Work-in-Progress: Boot Sequence Integrity Verification with Power Analysis

Arthur Grisel-Davy, Amrita Milan Bhogayata, Srijan Pabbi, Apurva Narayan, Sebastian Fischmeister

Embedded Software Group, University of Waterloo

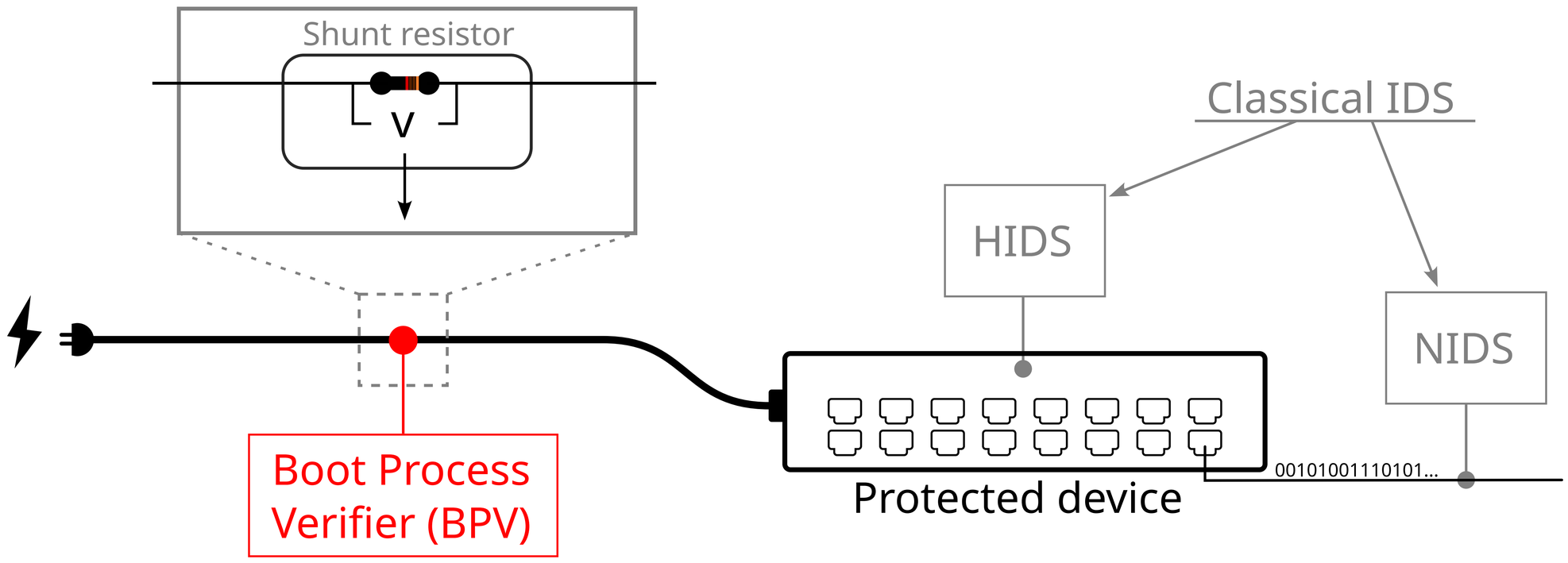

Figure 1:Typical Intrusion Detection Systems (IDS) are Host-based (HIDS) or Network-Based (NIDS). This new Physics-Based IDS performs anomaly detection using global power consumption.

Power Traces

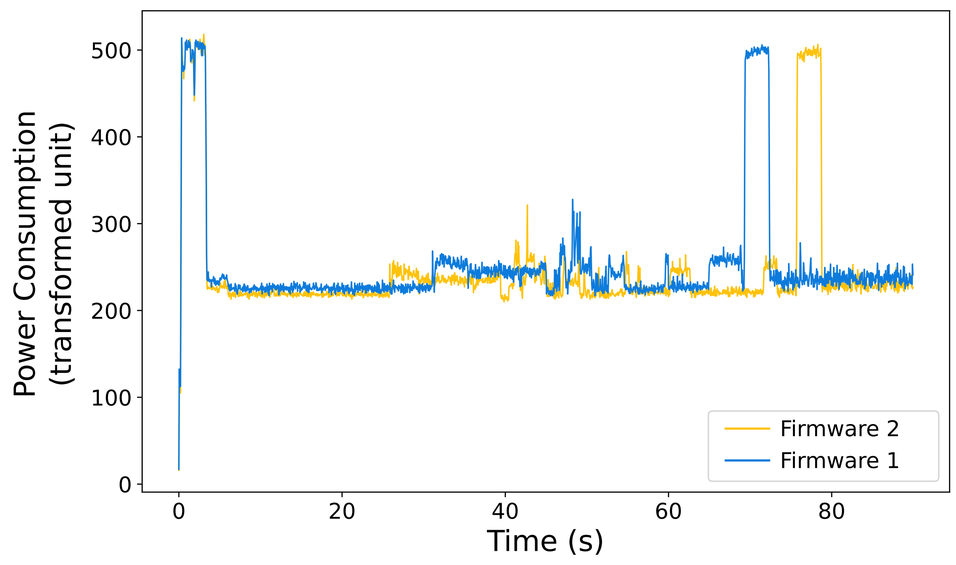

Figure 2:Power consumption of the bootup sequence of a TP-Link switch with two different firmware versions

- The power consumption offers an accurate and trusted representation of the system's state.
- We measure the power consumption at the main power cable after the Alternating Current (AC) to Direct Current (DC) conversion.
- A script extracts and synchronizes the bootup sequences using the rising edge of the first power spike.

Boot Process Verifier (BPV)

The BPV

- trains on a small training set of ≈10 normal traces.
- does not require anomalous data to perform detection.
- uses the IQR to set the distance threshold: $threshold = Q3 + 1.5 \times (Q3 - Q1)$ [2].
- performs detection by comparing the Euclidean distance of a new trace to the average training trace.
- detects as anomalous the bootup sequences that deviate from training. It can be due to malicious or wrong version firmware.

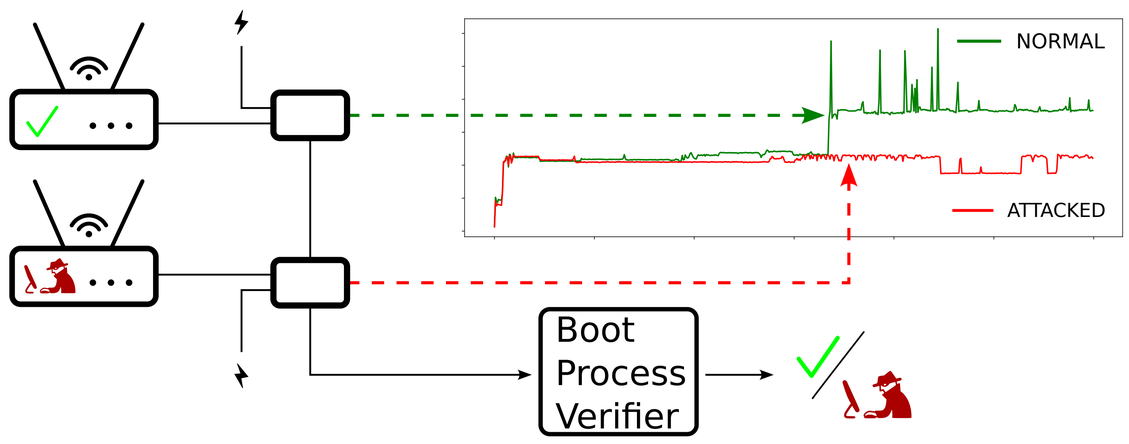

Figure 3:Overview of the BPV detection procedure

Case Study: Networking devices

- We selected four consumer-available networking devices.
- We installed OpenWRT on routers and downgraded the firmware on switches to represent firmware attacks.
- We extracted 500 bootup sequences [1] per attack per machine.

Machine	Detection F_1 Score	Overall F_1 Score
TP-Link switch	0.866	0.942
HP switch	0.983	
Asus router	1	
Linksys router	0.921	

Table 1:Results of detection. F_1 scores are averaged per machine from 20 experiments.

Conclusion

The BPV:

- can reliably detect firmware tampering from the power consumption trace.
- requires minimal training data and training time.
- can be implemented with minimal downtime and hardware modification and applies to clientless equipment.

Future Work

- Application to a greater range of devices such as OT systems or general purpose computers.
- Evaluation of data augmentation techniques to improve detection of low-impact attacks.

References

[1] A. Grisel-Davy. Dataset of bootup power consumption traces for four networking equipment `https://doi.org/10.5281/zenodo.6419214`, Apr. 2022.

[2] J. Han, J. Pei, and M. Kamber. *Data mining: concepts and techniques*. Elsevier, 2011.