Central Office
for Information Technology
in the Security Sector

ZITiS

Analysis of suspicious applications from evidence-relevant Android devices under real reconstructed conditions

Christopher Lenk

ZITiS, Department for Digital Forensics, Research group

CODE Conference 2020, Science Track / PhD Forum, 12.11.2020

Agenda

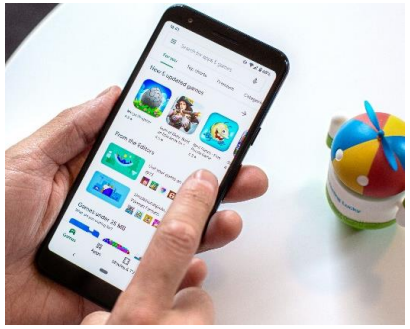
- Introduction
- Current work – Z-A³L
- Forensic malware analysis
  - Requirements
  - Goals and approaches
  - Planned methodology
- Summary
- Q&A

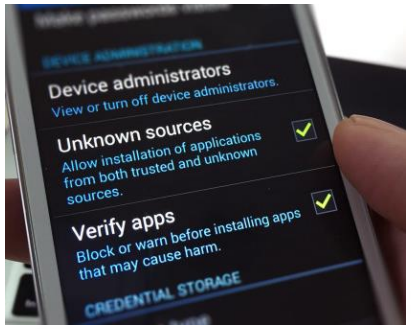
Central Office for Information Technology in the Security Sector

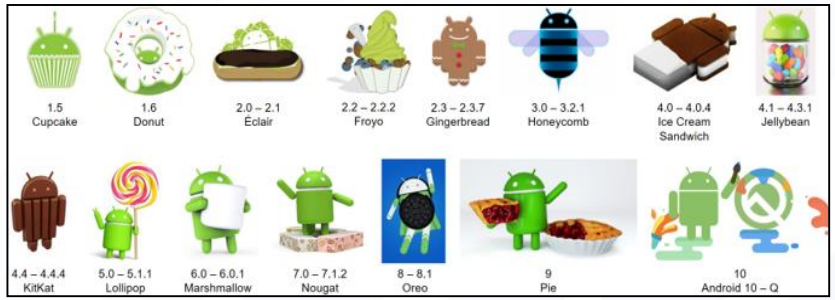
This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800

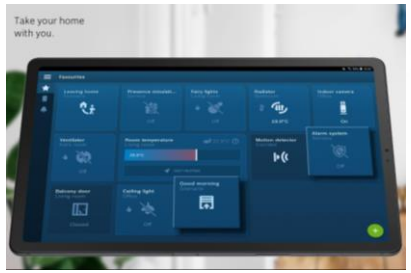
Introduction

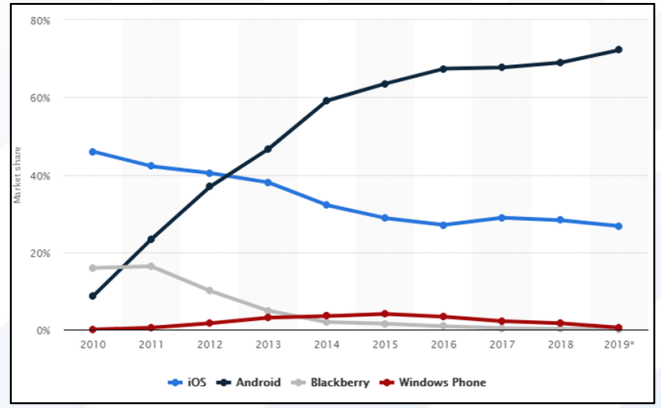
Android as a target of attack – challenges and problems









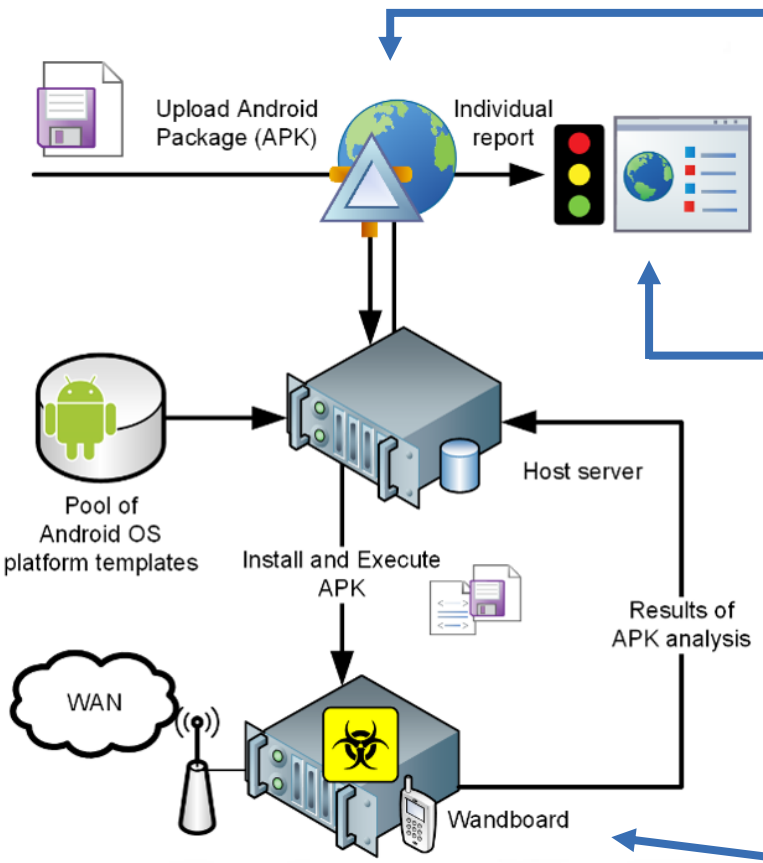


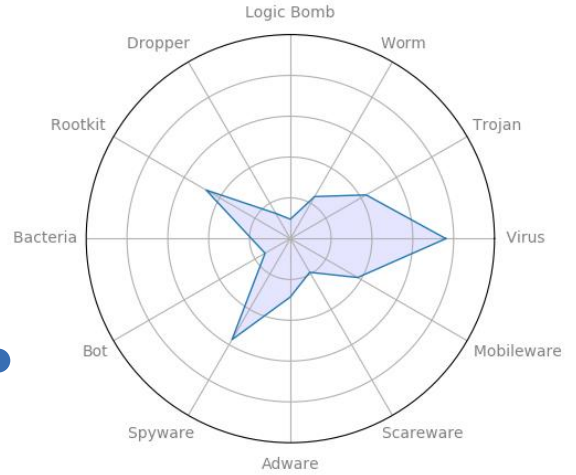
Central Office for Information Technology in the Security Sector

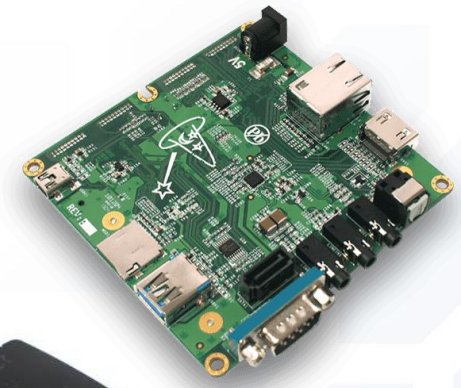
This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800

Current work

Z-A³L – The Automated Android Analysis Lab of ZITiS







Central Office for Information Technology in the Security Sector

This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800

Forensic malware analysis

Requirements of the forensic process

- The following principles apply when securing and evaluating evidence devices and data:
  - Procedure only according to legal regulations
  - No adulteration or changes
  - No destruction of evidence
- The forensic work directly influences the course of the judicial process.
- Falsified evidence leads to false conclusions.

This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800

Forensic malware analysis

Forensics vs. malware analysis

Forensics

- Requirement for forensic reconstruction – equal conditions:
  - Analysis system == original system on the evidence device
- Investigation not on the original device (risk of alteration!)
- No adulteration or destruction of evidence
- No statements about program sequences and behaviour possible (forensic memory image)

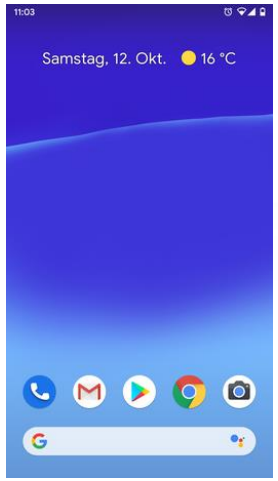
Malware analysis

- Randomly generated analysis systems or analysis methods for real devices
- Different conditions (events, services, apps)
  - Possibly alternative program sequence
- Detection of virtualized or emulated analysis environments using defense strategies
  - Termination of any behaviour
  - Execution of benign or different behaviour
- Execution and monitoring of the application

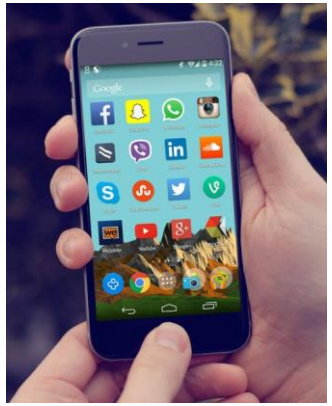
This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800

Forensic malware analysis

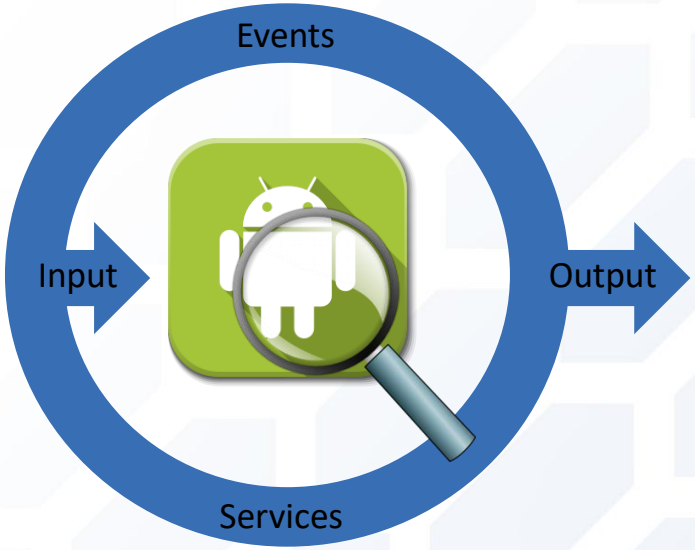
The way from application analysis to crime investigation



System



Program Flow



Analysis

Central Office
for Information Technology
in the Security Sector

This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800

Forensic malware analysis

Goals and approaches

- **RQ1:** Is it possible to set up the manufacturer-specific image of a smartphone on a general analysis platform and make it run without errors?
- **RQ2:** How does the adaptation of the Android system with regard to hardware, processes and other applications influence the program flow of the examination object? To what extent do analysis and results differ from randomly generated environments and analyses on real mobile devices?

System

- **RQ3:** What log data and similar artifacts can be obtained from the forensic image after the application has been executed on the original device?
- **RQ4:** How does the data from RQ3 affect stimulation of the program by adjusting the input? Are there any differences to unaffected program execution?

Program Flow

- **RQ5:** Is it possible to hide the analytical processes in a way that makes it difficult or impossible for the application to recognize the analysis and to activate defense mechanisms?
- **RQ6:** Can larger quantities of different malware samples and thus more functions or behaviours be analyzed and evaluated with the hidden processes than with existing approaches? How does camouflaging the analysis affect the results?

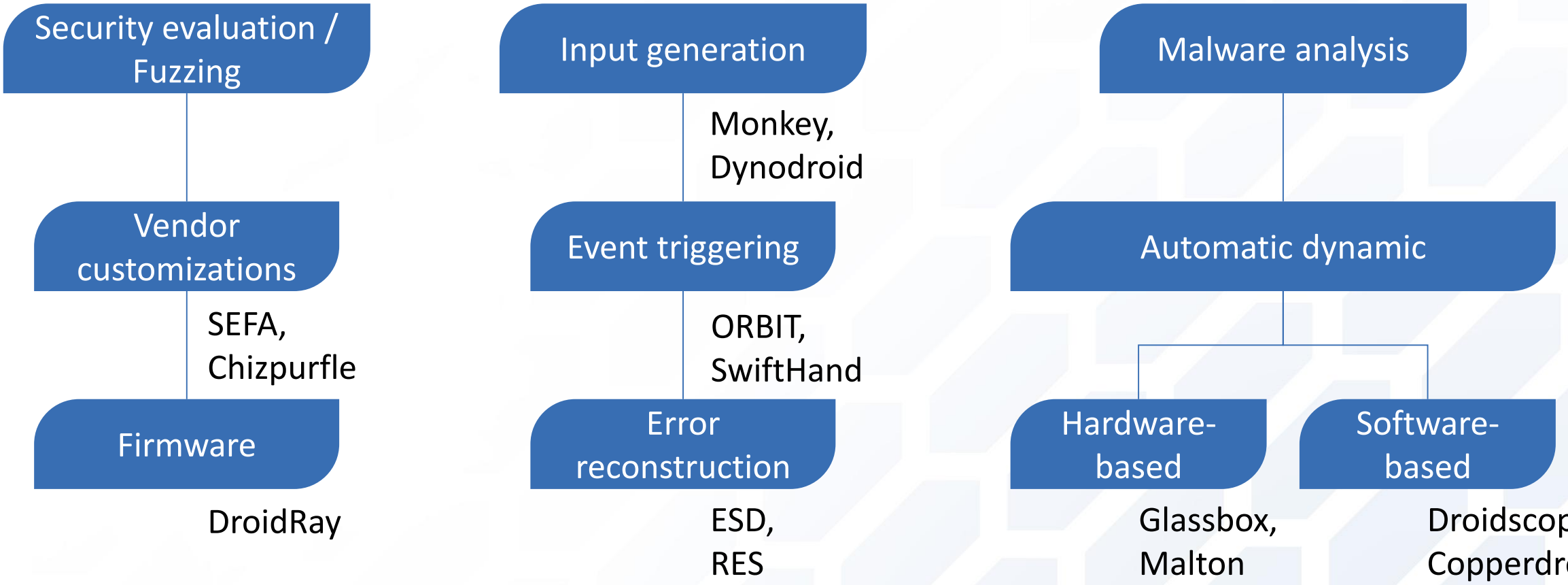
Analysis

Central Office for Information Technology in the Security Sector

This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800

Forensic malware analysis

Research approaches and tools – State of the art

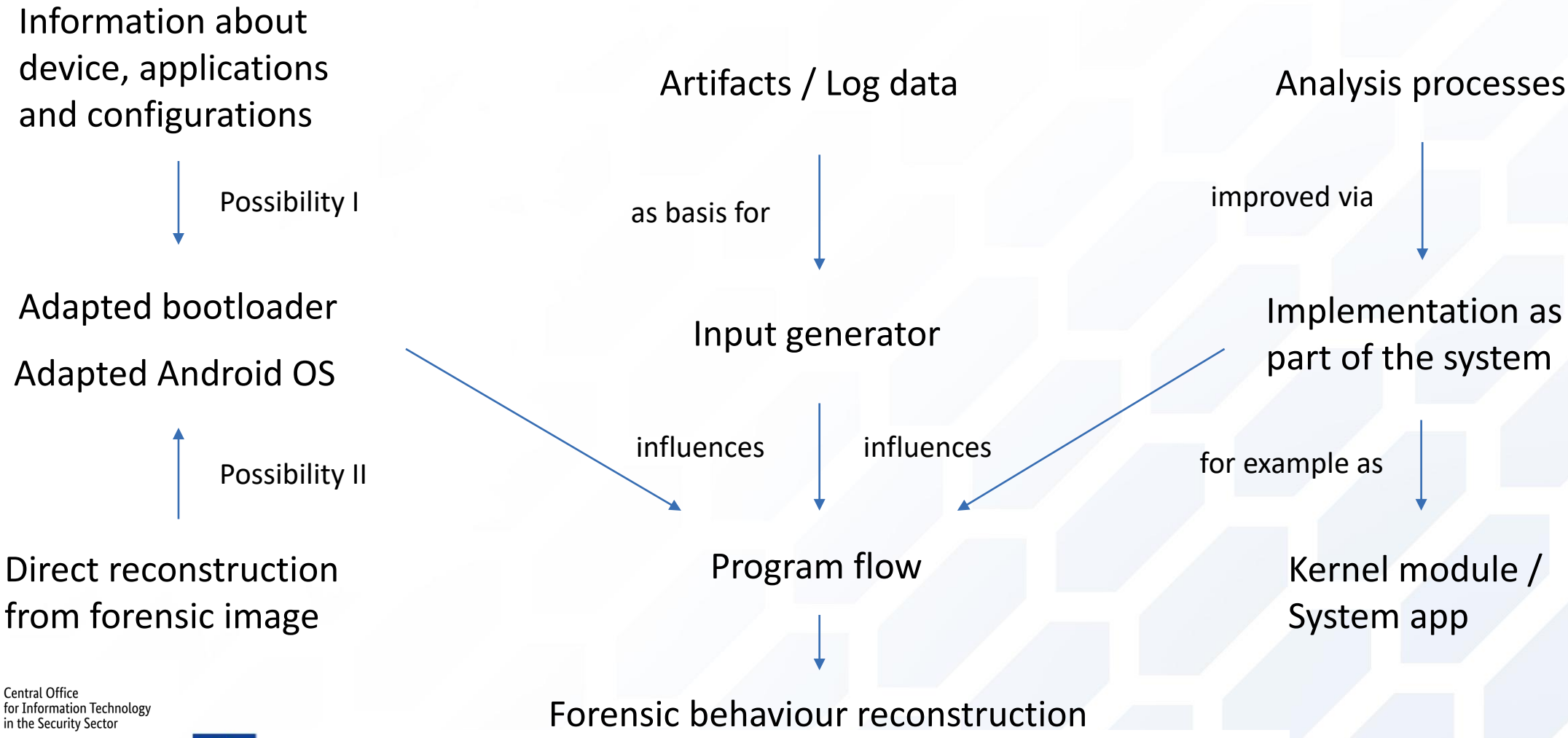


Central Office for Information Technology in the Security Sector

This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800

Forensic malware analysis

Planned methodology



Central Office for Information Technology in the Security Sector

This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800

Summary

- Realistic simulated examination of suspicious Android applications

- Customization of the Android system
- Stimulation of the program flow that led to a criminal offense
  - Generation of adapted inputs and events based on artifacts extracted from the original device
- Analysis techniques that prevent the activation of defense mechanisms and ensure an unadulterated and complete investigation

- Enriched information that can be used to detect and better understand criminal events related to malicious software
- Not possible with traditional forensic methods and current analysis techniques

This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800

Thank you for your attention!
Questions?

Christopher Lenk

EU project FORMOBILE – Task leader “Malware analysis”
PhD student UniBw Munich – RI CODE

Christopher.Lenk@zitis.bund.de
www.zitis.bund.de

ZITiS – Central Office for Information Technology in the Security Sector
Zamdorfer Str. 88
81677 Munich

Central Office for Information Technology in the Security Sector

This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, H2020-SU-SEC-2018, under grant agreement no. 832800