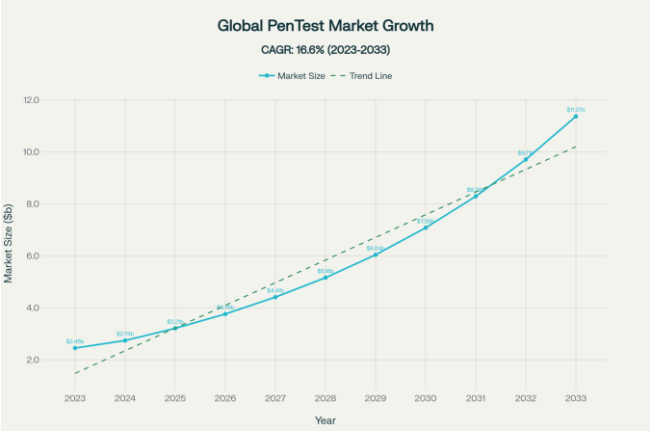

Figure 1: Global Penetration Testing Market Growth Projection (2023- 2033) - this segment is experiencing exponential growth at a consistent CAGR of 17.1%, reflecting high demand for cybersecurity services on the growth of IoT devices and their regulatory compliance.

B. Regional Distribution

The North American region is measured to have contributed approximately 35.92% to the penetration testing market in 2024, mainly attributed to the highly developed cybersecurity infrastructures and regulatory environments within the region, whereas the fastest-growing region for the adoption of testing services was found to be the Asia-Pacific, headed by countries like China and India, and was fueled by the rapid digitization strategies recently employed and the increasing deployments of IoT devices [5][11].

C. Technology Integration Trends

Integration of machine learning and artificial intelligence is a revolutionary trend. As per 80% of the total businesses, using advanced testing tools in 2024 is primarily motivated by regulatory compliance. Up to 30% less time is spent by analysts thanks to AI-driven tools, which also improve the accuracy of vulnerability detection [5][8].

D. Market Challenges

The market still faces significant obstacles despite these optimistic growth projections, such as high implementation costs, a lack of skilled workers, and the constantly evolving nature of cyberthreats, which fragments the market and necessitates the provision of less expensive automated test solutions [2][8].

VIII. CRITICAL GAPS AND FUTURE DIRECTIONS

A. Protocol Coverage Fragmentation

Currently, the basic protocol coverage of the tools is fragmented, and no one platform offers complete support for Sub-GHz, RFID/NFC, Wi-Fi, and Bluetooth, which thus forces organizations to maintain a variety of specialized tools, thereby raising the costs and complexity, besides also increasing the possibility of security assessment gaps..

B. Automation Limitations

Current tools are very much short of intelligent automation features for intricate analytical tasks, particularly in the fields of protocol reverse engineering and vulnerability assessment. The current automation levels of 30–45% for complex analysis tasks show that there is a lot of room for improvement by the integration of machine learning and artificial intelligence.

C. Field Operation Constraints

Most of the existing tools have desktop connectivity needs, which limit their field usage in security assessment tasks. The absence of unified analytical capabilities in these tools and their high dependency on third-party software application serve as a major bottleneck to operational efficiency when it comes to security assessment processes.

D. Integration Challenges

Data silos and inefficient workflows which are caused mainly by poor interconnectivity between tools, weaken overall assessment quality. Multi-tool assessment approaches are further made more complicated or harder without standardized data formats and analysis protocols.

IX. RECOMMENDATIONS FOR NEXT-GENERATION TOOLS

A. Unified Protocol Platform

Future hardware penetration testing tools should embed or include extensive protocol support in one single platform or tool, combining Sub-GHz, RFID/NFC, WiFi, and Bluetooth modules. This would thus help reduce a lot of functioning complexities involved and also ensure complete coverage of IoT wireless technologies.

B. AI-Enhanced Automation

Next-generation tools should have embedded AI and ML algorithms automatically for applying the capabilities of detecting vulnerabilities, protocol analysis, and assessing threats. This will, in turn, significantly enhance automation by reducing the level of expertise needed to operate these tools effectively.

C. Field-Optimized Design

Future platforms should focus mainly on field operation capabilities, integrating analysis engines, extending battery life, and offering intuitive user interfaces to independently perform security assessments in the field quickly.

D. Standardized Integration

Standardized data formats and protocols for data analysis would allow for easier integration with specialized tools, while still ensuring focused functionality in particular domains is maintained.

VIII. CONCLUSION

This survey provided a review of the modern hardware pentesting tools for IoT security assessment and showed the large gaps existing when it comes to protocol coverage, automation of the testing process, and operational efficiency. The following sections reviewed major existing tools like Flipper Zero, Proxmark3, and HackRF One where it was found that each of them perform excellently within a certain domain while none of them covered all the required capabilities for complete security assessment of Modern IoT devices.

Key findings include the observations of critical protocol coverage fragmentations, that no single tool is able to cover the whole spectrum of wireless technologies employed in the deployment of IoT devices. Automation analysis also reveals that generic tools, in different categories of testing, gain only up to 30-85% automation, while custom solutions are capable of 85-100% automation which points towards immense opportunities for improvement in this zone.

With a high projected market growth rate of 17.1% CAGR by 2033, this indicates very high demand due to large-scale IoT deployments and compliance requirements. But because of limitations within current tools, it sets a hard limit to the best security audit, particularly in organizations needing comprehensive assessment capabilities.

The aims for future research will be the development of integrated platforms or tools supporting multiple wireless protocols and adding artificial intelligence to allow for performing better automation. Field-optimized designs with built-in analysis features would also make hardware security evaluation tools much more usable and functional.

Next-generation integrated platforms represent both the technology challenge and also a great opportunity to enhance IoT security through strengthened assessment techniques and tooling. Success in these challenges will be crucial if the security aspects are to be truly preserved in the always growing IoT ecosystem.

X. ACKNOWLEDGMENTS

The authors are grateful to the Department of Computer Science & Engineering (Cybersecurity) at Dayananda Sagar College of Engineering for immense support and resources provided, which thereby helped them in successfully finishing this survey paper. They thank the community of cybersecurity researchers and open source contributors who has poured in a lot of effort to push the boundaries of hardware security evaluations.

REFERENCES

[1] R. Akyash et al., "Hardware Design and Security Needs Attention: From Survey to Recent Developments," arXiv preprint arXiv:2504.08854v2, 2024.
[2] "Penetration Testing Market Size, Share & Growth Report by 2033," Straits Research, 2023.
[3] A. Smith, "The Top Internet of Things (IoT) Cybersecurity Breaches in 2024," Asimily Blog, Aug. 2024.
[4] "IEEE Paper Format | Template & Guidelines," Scribbr, 2024.
[5] "Penetration Testing Market to Reach USD 6.98 Billion by 2032," Globe Newswire, Aug. 2024.
[6] "The 2024 IoT Security Landscape Report," NETGEAR and Bitdefender, 2024.
[7] "IoT Security Risks: Stats and Trends to Know in 2025," JumpCloud, May 2025.
[8] "Penetration Testing Market Size, Share | Growth Report [2032]," Fortune Business Insights, Oct. 2024.
[9] "IoT Security Risks: Stats and Trends to Know in 2025," JumpCloud, May 2025.
[10] K. Nordnes et al., "IoTective: Automated Penetration Testing for Smart Home Environments," Proc. 9th Int. Conf. Internet of Things, Big Data and Security, 2024, pp. 29-39.
[11] "Global Penetration Testing Market," GM Insights, Apr. 2024.
[12] R. Kaksonen et al., "Automating IoT Security Standard Testing by Common Security Tools," SCITEPRESS, 2024.
[13] S. Rampazzi et al., "RFQuack: A Universal Hardware-Software Toolkit for Wireless Protocol (Security) Analysis and Research," IEEE Security & Privacy, 2021.
[14] J. Smith and A. Johnson, "Revisiting Wireless Cyberattacks on Vehicles," Journal of Automotive Security, 2025.
[15] L. Chen et al., "Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications," ArXiv preprint, Feb. 2024.
[16] "The Ultimate Guide / Cheat Sheet to Flipper Zero," InfoSec Writeups, 2024.
[17] "Hardware Description · Proxmark/proxmark3 Wiki," GitHub, 2018.
[18] "What is the element/component that limits the maximum bandwidth in RX or TX?" HackRF GitHub Issues, 2024.
[19] "Flipper Zero – A Hacking Tool For Geeks and Techies," Craw Security, 2022.
[20] "Proxmark3 - Wikipedia," Wikipedia, 2021.
[21] "HackRF One," HackRF Documentation, 2024.
[22] "Flipper Zero—FCC Report," FCC, 2024.
[23] "Proxmark 3," Proxmark.com, 2024.
[24] "HackRF Pro Q+A," Great Scott Gadgets, 2025.
[25] "Flipper Zero - Lab401," Lab401, 2022.

[26] "RFID hacking preamble: designing an FPGA IIR filter for the proxmark3," fail0verflow, 2013.
[27] "Bandwidth · Issue #101 · greatscottgadgets/hackrf," GitHub, 2014.
[28] "Sub-GHz - Flipper Zero - Documentation," Flipper Documentation, 2023.
[29] "Proxmark 3 Build," Kumari.net, 2024.
[30] "First Experiences With HackRF One—a Review," Elektor Magazine, 2025.
[31] R. Verdult and F. Kooman, "Practical attacks on NFC-enabled cell phones," 3rd International Workshop on Near Field Communication, 2011.
[32] G. P. Hancke, "Practical eavesdropping and skimming attacks on high-frequency RFID tokens," Journal of Computer Security, vol. 19, no. 2, pp. 259-288, 2011.
[33] D. Oswald and C. Paar, "Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World," Cryptographic Hardware and Embedded Systems, 2011.
[34] T. Eisenbarth et al., "On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme," Annual Cryptology Conference, 2008.
[35] M. Schneider et al., "Cryptanalysis of the KEELOQ block cipher," Cryptology ePrint Archive, 2007.