Funded By

CERIAS

The Center for Education and Research in Information Assurance and Security

A PRELIMINARY STUDY ON THE CHARACTERISTICS AND DETECTABILITY OF VULNERABILITIES IN REAL TIME OPERATING SYSTEMS

PASCHAL AMUSUO, ARAVIND MACHIRY, JAMES DAVIS

1. Motivation

Figure 1: Vulnerabilities in RTOS can lead to catastrophic consequences

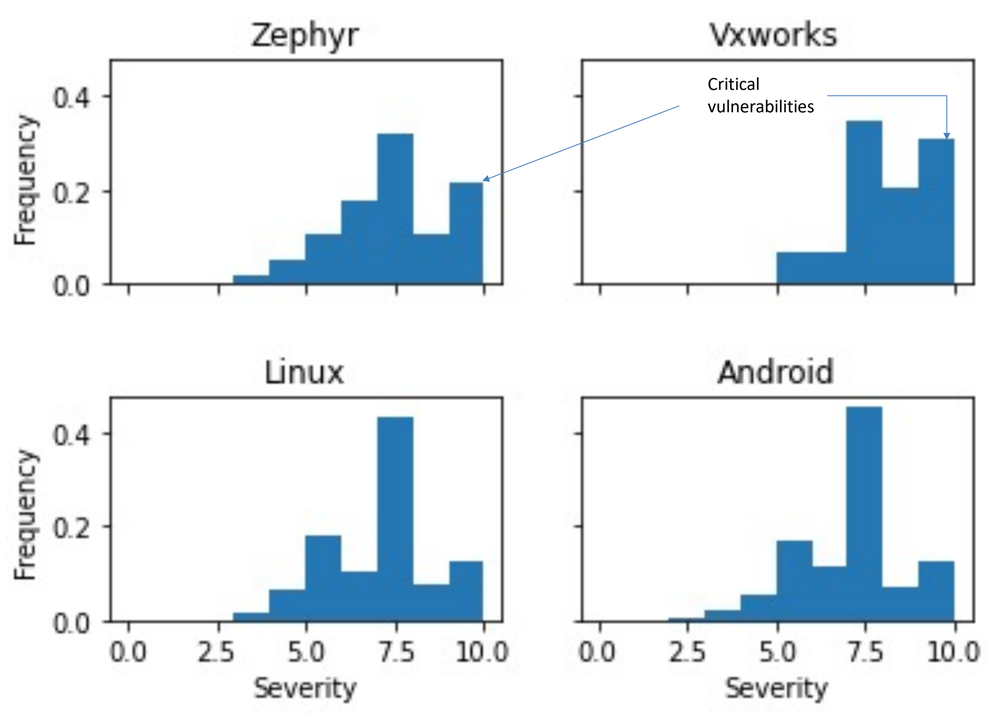

Figure 2: Over 20% of Vulnerabilities in RTOS (Zephyr and VxWorks) are critical, unlike regular OS (Linux and Android)

2. Research Questions

RQ1: The characteristics of vulnerabilities in Real Time Operating Systems

a. How do these RTOS vulnerabilities manifest?
b. What are the possible consequences and severities of these vulnerabilities
c. What is the distribution of vulnerabilities across RTOS components
d. Do these vulnerabilities have some unique embedded systems characteristics?

RQ2: The characteristics of the vulnerable functions in the Real Time Operating Systems

a. How do software metrics of the vulnerable functions compare with those of the entire project?
b. How long do the vulnerability exist in the RTOS before they are reported, published and fixed?
c. How easy would it be to reach and trigger the vulnerabilities in the vulnerable functions?

3. Methodology

1. Extract all the vulnerabilities of 4 popular real-time operating systems – Zephyr, RIOT, FreeRTOS and VxWorks from the NVD
2. Go through the vulnerability reports and characterize each of the vulnerability to identify their manifestation, severity, possible consequence and component affected.

1. Study the vulnerability patches of the open source RTOS to identify the vulnerable functions, affected lines of codes and vulnerability life cycle.
2. Add programmatic annotations to these vulnerable functions and lines of codes.
3. Develop an LLVM analysis pass to infer various software, file, function and line level metrics of the vulnerable functions and lines of codes.
4. Analyze the data collected and report our findings.

4. Practical Applications

1. **Vulnerability Detection**
   a. Our findings could reveal the limitations of current vulnerability detection tools for RTOS.
   b. Our results could influence future research on the design of novel vulnerability detection tools better suited for embedded systems.

2. **Dynamic Analysis and Fuzzing**
   a. Our results could inspire new and improved techniques for fuzzing RTOS and embedded systems

3. **RTOS Design**
   a. Our work could reveal architectural flaws in the design of RTOS that could be exploited by attackers.

Operating Systems	Linux	Android	Zephyr	VxWorks
Count since 2017	2567	4508	54	27

Table 1: RTOS (Zephyr and VxWorks) vulnerabilities are under-detected and under-studied

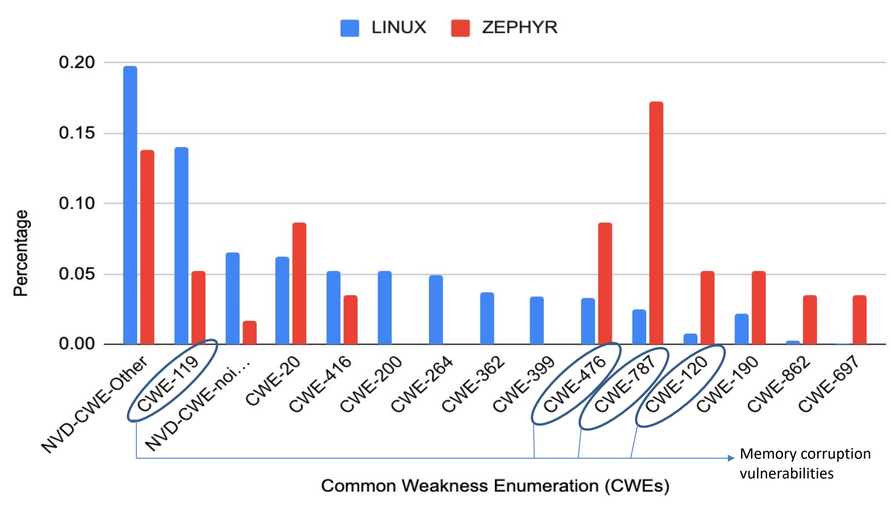

Figure 3: CWE distributions between regular OS (Linux) and a RTOS (Zephyr) are different. Memory corruption vulnerabilities top the list of top 5 CWEs in Zephyr

PURDUE UNIVERSITY Discovery Park

CERIAS