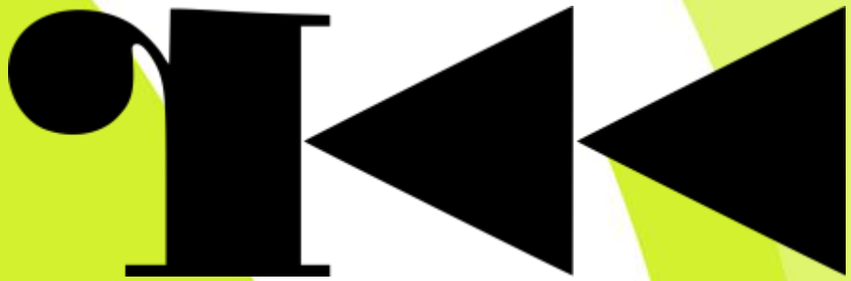
riscure



CON

2017

Rhme3

The world's first automotive CTF

Eduardo Novella & Dana Geist

Agenda

1. About Riscure
2. Rhme series
3. What is new about RHme3?
4. How can you participate?

Riscure

1. Side Channels (smartcards, chipsets (SoCs), IoT,…)
2. Fault Injection (smartcards, chipsets (SoCs), IoT,…)
3. Embedded Devices (gas meters, routers, STBs, IoT,…)
4. Software (TEE, HCE (mobileSec), DRM, WB crypto)
5. Tooling (Inspector and its HW gadgets)

What is Rhme a.k.a Riscure Hack ME?

Embedded hardware CTF

DO
ALL THE CHALLENGES!
memegenerator.net

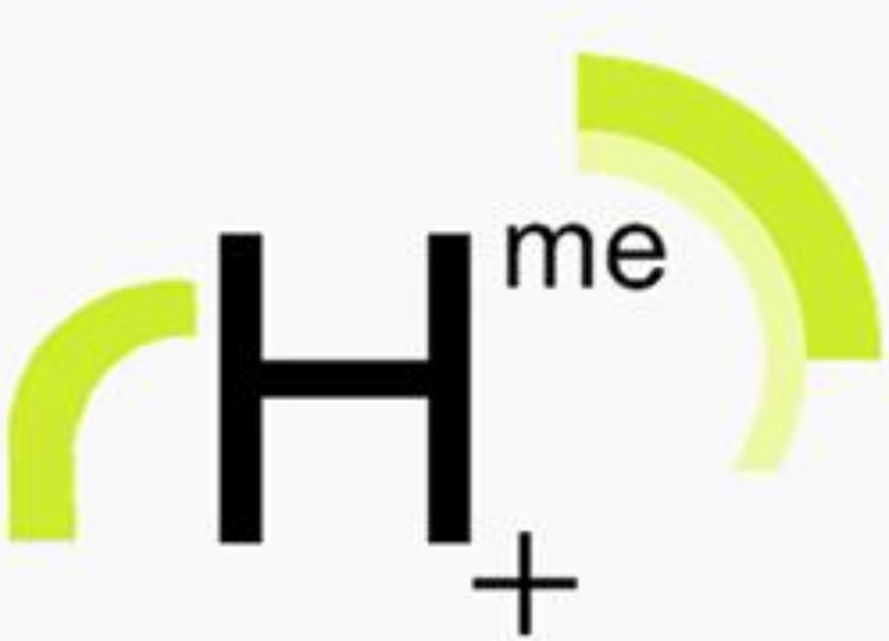
Rhme Series

2015

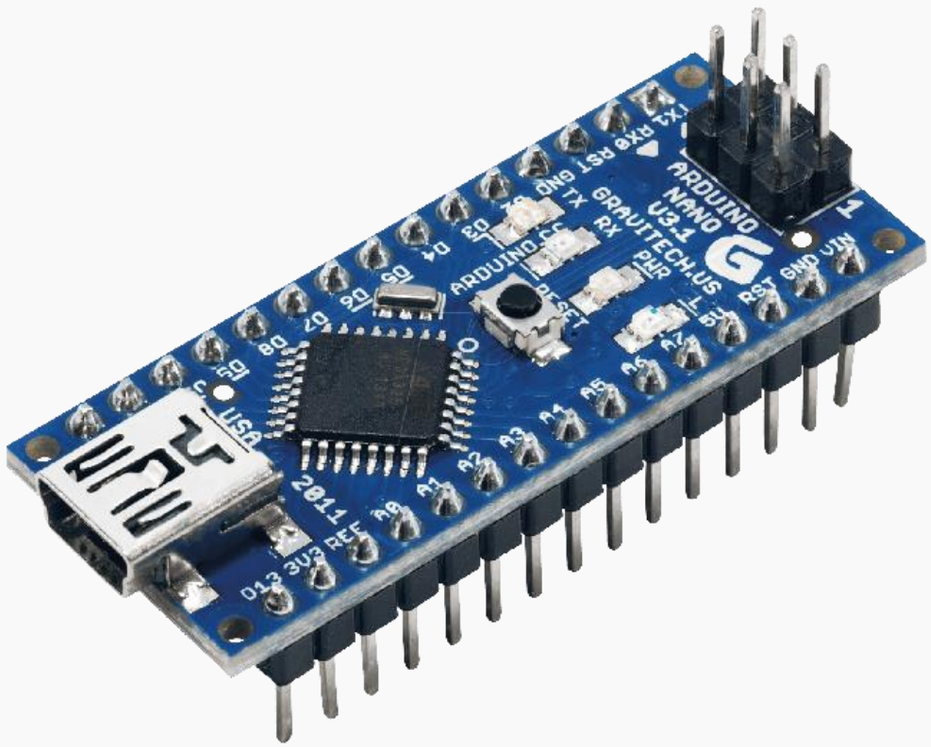
2016

2017

Rhme



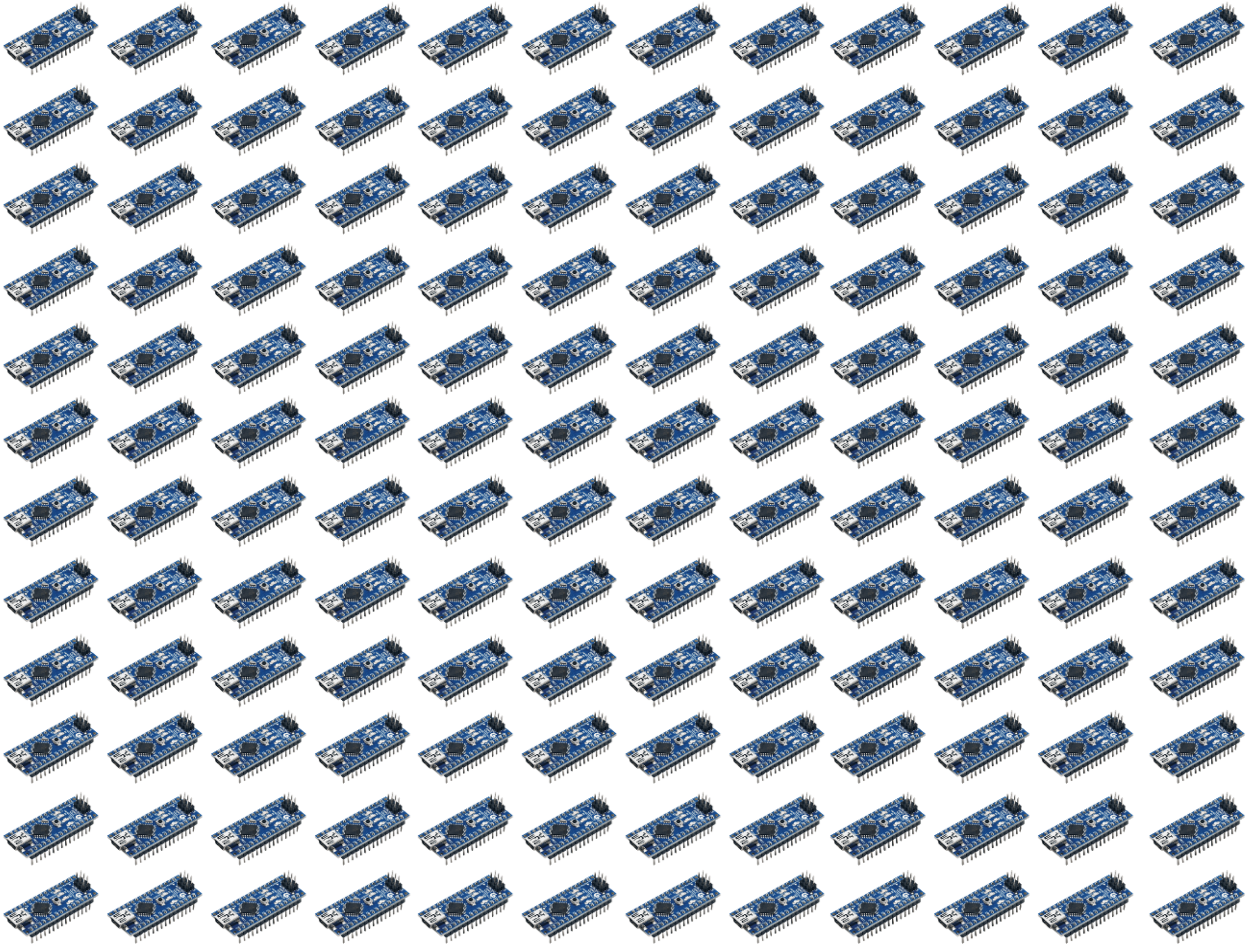
- CTF challenge running in an Arduino Nano clone
- First hardware CTF ever published



Team

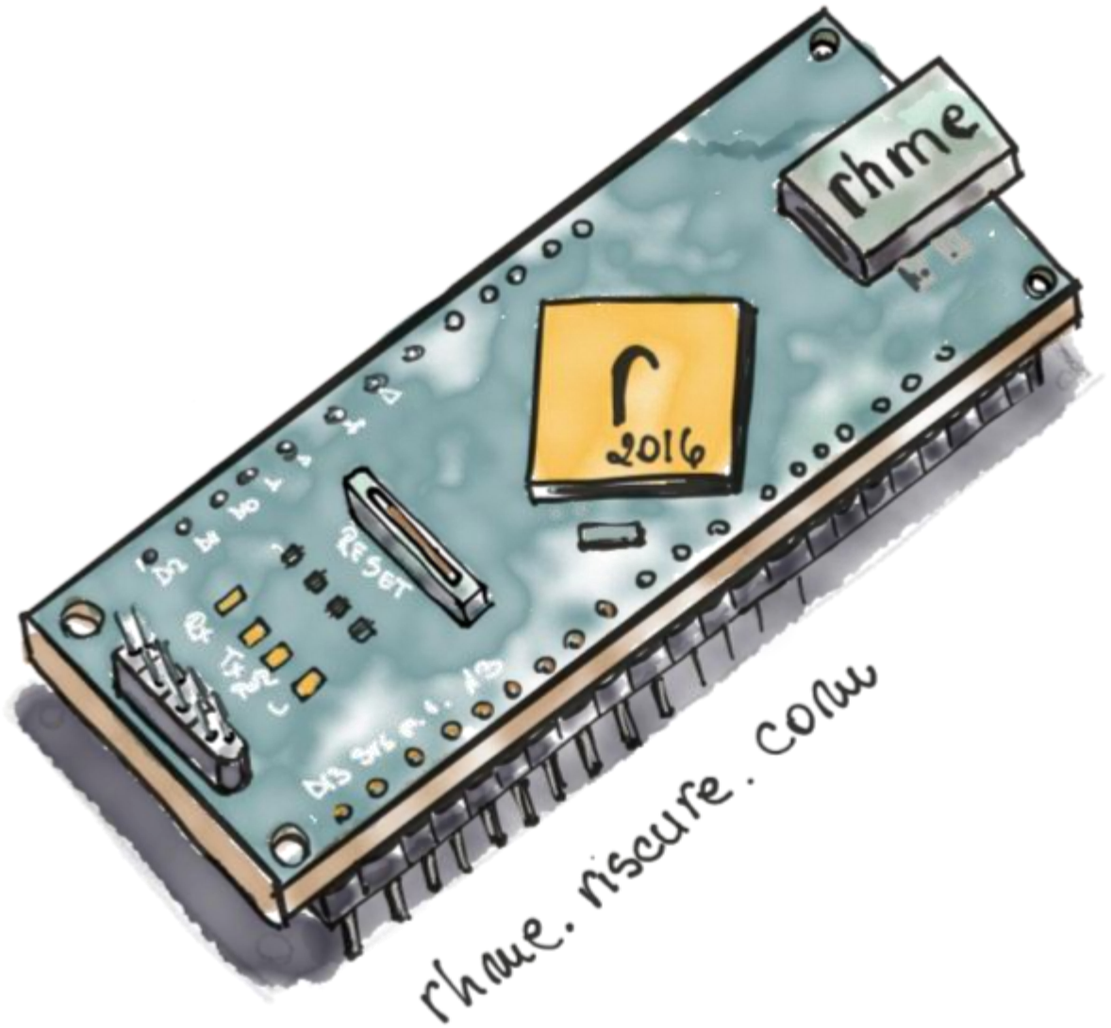
Alexandru Geana

Ramiro Pareja



CISCO
TM

Rhme2



Embedded hardware CTF

- Usual types of challenges
- Side Channel Analysis
- Fault Injection
- Other PCB-related challenges

the Faulty Islands
Finetuning
Revenge
Fiesta
Fiasco
twist wasp
Emergency Transmitter
the state of Crypto
Ave keyserver
AVR Secure Filesystem v1.9.r1.
Sergei's secret sauce
AVR Secure Filesystem
whoe-a-mole
Animals
Casino
Photo manager
weird machine
United Exploitation
Hide and Seek
Jumpy
impostor
FridgeJit
Piece of Snake
Still not scary
Escalate
Republic of Side Channel Analysis
Desert of Reversing
Boot loader Territory

Team

riscure

rH_2^{me}

Player solves challenge and reserve board

Riscure sends RH_2^{me} boards

early November 2016.

Player registers board

early November 2016

Private key is personalized

early November 2016.

Load challenge into board

November – January
2016 2017

Download an encrypted challenge

Solve the challenge

Winners

riscure

Hydra Bus

1

Gijs

2

4

Balda

3

SOS1

5

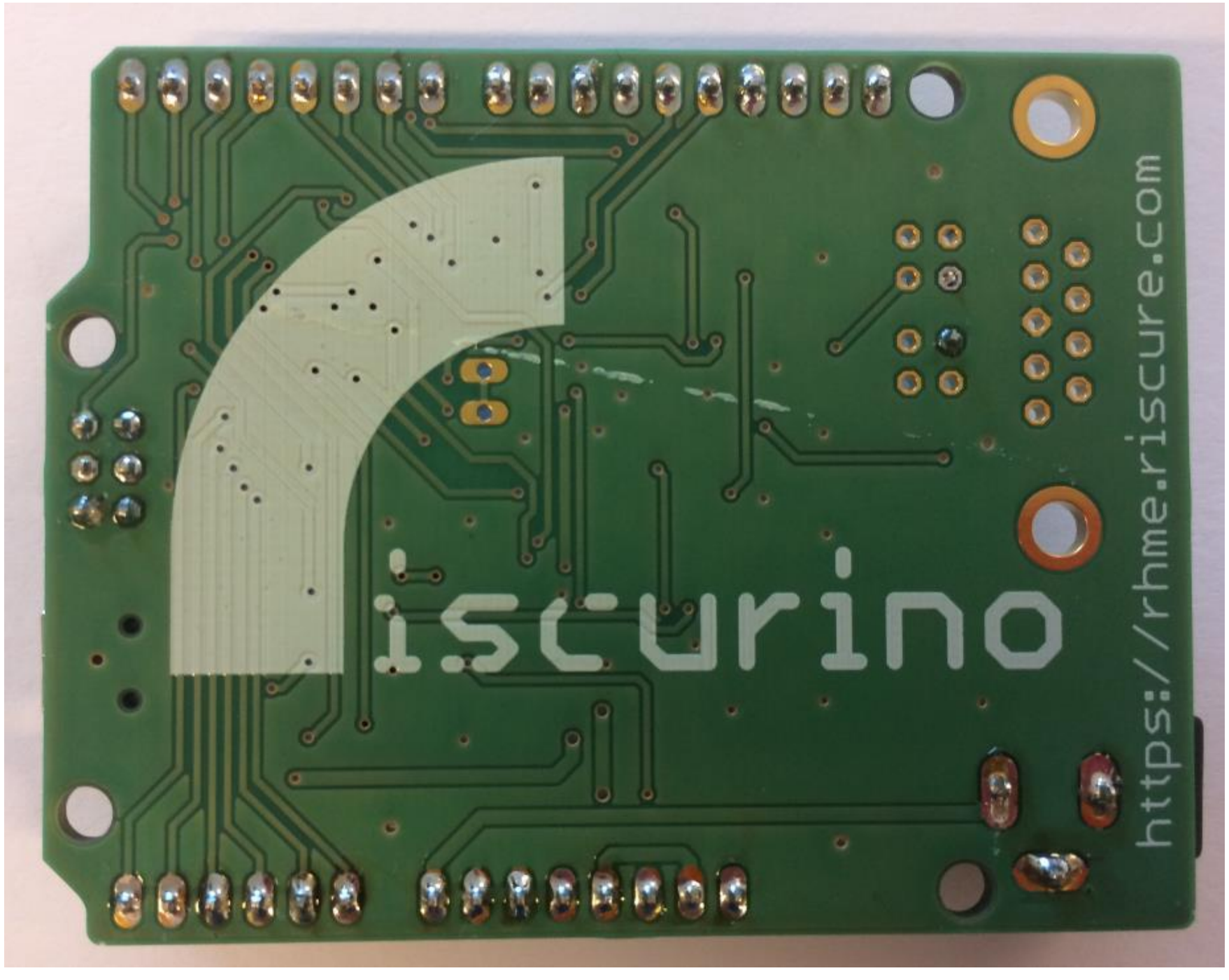
What is new about

Rhme3

- Embedded CTF created by Riscure in partnership with Argus Cyber Security.
- Automotive flavor
- Challenges that simulate real-life scenarios

Rhme3

A custom board has been developed for RHme3!

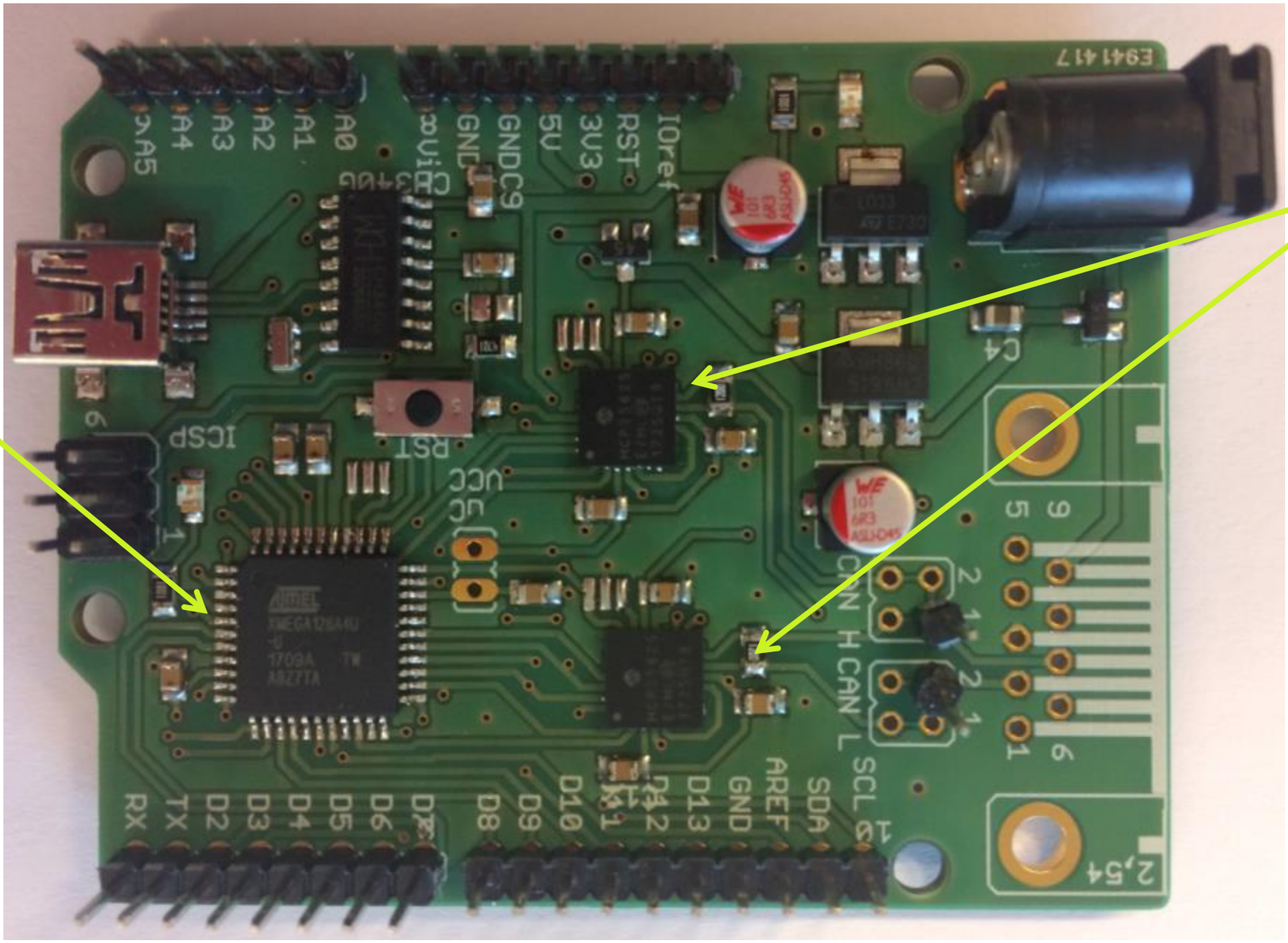


RHme3

A custom board has been developed for the RHme3!

Atmel XMEGA

CAN controllers



RHme3

- The pre-qualification stage finished on the 28th of August
- It included three challenges
  - Exploitation
  - White-box cryptography
  - SCA
- We had a limit of 500 boards, and participants had to solve at least one challenge to qualify for a board
- ~1000 participants registered

internal

riscure

Do you still want to play?

We have 5 boards to give out to the first participants that solve:

- RE binary: **antir2**
- EXP binary: **main.elf**

https://github.com/enovella/r2con-prequals-rhme3

Rules…

- First come, first served
- Solutions to: eduardo@riscure.com
  - Subject : **r2con2017 RHme3**
  - **[name || nickname]**
  - **Write-up including the flag & full r2 log**
- The winners will be announced at the end of the conference and will receive their boards at home in November

USE RADARE TO FIND THE SOLUTION!

Brace Yourselves
RHme3 is coming

RISCURE IS HIRING!
CONTACT US ☺

Eduardo Novella
eduardo@riscure.com

Dana Geist
geist@riscure.com