|  |
| --- |
| APIC |
| Comprehensive Security Analysis on  Raspberry Pi Devices in the Automotive Industry |

4-29-2024

Contents

[Abstract 2](#_Toc165280630)

[Overview 3](#_Toc165280631)

[1. Raspberry Pi's Unique Security Vulnerabilities 3](#_Toc165280632)

[2. Illustration of Assault Mechanisms 4](#_Toc165280633)

[3. Methods for reducing the impact of security threats and the use of tools to enhance security. 4](#_Toc165280634)

[5. Difficulties in Safeguarding the Raspberry Pi 6](#_Toc165280635)

[6. Security measures related to cryptography 8](#_Toc165280636)

[In conclusion 9](#_Toc165280637)

# Abstract

A cost-effective and flexible solution for running crucial control and supervisory systems inside a manufacturing facility may be achieved by applying Raspberry Pi devices to automotive electronics used in car manufacture. However, stringent security measures are still necessary for the installation of these approaches to ward off any cyber threats that might compromise their security and integrity. Security breaches and eavesdropping are unavoidable due to Raspberry Pi security vulnerabilities, such as default setups and the vulnerability of unencrypted connections. This work aims to solve these issues fully. Since these updates leave missing gaps that make the computer subject to attacks, the essay maintains that version upgrading is another important area where regular issues commonly develop. Among the many attack types cited, MIT assaults stand out for their reputation to "brute force" their way into systems, however, there are other variants of MitM attacks as well. We recommend a more stringent authentication procedure in addition to confirmed encryption techniques as a defence against these threats. This will promote regular software upgrades, which are crucial in and of themselves. A combination of both physical and digital security measures is necessary to create robust security frameworks, which is why security strategies will be evaluated using the Confidentiality, Integrity, and Availability (CIA) framework. Balancing safety and efficiency in settings with limited resources is not a simple task, especially when considering the safety of Raspberry Pi devices and their low processing powers and physical security flaws. The essay finishes by looking into elliptic curve cryptography (ECC) as a method for enhancing security on low-resource platforms by using the generation of keys, encryption, and decryption. We examine the challenges that ECC may face in its efforts to become a reality in the automotive sector as a top choice for Internet of Things (IoT) device security, as well as how innovations are working to overcome these obstacles. To effectively safeguard Raspberry Pi devices in intricate industrial environments, this thorough rethinking proposes an integrated solution that integrates strong cybersecurity technologies with physical security measures.

# Overview

The adaptability and low cost of Raspberry Pi devices make them ideal for usage in the automotive industry. To prevent cyber-attacks that might cause system crashes and endanger operational integrity and safety, thorough security audits should be conducted on these technologies before they are integrated into key control and supervisory systems.

## Raspberry Pi's Unique Security Vulnerabilities

Numerous devices are implemented with pre-established configurations, such as usernames and passwords, that are frequently left unaltered throughout field operations, rendering them vulnerable to illegal access (Source: As Bento notes, Linux distributions such as Ubuntu also provide security notifications (Linux-Security-Enhancements-Patches) through their standard services summarizing security vulnerabilities (Roy, 2023).

Unauthorised parties may easily gather or spy on Raspberry Pi since it sometimes exchanges data over an unencrypted connection. This jeopardises the privacy of the transmitted data (Source: To address reported vulnerabilities, we retested the software quickly to ensure that the most recent version is fully secure, as evidenced by various reports, such as Ubuntu Security Notices).   
  
Lack of Regular Updates: Without timely firmware updates for Raspberry Pi devices, they could be vulnerable to security flaws that compromise the operating system's efficiency and overall productivity (note: "can compromise the system's effectiveness as well as its general productivity" rather than "affect the efficiency of the system, too, as well as its in general productivity" #security issue) (Roy, 2023).

## Illustration of Assault Mechanisms

By repeatedly trying the incorrect default credentials, attackers may illegally access the device in a brute force assault. According to Canavese, D. et al. (2024), if attackers get unauthorised access, they might potentially take control of their activities and interrupt routine operations.   
In the MitM Attack, or Man in the Middle, by eavesdropping on non-encrypted traffic, attackers may alter or steal important information and affect the processes controlled by the Raspberry Pi.

## Methods for reducing the impact of security threats and the use of tools to enhance security.

A stronger defence against illegal access and an improved security environment may be achieved by instituting stringent password rules and using multifactor authentication. These safeguards prevent the dissemination of default credentials as the only means of access. Interaction between plaintext information that is publicly available and a secret code that is generated when sensitive material is removed. Data security and non-interception are ensured from beginning to finish by implementing the use of secure communication protocols such as HTTPS/SSL and SSH for all data sessions.

1. Evaluation in Contrast to CIA Principles

*Brute Force Attack:*

**Confidentiality:**   
During this assault, the perpetrators could get access to sensitive data that might be exposed to unauthorised individuals. At this point, hackers can breach the system and access the restricted files since they have obtained or deciphered the login credentials. When the default passwords are either not changed or are weak and readily anticipated, the risk becomes much greater, which is a possible disadvantage of this attack route. Intentional disclosure of sensitive information may constitute a violation of confidentiality (Canavese, D. et al., 2024).

​

**Integrity:**  
When hackers get illegal access to databases by utilising brute force techniques, the data integrity is compromised; strong security mechanisms are consequently necessary. Giving hackers the ability to corrupt, alter, or delete arbitrary elements from data becomes so easy that it becomes one of the largest risks to systems. By manipulating the settings of a seemingly insignificant device, a villain might cause it to provide inaccurate data or feedback. Threats to system completeness, such as the introduction of a backdoor or other malicious means of gaining access to the system and launching a new intrusion that circumvents previously implemented security measures, pose a significant risk to the integrity of the data stored therein (AlSalem, 2023)

**Possible Effects on Access:**  
  
Such attacks have the potential to severely disrupt and possibly destroy whole systems and data. Account lockouts, which occur when the account holder is unable to access their account due to a string of unsuccessful login attempts, may be caused by these types of assaults. Also, the bad guy could get into the network through top-notch brute force attacks and install ransomware or other malicious software, which would then paralyse the network's critical systems for hours, causing users inconvenience.

*Man-in-the-Middle Attack:*

​

**Privacy Concerns:**   
  
A MitM attack involves listening in on a conversation between two people for the benefit of an unauthorised third party, which compromises their ability to keep their information private. Communication channels that do not use encryption or have weak security measures leave themselves open to interception, allowing the adversary to eavesdrop on and steal sensitive data in transit. Information about the company's finances, employees, and private relationships is just as sensitive as this. Considering how data breaches are changing over time, it's strange how they might take on a life of their own via the ongoing unauthorised disclosure of information, even if no one is watching (Canavese, D. et al., 2024).

**Integrity:**   
  
In a MitM attack, the attacker alters and cuts the data before it reaches its target, making it impossible to defeat the data while it is transferring. To improve, a malevolent individual may intercept sensitive information, such as a phone message including the transfer of money to the incorrect account, and then alter the account numbers to suit their needs. The data might be altered, which would compromise its dependability and lead to its eventual demise. Data integrity must be guaranteed by implementing tough tests, such as cryptographic hash validation, to catch even the most minute of alterations (AlSalem, 2023; Roy, 2023).

**System Availability:**

In most cases, MitM assaults start with the system's availability name and then proceed to become available. Still, issues may arise when malicious actors utilise their legitimate access to trigger an unmanageable and, in the majority of cases, catastrophic interruption or junction in messaging. The availability of the system might be disrupted by empirical situations such as continual data feed disruption and system crashes caused by this. Beyond that, an adversary may deploy a Man-in-the-Middle (MitM) attack to deliberately block unauthorised users from getting necessary information, a purposeful strike.

Every member of the CIA triad is in grave danger because of the combined force assessments and the MitM assaults. To quickly detect and combat such attacks, it is necessary to develop security systems with strong authentication, the use of encryption, and vigilance mechanisms.

## Difficulties in Safeguarding the Raspberry Pi

*Limitations on available resources*

Since Raspberry pirates currently have limited resources, the plan to establish robust preventative measures would be complicated—regardless of the general value that arises from their flexibility and cost efficiency. Some of the most fundamental features of these devices are the limited processing capacity and memory that are necessary for the operation of certain security protocols and tools. For instance, it's easy to imagine scenarios where the Pi lacks the necessary hardware or software to run resource-intensive antivirus apps or sophisticated intrusion detection systems, each of which has its own set of restrictions in terms of memory and processing capacity (Okporokpo, 2023) Furthermore, this device's performance is constrained because demanding complicated encryption may significantly decrease CPU speeds. Many technologies are forced to choose between slower working speed and inferior practical performance for real-time operations, such as controlling robotic systems in the automobile production field, due to the argument of either/or. In this case, it's important to practise well-tuned security precautions that are lightweight and compact while yet providing enough protection from any dangers. In the context of physical security, vulnerabilities may be defined as openings that unapproved parties can use to gain access to a protected system or area. Access control that isn't set up correctly, weak perimeter security, an area-wide surveillance system that isn't working, and inefficient security procedures are all examples of potential problems. Although Raspberry Pi devices are inherently vulnerable to physical security risks like theft or damage due to their small size and portability, these risks cannot be disregarded. In locations without sufficient physical safety precautions, these devices might be stolen or tampered with, giving the enemy access to important information or even controls. Physical security and assurance are therefore major concerns when using Raspberry Pis in the automotive sector, whether in a motor vehicle or on a production floor. Problems may arise when underlying procedures, such as keeping equipment in cabinets with severe tampering situations and having seals, are not always implemented. Danger lurks in situations with a poor security level. There is no way to conduct security checks or continuous monitoring there. (Rullo, 2023)  
In contrast, attackers may find it easy to compromise the system if they connect malicious devices to it during the installation of simple peripherals like radios or Arduino boards, which might compromise system performance control. To avoid unauthorised access or interference, it is important to develop thorough security policies that include both software-based solutions and tactical approaches to physically protected equipment and the surrounding surroundings (Lee, 2021). To safeguard the device from both physical and digital threats in its environment, it is crucial to have a thorough security strategy that makes the most of limited resources. This will allow for the implementation of realistic measures that safeguard the device from these threat types. It is believed that these solutions will help mitigate the dangers associated with deploying Raspberry Pi in critical areas of the automotive sector.

## Security measures related to cryptography:

*Elliptic Curve Cryptography (ECC)*

Devices like Raspberry Pi, which have limited processing capabilities, are well-suited to ECC (Elliptic Curve Cryptography), which improves efficiency while increasing security via the use of shorter key lengths. Along with ensuring the safety of data transmission and preventing unauthorised actions, its speed is very astonishing (Moradi, 2022). Because ECC permits the use of drastically decreased key sizes, which results in greater performance, it is more efficient than RSA. For space-constrained devices (Raspberry Pi) that need to install the Internet of Things, the most pressing challenge is ensuring low power consumption and RAM use. The reduced key lengths associated with elliptic curve cryptography and the difficulty of solving the discrete logarithm problem with elliptic curves are two features that make EC encryption very resistant to brute force assaults.

*Obstacles in Execution*

Resource limitations: The main advantages of ECC can be realized in situations that involve high-volume data transmission, but this technology might be a difficult proposition to apply and design for devices with almost zero resources, like the Raspberry Pi. Performing the ECC involves rather complicated mathematical operations that can result in a computation burden for Raspberry Pi whose computing power is very reduced (Canavese, D. et al., 2024) Compatibility and integration: For it to be ready to use together with the inter-communication protocols or security systems in place might create an additional stumbling block. Execution of ECC requires modifications and testing of all equipment endpoints. These include PCs, laptops, tablets, and wearable devices (Tawalbeh, L. et al., 2020)

*Latest Progress:*

While the ECC implementation field has been focused on developing algorithms with improved effectiveness on units with merger resources, failure-to-detect rates remain unacceptably high. In the IEEE Transactions on Dependable and Secure Computing recent article published, they looked at innovative approaches that will enrich the efficiency of ECC procedures with that efficiency being on a performance-to-IoT devices device level. While developing cryptographic libraries with emphasis on embedded systems has promoted Elliptic Curve Cryptography (ECC) for IoT developers, there are some limitations due to certain hardware and infrastructure requirements that put a limit on the use of public key encryption for the Internet of Things. Libraries such as `micro ECC` are tailor-made and they render ECC capabilities in an eclectic manner where resources are not consumed in excess, making it a perfect software for platforms like Raspberry Pi (Mitchell, R., 2023)

# Conclusion:

There must be a solid plan in place that addresses both cyber and physical security concerns if they arise. Safety precautions must be put in place to deal with the resource constraints and physical accessibility issues of Raspberry Pi devices: To overcome the resource constraints and physical accessibility issues with Raspberry Pi devices, it is necessary to adopt particular security measures: Keeping software up to date is crucial to protect against known vulnerabilities. That is, in this respect, it is important to consistently update an operating system, software, and security populations that are scanned for new threats. By including powerful authentication measures like multi-factor authentication (MFA), the likelihood of unauthorised users gaining access is lowered, ensuring that only authorised staff may utilise and control device properties. Encouraging data integrity and storage privacy via the implementation of effective cryptographic algorithms to protect information at rest and in transit safeguards data against unauthorised change and interception. A different approach to implementation might include creating controlled-access settings that carefully monitor and physically safeguard the devices, as opposed to employing centrally centralised secure enclosures and tamper-proof case boxes. Aside from the monitoring systems revealing any modifications in the region of the devices, the sensors' ability to detect any unauthorised entrance makes it obvious that illicit access or adjustments are feasible. Here, the opportunity to detect security problems early on also exists. You may use the firm's smart gadgets with complete confidence in their vital usage in automotive systems since these approaches reinforce them against a wide spectrum of cyberattacks.

# References:

AlSalem, T., Almaiah, M. and Lutfi, A. (2023) “Cybersecurity risk analysis in the IoT: A systematic review,” *Electronics*, 12(18), p. 3958. doi: [10.3390/electronics12183958.](https://www.mdpi.com/2079-9292/12/18/3958)

Canavese, D. *et al.* (2024) “Security at the edge for resource-limited IoT devices,” *Sensors (Basel, Switzerland)*, 24(2), p. 590. doi: [10.3390/s24020590](https://www.mdpi.com/1424-8220/24/2/590)

*Enterprise IoT and OT Threat Report by Zscaler ThreatLabz* (2023) *Zscaler.com*. Available at: <https://www.zscaler.com/resources/2023-threatlabz-enterprise-iot-ot-threat-report> (Accessed: April 29, 2024)

Lee, J. Y. and Lee, J. (2021) “Current research trends in IoT security: A systematic mapping study,” *Mobile Information Systems*, 2021, pp. 1–25. doi: [10.1155/2021/8847099.](https://www.hindawi.com/journals/misy/2021/8847099/)

Mitchell, R. (2023) “New side-channel attack on ARM: Implications for IoT security,” *Electropages.com*, 15 May. Available at: <https://www.electropages.com/blog/2023/05/new-side-channel-attack-arm-implications-iot-security> (Accessed: April 29, 2024)

Moradi, M., Moradkhani, M. and Tavakoli, M. B. (2022) “Security-level improvement of IoT-based systems using biometric features,” *Wireless communications and mobile computing*, 2022, pp. 1–15. doi: [10.1155/2022/8051905.](https://www.hindawi.com/journals/wcmc/2022/8051905/)

Okporokpo, O. *et al.* (2023) “Trust-based approaches towards enhancing IoT security: A systematic literature review,” *arXiv [cs.CR]*. Available at: <http://arxiv.org/abs/2311.11705> (Accessed: April 29, 2024).

Rullo, A., Ianni, M. and Serra, E. (2023) “Editorial: Security and privacy for the internet of things,” *Frontiers in Computer Science*, 5. doi: [10.3389/fcomp.2023.1173296.](https://www.frontiersin.org/articles/10.3389/fcomp.2023.1173296/full)

Roy, A. *et al.* (2023) “Device-specific security challenges and solution in IoT edge computing: a review,” *The Journal of Supercomputing*, 79(18), pp. 20790–20825. doi: [10.1007/s11227-023-05450-6.](https://link.springer.com/article/10.1007/s11227-023-05450-6)

Tawalbeh, L. *et al.* (2020) “IoT privacy and security: Challenges and solutions,” *Applied sciences (Basel, Switzerland)*, 10(12), p. 4102. doi: [10.3390/app10124102.](https://www.mdpi.com/2076-3417/10/12/4102)

*Tuvsud.com*. Available at[: https://www.tuvsud.com/en/resource-centre/infographics/top-10-consumer-iot-cybersecurity-vulnerabilities-in-2023](:%20https:/www.tuvsud.com/en/resource-centre/infographics/top-10-consumer-iot-cybersecurity-vulnerabilities-in-2023) (Accessed: April 29, 2024).

*USN-6416-3: Linux kernel (Raspberry Pi) vulnerabilities* (no date) *Ubuntu*. Available at: <https://ubuntu.com/security/notices/USN-6416-3> (Accessed: April 28, 2024).