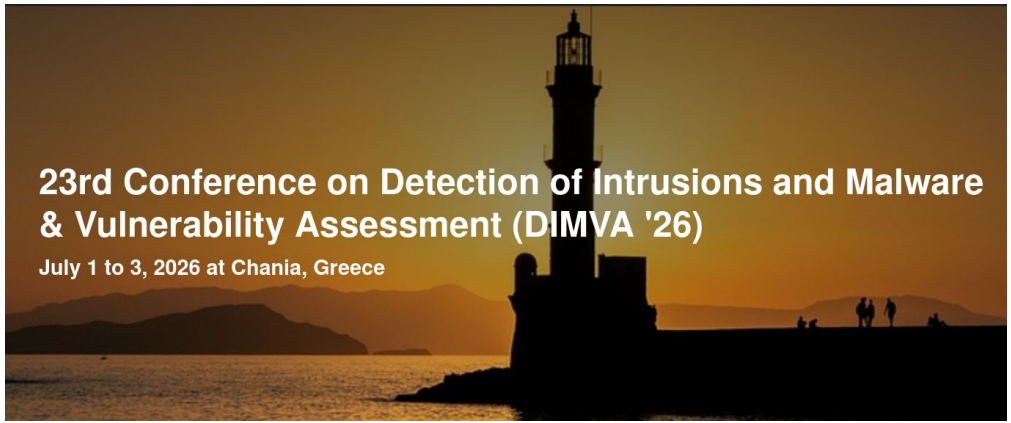
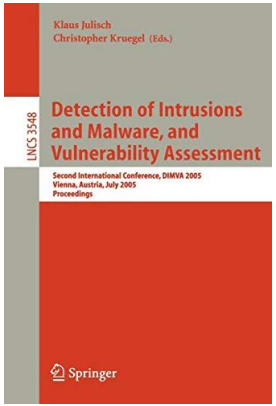
# IoT Threat Assessment with the AttackDefense Framework




Daniele Antonioli
EURECOM (FR)

# Threat Assessment and DIMVA




- **Threat assessment**
  - *Identify*, *prioritize*, and *remediate* threats
- **Core topic at DIMVA!**
  - *25: Sourcerer: Channeling the void* [ref]
  - *24: Acoustic Side-Channel Attacks on a Computer Mouse* [ref]
  - *23: White-Box Concealment Attacks Against Anomaly Detectors for Cyber-Physical Systems* [ref]
- **Talk on IoT Threat Assessment**
  - AttackDefense Framework (ADF) [TECS'25]

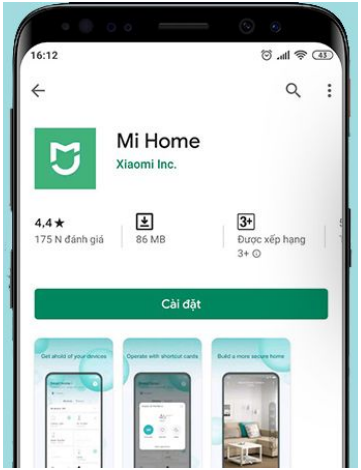
# Talk Outline

1. Emerging IoT Threats
2. Threat Modeling
3. AttackDefense Framework (ADF)
4. ADF Evaluation on Crypto Wallet
5. Future of ADF and Conclusion

# Emerging IoT Threats

# Internet of Things (IoT)



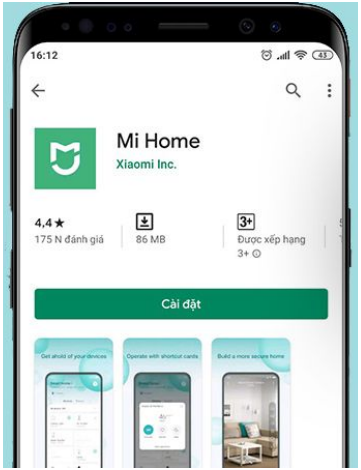



Dongles, EV chargers, E-scooters, home automation, …

More embedded computers than laptops, desktop, and servers!

# IoT Threat Assessment is Essential






**IoT is a huge attack surface**: hw, sw, fw, supply chain, …

**Large-scale impact**: security, privacy, safety

# IoT Threats: **User Authentication**

**CTRAPS: CTAP Client Impersonation and API Confusion on FIDO2**


Marco Casagrande
*Department of Digital Security*
*EURECOM*
*Sophia Antipolis, France*
*marco.casagrande@eurecom.fr*

Daniele Antonioli
*Department of Digital Security*
*EURECOM*
*Sophia Antipolis, France*
*daniele.antonioli@eurecom.fr*

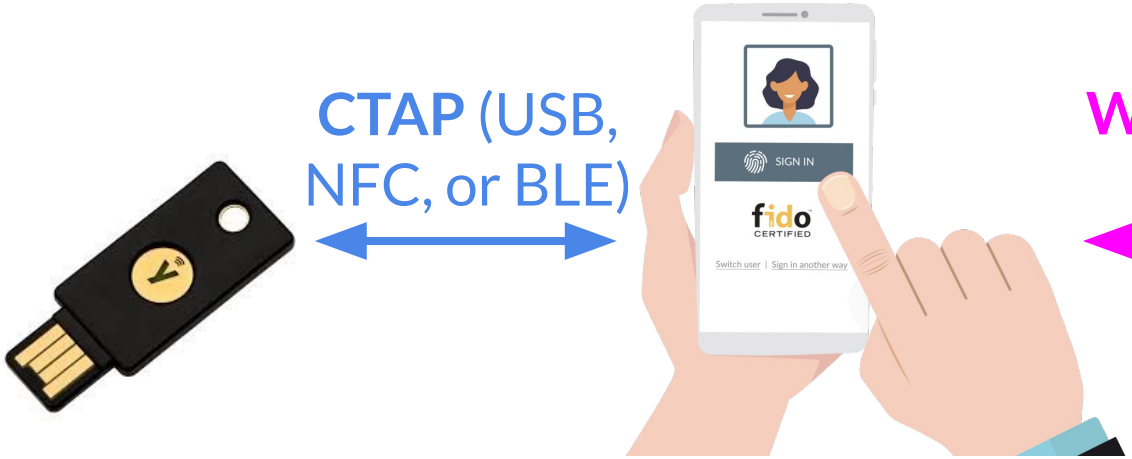


Venice, June 30 - July 4, 2025

10th IEEE European Symposium on Security and Privacy

# FIDO2 Authentication (2FA, 1FA)

**Client**

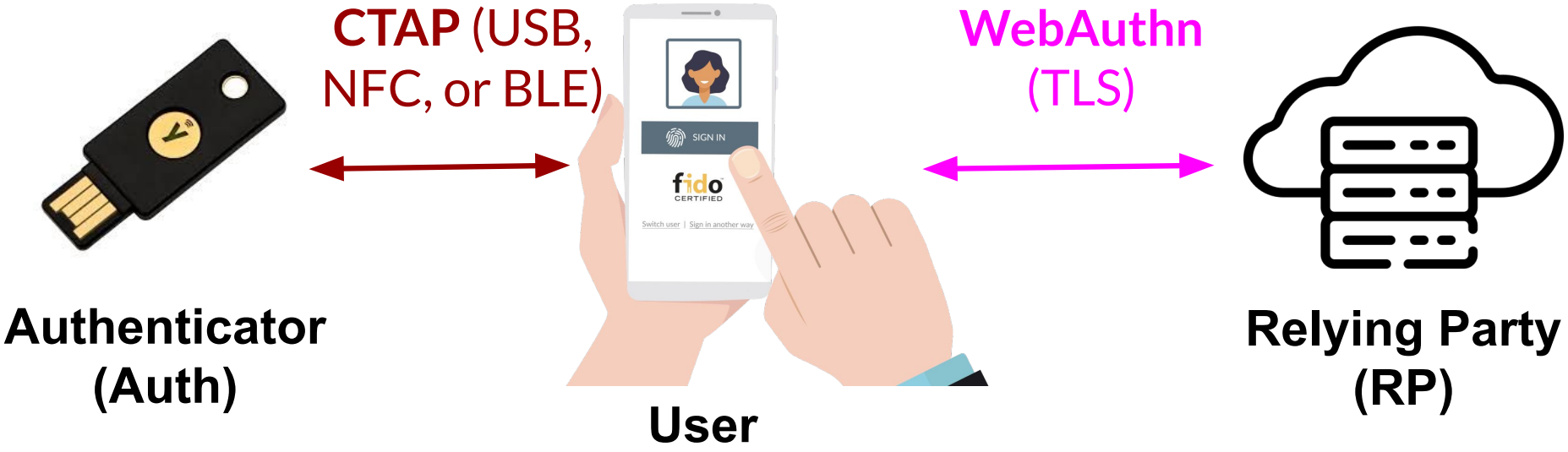



**Authenticator (Auth)**

**User**

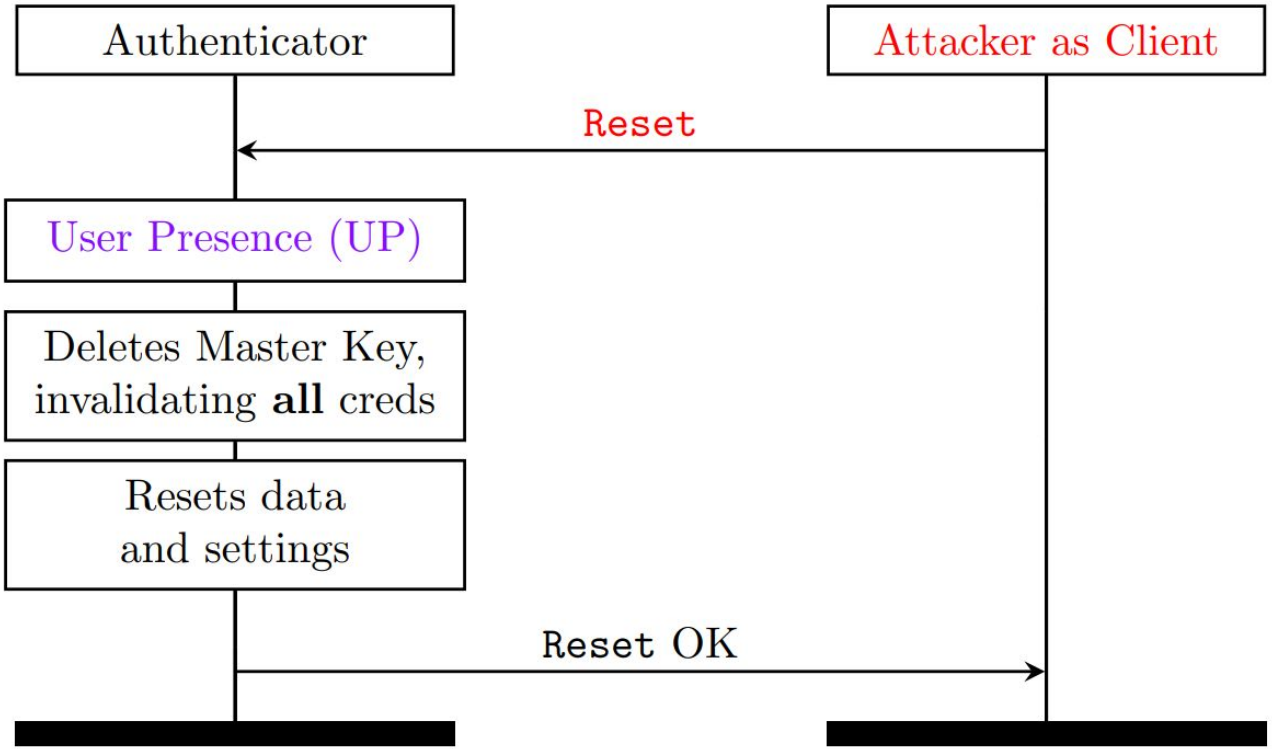
**Relying Party (RP)**

# CTRAPS threats on FIDO2 [ref]




**Impersonation and MitM threats on CTAP?**

# CTRAPS $CI_1$ Attack: Factory Reset Auth via NFC



# IoT Threats: **Electric Vehicles**

**EmuOCPP: Effective and Scalable OCPP Security and Privacy Testing**


Soumaya Boussaha
*SAP, EURECOM, Biot, France*
*soumaya.boussaha@sap.com*

Victor Fresno Gómez
*EURECOM, UPM, Madrid, Spain*
*victorfresno@live.com*

Thomas Barber
*SAP SE, Walldorf, Germany*
*thomas.barber@sap.com*

Daniele Antonioli
*EURECOM, Biot, France*
*daniele.antonioli@eurecom.fr*


OCPP

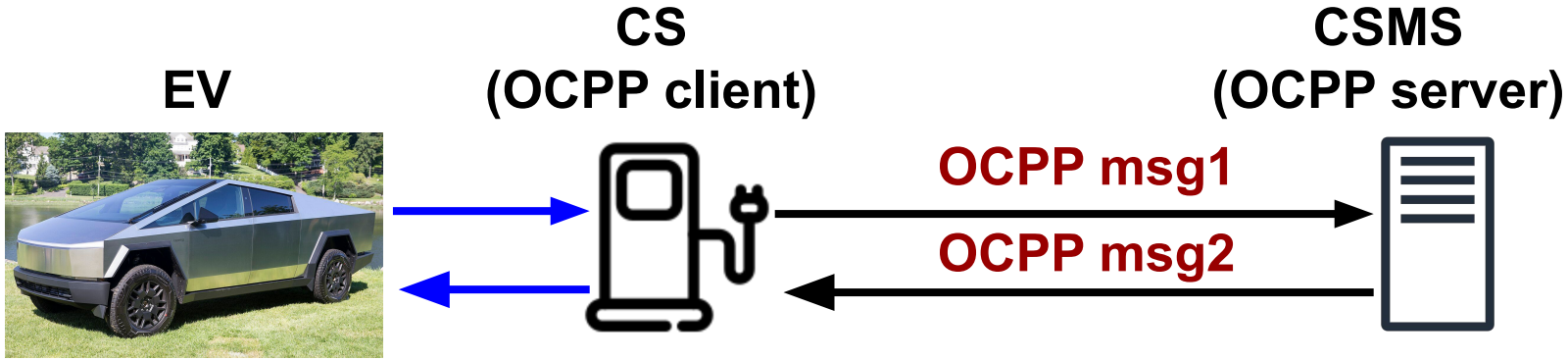
VehicleSec '25

3rd USENIX Symposium on Vehicle Security and Privacy

AUGUST 11–12, 2025
SEATTLE, WA, USA
Co-located with USENIX Security '25

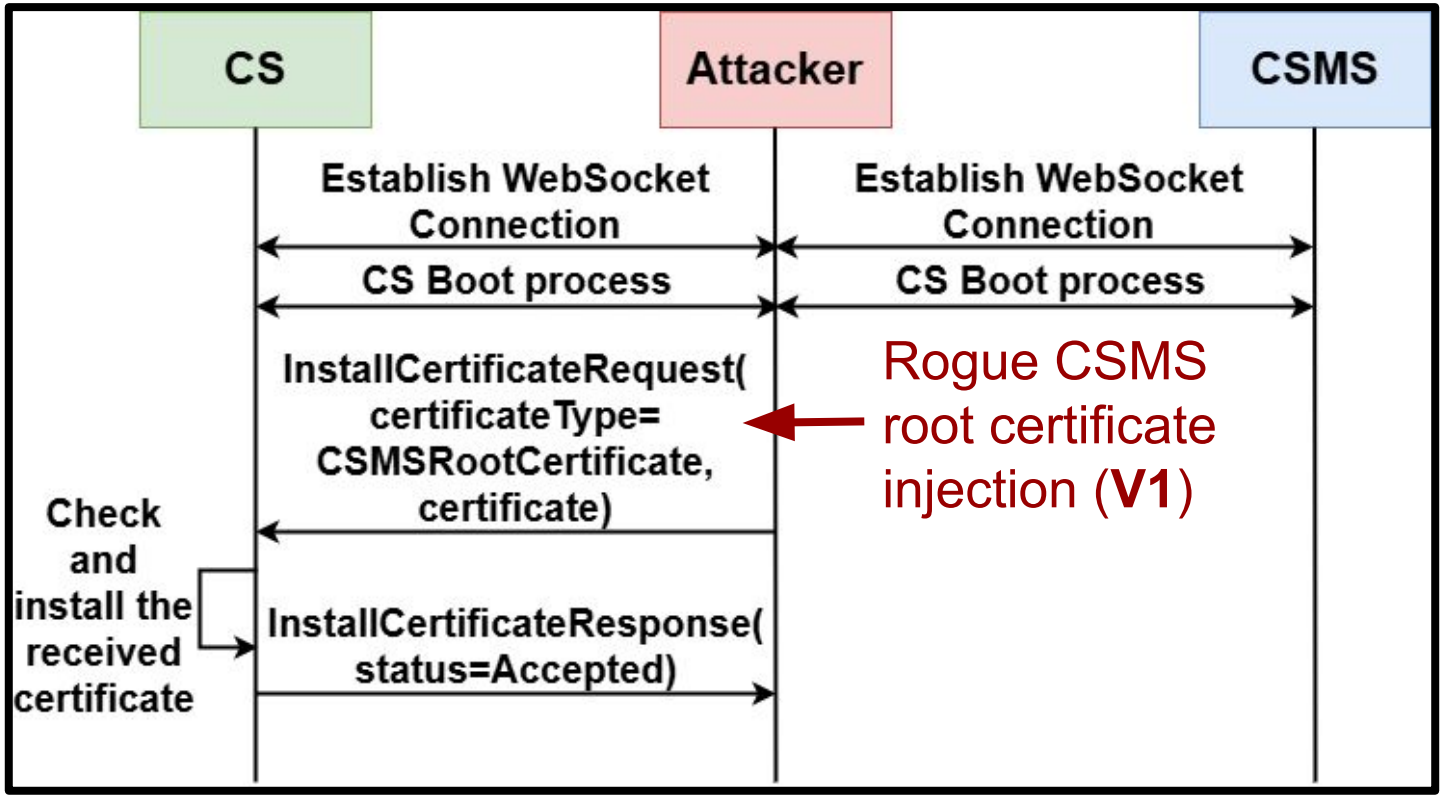
DEFCON SINGAPORE

# EmuOCPP threats on OCPP [ref]




**Impersonate/MitM CS and CSMS via OCPP?**

# M2: OCPP MitM via Insecure SP2 Upgrade



# So many IoT Threats → Threat Modeling!

More uncovered IoT threats: E-Trojans, MaDoS, BLERP, …

LLM and agents speed up (Glasswing, …)

**IoT is and will be vulnerable!**

**Threat modeling** to assess IoT vulns **quickly**, **at scale** with **low-cost**

# Threat Modeling

# Threat Modeling Core Questions (Shostack)

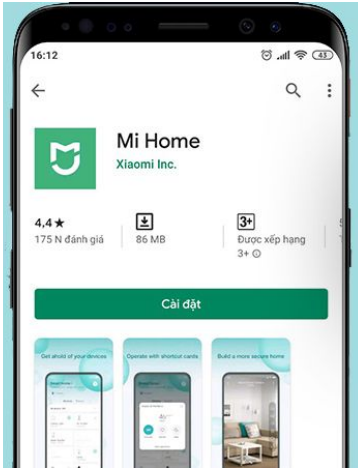
- What are we working on?
- What can go wrong?
- What are we going to do about that?
- Did we do a good enough job?

# Threat Modeling Phases

| | |
|---|---|
| **1. System model** | Data Flow Diagram, Sequence Diagram, … |
| **2. Threat identif.** | STRIDE, LINDDUN, Attack trees, … |
| **3. Risk score** | CVSSv2, CVSSv3, … |
| **4. Defense plan** | Tests, report, mitigations, patches, … |

# IoT Threat Modeling? An Open Problem!

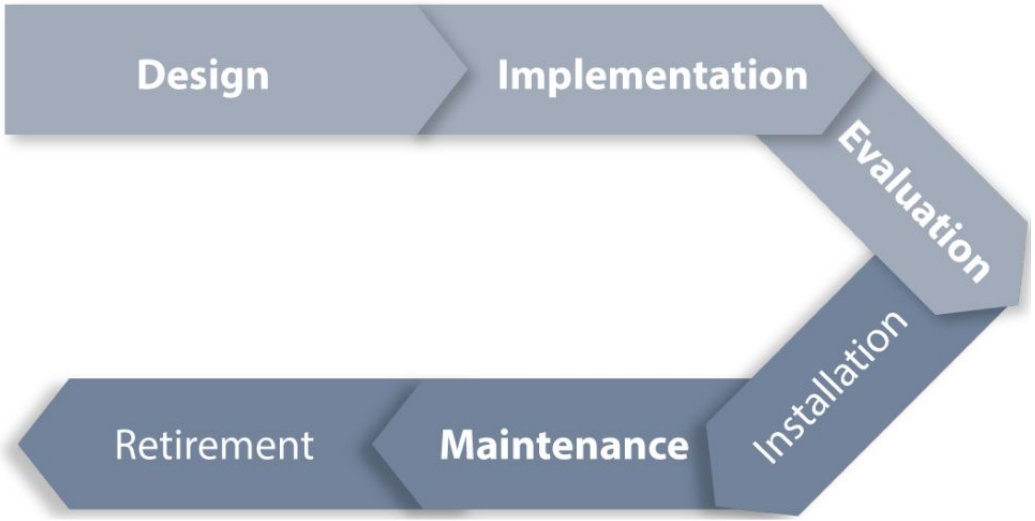





**New surfaces:** hardware, firmware, supply, sensors, actuators, …

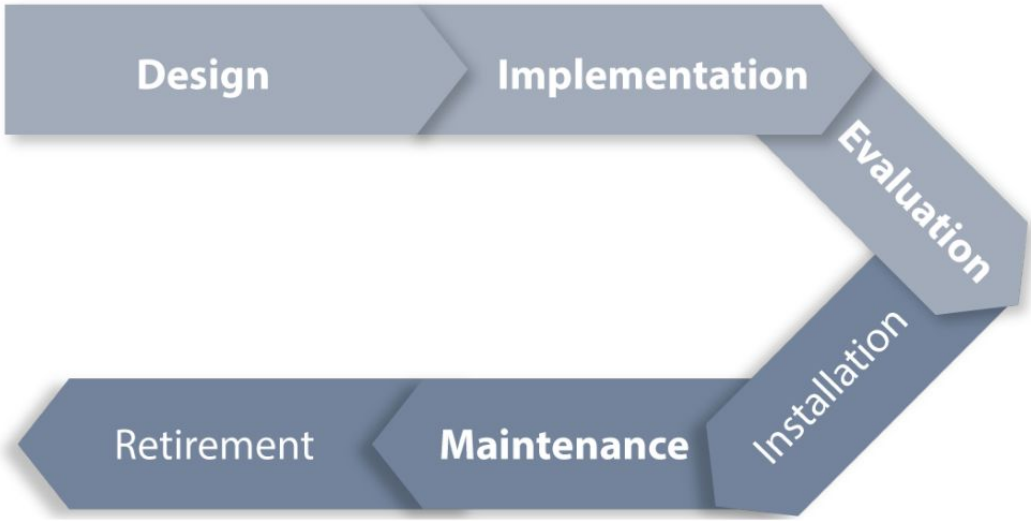
**New attacks:** Side channel, Fault injection, Supply chain, Wireless, Tracking, …

# IoT Device Lifecycle




IoT device must be secure from its inception until it is disposed → **Secure IoT Lifecycle and Supply Chain**

# IoT Lifecycle Threat Modeling? **Nada!**




**Jim Allchin, 2006.** It's too late if you find problems in **testing**. And it's too late if security holes make it into **a build** of the software.

# Solution: **AttackDefense Framework** [TECS25]

**AttackDefense Framework (ADF): Enhancing IoT Devices and Lifecycles Threat Modeling**


TOMMASO SACCHETTI, Digital Security, EURECOM, Sophia Antipolis, France
MARTON BOGNAR, KU Leuven, Leuven, Belgium
JESSE DE MEULEMEESTER, KU Leuven, Leuven, Belgium
BENEDIKT GIERLICHS, KU Leuven, Leuven, Belgium
FRANK PIESSENS, KU Leuven, Leuven, Belgium
VOLODYMYR BEZSMERTNYI, NXP, Hamburg, Germany
MARIA CHIARA MOLTENI, Security Pattern, Mazzano, Italy
STEFANO CRISTALLI, Security Pattern, Mazzano, Italy
ARIANNA GRINGIANI, Security Pattern, Mazzano, Italy
OLIVIER THOMAS, Texplained, Valbonne, France
DANIELE ANTONIOLI, Digital Security, EURECOM, Sophia Antipolis, France



ACM Transactions on Embedded Computing Systems


# ADF

# ADF 7 Requirements (genius of the AND)

1. Attack **and** Defense
2. Security **and** Privacy
3. Hardware **and** Software
4. Product **and** Lifecycle
5. Fine **and** Coarse grain
6. Reusable **and** Updatable
7. Machine **and** Human friendly

# ADF Workhorse: **AD Object**

Data structure to model a threat.

Multi-dimensional: attack, defense, surface, …

Generic: hw, sw, …

PL agnostic: JSON, YAML, Python, …

```yaml
ad_name:
  # Primary fields
  a: attack
  d:
    policy1: [mech1, mech2]
    policy2: [mech1, mech2]
    ...
  surf: [surf, subsurf, subsubsurf, ...]
  vect: [vector1, vector2, ...]
  model: [model1, model2, ...]
  tag: [tag1, tag2, ...]
  # Optional fields
  risk: [score1, score2, ...]
  year: 2023
  cve: ["123", "456", ...]
  cwe: ["123", "456", ...]
  capec: ["123", "456", ...]
  vref: ["vendor-ref1", ...]
  ...: ...
```

# AD Object: ad_name

**ad_name**: unique string describing a threat.

Eg: knob_bc, krack_wifi, spectre_v1, …

```
ad_name:
  # Primary fields
  a: attack
  d:
    policy1: [mech1, mech2]
    policy2: [mech1, mech2]
    ...
  surf: [surf, subsurf, subsubsurf, ...]
  vect: [vector1, vector2, ...]
  model: [model1, model2, ...]
  tag: [tag1, tag2, ...]
  # Optional fields
  risk: [score1, score2, ...]
  year: 2023
  cve: ["123", "456", ...]
  cwe: ["123", "456", ...]
  capec: ["123", "456", ...]
  vref: ["vendor-ref1", ...]
  ...: ...
```

# AD Object primary fields: a

**a**: string describing an **attack** with an arbitrary level of abstraction (e.g., coarse-grained or fine-grained)

```
ad_name:
  # Primary fields
  a: attack
  d:
    policy1: [mech1, mech2]
    policy2: [mech1, mech2]
    ...
  surf: [surf, subsurf, subsubsurf, ...]
  vect: [vector1, vector2, ...]
  model: [model1, model2, ...]
  tag: [tag1, tag2, ...]
  # Optional fields
  risk: [score1, score2, ...]
  year: 2023
  cve: ["123", "456", ...]
  cwe: ["123", "456", ...]
  capec: ["123", "456", ...]
  vref: ["vendor-ref1", ...]
  ...: ...
```

# AD Object primary fields: d

**d**: dict modeling **defense strategies.**

A dict has a **abstract policy** string and a list of **concrete mechanisms** strings satisfying it.

```
ad_name:
  # Primary fields
  a: attack
  d:
    policy1: [mech1, mech2]
    policy2: [mech1, mech2]
    ...
  surf: [surf, subsurf, subsubsurf, ...]
  vect: [vector1, vector2, ...]
  model: [model1, model2, ...]
  tag: [tag1, tag2, ...]
  # Optional fields
  risk: [score1, score2, ...]
  year: 2023
  cve: ["123", "456", ...]
  cwe: ["123", "456", ...]
  capec: ["123", "456", ...]
  vref: ["vendor-ref1", ...]
  ...: ...
```

# AD Object primary fields: surf

**surf**: ordered list of strings describing the **attack target**

Each list element narrows down the attack surface.

```
ad_name:
  # Primary fields
  a: attack
  d:
    policy1: [mech1, mech2]
    policy2: [mech1, mech2]
    ...
  surf: [surf, subsurf, subsubsurf, ...]
  vect: [vector1, vector2, ...]
  model: [model1, model2, ...]
  tag: [tag1, tag2, ...]
  # Optional fields
  risk: [score1, score2, ...]
  year: 2023
  cve: ["123", "456", ...]
  cwe: ["123", "456", ...]
  capec: ["123", "456", ...]
  vref: ["vendor-ref1", ...]
  ...: ...
```

# AD Object primary fields: vect

**vect**: list of strings containing the **attack techniques**

Eg: downgrade, brute-force, replay, bof, fault, side chan, …

```
ad_name:
  # Primary fields
  a: attack
  d:
    policy1: [mech1, mech2]
    policy2: [mech1, mech2]
    ...
  surf: [surf, subsurf, subsubsurf, ...]
  vect: [vector1, vector2, ...]
  model: [model1, model2, ...]
  tag: [tag1, tag2, ...]
  # Optional fields
  risk: [score1, score2, ...]
  year: 2023
  cve: ["123", "456", ...]
  cwe: ["123", "456", ...]
  capec: ["123", "456", ...]
  vref: ["vendor-ref1", ...]
  ...: ...
```

# AD Object primary fields: model

**model**: list of strings with **attacker models** capable of performing the attack

Eg: remote, physical, proximity

```
ad_name:
  # Primary fields
  a: attack
  d:
    policy1: [mech1, mech2]
    policy2: [mech1, mech2]
    ...
  surf: [surf, subsurf, subsubsurf, ...]
  vect: [vector1, vector2, ...]
  model: [model1, model2, ...]
  tag: [tag1, tag2, ...]
  # Optional fields
  risk: [score1, score2, ...]
  year: 2023
  cve: ["123", "456", ...]
  cwe: ["123", "456", ...]
  capec: ["123", "456", ...]
  vref: ["vendor-ref1", ...]
  ...: ...
```

# AD Object primary fields: tag

**tag**: list of strings storing useful **metadata**

Eg: AD type, S&P tradeoffs, …

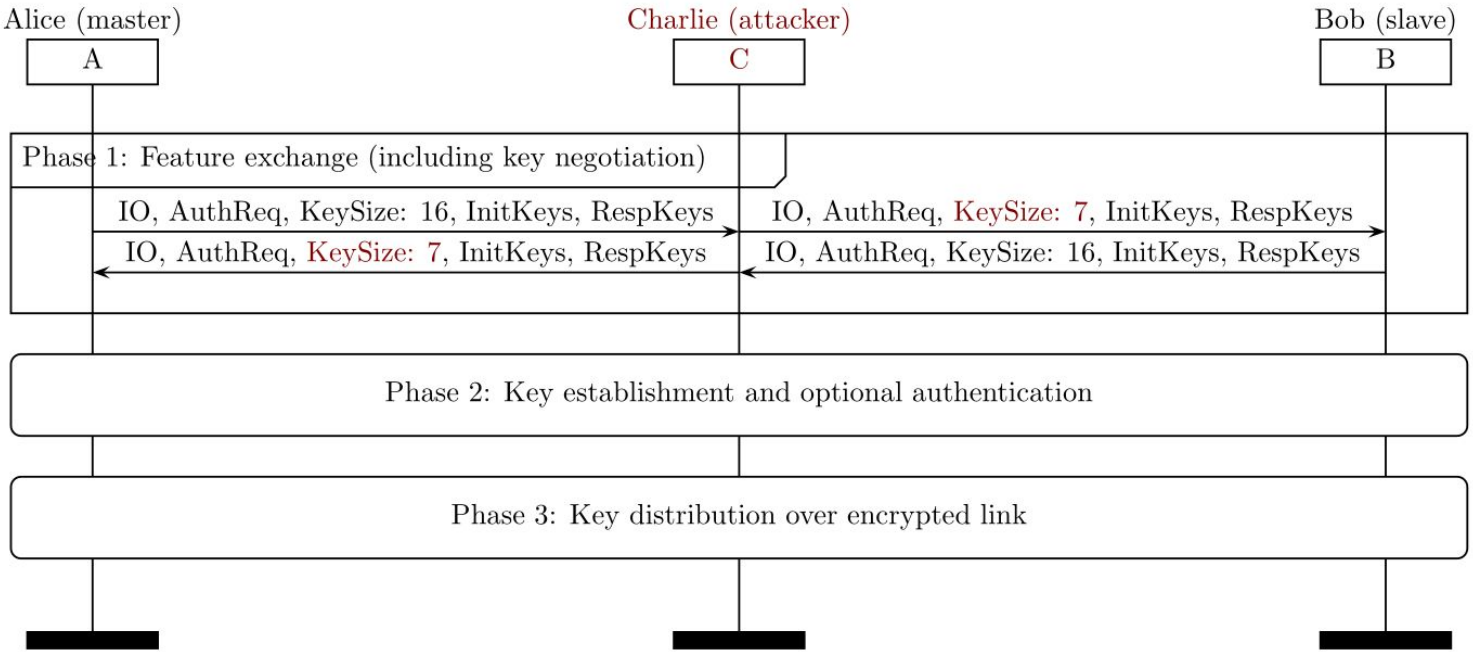
```
ad_name:
  # Primary fields
  a: attack
  d:
    policy1: [mech1, mech2]
    policy2: [mech1, mech2]
    ...
  surf: [surf, subsurf, subsubsurf, ...]
  vect: [vector1, vector2, ...]
  model: [model1, model2, ...]
  tag: [tag1, tag2, ...]
  # Optional fields
  risk: [score1, score2, ...]
  year: 2023
  cve: ["123", "456", ...]
  cwe: ["123", "456", ...]
  capec: ["123", "456", ...]
  vref: ["vendor-ref1", ...]
  ...: ...
```

# AD Object optional fields

**Optional** and user extensible **fields** like **year**, **cve**, **cwe**, **capec**, **vref**, …

```
ad_name:
  # Primary fields
  a: attack
  d:
    policy1: [mech1, mech2]
    policy2: [mech1, mech2]
    ...
  surf: [surf, subsurf, subsubsurf, ...]
  vect: [vector1, vector2, ...]
  model: [model1, model2, ...]
  tag: [tag1, tag2, ...]
  # Optional fields
  risk: [score1, score2, ...]
  year: 2023
  cve: ["123", "456", ...]
  cwe: ["123", "456", ...]
  capec: ["123", "456", ...]
  vref: ["vendor-ref1", ...]
  ...: ...
```

# Eg: AD for KNOB Attack on BLE [ref]



# Eg: AD for KNOB Attack on BLE [ref]

```
knob_ble:
  a: KNOB entropy downgrade attack on BLE pairing
  d:
    Mutually auth entropy negotiation: [Auth entropy with BLE pairing key]
    High key entropy: [Disallow entropy values lower than 16]
  surf: [BLE, Pairing, Entropy negotiation]
  vect: [Entropy downgrade, Key brute force]
  model: [Proximity, MitM]
  tag: [Protocol, SMP]
  risk: [cvss3_high, cvss2_medium]
  year: 2019
  cve: ["9506"]
  cwe: ["310", "327"]
  capec: ["668"]
```

# Our ADs on GitHub!


https://github.com/francozappa/adf/tree/main/catalog

# AD homework for you: `bleed.yaml`

```
cd; mkdir ads; cd ads
```

```
touch bleed.yaml
```

Fill the files with ADs modeling **bleed-attacks (with logos)**

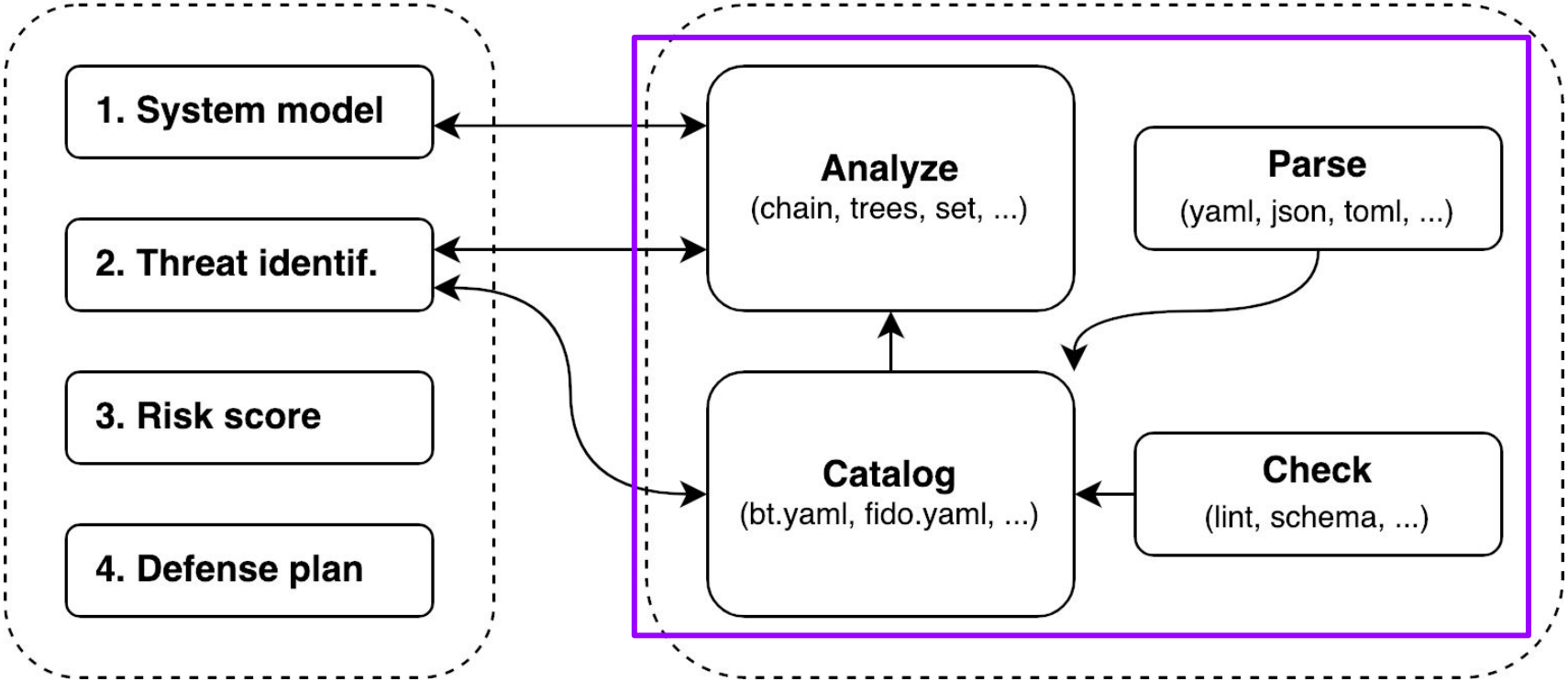
Send a pull request to here



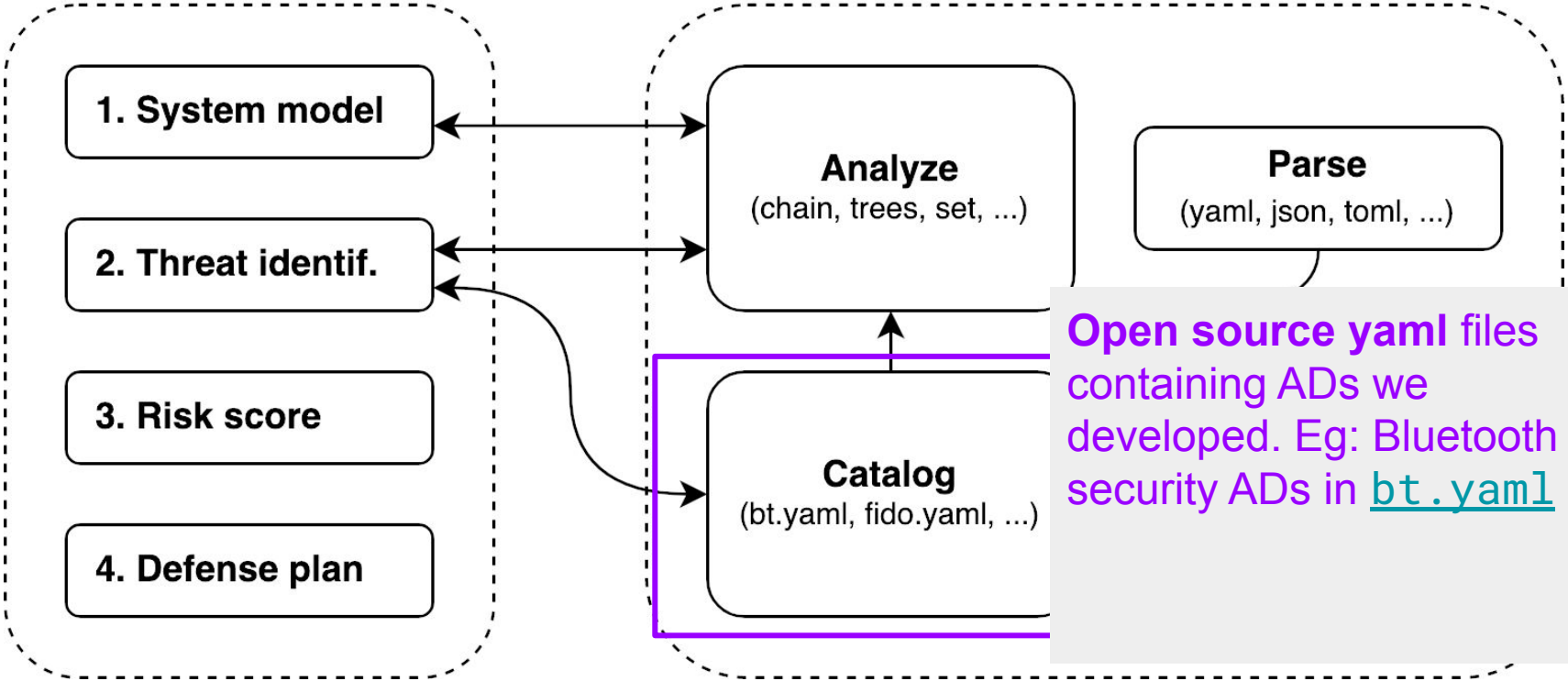



# ADF Components

# AttackDefense Framework Block Diagram

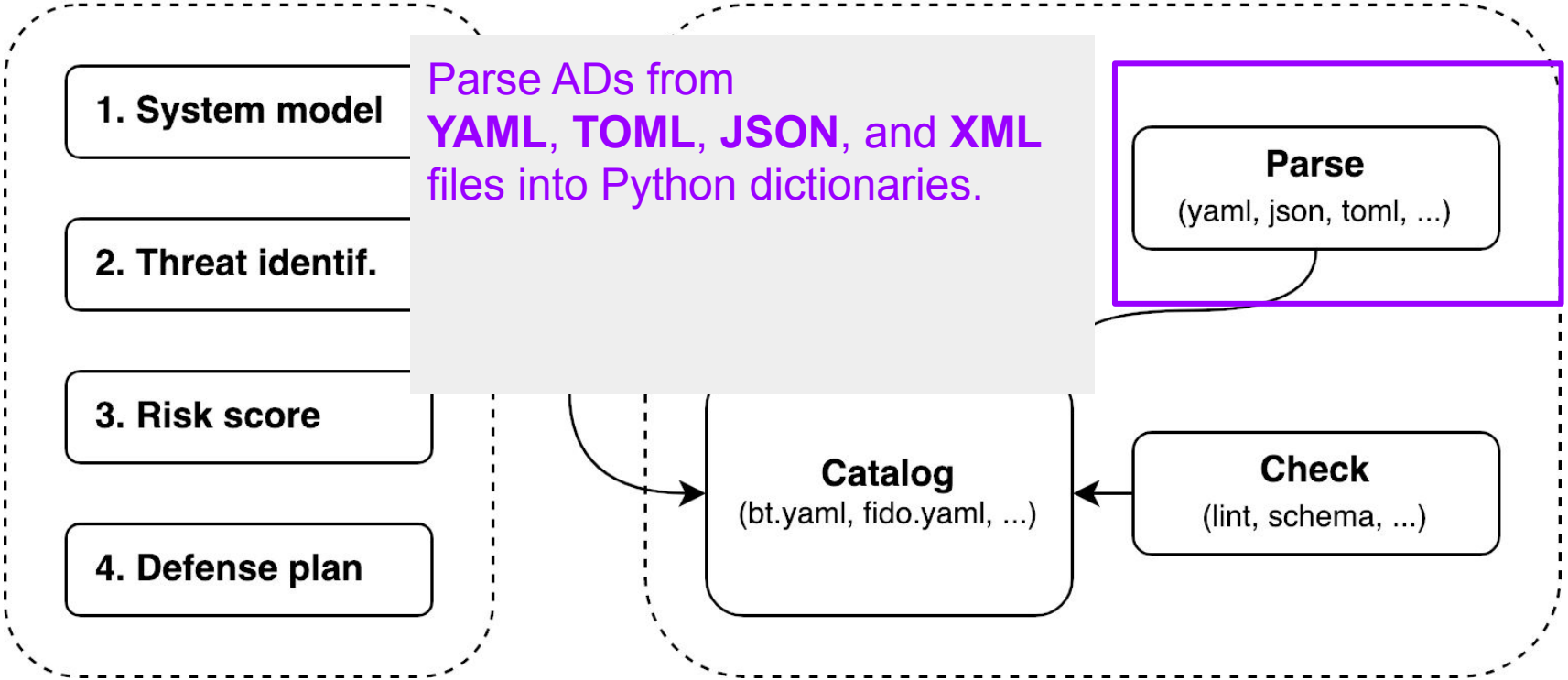


# AttackDefense Framework: Catalog [ref]

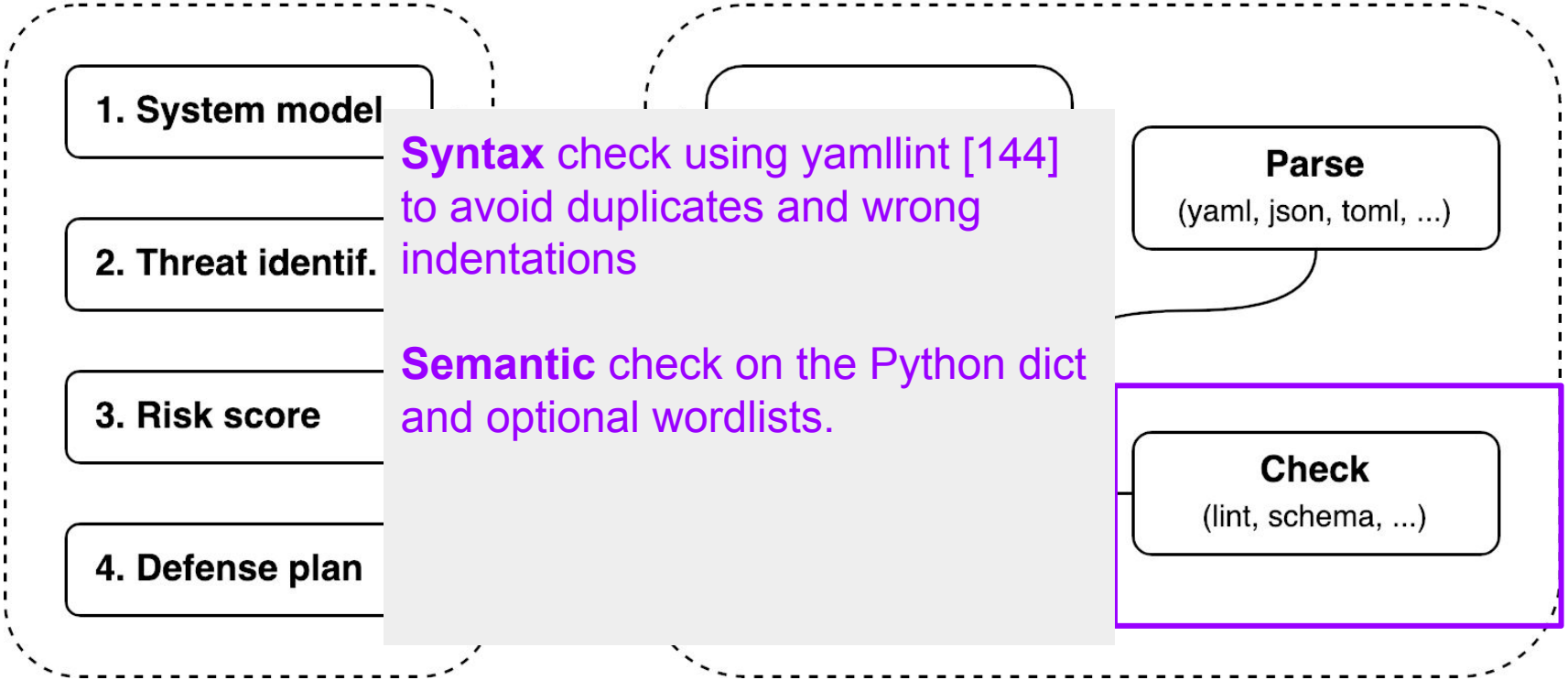



**Open source yaml** files containing ADs we developed. Eg: Bluetooth security ADs in `bt.yaml`

# AttackDefense Framework: Parse



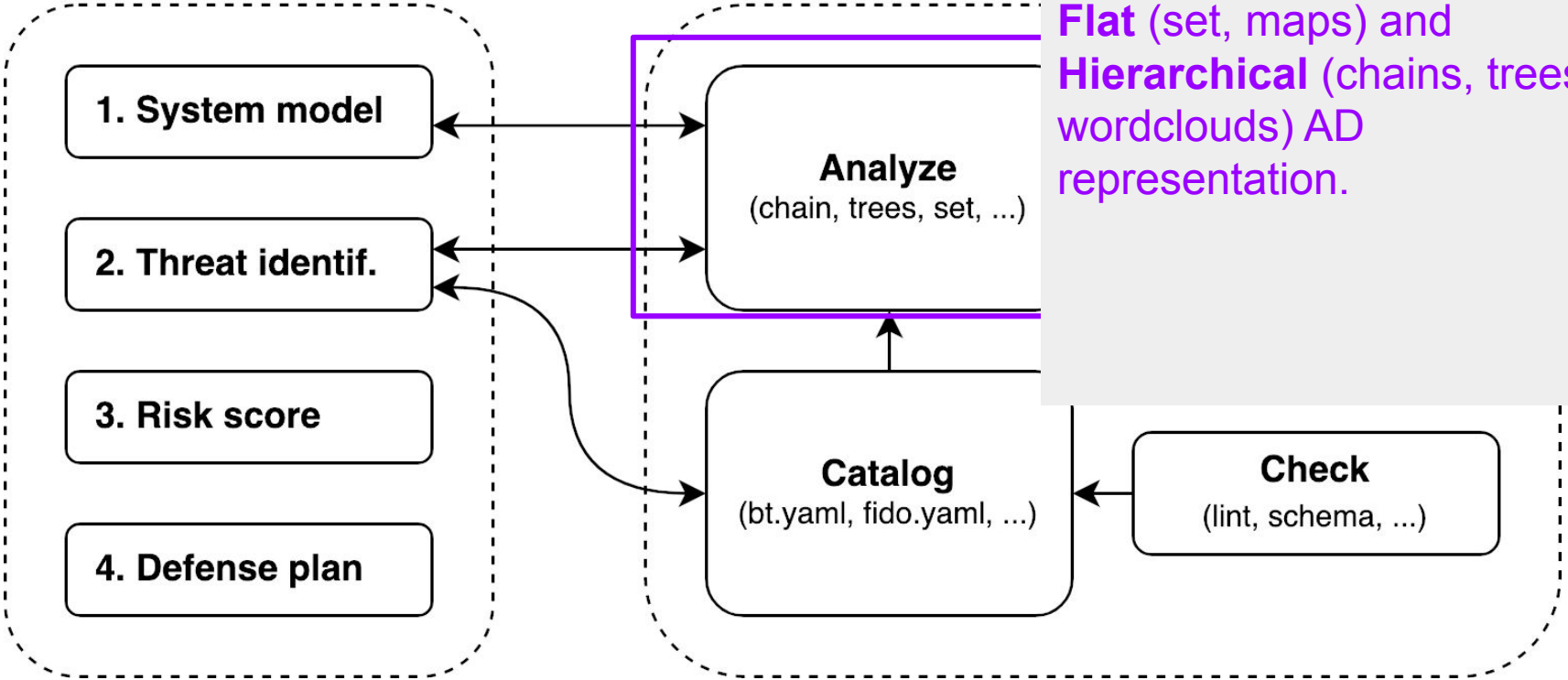
# AttackDefense Framework: Check




**Syntax** check using yamllint [144] to avoid duplicates and wrong indentations

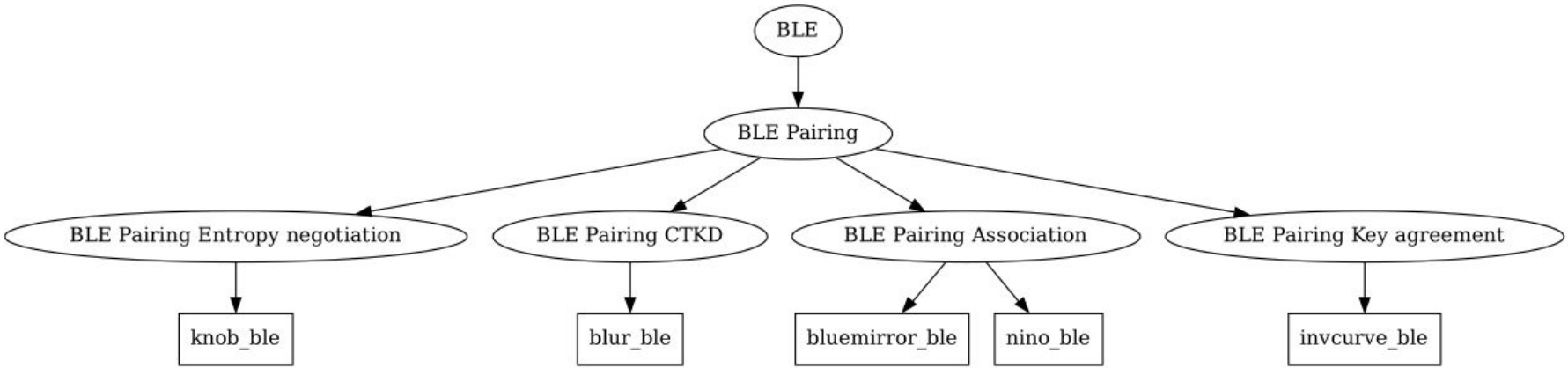
**Semantic** check on the Python dict and optional wordlists.

# AttackDefense Framework: Analyze




**Flat** (set, maps) and **Hierarchical** (chains, trees, wordclouds) AD representation.

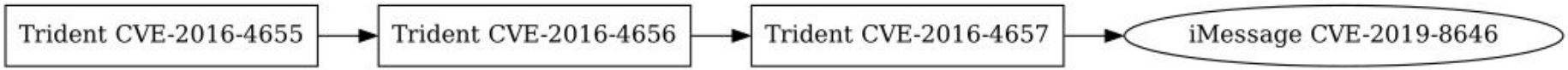
# BLE Pairing Security AD Tree




Branches gen from ADs surf vectors, eg: [BLE, Pairing, Association]

# ADF Bluetooth Security Word Cloud

# iOS Pegasus Spyware AD Chain [ref]



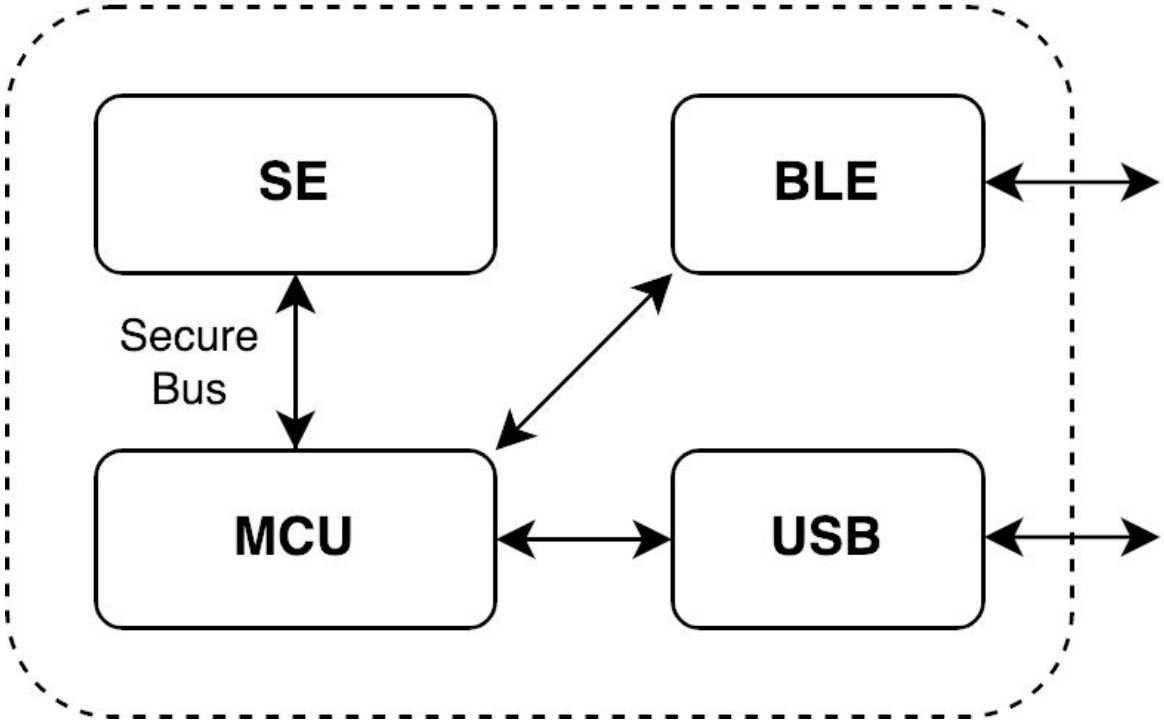
# ADF Evaluation

# Eval target: Crypto Wallets

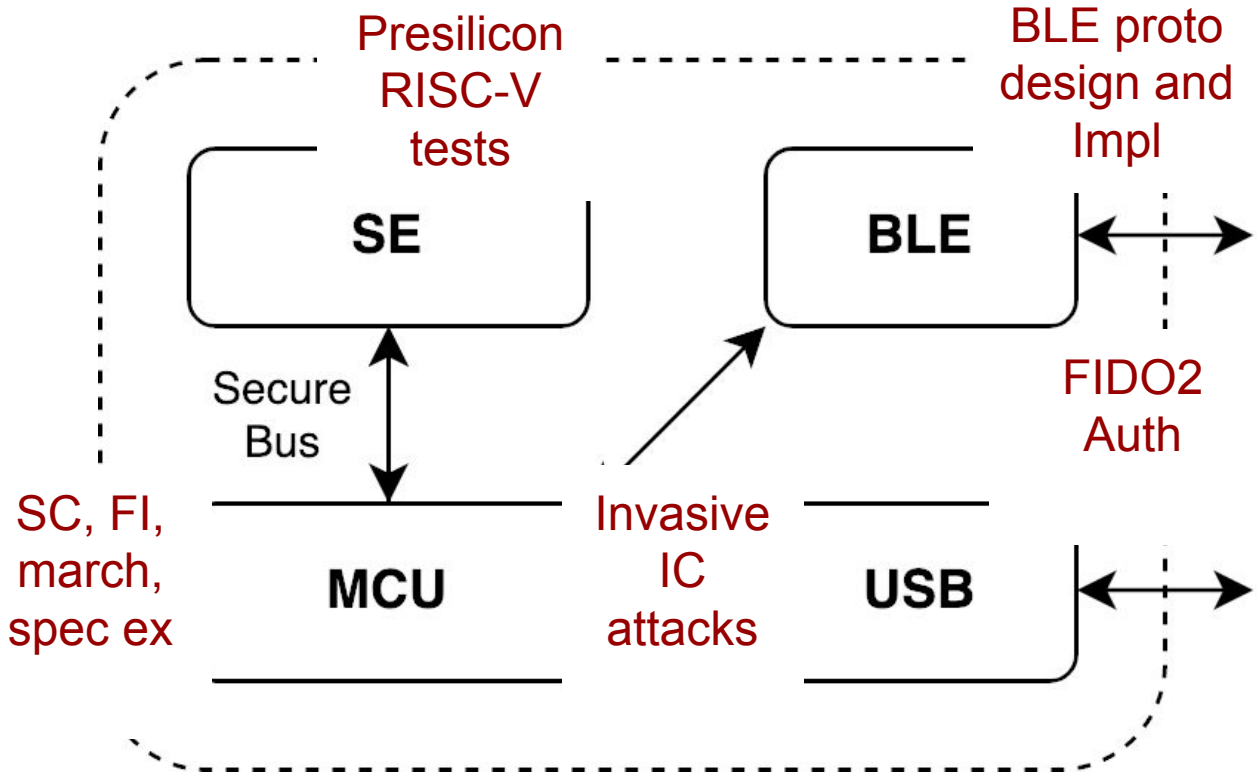
LEDGER


TREZOR
a part of SatoshiLabs Group.

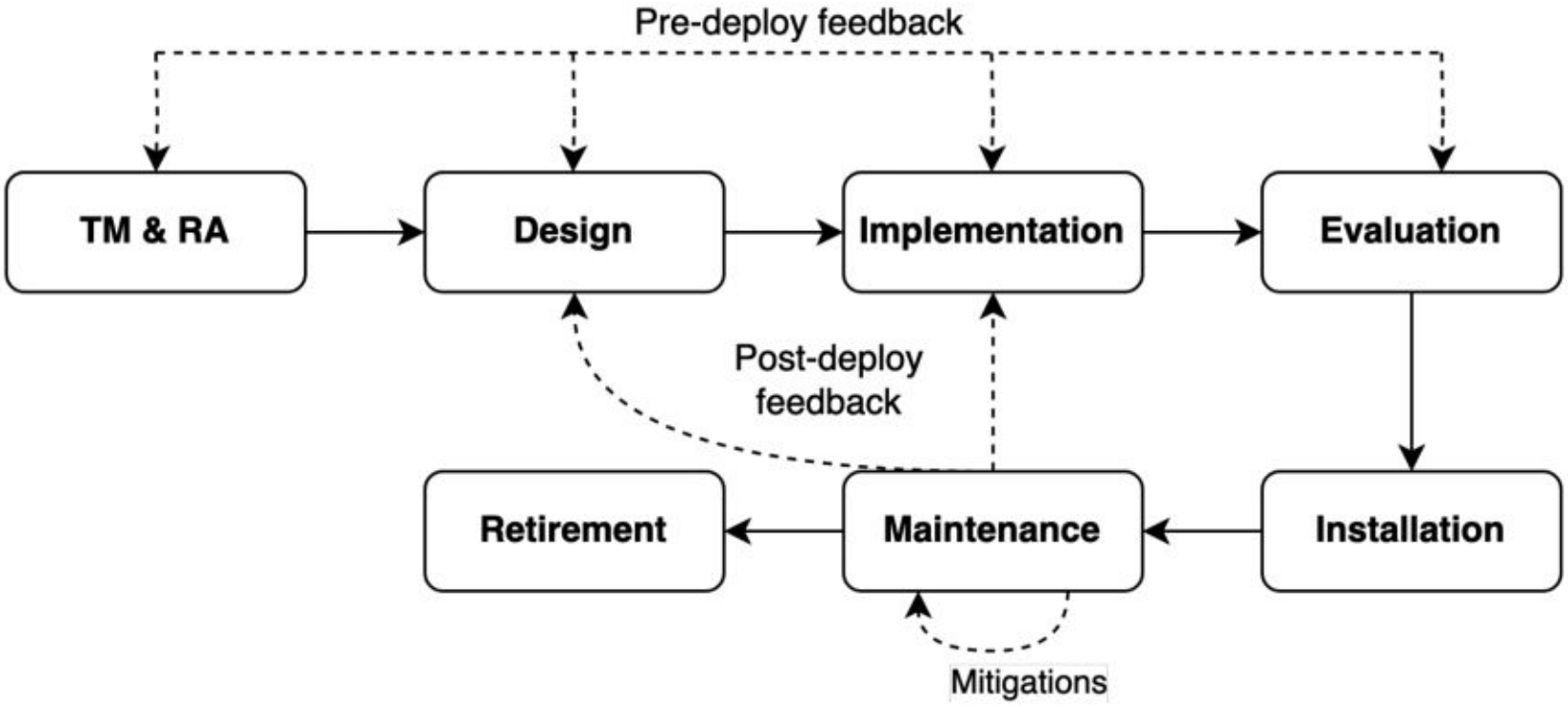
# Crypto Wallet Block Diagram



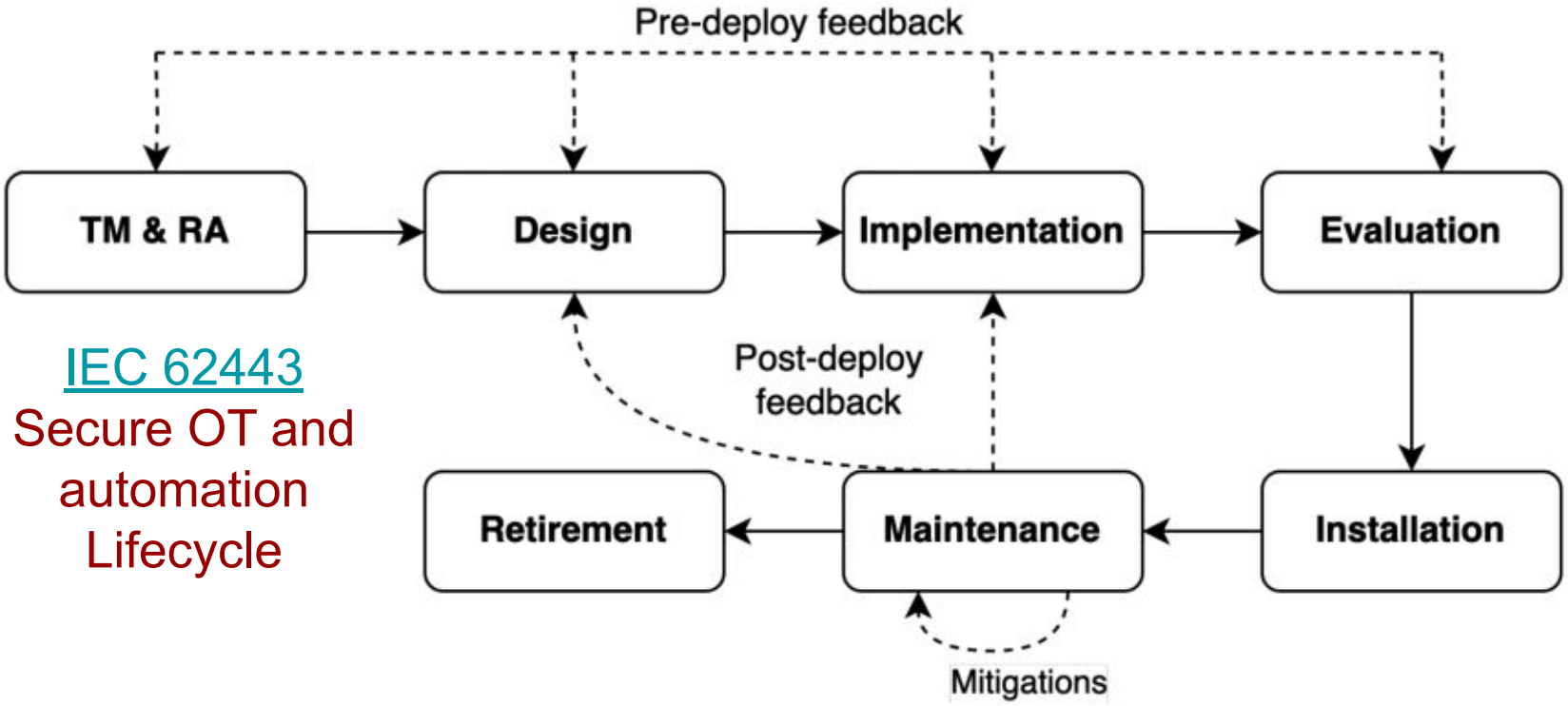
# Crypto Wallet Attack Surfaces



# Crypto Wallet Lifecycle



# Crypto Wallet Lifecycle Threats




IEC 62443
Secure OT and automation Lifecycle

# **Full stack coverage** with 7 Expert Teams!

1. EURECOM (BLE)
2. Security Pattern (FIDO2)
3. Security Pattern (Lifecycle)
4. KUL (FI, SCA)
5. KUL (march)
6. NXP (SE)
7. Texplained (PHY IC)



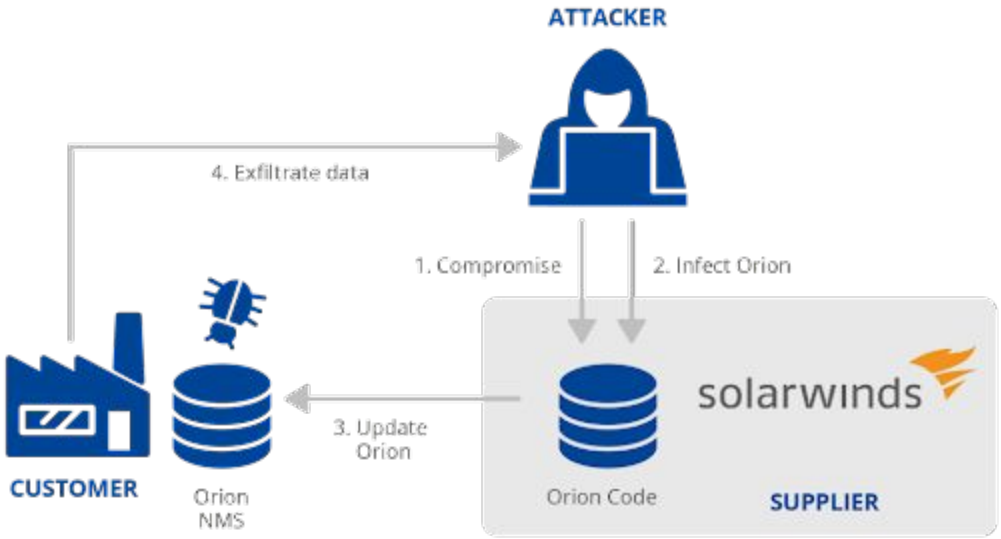


# Crypto Wallet ADF Evaluation (175 ADs)

| TM domain | Sec | Coverage | ADs | Files |
|---|---|---|---|---|
| ISA/IEC 62443-4-1 SecDev Lifecycle | 5.3 | LC, SE | 40 | `62443-4-1/*.yaml` |
| Physical Side-Channel and Fault inj. | 5.4 | PO, HW, SE, FW | 20 | `sc-fi.yaml` |
| Microarch. and Speculative Execution | 5.5 | PO, HW, SW, SE | 14 | `microa.yaml` |
| Presilicon RISC-V SE Testing | 5.6 | PO, HW, SW, FW, SE | 8 | `presil.yaml` |
| Invasive Physical IC Attacks | 5.7 | PO, HW, FW, SE, PR | 26 | `physical.yaml` |
| Bluetooth Protocol and Impl. Attacks | 5.8 | PO, SW, FW, PT, SE, PR | 46 | `bt.yaml` |
| FIDO2 Authentication Attacks | 5.9 | PO, HW, SW, FW, PT, SE | 21 | `fido*.yaml` |

**175 ADs**, **7 expert teams** across industry and academia.
Coverage: **LC**: Lifecycle, **SE**: Security, **PO**: Product, **HW**: Hardware, **FW**: Firmware, **PR**: Privacy, **SW**: Software, **PT**: Protocols

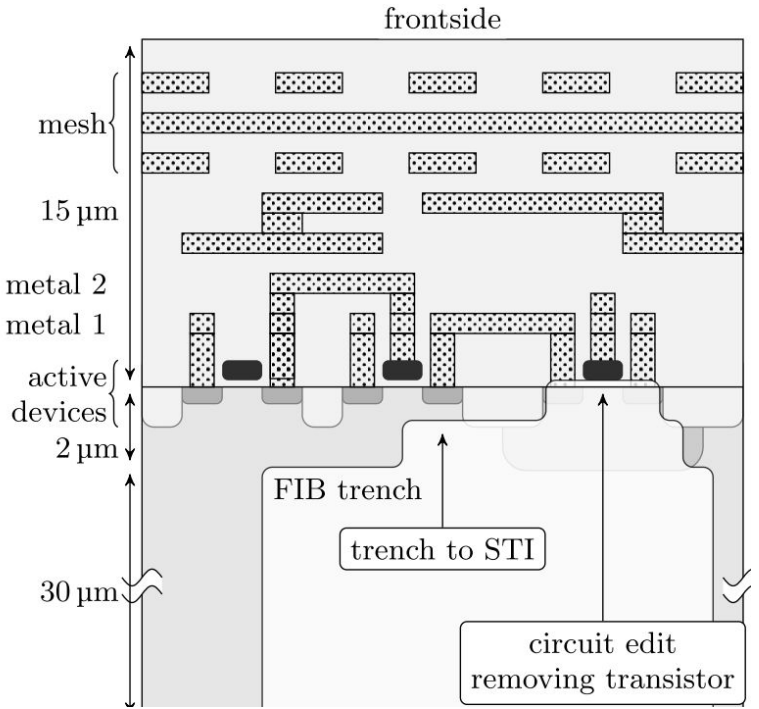
# SolarWinds Supply Chain Attack [ref]



# SolarWinds Supply Chain Attack AD [ref]

```
sw_orion:
  a: SolarWinds Orion codesign auth bypass
  d:
    Auth software supply chain: [Update and revoke code signing certs]
  surf: [Windows, SolarWinds, Orion Platform]
  vect: [Software mod, Malware distr]
  model: [Remote]
  tag: [SChain, SUNBURST, SUPERNOVA]
  risk: [cvss3_critical, cvss2_high]
  year: 2020
  cve: ["10148"]
  cwe: ["287", "288"]
```

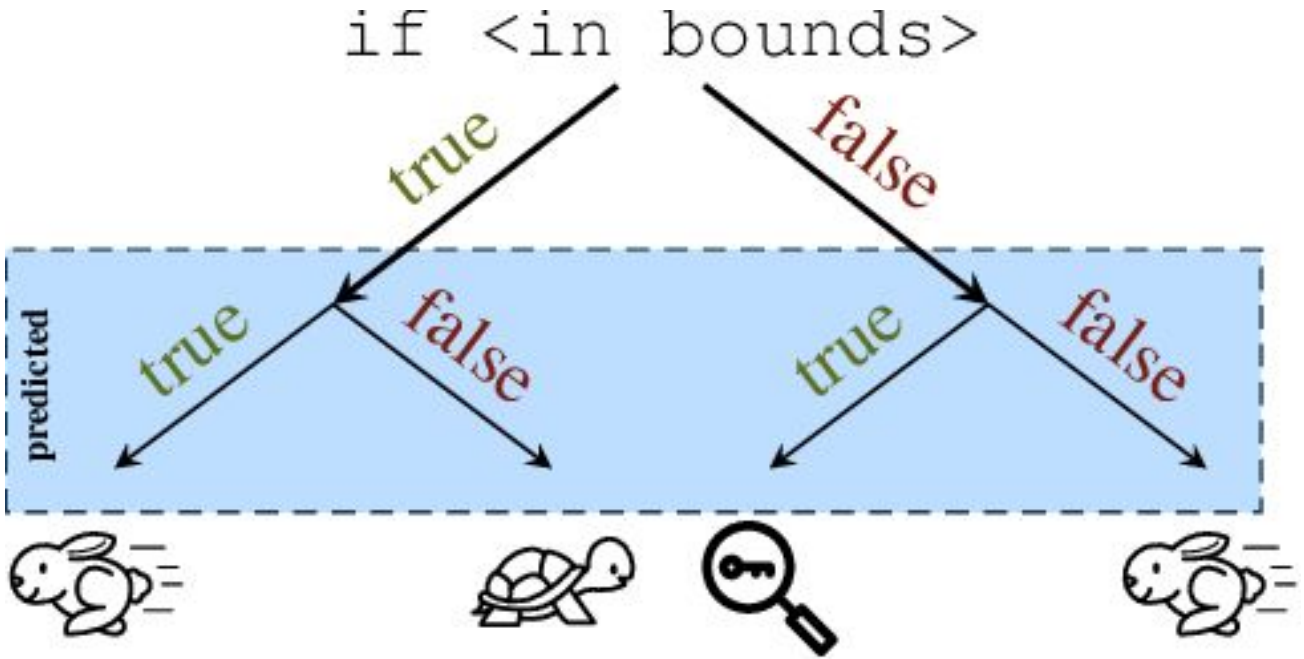
# Focused Ion Beam (FIB) Invasive Attack [ref]



# Focused Ion Beam (FIB) Mod Attack AD [ref]

```
attack_4:
  a: FIB modification
  d:
    Modifying or accessing internal signals should be rendered difficult.:
      - Packing the signals of interest.
  model:
    - invasive
  surf:
    - instruction skip
    - instruction modification
    - execution flow modification
    - counter-measure deactivation
    - read internal signals
  vect:
    - FIB editing
```

# Spectre microarch leak [ref]



# Spectre microarch leak AD [ref]

```
spectre-btb:
  a: Transient execution resulting from mispredicted indirect branches can cause
     persistent changes in the microarchitecture, which can be used to
     intentionally leak secrets from a victim process using a covert channel.
  d:
     "preventing speculation altogether" : [ "Inserting fence instructions at every
      indirect jump", "Disabling speculation in the hardware" ]
     "preventing speculation on secrets" : [ "Implementing a secure speculation
     scheme in the hardware, such as ProSpeCT" ]
     "removing the covert channel": [ "Cache partitioning", "Disabling
     hyperthreading", "(more depending on the microarchitectural side channels)" ]
  surf : [ "Shared resource enabling a covert channel between the victim and the
     attacker", "Shared branch target buffer (BTB) between the victim and the
     attacker" ]
  vect : [ "Controlling a shared resource leading to the covert channel", "
     Poisoning the BTB" ]
  model : [ "code execution", "remote" ]
  tag : [ "transient attack" ]
  year : 2018
  cve : [ "CVE-2017-5753", "CVE-2017-5715" ]
```

# ISA/IEC 62443-4-1 Secure Lifecycle [ref]

**Processes** a vendor must follow to **develop**, **test** and **maintain** an **ICS** securely throughout its lifecycle.

**Four maturity levels** to assess these processes.


**Eight Secure Dev Practices**

1. Security Mgmt (SM)
2. Spec of Security Reqs (SR)
3. Secure by Design (SD)
4. Secure Impl (SI)
5. Security Verif and Valid (SVV)
6. Incident Response (DM)
7. Security Update (SUM)
8. Security Guidelines (SG)

# ISA/IEC 62443-4-1 Secure Lifecycle AD [ref]

```
sm_1_dev-proc:
  a: Undefined development/maintenance/support processes
  d:
    Implement config mgmt with change control and audit logging: ["Redmine"]
    Require product desc and reqs def with req traceability:: ["Redmine"]
    Define design practices: [Addressed in @sd-4-secure-design-best-practices]
    Define implementation practices: [Addressed in @si-2-secure-coding-standards]
    Implement repeatable testing and validation processes: [Addressed in @svv-*]
    Enforce review and approval of all development process records: [Addressed in
    @sm-12-process-verification]
    Implement life-cycle support: ["..."]
  surf: [Processes]
  vect: [Unclear definition]
  tag: [Processes, Requirements, Design, Implementation, Testing, Review,
    Vulnerability management, Maintenance]
```

# Future of ADF and Conclusion

# ADF Limitations and Next Steps

Module generating ADs from text, voice, …

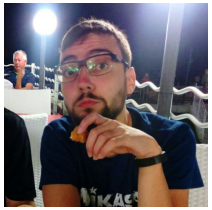
Module trained with our catalogue discovering new threats!

Agents threat modeling!

More attack surfaces! (Rowhammer, …)

Funding!

# Ack to papers **co-authors!**



**AttackDefense Framework (ADF): Enhancing IoT Devices and Lifecycles Threat Modeling**


TOMMASO SACCHETTI, Digital Security, EURECOM, Sophia Antipolis, France
MARTON BOGNAR, KU Leuven, Leuven, Belgium
JESSE DE MEULEMEESTER, KU Leuven, Leuven, Belgium
BENEDIKT GIERLICHS, KU Leuven, Leuven, Belgium
FRANK PIESSENS, KU Leuven, Leuven, Belgium
VOLODYMYR BEZSMERTNYI, NXP, Hamburg, Germany
MARIA CHIARA MOLTENI, Security Pattern, Mazzano, Italy
STEFANO CRISTALLI, Security Pattern, Mazzano, Italy
ARIANNA GRINGIANI, Security Pattern, Mazzano, Italy
OLIVIER THOMAS, Texplained, Valbonne, France


Texplained
HARDWARE SECURITY INSIGHT

EURECOM
Sophia Antipolis

SAP

NXP

KU LEUVEN

SECURITY PATTERN

# Ack to **ORSHIN** [ref]

**ORSHIN: Open-source ReSilient Hardware and software for Internet of thiNgs**

ORSHIN

How to design embedded and connected devices taking advantage of open source hardware (and software)

**Technical Lead**
Daniele Antonioli
EURECOM
France
Get in contact

**Scientific Lead**
Benedikt Gierlichs
KU Leuven
Belgium
Get in contact

**Project Coordinator**
Barbara Gaggl
Technikon
Austria

Get in contact

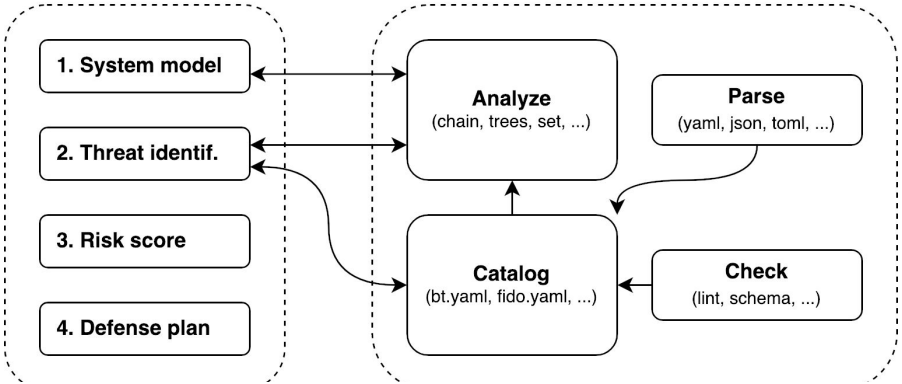
# Ack to **funding bodies**



# References (more)

- https://francozappa.github.io/publication/2026/blerp/
- https://francozappa.github.io/publication/2025/ctraps/
- https://francozappa.github.io/publication/2025/adf/
- https://francozappa.github.io/publication/2026/mados/
- https://francozappa.github.io/publication/2025/emuocpp/
- https://francozappa.github.io/publication/2023/espoofer/

# Threat Model IoT! Thanks. Q&A




| TM domain | Sec | Coverage | ADs | Files |
|---|---|---|---|---|
| ISA/IEC 62443-4-1 SecDev Lifecycle | 5.3 | LC, SE | 40 | `62443-4-1/*.yaml` |
| Physical Side-Channel and Fault inj. | 5.4 | PO, HW, SE, FW | 20 | `sc-fi.yaml` |
| Microarch. and Speculative Execution | 5.5 | PO, HW, SW, SE | 14 | `microa.yaml` |
| Presilicon RISC-V SE Testing | 5.6 | PO, HW, SW, FW, SE | 8 | `presil.yaml` |
| Invasive Physical IC Attacks | 5.7 | PO, HW, FW, SE, PR | 26 | `physical.yaml` |
| Bluetooth Protocol and Impl. Attacks | 5.8 | PO, SW, FW, PT, SE, PR | 46 | `bt.yaml` |
| FIDO2 Authentication Attacks | 5.9 | PO, HW, SW, FW, PT, SE | 21 | `fido*.yaml` |

```yaml
ad_name:
  # Primary fields
  a: attack
  d:
    policy1: [mech1, mech2]
    policy2: [mech1, mech2]
    ...
  surf: [surf, subsurf, subsubsurf, ...]
  vect: [vector1, vector2, ...]
  model: [model1, model2, ...]
  tag: [tag1, tag2, ...]
  # Optional fields
  risk: [score1, score2, ...]
  year: 2023
  cve: ["123", "456", ...]
  cwe: ["123", "456", ...]
  capec: ["123", "456", ...]
  vref: ["vendor-ref1", ...]
  ...: ...
```

https://francozappa.github.io/publication/2025/adf/