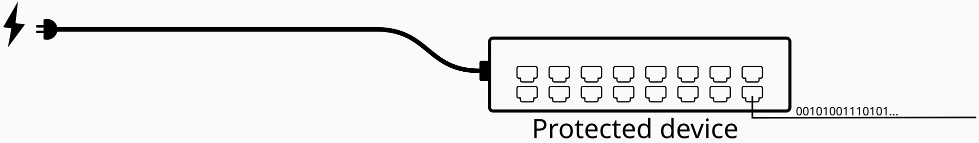
WIP: Firmware Integrity Verification with Side-Channel Power Consumption Analysis

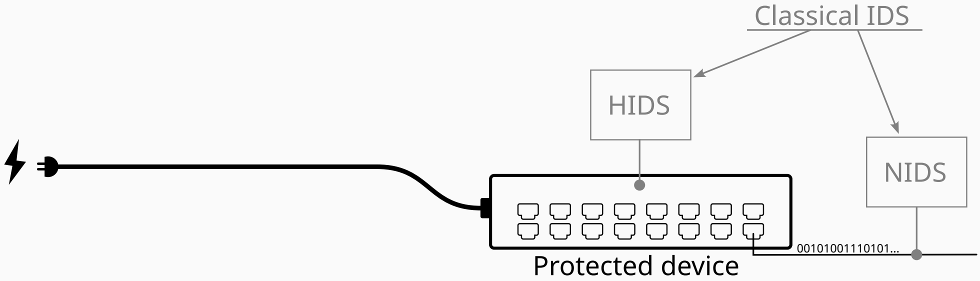
Arthur Grisel-Davy, Amrita Milan Bhogayata, Srijan Pabbi, Apurva Narayan, Sebastian Fischmeister

University of Waterloo, Canada

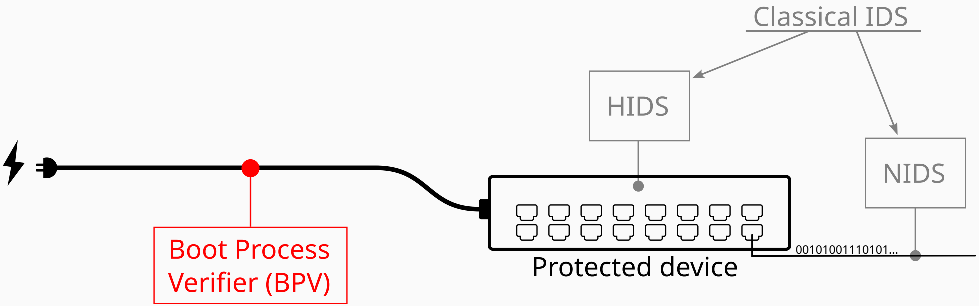
Introduction



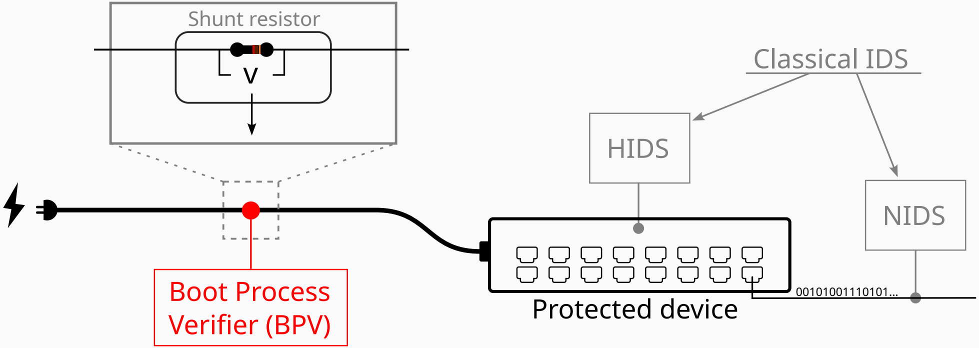
Introduction



Introduction



Introduction



Power trace

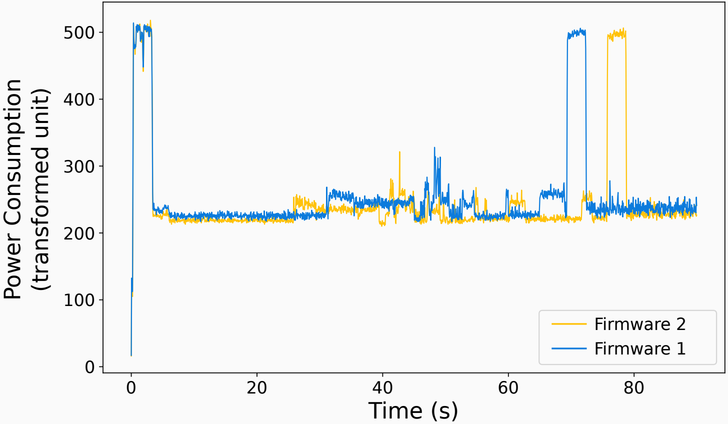
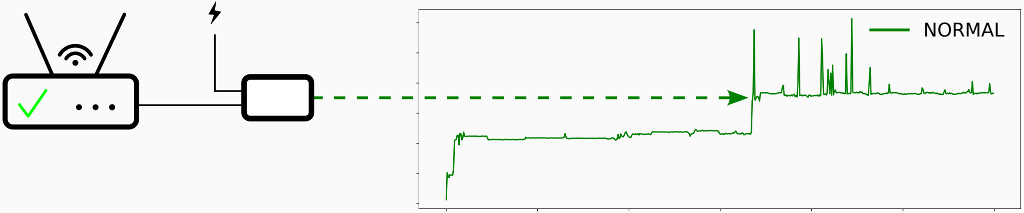


Figure 1: Power consumption for two firmware versions illustrating the impact of firmware change on the consumption pattern.

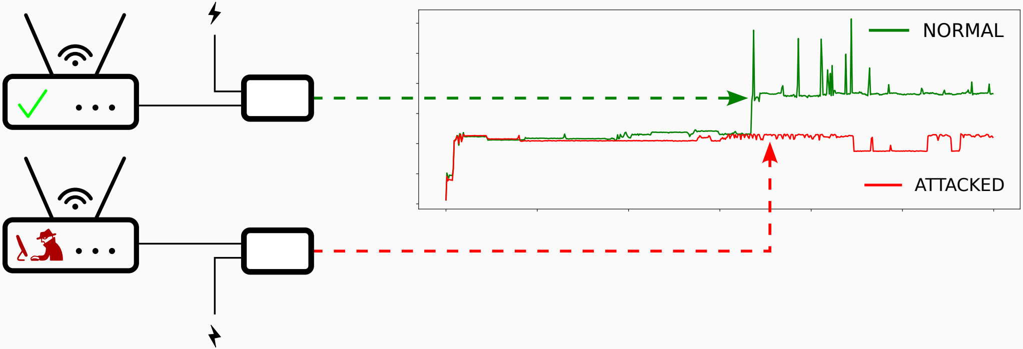
Boot Process Verifier (BPV)

Distance threshold = $1.5 \times IQR$



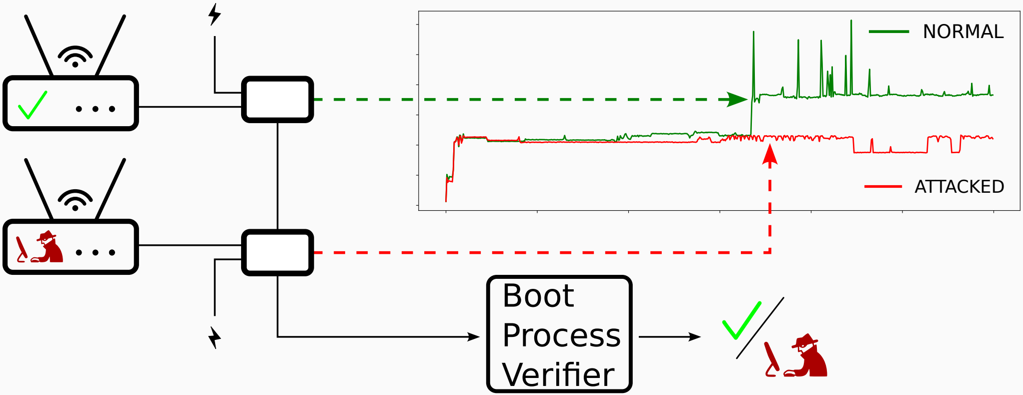
Boot Process Verifier (BPV)

Distance threshold = 1.5 × *IQR*



Boot Process Verifier (BPV)

Distance threshold = 1.5 × *IQR*



Case Study: Networking Devices

- Four devices
- Attacks: firmware replacement, firmware downgrade.
- 500 bootups sequences per device per attack.[1]
- BPV trained with ten training samples.

[1] dataset publicly available, see the paper.

Case Study: Networking Devices

- Four devices
- Attacks: firmware replacement, firmware downgrade.
- 500 bootups sequences per device per attack.[1]
- BPV trained with ten training samples.

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.

[1] dataset publicly available, see the paper.

Future Work

- Expand results to other types of machines.
- Improve anomaly detector to make it less susceptible to outlier in training data.
- Explore more sophisticated attacks.

Thank you for your attention.