Initial study towards anomaly-based detection of APTs attacks

Andrea Ceccarelli

University of Florence

RCL

RESILIENT COMPUTING LAB

UNIVERSITÀ
DEGLI STUDI
FIRENZE

DIMAI
DIPARTIMENTO DI
MATEMATICA E INFORMATICA
"ULISSE DINI"

Advanced Persistent Threats

Advanced, well-financed attack campaign with a full spectrum of intelligence-gathering techniques.

Persistent, from highly determined and persistent attackers. One of the attackers' goals is maintaining long-term access to the target.

Threats executed by coordinated human actions rather than mindless automated code.

Reconaissance, Scanning,

Exploitation, Maintaing access

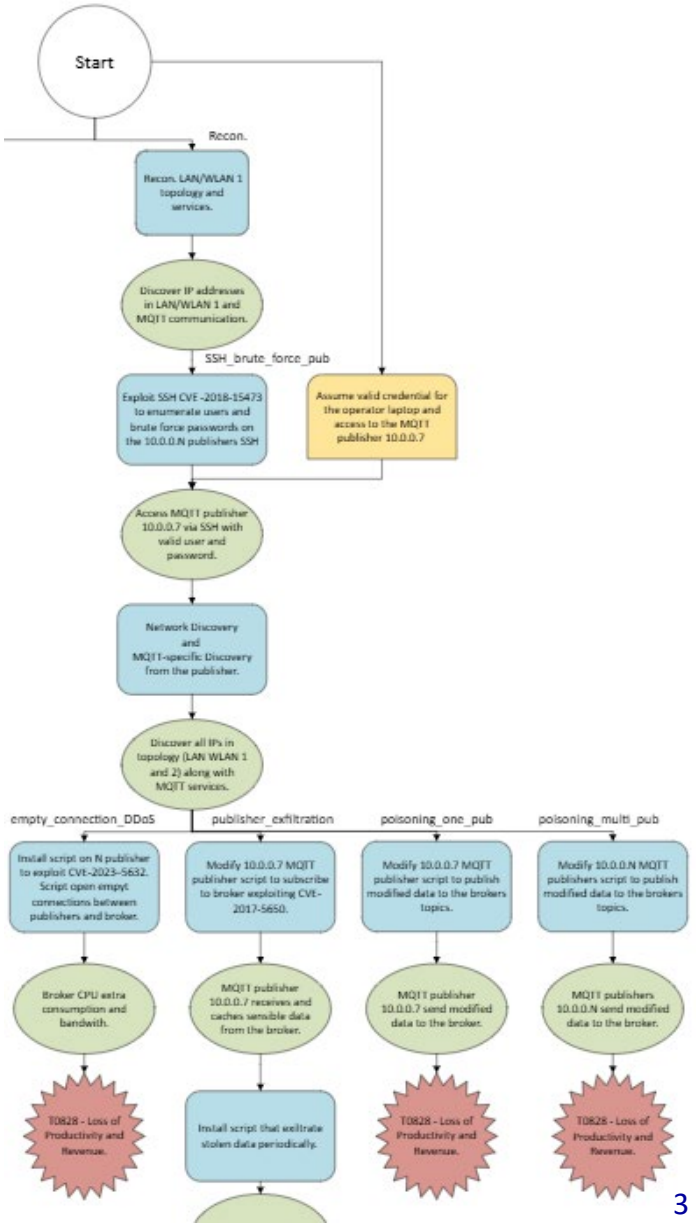
Anomaly detectors for APTs

A shift of perspective:

- not just «detect an attack»,
  but
- interrupt the attack path before the goal is reached

What is missing:

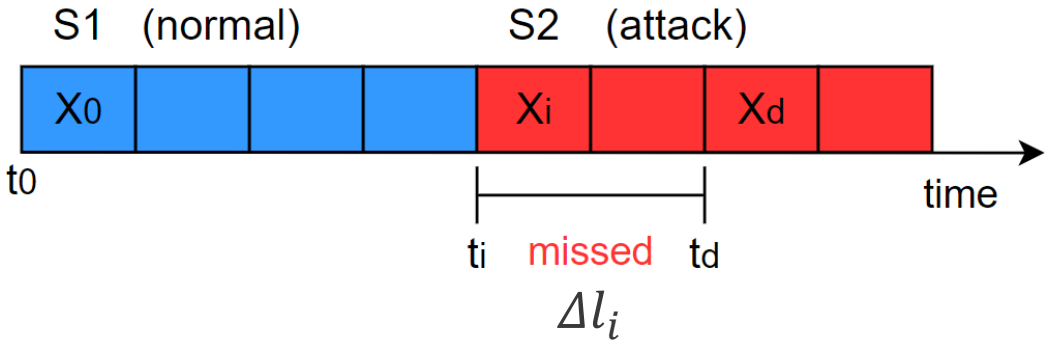
- Above all, datasets!
- Then, algorithms for time series exists (even if *maybe* not so much applied to IDS *yet*)



Need to measure attack latency

How long was the attacker into the system before being detected? Or: given a complex attack, how long did it take to detect it?

- **Average Latency** = $\boldsymbol{\Delta L} = \frac{\sum_{i=0}^{N} \Delta l_i}{N}$
- **Sequence Detection Rate SDR** (as there is the case in which x_d never occur)



Tommaso Puccetti and Andrea Ceccarelli , Detection Latencies of Anomaly Detectors: An Overlooked Perspective?, *ISSRE 2024*

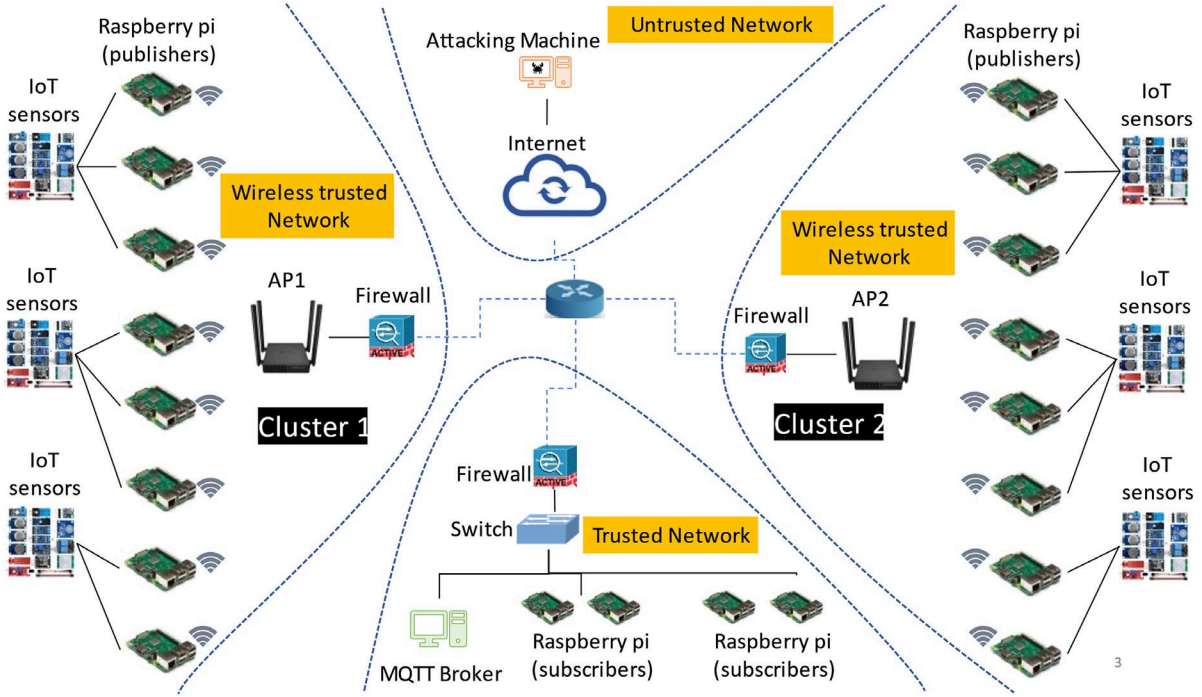
Puccetti, T., Nardi, S., Cinquilli, C., Zoppi, T., & Ceccarelli, A. (2024). ROSPaCe: Intrusion Detection Dataset for a ROS2-Based Cyber-Physical System and IoT Networks. *Scientific Data*, *11*(1), 481.

Let's try to build a dataset

Industrial network traffic dataset DoS/DDoS-MQTT-IoT (publish/subscribe)

Simulate Network environment using DDoShield-IoT

Can replay dataset .pcap file and simulate network normal behavior ← **and we can craft attack!**



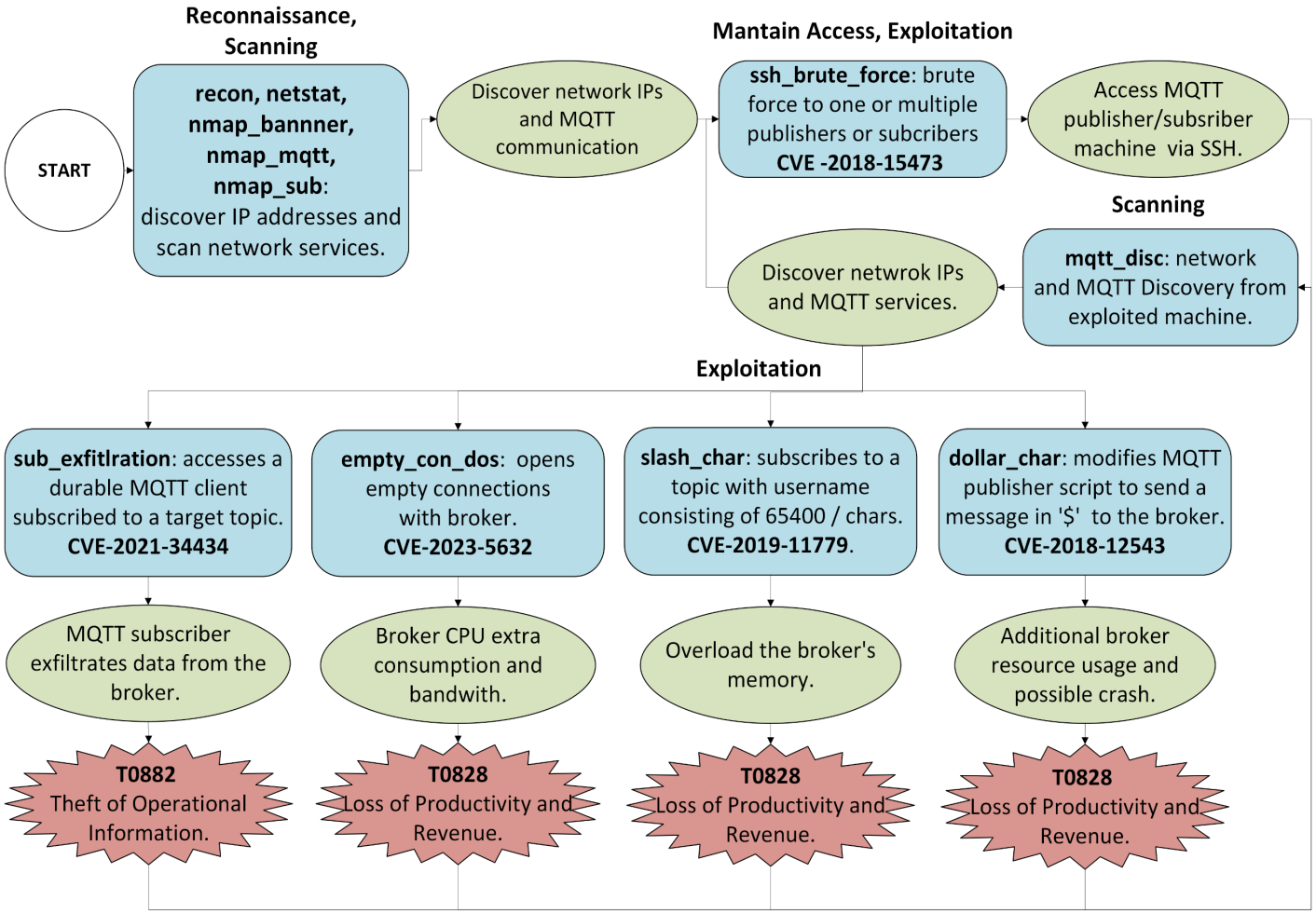
Alatram, Alaa, et al. "DoS/DDoS-MQTT-IoT: A dataset for evaluating intrusions in IoT networks using the MQTT protocol." *Computer Networks* 231 (2023): 109809.

De Vivo, Simona, et al. "DDoShield-IoT: A Testbed for Simulating and Lightweight Detection of IoT Botnet DDoS Attacks." *DSN-W*, 2024.

Design and implement the attack paths

MITRE | ATT&CK®

CVE®



MUR FLEGREA - *Federated Learning for Generative Emulation of Advanced Persistent Threats*

Bad results but just our first try