How automatisation can improve firmware analysis ?

Introduction to Pyrrha: a firmware mapper

Eloïse Brocas <ebrocas@quarkslab.com>
Jean-Marc Bourgeois <jbourgeois@quarkslab.com>
Robin David <rdavid@quarkslab.com>

IN CYBER FORUM

Quarkslab

Quarkslab

Securing every bit of your data

Société de cybersécurité française fondée en 2011

€ 7,5m de levée de fond 2020

100+ employés
20% Docteurs

Bureaux en France et en Argentine

QLab

Sécurité offensive et défensive
Audit de sécurité et R&D appliquée
SW, FW, HW
Blockchain, librairies cryptographiques
Formation
Certification de sécurité (CESTI - CSPN)

R&D

Ouvrir la voie aux futures innovations utilisées dans le développement de **produits** et **services**

Produits

QShield

Protection logicielle du code, des données et des clés

QFlow

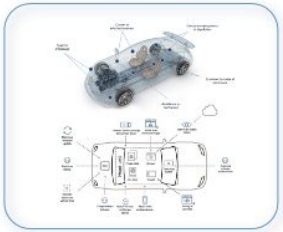
Plateforme d'analyse automatique de fichiers

Missions QLab

OBJET CONNECTÉ
CONSEIL ET AUDIT DE SÉCURITÉ

CRYPTOGRAPHIE
CONSEIL ET AUDIT DE SÉCURITÉ

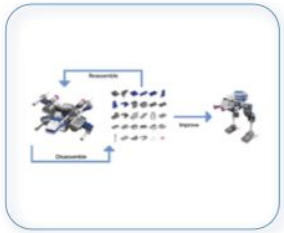
CSPN



AUTOMOTIVE
CONSEIL ET AUDIT SÉCURITÉ

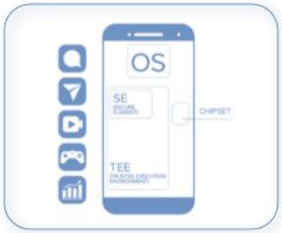
TECHNICAL DUE DILIGENCE

PROTECTION PROPRIÉTÉ INTELLECTUELLE



RECHERCHE EXTERNALISÉE

CLOUD
AUDIT D'ENVIRONNEMENT



ÉCOSYSTÈME MOBILE
CONSEIL ET AUDIT DE SÉCURITÉ

BLOCKCHAIN
CONSEIL ET AUDIT DE SÉCURITÉ

Use-Case

Firmware Analysis

Definition / Problematic

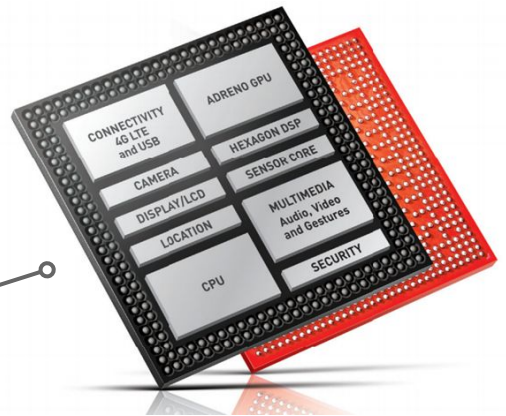
Definition: Firmware Package

Set of files to update the various components of a whole system.

⇒ Fully-featured OS:

- base operating system
- various libraries, SDKs etc
- vendor application specific code

⇒ Can be composed of **multiple sub-firmwares** *(OSes)* for the different components of the SoC *(for instance)*.



Problematic: Aggregate of components, binaries, files coming from various **third-parties**.

Why Analyzing Firmwares ?

- Finding vulnerabilities
- Artifacts left *(private keys, build files, symbols)*
- Compliance:
  - checking patches are applied
  - checking firmware signatures *(trust management)*
- Bill-of-Materials

Exemple: Netgear RAX30

Components:

- SoC ARM
- Linux *(base OS)*
- network configuration softwares
- web administration panel
- firmware upgrade features

Metrics: *(2275 files)*

- 713 Executable files
  - 255 579 functions
  - 12,612,710 asm instructions
- 1562 Files
  - 152 php files
  - 125 shell scripts
  - …

Netgear RAX30

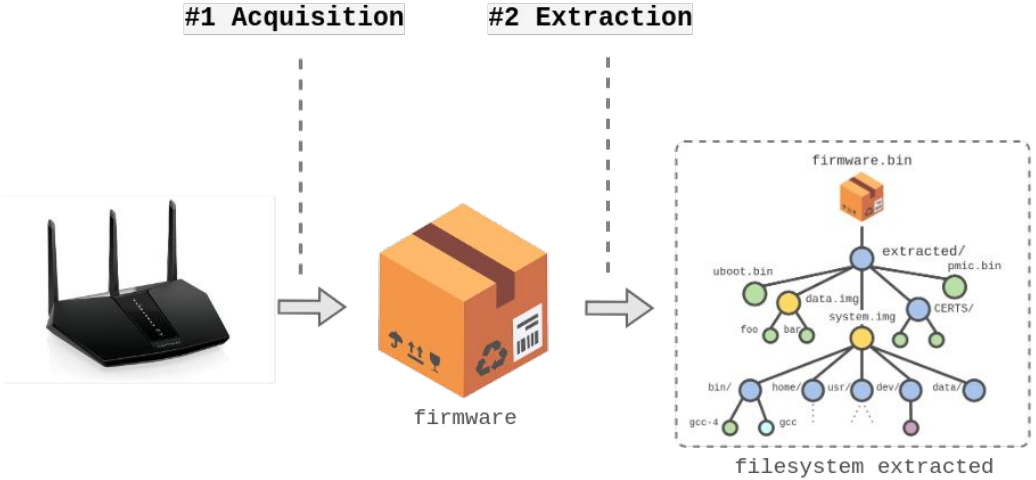
Analysis Workflow

Analysis Workflow

#1 Acquisition

firmware

Analysis Workflow



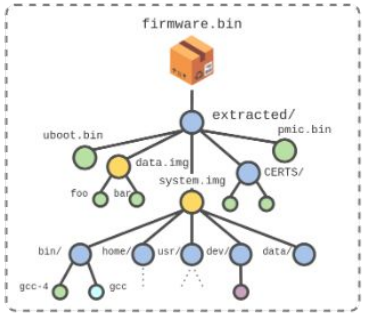
Analysis Workflow

#1 Acquisition

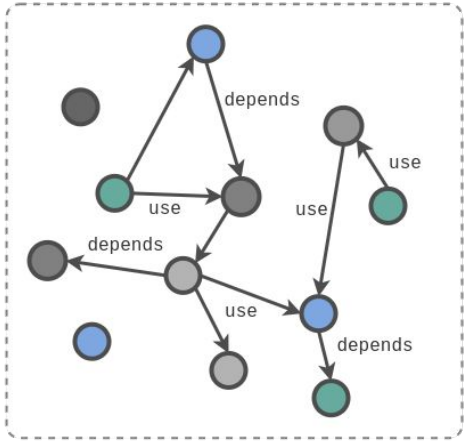
#2 Extraction

#3 Mapping / Correlations

firmware

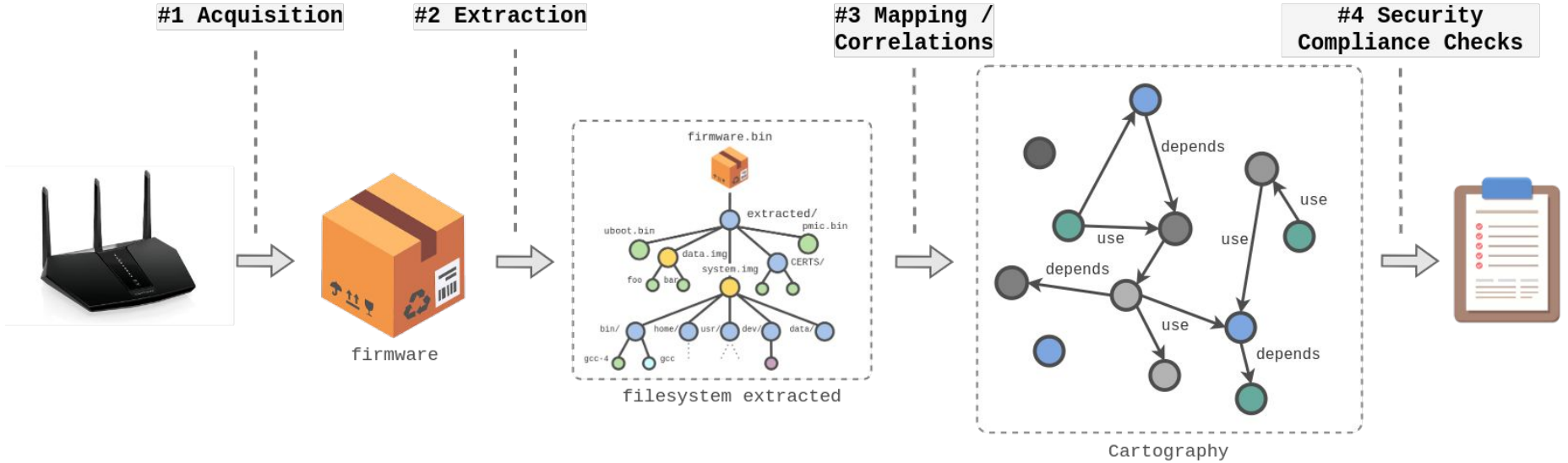


filesystem extracted

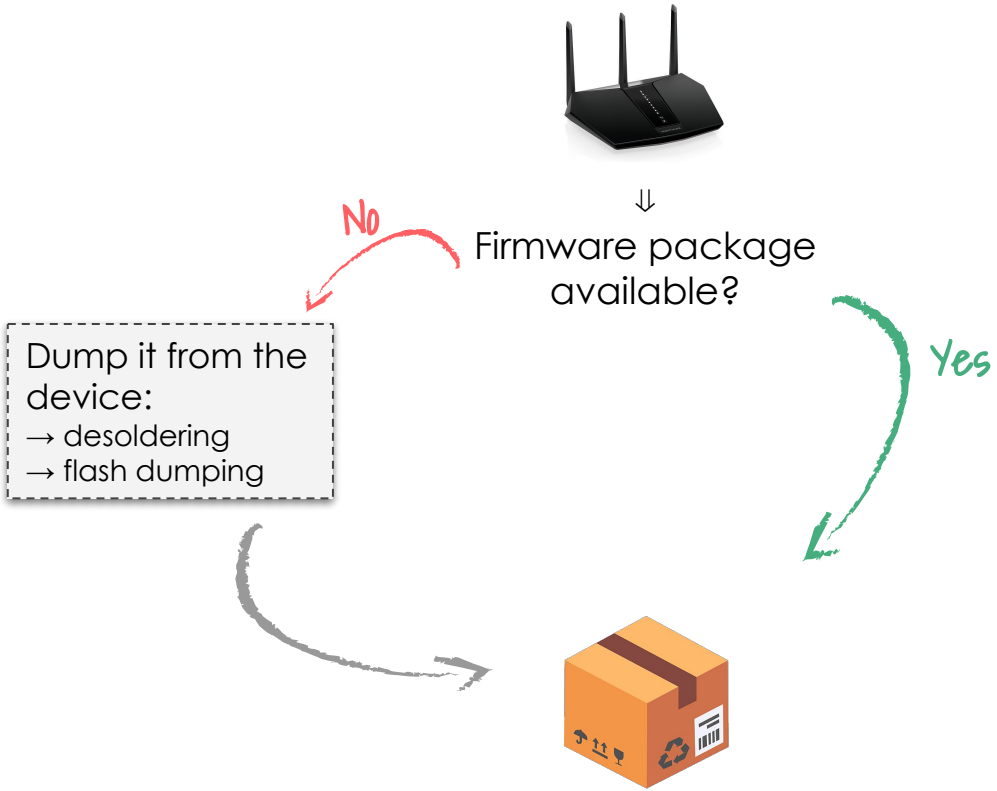


Cartography

Analysis Workflow



Acquisition (#1)



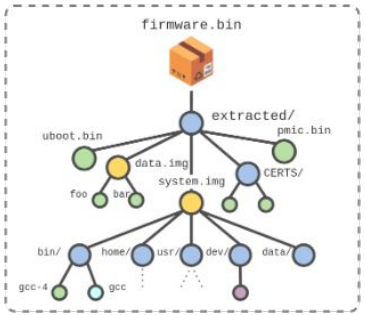
Firmware Extraction

⇒ **Problem:** Usually custom **proprietary format** !

Unblob *(by OneKey)*
https://unblob.org/

binwalk *(by ReFirmLabs)*
https://github.com/ReFirmLabs/binwalk

firmware



filesystem extracted

Firmware Cartography

(with Pyrrha)

Quarkslab

What is it ?

What ?

Mapping dependencies between executables, and between files as a **graph**.

Why ?

Saving time & be more **efficient**.

How ?

> Analyse executables and shared libraries dependencies *(.so / .dll)*
> Resolve symbolic links
> Resolve mount points
> etc..

⇒ Put all this data into a **graph database** and **visualize** it.

Introducing Numbat & Pyrrha

Pyrrha

PYRRHA

Developed by Quarkslab

⇒

Numbat

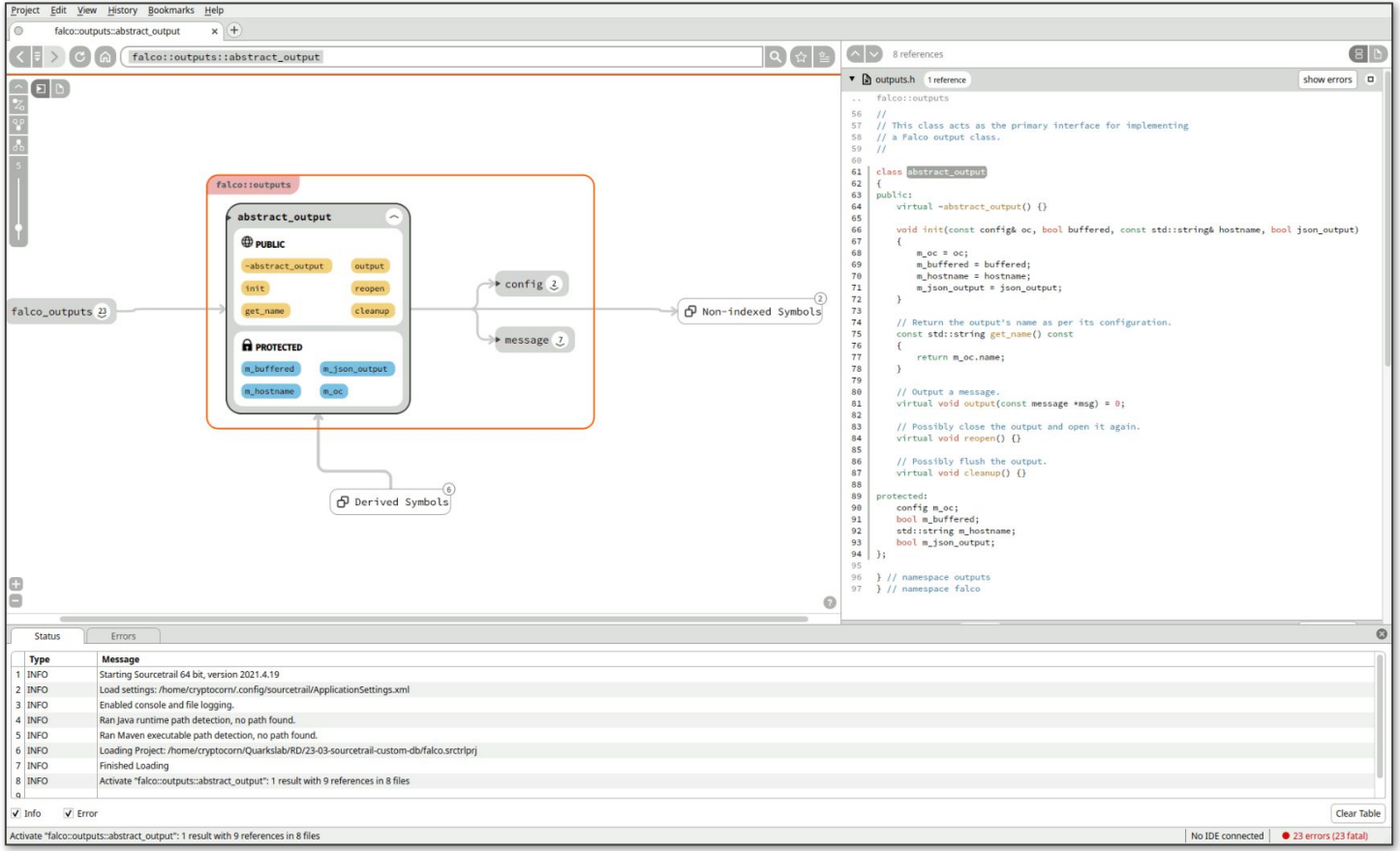
Developed by Quarkslab

Both open source !

SOURCETRAIL

https://blog.quarkslab.com/leveraging-sourcetrail-to-a-mapping-tool-meet-numbat-and-pyrrha.html

Demo #1: Sourcetrail

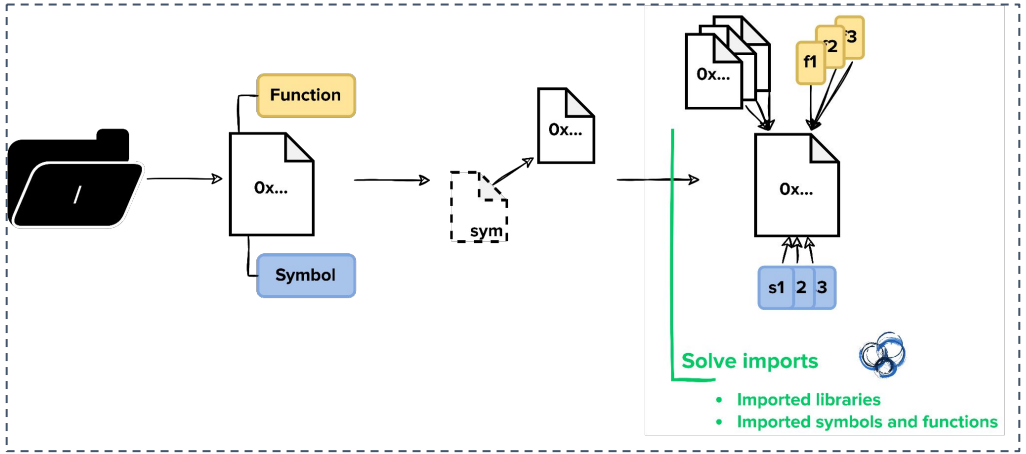


Pyrrha

Quarkslab

Pyrrha *(in short)*

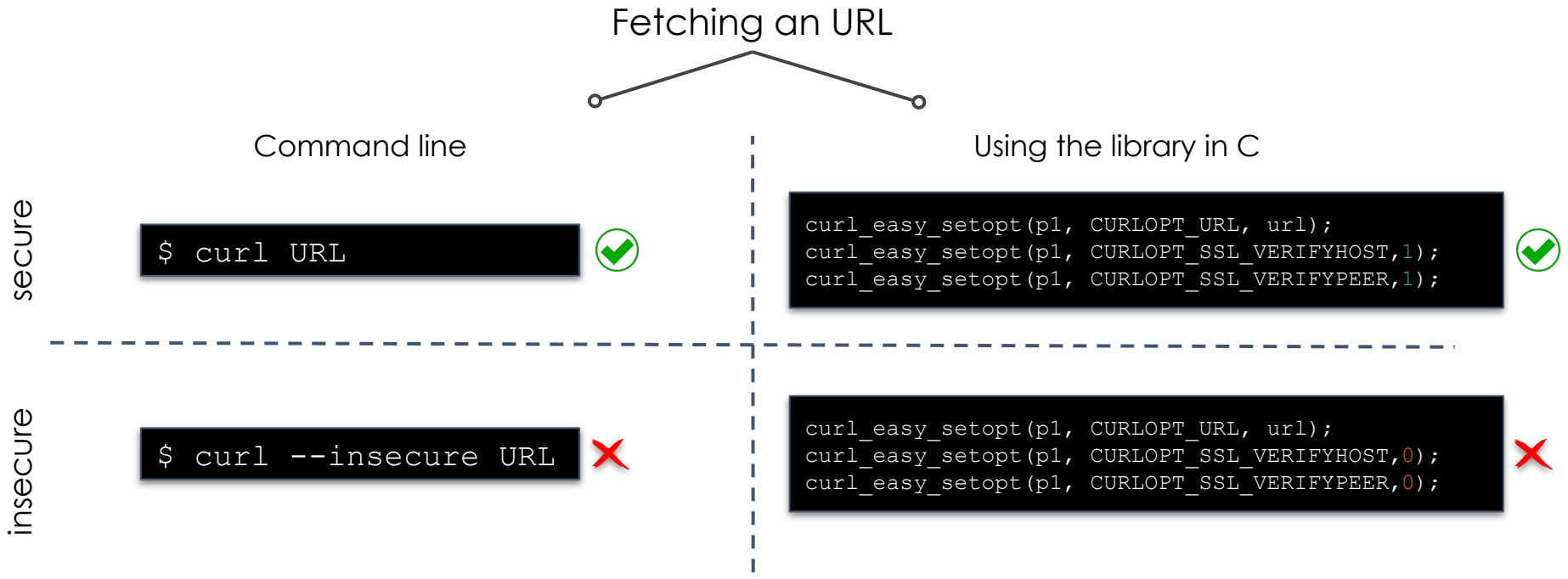
1. Scan the root/ filesystem
2. Parse executable files
   a. Parse **symbols**
   b. Parse **dependencies** *(shared libraries)*
3. Resolve symbolic links
4. Create the **graph** based on imported symbols (using Numbat)



Demo #2: Pyrrha

Pyrrha result on
Netgear RAX30

Firmware Update *(Netgear RAX30)*



pucfu binary checks for firmware upgrade online using the library.

Demo #3

Which executables are
using libcurl.so ?

Conclusion

Benefits:

- **Speed-up** security assessments
- **Automate** analysis and checks in client's workflows

Checks:

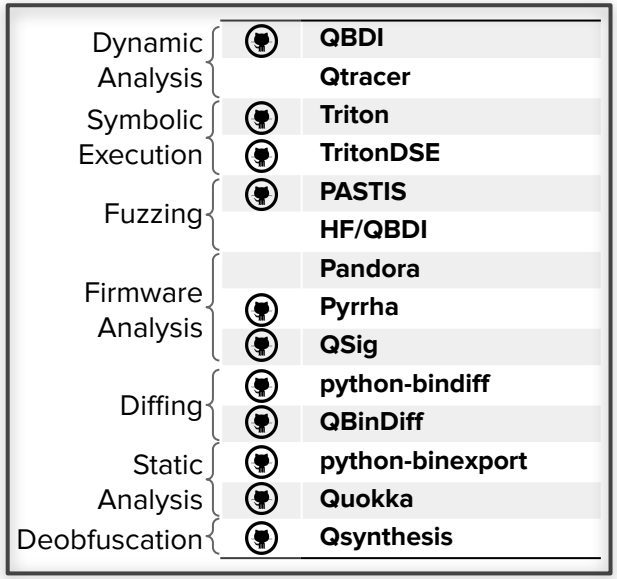
- Configuration compliance
- Firmware signatures
- CVEs
- Cryptographic keys
- Additional properties
- Bill-of-materials

Research in the Lab

Conferences

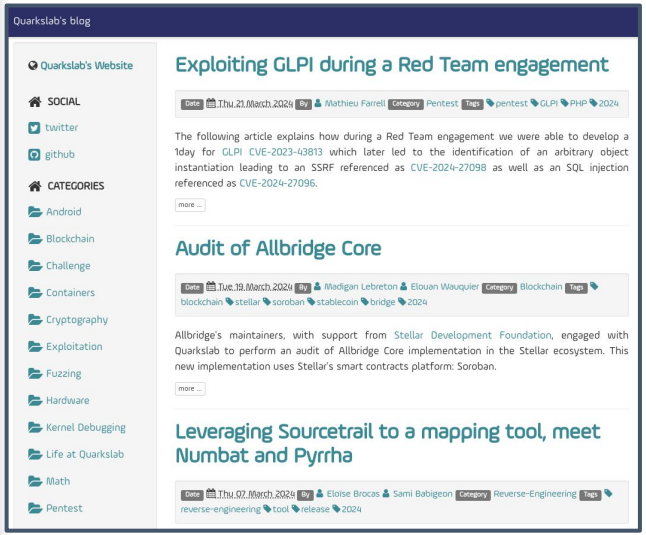
https://github.com/quarkslab/conf-presentations

Open source



https://github.com/quarkslab/

Blog



https://blog.quarkslab.com

Thank you

Contact information:

Email: contact@quarkslab.com

Phone: +33 1 58 30 81 51

Website: quarkslab.com

@quarkslab

Quarkslab