FUZZCON EUROPE

FUZZ YOUR SOFTWARE

SEPTEMBER 8, 2020

code intelligence

FuzzCon Europe 2020

2018

Started as a meetup

~ 20 people

2019

FuzzCon Europe 2019 -
What's all the Fuzz About?

~ 60 people

2020

ONLINE

FuzzCon Europe 2020 -
Fuzz Your Software

~ 600 people

Code Intelligence Hosting FuzzCon Europe 2020

Sergej Dechand
CEO & Co-Founder

Usable Security Background

Fraunhofer FKIE

UNIVERSITÄT BONN

Code Intelligence

Vision: Easier access to modern software testing techniques for everyone

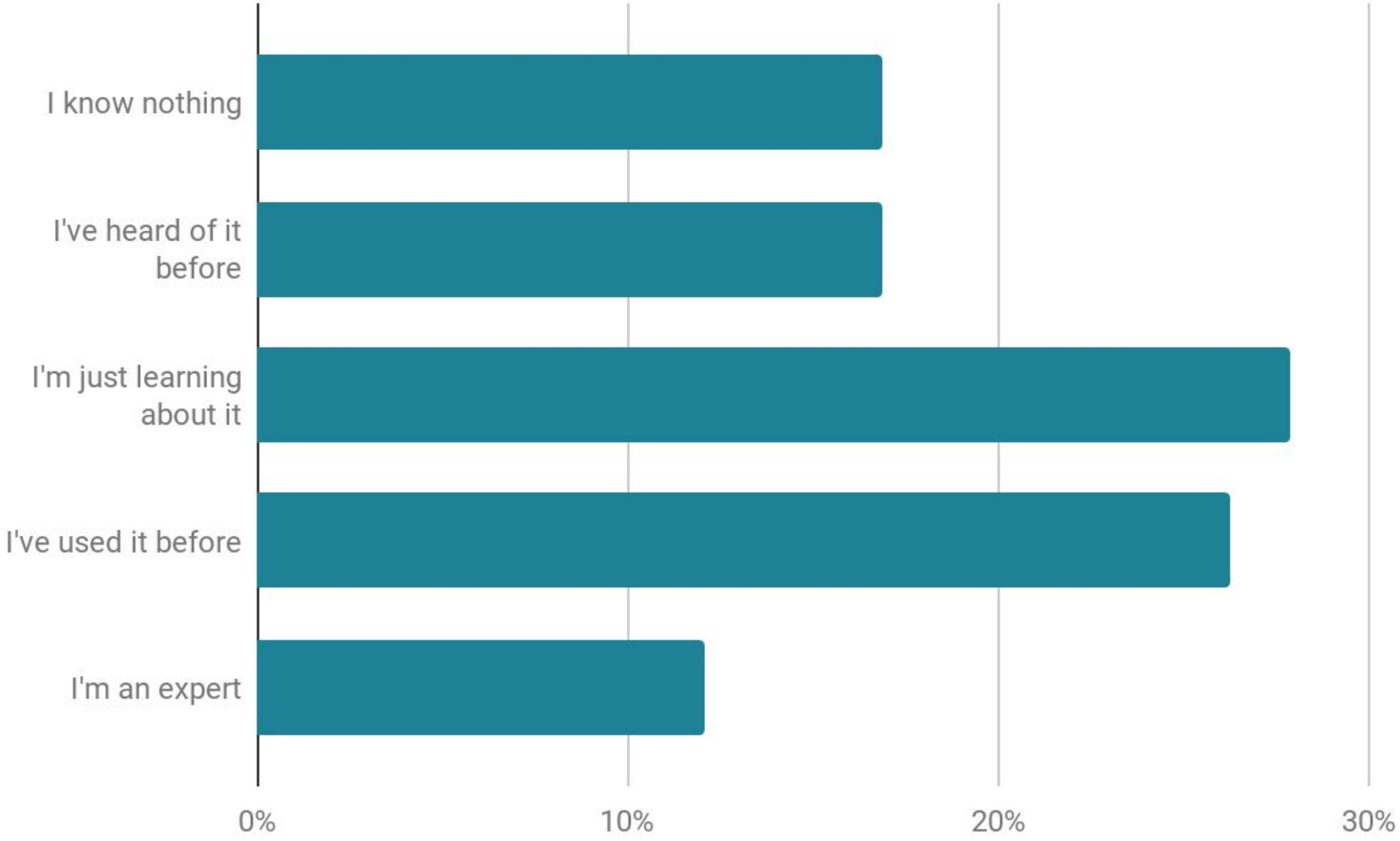
www.code-intelligence.com

Code Intelligence Team

What is Fuzzing?

1. Oh yes, I heard about fuzzy logic in university
2. Just testing with random inputs
3. I want to use fuzzing ASAP

Participants of FuzzCon Europe



Evolution of Software Testing

Manual testing

Techniques:
Code reviews, manual checks & exploitations

Advantage:
Finds deep bugs

Disadvantage:
Time-consuming, needs experts to conduct

Static analysis

Techniques:
Pattern search: CFG, DDG

Advantage:
Works without running

Disadvantage:
Finds too much or nothing at all

Modern Fuzzing

Techniques:
Coverage-guided fuzzing

Advantages:
Finds lots of bugs!
(Almost) no false positives

Icons by Noun Project

Fuzz Testing in Security Research

Automated Software Testing is an almost solved problem: Fuzzing + Symbolic Code Execution

Ain’t nobody got time for that

Tech Leaders find

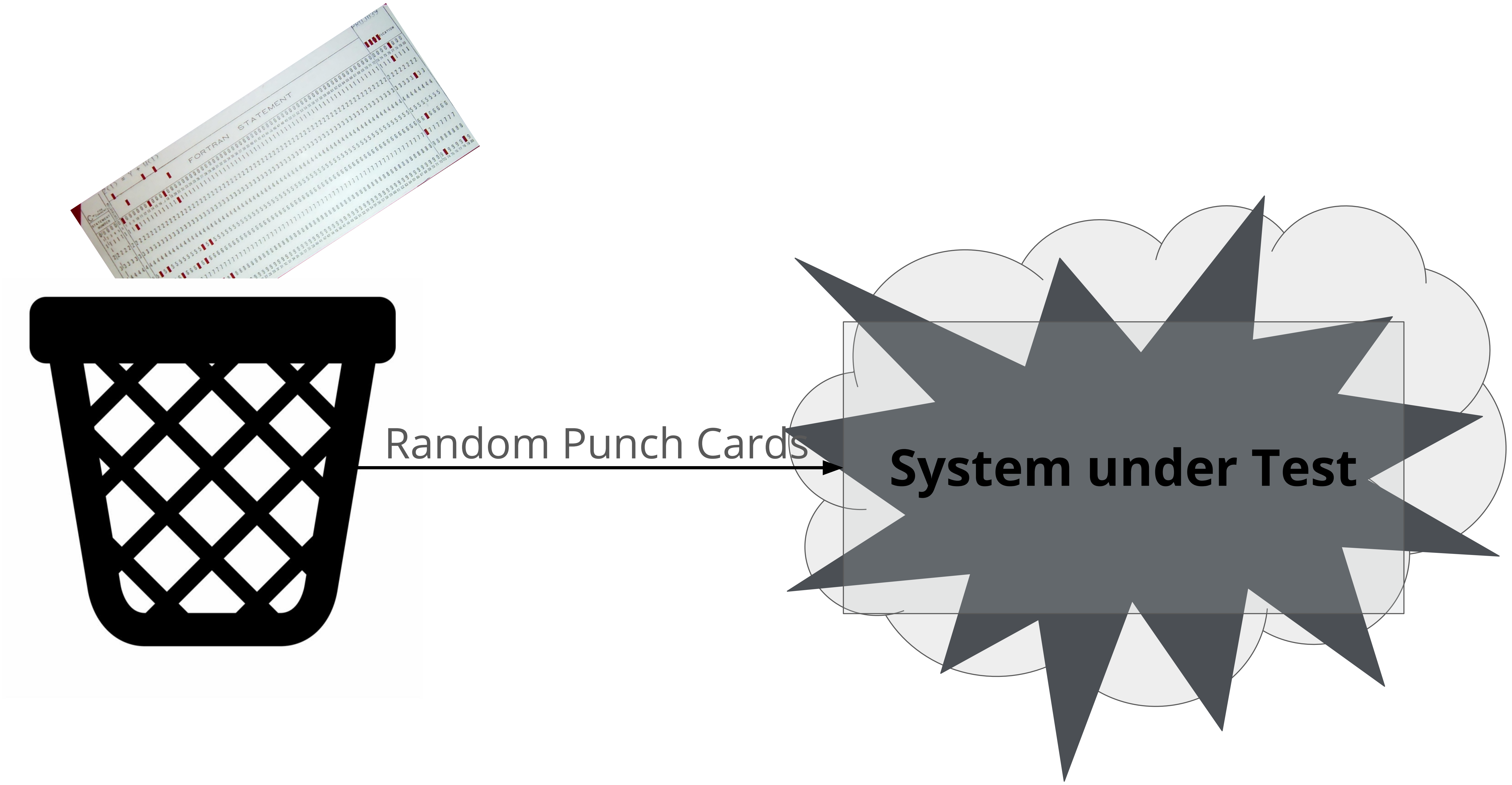
80 %

of their bugs with **FUZZING**

Fuzzing in Large Scale

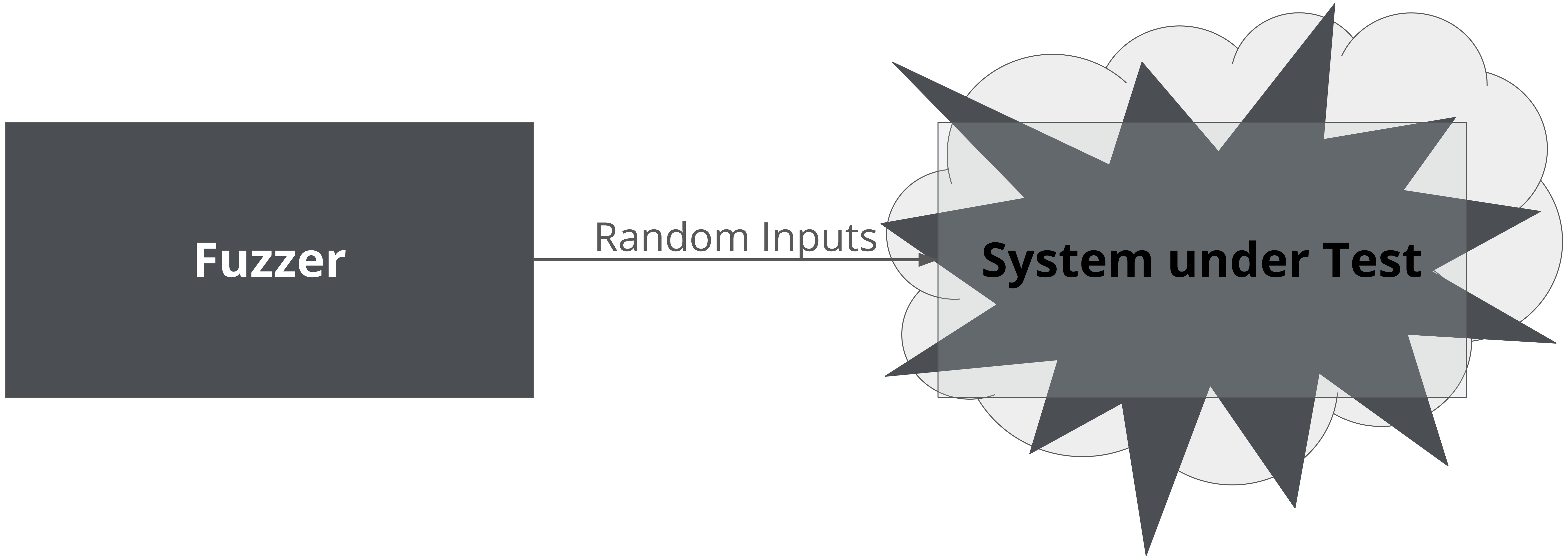
1 800	MICROSOFT OFFICE
11 687	LINUX
19 789	GOOGLE CHROME
16 108	OSS-FUZZ
5 200	MOZILLA FIREFOX

Early Random Testing



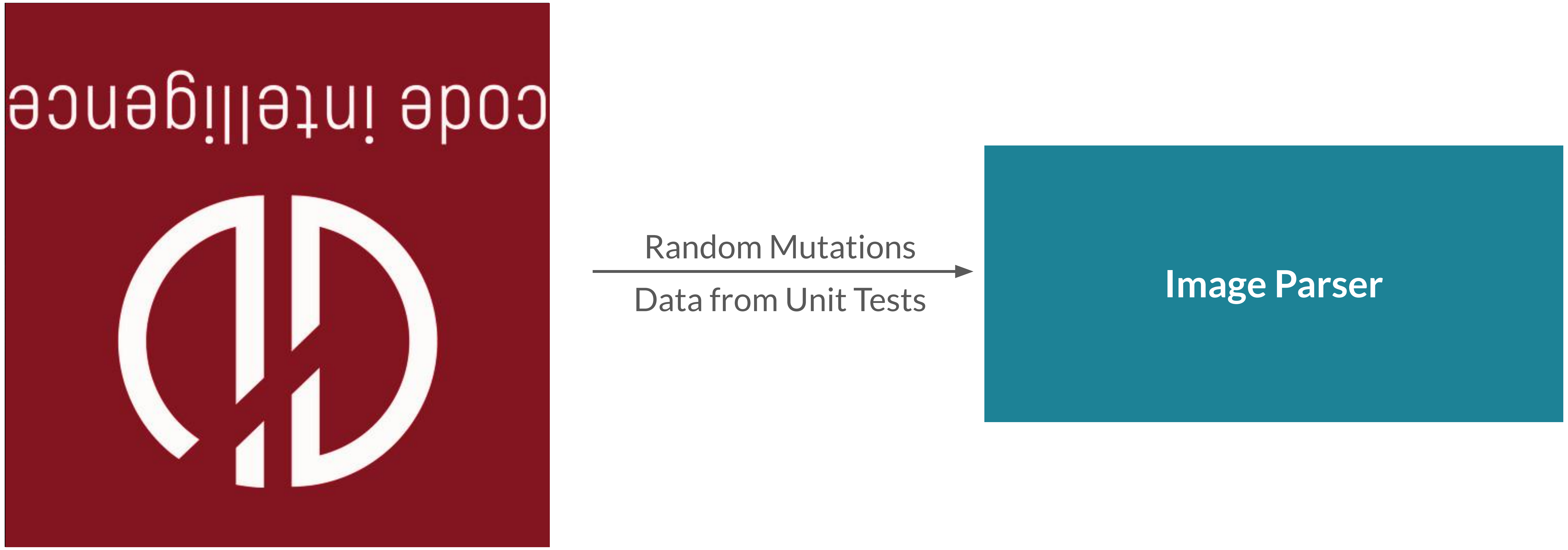
1960s

Fuzz it like it’s 89



1989

Unit Testing and Dumb Fuzzing

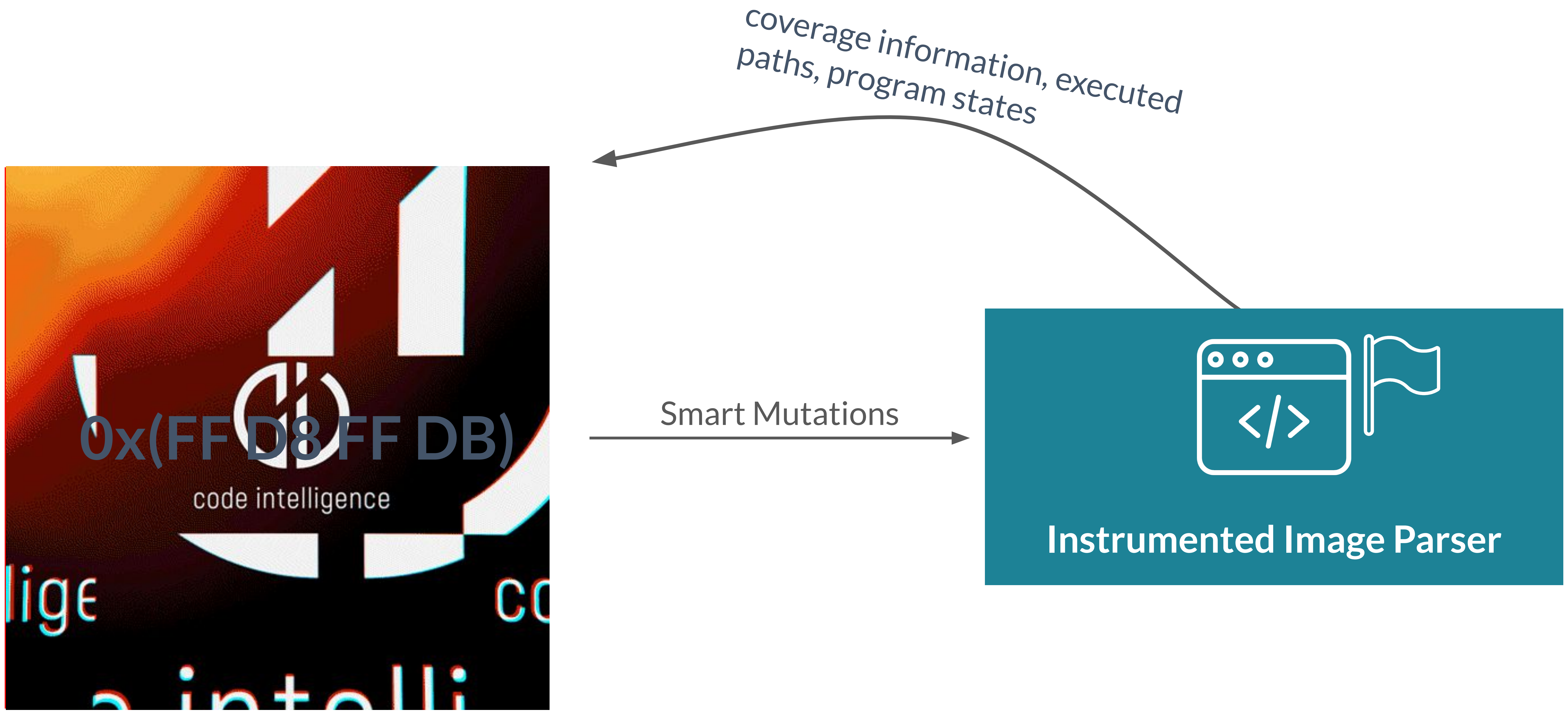


Random Mutations

Data from Unit Tests

Image Parser

Modern Fuzzing Using Instrumentation for a Feedback Loop



coverage information, executed paths, program states

Smart Mutations

Instrumented Image Parser

FUZZCON EUROPE

FUZZ YOUR SOFTWARE

SEPTEMBER 8, 2020

code intelligence

Human Aspects

Developer Acceptance

- Developer acceptance when setting up the first time
- Not all bugs are equal
- NIH

Learning Curve

- How to deal with new technology
- Understand new concepts

Source Graphic Freepik

FUZZCON EUROPE
SEPTEMBER 8, 2020

Matthew Smith

Professor
University of Bonn, Fraunhofer FKIE

10:30 - 11:00
Usability Issues of Modern Fuzzers

Christian Holler

Staff Security Engineer
Mozilla

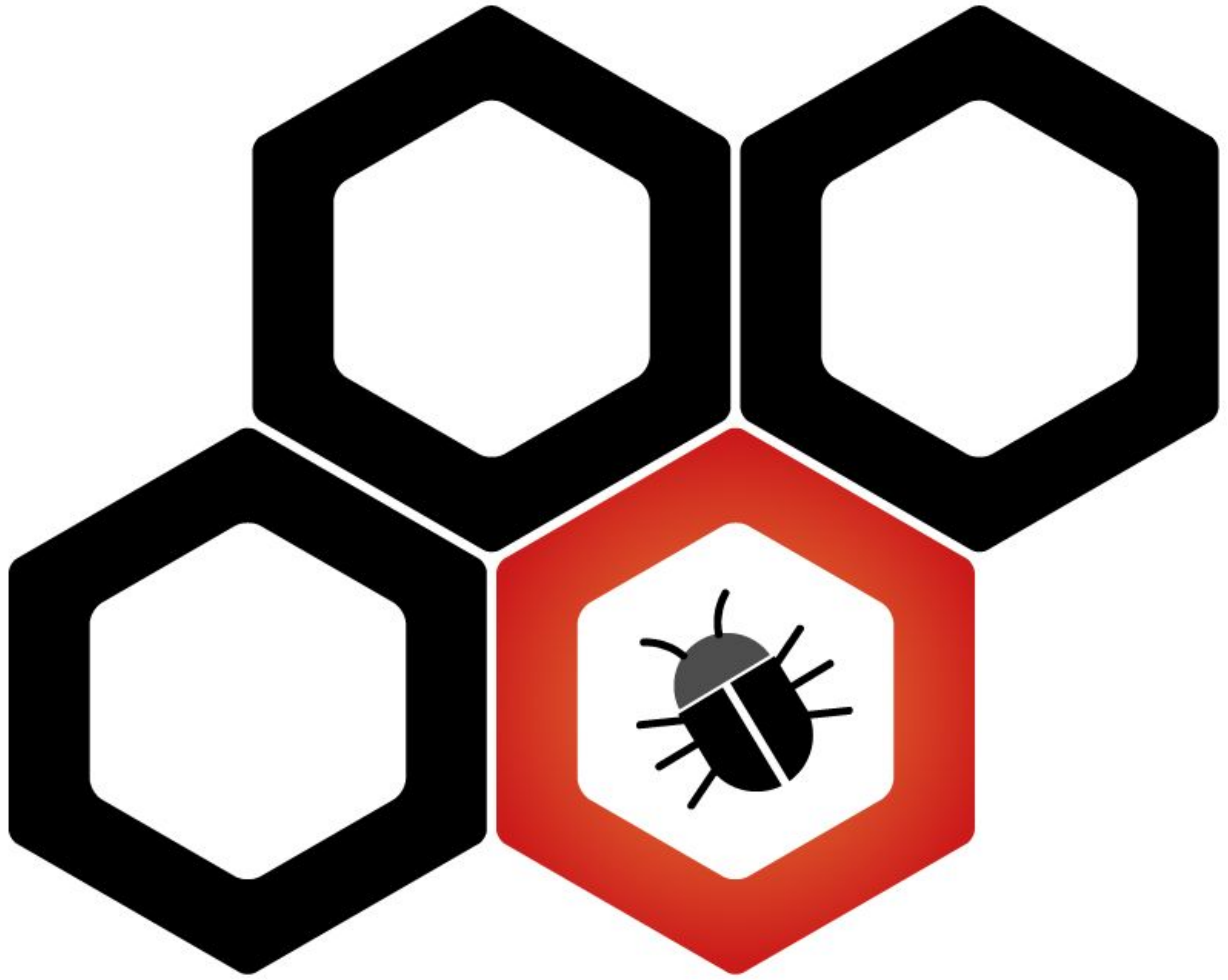
11:30 - 12:00
The Human Component in Automated Bug Finding

Caroline Lemieux

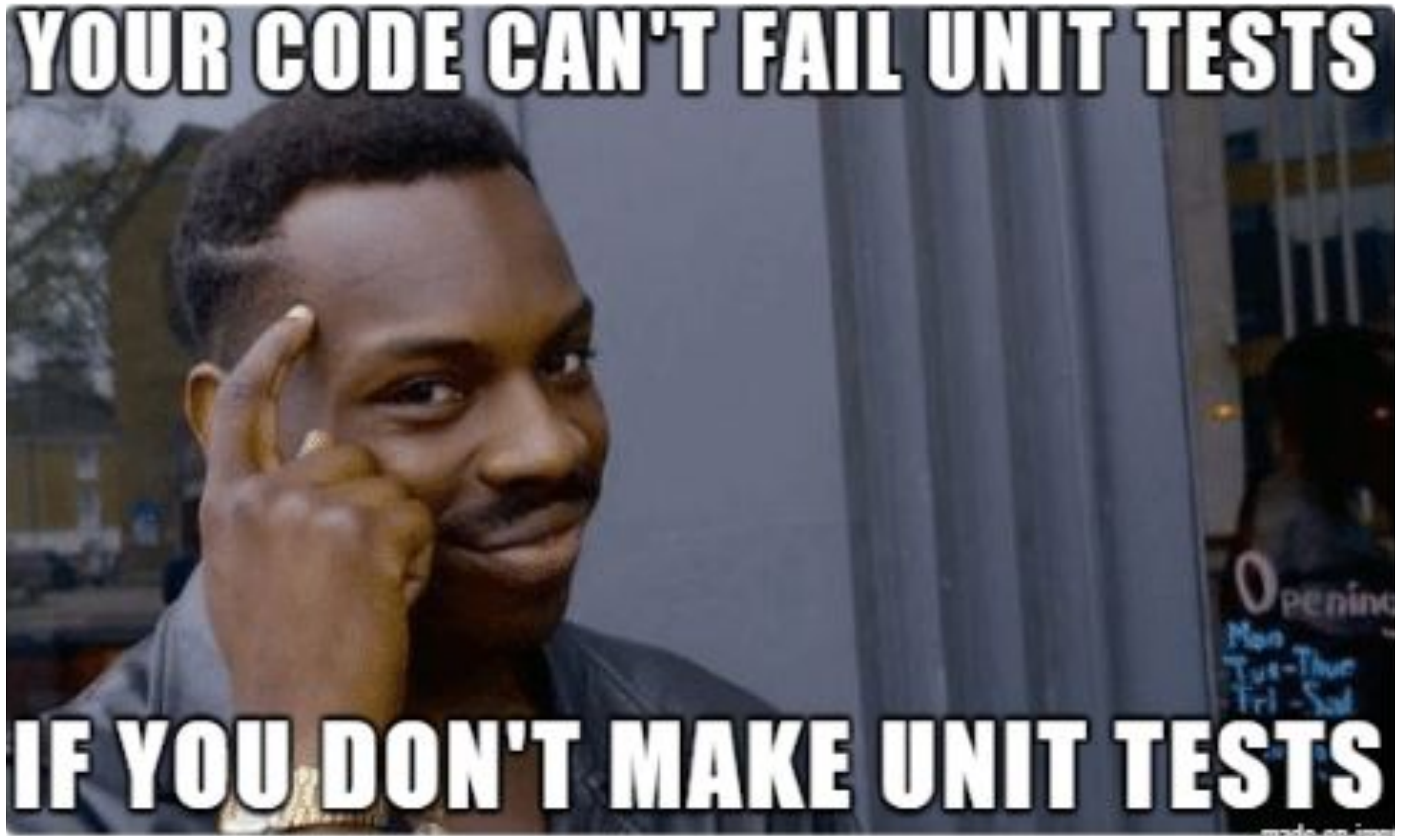
Security Researcher
University of California, Berkeley

18:00 - 18:30
Expanding the Reach of Fuzz Testing

Development Processes / Corporate Aspects



- Scalable fuzzing infrastructure finding security and stability issues in software
- Google uses ClusterFuzz to fuzz the Chrome Browser / OSS-Fuzz



Unit Tests? We can't do that here!

FUZZCON EUROPE
SEPTEMBER 8, 2020

Götz Martinek
Managing Director
sodge IT

Tobias Esser
Head of Security Testing
imbus

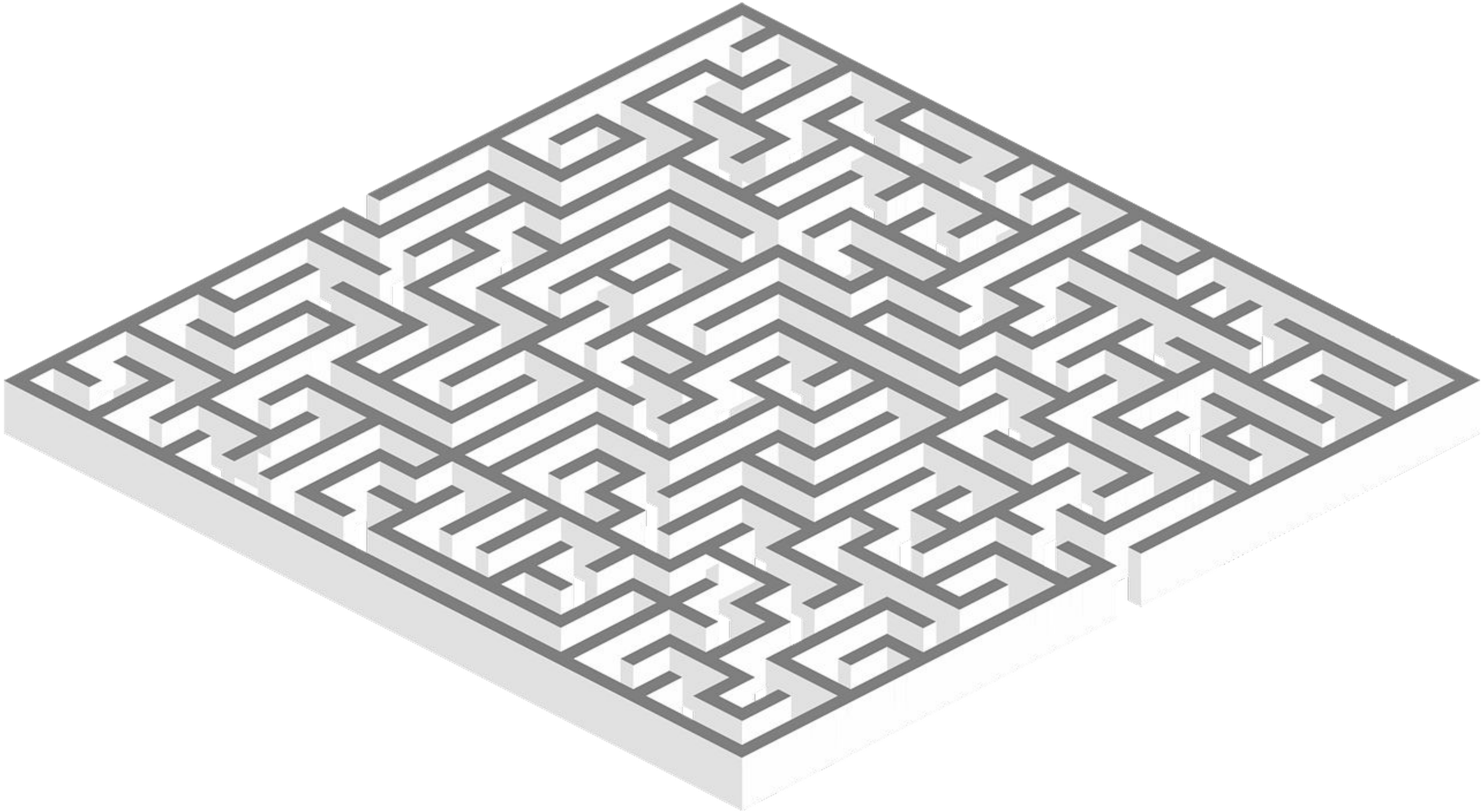
Alexander Weise
Vice President
Code Intelligence

Rakshith Amarnath
Project Lead R&D
Bosch Corporate Research

12:00 - 12:30
Fireside Chat: Fuzzing for Industry Use Cases

14:45 - 15:15
What's different about fuzzing Automotive Software?

Structure Awareness



FUZZCON EUROPE

SEPTEMBER 8, 2020

Sirko Höer

Vulnerability Expert

German Federal Office for Information Security (BSI)

14:15 - 14:45

Fuzzing Suricata: Finding Vulnerabilities in Large Projects

Cornelius Aschermann

Security Researcher

Facebook

Sergej Schumilo

Security Researcher

Ruhr-University Bochum

15:15 - 15:45

Stateful Fuzzing with Snapshots

Bhargava Shastry

Security Engineer

Ethereum Foundation

16:30 - 17:00

Fuzzing the Solidity compiler

Further Issues to do “Deep Fuzzing”

Source Graphic Freepik

FUZZCON EUROPE

SEPTEMBER 8, 2020

Marcel Böhme

Senior Lecturer

Monash University

11:00 - 11:30

Fuzzing: Challenges and Reflections

Andreas Zeller

Professor

CISPA Helmholtz Center for Information Security

13:30 - 14:15

Taming Fuzzers

Sebastian Pöplau

Security Researcher

Systems Security Group Eurecom (France)

15:45 - 16:15

Symbolic Execution - what's that, and how to make it efficient?

Kostya Serebryany

Principal Software Engineer

Google

17:30 - 18:00

Top N challenges of "deep" fuzzing

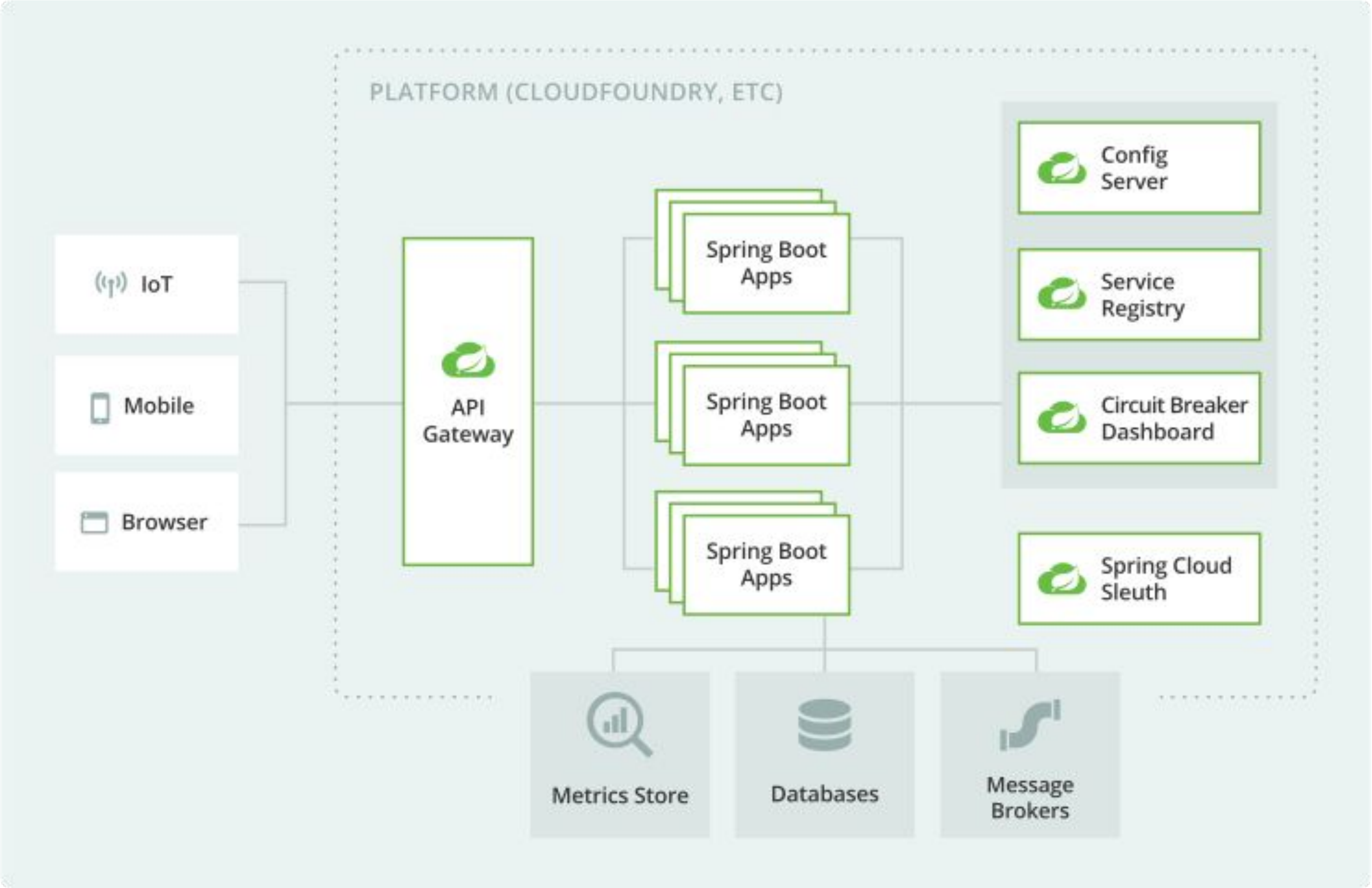
Web Applications

Most-Common Use Cases: Web Services

- REST + URL-Encoded
- Protobuf

OWASP Top 10

- Black-box approaches (OWASP Zap, etc)
- Guided fuzzing just starting for Java etc.



OWASP
Open Web Application Security Project

FUZZCON EUROPE

Khaled Yakdan

Chief Scientist
Code Intelligence

17:00 - 17:30
CI Fuzz - Continuous Fuzzing of Network Services

Open Q&A Session

18:30 - 19:00
Ask the Experts
Open Q&A

Fuzzing in the Industry

“With Code Intelligence, securing your software can take new paths in terms of quality and efficiency.”

Thomas Tschersich // Chief Security Officer // Deutsche Telekom AG

“Code Intelligence enables us to easily integrate alternative automated approaches to ensure quality.”

Helge Harren // SVP Application Development Trading // Deutsche Börse AG

DEUTSCHE BÖRSE GROUP

“Such software security testing approaches have uncovered vulnerabilities in open source projects.”

Rakshith Amarnath // Project Lead // Bosch Corporate Research

BOSCH
Technik fürs Leben

DCSO ENGINEERING SECURITY

sopra steria

axxessio we make projects happen. all the way.

escrypt Embedded Security by ETAS

Intevation GmbH

sodge IT

and more

"With the Open Bosch Award, we honor the best startup collaboration worldwide."

- Dr. Michael Bolle, CTO Bosch

Conclusion

1. Fuzzing superior
2. Get's traction in practice
3. Today: Talks from fuzzing experts tackling challenges

DEUTSCHE BÖRSE GROUP
T · ·
BOSCH Technik fürs Leben
DCSO ENGINEERING SECURITY
axxessio we make projects happen. all the way.
escrypt Embedded Security by ETAS
sopra steria
Intevation GmbH