dtec.bw

JAHRESTAGUNG 2024

Robustness Testing for Embedded Devices Against DoS Attacks

Florian Förster[1], Song Son Ha[2], T.R. Doebbert[2], H. Beuster[2], G.J. Scholl[2], D. Merli[1]
[1]Institut für innovative Sicherheit, Technische Hochschule Augsburg
[2]Chair for Electrical Measurement Engineering, Helmut Schmidt University, Hamburg

Motivation

Denial-of-service (DoS) attacks have garnered significant attention in both industry and research for decades due to their capacity to inflict damage using relatively simplistic methods and minimal expertise. However, the topic is mainly discussed in relation to the Internet and network level technologies as well as use cases. It is important to note that Industrial Control System components, such as Programmable Logic Controller and other real-time devices, are susceptible to DoS attacks as well. This is demonstrated in research scenarios like the malware PLC-Blaster [1] and in practical instances such as Industroyer [2].

Currently, no best practice against DoS attacks on embedded devices seem to exist. This research is part of the "Digital Sensor-2-Cloud Campus Platform" (DS2CCP) project [3], which aims to demonstrate reliable communication between the industrial shop floor and the edge cloud. The main goal is to provide a set of best practice methods as well as solutions to increase the resilience of embedded devices against network based DoS attacks.

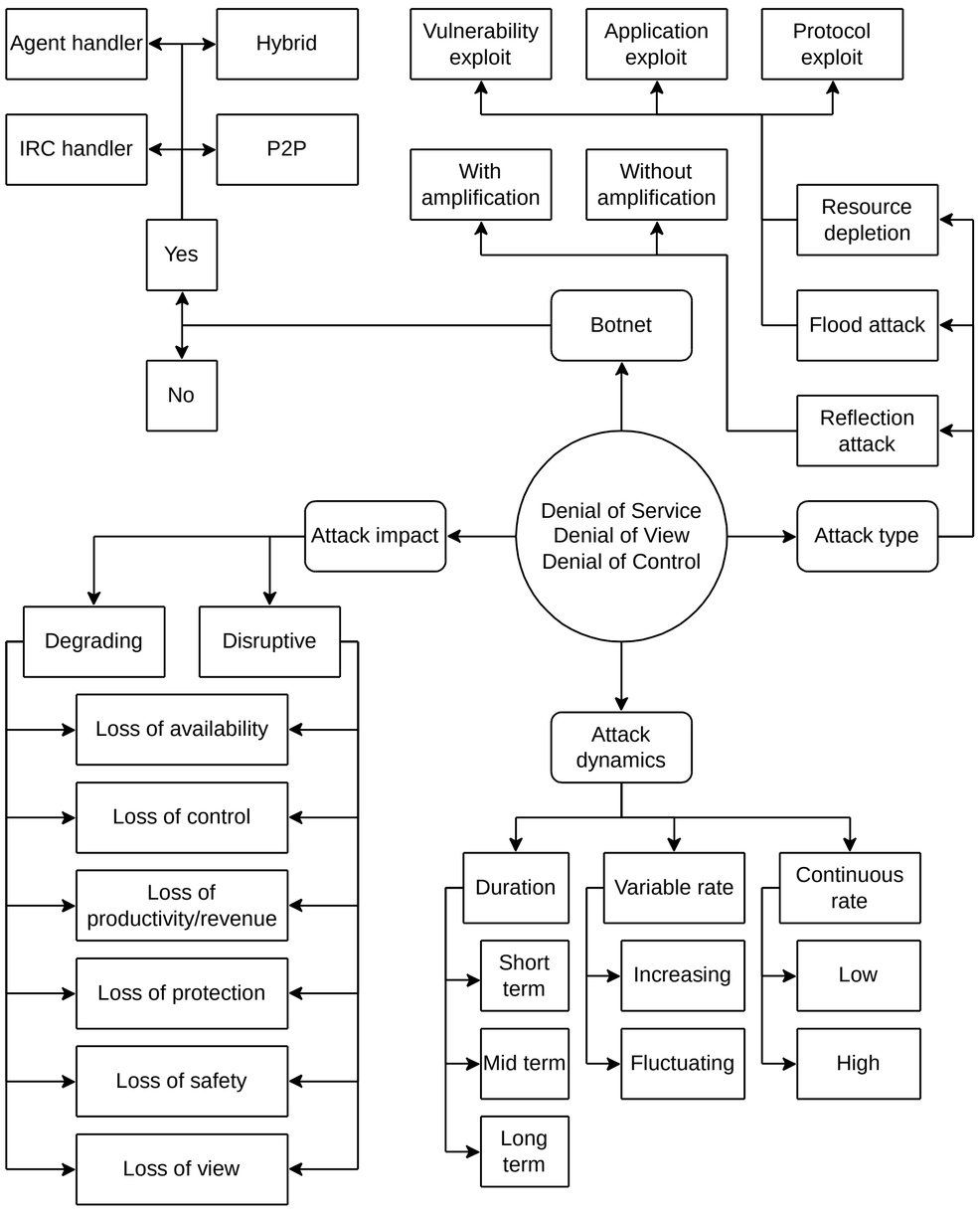

Fig. 1. Taxonomy of DoS attacks based on [4] and [5]

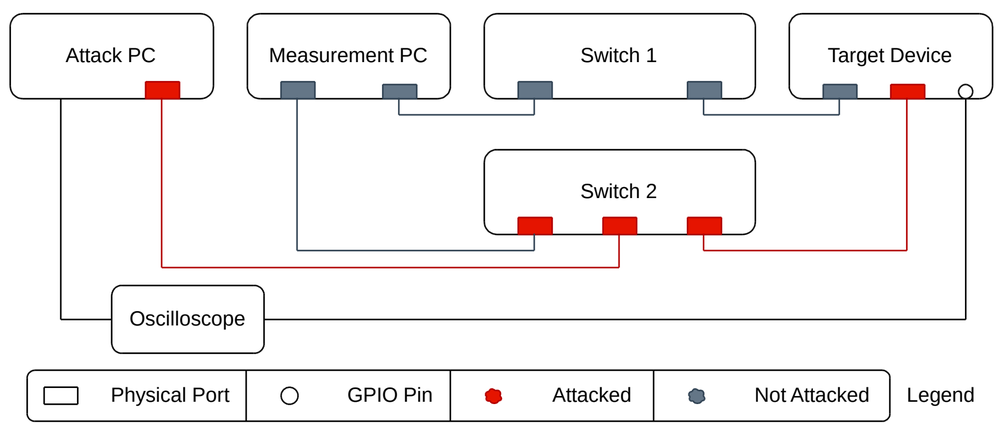

Fig. 2. Proposed Measurement Setup Scheme for Robustness Testing of Embedded Devices against DoS attacks

Robustness Testing of Embedded Devices

Testing embedded devices for their robustness against DoS attacks cannot be done the way most DoS testbeds are designed today: testing the impact on the whole network at once. Instead, only the impact of the DoS attack on the attacked device itself should evaluated when discussing device robustness. Thus, some precautions have to be made. The proposed approach consists of two elements. Firstly, using a redundant network topology to allow reference communication over infrastructure suffering attack and infrastructure not suffering an attack. The other part of the approach consists of evaluating the Quality of Service of essential functions of the device as well as detailed profiling of the victim device itself.

References

[1] R. Spenneberg, M. Brüggemann, and S. Schwartke, PLC-Blaster: A Worm Living Solely in the PLC, https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster - A - Worm - Living - Solely - In - The - PLC - wp . pdf, Black Hat Asia 2016, Accessed: 2024-01-19, 2016. (visited on 02/27/2024).
[2] Win32_industroyer. [Online]. Available: https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf (visited on 02/27/2024).
[3] Helmut-Schmidt-University, "DS2CCP – Entwicklung einer digitalen Sensor-2-Cloud Campus-Plattform," dtec.bw Project website: http://dtecbw.de/home/forschung/hsu/project-ds2ccp.
[4] M. Salim, S. Rathore, and J. Park, "Distributed denial of service attacks and its defenses in IoT: a survey," Journal of Supercomputing, vol. 76, no. 7, pp. 5320–5363, 2020.
[5] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, "Analysis of DDoS-capable IoT malwares," in 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Sep. 2017, pp. 807–816.

Technische Hochschule Augsburg | THA_innos Institut für innovative Sicherheit

unibw.de hsu-hh.de dtecbw.de

Digital Sensor-2-Cloud Campus-Platform

gefördert durch
dtec.bw Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr
Finanziert von der Europäischen Union NextGenerationEU