
black hat®
ARSENAL
DECEMBER 10-11, 2025
EXCEL LONDON / UNITED KINGDOM
#BHEU @BlackHatEvents

black hat ARSENAL
DECEMBER 10-11, 2025
EXCEL LONDON / UNITED KINGDOM

DICE: Device Identification and Classification Engine

Ricardo Yaben (rmyl@dtu.dk)
Emmanouil Vasilomanolakis (emmva@dtu.dk)

Ricardo Yaben

Ph.D. student
- Technical University of Denmark (DTU)
- Department of Applied Mathematics and Computer Science (COMPUTE)
- Section for Cybersecurity Engineering
- Cyber-deception group*
- Soon postdoc 🎉

Research area and interests
- Internet measurements
- Vulnerability assessment
- Operational Technology (OT)
- Society behavioral aspects related to cyber
- Cyber-deception*

(*) Cyber-deception is a side-quest for me

Danish Pump Manufacturer DESMI Reports Cyberattack on IT Systems and Operations

By CISOMAG - April 14, 2020

Vestas impacted by cyber security incident

Vestas Wind Systems A/S, Aarhus, 20 November 2021

The attack against Danish, critical infrastructure

Published: November 2023

Investigation: WannaCry cyber attack and the NHS

Date: 27 Oct 2017

Topics: Cyber security, Digital services, Digital, data and technology, Health and social care

Departments: Department of Health and Social Care

South Staffs Water: Cyber-attack

Volume 724: debated on Wednesday 14 December 2022

Cyber-Attack Against Ukrainian Critical Infrastructure

Last Revised: July 20, 2021

Alert Code: IR-ALERT-H-16-056-01

UK health officials say patient's death partially down to cyberattack

BlackEnergy APT Attacks in Ukraine

Ukraine's largest telecom operator shut down after cyberattack

This article was updated at 10:40 a.m. EST

Cyber attack on HSE systems

From: Department of the Taoiseach

Published on: 21 May 2021

Maersk upbeat on shipping outlook, faces hefty cyber attack bill

By Jacob Gronholt-Pedersen

August 16, 2017 3:36 PM GMT+2 · Updated August 16, 2017

CrashOverride Malware

Last Revised: July 20, 2021

Alert Code: TA17-163A

Synnovis cyber attack – statement from NHS England

21 June 2024

TV5Monde Cyberattack (2015): The Day a TV Network Went Dark

Die Lage der IT-Sicherheit in Deutschland 2014

Central bank of Denmark hacked as part of 'the world's most sophisticated hacker attack'

It-sikkerhed 29. juni 2021 kl. 12:24 3 kommentarer

Millions of Internet-facing devices are poorly maintained, obsolete, or already compromised

The state of the Internet

As digitization gains momentum across all sectors, we see a surge to expose to the Internet networks previously hidden, which now can be accessed and controlled remotely. However, this is all the effort being done, which often results in security headlines, financial loses, and even deaths.

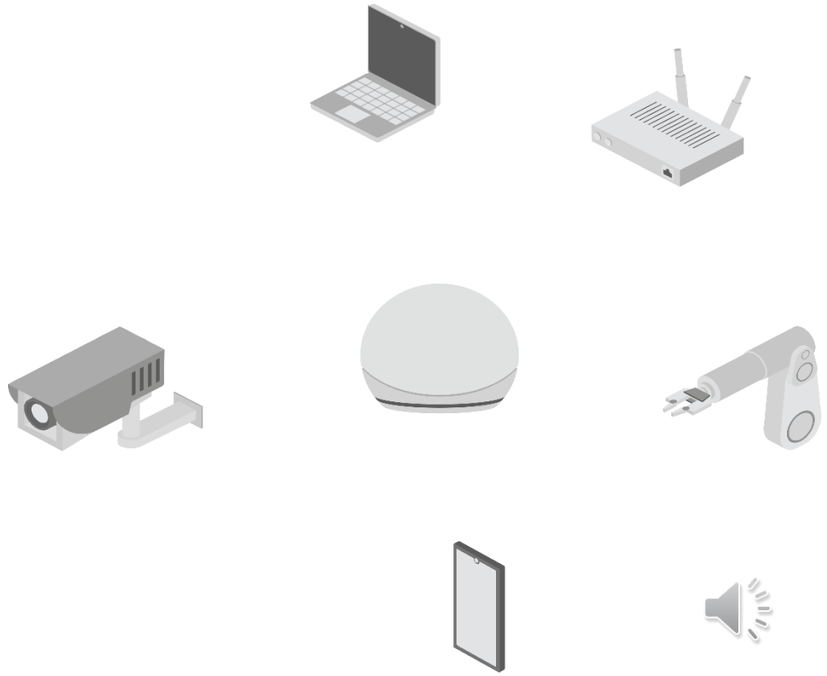
One-shot configurations untouched for years, with deprecated (often insecure) functionalities, obsolete devices well beyond their end-of life, services lacking authentication or any access control, encryption, or still using default values, with extreme cased of hard-coded unchangeable properties, such as credentials, certificates, and whole firmwares.

Our contributions

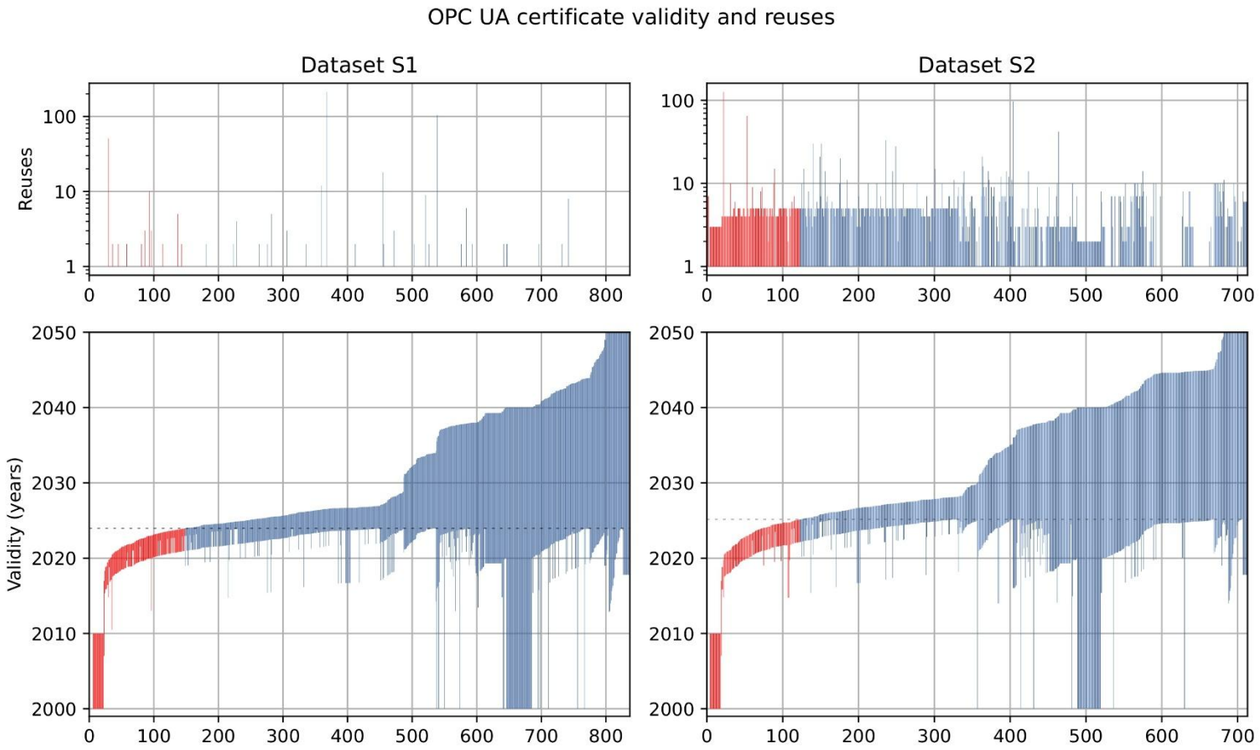
- Published the results of our numerous vulnerability assessments through Internet measurements (i.e., scanning the Internet for vulnerable devices).
- We conducted several ethical disclosure campaigns (i.e., we contacted the device maintainers).

Limitations

- Lack of consensus on how to measure and evaluate (i.e., no ground truth or correct “method”).
- Available tools not suitable for Internet-wide surveys.
- Cannot compare results



Systemic issues affecting +1M devices in the wild



Most vulnerabilities are associated with poor security management

- Lack of authentication, access control, or encryption
- Certificate management issues
- Misconfigurations
- Deprecated implementations

Maintainers ignore advice

- +50% of vulnerable OT devices remain active and exposed for years
- From +100 organizations notified, less than 5 responded

Mitigating the threat

DICE

Device Identification and Classification Engine

Advice is simple

but fails to get through

1. Patch in time
2. Update regularly
3. Monitor constantly
4. Retire eventually

We continue working

- Suggested stricter regulatory measures
- Identified key points where society fails to secure devices
- Proposed countermeasures for +10 widely used OT and IoT protocols
- **Developing DICE**

The Internet is flooded with vulnerable devices, but current identification methods fail to detect even basic vulnerabilities

VirusTotal

AbuseIPDB

ZoomEye

censys

zmap

NMAP

RIPE NCC

RIPE Atlas

GREYNOISE

IPinfo

SHODAN

SHADOWSERVER

Rolling the DICE

1. How can we ingest data from all these sources?
2. How can we orchestrate smarter measurements?
3. How can we make results reproducible?
4. How can we make researchers and industry collaborating into sharing their identification methods?
5. How can we compare our methods?
6. How can we compare our results?
7. How can we measure changes on the Internet over time? (monitoring)

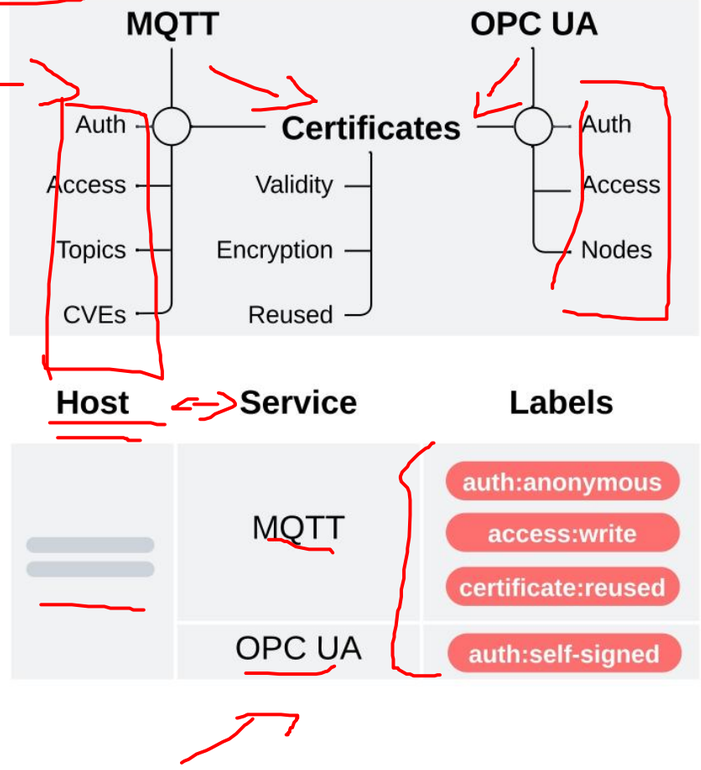
DICE: The Engine

```
$ dice scan -s opcua,mqtt
```

```
// opcua.dice
cls opcua-auth
cls opcua-access (cls: opcua-auth)
cls opcua-nodes  (cls: opcua-auth)
sig certificates (cls: opcua-auth)

// mqtt.dice
cls mqtt-auth
cls mqtt-access  (cls: mqtt-auth)
cls mqtt-topics  (cls: mqtt-auth)
cls mqtt-cve     (cls: mqtt-auth)
sig certificates (cls: mqtt-auth)

// certificates.dice
cls x509-validity
cls x509-encryption
cls x509-reused
```



- Dice is designed to identify and classify vulnerable devices facing the Internet, a modular and scanner agnostic engine for complex Internet measurements.
- Opens new opportunities to **monitor** security events across the Internet, such as outages and systemic vulnerabilities.

Use cases

- Longitudinal studies identifying trends and persistent issues.
- Artificial Intelligence trained on datasets classified with DICE.
- Improve IP exploitation techniques based on results from multiple measurements.
- Conducting responsible disclosure campaigns to notify affected owners.
- Mitigate Internet churn for time-sensitive measurements.

$ dice scan --signatures mqtt,opcua

First, DICE searches for the given signatures to load their modules and dependancies.

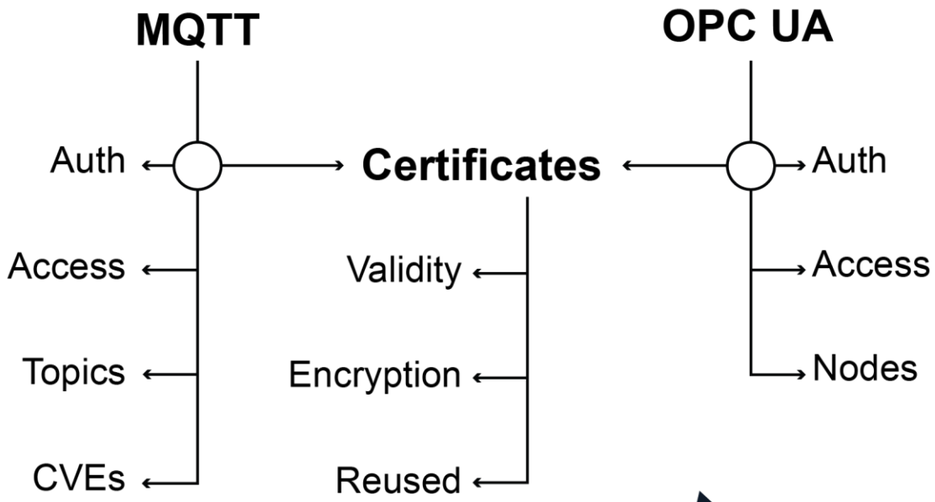
Modules are the signature's **processing units.** They either collect device information, identify devices, or detect vulnerabilities.

```
// opcua.dice
cls opcua-auth
cls opcua-access   (cls: opcua-auth)
cls opcua-nodes (cls: opcua-auth)
sig certificates (cls: opcua-auth)
// mqtt.dice
cls mqtt-auth
cls mqtt-access (cls: mqtt-auth)
cls mqtt-topics (cls: mqtt-auth)
cls mqtt-cve (cls: mqtt-auth)
sig certificates (cls: mqtt-auth)
// certificates.dice
cls x509-validity
cls x509-encryption
cls x509-reused
```

Signatures define **dependancies** between modules and other signatures.

Then, links signatures and modules verifying there are no cycles.

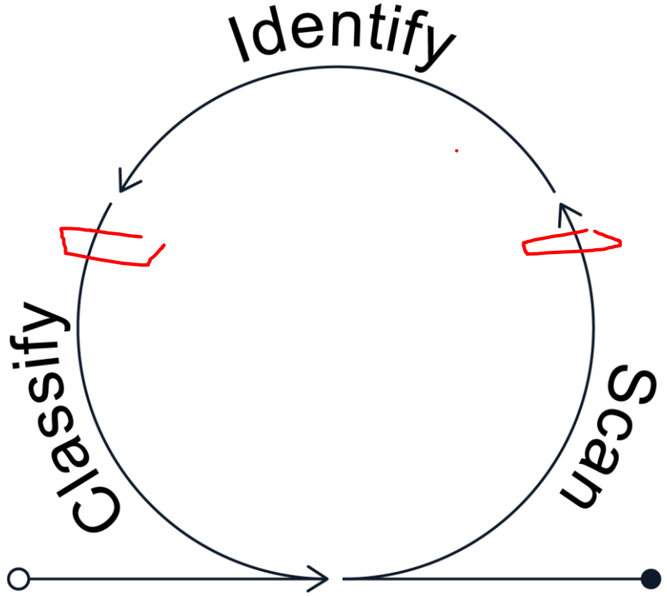
Signatures describe how and which modules are needed to identify and classify devices.



Signatures form **directional acyclic graphs (DAGs)** to sequence modules.

Finally, sends addresses to its components to scan, identify and classify as needed.

Components orchestrate the **scanning**, **identification** and **classification** tasks.

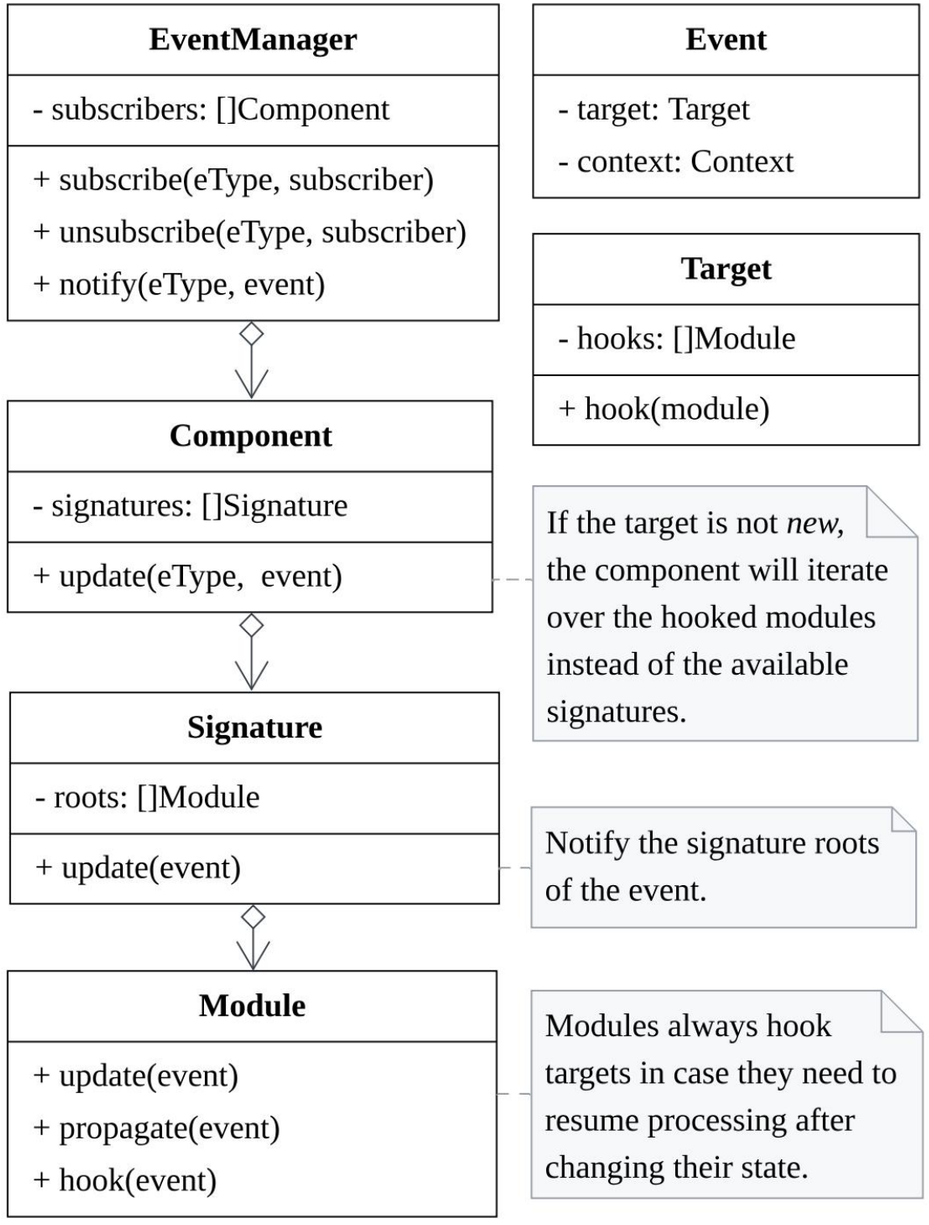


Components work **independently** and **collaborate** to profile devices.

The classifier component receives target events. Events fire when new targets are introduced or change their state (e.g., new data). Classifier modules analyze targets, propagate to their children, and may publish scanning events if needed.

The scanner component receives events to scan targets and a context (e.g., probe and parameters). These modules fetch information from multiple sources (e.g., Shodan, WHOIS, Greynoise, or Virustotal). On completion, this component updates targets with raw results.

The identification component receives notifications to normalize scanning results, helping classifiers working with data from multiple sources. Identification modules may pre-process data to identify OS versions, services, certificates, etc.



DICE
DEMO