IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 2, February 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|| A Monthly Peer Reviewed & Referred Journal |

||Volume 11, Issue 2, February 2022||

|DOI:10.15680/IJIRSET.2022.1102136|

Comprehensive Survey of Threats, Cyberattacks, and Enhanced Countermeasures in RFID Technology

Ujas Bhadani

Cybersecurity Expert, Northeastern University, Boston MA, United States

ABSTRACT: Various sectors, such as healthcare, retail, supply chain management, and security, have been transformed by Radio Frequency Identification (RFID) technology. Nevertheless, its pervasive adoption has also rendered it an ideal target for a variety of cyber threats and attacks. The security challenges and vulnerabilities associated with RFID technology are comprehensively examined in this article, which also delineates the nature of common assaults, including surveillance, cloning, relay attacks, and denial-of-service (DoS) attacks. A comprehensive survey is provided. Additionally, it investigates the development of new countermeasures that are intended to mitigate these threats, such as secure communication frameworks, cryptographic protocols, and authentication mechanisms. The objective of this survey is to facilitate the development of more secure and resilient RFID applications in critical domains by assessing the current state of RFID security and suggesting future directions for improving system robustness.

KEYWORDS: RFID Security, Privacy and Data Integrity in RFID, Intrusion Detection, DoS, DDoS

I. INTRODUCTION

RFID technology has revolutionized a variety of industries by facilitating the efficient monitoring, data administration, and automation of various processes. RFID systems have emerged as an indispensable element of contemporary infrastructure, spanning from supply chain logistics and retail to healthcare and transportation. Nevertheless, the risk landscape has expanded substantially as a result of the increasing adoption of RFID technology. RFID communication's inherent wireless nature introduces a wide range of security vulnerabilities, such as data manipulation, replication, unauthorized access, and espionage. This paper provides a thorough examination of the current and potential threats to RFID technology, with a particular emphasis on the vulnerabilities that cybercriminals exploit to execute sophisticated attacks. The analysis investigates the effects of a variety of attack vectors, including replay attacks, Denial of Service (DoS), and man-in-the-middle (MITM) attacks, on system availability, data integrity, and privacy. Furthermore, this investigation assesses sophisticated countermeasures that are explicitly engineered to mitigate these security concerns, such as intrusion detection systems, authentication protocols, and encryption techniques that are optimized for RFID environments. The robust solutions to improve the resilience of RFID systems against evolving cyber threats and identify critical voids in existing security frameworks through this in-depth exploration. The objective of this survey is to serve as a valuable resource for researchers and practitioners, thereby facilitating the secure implementation and deployment of RFID technology.

II. THREATS AND ATTACKS

RFID (Radio Frequency Identification) systems are widely used computing technologies, offering both technological and commercial potential in a wide range of applications. Their minimal cost and extensive applicability are among their advantages. Although RFID systems have a lot of potential for innovation and automation, they also come with several built-in weaknesses. RFID systems are vulnerable to a broad range of malicious threats, including active interference and passive eavesdropping [2]. Simple RFID tags, for instance, can be read without permission, making the items of a handbag or shopping cart accessible to infringers without leaving a trace. This section provides a structural methodology for threats that RFID networks encounter by classifying RFID assaults, outlining their key characteristics, and presenting potential countermeasures.

Threat models are required for effective risk management. In this section, we will cover the most frequent RFID attacks (like, but different from, OSI protocol layering), identifying the vulnerabilities and proposing potential

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|| A Monthly Peer Reviewed & Referred Journal |

||Volume 11, Issue 2, February 2022||

|DOI:10.15680/IJIRSET.2022.1102136|

countermeasures for each layer. We differentiate (Fig. 3) between single-layer attacks that target a single layer and multilayer assaults that target many layers [2]. Single-layer attacks include those that are deployed in the physical layer, network-transport layer, application layer, and strategic layer.

Cost Vs Utility tradeoffs	Logistical Factors	Real-world Constraints	Strategic layer
EPCIS/ONS	Oracle/SAP	Commercial enterprise middleware	Application layer
ISO 15693/14443	EPC 800 Gen-2	Proprietary RFID protocols	Network-Transport layer
RF	Reader HW	RFID Tags	Physical layer

Fig. 1. Layers of RFID communication

Attacks on the radio frequency (RF) signals as well as physical devices like readers and tags are included in the physical layer. We discuss attacks that take advantage of RFID protocols featured in standards like ISO 15693/14443, the EPC 800 Gen-2, or other proprietary protocols on the network-transport layer. At the application layer, we include attacks that target vulnerabilities in commercial enterprise middleware and applications such as Oracle, SAP, the Object Name Service (ONS), or the EPCIS. Finally, attacks based on logistical constraints, real-world limitations, and cost versus utility trade-offs are included in the strategic layer. More specifically, this layer includes targeted and privacy-related security risks as well as attacks that rely on company secrets and crucial information linked to production, organization, and expansion policies used in competitive business environments. Furthermore, we have created a distinct category for multiple layers attacks that exploit vulnerabilities in multiple layers. The Detailed categorization is shown in Fig. 2.

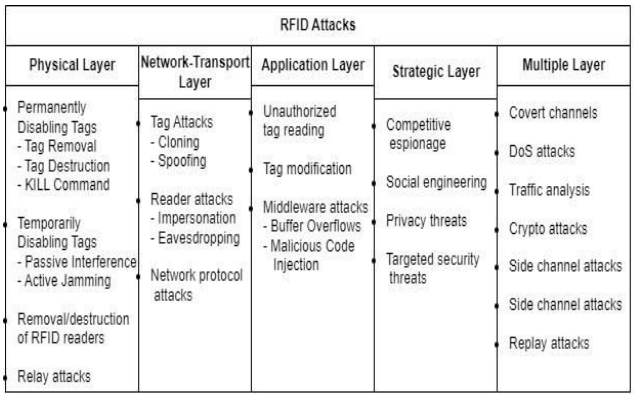

Fig. 2. Frequency allocation of the RFID

A. Physical Layer

In RFID communications, the physical layer consists of the physical interface, radio signals, and RFID devices. The attacker in this layer takes advantage of RFID communication's wireless characteristics, lack of physical security, and vulnerability to physical manipulation [2]. This layer covers attacks that disable RFID tags permanently or temporarily, as well as relay attacks.

- *Permanently disabling tags*: Permanent RFID tag disablement includes all potential hazards or threats that could result in the complete destruction or significantly reduced performance of an RFID tag. Physical Tag Removal or Tag Destruction are two methods for making an RFID tag permanently dysfunctional. Furthermore, privacy-related countermeasures such as the KILL Command [3] might be manipulated to achieve the same result.
- *Temporarily disabling tags*: A temporary disablement of an RFID tag is still a possibility, even if it avoids the threat of permanent disablement. A potential thief can use a Faraday cage, such as a bag coated with aluminium foil, to protect their target from electromagnetic waves (like those from the checkout reader) and steal anything

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|| A Monthly Peer Reviewed & Referred Journal |

||Volume 11, Issue 2, February 2022||

|DOI:10.15680/IJIRSET.2022.1102136|

they want unnoticed [4]. RFID tags may unintentionally get temporarily disabled due to environmental factors (e.g., a tag covered with ice). The temporary deactivation of tags may also be caused by passive radio interference and active jamming.

- *Removal or destruction of RFID readers*: RFID readers can also be destroyed or stolen, even though the small size of RFID tags makes them more vulnerable to physical attacks. RFID scanners are vulnerable to theft, especially if they are left unattended. A malevolent intruder may attack an RFID reader that contains vital information like the cryptographic credentials (i.e., keys) required to access tags. The consequences of an RFID reader loss are significant since malicious attackers may be able to access not only RFID tags but also the back-end system, which they could also modify to facilitate more data manipulation.
- *Relay attacks*: An attacker stands as the man-in-the middle in a relay attack. The legitimate RFID tag and reader are secretly separated by an adverse device in this type of attack. The radio transmission between a valid tag and reader can be intercepted and altered by this device. The hostile device then relays an ephemeral connection to the legitimate tag/reader from the legitimate tag/reader [4]. The genuine tag and reader are led to believe that they are speaking with one another directly. Separate devices, one for communication with the reader and one for communication with the RFID tag, might be utilized to make this kind of attack even more sophisticated.

B. Network—Transport layer

This layer contains all attacks that are focused on how RFID systems communicate and transfer data among their constituent components (tags and readers). In this section, we categorize attacks on the network transport layer into three categories: tag attacks, reader attacks, and network protocol attacks.

- Tag attacks: RFID systems are vulnerable to attacks even with their most significant and distinguishing feature their unique identifier. Given the widespread availability of writing and reprogrammable tags, reproducing RFID tags does not need a lot of money or experience, even though, in theory, you cannot ask an RFID manufacturer to generate a clone of an RFID tag 5. Cloning simply involves copying the ID and any associated data from the original RFID tag to the clone tag if it lacks security measures. However, if the tag incorporates additional security characteristics, the attacker will need to carry out a more complex attack such that the reader will mistakenly accept the rogue clone tag as a legitimate one. Cloning leads to the circulation of identical tags, a lack of clarity regarding the associated tagged objects, and a breach of the system's integrity.

Spoofing is a type of cloning that does not physically duplicate an RFID tag. Attackers use specialized equipment with expanded capability that can simulate RFID tags given specific data content to perform spoofing. An attacker impersonates a legitimate RFID tag in this kind of attack to obtain its rights.

- Reader attacks: Given that RFID transmission is frequently unauthenticated, adversaries could simply impersonate a legitimate reader to obtain sensitive information or change data on RFID tags. The effectiveness of these assaults varies from "practically impossible" to "extremely trivial", depending on the security measures used to authenticate the RFID reader. If credentials are kept on the reader, for instance, a stolen reader may reveal the details needed to access RFID tags and back-end systems.

Eavesdropping is one of the most severe and frequently exploited threats to RFID systems due to its wireless nature. Eavesdropping is the act of listening in on communications between authorized RFID tags and readers using an antenna [6]. In both reader-to-tag and tag-to-reader attacks, this kind of action is possible. In contrast to tags, which broadcast information at considerably lower power, readers communicate information at much higher power, making them more vulnerable to attacks of this type over a wider range of distances.

- Network protocol attacks: RFID systems are usually integrated with a company's backend databases and networking devices. However, these devices have the same security flaws as general-purpose networking equipment. Malicious attackers can launch attacks and compromise the back-end infrastructure by exploiting flaws in the network protocols and operating systems that are in use.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|| A Monthly Peer Reviewed & Referred Journal |

||Volume 11, Issue 2, February 2022||

|DOI:10.15680/IJIRSET.2022.1102136|

C. Application layer

This layer contains all the attacks that target data about applications and the connection between users and RFID tags. Attacks in the application layer make use of unauthorized tag reading, tag data modification, and application middleware attacks.

- *Unauthorized tag reading*: Unlike many electrical items, RFID tags do not include an on/off switch. Additionally, not all RFID tags provide protocols for authenticated read operations. As a result, adversaries can read RFID tags' contents very easily and quietly. However, because such attacks necessitate being in close contact with the RFID tag, their scope is relatively limited.
- *Tag modification*: Most RFID tags in use today include user-writeable memory, which an attacker can take advantage of to change or remove important data. It is important to note that the use of the RFID standard and the READ/WRITE protection have a significant impact on how easily such an attack can be carried out. In more advanced and specific cyberattacks, data may be manipulated while maintaining the tag ID and any security related information (such as keys or credentials). As a result, while crucial information may have been fabricated, the reader would be persuaded to believe that it is interacting with an unmodified tag.
- *Middleware attacks*: Buffer overflows is one of the major vulnerabilities and most challenging software security issue. In a buffer overflow, it exploits storing data or code outside the boundaries of a fixed-length buffer. Buffer overflows on the back-end RFID middleware may be launched by adversaries by using RFID tags. Although this may not be simple given the memory storage capacity of RFID tags, some commands permit an RFID tag to repeatedly communicate the same data block to overflow a buffer in the back-end RFID middleware [7].

RFID tags can be used to spread malicious code that could then infect other RFID network components (readers and connecting networks). In this scenario, an adversary stores and distributes infectious viruses or other RFID malware in the back-end system using the memory space of RFID tags [7]. Even though these attacks are uncommon, laboratory studies have shown that they are possible.

D. Strategic layer

Attacks on organizations and business applications fall under this category, which relies on poor infrastructure and application architecture. Competitive espionage, social engineering, privacy threats, and targeted security threats are more explicitly included in this layer.

- *Competitive espionage*: Rival businesses or industries are often the focus of adversaries. They can obtain critical and private information to sabotage their rivals by taking advantage of the ability to track and locate tagged items. Such information may include the target's strategies and tactics about shifting costs, production plans, marketing hypotheses, stock availability, or warehouse contents [8]. Such assaults can be carried out by listening in on conversations or by breaking into back-end databases, among other methods.
- *Social engineering*: To breach an RFID system and get unauthorized access to restricted areas or information, an attacker may even utilize social engineering techniques. The attacker can trick users into disclosing sensitive information without having to go through the difficult process of hacking or breaking RFID communications.
- *Privacy threats*: RFID tags respond to any reader, whether legitimate or illegitimate, without letting their owners know. Adversaries may use this unique capability to track and profile individuals [3]. One of the biggest risks associated with RFID systems is the possible collection of personal data, which might include everything from purchase patterns to medical data.
- *Targeted security threats*: An adversary can launch physical or electronic attacks or malicious events by using the data gathered by an association or location threat. Targeting and robbing persons who collect precious objects (e.g., watches or jewellery), snatching purses with marked bank notes, and scanning vehicles or ships carrying costly or important items are typical examples of this attack.

E. Multi-layer

Some of the attacks on RFID communication don't only target one layer. This category includes attacks that target the physical, network-transport, application, and strategy layers, as well as other layers. Covert channels, denial of service, traffic analysis, crypto and side channel attacks are all notably included in this layer.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|| A Monthly Peer Reviewed & Referred Journal |

||Volume 11, Issue 2, February 2022||

|DOI:10.15680/IJIRSET.2022.1102136|

- *Covert channels*: RFID tags may be used by attackers to open secret communication channels and transmit information. Adversaries may leverage the unused memory storage of several RFID tags to transfer data securely in a way that is hard to notice [8]. For example, a set of RFID tags placed in humans that are normally used to identify them might also be used to covertly report information about their social or medical activities.
- *Denial of service (DoS) attacks*: In Denial-of-Service attacks, RFID tags' regular operation could be disrupted if access to them is deliberately denied. Malicious usage of "blocker tags" [1] or the RFID Guardian may result in the purposeful blocking of access and subsequent denial of service for RFID tags. The unauthorized use of LOCK commands is another denial-of-service attack method. To prevent unauthorized writing on RFID tags' memory, LOCK commands are provided in several RFID standards [5].
- *Traffic analysis*: Traffic analysis attacks can also target RFID communication. Messages can be intercepted, and data can be extracted from a communication pattern by an eavesdropper. RFID communication is still vulnerable to traffic analysis attacks even when it is secured by encryption and authentication methods. The effectiveness of a traffic analysis assault increases with the volume of communications intercepted.
- *Crypto attacks*: Several encryption techniques are used to secure the integrity and confidentiality of the protected data when it is stored on RFID tags. Despite this, skilled attackers are using crypto assaults to break the encryption methods in use and expose or manipulate sensitive data.
- *Side channel attacks*: In contrast to theoretical vulnerabilities, side channel attacks make use of a cryptographic algorithm's actual physical implementation. The information that is typically exploited in these attacks comprises timing data, power consumption, or even electromagnetic fields. A deep understanding of the inner operations of the system on which cryptographic algorithms are implemented is necessary for the effective implementation of side channel attacks.
- *Replay attacks*: In a replay attack, a malicious party copies legitimate RFID communication responses and broadcasts them to one or more parties later to impersonate them. Typically, attackers initiate sessions or engage in eavesdropping to get the copied messages [2]. An example of this attack is the broadcasting of an exact replay of the radio signal sent from a valid tag to the reader that enables access, which allows attackers unauthorized access to prohibited areas.

III. COUNTERMEASURES AND IMPROVEMENTS

RFID devices are required to apply various security methods designed to counter various attacks to manage the multiple security threats. In this section, we will outline various strategies and countermeasures that have been recommended to improve the security and privacy of RFID. We will discuss countermeasures and improvements for the attacks.

A. Defences against physical layer attacks

- Traditional countermeasures like enhanced physical security with guards, fences, gates, locked doors, and cameras should be utilized to protect RFID systems against low-tech attacks like permanently or temporarily deactivating tags [8].
- An effective defence against tag removal would be a strong mechanical bond or glue that would make it hard to remove the tag from the tagged object without damaging it.
- Radio interference, whether intentional or unintentional, could also be reduced by employing walls that are nontrans parent to relevant radio frequencies.
- Effective password management could stop unauthorized users from using KILL commands.
- Possible solutions for relay attack protection include RFID communication encryption and the inclusion of a secondary authentication method, such as a password, PIN, or biometric data.

B. Defences against network-transport layer attacks

- Possible solutions for relay attack protection include RFID communication encryption and the inclusion of a secondary authentication method, such as a password, PIN, or biometric data. Challenge-response authentication protocols help to prevent cloning attacks. These need to have strong anti-brute force defenses as well. Another method of detecting cloning is simply comparing data in the back-end system.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|| A Monthly Peer Reviewed & Referred Journal |

||Volume 11, Issue 2, February 2022||

|DOI:10.15680/IJIRSET.2022.1102136|

- By employing authentication protocols or the second method of authentication such as one-time passwords, PINs, or biometrics, spoofing and impersonation could be prevented [2].
- Attacks on passive eavesdropping can be mitigated by encrypting the RFID communication channel.
- Attacks on network protocols could be prevented by hardening all RFID communication-supporting components, implementing secure operating systems, disabling unused and unsecured network protocols, and configuring active protocols with the minimal privileges possible.

C. Defences against the application layer

- Controlling access to RFID tags should be a primary concern to protect against unauthorized tag reading and tag manipulation. Tags with read-only capabilities effectively prevent unauthorized tampering.
- Another method for preventing unauthorized tag reading is through blocker tags. A blocker tag is a device with more features that can seem to a reader as multiple RFID tag at once. As a result, the blocker tag generates many virtual tags that conceal the existence of any legitimate tags.
- Simple countermeasures like periodic code reviews and extensive sanity checks can be done to assure the security of the system against flaws and vulnerabilities, preventing buffer overflows and malicious code injection in middleware [7].

D. Defences against strategic layer attacks

- A wide range of technological solutions have been recommended for privacy and targeted security risks, including destroying or momentarily silencing tags, preventing access to unwanted readers, relabelling or clipping tags, and employing pseudonyms, distance measurements, and encryption methods.
- Organizations that make use of RFID systems should create and maintain privacy and data protection policies and conduct risk assessments to identify threats and dangers related to the RFID infrastructure [8].
- Employees need to receive continuous training and education on the organization's RFID security and privacy policies since doing so improves awareness and control over sensitive information.

E. Defences against multilayer attacks

- A covert channel attack is difficult to detect and protect against. Limiting the memory resources available in an RFID tag is a potential defence strategy.
- In all kinds of networks, traffic analysis and denial of service attacks create significant security risks. Although there is a theoretical way to defend against these attacks, it is still a research topic because RFID tags have limited resources.
- Crypto cyberattacks can be prevented by using powerful cryptographic algorithms that comply with open cryptographic standards and having keys that are long enough.
- Minimizing the system's electromagnetic interference helps to prevent side-channel attacks. Another technique for countering side-channel threats is to make the internal circuit of the RFID chip more sophisticated, making it much harder for the attacker to comprehend the internal system and activities.
- There are a few countermeasures against replay attacks, including timestamps, OTPs, and strong authentication encryption involving nonces, progressive sequence numbers, or clock synchronization.

IV. CONCLUSION

Although RFID technology is transformative, it is still vulnerable to a wide range of security threats and intrusions. From unauthorized access and data manipulation to more sophisticated attacks such as relay and cloning operations, this comprehensive survey underscores the critical vulnerabilities that are inherent in RFID systems. Despite the substantial progress that has been achieved in the prevention of these threats by implementing improved authentication techniques, secure communication protocols, and enhanced cryptographic methods, there are still voids. The development of robust security solutions necessitates a proactive approach and continuous innovation due to the dynamic nature of cyber threats. In order to enhance RFID systems, future research should concentrate on the integration of AI-driven anomaly detection, blockchain, and machine learning. Ultimately, the secure implementation of RFID technology is crucial for its sustained growth and application across industries, assuring the protection of both data integrity and privacy.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|| A Monthly Peer Reviewed & Referred Journal |

||Volume 11, Issue 2, February 2022||

|DOI:10.15680/IJIRSET.2022.1102136|

REFERENCES

1. Ayoade, J. (2007). Privacy and RFID systems, roadmap for solving security and privacy concerns in RFID systems. Computer Law & Security Report, 23, 555–561
2. Khattab, A., Jeddi, Z., Amini, E., Bayoum, M.: RFID security threats and basic solutions. In: Ismail, M., Sawan, M. (eds.) RFID Security. Analog Circuits and Signal Processing, pp. 27–41, Springer, AG (2017)
3. Laurie, Adam. "Practical attacks against RFID." Network Security 2007.9 (2007): 4-7.
4. Federal Office for Information Security (2004). Security aspects and prospective applications of RFID systems. RFID consultation website. Accessed July 2009.
5. Rieback, M., Bruno Crispo, and A. Tanenbaum. "Is your cat infected with a Computer Virus?“, Vrije Universiteit, Amsterdam." Computer Systems Group (2006).
6. Karygiannis, T., Eydt, B., Barber, G., Bunn, L., & Phillips, T. (2007). Guidelines for securing radio frequency identification (RFID) systems: Recommendations of the national institute of standards and technology. NIST Special Publication 800–98.
7. Bhadani, Ujas. "Hybrid Cloud: The New Generation of Indian Education Society." (2020).
8. Karygiannis, A., Phillips, T., & Tsibertzopoulos, A. (2006). RFID security: A taxonomy of risk. In Proceedings of the 1st international conference on communications and networking in China (ChinaCom’06) (pp. 1–7). Beijing: IEEE

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details