Chapter 14
Machine Learning–Based Collection and Analysis of Embedded Systems Vulnerabilities

Aissa Ben Yahya
https://orcid.org/0000-0002-5437-2745
Faculty of Sciences, Moulay Ismail University of Meknes, Morocco

Hicham El Akhal
Faculty of Sciences, Moulay Ismail University of Meknes, Morocco

Abdelbaki El Belrhiti El Alaoui
https://orcid.org/0000-0001-9462-2932
Faculty of Sciences, Moulay Ismail University of Meknes, Morocco

ABSTRACT

The security of embedded systems is deteriorating in comparison to conventional systems due to resource limitations in memory, processing, and power. Daily publications highlight various vulnerabilities associated with these systems. While significant efforts have been made to systematize and analyze these vulnerabilities, most studies focus on specific areas within embedded systems and lack the implementation of artificial intelligence (AI). This research aims to address these gaps by utilizing support vector machine (SVM) to classify vulnerabilities sourced from the national vulnerabilities database (NVD) and specifically targeting embedded system vulnerabilities. Results indicate that seven of the top 10 common weakness enumeration (CWE) vulnerabilities in embedded systems are also present in the 2022 CWE Top 25 Most Dangerous Software Weaknesses. The findings of this study will facilitate security researchers and companies in comprehensively analyzing embedded system vulnerabilities and developing tailored solutions.

DOI: 10.4018/979-8-3693-0497-6.ch014

1. INTRODUCTION

The last few years have seen remarkable progress in a variety of fields, such as astronomy, healthcare, agriculture, connected cars, and smart devices, to name a few. Smart homes equipped with voice-activated digital assistants (Wellsandt et al., 2020) remote patient monitoring systems, and connected cars designed to prevent accidents and collisions are just a few examples of technologies that have made users' lives easier and helped people with disabilities (Gulati et al., 2020) Embedded systems are the basic building blocks and key technologies that make these applications possible. Embedded systems serve as the fundamental building blocks and vital technologies that facilitate the development of various applications. The progress observed in these applications is largely dependent on the advancements in embedded systems, as noted by (Prasad et al., 2021). These systems are designed to operate with limited resources, such as memory, processing power, and energy consumption, as well as operating in harsh environments and using customized components and software, also the absence of standardization makes them vulnerable to cyber-attacks. The vulnerabilities in these systems can be exploited to cause serious harm to human life and privacy. For example, in 2017, the US Food and Drug Administration (FDA) (Hern, 2017) recalled 500,000 pacemakers due to cybersecurity vulnerabilities that could allow hackers to access the device and reprogram it. The vulnerability could lead to the battery running flat or the administration of inappropriate pacing, which could result in the death of the patient. In 2020 a critical vulnerability in a traffic light controller deployed on roads across Europe could cause "sustained traffic chaos" (*Critical Traffic Light System Vulnerability Could Cause 'Chaos' on the Roads*, 2020). While in 2021, Trend Micro (*Connected Cars Technology Vulnerable to Cyber Attacks*, n.d.) reported that connected cars are vulnerable to cyber-attacks that could threaten the safety of drivers and passengers. The report revealed that distributed denial-of-service (DDoS) attacks on Intelligent Transportation Systems (ITS) could overwhelm connected car communications and represent a high risk. Exposed and vulnerable connected car systems are easily discovered, making them at higher risk of abuse. Buffer overflow flaws in the privacy-preserving TPM 2.0 protocol were discovered in March 2023 (Nuspire, 2023), potentially putting billions of IoT devices at risk. In comparison to general-purpose systems, the security of embedded systems is declining, mainly due to their limited resources. As a result, the security measures that are commonly applied in general-purpose systems cannot be utilized in embedded systems. As vulnerabilities in embedded systems (ESs) continue to rise, it has become evident that the security solutions applied to general-purpose systems cannot be used in ESs. Therefore, it is crucial to study and analyze vulnerabilities in ESs to address current issues and prevent future zero-day attacks. Although vulnerability databases hold most of the reported vulnerabilities, they do not provide information on the classification of vulnerabilities into specific categories, such as embedded systems, general-purpose PCs, web browsers, operating systems, or protocols.

The significant advancement achieved in the fields of machine learning (ML) and deep learning (DL) have unveiled opportunities for the automation of classification processes. An exemplary demonstration of this can be seen in the research conducted by (Huang et al., 2019), the authors introduced TFI-DNN model, a novel approach that merges Term Frequency-Inverse Document Frequency (TF-IDF) and information gain (IG) techniques with a Deep Neural Network (DNN) to effectively categorize vulnerabilities into their respective types. (Chen et al., 2020) in the other hand propose a novel framework for classifying vulnerability severity in software development using the term frequency-inverse gravity moment (TF-IGM) instead of the traditional TF-IDF model. TF-IGM shows promise, and feature selection enhances classification performance on various datasets. (Sharma et al., 2021) introduced a vulnerability