



# HoliSec

*Holistic Approach to Improve Data Security*

## Bug Bounties – the Past and the Road Ahead

Dr. Ana Magazinius, RISE Viktoria

Dr. Jonas Magazinius, Assured

April 26 2019, 15.00-15.45



ARC CORE

CHALMERS





# Overview

- Automotive bug bounties, state of practice
- HoliSec case
- BusGoat
- Bug bounties, state of research
- The road ahead

# Automotive Bug Bounties (open)

- Hackerone/Bugcrowd:

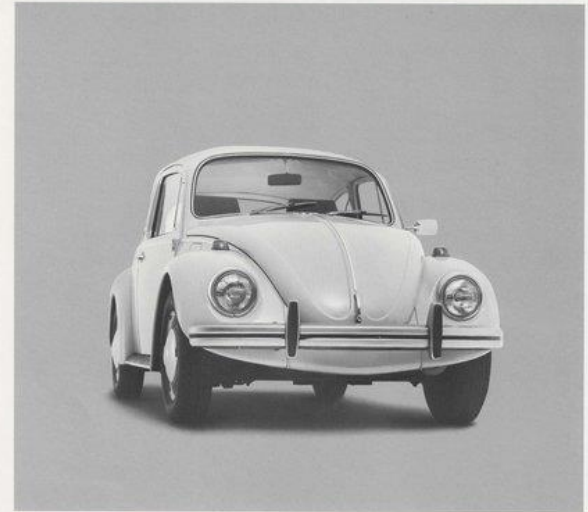
- Vehicles (and web resources):

- Tesla
    - Ford
    - FCA
    - GM

Amat Cama and Richard Zhu of team Fluoroacetate targeted the infotainment system on the Tesla Model 3 and used “a JIT bug in the renderer” to manage to take control of the system. (Pwn2Own conference)

- Web resources only:

- Toyota
    - *Uber*



## Get a bug if you find a bug.

Show us a bug in our VRTX® real-time operating system and we'll return the favor. With a bug of your own to show off in your driveway.

There's a catch, though. Since VRTX is the only microprocessor operating system completely sealed in silicon, finding a bug won't be easy.

Because along with task management and communication, memory management, and character I/O, VRTX contains over 100,000 man-hours of design and testing.

And since it's delivered in 4K bytes of ROM, VRTX will perform for

you the way it's performing in hundreds of real-time applications from avionics to video games.

Bug free.

So, to save up to 12 months of development time, and maybe save a loveable little car from the junkyard, contact us. Call (415) 325-2950, or write Hunter & Ready, Inc., 445 Sherman Avenue, Palo Alto, California 94306.

Describe your application and the microprocessors you're using—Z8000, Z80, 68000, or 8086 family. We'll send you a VRTX evaluation package, including timings for system

calls and interrupts. And when you order a VRTX system for your application, we'll include instructions for reporting errors.\*

But don't feel bad if in a year from now there isn't a bug in your driveway. There isn't one in your operating system either.

**HUNTER & READY**  
**VRTX**  
Operating Systems in Silicon.

\*Call or write for details. But, considering our taste in cars, you might want to accept our offer of \$1,000 cash instead. © 1983 Hunter & Ready, Inc.

1983

# Automotive Bug Bounties (Hackerone report 2018)



“ Hackers have become an essential part of our security ecosystem.

**JEFF MASSIMILLA**

Vice President Global Cybersecurity, GM



**VULNERABILITIES RESOLVED**

**700+**

**COMPANY HEADCOUNT**

**180,000+**

**PARTICIPATING HACKERS**

**500+**

**PRODUCT**

**HackerOne Response**

*As of March 2018*

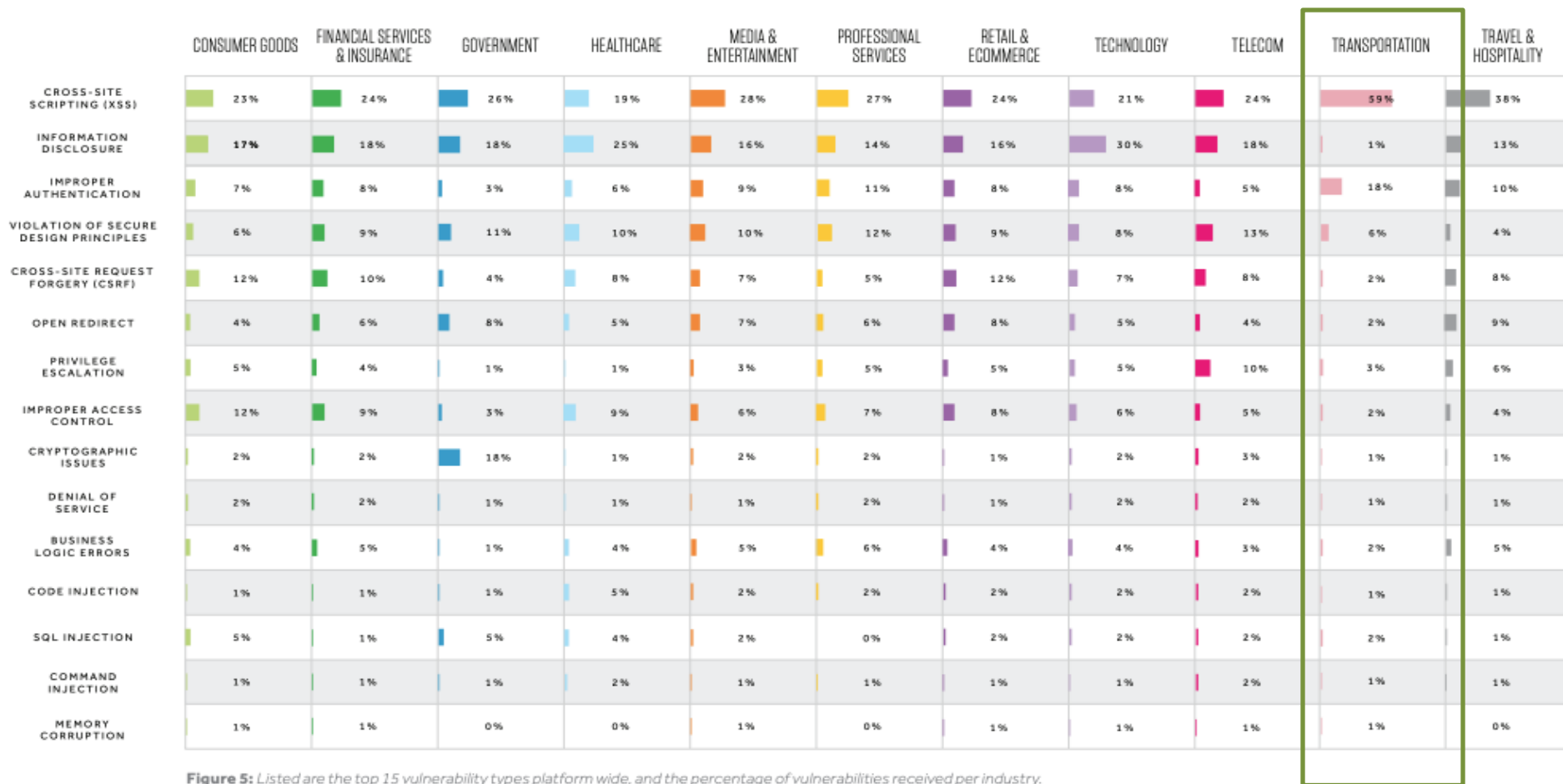
HACKER-POWERED SECURITY REPORT 2018 18

**Percent Total Programs by Industry**

	2014-2015	2015-2016	2016-2017	2017-2018
CONSUMER GOODS	1%	1%	1%	1%
FINANCIAL SERVICE & INSURANCES	11%	9%	8%	8%
GOVERNMENT	0%	0%	2%	2%
HEALTHCARE	0%	2%	11%	10%
MEDIA & ENTERTAINMENT	5%	10%	9%	9%
PROFESSIONAL SERVICES	5%	6%	5%	4%
RETAIL & ECOMMERCE	3%	3%	4%	4%
TECHNOLOGY	60%	59%	58%	58%
TELECOM	1%	1%	1%	1%
TRANSPORTATION	1%	1%	1%	1%
TRAVEL & HOSPITALITY	3%	3%	3%	3%

**Figure 4:** Industries that launched programs from the overall share of programs for that time period.

# Vulnerabilities by Industry





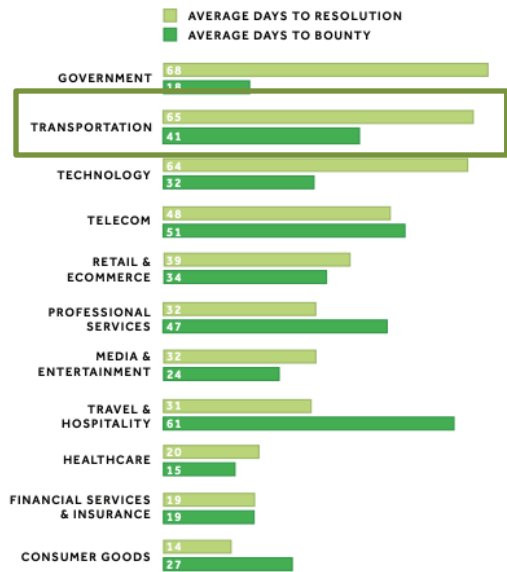
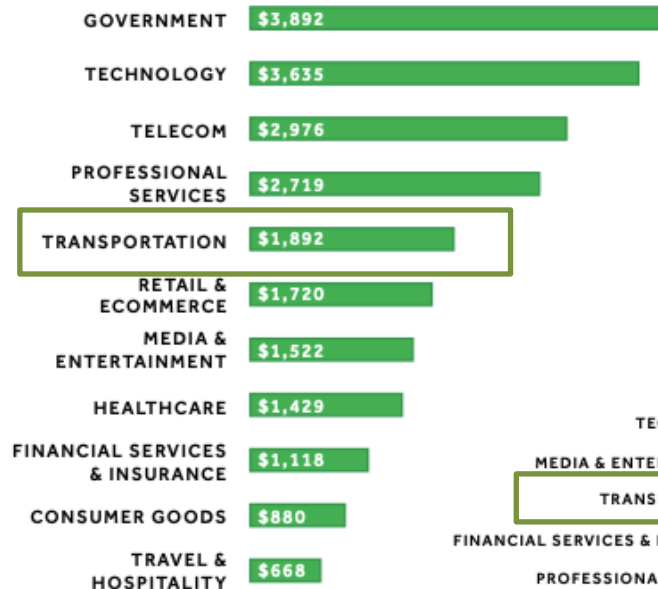


Figure 6: Average number of days to resolution and to reward, measured from May, 2017 to April, 2018.

### Average Bounty Payout Per Industry for Critical Vulnerabilities



### Total Bounties Paid by Industry

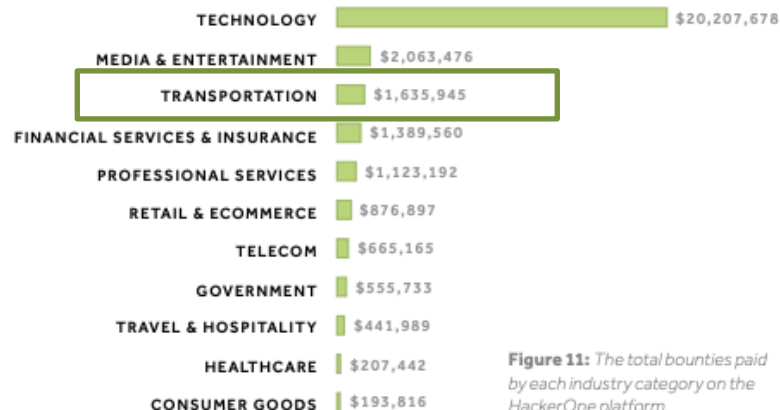


Figure 11: The total bounties paid by each industry category on the HackerOne platform.

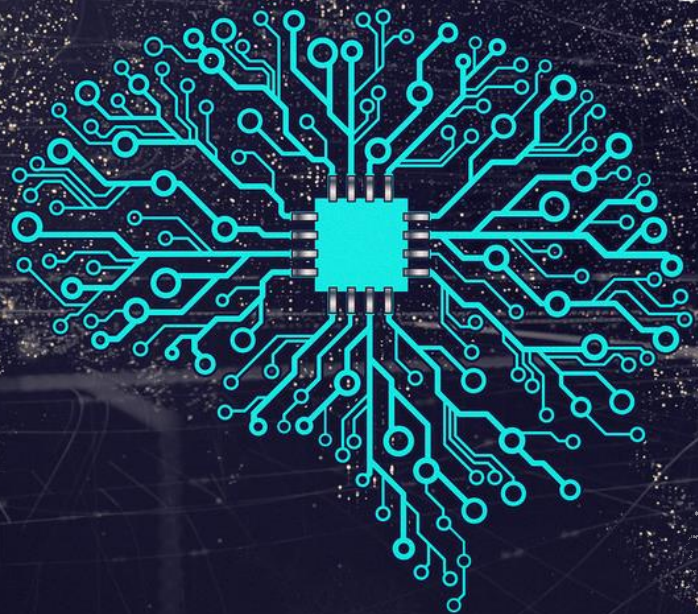
# Automotive Bug Bounties

# HoliSec case

---

- A bugbounty initially planned for 2017
- Postponed past HoliSec end due to resource constraints in the possible time intervals for the event.
- Positive aspects
  - Enthusiasm and will to succeed at AB Volvo
  - Enthusiasm from the security community
  - Many interested bug hunters





- Planning the event
  - A bug bounty involves the entire organisation, formal and informal decision makers.
  - Information sharing within and between organisations is crucial.
  - A bug bounty requires careful timing.
- Hunting bug hunters
  - How do we attract the best?
  - How do we handle disclosure?
  - What do we do when (too) many are interested?

## What did we learn?





# HoliSec

*Holistic Approach to Improve Data Security*

## BusGoat

Jonas Magazinius

September 18, 2018, 15:15– 15:30



ARC CORE

CHALMERS

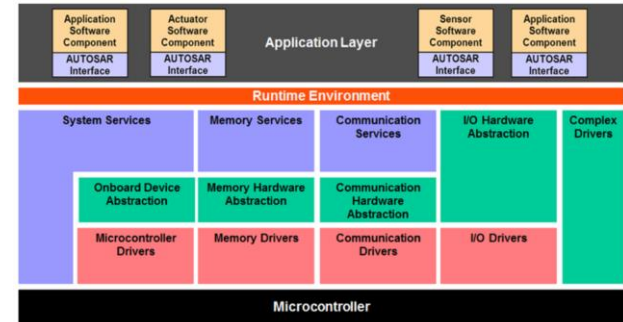


# The BusGoat

- An intentionally vulnerable ECU
  - Several vulnerabilities implemented as challenges
  - Inspired by vulnerable web application WebGoat (stems from “scapegoat”)
- Test automotive security knowledge
  - Intended as a qualifier for the bug bounty
  - Select bug hunters who performed well and showed creativity

# Technology

- The hardware
  - Is based on the MPC5748G DEVKIT from NXP
  - CAN interface
  - Multiple LEDs, potentiometer, buttons
- The software
  - Based on ARCCOREs “Arctic Core”
  - AUTOSAR compliant
  - Custom applications





# Challenge 1

## Objectives:

- To establish CAN knowledge (automotive)
- To establish creative thinking ability

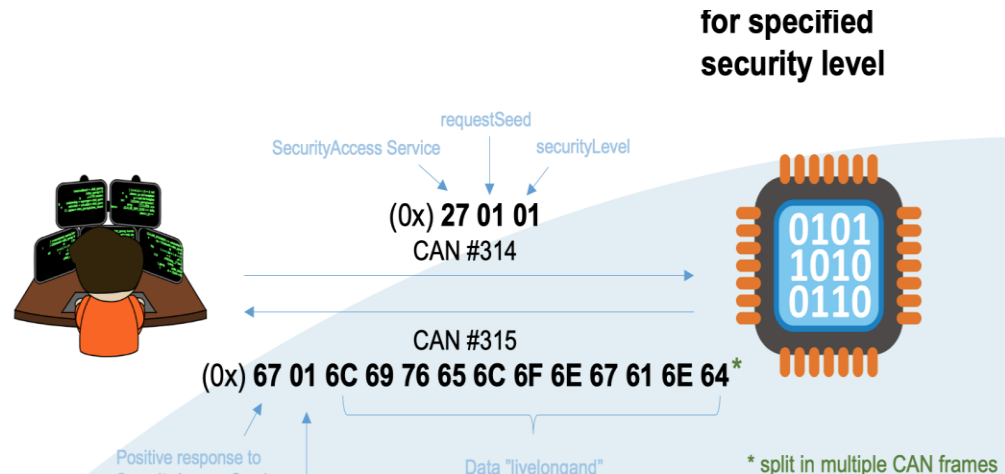
A CAN frame with a particular ID had to be sent to light up a LED. The LED conveyed a message in morse code carrying clues to the next exercise.

A non-automotive-professional with enough determination could, by using information available online, solve it.



# Challenge 2

Objective: to establish automotive diagnostic knowledge

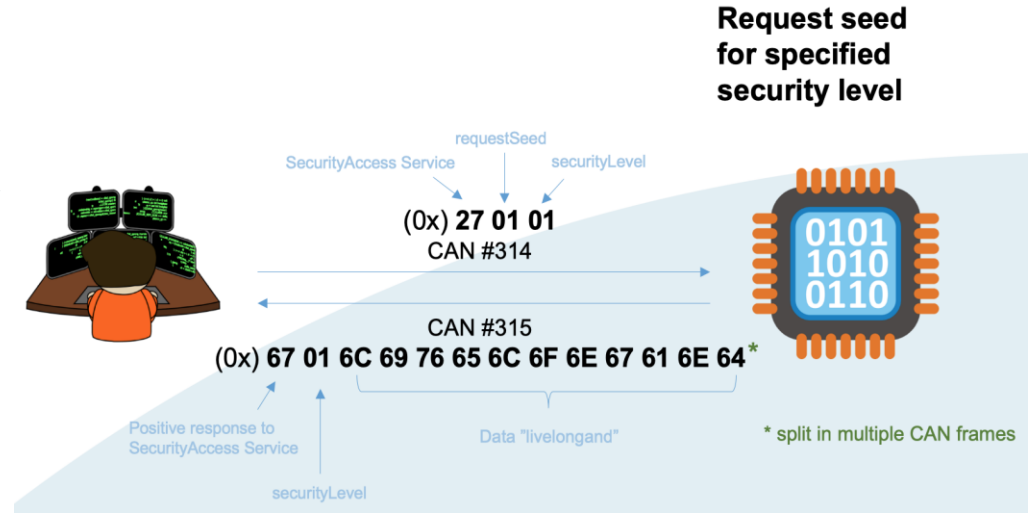


# Challenge 3

## Objectives:

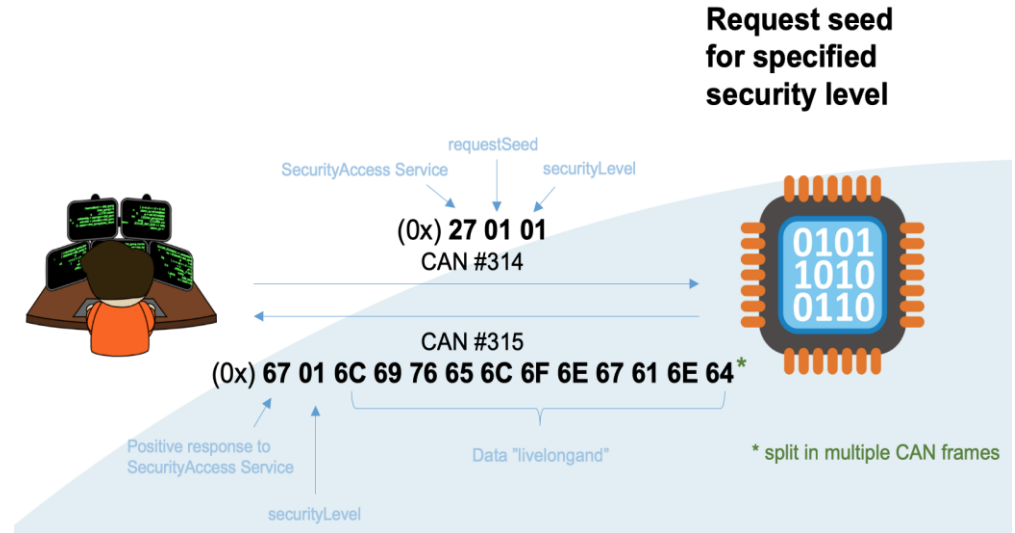
1. To further establish automotive diagnostics knowledge.
2. To establish cryptography proficiency.

## Step 1

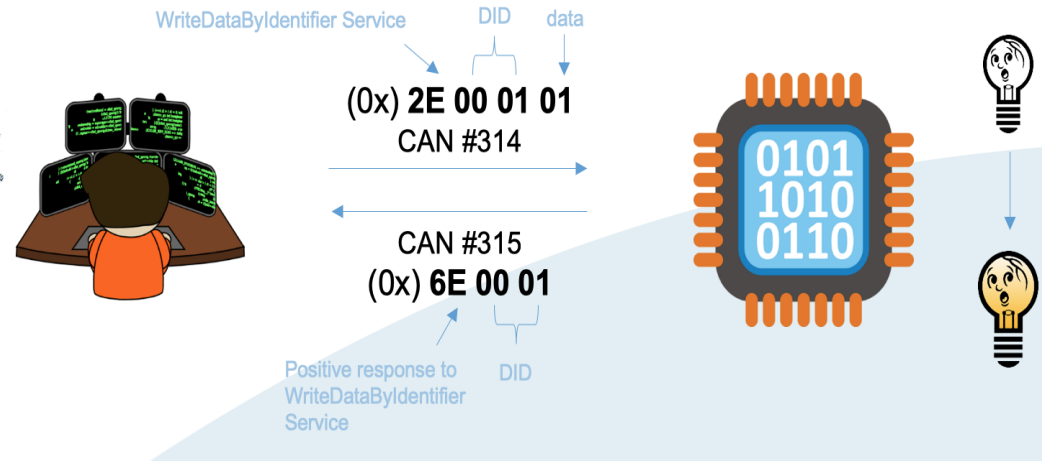


# Challenge 3

## Step 2



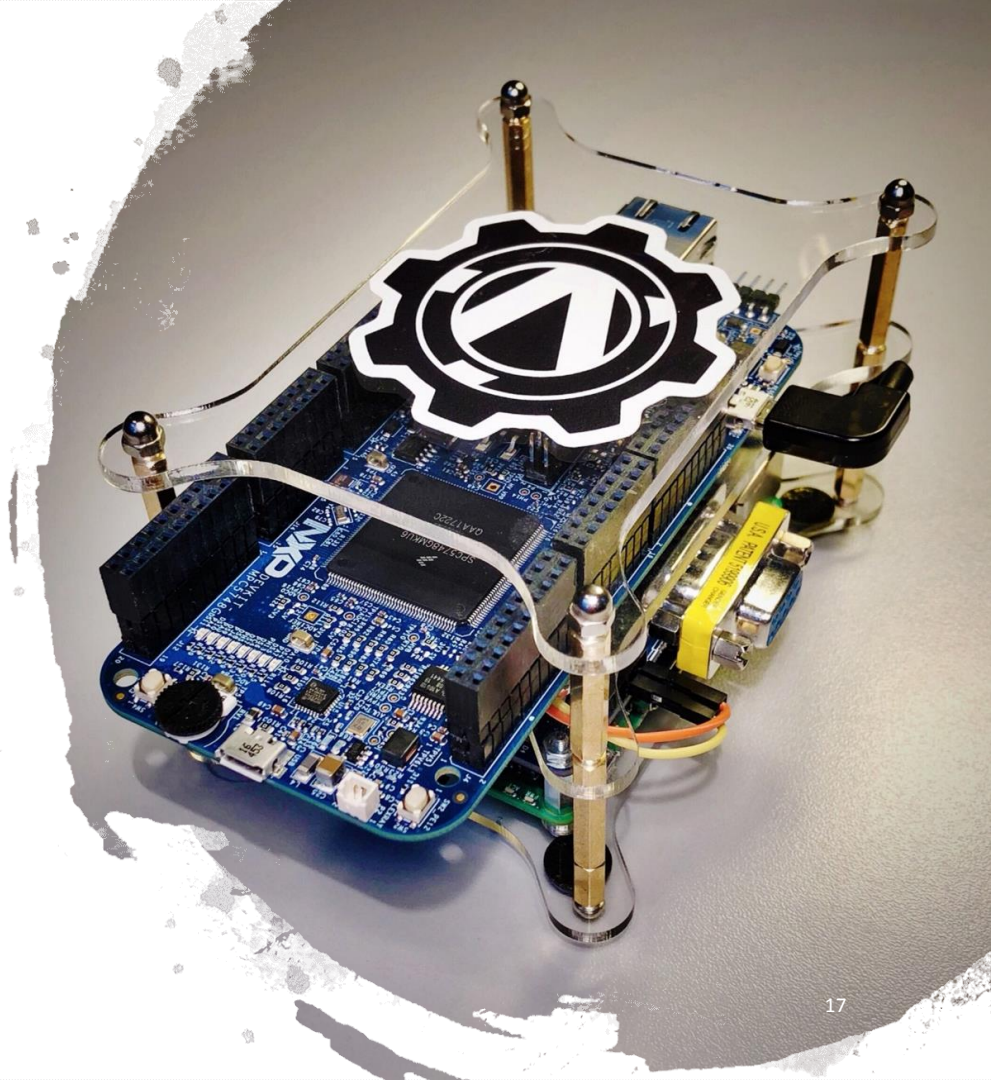
# Challenge 3 step 3





# Future

- Security education for automotive developers
  - Vinnova funded project
  - Real world security challenges
  - Theoretical session on automotive security
  - Practical session hands-on capture-the-flag style
  - Target audience: automotive developers interested in security
- The BusGoat
  - Refined existing challenges to better match real world problems
  - Extended the number of challenges
  - Extended the hardware to two ECUs





# HoliSec

*Holistic Approach to Improve Data Security*

## State of research

Ana Magazinius

April 26 2019, 15.30-15.45



ARC CORE

CHALMERS





Bug hunter

*Thousands of papers  
condensed into 72*



Product owner

## Dimensions




# Product Owner

---

- Guidelines
- Experience reports
- Economic aspects
- Vulnerability life-cycle





A woman's face is shown in profile, looking towards the right. Her face is partially obscured by a large, semi-transparent dark circle. Overlaid on her face and the background are numerous binary digits (0s and 1s) in a glowing blue and green color. The background is dark with a grid of binary digits.

# Bug Hunters

- Growing interest among white hats
- Top hunters are highly skilled, the crowd is very diverse
- Incentives:
  - Money
  - Fun/challenge
  - Curiosity and will to learn
  - Making products safer

# Market

---

- Theoretical models
- Empirical investigations
- Descriptions of the market





- All three categories include ethics
  - Be kind to each other
  - Do not weaponize
  - Do not sell to those who will hurt others

Bug Bounties – the Past and the Road Ahead  
Ana Magazinius  
April 26, 15.15-15.30



# HoliSec

*Holistic Approach to Improve Data Security*

## The Road Ahead

Ana Magazinius

April 26 2019, 15.00-15.45



ARC CORE

CHALMERS





# The Road Ahead

- The entire organisation has to be onboard.
- Timing is of essence!
- Help of external resources or internal work force?
- Closed or open event?
- Research?

Bug Bounties – the Past and the Road Ahead  
Ana Magazinius  
April 26 2019, 15.00-15.45



# HoliSec

*Holistic Approach to Improve Data Security*

**Thank you for your attention!**  
**Questions?**