Basic Details of the Team and Problem Statement

Ministry/Organization Name/Student Innovation:

Ministry of Power

PS Code: 1387

Problem Statement Title: Detection of Embedded Malware/ Trojan in Hardware devices used in Power Sector.

Team Name: Cyber-Sentinels

Team Leader Name: Pooja LH

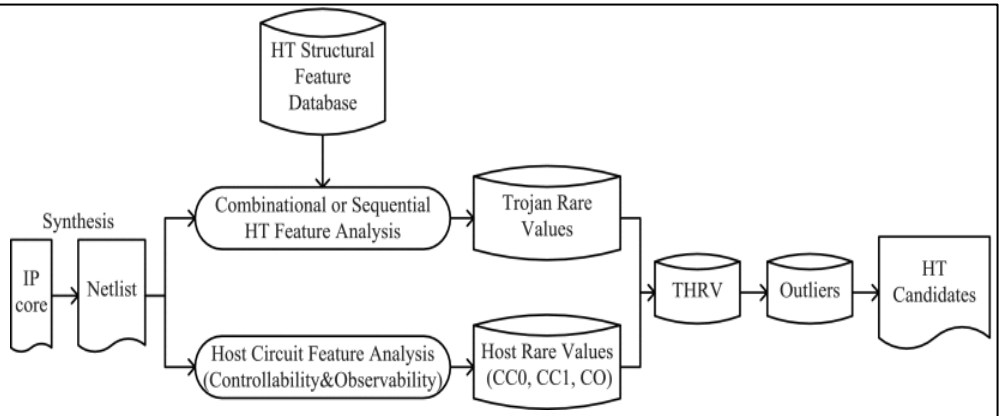
Institute Code (AISHE): C-1341

Institute Name: GSSS Institute of Engineering and Technology for Women

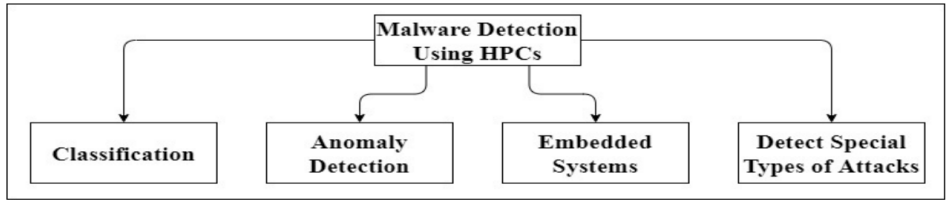
Theme Name: Blockchain & Cybersecurity

Idea/Approach Details

- In the realm of resource-constrained embedded systems, where traditional software-based malware detection methods fall short due to computing limitations and the impracticality of continuous updates, we introduce a pioneering solution.
- Our approach leverages Hardware Performance Counter (HPC) registers and Machine Learning (ML) classifiers to enable runtime malware detection tailored for the unique challenges of embedded devices. To address the scarcity of available HPC registers and enhance accuracy, we propose a customized HMD approach that classifies various malware classes at runtime.
- A database that contains HT structural feature templates is established. The structural templates in the database are the basic elements. An HT can contain multiple and various basic elements cascaded deeply and widely. First, the third-party IP core under test is synthesized to a gate-level netlist.
- Then, the netlist goes through HT feature analysis and host circuit feature analysis. In the HT feature analysis process, the netlist is searched to find circuit elements which match to the structural feature templates in the database. Once a template is matched, an integer score is given to the circuit element. The score indicates how inactive the circuit element is and is called Trojan rare value.
- In the host circuit feature analysis process, the controllability and observability (called host rare value) of each circuit element including logical gates and flip-flops are examined. Afterwards, the Trojan rare value and the host rare value are combined to be a comprehensive rare value defined as THRV (Trojan-Host Rare Value) for each circuit element. Finally, the circuit elements are sorted in a descending order of THRV values and HT candidates are found by looking for THRV outliers.
- By combining structural feature analysis, HPC features, and ML classifiers, our innovative hardware-based solution offers a powerful defense against malware in embedded systems, particularly suited for the power sector's stringent security needs. This solution not only improves detection accuracy but also addresses resource constraints, making it a valuable addition to the arsenal of cybersecurity measures for critical infrastructure.



Flow of the proposed HT detection method.



Categorizing Malware Detection Using Machine Learning Algorithms Based on HPCs

Technology stack :

- VHDL / Verilog,
- Microcontrollers and Microprocessors,
- Pytorch , TensorFlow and scikit-learn,
- MySQL / NoSQL variants
- IDA Pro and Wireshark,
- C and C++,
- ModelSim and QEMU, Linux and RTOS

Idea/Approach Details

Use cases :

- Protection of Critical Infrastructure: The power sector is a critical infrastructure, and any compromise in its systems can lead to widespread disruptions and even threats to national security. Detecting malware and trojans in power sector hardware devices helps protect the integrity and availability of the electrical grid, ensuring uninterrupted power supply to consumers.
- Zero-Day Attack Mitigation: Zero-day attacks are especially dangerous because they exploit vulnerabilities unknown to software developers and security experts. By continuously monitoring and detecting embedded malware and trojans, the power sector can mitigate the risks associated with zero-day attacks and respond swiftly to emerging threats.
- Maintenance and System Reliability: Regular malware and trojan detection in power sector hardware devices can also be used for predictive maintenance. Identifying compromised or vulnerable devices allows for proactive maintenance, reducing the chances of unexpected failures and minimizing downtime.
- Grid Resilience: Ensuring the resilience of the power grid is vital in the face of natural disasters or cyberattacks. Detecting and removing malware and trojans from hardware devices contributes to the grid's overall resilience, making it more robust and adaptable during challenging circumstances.
- Data Protection: Power sector devices often collect and transmit sensitive data, including customer information and operational data. Detecting and preventing malware in these devices safeguards the confidentiality and integrity of this data, protecting both consumers and the power companies.
- Environmental and Safety Concerns: A compromised power grid can have environmental consequences, such as power surges or outages that affect critical systems. Additionally, safety concerns arise if power sector devices are compromised and fail to operate as intended. Detecting malware helps mitigate these environmental and safety risks.

Dependencies :

- In response to the growing challenge of malware threats in resource-constrained embedded systems, we present a pioneering hardware-based malware detection (HMD) solution designed to safeguard critical infrastructure in the power sector and beyond.
- Traditional software-based approaches are ill-suited for embedded systems due to limited computing resources and the impracticality of continuous software updates.
- Our innovative HMD approach harnesses the potential of Hardware Performance Counter (HPC) registers and Machine Learning (ML) classifiers to achieve accurate real-time malware detection.
- Efficient feature analysis algorithms are developed to search small piece of circuits which match the features in the database and are assigned with a score. A score outlier determination algorithm is developed to identify suspicious Trojan elements.
- The experimental results show that the proposed method is capable of detecting all stealth Trojans from the benchmarks with short runtime and low false positive rate, compared to the existing HT detection methods.
- The Hardware Performance Counter (HPC)-based approach, coupled with machine learning classifiers, excels in detecting malware variants and Trojans that capitalize on zero-day vulnerabilities.
- By focusing on structural features and employing score outlier determination algorithms, our solution can identify suspicious elements and behaviors even in previously unseen malware strains. This capability enhances the resilience of embedded systems in the power sector and beyond, protecting critical infrastructure from evolving and unpredictable cyber threats, including zero-day attacks.
- The project relies on the presence and functionality of IEDs such as Relays, BCUs, Smart Meters, and RTUs. These devices serve as the hardware components that need to be tested for malware and Trojan threats.
- Hardware Systems: The project depends on various hardware systems including System on Chip (SoC), Microcontrollers, Microprocessors, Digital Signal Processors (DSP), and Field-Programmable Gate Arrays (FPGAs). These components house the firmware and application programs where malicious codes could potentially be embedded.

Team Member Details

Team Leader Name: **Pooja LH**

Branch : B E | Stream : CSE | Year : III

Team Member 1 Name: **Nanditha S**

Branch : B E | Stream : CSE | Year : III

Team Member 2 Name: **Srashti Kumbar**

Branch : B E | Stream : CSE | Year : III

Team Member 3 Name: **Tanushree S**

Branch : B E | Stream : CSE | Year : III

Team Member 4 Name: **Vandana H**

Branch : B E | Stream : CSE | Year : III

Team Member 5 Name: **Varshini N**

Branch : B E | Stream : CSE | Year : III

Team Mentor 1 Name: Type Your Name Here

Category (Academic/Industry): | Expertise (AI/ML/Blockchain etc): | Domain Experience (in years):

Team Mentor 2 Name: Type Your Name Here

Category (Academic/Industry): | Expertise (AI/ML/Blockchain etc): | Domain Experience (in years):