



HoliSec

Holistic Approach to Improve Data Security

Volvo Busses Bug Bounty

Dr Ana Magazinius, Senior Researcher at RISE Viktoria

September 7, 2017. Time 13:20 – 13:40

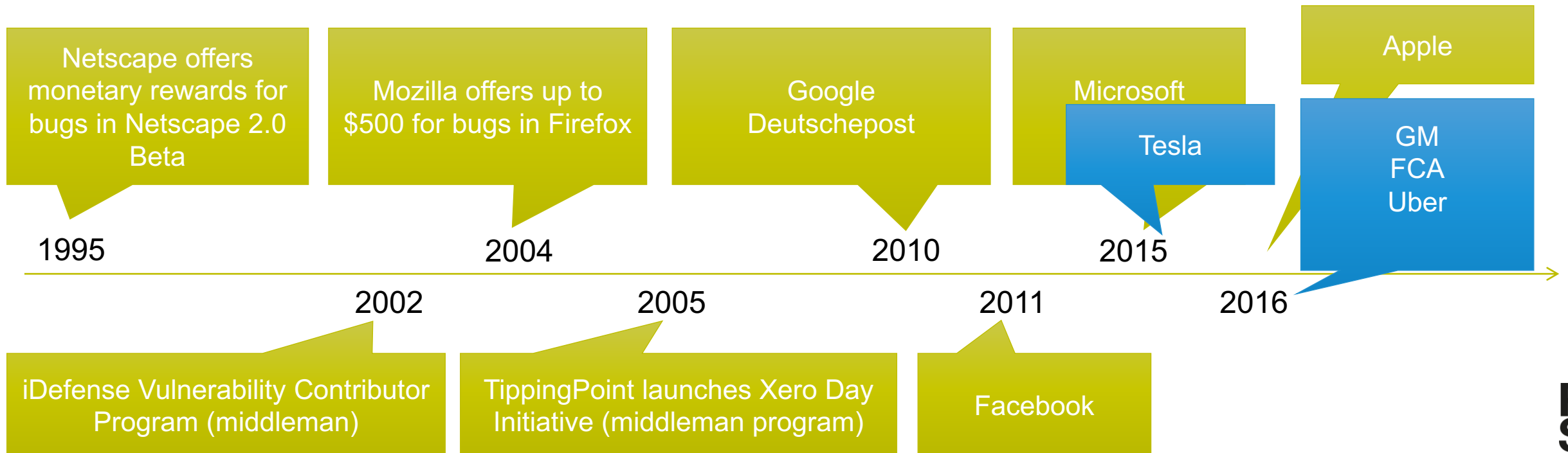


Content

- Bug bounties
 - History
 - Statistics
 - Automotive domain
- Volvo Busses bug bounty
- What do we want to learn?

Bug bounties

- What is a bug bounty?
 - **Wikipedia:** A bug bounty program is a deal offered by many websites and software developers by which **individuals can receive recognition and compensation for reporting bugs**, especially those pertaining to **exploits and vulnerabilities**. These programs allow the developers to discover and resolve bugs before the general public is aware of them, **preventing incidents of widespread abuse**.



Statistics of bug bounties, Bugcrowd

■ Economics

- 72 companies (FCA, Tesla, MasterCard, etc.)
- Total payouts of \$6,392,992, up 211% since 2016
- The average payout is now \$451 (vs. \$295 in 2016)
- The average payout on Critical (P1) vulnerabilities is \$1,776
- The industry with the top average payouts is automotive at \$1,514 and the lowest is Retail/ E-commerce at \$403

■ The crowd

- The community has nearly doubled in 53,332, (26,782 in 2016)
- Leading countries (in number of researchers/hackers):
 - USA
 - India
 - UK

AVERAGE PRIORITY BY INDUSTRY



Bug bounties at vehicle (car) companies

- Scope

- Included:

- A HW product that you own or are authorized to test against
 - Company webpage...

- Excluded:

- Third party websites(e.g. shop.teslamotors.com) or other products by the same brand

- Bounties:

- **Tesla:** \$100 - \$10 000 per bug (bugcrowd.com: 232 rewarded, average payout \$1 143 → total \$265 176)
 - **FCA:** \$150 - \$1 500 per bug (bugcrowd.com: 54 rewarded, average payout \$267 → total \$14 418)
 - **GM:** only fame
 - **Uber:** minimum \$500 per bug (hackerone.com: on average \$500-\$700, total \$1 184 445)
 - *Audi (closed event): “cash”*

Why are we doing this?
What are we afraid of?



2. HACKERS COULD TAKE CONTROL OF YOUR CAR WHILE YOU'RE DRIVING.



Who else?



Top 10
motivational
quotes
for hackers

*“I was addicted to hacking, **more for the intellectual challenge, the curiosity, the seduction of adventure**; not for stealing or causing damage or writing computer viruses”*

Kevin Mitnick

*“I got so passionate about technology. Hacking to me was **like a video game**. It was about getting trophies. I just kept on going on and on, despite all the trouble I was getting in to, because I was hooked.”*

Kevin Mitnick

...

*“If you give a hacker a **new toy**, the first thing he’ll do is take it apart to figure out how it works”*

Jamie Zawinski

*“Hacking involves a **different way of looking at problems** that no one’s thought of.”*

Walter O’Brien

*It is a fairly open secret that almost all systems can be hacked, somehow. It is a less spoken of secret that such hacking **has actually gone quite mainstream**.*

Dan Kaminsky 

Why are we doing this?
What are we afraid of?



2. HACKERS COULD TAKE CONTROL OF YOUR CAR WHILE YOU'RE DRIVING.



What makes us special?



nya elbussen är tyst och släpper inte ut några avgaser.
För kan vi lägga hållplatser inomhus, till exempel i bibliotek.
Electric bus is quiet and has zero emissions. Now we can put stops indoors. Even in libraries.

stannar den 113

What makes us special?!

You don't have to buy a bus!



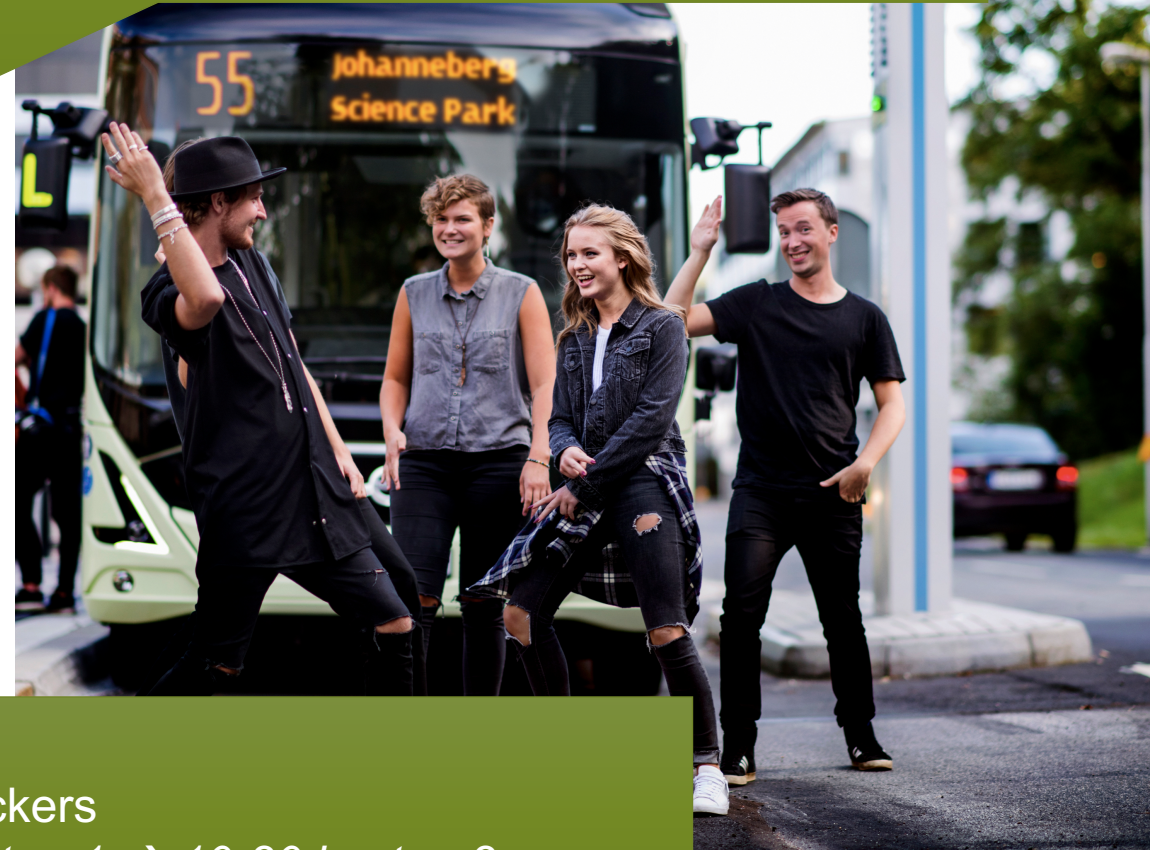
Step 1:
BusGoat

Step 2:
the Bus



Step 2:

- Beginning of summer 2018
- 10-20 hackers in place in Gothenburg
- Scope: one ElectriCity bus and one charging station



Why step 1:

- To aid selection of the bus hackers
All applicants → max 100 in step 1 → 10-20 in step 2
- Educational effort

What do we want to learn?

- What kind of vulnerabilities will the hackers find?
- Will those vulnerabilities differ from those found during common security testing (in-house and pen-testing by consultants)?
- How do the hackers approach a product like this?
 - When they succeed?
 - When they don't succeed?
- Is this type of event a good addition to the existing security engineering work at a company like Volvo Busses?
 - Additional events of this type?
 - Building relationships with the hacker community?



HoliSec

Holistic Approach to Improve Data Security

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



THANK YOU!

Dr Ana Magazinius

ana.magazinius@ri.se

Research Institutes of Sweden

RISE VIKTORIA

