Virtualizing QR Code Fuzzing

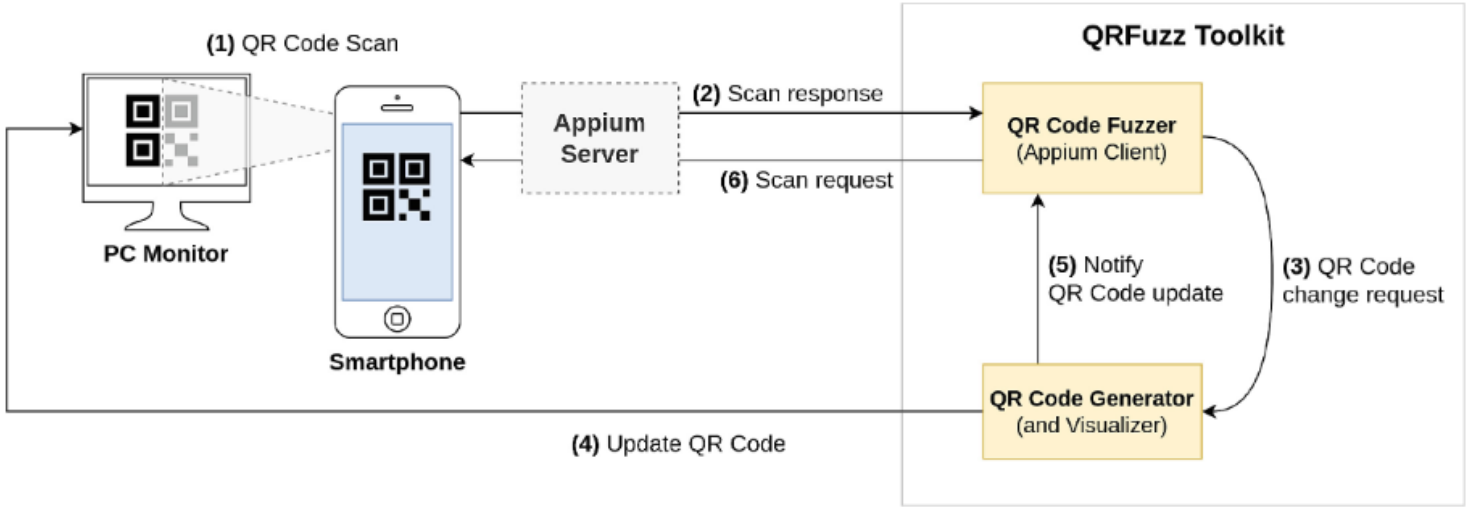
Advanced Topics in Computer Network and Security exam, 8th February 2024

Alberto Lazari - 2089120
Elia Scandaletti - 2087934
Francesco Protopapa - 2079466

QRFuzz

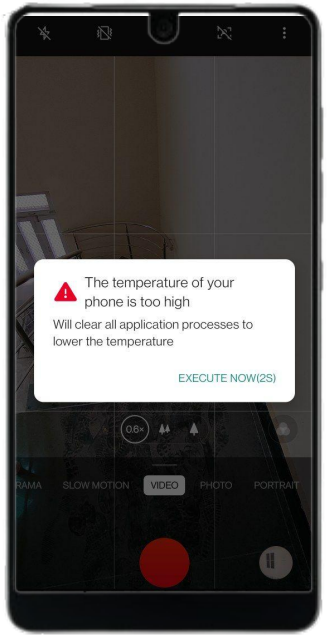
- Fuzz testing with QRs
- Around 20 mobile apps tested
- Discovered bugs on Instagram and Verifica C19

QRFuzz architecture

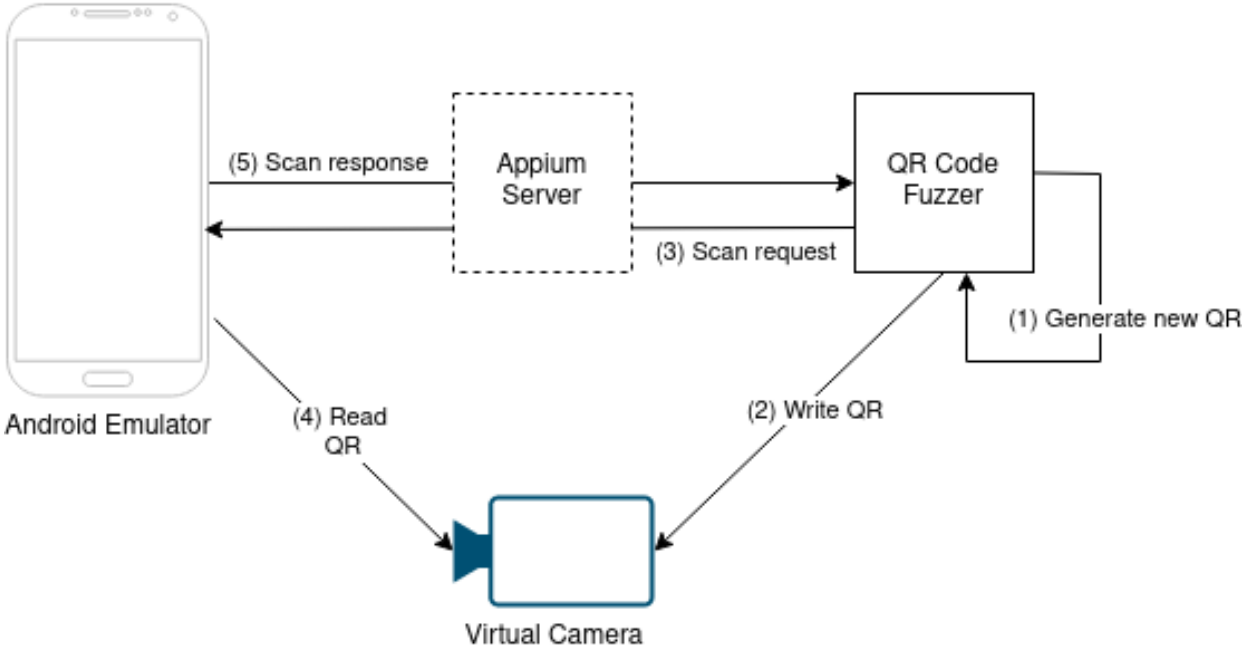


QRFuzz issues

- Camera overheating
- Not scalable
- Difficult to replicate
- Communication between components



New Architecture



Camera virtualization

- OBS Virtual Camera

- GStreamer

- v4l2loopback

v4l2loopback Public

Camera virtualization

- OBS Virtual Camera
- GStreamer
- v4l2loopback

v4l2loopback Public

FFmpeg

Camera virtualization

- OBS Virtual Camera
- GStreamer
- v4l2loopback

v4l2loopback Public

FFmpeg

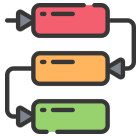
Device virtualization

- Integrates with virtual camera
- Scalable
- Reproducible environment

Automation

- Install script

- Dependency management



- Components manage own dependencies

Towards integration

Virtualizing old architecture

Virtualize device and webcam

Towards integration

Virtualizing old architecture	Problem
Virtualize device and webcam	QR displayed by generator on screen

Towards integration

Virtualize device and webcam

QR displayed by generator on screen

Use a static image as a video

Towards integration

Virtualizing old architecture	Problem	Temporary solution	Solution
Virtualize device and webcam	QR displayed by generator on screen	Use a static image as a video	Rewrite the generator

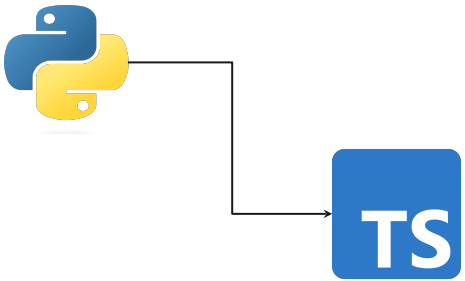
Towards integration

Virtualizing old architecture	Problem	Temporary solution	Solution	Bonus
Virtualize device and webcam	QR displayed by generator on screen	Use a static image as a video	Rewrite the generator	The components can be merged

Improvements

QR Generator: Python → TypeScript

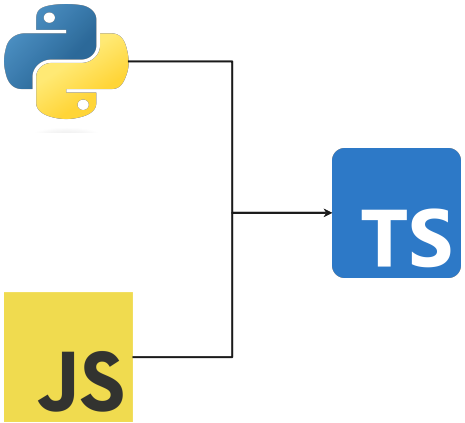
- Support for invalid utf-8 strings
- Save state/resume



Improvements

QR Generator: Python → TypeScript
- Support for invalid utf-8 strings
- Save state/resume

QR Fuzzer: JavaScript → TypeScript
- Bug fixes

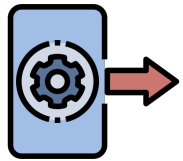


Merging components benefits

- Error management across components
- Improved dictionary iteration
- Simpler intercomponent communication
- Easier dependency management

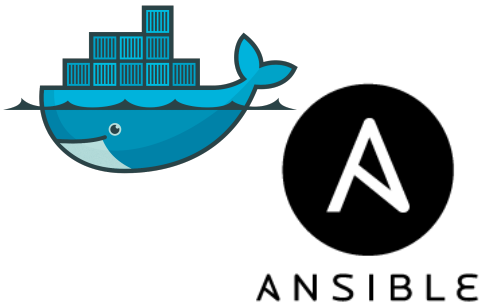
Future Work

- Dynamically generated fuzzing payload

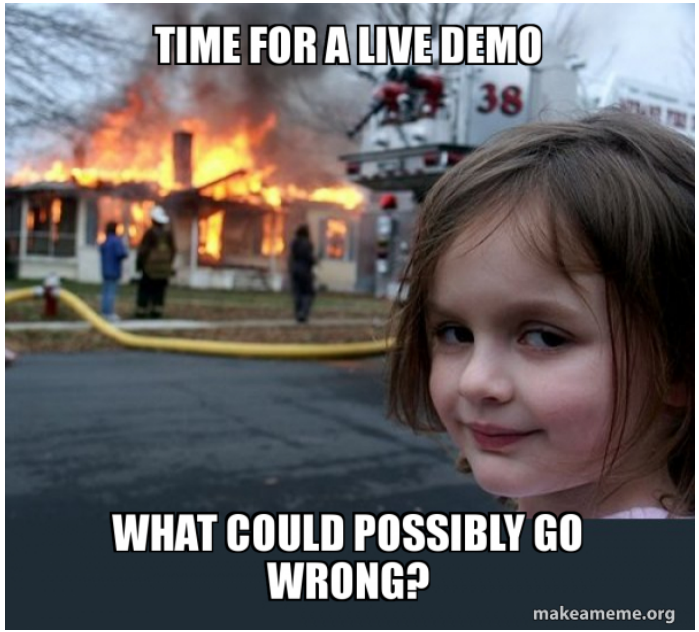


- More inspectors

- Containerization



Live Demo


TIME FOR A LIVE DEMO
38
WHAT COULD POSSIBLY GO WRONG?
makeameme.org

DO NOT USE THIS SLIDE - EMERGENCY ONLY