DistriNet@Ghent

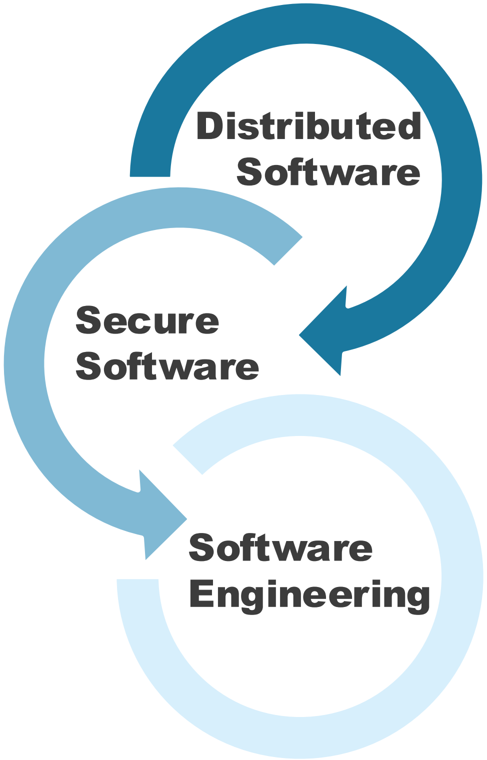
DistriNet in a Nutshell

120+ people

16 professors
9 research managers
3 business office
11 postdocs
85+ PhD students

40+ years track record

6 spin off companies

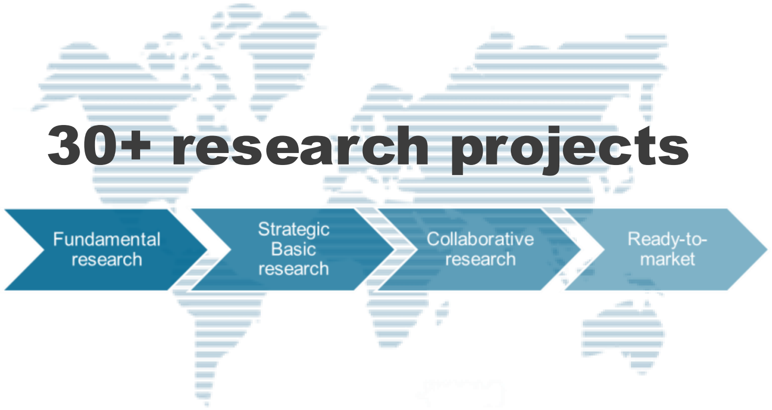


Distributed Software

Secure Software

Software Engineering

30+ research projects

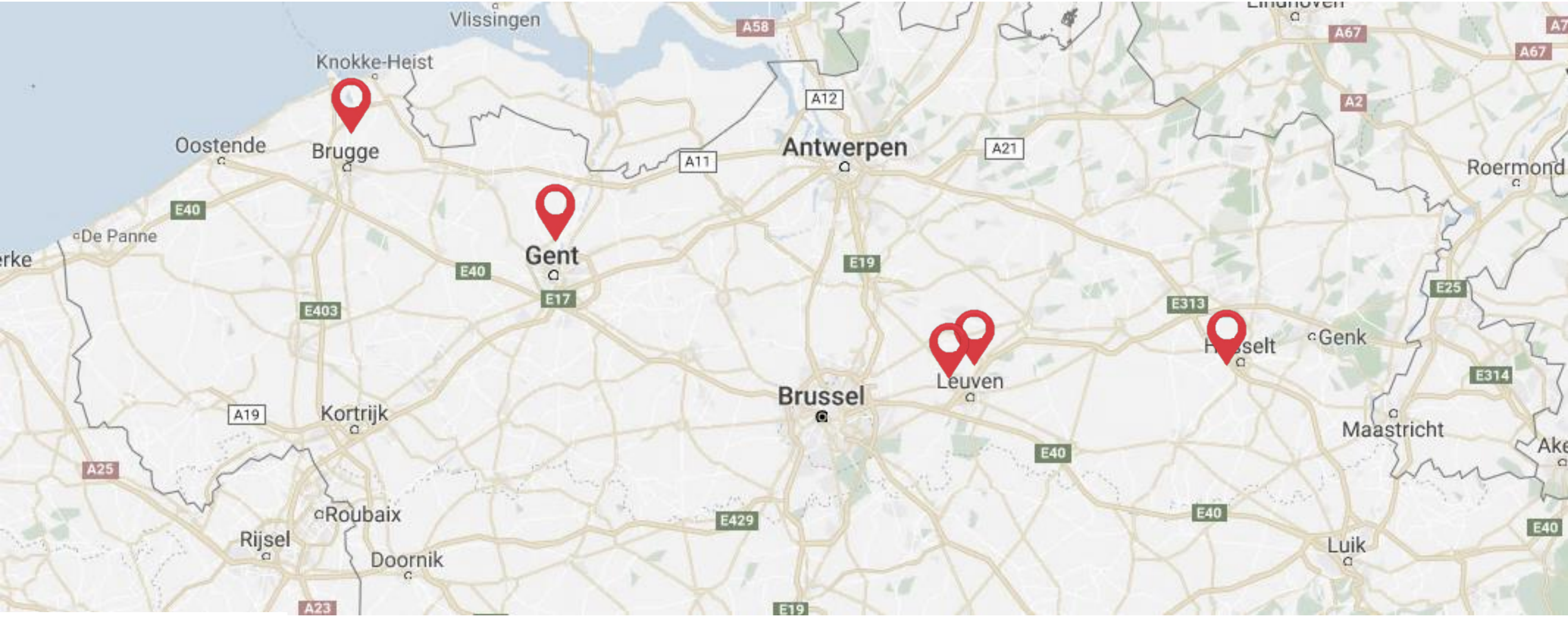


Fundamental research → Strategic Basic research → Collaborative research → Ready-to-market

100 + industry collaborations

KU LEUVEN DistriNet

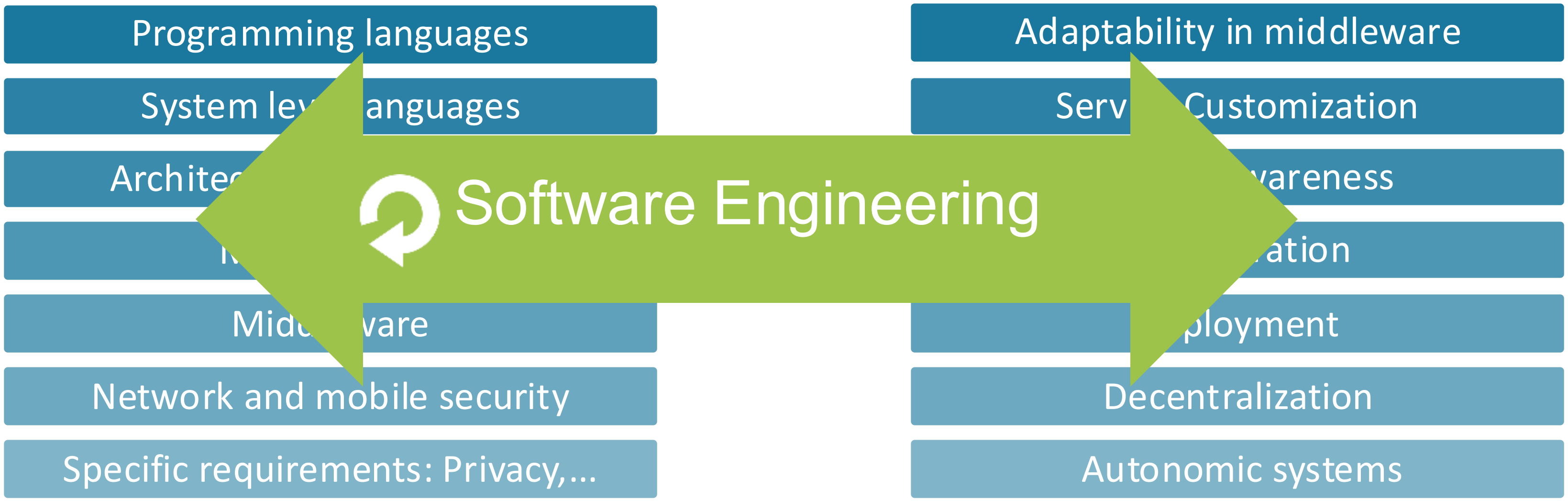
DistriNet Presence in Flanders



Domains of Expertise

Secure Software

Distributed Software



Programming languages

System lev anguages

Archite

N

Mid vare

Network and mobile security

Specific requirements: Privacy,...

Software Engineering

Adaptability in middleware

Serv Customization

vareness

ation

ployment

Decentralization

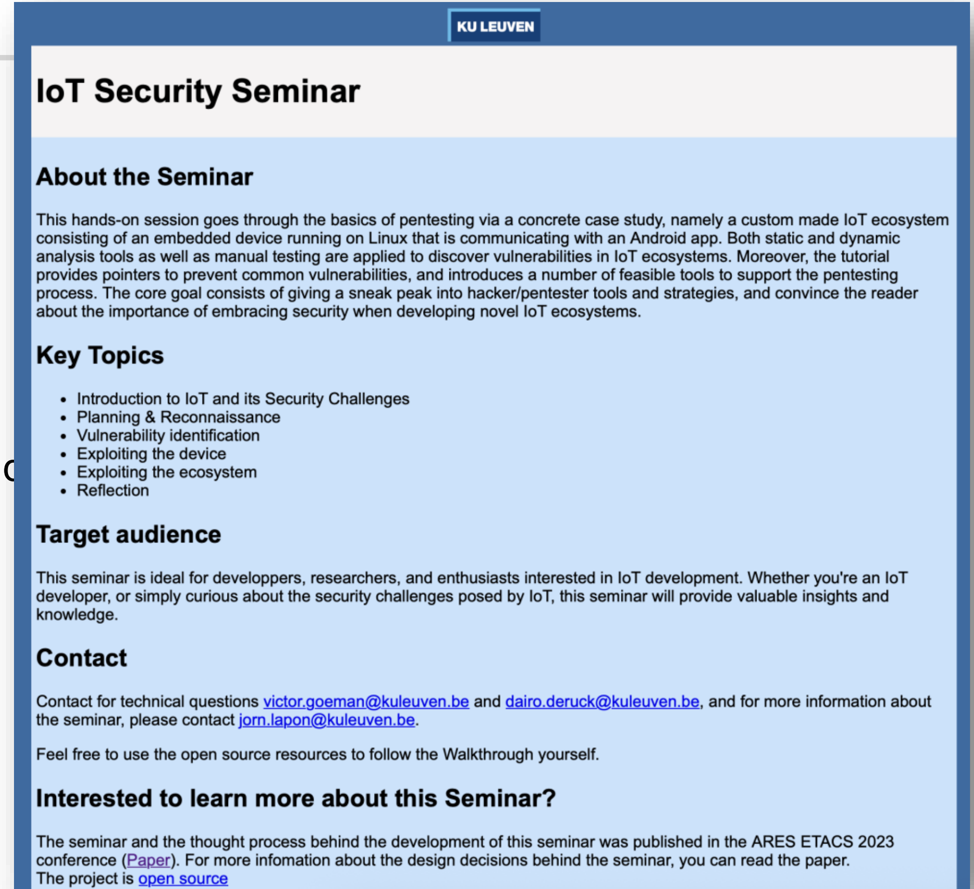
Autonomic systems

Research activities in Ghent

- Embedded Security
  - → detection, mitigation, handling, compliance, legislation…
- Privacy Enhancing Technologies
  - → anonymization, controlled release and retention of sensitive data…
- System security
  - → multi-variant execution, memory vulnerability mitigations…

Former Tech Transfer Projects

- VELCRO:
  - VLAIO/TeTra project
    - KU Leuven, Gent (J. Lapon, V. Naessens)
    - VUB, Indi (A. Braeken, K. Steenhaut)
  - Securing Embedded Devices
  - Hands-on Tutorial for embedded software d
    - Awareness
    - Expertise
    - Tools



IoT Security Seminar

About the Seminar

This hands-on session goes through the basics of pentesting via a concrete case study, namely a custom made IoT ecosystem consisting of an embedded device running on Linux that is communicating with an Android app. Both static and dynamic analysis tools as well as manual testing are applied to discover vulnerabilities in IoT ecosystems. Moreover, the tutorial provides pointers to prevent common vulnerabilities, and introduces a number of feasible tools to support the pentesting process. The core goal consists of giving a sneak peak into hacker/pentester tools and strategies, and convince the reader about the importance of embracing security when developing novel IoT ecosystems.

Key Topics

- Introduction to IoT and its Security Challenges
- Planning & Reconnaissance
- Vulnerability identification
- Exploiting the device
- Exploiting the ecosystem
- Reflection

Target audience

This seminar is ideal for developpers, researchers, and enthusiasts interested in IoT development. Whether you're an IoT developer, or simply curious about the security challenges posed by IoT, this seminar will provide valuable insights and knowledge.

Contact

Contact for technical questions victor.goeman@kuleuven.be and dairo.deruck@kuleuven.be, and for more information about the seminar, please contact jorn.lapon@kuleuven.be.

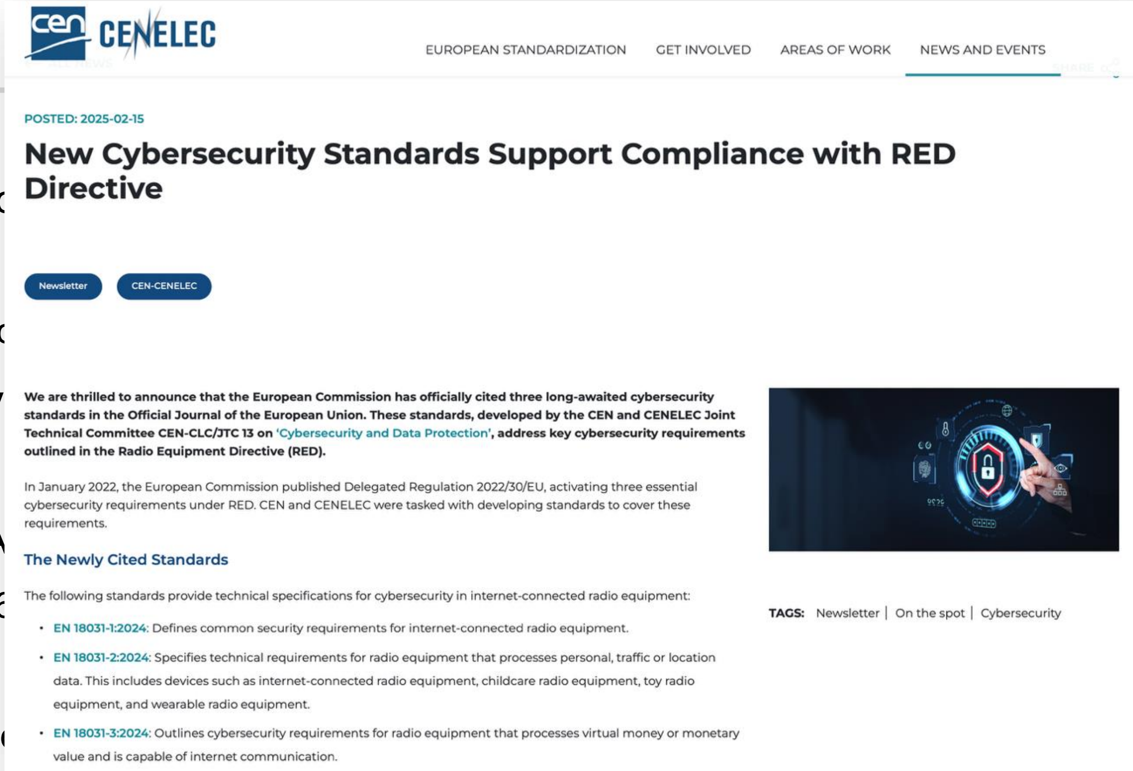
Feel free to use the open source resources to follow the Walkthrough yourself.

Interested to learn more about this Seminar?

The seminar and the thought process behind the development of this seminar was published in the ARES ETACS 2023 conference (Paper). For more infomation about the design decisions behind the seminar, you can read the paper.
The project is open source

Former Tech Transfer Projects

- CoAssurance:
  - VLAIO/TeTra projec
    - DistriNet@Gent
    - M-group (J. Boyd
  - Safety and security
  - Discussed:
    - Regulation: CRA
    - Standards: IEC 6
    - Now: harmonize



CEN CENELEC

EUROPEAN STANDARDIZATION GET INVOLVED AREAS OF WORK NEWS AND EVENTS

POSTED: 2025-02-15

New Cybersecurity Standards Support Compliance with RED Directive

Newsletter CEN-CENELEC

We are thrilled to announce that the European Commission has officially cited three long-awaited cybersecurity standards in the Official Journal of the European Union. These standards, developed by the CEN and CENELEC Joint Technical Committee CEN-CLC/JTC 13 on 'Cybersecurity and Data Protection', address key cybersecurity requirements outlined in the Radio Equipment Directive (RED).

In January 2022, the European Commission published Delegated Regulation 2022/30/EU, activating three essential cybersecurity requirements under RED. CEN and CENELEC were tasked with developing standards to cover these requirements.

The Newly Cited Standards

The following standards provide technical specifications for cybersecurity in internet-connected radio equipment:

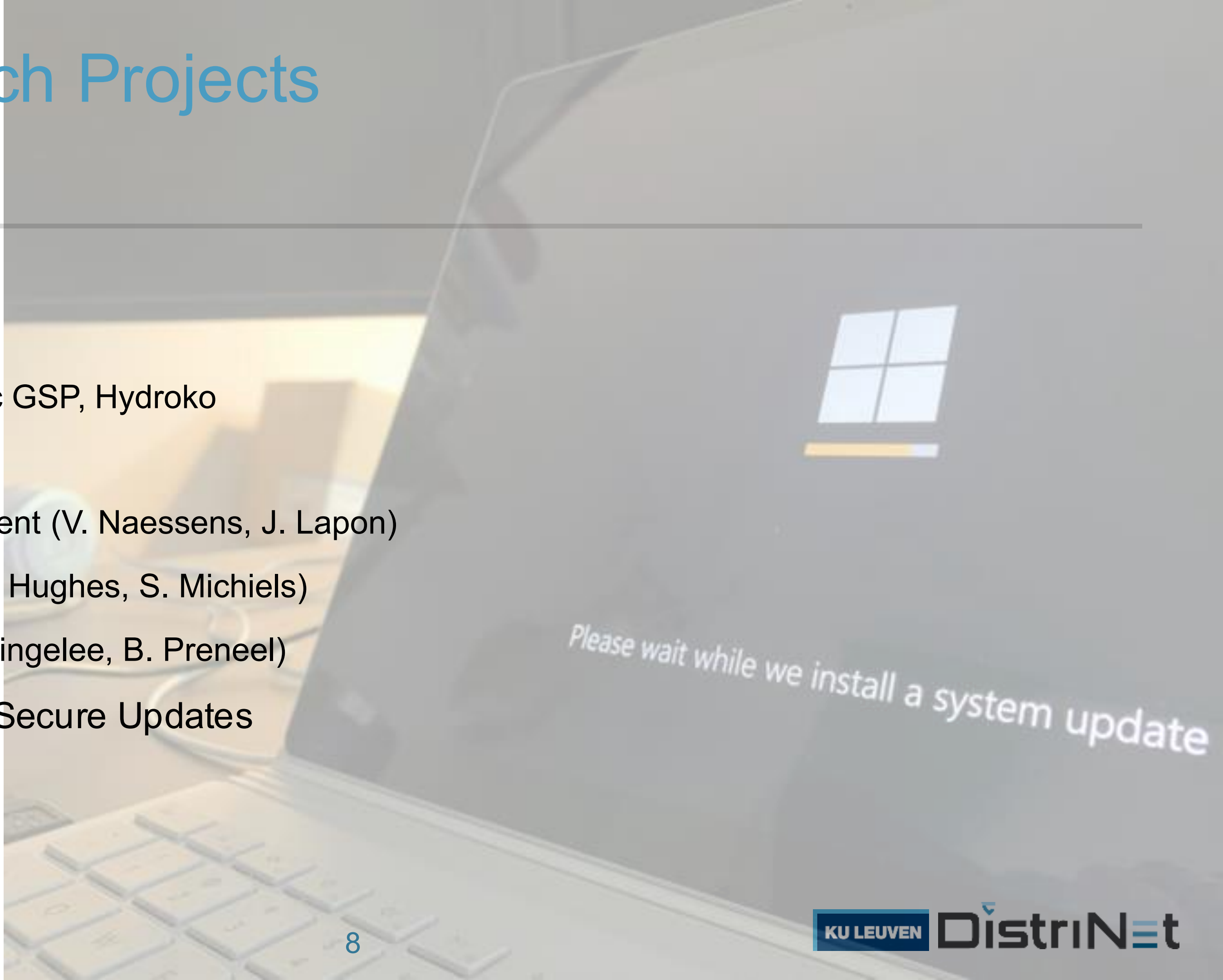
- EN 18031-1:2024: Defines common security requirements for internet-connected radio equipment.
- EN 18031-2:2024: Specifies technical requirements for radio equipment that processes personal, traffic or location data. This includes devices such as internet-connected radio equipment, childcare radio equipment, toy radio equipment, and wearable radio equipment.
- EN 18031-3:2024: Outlines cybersecurity requirements for radio equipment that processes virtual money or monetary value and is capable of internet communication.

TAGS: Newsletter | On the spot | Cybersecurity

OF
EGULATION
DARDS
OPMENT OF
STEMS,
RPLAY WITH
NCERNS.
d guidelines

Former Research Projects

- TRUSTI:
  - VLAIO/ICON project
    - QuickSand, Televic GSP, Hydroko
    - KU Leuven:
      - DistriNet@Gent (V. Naessens, J. Lapon)
      - DistriNet (D. Hughes, S. Michiels)
      - COSIC (D. Singelee, B. Preneel)
  - Research project on Secure Updates
    - Multi-party
    - Battery powered



Ongoing Tech Transfer Projects

- SSB: Secure Smart Buildings
  - VLAIO/TeTra project
    - DistriNet@Gent (T. Cordemans, V. Naessens)
    - UCLL, Diepenbeek (J. Huybrichs)
  - Best practices and tools to increase **Resilience of Smart Buildings**
  - Target: vendors, integrators, operators, and building managers

Protocol Testing (prof. M. Vanhoef)

VPN: TunnelCrack (2023)

4 Million VPN tunneling hosts insecure and easily exploited.

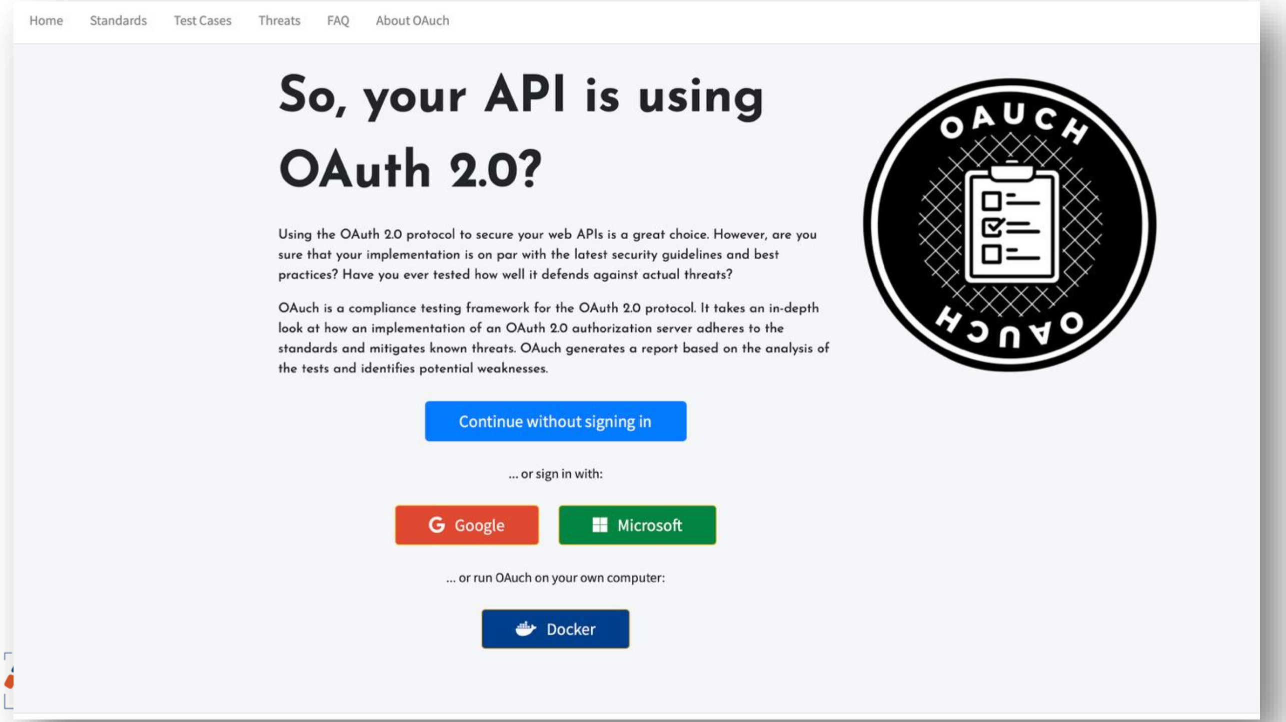
- Hide identity
- Access private networks
- DoS attacks

WiFi:

API Testing (dr. P. Philippaerts, prof. W. Joosen)

Oauth 2.0 - API Testing

Compliance with security guidelines and best practices



So, your API is using OAuth 2.0?

Using the OAuth 2.0 protocol to secure your web APIs is a great choice. However, are you sure that your implementation is on par with the latest security guidelines and best practices? Have you ever tested how well it defends against actual threats?

OAuch is a compliance testing framework for the OAuth 2.0 protocol. It takes an in-depth look at how an implementation of an OAuth 2.0 authorization server adheres to the standards and mitigates known threats. OAuch generates a report based on the analysis of the tests and identifies potential weaknesses.

Continue without signing in
... or sign in with:
Google
Microsoft
... or run OAuch on your own computer:
Docker
OAUCH
OAUCH

https://oauch.io