UNIVERSITÀ DEGLI STUDI DI PADOVA

SPRITZ SECURITY & PRIVACY RESEARCH GROUP

HUMAN INSPIRED TECHNOLOGY Research Centre

DIPARTIMENTO MATEMATICA

The Android Virtualization Technique: a Double-Edged Sword for Developing Attacks and Defences

Eleonora Losiouk

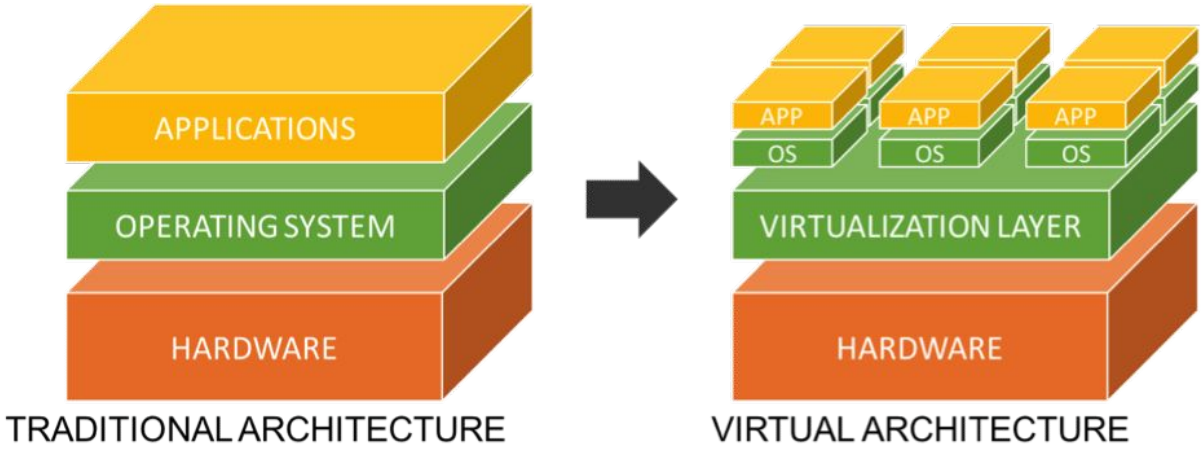
Postdoc in the Spritz Group

Department of Mathematics, University of Padua

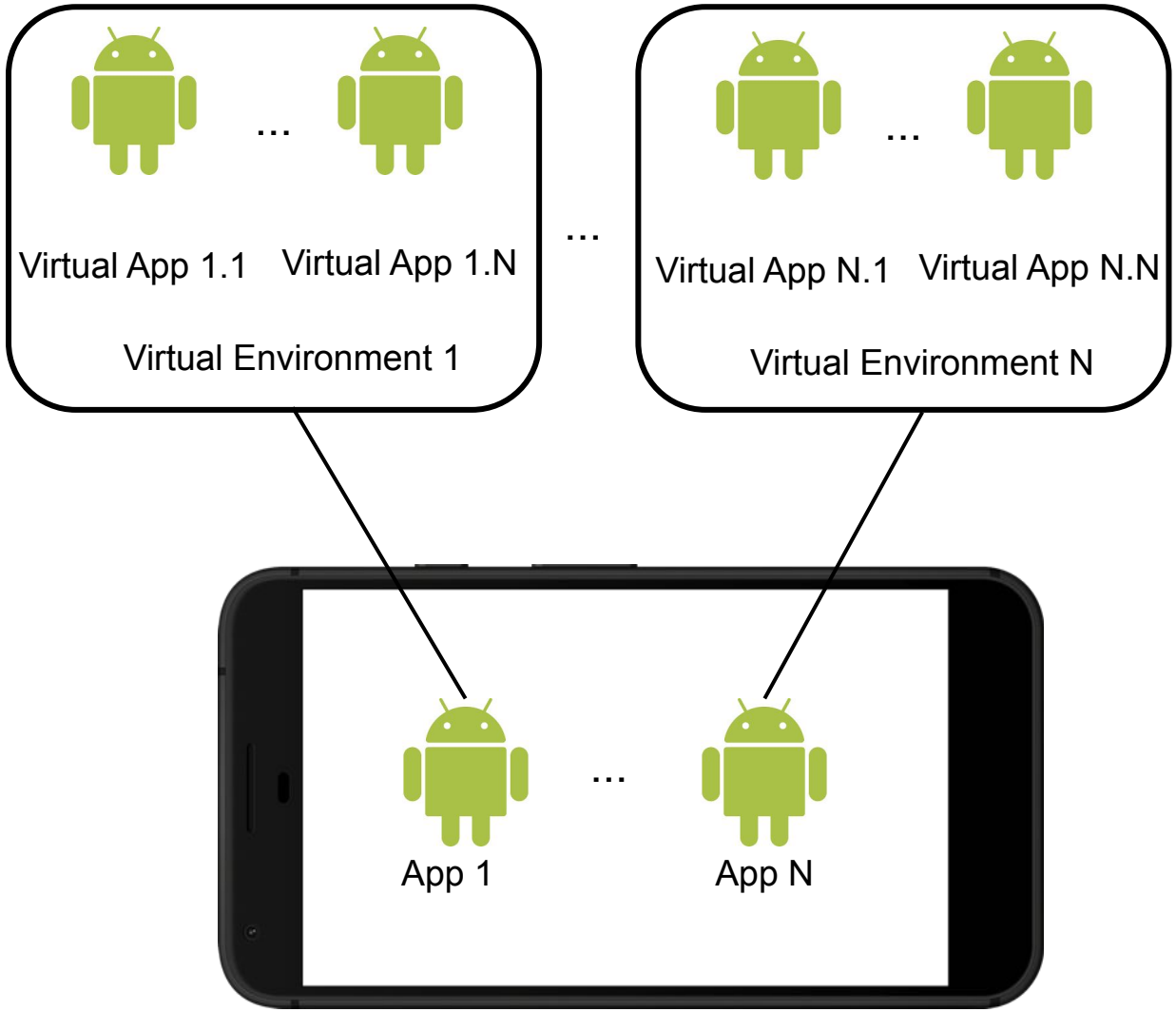
Outline

- Intro on Android Virtualization
- Android Virtualization as an Attack Vector
- Android Virtualization as a Defence Mechanism

The First Idea of Virtualization You Might Have



Android Virtualization



Where Does Android Virtualization Come From?

- Dynamic Code Loading
- Dynamic Proxy Hooking

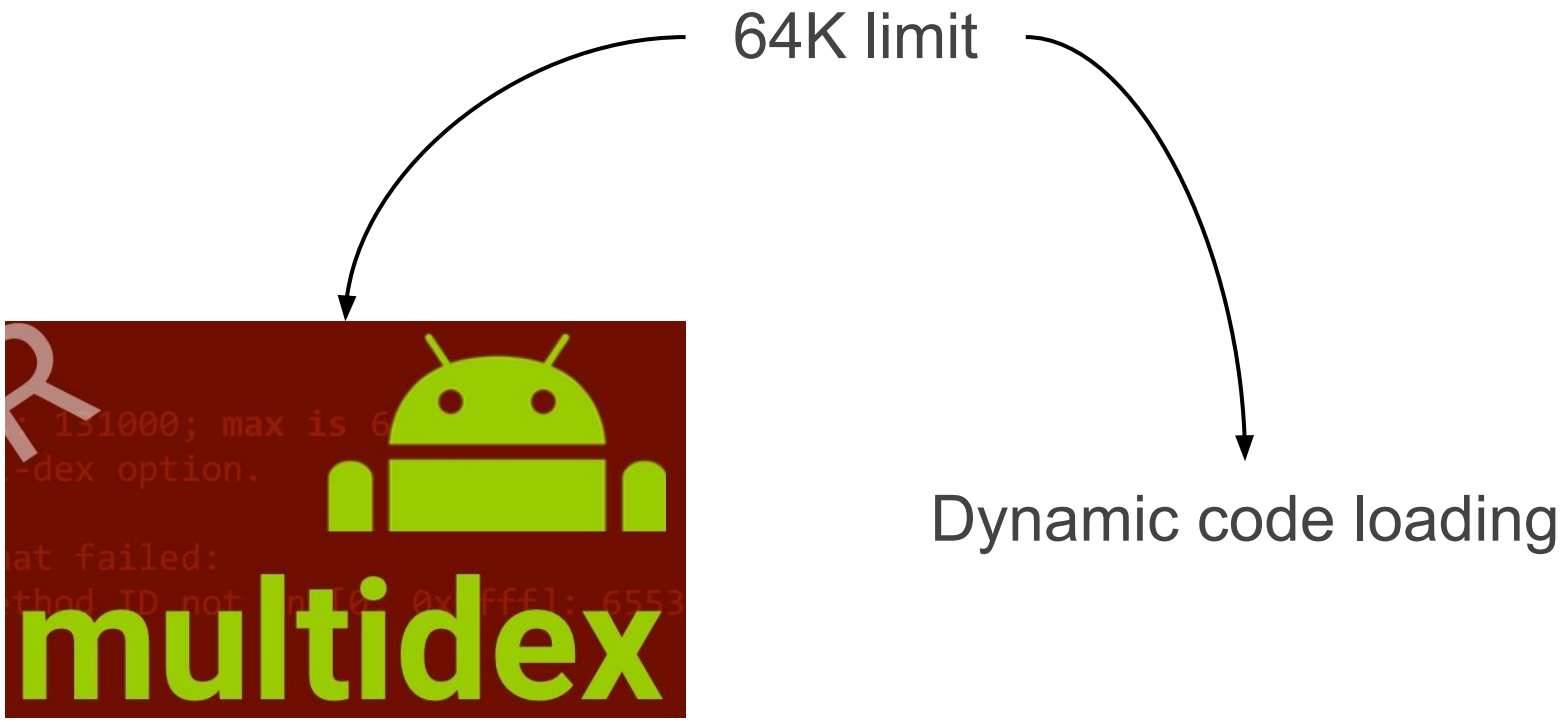
Where Does Android Virtualization Come From?

- Dynamic Code Loading

"The Dalvik Executable specification limits ***the total number of methods that can be referenced within a single DEX file to 65,536****—including Android framework methods, library methods, and methods in your own code. In the context of computer science, the term Kilo, K, denotes 1024 (or 2^10). Because 65,536 is equal to 64 X 1024, this limit is referred to as the* ***'64K reference limit'****"* [1]

[1] https://developer.android.com/studio/build/multidex

Where Does Android Virtualization Come From?

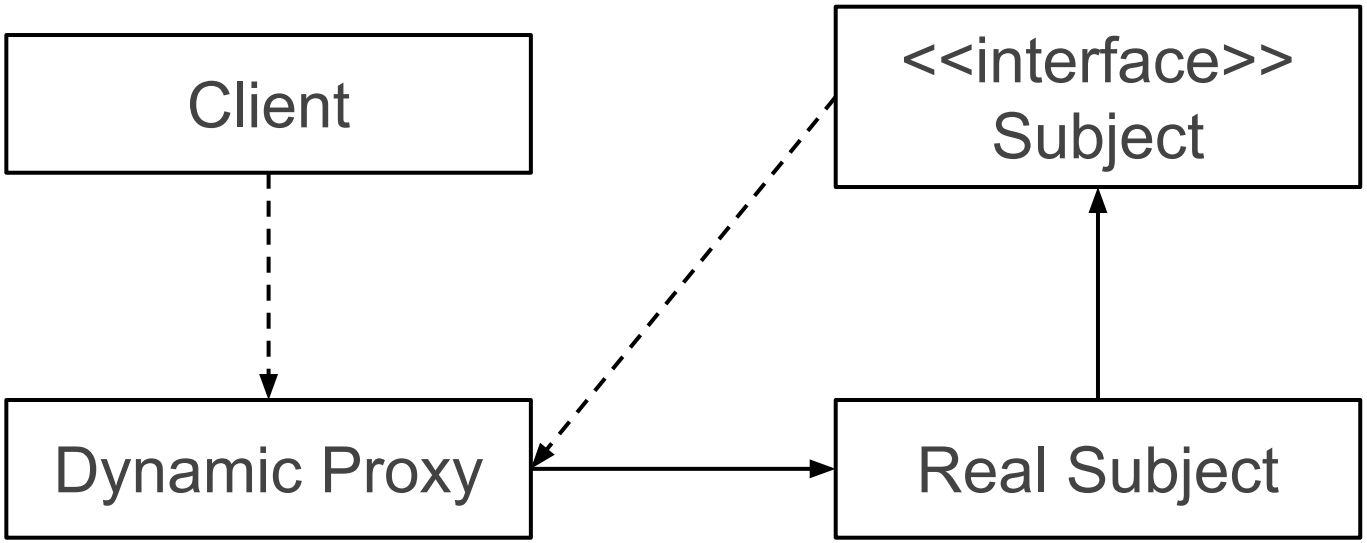


Where Does Android Virtualization Come From?

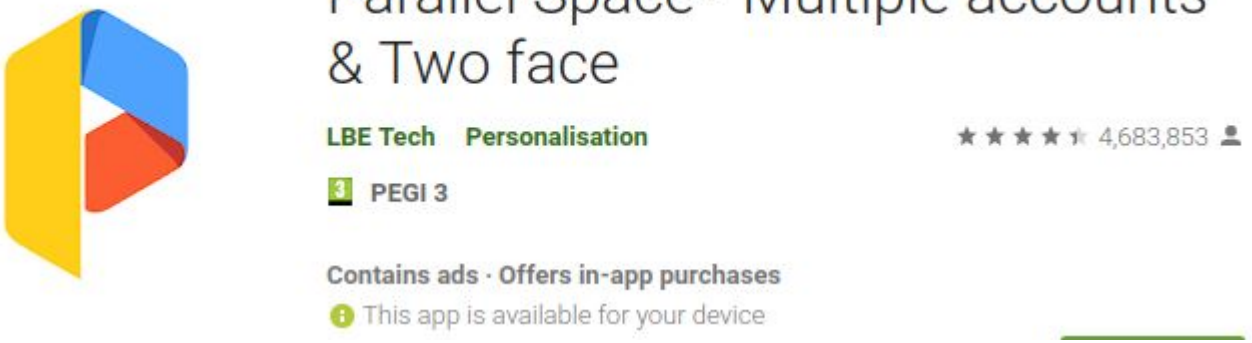
- Dynamic Code Loading
- Dynamic Proxy Hooking

Where Does Android Virtualization Come From?

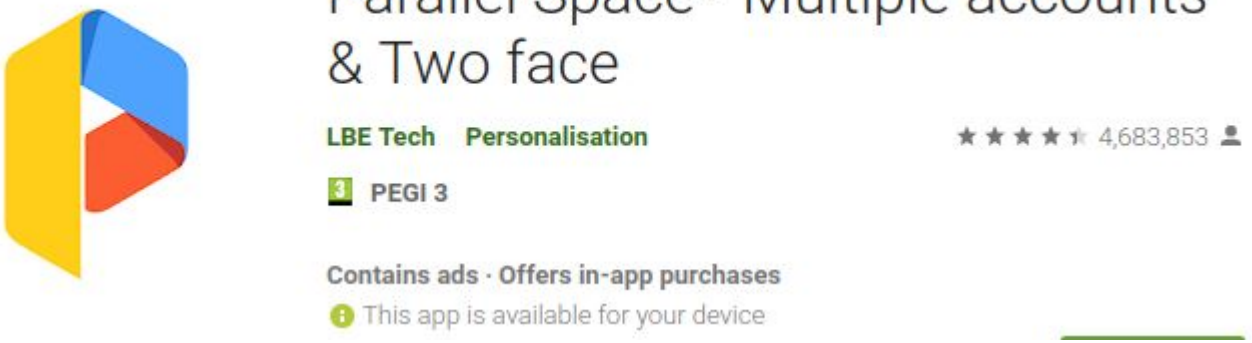
- Dynamic Proxy Hooking

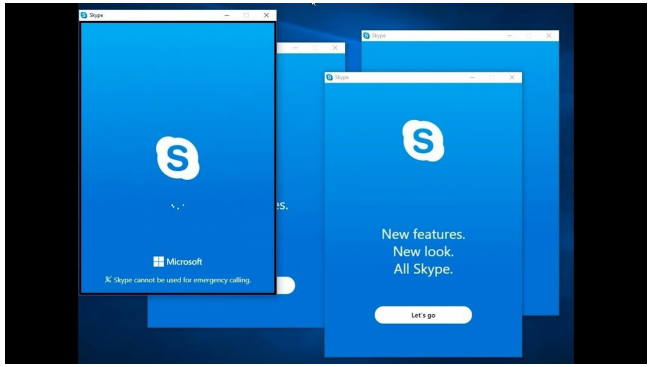


Legitimate Usage of Android Virtualization



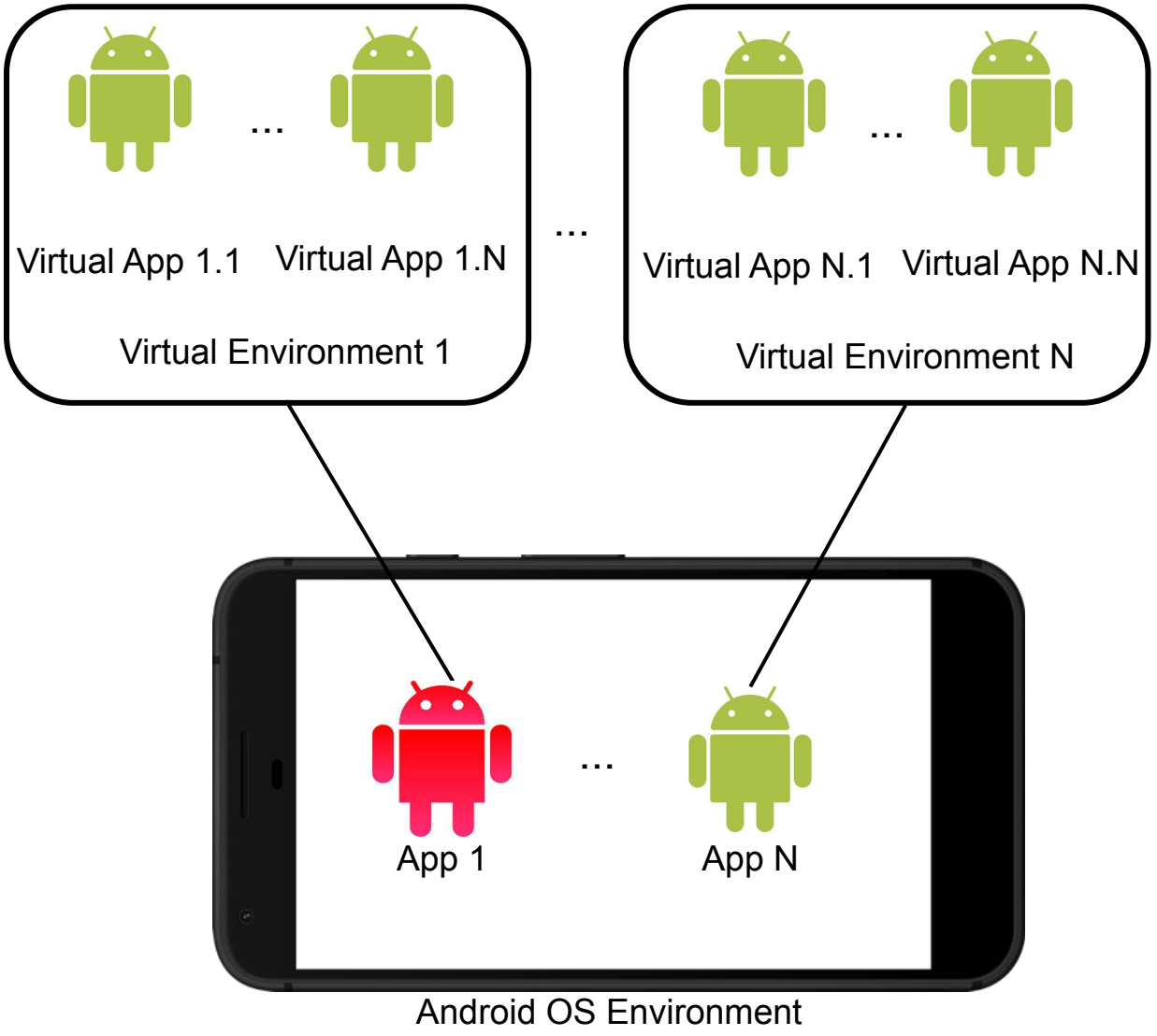
Legitimate Usage of Android Virtualization



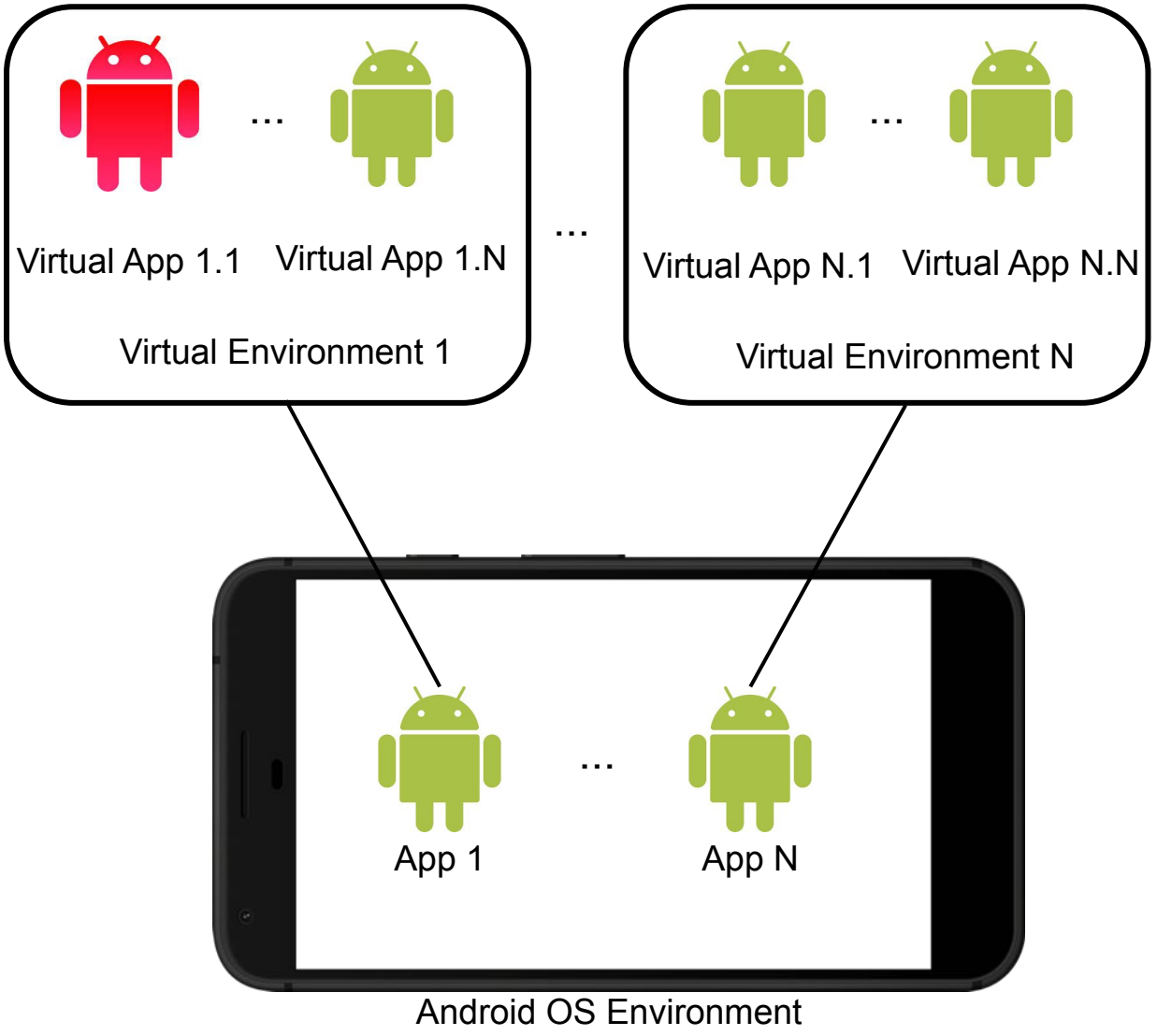



WHaT
CAN
GO WRONG?

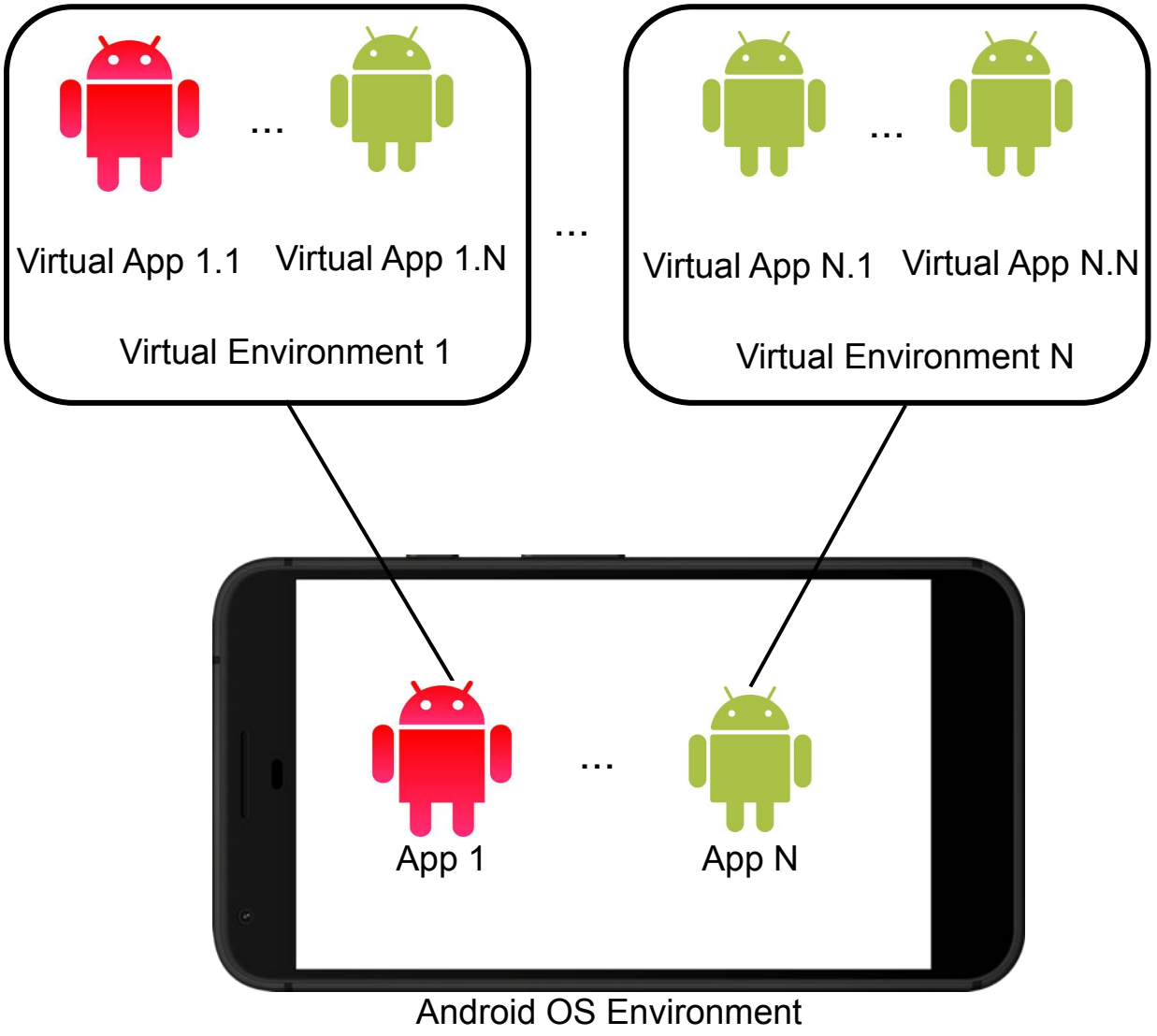
Malicious Container App



Malicious Plugin App



Malicious Container and Plugin App

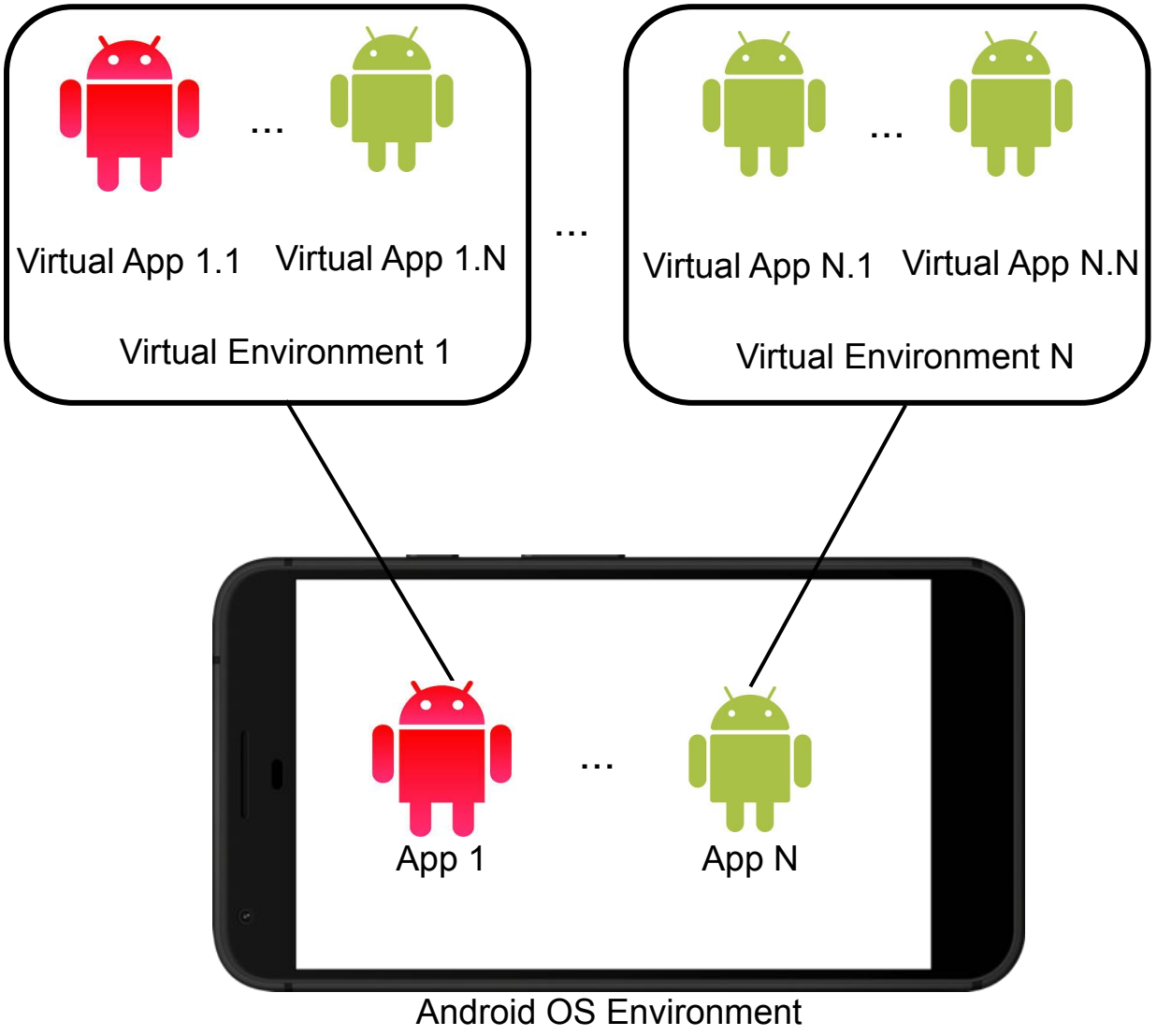


Anti-Virtualization Mechanisms

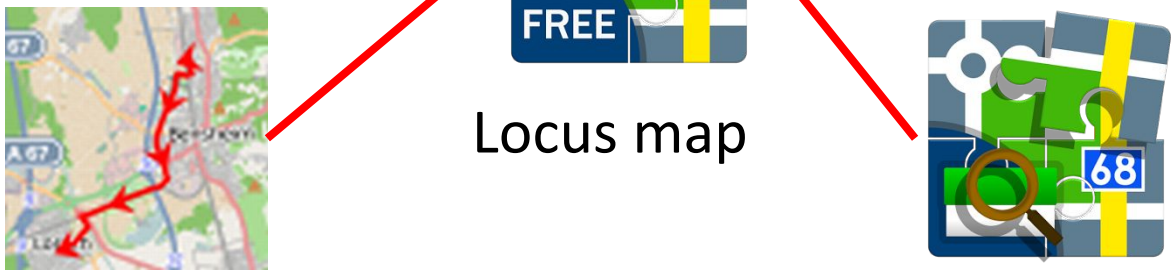
1. L. Shi, J. Fu, Z. Guo, and J. Ming. 2019. "Jekyll and Hyde" is Risky: Shared-Everything Threat Mitigation in Dual-Instance Apps. In Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '19).
2. L. Zhang, Z. Yang, Y. He, M. Li, S. Yang, M. Yang, Y. Zhang, and Z. Qian. 2019. App in the Middle: Demystify Application Virtualization in Android and its Security Threats. In Abstracts of the 2019 SIGMETRICS/Performance Joint International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS '19).
3. Dai, D., Li, R., Tang, J., Davanian, A., & Yin, H. (2020, June). Parallel Space Traveling: A Security Analysis of App-Level Virtualization in Android. In Proceedings of the 25th ACM Symposium on Access Control Models and Technologies (pp. 25-32).
4. T. Luo, C. Zheng, Z. Xu, and X. Ouyang. (2017). Anti-Plugin: Don't let your app play as an Android plugin. Proceedings of Blackhat Asia.

Anti-Virtualization Mechanisms

Màscara


Virtual App 1.1
Virtual App 1.N
Virtual Environment 1
Virtual App N.1
Virtual App N.N
Virtual Environment N
App 1
App N
Android OS Environment

Android Add-On

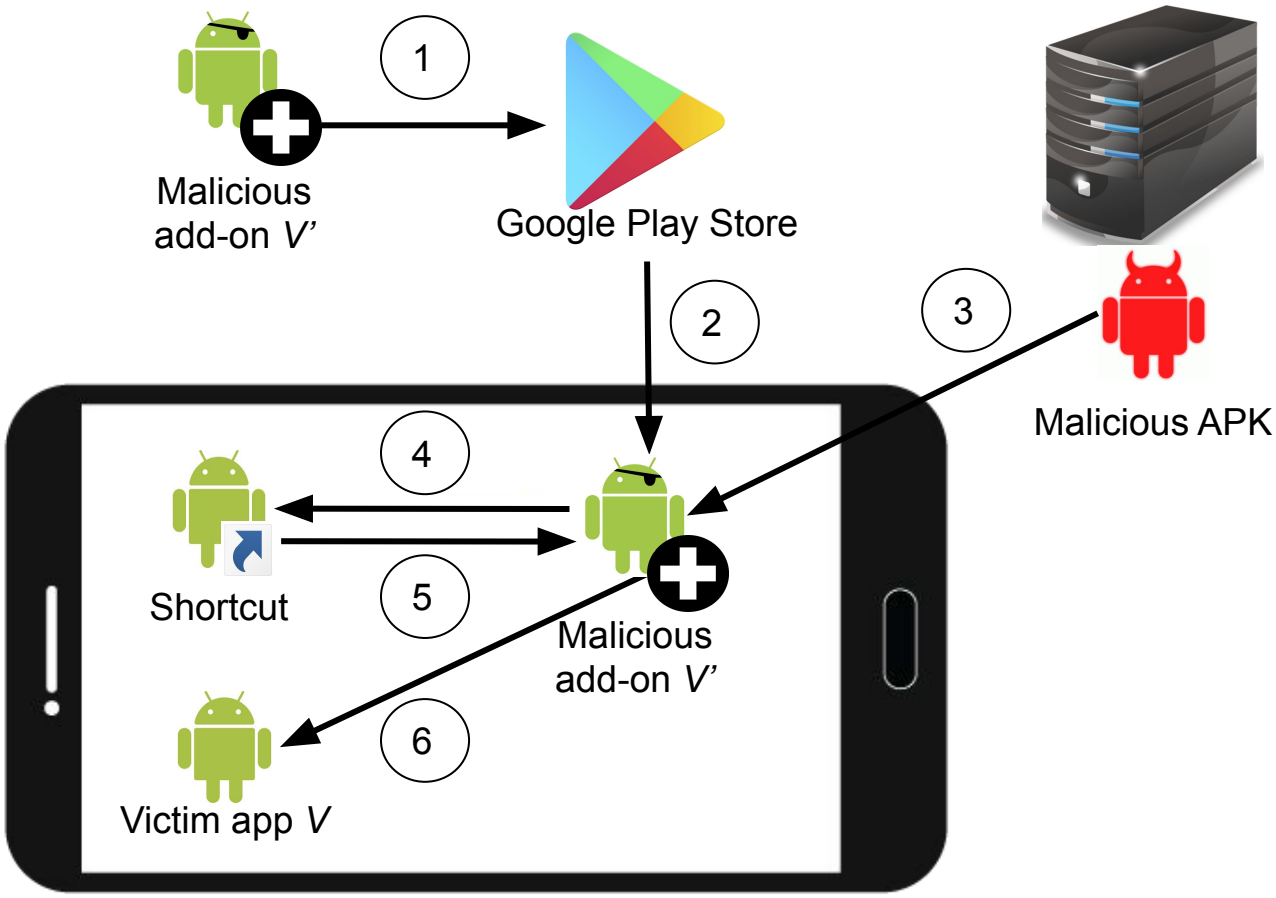


Locus map

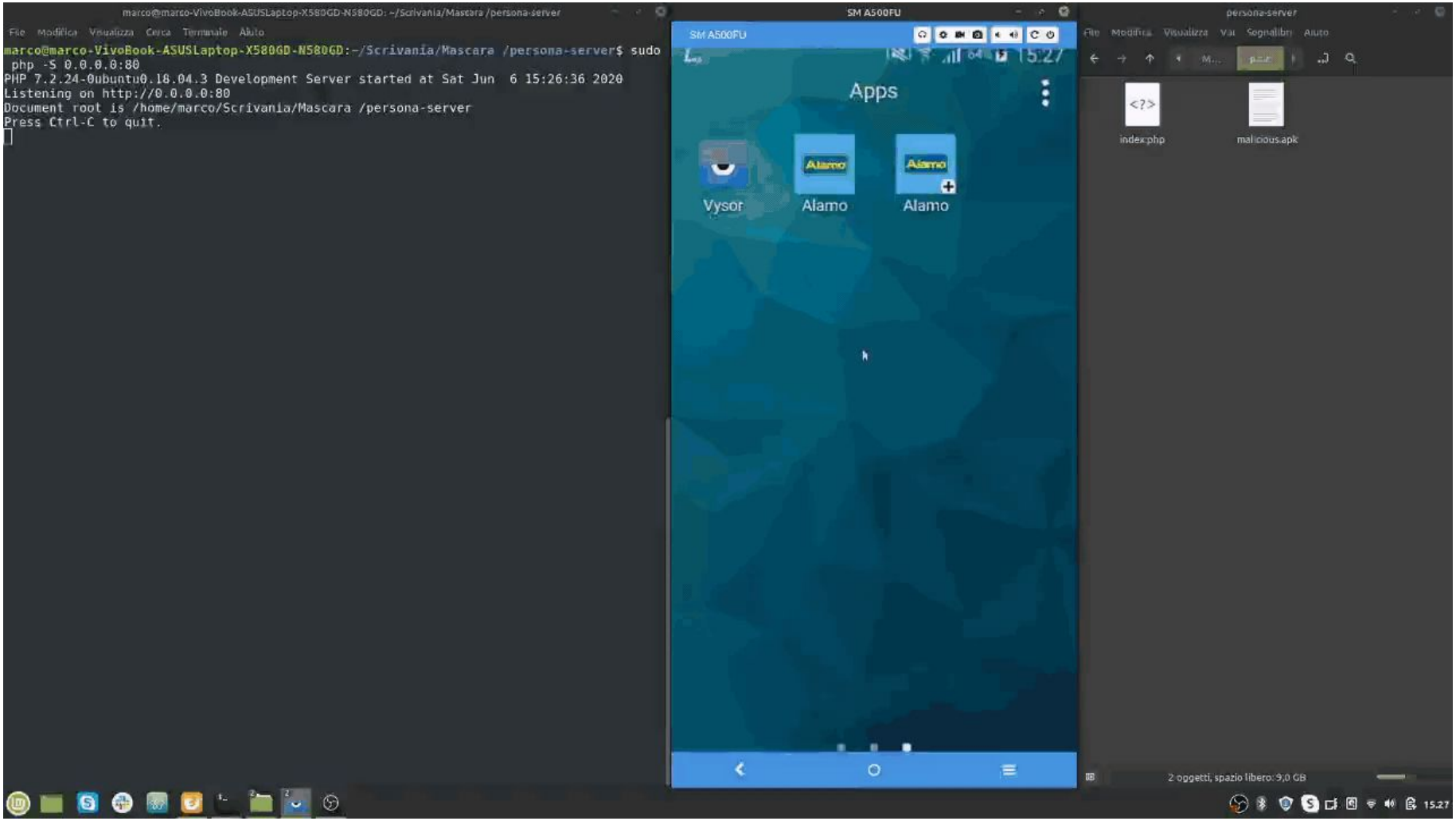
BRouter Offline Navigation

Geocaching4Locus

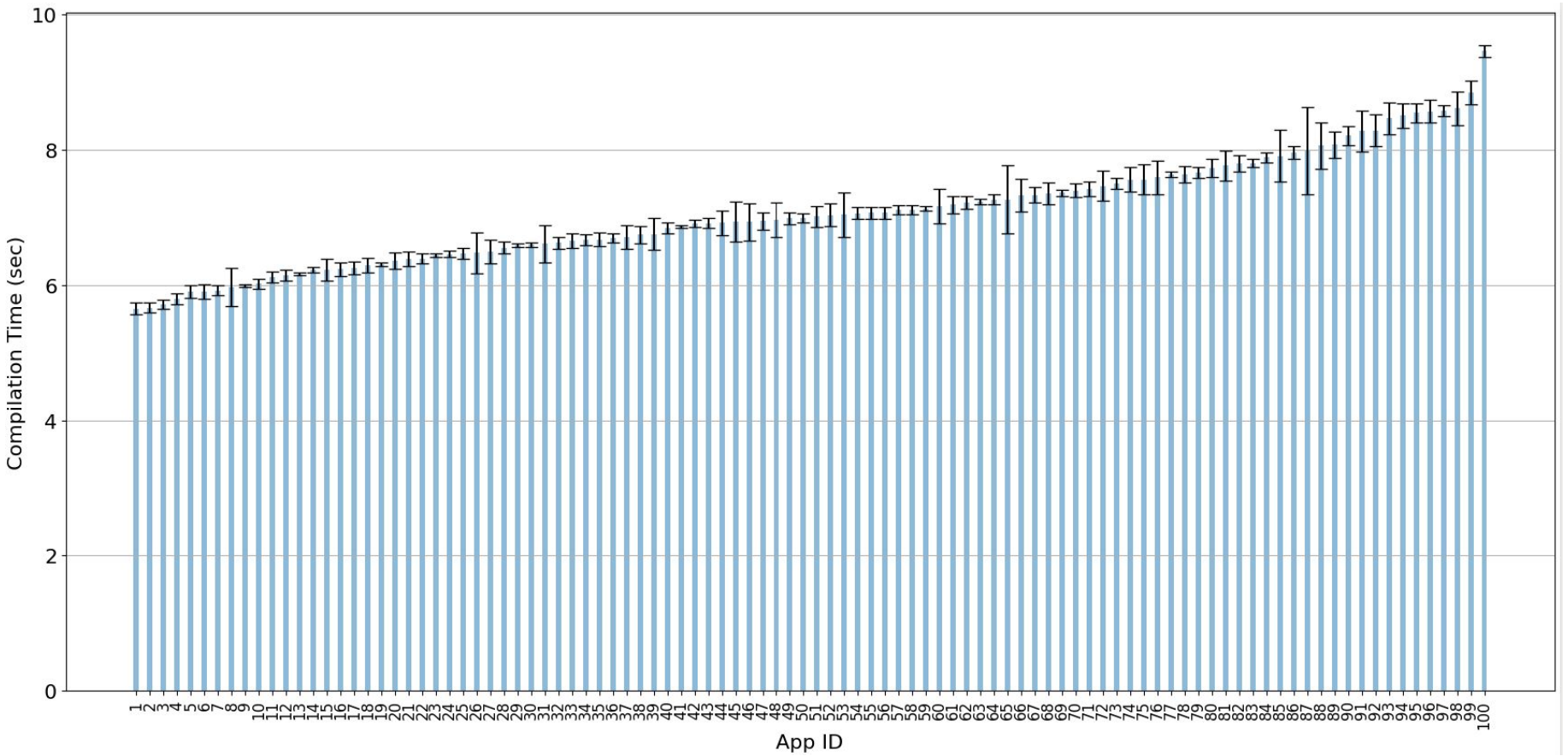
Màscara Workflow



Màscara Demo Against Alamo App



Màscara Evaluation

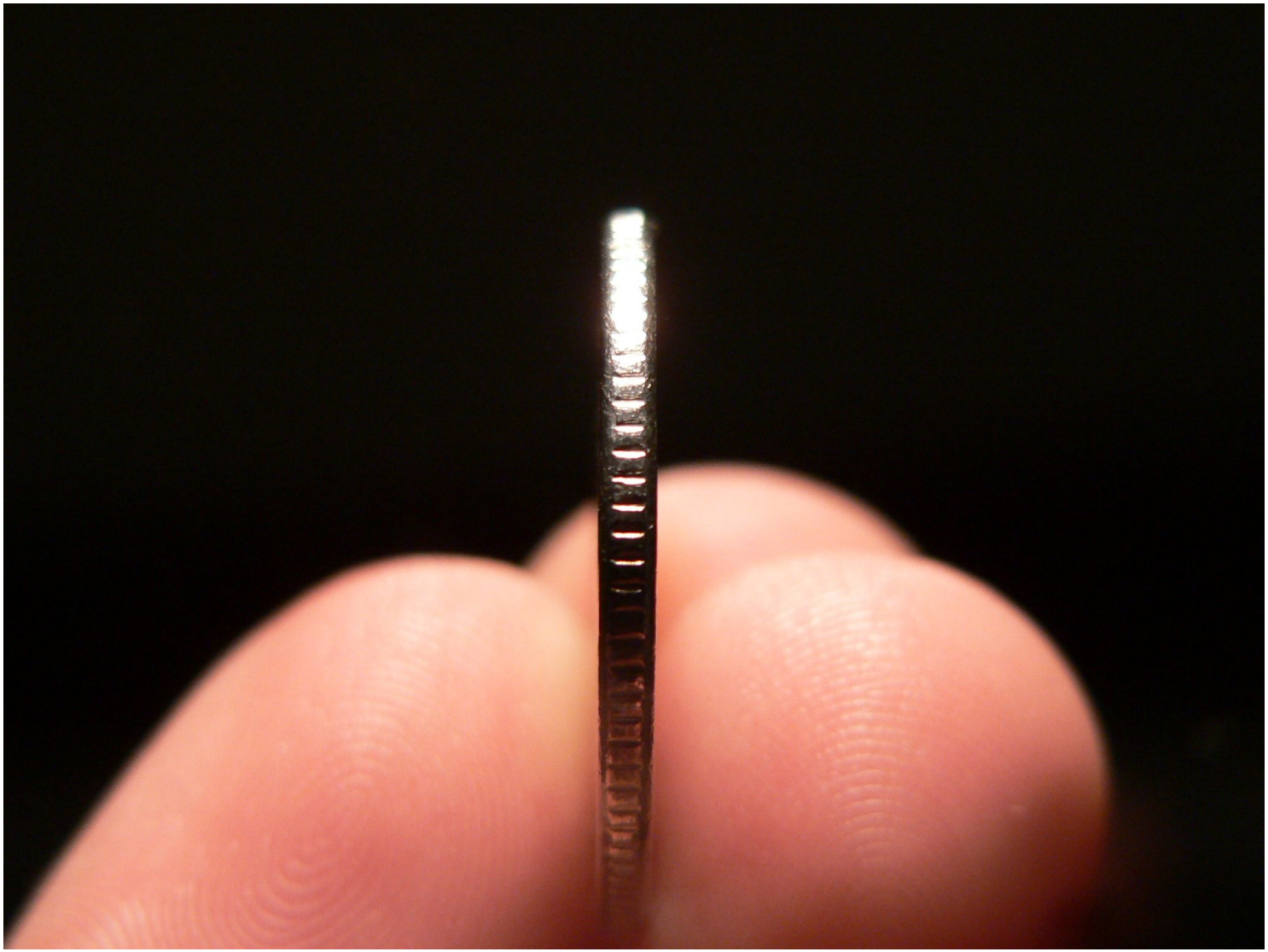


Check out the paper and the GitHub repo!

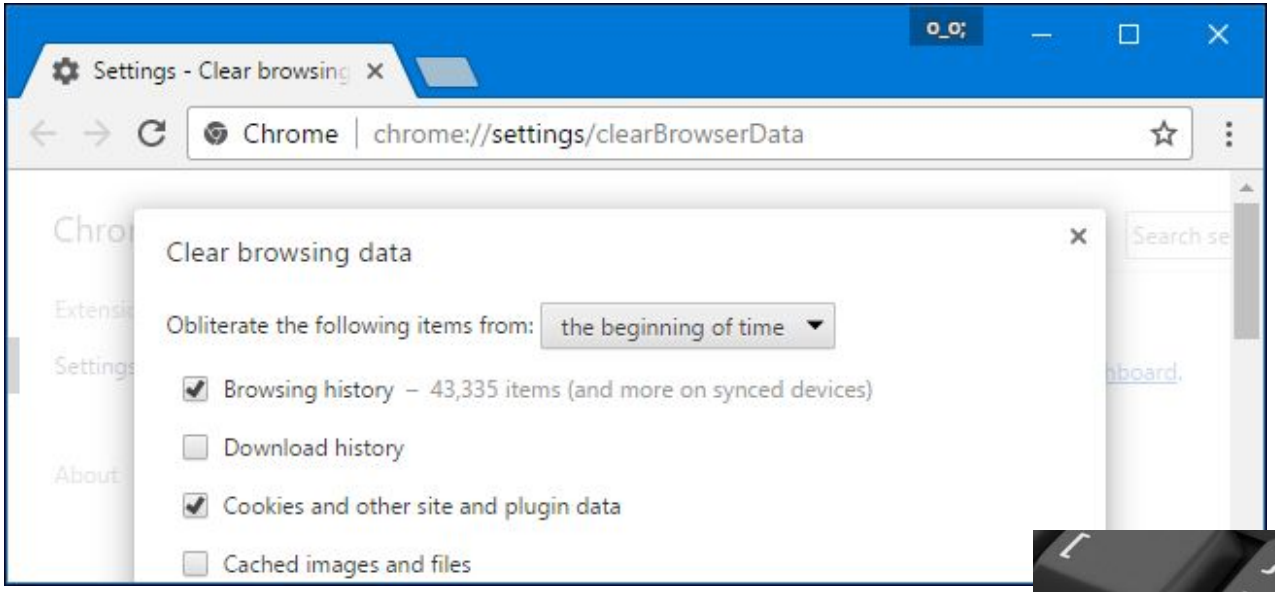
https://arxiv.org/pdf/2010.10639

https://github.com/SPRITZ-Research-Group/Mascara

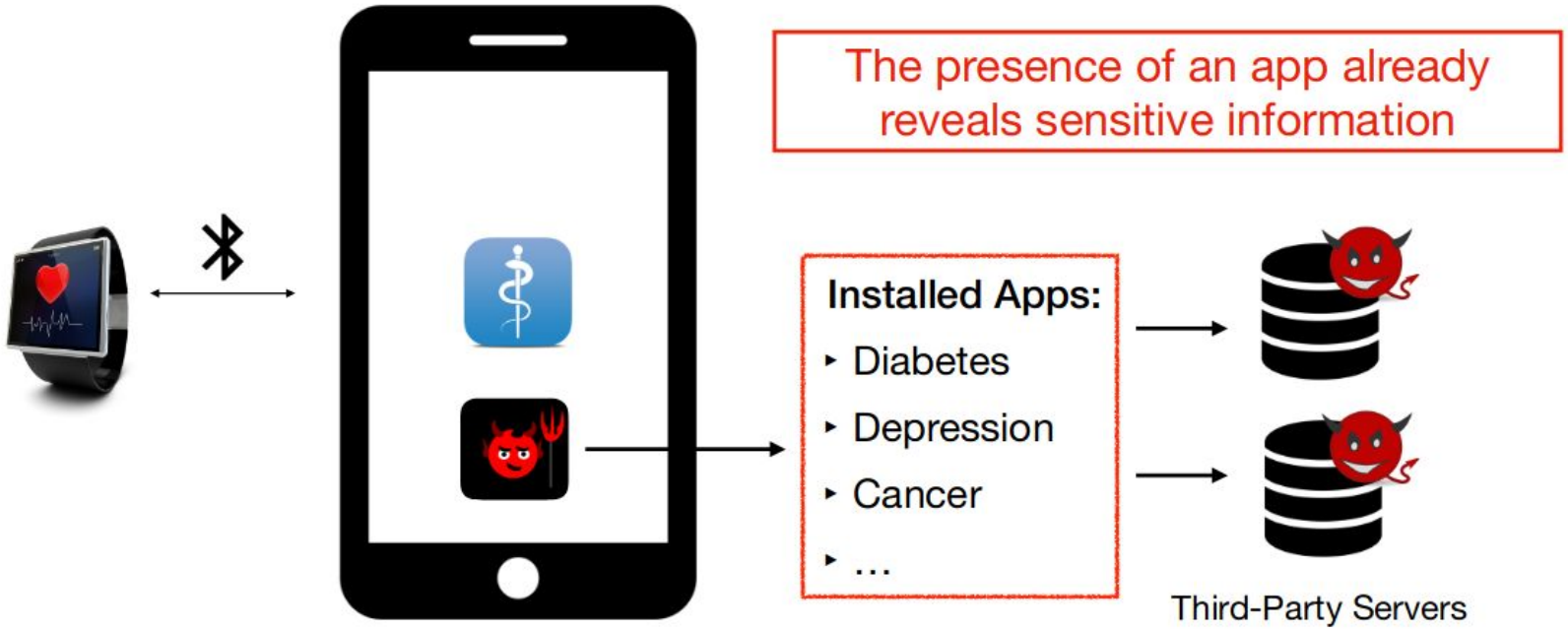
The Other Side of the Virtualization Technique



User Profiling



Background


The presence of an app already reveals sensitive information
Installed Apps:
Diabetes
Depression
Cancer
...
Third-Party Servers

Aims

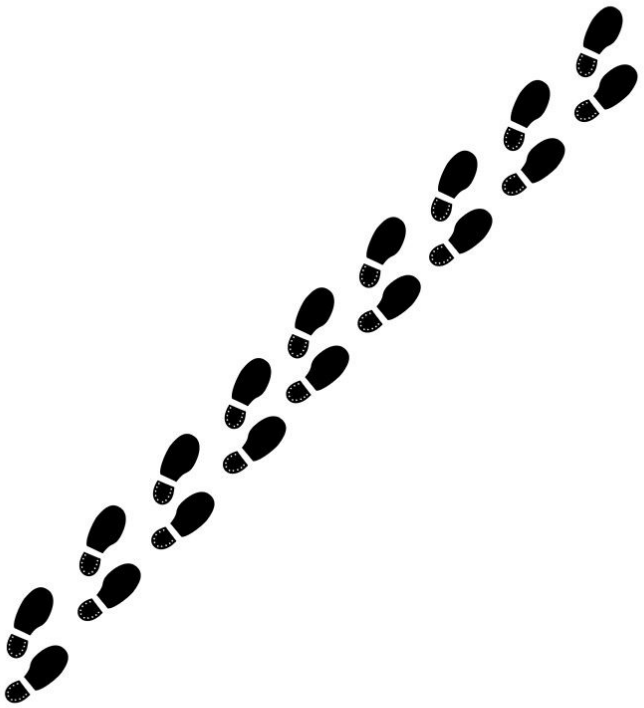
Fingerprintability of apps

Apps' interest in fingerprinting other apps

HMA

Our solution (HideMyApp)

Fingerprintability of Apps



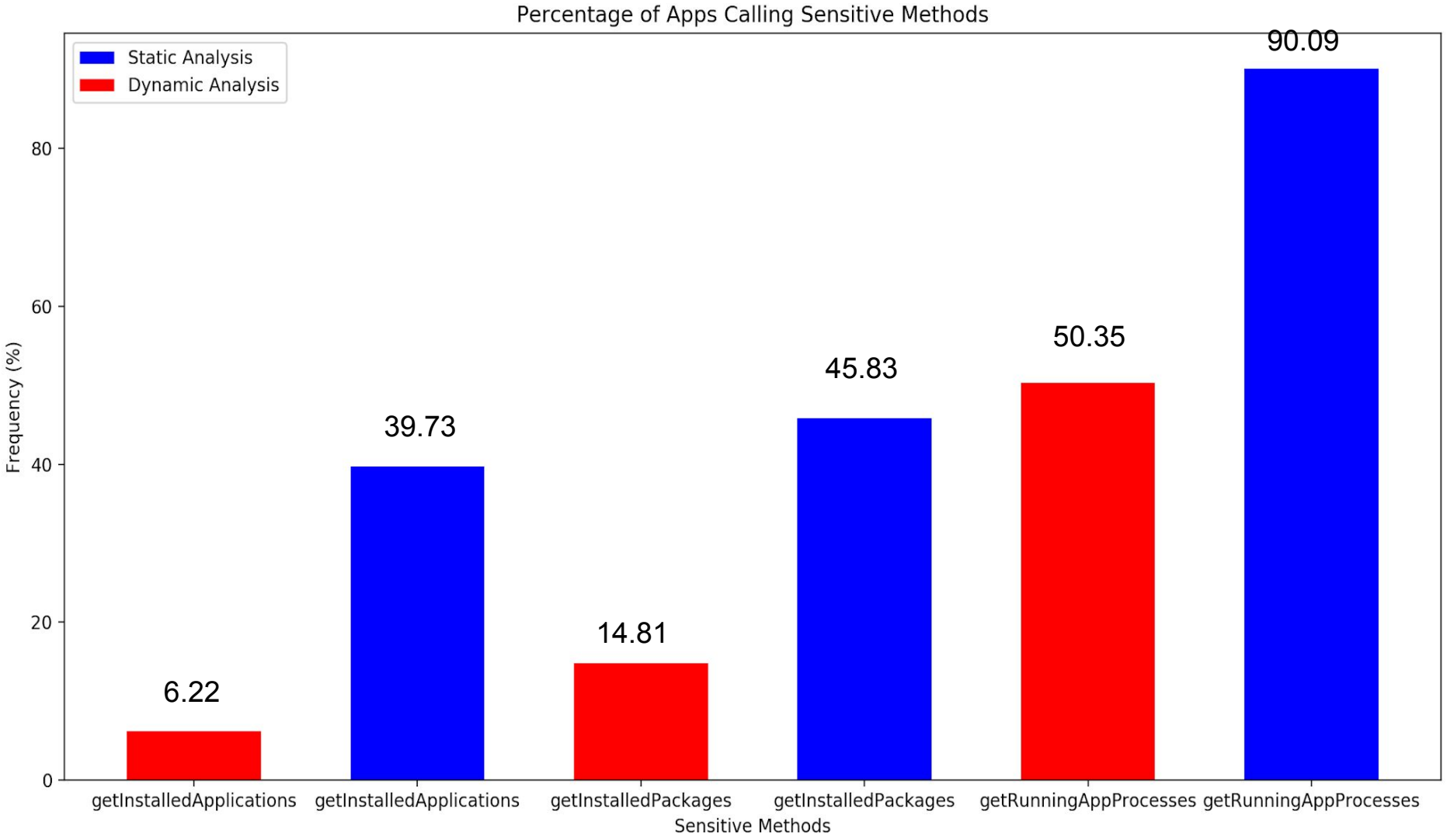
Android API Framework

File system

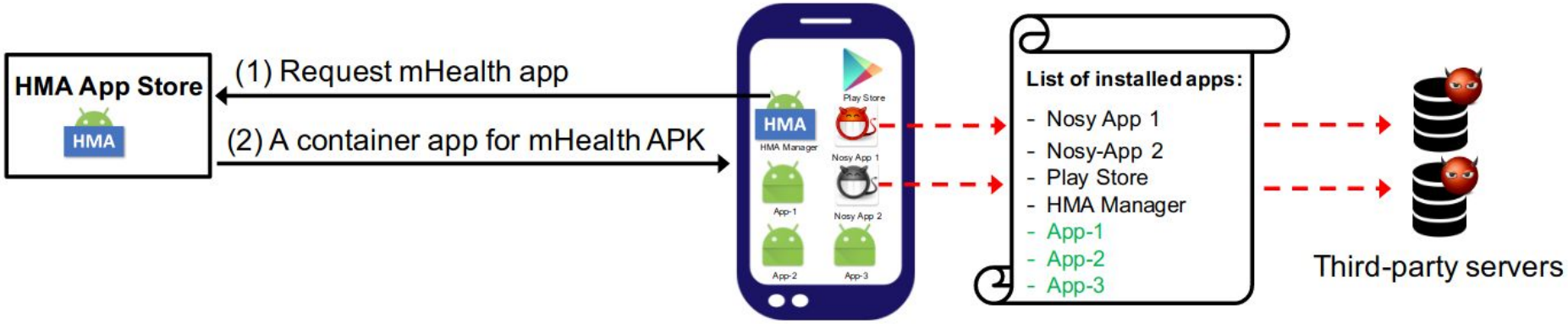
Running processes

System events

Apps Interest in Fingerprinting Other Apps



Design of HideMyApp



Demo!

Check out the paper and the GitHub repo!

A. Pham, I. Dacosta, E. Losiouk, J. Stephan, K. Huguenin and J.P. Hubaux, “HideMyApp: Hiding the Presence of Sensitive Apps on Android”, in Proceedings of 28th USENIX Security Symposium (USENIX Security 19)

https://github.com/ldsec/HideMyApp