riscure

driving your security forward

FIRMWARE TESTING

MARC WITTEMAN

OUTLINE

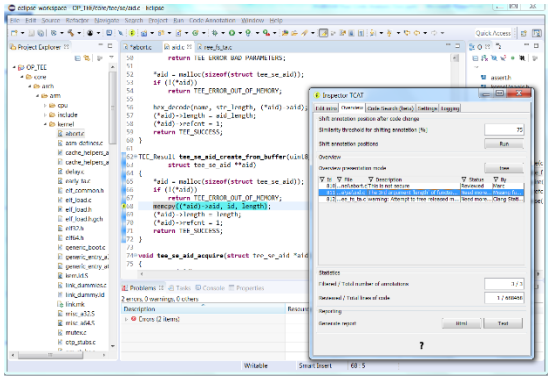
- Introduction
- Firmware security
- Static vs Dynamic testing
- Fuzzing challenges
- Approach
- Demo
- What’s next?

We are Riscure

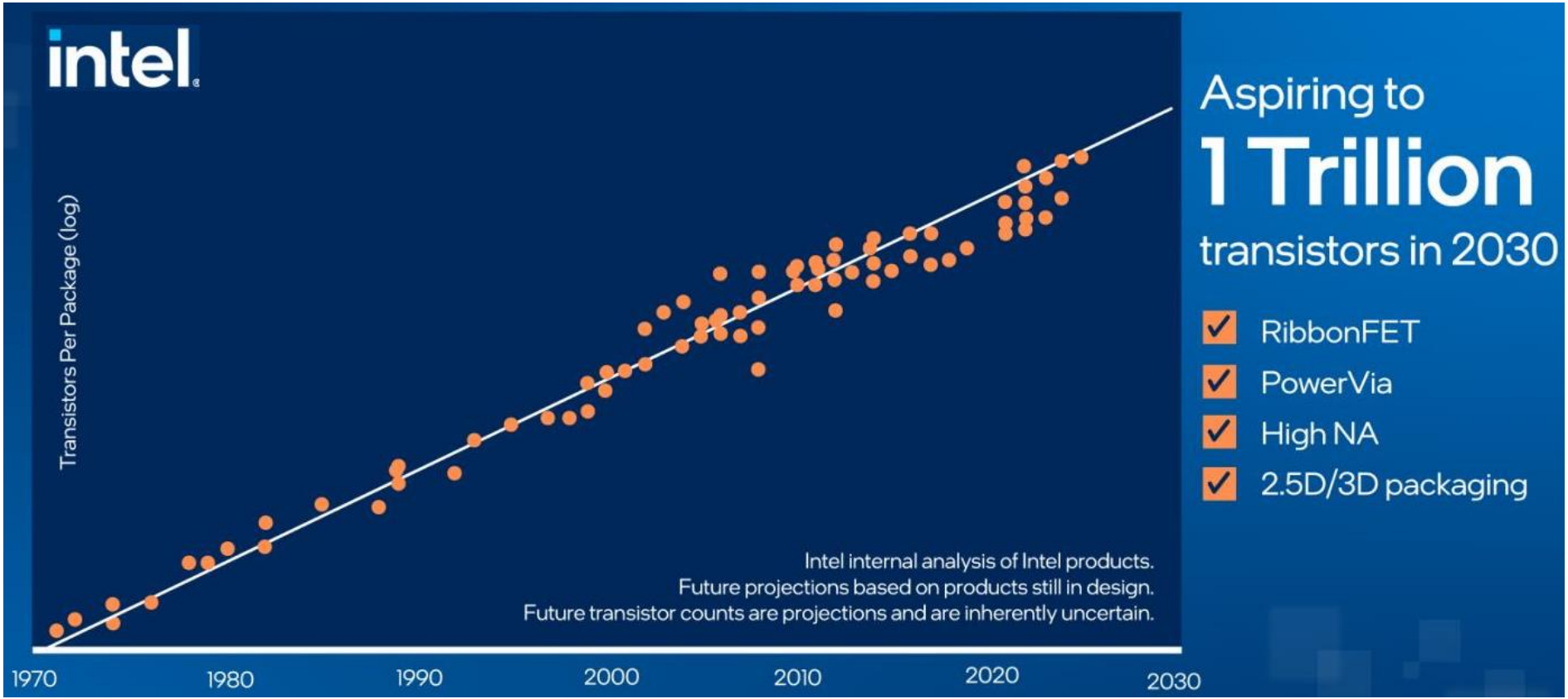




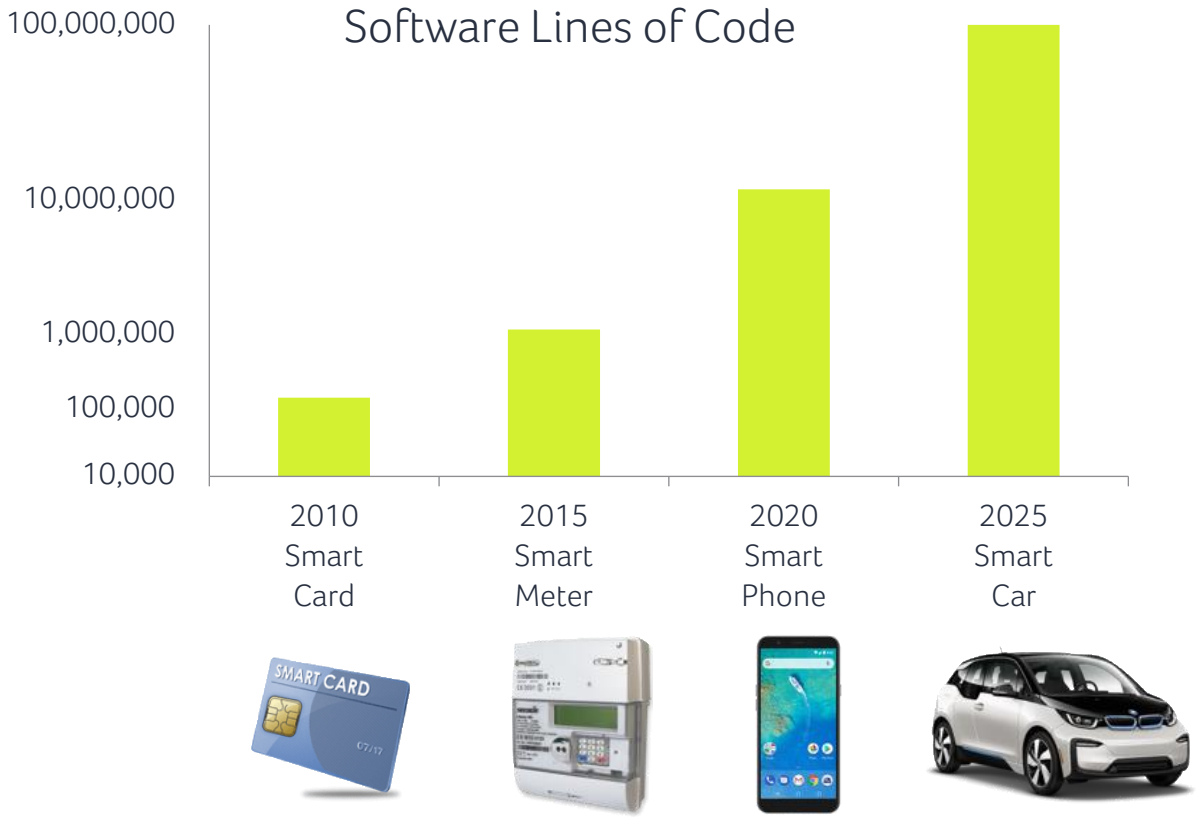

- We care about **devices** that must be **secure** in a hostile environment
- We serve customers with our security **test tools**, **services**, and **training**
- We develop ~~attack~~ test methods and tooling




MOORE'S LAW RULES



SOFTWARE COMPLEXITY BECOMES DAZZLING



CODE REVIEW VS AUTOMATED ANALYSIS

Why code reviews are still needed but also a dead end

- Immature code has 1 vuln / kloc
- Analysts can review 1 kloc / day

} Analysts find 1 vulnerability / day

→ Manual reviews bring results, but it doesn't scale to 100kloc+ code bases

- Tooling exists, but suffers from multiple issues:
  - False positives (excessive warnings that turn out to be innocent)
  - False negatives (missed issues due to limited coverage and depth)
  - Weak reporting (what and where is the problem)

→ There is an urgent need for better tooling

FIRMWARE SECURITY

Why firmware is more sensitive than application software

Firmware sits directly on the hardware. It differs from other software in multiple ways:

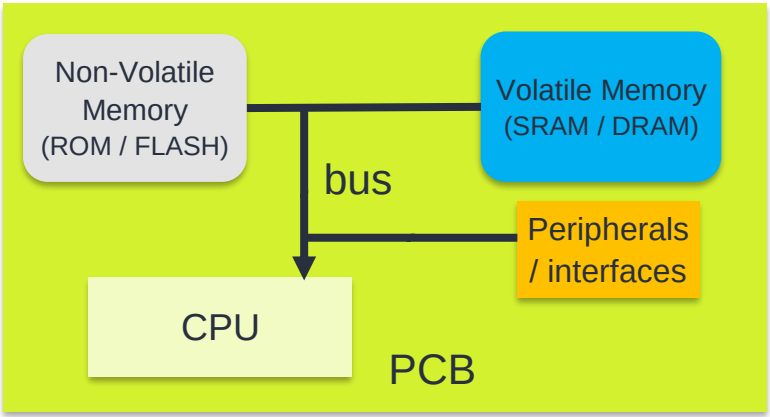
- Full access to all HW/SW components → coding flaws may compromise complete product
- Heavy dependance on hardware properties → sensitive to hardware weaknesses

Storage evolution allowed firmware to grow and become updateable

Security perspective: firmware enables or mitigates attacks that exploit hardware weaknesses

DEVICE FIRMWARE THREATS

How is firmware security affected by hardware?



Devices contain a Printed Circuit Board, with components connected via a bus

Firmware dependencies on hardware:

1. Address agnostic
   → threat: out-of-bounds access & wild code jumps not prohibited
   → test through logical security tests
2. Physical constraints (e.g., clock frequency and operating voltage)
   → threat: Glitching
   → test through fault testing

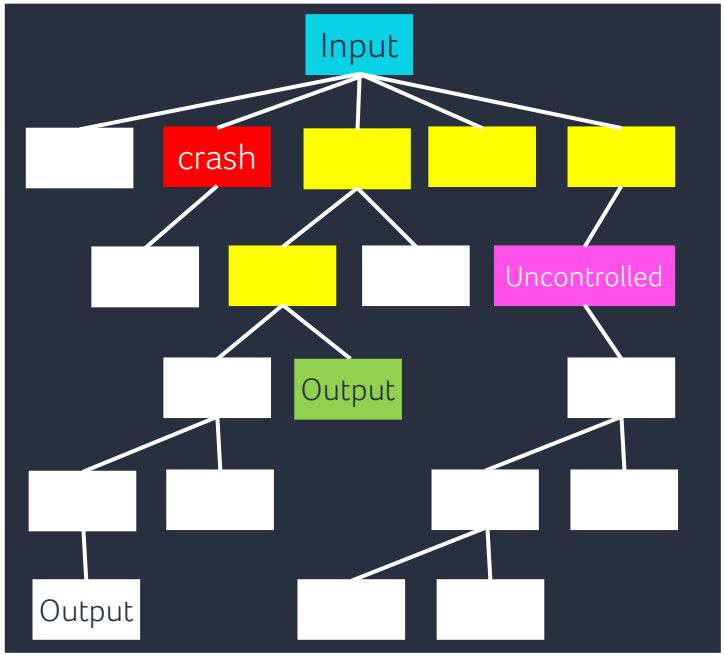
We develop a test platform that addresses both threats

SECURITY TESTING: STATIC VS DYNAMIC

- Static Code Analysis
  - Analyze code like a human, search for specific issues
    e.g., integer overflow, input validation, etc.
  - Hard to judge exploitability → false positives
- Dynamic Code Analysis
  - Run code with ‘exhaustive’ inputs and monitor coverage and outputs/crashes
  - Complex to configure and understanding results
  - We addressed these aspects to support developers with limited security expertise
    - White-Box fuzzing to detect logical issues in source code
    - Fault Simulation to detect fault injection weaknesses in source code

FUZZING CHALLENGES

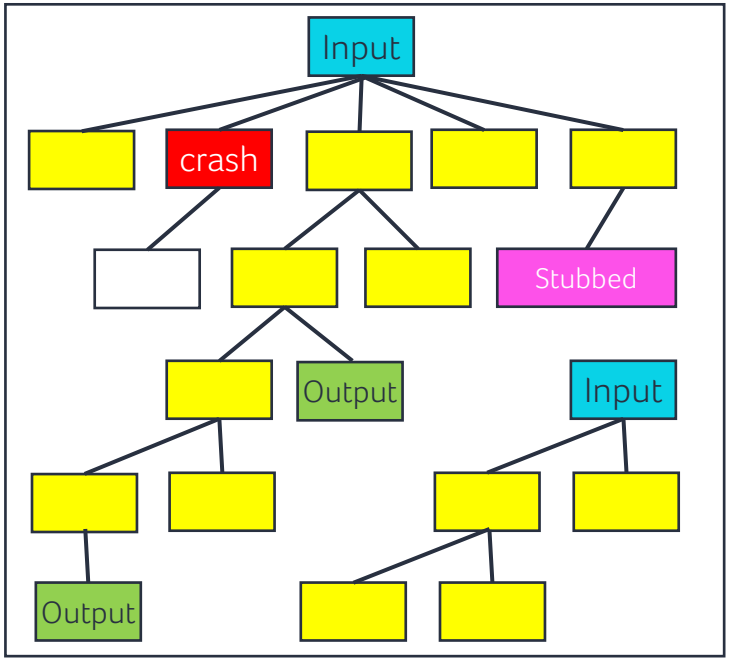
Understanding the nature of fuzzing



1. Building a harness to map fuzzer input on function parameters
2. Achieving and observing coverage
3. Uncontrolled functionality (HW or state)
4. Debugging crashes
5. Workflow alignment

WHITE BOX FUZZING IN TRUE CODE

How True Code addresses the fuzzing challenges



1. Building a harness
   → automated harness creation
2. Achieving and observing coverage
   → white box coverage reporting
3. Uncontrolled functionality (HW / state)
   → stubbing support
4. Debugging crashes
   → source identification + sanitizer analysis
5. Workflow alignment
   → both GUI and CI/CD interface

Demo

OPEN ISSUES

Riscure wants to lower the barrier for fuzzing,
by simplifying the process while producing actionable results

Example research topics:

- Detecting other issues than crashes
- Improved handling of hardware dependencies and states
- Acceleration (AI?)

Riscure offers internships to students who like to
research fuzzing topics and make them practical

Questions?

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90
www.riscure.com

Riscure North America
550 Kearny St., Suite 330
San Francisco, CA 94108 USA
Phone: +1 650 646 99 79
inforequest@riscure.com

Riscure China
Room 2030-31, No. 989, Changle Road,
Shanghai 200031
China
Phone: +86 21 5117 5435
inforcn@riscure.com

riscure

driving your security forward