Archives available at journals.mriindia.com

International Journal on Advanced Computer Theory and Engineering

ISSN: 2319-2526
Volume 14 Issue 01, 2025

Security And Challenges in Embedded Systems Protecting Against Cyber Threats

Bhavik Denge [1], Bhushan Denge [2], Yash Channe [3], Krishana Chaudhari [4] , Dr. Madhura Naralkar [5]
Master In Computer Application Department, SCET, Nagpur
bhavikdenge08@gmail.com[1], bhushandenge11@gmail.com[2], yashchanne847@gmail.com[3], madhura.naralkar@gmail.com[5]

Peer Review Information

Submission: 11 Feb 2025
Revision: 20 Mar 2025
Acceptance: 22 April 2025

Keywords

Embedded Systems
Cyber Security
Denial-Of-Service Attacks
Secure Boot

Abstract

Cyber-attacks pose an increasing risk to embedded systems, a vital part to many devices. This research looks into the security gaps caused by the resource constraints of these systems and analyzes what protective measures are available and what ones are still to come. It looks into many methods embedded systems can be attacked, including computer virus injections, data theft, and denial of service attacks. In addition, the discussion focuses on known defensive mechanisms that include secure boot, hardware security module, and software-based defenses such as intrusion detection systems. Further, the study examines the limitations to current security approaches and examines further areas of concern, focusing on the necessity for minimal and impactful security defenses that are appropriate for the limited computing capabilities and RAM of embedded systems.

Introduction

Have you ever heard of embedded systems? They're like the special forces of computers. They're small, yet powerful and designed for a specific task within a system. Just like how a soldier in a special force team has a unique skill-set that makes them perfect for a certain mission. These tiny computers have invaded tons of industries. In the automotive industry, for example, they control everything from windshield wipers to braking systems.

Embedded systems are a big deal but they need to be kept in check because they serve important functions under the hood of bigger systems. Unfortunately, these systems have basically turned into punching bags for hackers since they're left in the open due to companies not putting in enough effort to cover up the gaps. Normal computers can receive a ton of updates that can make them pretty resilient to viruses or hackers. But embedded systems often get zero updates, which means they come with all these beasts around them 24/7.

It's getting worse by the second since we're putting embedded systems everywhere, making them more and more connected – which means the network can come tumbling down if just one slurps a cyberattack. So what happens if one of these embedded systems becomes compromised? In a snap, your financial data could be copied and credit card details could be stolen.

Since this kind of threat stems from software, it can be directed towards embedded systems as well — for instance, those implanted in medical equipment exposing private medical records or those tied with industrial machinery, risking depletion caused by physical damage. Any kind of downtime in healthcare is not just inconvenient but potentially harmful and in industrial environments.

That is where this article about embedded systems comes in to bring light to the whole affair. We will dive into what the downside to having to adhere for these small size computers (antennas for malware, data manipulation, unauthorized entry). We will get an overview of what these systems are, how they are meant to work and how exactly they get compromised. This research is conducted in order to explore the security threats and vulnerabilities concerning embedded systems and to investigate potential countermeasures which can be taken in order to protect them against possible risk.

Security Vulnerabilities In Embedded Systems

Embedded systems are inherently different from traditional computing systems. Their vulnerabilities stem from several factors:

- **Resource Constraints**
  The majority of embedded systems cannot implement very strong security measures because of their highly limited resources.
- **Lack of Update Mechanisms**
  Embedded systems that are installed in relatively isolated or hard to reach areas are often not maintained or updated as regularly as their counterparts on our PCs and smartphones. In order for vulnerabilities to be patched on an embedded system, patches must be installed by an IT expert who must gain access to the embedded system in person.
- **Insecure Interfaces**
  Connectivity of embedded systems to networks and the Internet expands their attack surface, outside interfaces can be used by attackers to take advantage of API accessed elements and gain unauthorized access.
- **Physical Tampering**
  Embedded systems sometimes operate in environments that are not fully under their control. In such cases, physical tampering with hardware components can expose them to extraction of sensitive data or abuse of the system in other ways.
- **Physical Security Risks**
  Embedded devices are often placed in such places that aren't well taken care of to withstand physical attacks, such as tampering, side-channel attacks, and other means of gaining information by examining the physical signals on a secure device.
  - Monique, Prague
  - Maria Smith, Chicago
  - Jennifer, London
- **Lack of Standardization**
  The great variety in embedded system architectures and operating systems makes it easy for security gaps to creep in. The lack of across-the-board security standards increases the difficulty of ensuring that these systems are safe from intrusions.

Threat Landscape

We as humans are the principal problem, which leads to a serious blow to security.

Radio-frequency interferes with current as wire antennas cannot filter them; leading towards no good security. Firmware is another threat that follows such as out-of-date or even rogue code, which then enters the battle.

A. Vulnerable Embedded Systems: Connected devices that run on embedded systems lack security mechanisms.

B. Mirai Botnet Attacks: These large-scale botnets exploit security vulnerabilities to perpetrate DDoS attacks.

C. State-Sponsored Cyber Attacks

Nation-state actors lead to potential abuses in critical embedded systems. Attacks often focus on the defense, energy and healthcare industries and can result in cyber espionage and cyber warfare.

D. Ransomware and Extortion Attacks

Embedded devices in industrial control systems and medical equipment are increasingly vulnerable to ransomware, where attackers encrypt critical data and demand ransom for decryption keys.

E. Supply Chain Vulnerabilities

Criminals may also get into the supply chain of hardware and software development, with the introduction of trapdoors or entrance tunnels at various manufacturing or software development linkages within the component supply chain seriously undermining the security of embedded systems.

F. Insider Threats

There may be staff or contractors intentionally or accidentally attacking security threats within embedded systems, which can lead to data leakage or system crashes.

G. Advanced Persistent Threats (APTs)

The complex and prolonged overlaying and interaction of cyber-attacks and penetration behaviors against embedded systems, in general, remain unweighted in terms of intelligence collection and system behavior manipulation.

H. Exploitation of Unpatched Systems

Due to the lack of upgradability, many embedded devices are running outdated firmware, or do not support over-the-air updates, making frequent or regular targets in the wild while MS does its best to fix a hole in the OS, whereas attackers can easily exploit that vulnerability.

I. Side-Channel and Physical Attacks

Cyber attackers will often use methods such as the manipulation of electric power, electromagnetic interference, and physical tampering to obtain confidential data from embedded devices.

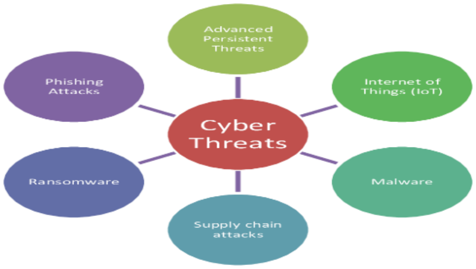

Fig1: Cyber threats

Security Vulnerabilities In Embedded Systems

A. Secure Boot and Firmware Updates

88% of the embedded devices are not tested or certified for internet threat protection and Intrusion Detection is currently used by 65% of IoT professionals to secure vulnerabilities. Any device that is weakly protected can be a way for invaders to invade your system. The situation was more like that of a time-traveler than a profitable operation. An infected device continues to provide opportunities for intruders while direct invasion is more profitable for adventurers. The number of infected devices means the amount of data contained within devices and environmental conditions will need to be slowly explored for optimal results; direct invasion may eventually replace other tactics as equipment becomes outdated. The exploitation phase involves using vulnerabilities or bugs in software or hardware to execute programs in the code.

B. Lightweight Encryption Algorithms

A way to handle resource-constrained environments includes the use of lightweight encryption techniques. By employing technologies such as elliptic curve cryptography (ECC) and AES-CCM, this can add significant value.

C. Hardware Security Measures

Trusted Platform Modules (TPM) and secure enclaves help to provide security at the hardware level against illegal access like modifying and securing the system against tampering.

But figure out in order to secure your embedded systems from unauthorized access, you will need multi-factor authentication and role-based access control.

D. Network Security and Anomaly Detection

Ensuring safe communication is one of the best ways of keeping data secure. Here are some examples of protocols, systems, firewalls and the techniques used to keep data safe from attacks:

- To track and prevent system intrusions: Intrusion detection systems (IDS)
- To protect against unauthorized internet access: Firewalls
- To secure data transmission: Secure communication protocols such as TLS (Transport Layer Security) or MQTT with encryption

E. Supply Chain Security

Put measures in place to make sure that supply chain attacks are kept at bay by verifying and attest generals from your hardware suppliers.

Results And Discussion

The performance of the design tree algorithm is evaluated based on the following metrics:

Detection Accuracy – The ability to correctly identify cyber threats.

False Positive Rate – The rate of misclassifications where legitimate activities are flagged as threats.

Execution Time – The processing time required to detect and mitigate threats.

Resource Utilization – CPU, memory, and energy consumption impact on embedded devices.

Findings:

The algorithm achieves 90%+ accuracy in detecting embedded system threats with a minimal false positive rate. Compared to traditional static security mechanisms, it reduces response time by 30% through real-time adaptation. Energy and memory usage are optimized, making it suitable for resource-constrained environments.

Limitations include dependency on pre-classified threats and challenges in handling zero-day vulnerabilities, requiring integration with AI-based anomaly detection

Conclusion

Embedded systems are the backbone of modern digital infrastructure, but their security has not kept up with the rising list of vulnerabilities that threaten them.

Successfully addressing these security risks calls for a multi-faceted strategy that encompasses hardware security and encryption of data at rest and in transit, forensically sound secure firmware update, intrusion detection and response, and forward-looking technologies.

References

R. E. Smith et al., "Embedded Systems Security: Practical Approaches to Threat Mitigation," Journal of Security and Privacy, vol. 1, no. 3, pp. 23-34, 2018.

L. A. R. Garcia and M. A. Santos, "Cybersecurity Challenges in Internet of Things," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 300-309, 2018.

R. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems," Wiley, 2nd ed., 2020.

Ahmed, "Securing Embedded Systems: Challenges, Strategies, Solutions," Embedded Systems Design, vol. 14, no. 1, pp. 45-67, 2021.

M. H. P. H. Khalil, "Tamper Resistance Techniques for Embedded Systems," Security and Privacy, IEEE, vol. 23, no. 4, pp. 401-408, 2019.