RF Exploitation and Detection Techniques using Software Defined Radio: A Survey

Martin Pozniak, Debanjan Sadhukhan, Prakash Ranganathan
School of Electrical Engineering & Computer Science
University of North Dakota, Grand Forks, ND, USA

***Abstract*— In order to mitigate the attacks involved in Radio Frequency (RF), various security techniques are developed in the literature. However, from replay attacks which can steal a car, to GPS attacks tricking vehicles into changing course, there are many threats that still exist today. With advancement of the technology, the vulnerabilities in RF also increases. The reverse engineering technique of wireless signals allows attackers to create dangerous new attacks every day. This paper provides a brief survey of various attack methodologies using software defined radio (SDR) and discusses common threats and defenses in detail.**

Keywords: Software Defined Radio, Reverse Engineering, Radio Frequency Exploitation

I. Introduction

The radio frequency (RF) wireless communication has become an integral part of human life, from browsing the internet using Wi-Fi, to controlling aircraft navigation in the sky. The application set of RF technology includes satellite communication, industrial automation, telecommunications, wireless power transmission, IoT, RADAR communication, medicine, intelligent transport systems and many more [1]. The wireless communication opens the door for malicious actors to take advantage of the technology. Through careful analysis of the frequency spectrum, attackers can gain insight into the wireless communicating devices. Software defined radio (SDR) devices are used to create a versatile platform to analyze the RF spectrum by implementing the radio functions through software as opposed to hardware. This allows SDRs to perform more operations on a broader frequency range than typical radios.

The attackers can capture a signal between a target source and its intended destination. An attacker can also produce radio signals masked to appear as if from a legitimate source. Since there is no efficient way to prevent attackers from intercepting or producing signals, developers of wireless systems must gain the knowledge of various attacks and build robust systems that can defend these threats. This paper analyses the capabilities of SDR, the methodologies used by attackers to exploit wireless systems, and the emerging defenses available to wireless systems in various applications such as industrial automation, Internet of Things (IoT) and unmanned aircraft systems (UAVs) [2], [3].

A. Contribution

The significance of this paper lies in its comprehensive summary of current attack vectors, and methodologies used to exploit radio frequency systems. Several papers appeared in the literature focusing on one specific attack type and details about specific methodologies. However, limited papers discuses about the comprehensive overview of various RF exploitation techniques and their mitigation. This paper provides a well written, concise survey outlining the most common attacks that exploit the RF systems. This paper also discusses about the main tools used by attackers, the common exploitation methodologies, and the common defenses against such exploitation attempts.

B. Software Defined Radio

SDRs are devices that implement radio functions such as transmitting and receiving signals, through software instead of hardware. This makes SDRs extremely versatile tools to perform analysis on the frequency spectrum and also allows for programmers to use software to create cracking tools [4]. The SDR receiver uses an antenna to receive an analog signal which is amplified and sent to an analog to digital converter (ADC) to convert into a digital signal, and can be processed by a processor for the use by a software application. Similarly, the SDR transmitter converts a digital signal produced by the software using a digital to analog converter (DAC) and sends the converted signal through the antenna as an analog signal [5]. Fig. 1 shows a graphical representation of SDR hardware architecture. The SDR devices range from $20 devices that operate with a small frequency range/bandwidth that only support simplex communication, to devices such as the per vices crimson nearing $7,000 capable of full duplex communication and a frequency range from DC6GHz and 1200MHz of bandwidth (refer Table1). A few of the free SDR programs that are commonly used with SDRs are listed in Table 2.

SDR	Frequency Range	Band-width	Commu-nication
R820T RTL2832U	24MHz-1.766GHz	3.2MHz	Simplex RX
Airspy R2	24MHz-1.75GHz	10MHz	Simplex RX
HackRF One	1MHz-6GHz	20MHz	Half Duplex
BladeRF	300MHz-3.8GHz	28MHz	Full Duplex
Per Vices Crimson	DC-6GHz DC-6GHz	1200MHz	Full Duplex

Table 1. Various types of SDRs

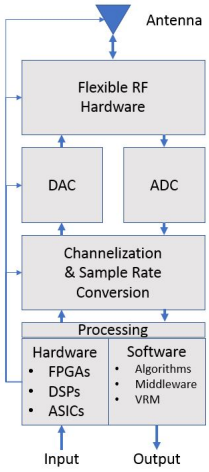

Fig. 1. Operational block diagram of SDR

Software Name	Supported OS
GQRX	Linux / MAC OS
SDR Touch	Android
GNU Radio	Linux/MAC/Windows
SDR Console	Windows

Table 2. Supporting softwares for SDR

Section II discusses the various attack vectors used to exploit wireless systems, and also provides a technical insight into the methodologies carried out for these attacks. The paper concludes in section III.

II. Exploit Methodologies

In this section, we discuss about each attack by providing the definition of the attack as well as a method to perform the attack using SDR and open source software. Defenses, and their drawbacks, to each attack that have been theorized or implemented are discussed. Each methodology follows the assumption that the attacker does not have any prior knowledge on the system that is being exploited.

Before any attack can be carried out, a thorough information gathering phase must be completed on the target. Some attacks require more information than others however each attack starts by gathering information on the target system. This information can be determined in several ways. One way to get the information as follows. In the United States, the Federal Communication Commission (FCC) requires all devices that transmit RF waves be registered with a visible ID and adhere to strict operating constraints. If someone gains physical access to the device or a similar device, the public FCC database can help determine much more information about the device. If physical access is difficult to gain for the device, similar information can be retrieved from the operational frequency range of the device, as determined by the National Telecommunications and Information Administration (NTIA). The complete allocation of the frequency spectrum can be found in [7].

From the chart provided by the NTIA an attacker can narrow down the frequency ranges that the targeted device may operate on, and in turn listen on each of the frequencies for the target device to transmit a signal. From there, the attacker can move on to other attacks. For example an attacker can listen on the cellular communication frequencies and intercept phone conversations, albeit this would take some work, to gain even more information about a target.

There are many papers written on the topic of reverse engineering. The coverage on the topic is limited in this paper to provide enough information to give an understanding of how it is used to exploit systems for information that can be used in later attacks using SDR. For information gathering, reverse engineering consists of identifying the device technology, extracting a device and gate-level netlist of integrated circuits (ICs) and inferring IC functionality using a logic analyser or data-sheet if available [8]. Information about a device can be reverse engineered through several methods described in detail in [8] and [9]. Counterfeiting a device is the process of reverse engineering the functionality of ICs closely enough to the authentic IC that it is indistinguishable at first use. Counterfeiting causes many problems in industry by creating devices that degrade faster than usual over time and undercutting genuine businesses by selling counterfeited devices at a cheaper price. Side-channel attacks are another method of reverse engineering that use physical properties of electronics to gain information about a device such as power usage and timing of logic operations. Differential power analysis (DPA) uses traces of power usage over time to discern encryption schemes or keys used to encrypt data on a hardware level. DPA is discussed at length in [10]. [20] discusses the use of digital image processing to reverse engineer ICs. All these methodologies can be combined with modern machine learning techniques to rapidly determine the functionality of hardware components. Interestingly, [22] proposes a novel method for automating printed circuit board (PCB) reverse engineering using machine learning and online resources. These techniques allow attackers to gain extreme insight into the inner workings of a device. For the attacks described below it is assumed the attacker has performed sufficient information gathering and reverse engineering to attain the prerequisite information required for the attack.

A. Reverse Engineering Signals

Reverse engineering (RE) using SDR is possible through software that allows attackers to visualize signals and perform signal processing on them. The standard method for reverse engineering signals follows 2 main steps, record and process. The recording step requires the attackers to have completed enough information gathering to determine the approximate operating frequency of the target transmitter. The attacker must also have supporting SDR hardware that can intercept the signal to reverse engineer. Processing the signal is more challenging. There are many methods used today for conveying data through wireless analog signals as well as many ways of encrypting that data in transit. However, attackers that can capture a signal can at the very least determine the signals modulation scheme which is the first step to more attacks.

Modulation is the method of altering properties such as

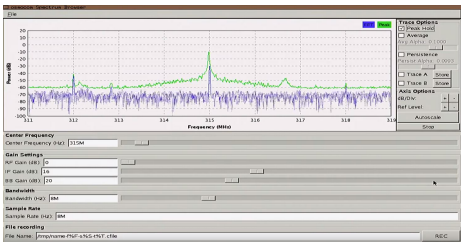

Fig. 2. Osmocom FFT readout of captured signal near 315MHz [12]

amplitude, frequency, or phase of analog signals in such a way that they can communicate meaningful information. Free software such as Audacity is a waveform editor that allows users to visualize and manipulate wave-forms like those that are generated by SDR. This software is typically only useful if the signal is already demodulated properly. There is also software like Inspectrum or Gnu Radio that allows for the signal processing of raw modulated signals which allow for a more extensive analysis to be performed.

Once an attacker has properly processed the signal, they can take the data and use mathematical or statistical methods to decrypt, decode, or otherwise determine meaningful information from the transmitted signal.

1) Execution: As discussed above the first step to reverse engineering a signal is to listen for and record the targeted signal. Osmocom FFT is used to visualize and record the captured signal. As shown in Fig. 2 the blue line represents current ambient noise as the antenna listens for a signal while the green line represents the historical peak of any signals that have been heard. In this case, Fig. 2 shows Osmocom FFT successfully recorded data from a powerful signal near 315MHz which it saved to a file to be analysed later [12]. The signal captured is a massive accumulation of raw modulated signal information that is infeasible to analyse by hand. Therefore, another software tool called Inspectrum is used to replay and visualize the captured signal over and over so that the attacker can perform a variety of techniques to discover modulation schemes which once known are used to demodulate the signal into its true data.

Today, there are many modulation schemes used to encode data in what is known as a carrier signal, which is the signal that carries the modulated data through the air. The simplest of these schemes is on-off keying (OOK) or amplitude shift keying (ASK). These modulation schemes mimic the well-known binary pattern of 0 or 1 by transmitting either on or off for particular time periods. This on off transmission creates a visible pattern that can be seen in tools like Inspectrum which attackers use to determine the binary equivalent of the signal. In the case of this example, pulse width modulation on off keying (PWM OOK) is used to transmit data. This can be seen below where the short bursts of signals over a three time unit section represent binary 100 (on-off-off) and the longer bursts represent binary 110 (on-on-off).

This is where things become interesting for reverse engineers, now the attacker has actionable data that they can use to determine encryption types or plain text codes if the signal is transmitting simple codes. From the Inspectrum output the attacker can determine the bitrate, frequency and modulation scheme. This can be used in conjunction with other tools such to decode further the data. Using SDR reverse engineering signals is a tried and true process that is effective in decoding private information right out of the air.

2) Defenses: One of the most important concerns when creating a cyber-physical system is protecting it from being reverse engineered on a hardware level. Strong protection against RE makes it exponentially harder for attackers to reverse engineer systems using only information they can gain externally. There are many techniques used to protect against reverse engineering attacks. [9] discusses physical unclonable functions (PUFs) as a measure for protecting devices from reverse engineering. As stated in [9] PUFs significantly increase physical security by generating volatile secrets that only exist in a digital form when a chip is powered on and running. This immediately requires the adversary to mount an attack while the IC is running and using the secret, a significantly harder proposition than discovering non-volatile keys. Another powerful method of hardware security is camouflaging which involves using gates and other hardware that do not directly impact the functionality of the device, therefor hiding the true hardware that controls the functionality. Watermarking and finger printing are used to embed the designers signature into the hardware making it possible to easily determine if a device is counterfeit. To prevent DPA attacks noise injection and leakage reduction techniques are used to mask the power consumption truly being used by a device. Detailed descriptions of these and more attacks are found in [8], [9], [10]. Rolling codes as discussed in the next section can help mitigate the effectiveness of reverse engineering attacks. If an attacker can reverse engineer the method used to encrypt the data but cant feasibly carry out a decryption attack, his efforts are wasted. Besides rolling codes other methods such as timing constraints and other added security measures can be implemented in systems that prevent the usefulness of the data gathered through reverse engineering a signal. Finally, [21], [6], [22], [23] discuss unique techniques used to mask circuitry, detect and mitigate reverse engineering threats.

B. Replay Attacks

Replay attacks are the most common RF attack to carry out. As the name indicates, a replay attack is performed by replaying a captured RF signal to a targeted receiver. Replay attacks can be used to unlock doors, open home garages or even take control of a remote-controlled device. Replay attacks do not require extensive knowledge of the target device or the signal being propagated. The only information necessary to perform a replay attack is the approximate frequency the target device operates on.

After determining the devices operating frequency using the information gathering techniques discussed above the attacker can replay the captured signal at an appropriate amplitude. If the receiver does not use advanced security measures, the receiver will interpret the signal and the

attacker successfully imitates a valid signal and comprises the target.

1) Execution: Using GRC on a Linux operating system it is possible to conduct a replay attack. Firstly, a program is written to intercept a signal on a specified frequency. Secondly, the intercepted signal behaviour is saved to a file that can be modified and interpreted by GRC. The attacker at this stage can use GRC to process the signal and determine the modulation scheme and otherwise reverse engineer the signal, however this is unnecessary for replay attacks. Thirdly, the attacker creates a program in GRC that is used to transmit the recorded signal after increasing the amplitude sufficiently for the receiver of the target to accept. To refine this attack, GRC can be used to filter or otherwise modify the signal to produce a cleaner and more reliable transmission.

2) Defenses: [24] presents a comparative analysis of authentication and access control protocols against a variety of wireless attacks including replay attacks. [25] proposes a design for a intrusion detection system to identify the existence of such wireless attacks. One of the primary lines of defense against replay attacks are rolling codes. Rolling codes are shared codes used by the transmitter and receiver that act as a shared key. The receiver only responds to signals that transmit with the shared key. The strength of rolling codes is that this shared key rolls or changes after every transmission and past codes are not accepted by the receiver [11]. That means if an attacker manages to sniff a signal, he/she can replay the signal, however the receiver will not accept the code. One major flaw exists with rolling codes and that is that the receiver will accept future codes. This is necessary in the event for example a user tries to unlock their vehicle out of range of the receiver. The transmitter will move onto the next shared key however the receiver will not. Therefore, to prevent users from being locked out of their vehicles the receiver must accept a certain number of future keys.

Sammy Kamkar, a prominent security researcher devised a clever method of defeating rolling codes based on this information. The method combines a jamming attack with a replay attack to defeat rolling codes. The exploit begins by first jamming a signal on the frequency the target is transmitting. The attacker jams and saves the received signal. The user will most likely send a second signal, with a future shared key, to the receiver in a second attempt to unlock the vehicle. Since the receiver has not heard the first signal it will still accept the first signal the user sent so the attacker replays that signal, emulating that it was the users second key press that unlocked the vehicle. The vehicle unlocks, and the target is happy and unaware what had happened. However, now the attacker has a future code that he can us to unlock the car later. This clever method uses a combination of attacks to complete the exploit of a wireless system. One defense against this attack that can be used as devices become more powerful is a two-way challenge response so that the receiver can verify with the key that it indeed sent the signal. If the attacker sent a future signal the key would not respond or respond with a false response, and the vehicle would remain locked.

If an attacker cannot capture a signal from a target, they may result to brute force attacks to achieve their goals. While not as sophisticated or fast, brute force attacks can be effective in trying each key within a key space. The most common defense for brute force attacks is using larger key spaces which can significantly increase the time it takes for an attacker to try every code. Another effective brute force defense method is requiring a preamble or sync word at the beginning of each key to prevent attackers from utilizing mathematical discoveries such as the De Bruijn sequence to rapidly try thousands of keys in less time.

C. Jamming Attacks

Similar to denial of service (DoS) attacks targeted at computer networks, RF jamming attacks use SDR to transmit noise at any targeted frequency or range of frequencies for the intended purpose of blocking a receiver from receiving an expected signal. This attack is not elegant however it is effective and is often used in combination with other attacks such as the replay attack. Jamming attacks can be used to block critical communication between systems that rely on communication for proper operation such as air traffic control and aircraft. The jamming attack can be used to jam GPS of UAVs, if the UAV does not have other onboard means for navigation the UAV can be hijacked or brought down. [26] details some jamming techniques sand defenses in wireless local area networks.

1) Execution: The most complex part of a jamming attack is obtaining the required hardware to execute the attack. Sufficient hardware that produces enough noise at a given frequency to jam a signal from a reasonable distance is challenging. Powerful amplifiers are needed to propagate the signal. Executing a jamming attack using GRC is simple by sending a powerfully amplified signal at a desired frequency. The attack can be done using slightly modified code to send the signal. Jamming attacks are risky for attackers because they are easily detected. As soon as excessive noise is detected on an RF frequency specialized tools such as signal strength meters can be used to localize the source of the jam and the attacker can be located. Therefore, powerful equipment is needed so the attacker can surmount an attack from safe distances. However, in most non-critical applications these special tools are not available and so there must be methods to continue transmission in the event of a jam.

2) Defenses: One defense to be used is secondary antennas that operate on variable frequencies in case of a jam. While performance of information transfer may be degraded, critical safety information can still be transmitted. This defense adds cost and infrastructure to the system. The use of proprietary dynamic reconfiguration schemes are popular in military applications [13]. Using focused directional antennas can help mitigate jamming attacks since the attacker may not know the specific configuration of the target antenna and the target receiver rejects any miss aligned signals. Overall,

jamming attacks are difficult to prevent and defend against, therefore, having alternative methods for communication in the event of a jam is critical for safety and continued operation of a wireless system.

D. GPS Spoofing

Global Positioning System (GPS) spoofing attacks target the unencrypted unauthenticated GPS signals sent by satellites to any device that is GPS enabled. It works by first matching the GPS signal a device receives and then slowly increasing the amplitude of the spoofed GPS signal until the device begins to respond to the new GPS transmission believing it is the legitimate source. Once the device begins to respond to the spoofed GPS signal the attacker can redirect autonomous vehicles [14] to their desired location or purposefully land or crash vehicles. GPS spoofing attacks typically target marine vehicles and aircraft since the spoofed trajectory can go unnoticed for a long time if not properly monitored by the vehicle operator.

1) Execution: [16] Uses cheap SDR hardware and software to spoof the GPS route of road vehicles. [17] Demonstrates how researchers at U.T. Austin used GPS spoofing attacks to misdirect an $80M marine vessel off its intended course. Executing a GPS spoofing is possible with SDR and open source software designed to perform the attack such as GPS-SDR-Sim, a software developed by Takuji Ebinuma [17]. Using this software, the SDR transmits a signal on the typical GPS frequencies such as 1575.2MHz. Since GPS signals received on earth sent from satellites in space are very weak from their long transmission, overpowering them and taking control of a GPS enabled device is easy with the typical transmitting power of most SDRs. Once a lock is established the attack is complete and the attacker can use the software to produce fraudulent GPS routes or modify the behaviour of the spoofed device in any way they see fit.

2) Defenses: GPS spoofing attacks are difficult to detect unless there are some authentication or monitoring methods on board the GPS enabled device. There is still much ongoing research on defenses against GPS spoofing attacks. Current methods for detecting GPS spoofing attacks include using some 3rd party authority that can verify the information that a device is receiving. This 3rd party can be a server containing information that is secret to valid satellite communication and the targeted device [18]. The Department of Homeland Security recommends measures that help defend against GPS spoofing and related attacks. Safeguards include obscuring antennas or installing decoy antennas to throw off attackers, adding sensors that can detect spoofing signals and send alerts to remote monitoring sites, and installing several antennas in different locations, which allow personnel to monitor for GPS discrepancies and other indicators of an attack [18]. More expensive but powerful solutions is to change the way GPS transmissions and receivers operate to have authentication methods in place to verify legitimate signals such as encryption. With the rapid development of computer vision technologies, new methods are emerging for protection against GPS spoofing. If the targeted device is travelling over land, or any area with visible landmarks, computer vision can be used to supplement GPS signals and verify a vehicles position. Also, other RF sources are used such as Wi-Fi to supplement GPS and improve the accuracy and validity of the GPS signal similarly to how some typical smartphones operate. [20] discusses using wireless signals typically present in urban environments which can provide navigation queues for UAVs in GPS weak or disabled environments.

E. Misdirection Attacks

Misdirection attacks use one or more of the above attacks to distract or divert attention away from the attackers true target. For example, a misdirection can be used to block a RADAR station in order to divert resources and employee attention to one area while the attacker makes a move on another target while people are distracted. The target can also use this attack as a piece of a social engineering attack. Social engineering is the art of exploiting security through human factors by manipulating people and using psychology to trick them into believing a ruse [14]. For example, an attacker can use a jamming attack to interfere with a system and then enter an organization claiming to be the repair technician who needs access to critical resources to fix the problem.

1) Execution: The execution of this attack will use the example of an attacker targeting a hospital. Using reverse engineering, an attacker can determine the frequency and requirements that activate alarms that alert nurses and doctors that a patient requires assistance. With enough time and preparation an attacker can use SDR in the same ways as discussed earlier to transmit the signals to activate various alarms. While the hospital staff is scrambling to deal with all the false alarms the attacker can use social engineering during the frenzy to attack his true target.

2) Defenses: Awareness is the first line of defense against misdirection attacks. Training employees about the common methods used by attackers and social engineers to comprise businesses and organizations is critical. Always checking for proper credentials and ensuring secured resources are under surveillance is necessary. Training staff that through social engineering, attackers can accumulate a lot of information about a system by gathering small bits of information from different sources. Always keeping a weather eye out for suspicious activity and having protocols to follow in the case of emergencies can help prevent misdirection attacks from being successful. Table 3 summarizes attacks and their defenses.

III. Conclusion

The invention and wide adoption of the wireless technologies made more difficult on manufactures and security researchers to ensure system safety and reliability. This paper discussed reverse engineering, replay attacks, signal jamming, GPS spoofing, and misdirection attacks. These attacks can be used to compromise the security of industrial control systems, domestic homes and property, transportation

Attack	Defences
Reverse [9], [10], [22], [23] Engineering [21], [6], [8]	1.Physically secure hardware 2. Implement hardware obfuscation techniques 3. Use supplemental security measures
Replay [11], [24], [25]	1. Use rolling codes 2. Verify timing 3. Use longer keys 4. Require preamble/sync word
Signal Jamming [13], [26]	1.Use dummy antenna 2. Have backup infrastructure 3.Use directional antennas 4. Use shielded cabling
GPS Spoofing [16], [17] [18], [20]	1. Utlilize onboard GPS monitoring systems 2. Use 3rd party verification tools 3. Use encrypted GPS transmission 4. Use visual landmark recognition 5. Use urban signals for verification 6. Position correlation with RTK
Misdirection [14]	1. Personnel Awareness 2. Social Engineering Training 3. Having protocol to follow 4. Staying alert 5. Preventing the attack in the first place using the above attack defenses

Table 3. Attacks and their defenses

systems and more. A thorough survey of the attack methodologies and the defenses against these attacks are provided. This survey provides the opportunity for security researchers to innovate new methods to secure cyber-space from new emerging threats.

REFERENCES

[1] Agarwal, T. (2018).Different Types of Wireless Communication Technologies. [online] Edgefx.in. Available at: https://www.edgefx.in/different-types-wireless-communication-technologies.

[2] El Mrabet, Zakaria, et al. "Primary User Emulation Attacks: A Detection Technique Based on Kalman Filter." Journal of Sensor and Actuator Networks 7.3 (2018): 26.

[3] El Mrabet, Zakaria, et al. "Cyber-security in smart grid: Survey and challenges." Computers & Electrical Engineering 67 (2018): 469-482.

[4] R. Chvez-Santiago, A. Mateska, K. Chomu, L. Gavrilovska and I. Balasingham, "Applications of software-defined radio (SDR) technology in hospital environments," 2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Osaka, 2013, pp. 1266-1269.

[5] Keim, R. (2017). "Introduction to Software-Defined Radio." [online] Available at: https://www.allaboutcircuits.com/technical-articles/introduction-to-software-defined-radio

[6] Xiao, K., Forte, D., Jin, Y., Karri, R., Bhunia, S., & Tehranipoor, M. (2016). Hardware Trojans: Lessons learned after one decade of research. ACM Transactions on Design Automation of Electronic Systems (TODAES), 22(1), 6.

[7] United States Frequency Allocations. (2016). [PDF] Washington DC: National Telecommunications and Information Administration. Available at: https://www.ntia.doc.gov/files/ntia/publications/january_2016_spectrum_wall_chart.pdf

[8] M. Rostami, F. Koushanfar and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1283-1295, Aug. 2014.

[9] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," 2007 44th ACM/IEEE Design Automation Conference, San Diego, CA, 2007, pp. 9-14.

[10] Kocher, Paul, Joshua Jaffe, and Benjamin Jun. "Differential power analysis." Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1999.

[11] George, P. "Can other people unlock my car door with their remote?" [online] Available at: https://electronics.howstuffworks.com/gadgets/automotive/unlock-car-door-remote1.htm

[12] Stolnikov, D., et al. GrOsmoSDR. http://sdr.osmocom.org/trac/wiki/GrOsmoSDR

[13] Digikey.com. (2015). "Jamming and Anti-Jamming Technologies for RF Links" [online] Available at: https://www.digikey.com/en/articles/techzone/2015/sep/jamming-and-anti-jamming-technologies-for-rf-links

[14] Hulme, G. and Goodchild, J. (2017). "What is social engineering? How criminals take advantage of human behavior." [online] Available at: https://www.csoonline.com/article/2124681/social-engineering/what-is-social-engineering.html

[15] S. King, et. al. "Designing and implementing malicious hardware" (2008) [PDF] Available at: https://www.usenix.org/legacy/event/leet08/tech/full-papers/king/king.pdf

[16] Zeng, K. "All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems." [E-Book] Available at: https://people.cs.vt.edu/gangwang/sec18-gps.pdf

[17] rtl-sdr.com. (2016). "Cheating at Pokmon Go with a HackRF and GPS Spoofing." [online] Available at: https://www.rtl-sdr.com/cheating-at-pokemon-go-with-a-hackrf-and-gps-spoofing/

[18] Phys.org. (2018). "New defenses sought against GPS spoofing attacks." [online] Available at: https://phys.org/news/2018-01-defenses-sought-gps-spoofing.html

[19] Janofsky, A. (2018). "How to Defend Against GPS Spoofing Attacks." [online]Available at: https://www.wsj.com/articles/how-to-defend-against-gps-spoofing-attacks-1537306495

[20] Kapoor, Rohan, et al. "UAV Navigation using Signals of Opportunity in Urban Environments: A Review." Energy Procedia 110 (2017): 377-383.

[21] Winograd, Theodore, et al. "Hybrid STT-CMOS designs for reverse-engineering prevention." Proceedings of the 53rd Annual Design Automation Conference. ACM, 2016.

[22] Kleber, S., Nlscher, H. F., & Kargl, F. (2017). Automated PCB Reverse Engineering. In 11th USENIX Workshop on Offensive Technologies (WOOT 17).

[23] Cocchi, Ronald P., et al. "Circuit camouflage integration for hardware IP protection." Proceedings of the 51st Annual Design Automation Conference. ACM, 2014.

[24] V. Mittal, S. Gupta, T. Choundhury, "Comparative Analysis of Authentication and Access Control Protocols Against Malicious Attacks in Wireless Sensor Networks" (2017) [E-Book]

[25] A. W. Al-Dabbagh, Y. Li and T. Chen, "An Intrusion Detection System for Cyber Attacks in Wireless Networked Control Systems," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 65, no. 8, pp. 1049-1053, Aug. 2018.

[26] W. Chen, D. Chen, G. Sun, Y. Zhang, "Defending Against Jamming Attacks in Wireless Local Area Networks" (2007)