RIOT:

Resilient Internet of Things

https://resilient-iot.se/

Financed by the Swedish Civil Contingencies Agency

CHALMERS UPPSALA UNIVERSITY

Team

- Chalmers
  - Magnus Almgren
  - Christos Profentzas
  - Francisco Blas Izquierdo Riera
  - *Wissam Aoudi, Charalampos Stylianopoulos + others*
- Uppsala
  - Christan Rohner
  - Tobias Mages

Given **their central role in critical infrastructure**, the applications driven by the Internet of Things need to be resilient.

Cyber attacks must be **discovered and mitigated**, and

the key function of **data collection** to drive the applications must **be resilient in the face of attack or device compromise**.

Project Vision

Project Goals

Goal I: Data Provenance and Trusted Data

Data in center in the IoT

- Rely and trust the collected data
- Provide mechanisms to verify the data source and data integrity even when single devices are under attack

Goal II: Distributed security management and attack detection

Attacks and device compromise in the IoT

- Cannot be prevented (big, heterogenous, distributed)
- Distributed anomaly detection and mitigation (including all devices, from small to big and new to old legacy)

Goal III: Interdisciplinary educational outreach

Understanding scenarios in the IoT

- IoT security is complex, broad, and not yet well understood by actors (buzz word)
- Outreach across disciplines and sectors to contribute to a secure adoption of the IoT in society

Project Goals

Goal I: Data Provenance and Trusted Data

Data in center in the IoT

- Rely and trust the collected data
- Provide mechanisms to verify the data source and dat

Goal II: Distributed security management and attack detection

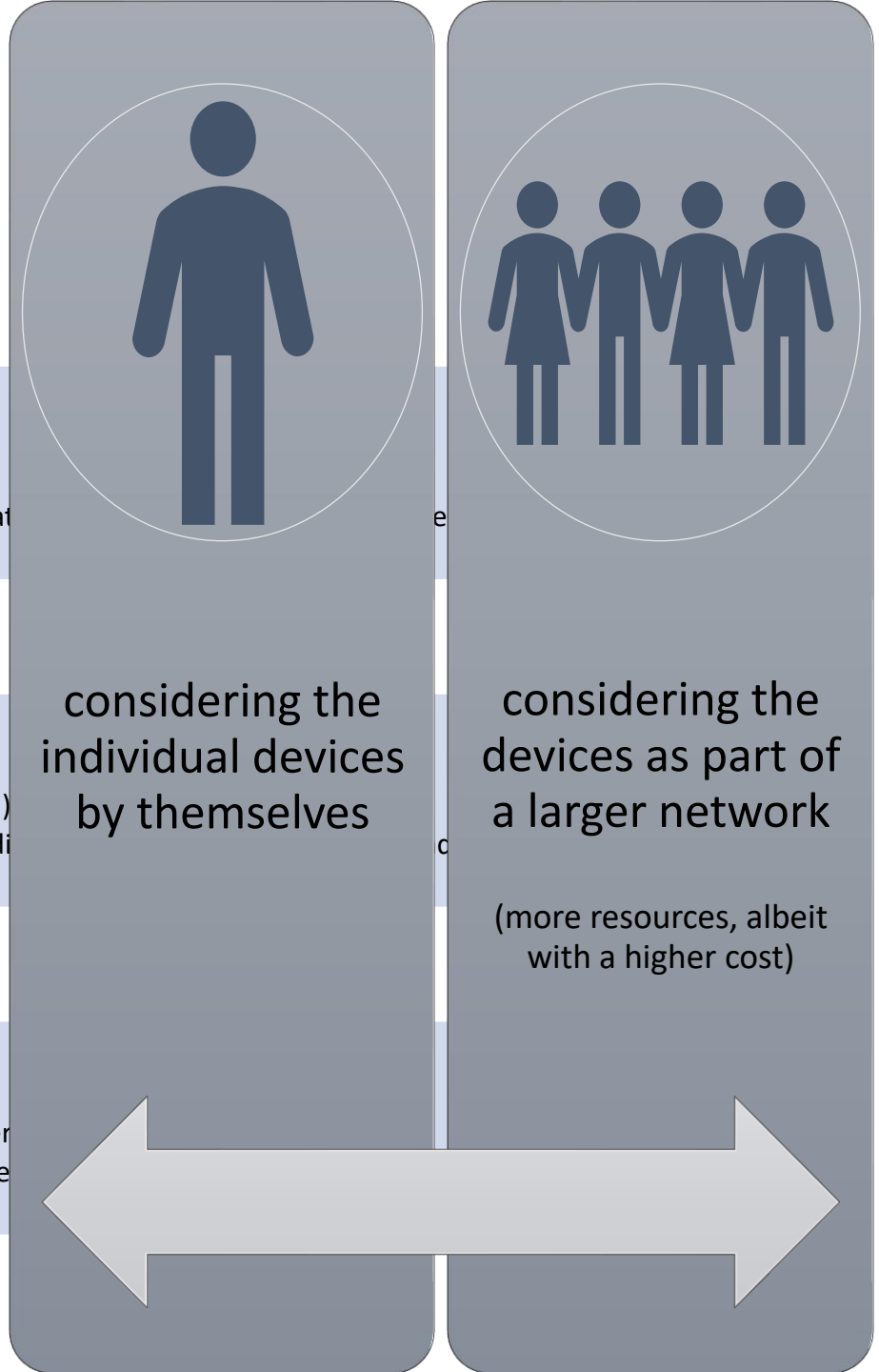
Attacks and device compromise in the IoT

- Cannot be prevented (big, heterogenous, distributed)
- Distributed anomaly detection and mitigation (includi

Goal III: Interdisciplinary educational outreach

Understanding scenarios in the IoT

- IoT security is complex, broad, and not yet well under
- Outreach across disciplines and sectors to contribute



Cloud / Fog / IoT

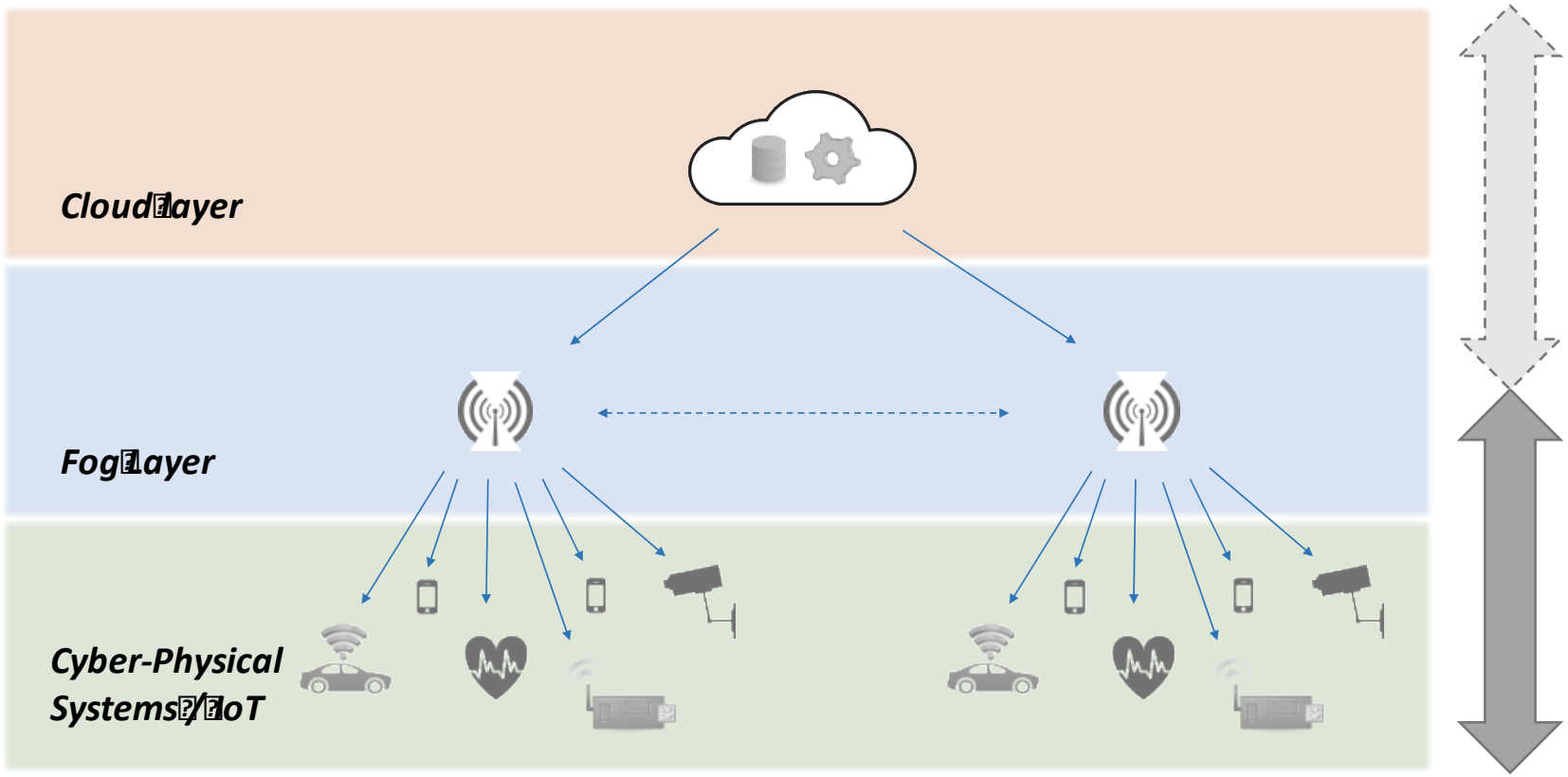


Image: Charalampos Stylianopoulos

Research activities

Research Output

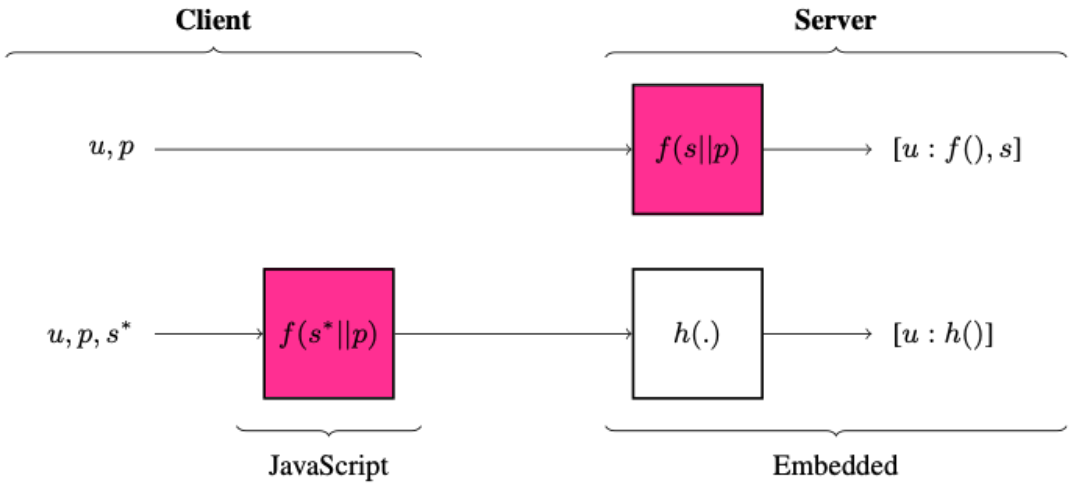
Doctoral & Licentiate theses

- Self-Reliance for the Internet of Things: Blockchains and Deep Learning on Low-Power IoT Devices, Doctoral thesis, 2022
- Enhancing Trust in Devices and Transactions of the Internet of Things, Licentiate thesis, 2020
- Process-Aware Defenses for Cyber-Physical Systems, Doctoral thesis, 2020
- Hardware-Aware Algorithm Designs for Efficient Parallel and Distributed Processing, Doctoral thesis, 2019

Hardening individual devices	Clipaha: A Scheme to Perform Password Stretching on the Client, 2023
	Performance of Secure Boot in Embedded Systems, 2019
Provenance and Trusted Data (in case of compromise)	TinyEVM: Off-Chain Smart Contracts on Low-Power IoT Devices, 2020
	IoTLogBlock: Recording Off-line Transactions of Low-Power IoT Devices Using a Blockchain, 2019
Attack Detection for IoT	A Framework for Determining Robust Context-Aware Attack-Detection Thresholds for Cyber-Physical Systems, 2021
	Spectra: Detecting Attacks on In-Vehicle Networks through Spectral Analysis of CAN-Message Payloads, 2021
	A probe into process-level attack detection in industrial environments from a side-channel perspective, 2019
	Co-Evaluation of Pattern Matching Algorithms on IoT Devices with Embedded GPUs, 2019
Deep Learning Classifiers for Attack Detection	Performance of deep neural networks on low-power IoT devices, 2021
	MicroTL: Transfer Learning on Low-Power IoT Devices, 2022
	MiniLearn: On-Device Learning for Low-Power IoT Devices, 2021
Understanding a collection of IDS	Towards an information-theoretic framework of intrusion detection for composed systems and robustness analyses, 2022

Hardening of the device

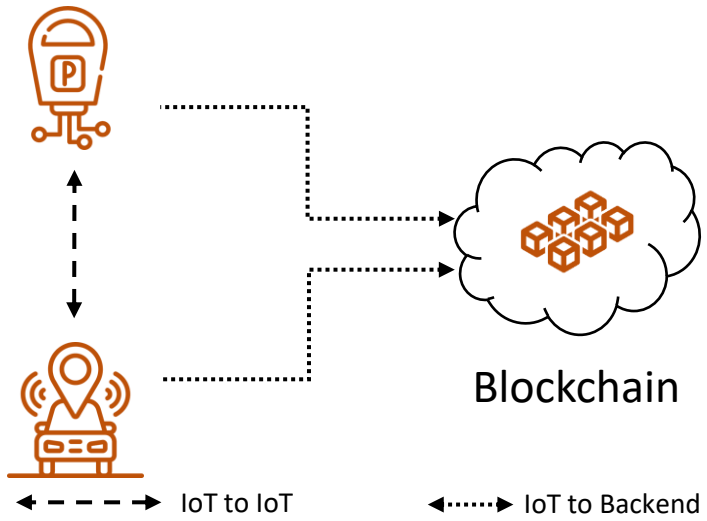
- Background
  - Many compromises from password weaknesses & breaches
  - New powerful algorithms (Argon2) → but incompatible with IoT
- Developed “Clipaha”
  A Scheme to Perform Password Stretching on the Client
  - Server-side implementation for embedded system (ESP8266)



Complex hashing function (eg, Argon2)
→ memory and runtime

Data in center
Provenance and Trusted Data

- Three main challenges for IoT:
  - Bandwidth overhead
  - Energy consumption
  - **No access to sensors & actuators**



- Contributions
  - Combined blockchains, smart contracts, and off-line contract signing protocols on IoT devices.
    - Ethereum Virtual Machine (EVM) on the IoT device
    - ***IoT specific opcodes*** – for sensor readings and actuators as part of IoT transactions
    - Off-chain smart contract
    - On-chain commit(s) on blockchain

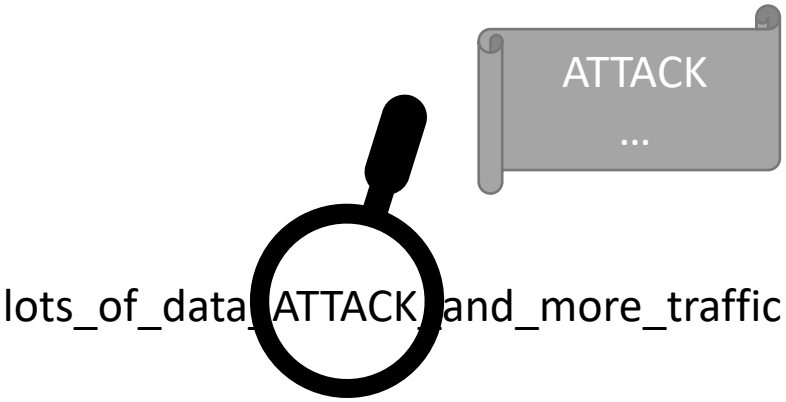
Moving intrusion detection algorithm to IoT devices

- Cloud
- Fog
- IoT

Types of Intrusion Detection Systems

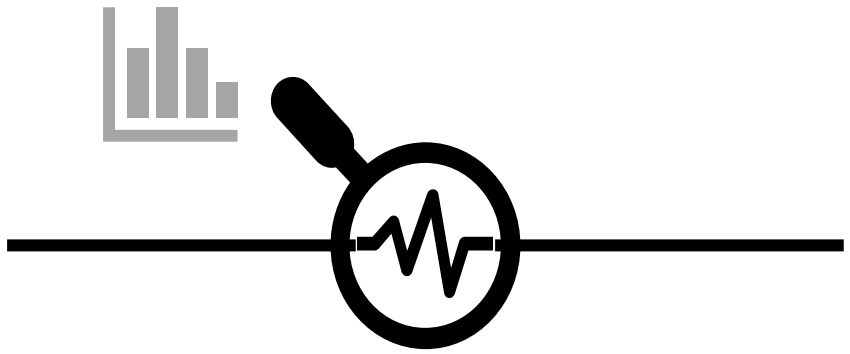
Knowledged-based

- Often focused on known attacks
- Encoded as “signatures”
- Example: Snort



Behavior-based

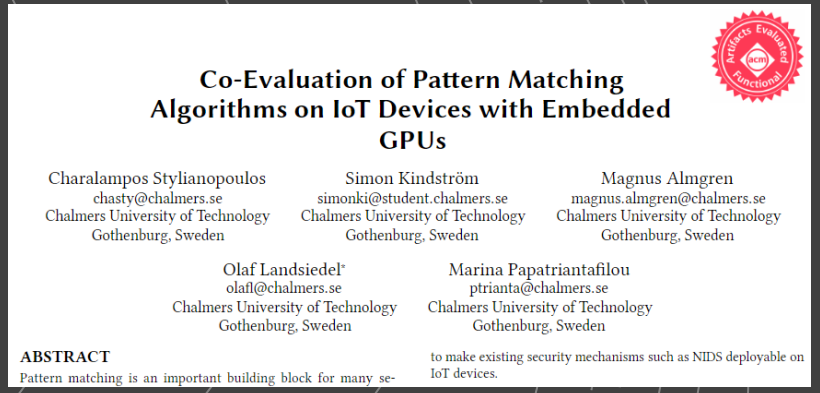
- Detects “anomlies” as something outside normal behavior
- Learn from data
- False alarms! → ICS system (M2M)



Acronym	Algorithm	Family	Code	Effort	Comment
AC (CPU)	Aho-Corasick [1]	state machine	Snort repository [34]	low	CPU baseline, used in Snort
DFC (CPU)	Direct Filter Classification [10]	filter	[10, 37]	low	CPU baseline (filter-based)
PFAC (GPU)	Parallel Failureless AC [22]	state machine	[4]	medium	code required some work to adapt to benchmark
DFC (GPU)	Direct Filter Classification [37]	filter	[37]	high	our own implementation (the first implementation of DFC for the GPU)
HYBRID (GPU)	Mix of DFC and PFAC	mixed	this paper	high	our own design: a hybrid combining DFC and PFAC, implemented for the GPU

IDS on IoT-architecture: Effectiveness of algorithms and optimizations

- Algorithms & Architectures
  - AC (CPU)
  - DFC (CPU)
  - PFAC (GPU)
  - DFC (GPU)



Co-Evaluation of Pattern Matching Algorithms on IoT Devices with Embedded GPUs

Charalampos Stylianopoulos
chasty@chalmers.se
Chalmers University of Technology
Gothenburg, Sweden

Simon Kindström
simonki@student.chalmers.se
Chalmers University of Technology
Gothenburg, Sweden

Magnus Almgren
magnus.almgren@chalmers.se
Chalmers University of Technology
Gothenburg, Sweden

Olaf Landsiedel*
olafl@chalmers.se
Chalmers University of Technology
Gothenburg, Sweden

Marina Papatriantafilou
ptrianta@chalmers.se
Chalmers University of Technology
Gothenburg, Sweden

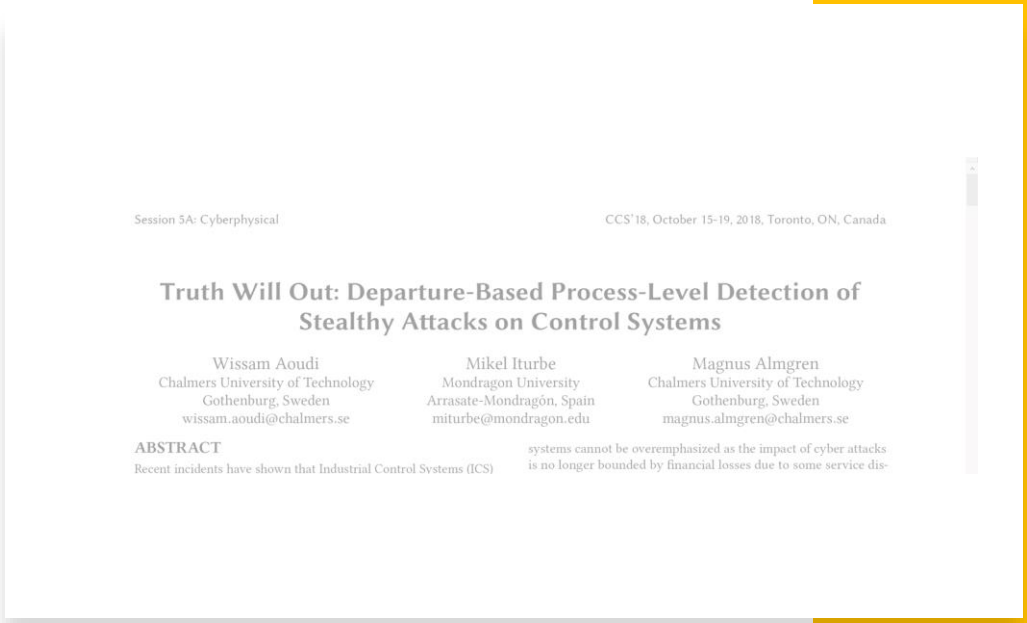
ABSTRACT

Pattern matching is an important building block for many se-

to make existing security mechanisms such as NIDS deployable on IoT devices.

Anomaly detection

- Developed for ICS
- Presented at ACM CCS fall 2018.
- Starting point for RIOT
  - Suitable also for IoT in some circumstances?
- Successfully changed and ported algorithm to work on very constrained devices



Session 5A: Cyberphysical CCS'18, October 15-19, 2018, Toronto, ON, Canada

Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems

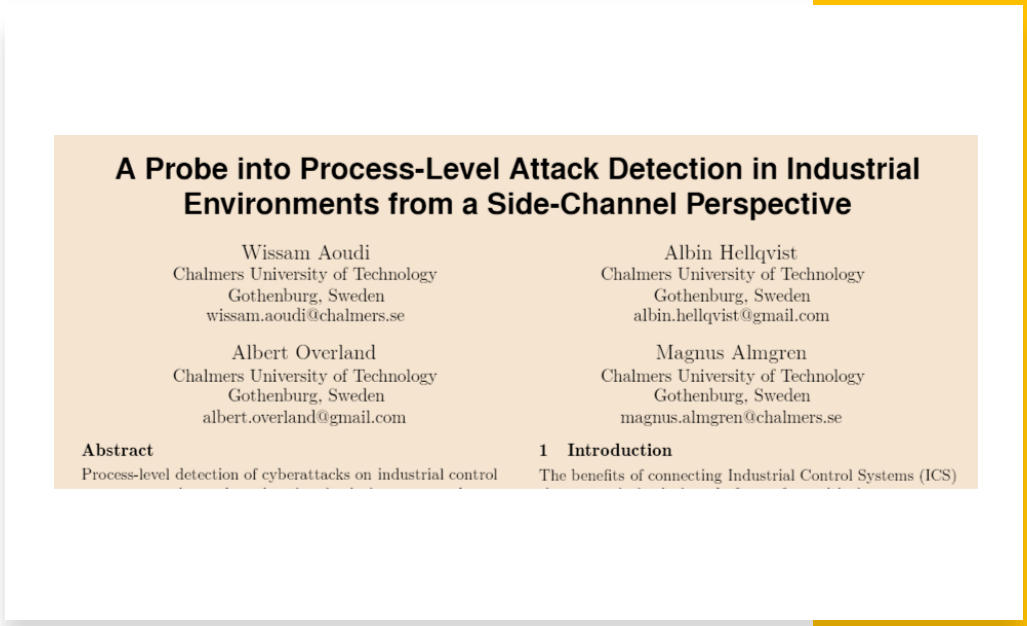
Wissam Aoudi
Chalmers University of Technology
Gothenburg, Sweden
wissam.aoudi@chalmers.se

Mikel Iturbe
Mondragon University
Arrasate-Mondragón, Spain
miturbe@mondragon.edu

Magnus Almgren
Chalmers University of Technology
Gothenburg, Sweden
magnus.almgren@chalmers.se

ABSTRACT

Recent incidents have shown that Industrial Control Systems (ICS) systems cannot be overemphasized as the impact of cyber attacks is no longer bounded by financial losses due to some service dis-



A Probe into Process-Level Attack Detection in Industrial Environments from a Side-Channel Perspective

Wissam Aoudi
Chalmers University of Technology
Gothenburg, Sweden
wissam.aoudi@chalmers.se

Albin Hellqvist
Chalmers University of Technology
Gothenburg, Sweden
albin.hellqvist@gmail.com

Albert Overland
Chalmers University of Technology
Gothenburg, Sweden
albert.overland@gmail.com

Magnus Almgren
Chalmers University of Technology
Gothenburg, Sweden
magnus.almgren@chalmers.se

Abstract

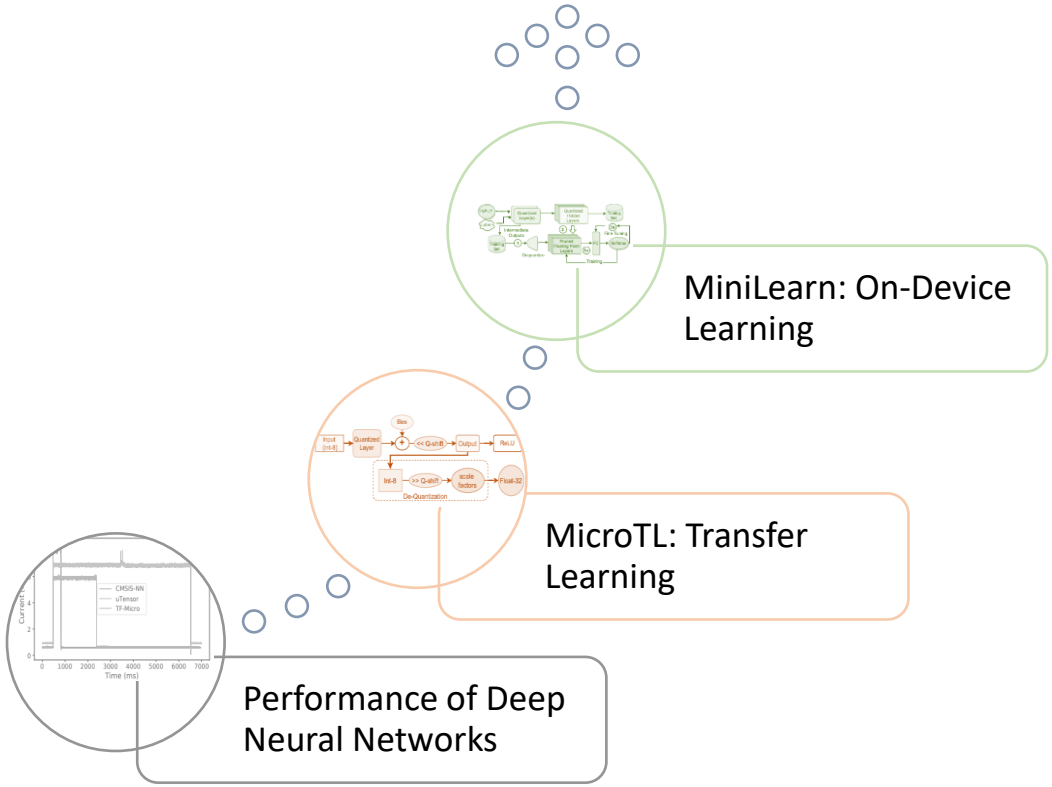
Process-level detection of cyberattacks on industrial control

1 Introduction

The benefits of connecting Industrial Control Systems (ICS)

Using more powerful classifiers

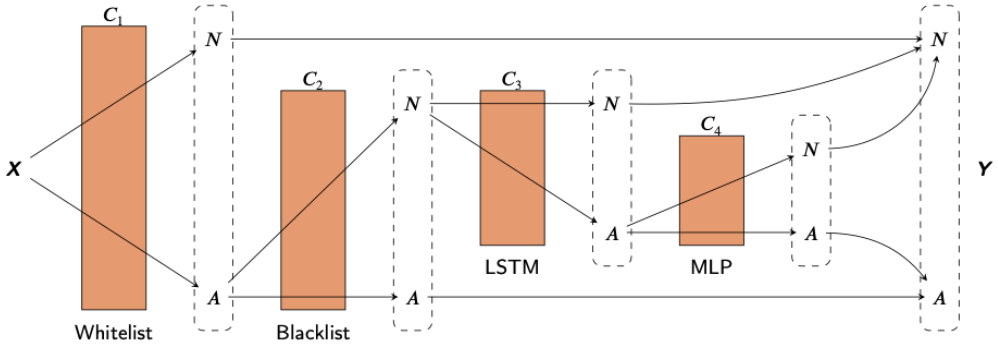
- Paradigm-shift in AI
  - RIOT context: Machine Learning to create ***powerful classifiers***
- Opportunities & Challenges
  - Powerful in the cloud
  - Significant challenges to bring to IoT: energy, CPU, memory
  - Even more difficult for training (!)



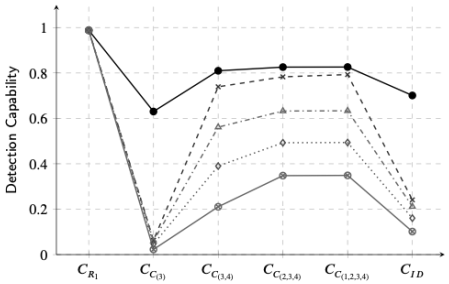
Composed Intrusion Detection Systems

- IoT is a collection of devices
- Reduction of false alarms at low base-rates
- Resilience against adaptive adversaries.
- Attribution of overall system performance to its individual components
  → fine tune parameters

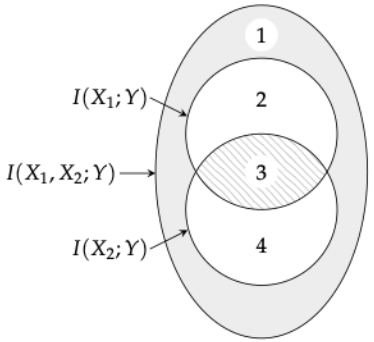
  (optimising the operation point of each component individually does not maximise the overall system performance)



$$C_{ID} = \frac{I(X,Y)}{H(X)} = \frac{H(X) - H(X|Y)}{H(X)}$$



Composed Intrusion Detection Systems

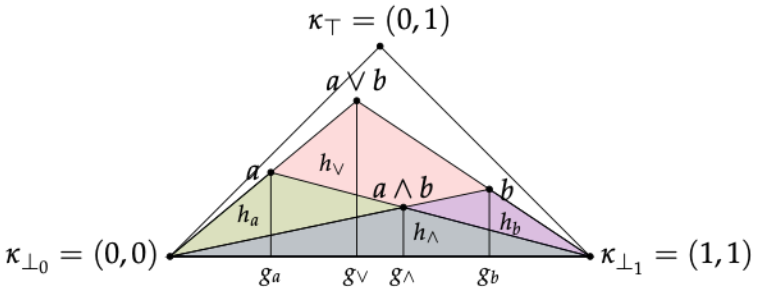


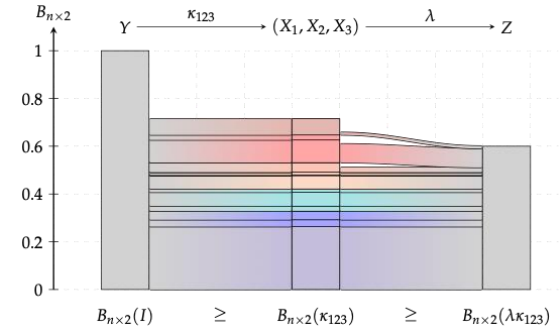
Synergy

Unique X_1

Redundancy

Unique X_2





What is a good measure for robustness of intrusion detection systems?

Approach using Partial Information Decomposition and Information Theory.

Challenge: Define a valuation over partial orders/lattices.