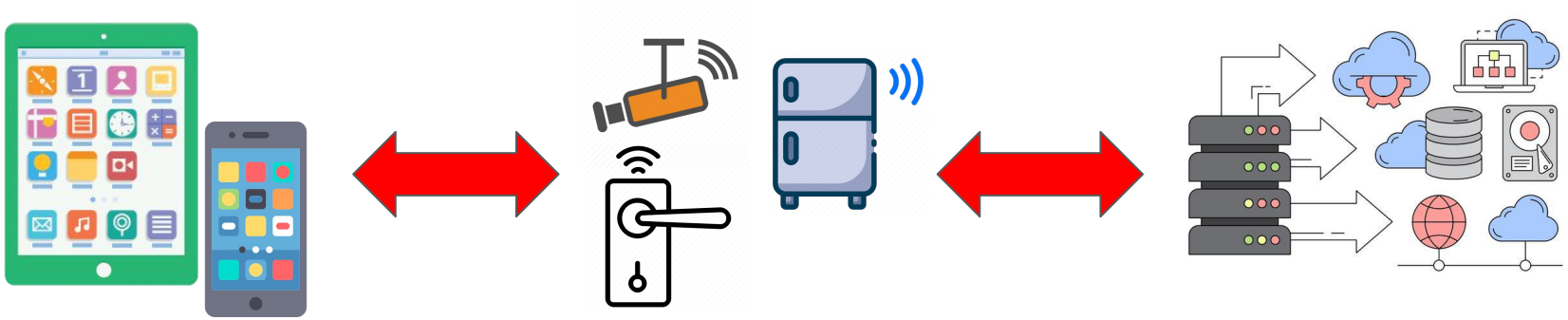
1st Workshop on Trustworthy Software Ecosystems

Emerging Software Ecosystems: a glimpse of challenges and opportunities

Luca Verderame

UNIVERSITÀ DEGLI STUDI DI GENOVA | Dibris

Emerging Computing Platforms



Mobile

Internet of Things (IoT)

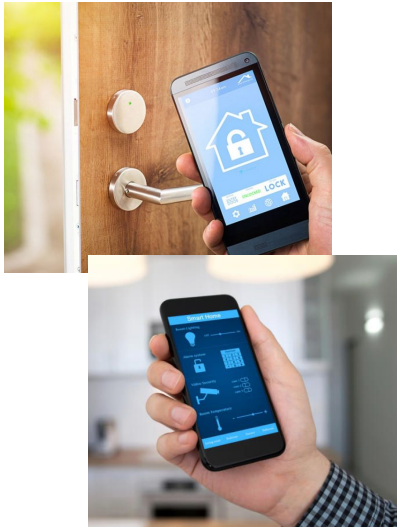
Cloud & Edge

- Real world scenarios require cooperation of different software paradigms
  - Shift from isolated environments to **<u>interconnected ecosystems</u>**

A Plethora of Use-Cases

Automotive

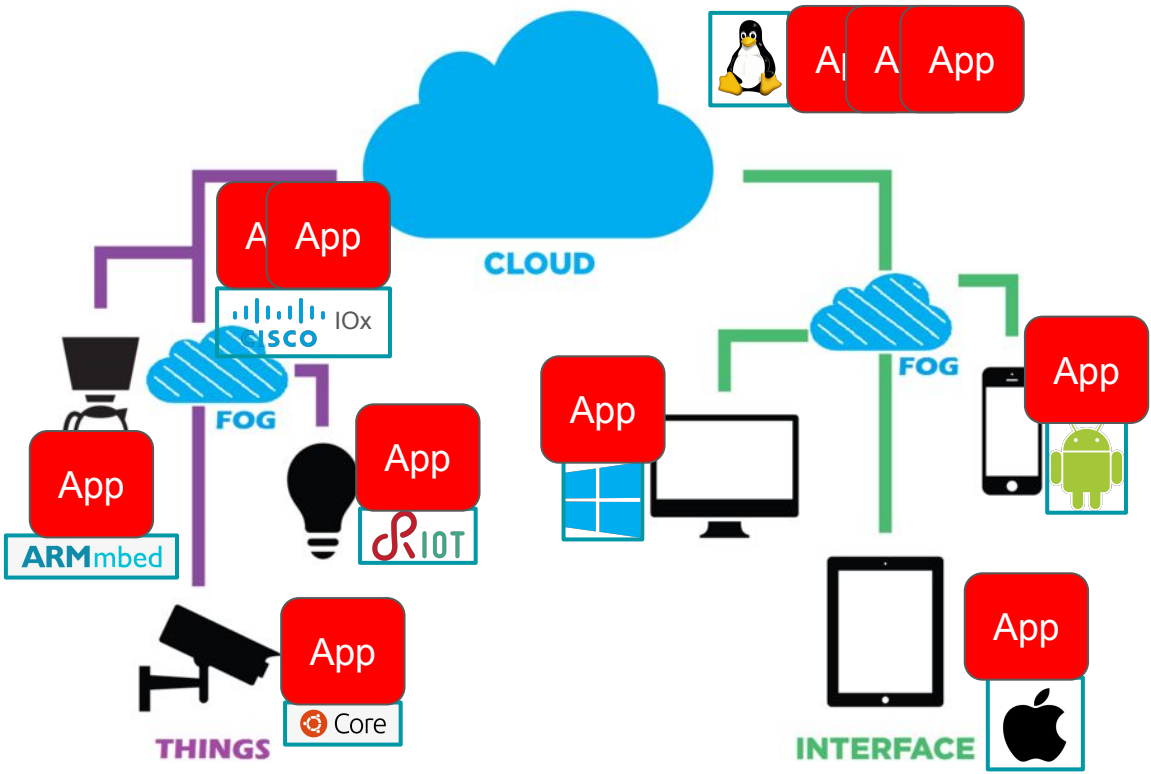
Smart Home



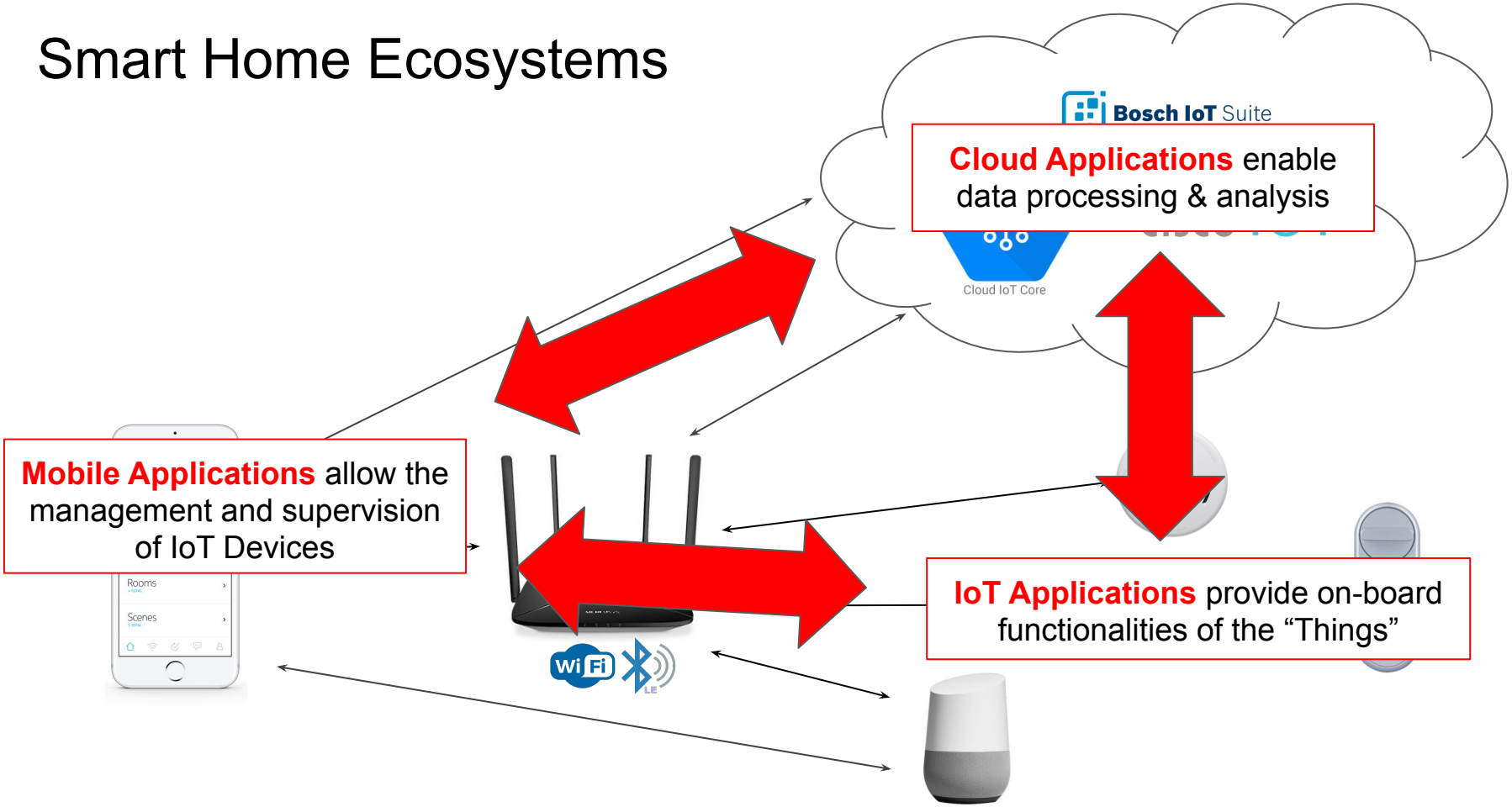
Industrial-IoT

Software Ecosystems

- Interconnected devices are managed through multi-layer/actor architecture
- Main actors:
  - Operating systems
  - Applications



Smart Home Ecosystems



OWASP IoT 2018 - TOP Security Risks

1 Weak, Guessable, or Hardcoded Passwords
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2 Insecure Network Services
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

3 Insecure Ecosystem Interfaces
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

4 Lack of Secure Update Mechanism
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

5 Use of Insecure or Outdated Components
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

Is There “Actually” a Security Problem?

“If the attacker is on the same internal network as the HG100 or a mobile device with the companion app (android or iPhone), he can **take control** of all the connected IoT devices.”

- CVE-2019-11061 : Broken access control in HG100
- CVE-2019-11063 : Broken access control in SmartHome app

Can it get worse?

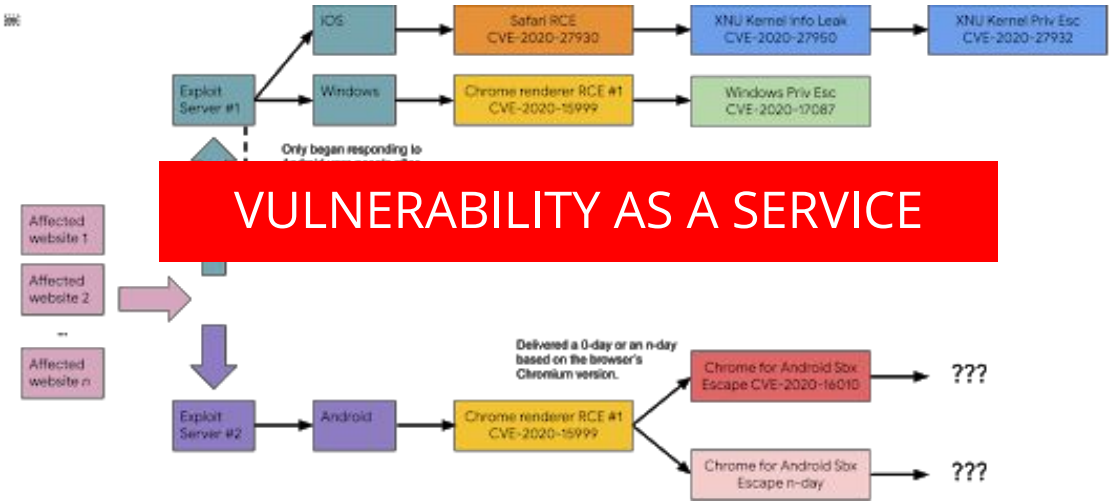
MASTER HACKERS —

“Expert” hackers used 11 0-days to infect Windows, iOS, and Android users

The breadth and abundance of exploits for unknown vulnerabilities sets group apart.

DAN GOODIN - 3/18/2021, 11:18 PM

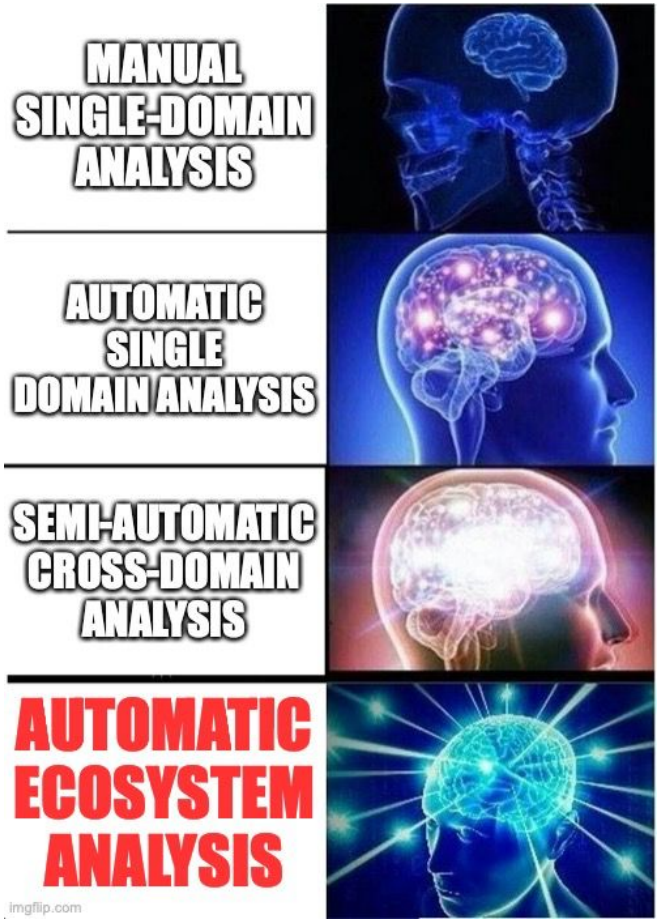
“In October 2020, Google Project Zero discovered seven 0-day exploits being actively used in-the-wild. These exploits were delivered via "watering hole" attacks in a handful of websites pointing to two exploit servers that hosted exploit chains for Android, Windows, and iOS devices.”



https://googleprojectzero.blogspot.com/2021/03/in-wild-series-october-2020-0-day.html

Security Issues

- Applications are the soft underbelly of ecosystems
- Heterogeneous technologies boost the complexity in security and risk assessment
- Manual inspection & testing does not scale
- Existing techniques are typically limited to single domains



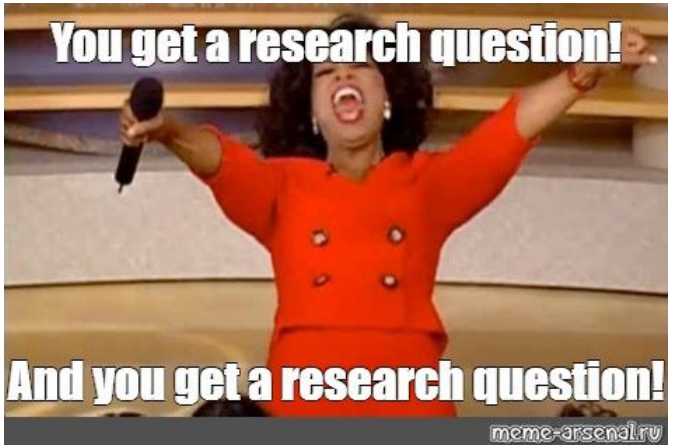
(Some) Research Opportunities/*Questions*

- **Model cross-domain interactions**
  - *Can we define a model to represent cross-domain interactions among apps?*
  - *Can we introduce a technology-agnostic solution to cope with heterogeneous apps and protocols?*
- **Define ecosystem-wide analysis methodologies**
  - *Can we compose static and dynamic analysis techniques to evaluate complex vulnerabilities?*
  - *Can we adapt existing VA/PT procedures for the evaluation of an entire ecosystem?*

(Some) Research Opportunities/*Questions*

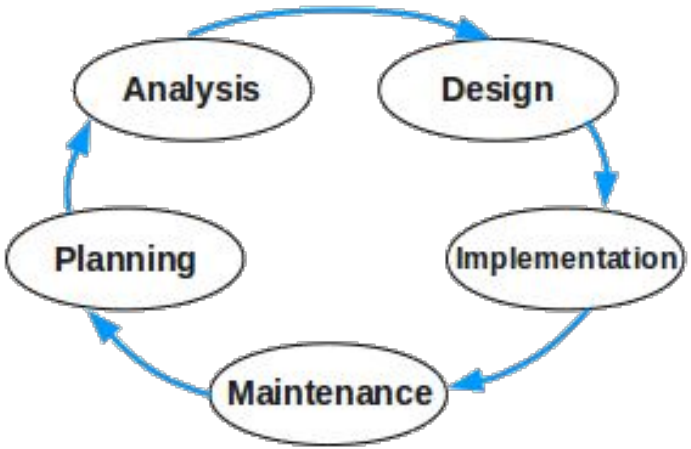
- **Move towards automated solutions**
  - *Can we automate the modeling and analysis phases?*
  - *Can we emulate/simulate a software ecosystem?*

- **Evaluate the entire lifecycle (and supply chain)**
  - *Can we define methodologies to detect cross-domain vulnerabilities during development?*
  - *Can we evaluate the security/integrity of apps in the supply chain to mitigate ecosystem vulnerabilities?*

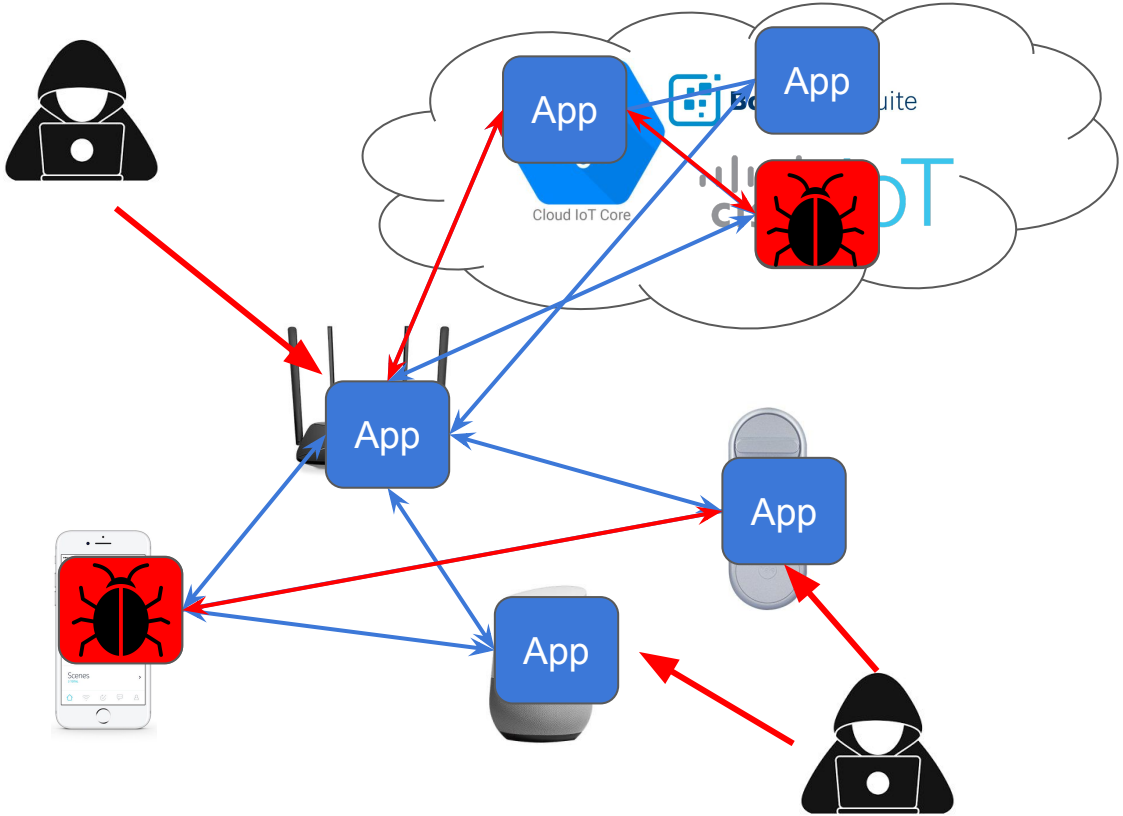


A (possible) Research Battle Plan

- Identify and model **cross-domain** security **threats** (a.k.a. what to check)
- Evaluate the **combination** of **SAST** and **DAST** technologies to propose novel detection methodologies and tools
- Empower **DevSecOps** pipelines to detect early stage vulnerabilities
- Define **VA/PT** processes to evaluate existing ecosystems



Research Challenge: Hybrid Ecosystem App Analysis



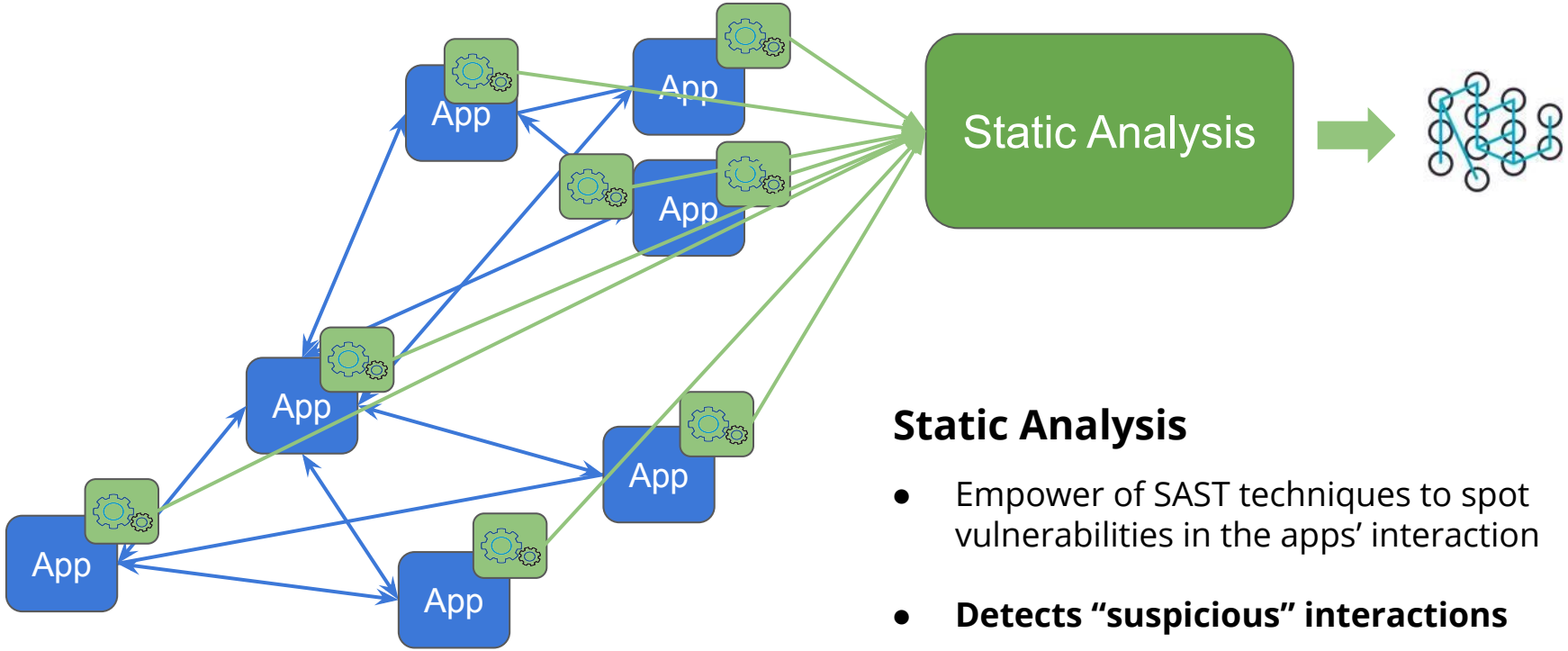
Ecosystem Modeling

- App extraction
- Interaction detection

Attack Surface

- Internal/external threats
- Malicious interactions

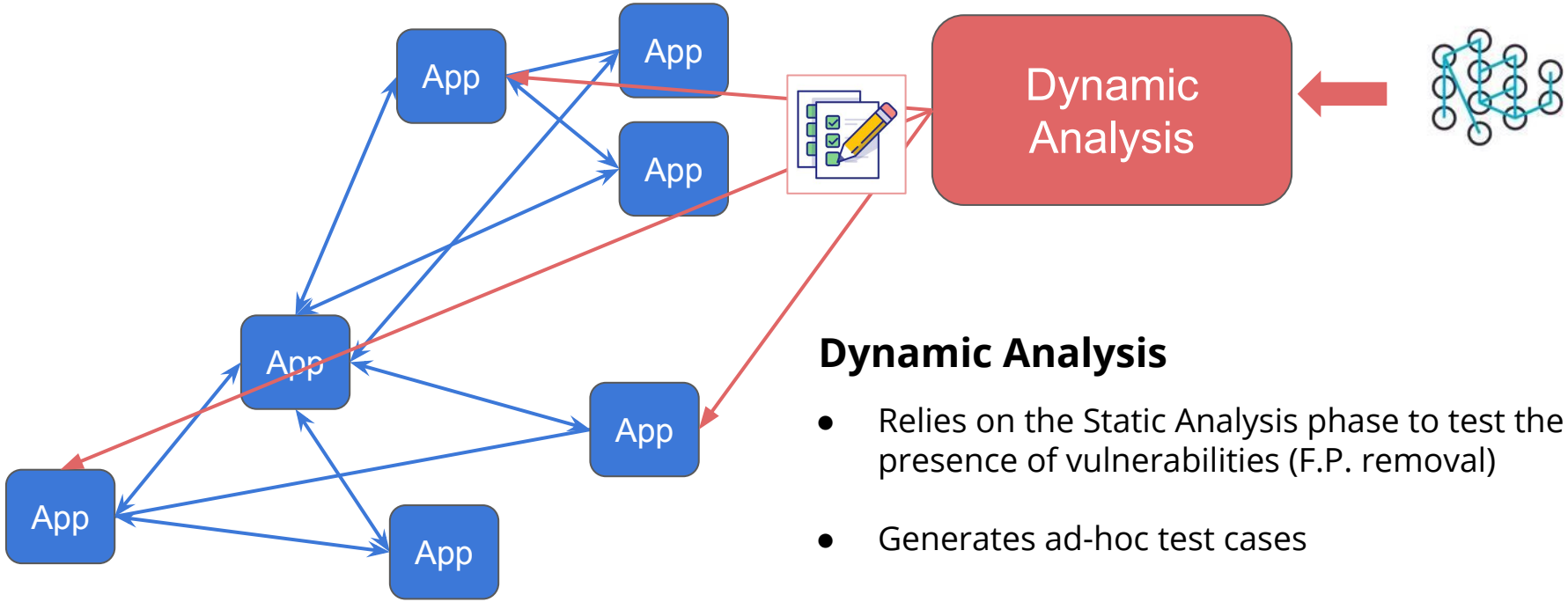
Research Challenge: Hybrid Ecosystem App Analysis



Static Analysis

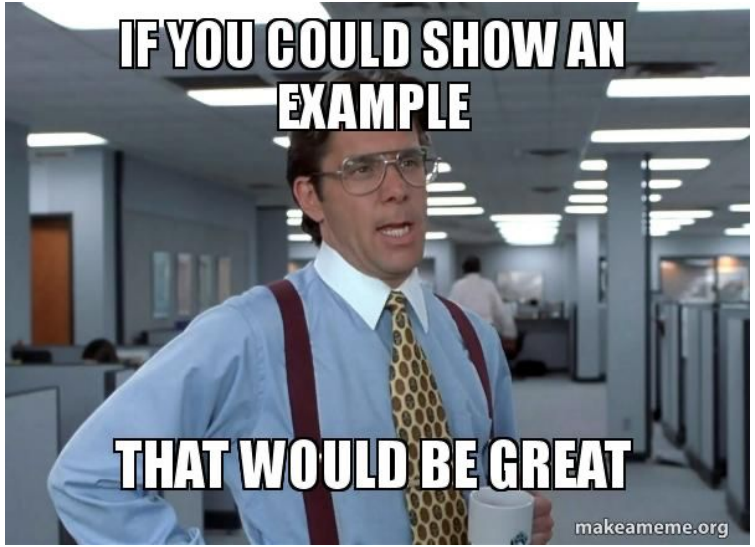
- Empower of SAST techniques to spot vulnerabilities in the apps' interaction
- **Detects "suspicious" interactions**

Research Challenge: Hybrid Ecosystem App Analysis



Dynamic Analysis

- Relies on the Static Analysis phase to test the presence of vulnerabilities (F.P. removal)
- Generates ad-hoc test cases
- **Detect ecosystem vulnerabilities**

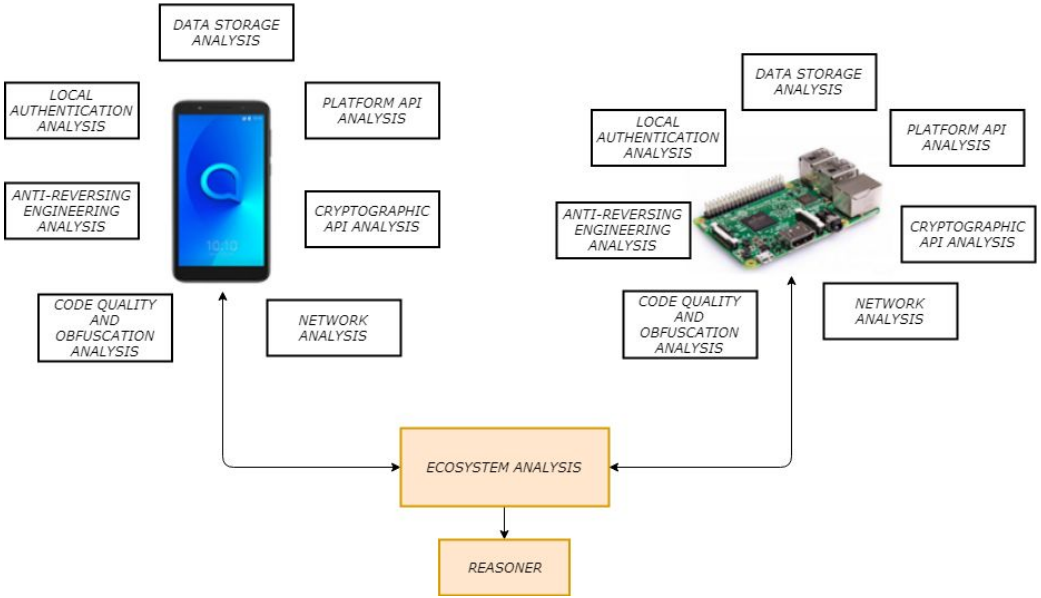


Two examples:

1) an **hybrid mobile-iot** vulnerability assessment methodology;

2) a **DevSecOps** pipeline to detect security vulnerabilities in **IoT firmwares**.

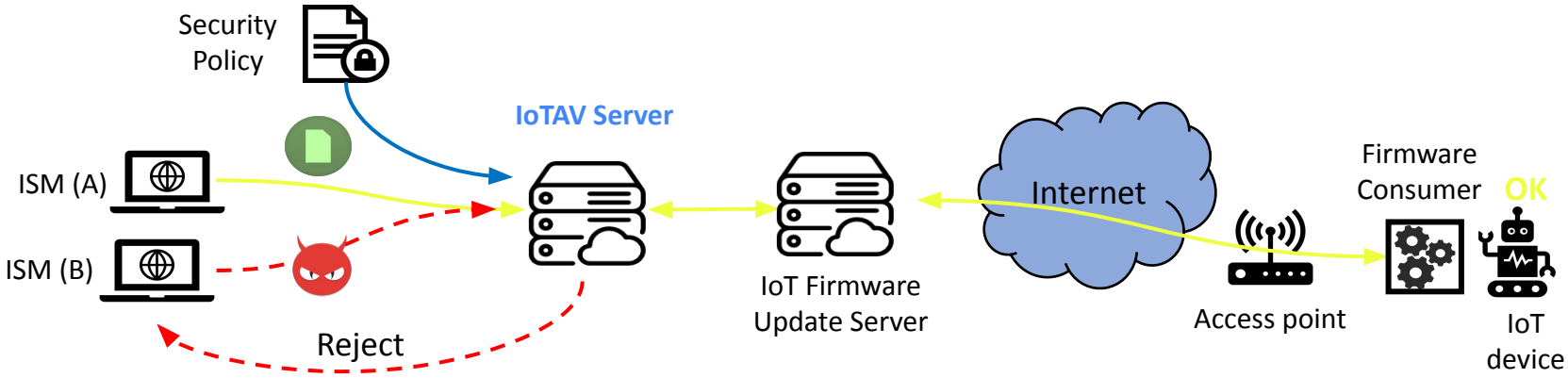
An App-IoT Testing Environment (AppIoTTE)



- AppIoTTE, a cross-domain security assessment methodology for mobile and IoT apps
- Includes both static and dynamic analysis techniques
- Prototype for Android ecosystems

Verderame, L., Caputo, D., Migliardi, M., & Merlo, A. (2020, April). AppIoTTE: an architecture for the security assessment of mobile-IoT ecosystems. In *Workshops of the International Conference on Advanced Information Networking and Applications* (pp. 867-876). Springer, Cham.

IoT Application Verification Framework (IoTAV)



- Static analysis module to **enforce security policies** on firmware software updates;
- Relies on **model extraction** and **model checking** techniques to evaluate software update coming from untrusted ISMs;
- Prototype evaluation for the **RIOT Ecosystem** and the **SUIT update** workflow
- Preliminary evaluation detected **26 policy violations** on 21 real-world RIOT apps

Dejon, N., Caputo, D., Verderame, L., Armando, A., & Merlo, A. (2019, December). Automated security analysis of IoT software updates. In *IFIP International Conference on Information Security Theory and Practice* (pp. 223-239). Springer, Cham.

Some Open Issues

- Model granularity and analysis scaling
- Emulation/simulation vs real systems
- Use of technology-agnostic methodologies
- Strategies to reduce F.P and F.N.
- Software availability (e.g., proprietary solutions, closed environments)

Conclusions

- Emerging computing paradigms shifted from isolation to interconnected ecosystems.
- Applications are the soft underbelly of ecosystems.
- Current approaches are focused on a single domain.
- We need to join forces to propose next-generation methodologies to evaluate the security of software ecosystems.

THANK YOU!

ANY QUESTIONS?

https://csec.it/people/luca_verderame/

luca.verderame@unige.it

/lucaverderame