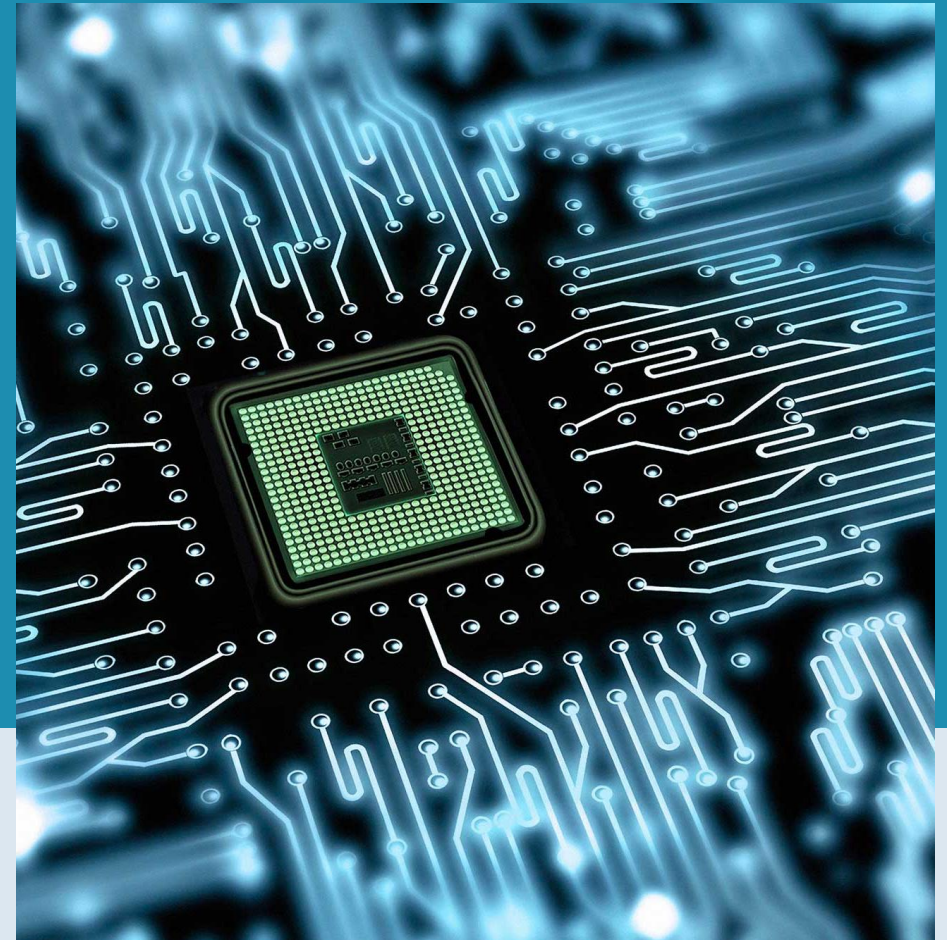


Implementation Industry 4.0 Paradigm in Education. Ukrainian Experience

“Boosting the role of HEIs in the industrial transformation towards the Industry 4.0 paradigm in Georgia and Ukraine” 609939-EPP-1-2019-1-BE-EPPKA2-CBHE-JP-HEIn4

Research & Education Computer science @ Gent Campus

Tony Wauters (coordinator)



Computer science @ Campus Gent

- Belongs to Department of Computer Science, KU Leuven
- Two active research units:

**Numerical Analysis
and Applied
Mathematics
(NUMA)**

**Distributed and
Secure Software
(DistriNet)**

Education

- Faculty of Engineering Technology
 - Electronics-ICT
 - Elektromechanics
- Advanced Master's Programme)
- Postgraduate Programme



Numerical Analysis and Applied Mathematics (NUMA)

- Houses research group: CODeS
- **CODeS** = Combinatorial Optimization and decision support



Application domains



Tony Wauters

Cutting & packing
Scheduling

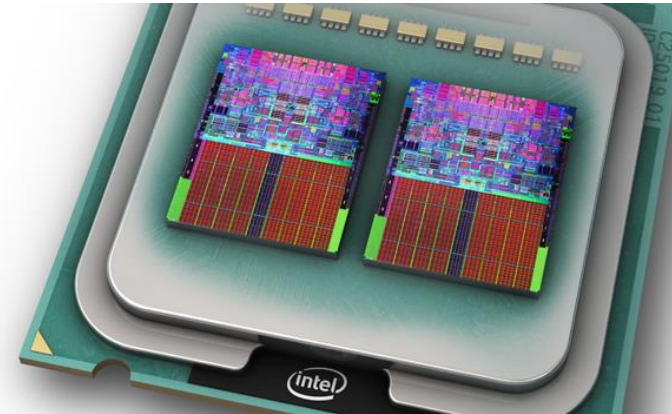


Greet Vanden Berghe

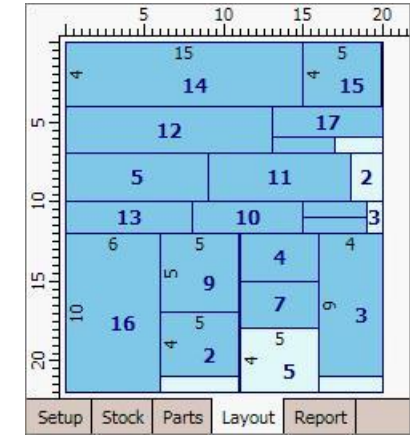
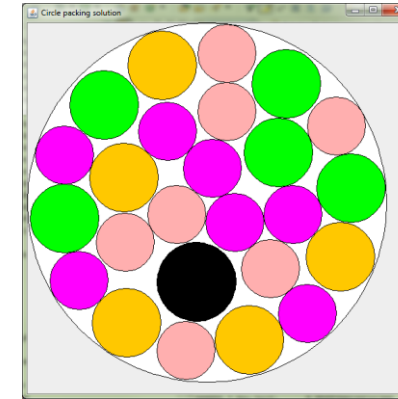
Timetabling, Rostering
Vehicle routing

Health care – Manufacturing – (Internal) Logistics

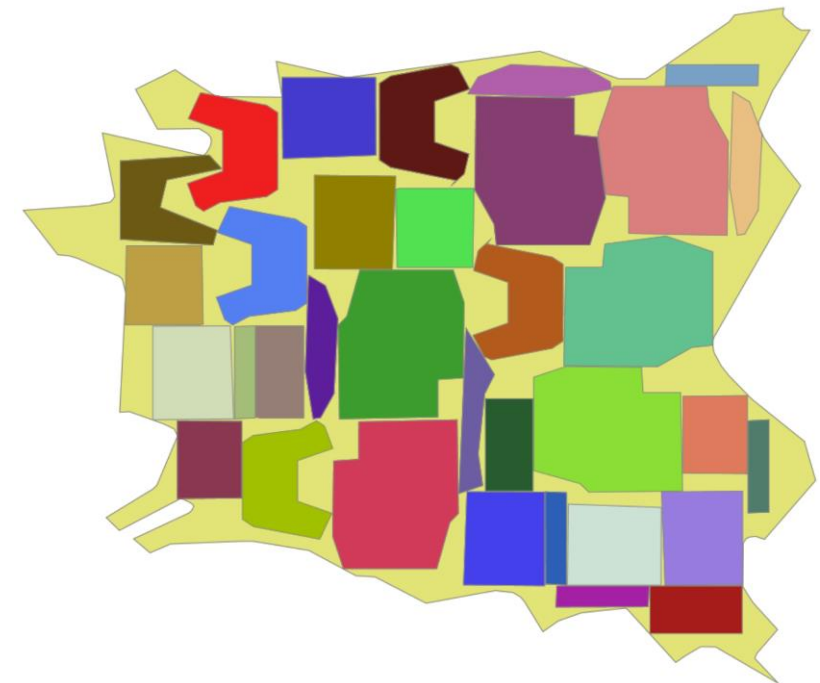
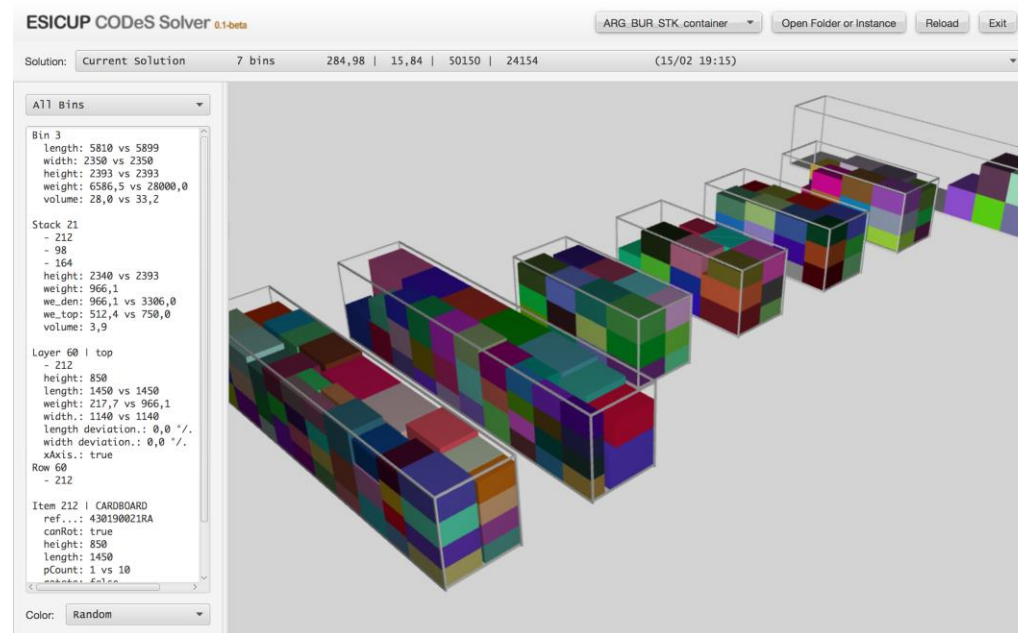
Parallel optimisation algorithms



Cutting & Packing Optimization



- 1D, 2D, 3D
- Containers
- Pallets
- Cutting Stock
- Irregular shapes
- Real-world constraints





HEALTH



LOGISTICS



MANUFACTURING



Research Tracks – DistriNet@Gent

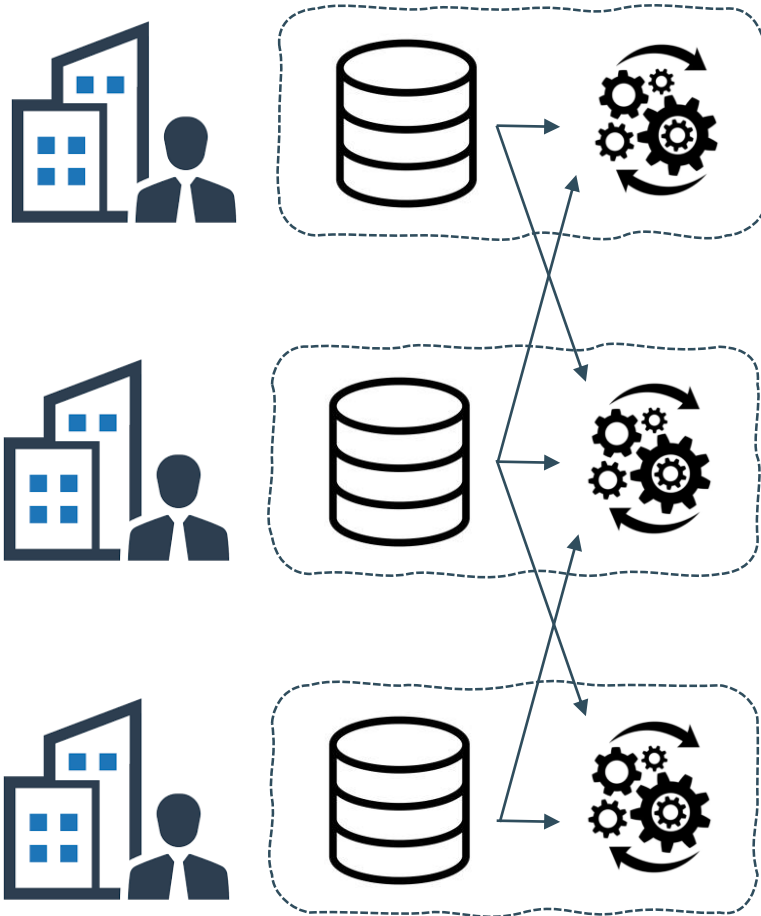
1. Controlled release of sensitive datasets
2. Vulnerability assessment of IoT firmware
3. Mitigating impact of software vulnerabilities

Controlled release of sensitive datasets

DistrIN_≡t



Problem statement




- **Increasing data collection**

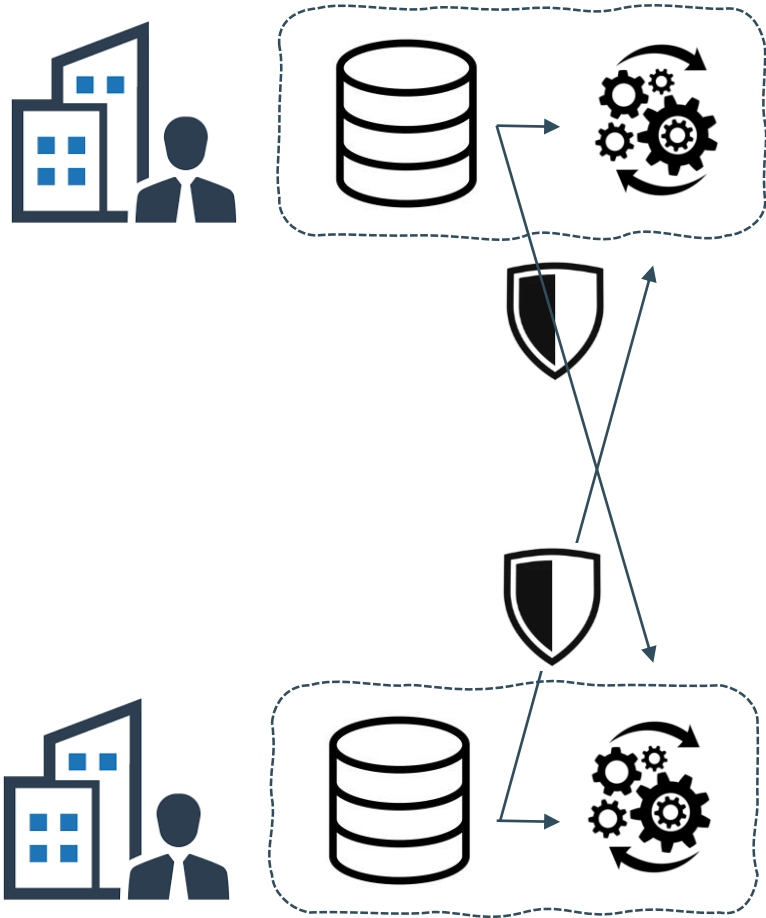


- » Fine-grained data collection
- » Integrating external data sources
- » *Increasing storage capacities*

- **Increasing processing power**

- » Machine learning and AI technology 
- » Optimization algorithms
- » *Increasing computing power*

Problem statement



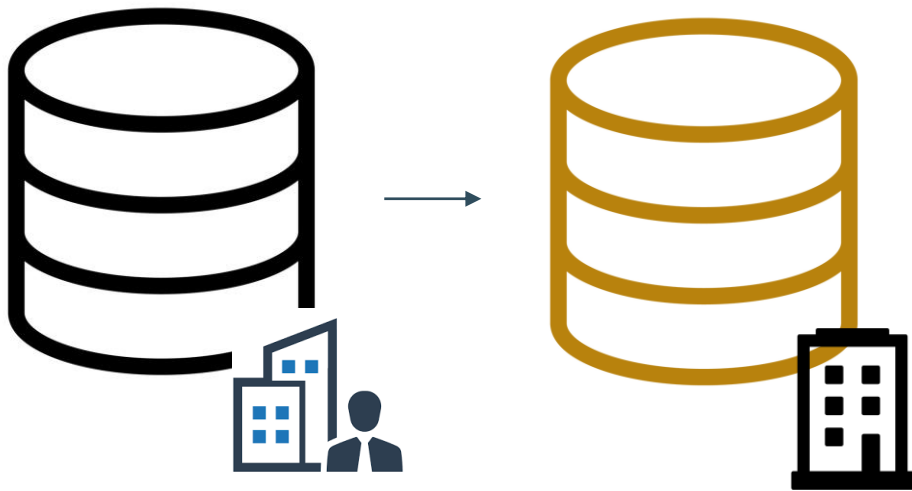
> **Why *controlled* release?**

- » Compliance with privacy regulation
- » Discrimination
- » Reputation damage
- » Economic loss

> **How *controlled* release?**

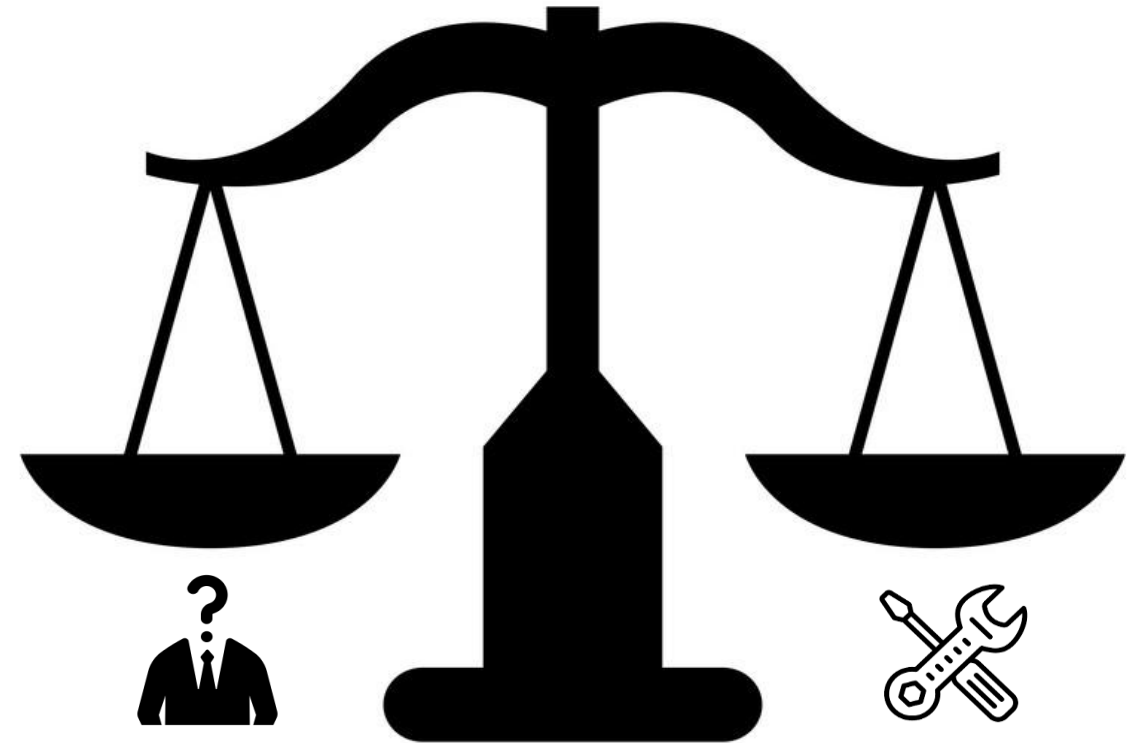
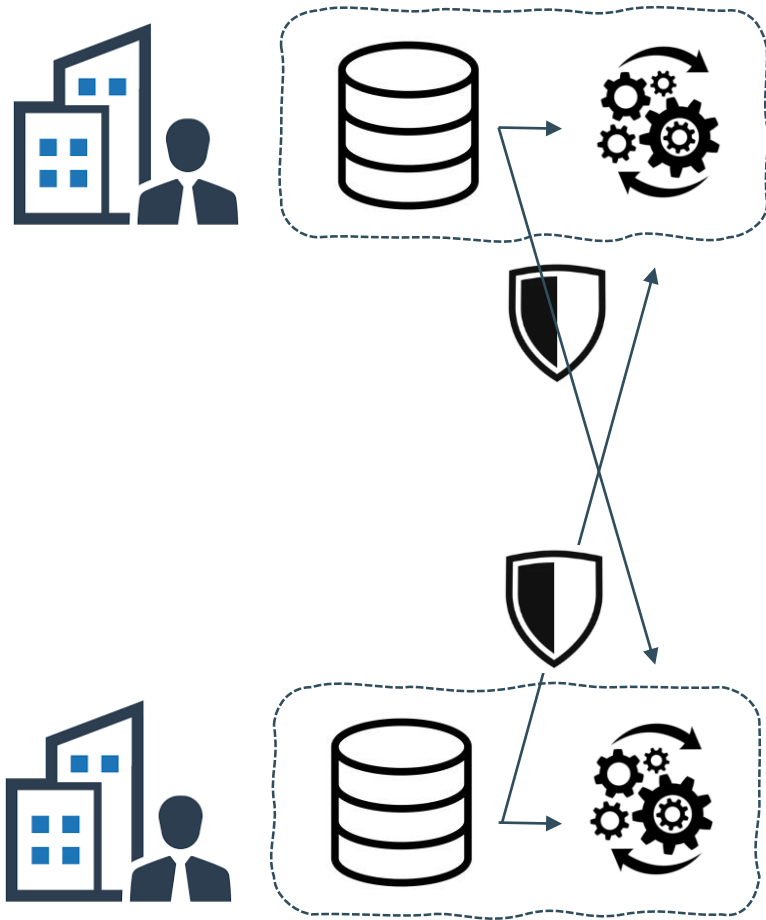
Research Theme:

Controlled dataset transfer :: anonymization

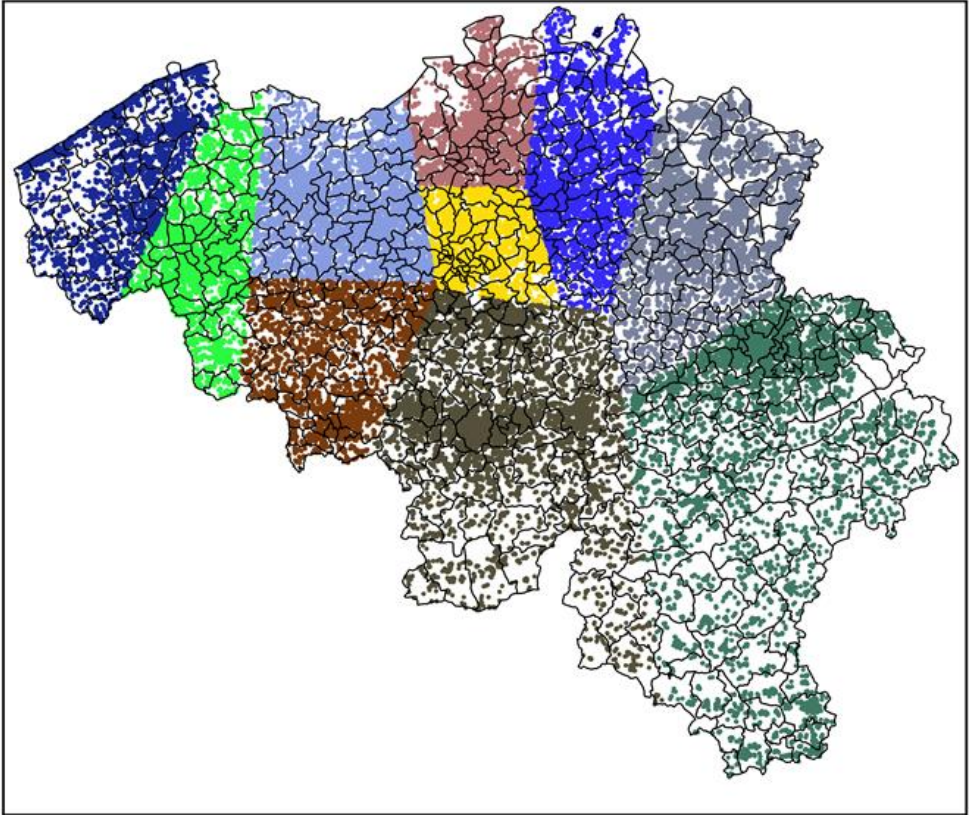
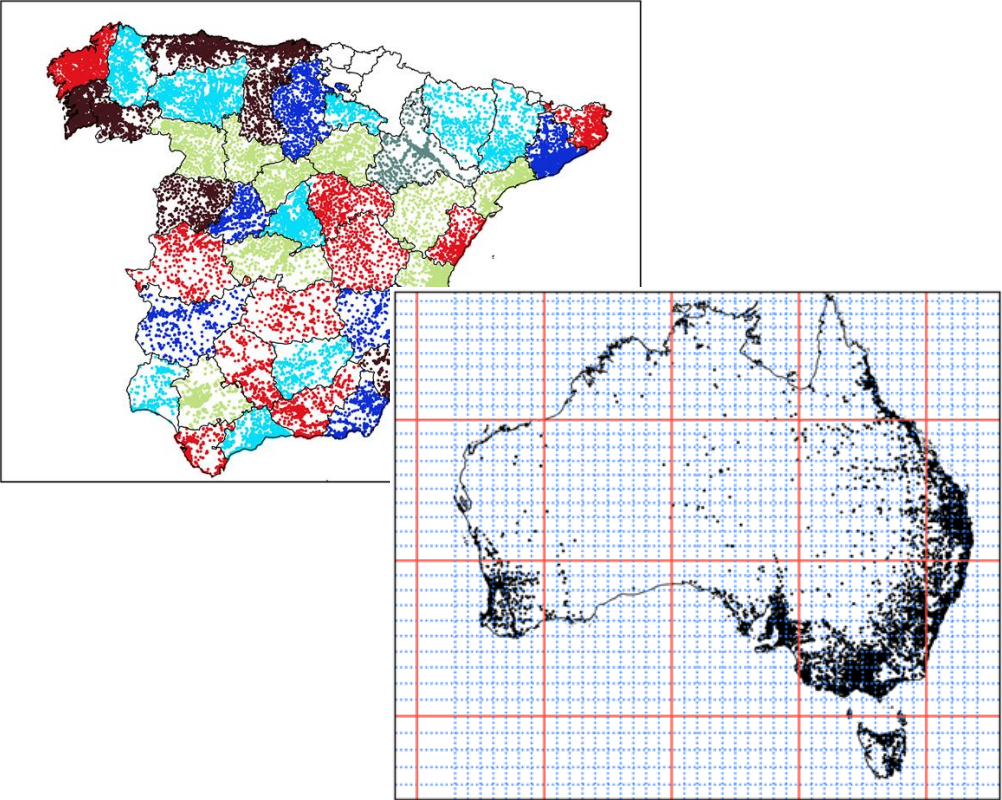


- **Non-perturbative techniques**
 - » Generalization
 - » Sampling
 - » Outlier suppression
- **Perturbative techniques**
 - » Randomization
 - » Data swapping
 - » Noise addition

Challenge 1: Improving the privacy/utility balance



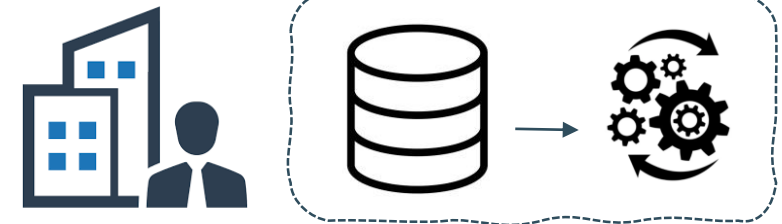
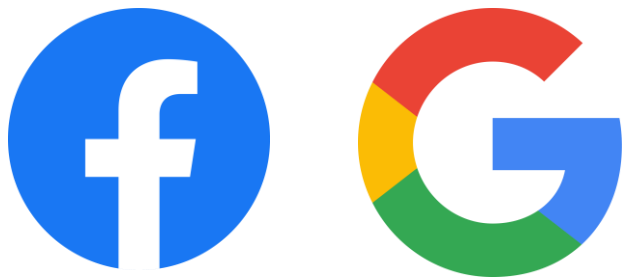
Challenge 2: Intelligent Generalization



Challenge 3: Advanced attacker models

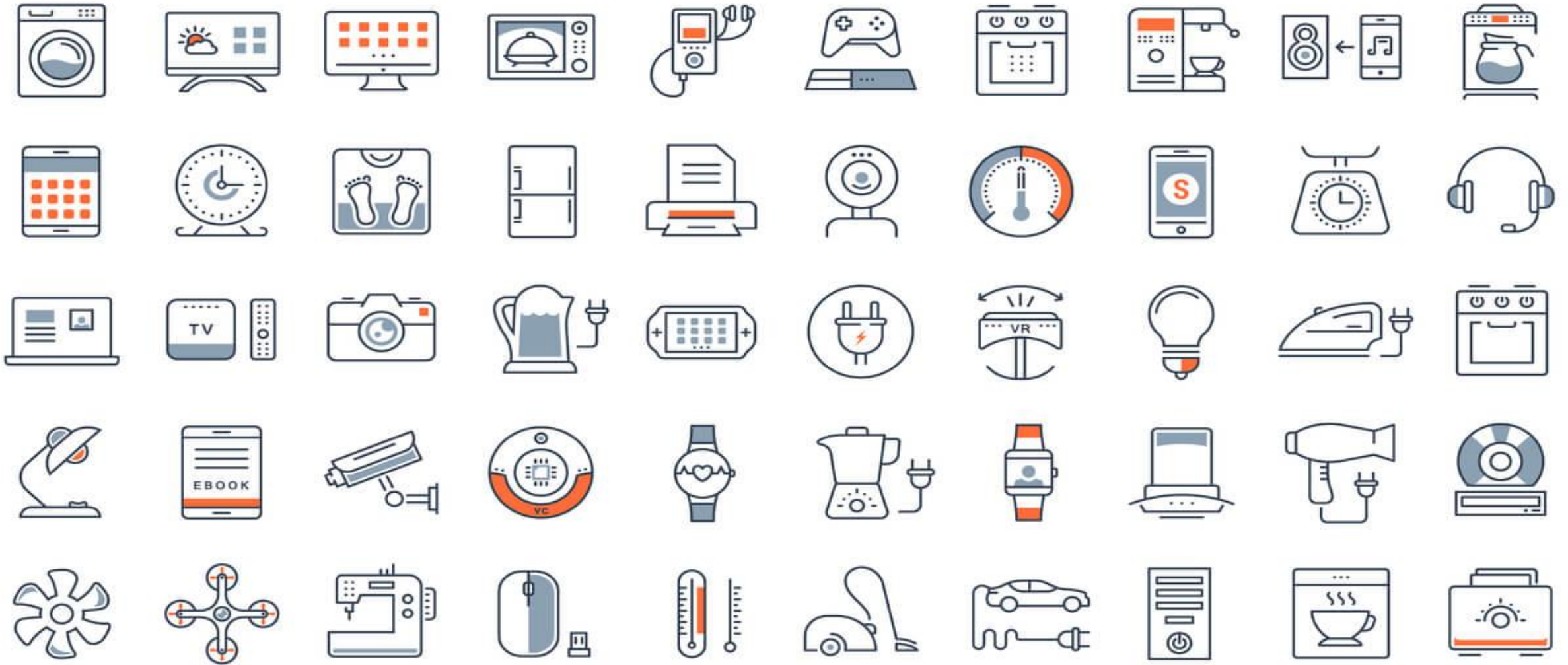
- Enriching with public data

- › Colluding service providers



Vulnerability assessment of IoT firmware

Problem statement



TM Tech Monitor

Hackers increasingly targeting Internet of Things devices

There has been a **92% rise in IoT-based attacks** year on year, rising 200% in North America. Malware attacks remained mostly steady since the beginning of 2021.

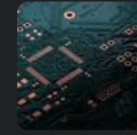
26 Oct 2022



H The Hacker News

New Flaws in TPM 2.0 Library Pose **Threat to Billions of IoT**

A pair of serious security defects has been disclosed in the Trusted Platform Module (TPM) 2.0 reference library specification that could potentially lead...



A New Attack Reveals Everything You Type With 95 Percent ...

Their work is actually a follow-up to a 2008 hack by MIT researchers, ... **being used against IoT gadgets** and better protect their products against them.

3 days ago

TC TechCrunch

Hackers exploit Citrix zero-days

TechNative

Home > News > Security

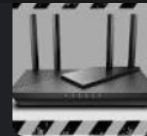
Cybercriminals Using ChatGPT to Build Hacking Tools, Write Code

AW Tripwire

Patch now! **The Mirai IoT botnet is exploiting TP-Link routers**

The high-severity security vulnerability was first disclosed by bug hunters in December 2022 at the Pwn2Own hacking contest in Toronto, earning them a US \$5,000...

04 May 2023

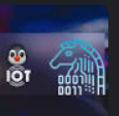


H HackRead

Patched OpenSSH **Exploited for IoT**, Linux Cryptomining

HACKREAD is a News Platform that centers on InfoSec, Cyber Crime, Privacy, Surveillance and Hacking News with full-scale reviews on Social Media Platforms &...

1 month ago



Dataconomy

What Is Flipper Zero And How Does It Work

Marketed to "geeks," red team hackers, and pen testers, Flipper Zero is ... of Flipper Zero as a **universal key for IoT**, which is somewhat misleading.

1 hour ago



Track 1: Framework for generating vulnerable Firmware

Benchmark
image

Full control of
content

Full disclosure
of tool
performance

Firmware Benchmark Generator

B4IoT [Home](#) [Generator](#)

Architecture:

Select your architecture:

- Latest Alpine Linux x86
- Alpine Linux x86 v3.14
- latest Alpine Linux for ARM32 v7
- latest Alpine Linux for ARM32 v6
- latest Alpine Linux for ARM64 v8
- latest Alpine Linux for i386
- latest Alpine Linux for ppc64le
- Alpine Linux for riscv64 edge
- latest Alpine Linux for s390x

Confirm

Track 2: Assessment of vulnerability detection tools

Tools (sometimes)
overpromise

Use benchmark to assess
vulnerability detection tools

	FACT	EMBA	Firmwalker	FwAnalyzer	TROMMEL
Weakly configured SSH	◐	◐	○	○	○
Weakly configured vsftpd	○	○	○	○	○
Weakly configured Telnet	○	◐	○	○	◐
Misplaced sudo right	○	●	○	◐	○
Vulnerable cronjob configuration	◐	●	○	○	○
Plaintext credentials	●	●	○	●	●
Password leak	●	●	◐	○	●
SSH with backdoor	○	○	○	○	○
Exploitable CoAP resource	○	○	○	○	○
Exploitable REST API	○	○	○	○	○
Exploitable HTTP server	◐	●	◐	○	◐
Exploitable Apache server	◐	●	◐	○	◐
Vulnerable Bash source code	○*	◐*	○	○	○
Vulnerable C binaries	○	◐	○	○	○
Vulnerable Java binaries	○	○	○	○	○
Vulnerable Python source code	○*	◐*	○	○	○



Mitigating impact of Software Vulnerabilities

DistrIN**≡t**

Track 1: Exploit Mitigations

- **Challenge:**

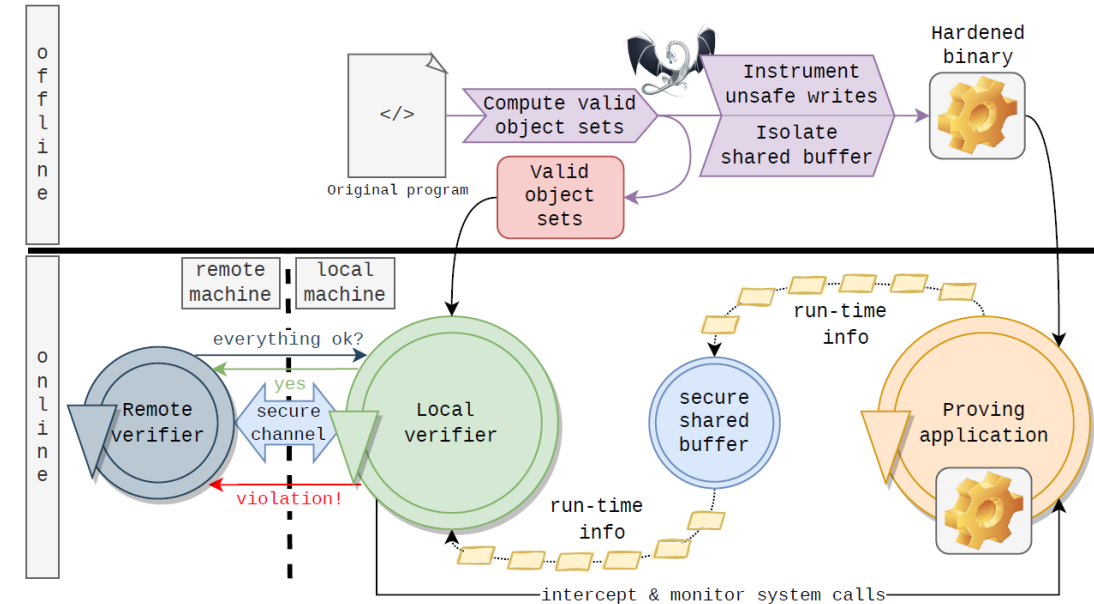
- » low-level software (e.g., operating systems, browsers, servers, SCADA systems, ...) is notoriously complex
- » security vulnerabilities are unavoidable
- » hackers (ab)use these vulnerabilities to infiltrate systems, install malware, steal data, ...

- **Solutions:**

- » integrity protection
- » software diversity
- » multi-variant execution

Track 1: Integrity Protection

- Analyze sensitive software
- Build a model of its benign behavior
- Add safety checks to catch (likely) malicious behavior
- State-of-the-art data-flow integrity system built in collaboration with Huawei



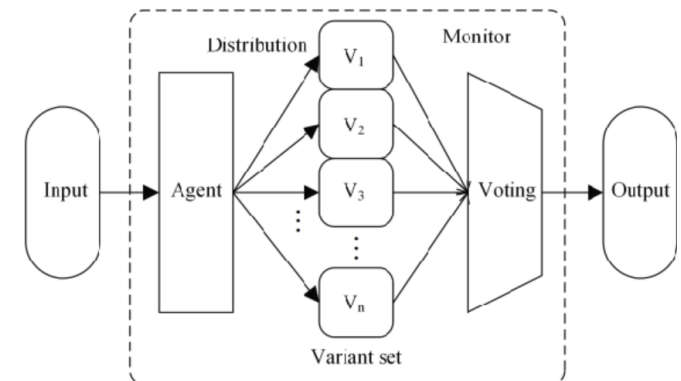
Track 1: Software Diversity

- Exploits/attacks typically target one specific instance/version of the program
- **Software diversity** techniques can automatically generate (a potentially infinite number of) different program versions
- All versions are semantically/functionally equivalent but look different
- Exploits only work on one version
- **Software diversity** creates **digital herd immunity**
- European projects in collaboration with UniBw Munich, SCCH, EPFL, JKU, and many industrial partners



Track 1: Multi-Variant Execution

- Software diversity on steroids
- Run multiple program versions on the same inputs and compare their output/behavior
- Normal operation: output/behavior is identical
- Under attack: output/behavior diverges
- Most advanced multi-variant execution system in the world developed here!
- Several projects sponsored by FWO, DARPA, ONR
- Industrial partners in defense industry



Track 2: Safe Language Migration

- Modern programming languages provide immunity to common software vulnerabilities
- Migrating existing software to modern languages is extremely tedious
- Ongoing research/outreach projects:
 - » Teach local companies how to use the **Rust programming language** and how to migrate software
 - » Build tools and techniques to automate/facilitate migration

