Update at Your Own Risk: Analysis and Recommendations for Update-related Vulnerabilities

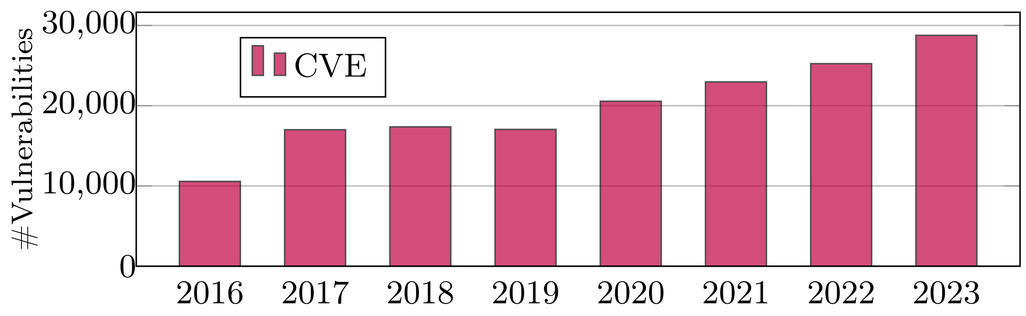
Ahmad B. Usman, Linköping University
Dept. of Computer and Information Science
Supervisor: Mikael Asplund

LINKÖPINGS UNIVERSITET

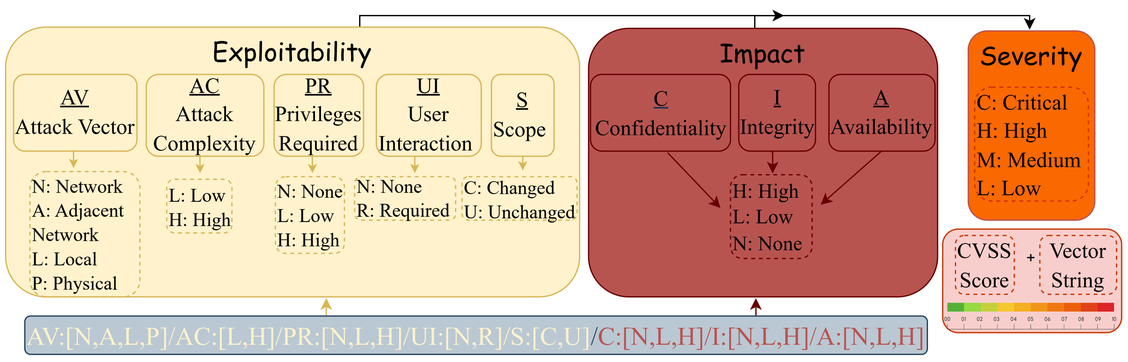
Motivation & Research Goals

Modern computer-based systems play a vital role in various sectors. A key feature of such devices is their ability to receive software or firmware updates for security and other purposes[1].
Unfortunately, many current update mechanisms lack security, and vendors often fail to adhere to best security practices.
This study aims to investigate update-related vulnerabilities, their impact/trends over the past eight years, identify the most common weaknesses, and develop a recommendation matrix to mitigate the causes of these weaknesses during update process.

Methods



The number of vulnerability incidents disclosed by the official CVE organization has been increasing over the past eight years.



Analysis of Selected Metrics: We let $\mathcal{D}$ represent the dataset containing V vulnerabilities, $\mathcal{D} = \{\text{CVE}_1, \text{CVE}_2, \ldots, \text{CVE}_V\}$. We analyzed the following metrics:

- Impact metrics: $\{C_i, I_i, A_i\}$
- Access metrics: $\{AV_i, AC_i\}$.
- Severity metrics: $\{S_i\}$.

Let $Freq(X)$ denote the frequency of counter for a given metric X, the cumulative counters can be expressed as:

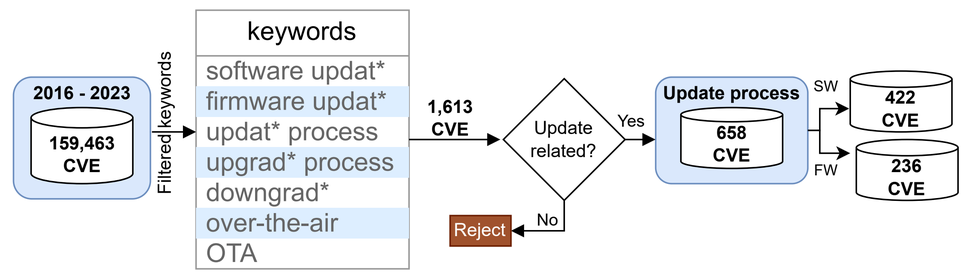
$$Freq(X) = \sum_{i=1}^{V} \mathbb{I}(X_i),$$

Mapping CVE to CWE Algorithm: We computed the number of CVEs associated with each CWE in the dataset.

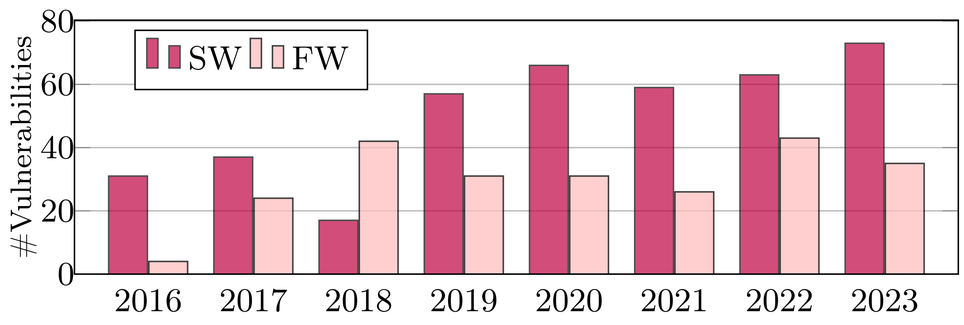
$$N_i = \sum_{j \in J} e_{ij} \quad \text{where} \quad e_{ij} = \begin{cases} 1, & \text{if CVE } j \text{ maps to CWE } i \\ 0, & \text{otherwise} \end{cases}$$

To account for update-related vulnerabilities, it most include e.g., flaws exploited during updates, compromised update integrity, issues in the upgrade or downgrade processes.

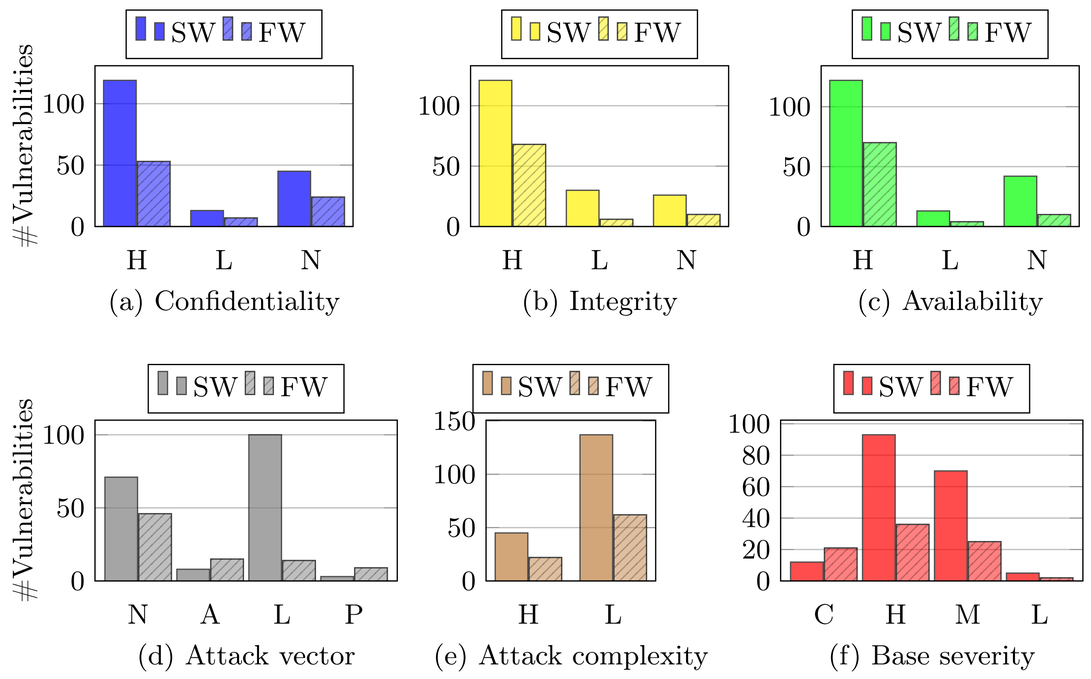
Selected Results

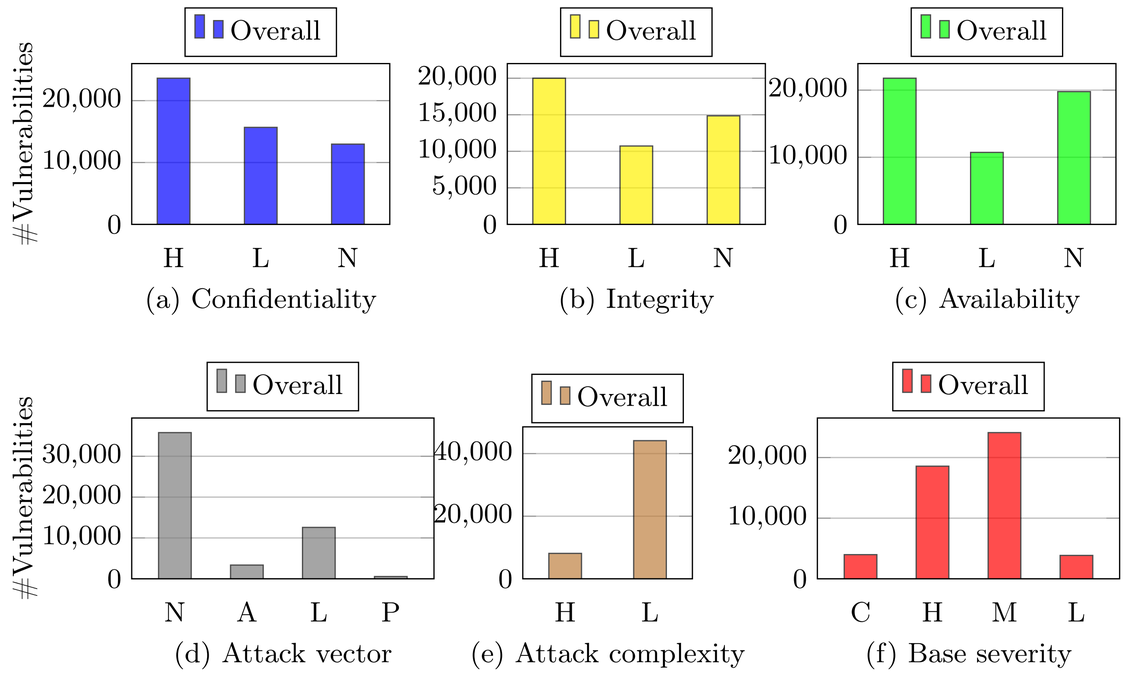


Distribution of update-related vulnerabilities:



Comparison of update-related vulnerabilities against overall:





References

[1] Remote Attestation with Software Updates in Embedded Systems
Ahmad B. Usman and Mikael Asplund
IEEE Conference on Communications and Network Security - Cyber Resilience Workshop 2024

WASP WALLENBERG AI, AUTONOMOUS SYSTEMS AND SOFTWARE PROGRAM