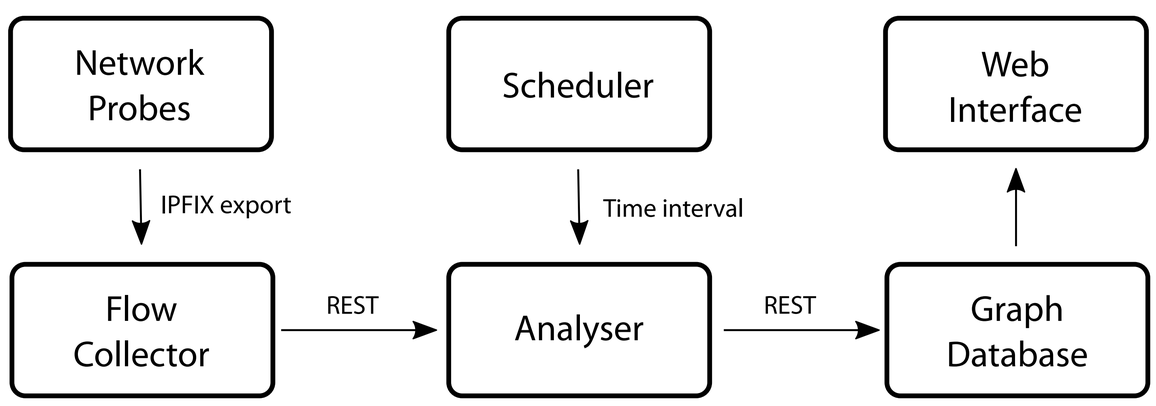
Passive OS Fingerprinting Prototype Demonstration

Martin Laštovička, Daniel Filakovský

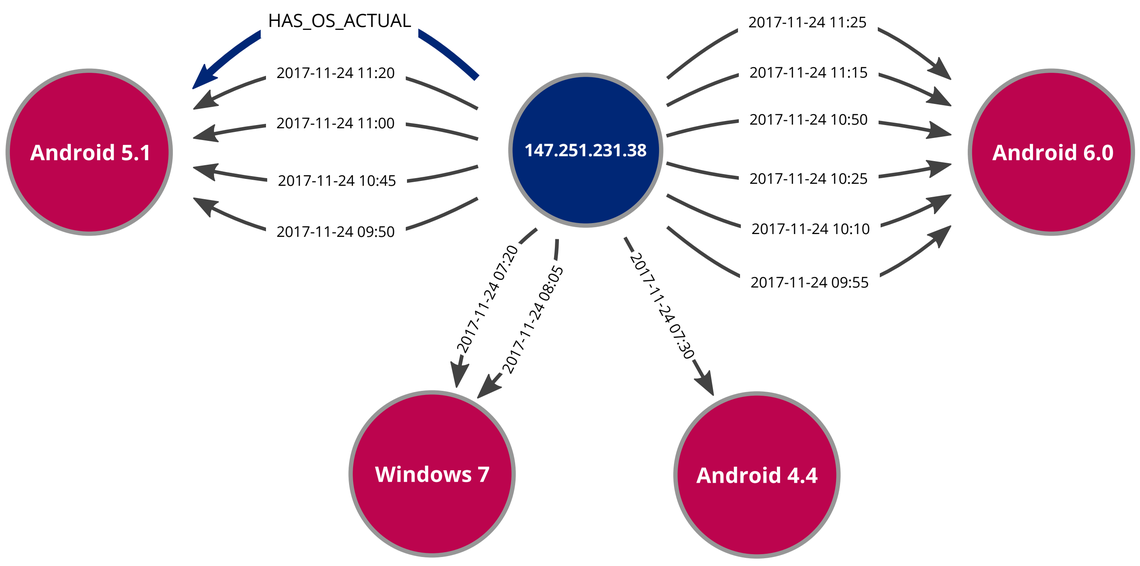
Institute of Computer Science, Masaryk University, Brno, Czech Republic
Faculty of Informatics, Masaryk University, Brno, Czech Republic
lastovicka@ics.muni.cz, filakovsky@mail.muni.cz

Operating system identification of communicating devices plays an important role in network protection. However, current networks are large and change often which implies the need for a system that will be able to monitor the network continuously and handle changes in identified operating systems. We propose an architecture of an OS fingerprinting system based on passive network monitoring and a graph-based data model to store and present information about operating systems in the network. We implemented the proposed architecture and tested it on the backbone network of Masaryk University. Our results suggest that it is suitable for monitoring a large network with tens of thousands of actively communicating devices.

System Architecture



Database Record Structure



Host – element in the network. Has one attribute corresponding to its IP address for identification during OS detection.

Operating System – specific version of OS with name attribute filled by our hierarchy format [1] - *OS name, Major version, Minor version*.

Has_OS_Actual – the last discovered relationship of *Host* to *OS*. Carries time attribute to check when the last calculation was triggered. One *Host* node can have at most one adjacent *Has_OS_Actual* edge.

Has_OS_History – edges to track the Host to OS relation in time. Every time OS is detected for a host, its current *Has_OS_Actual* edge is replaced by *Has_OS_History* with the same timestamp attribute and a new *OS_actual* edge is created.

Graph Database

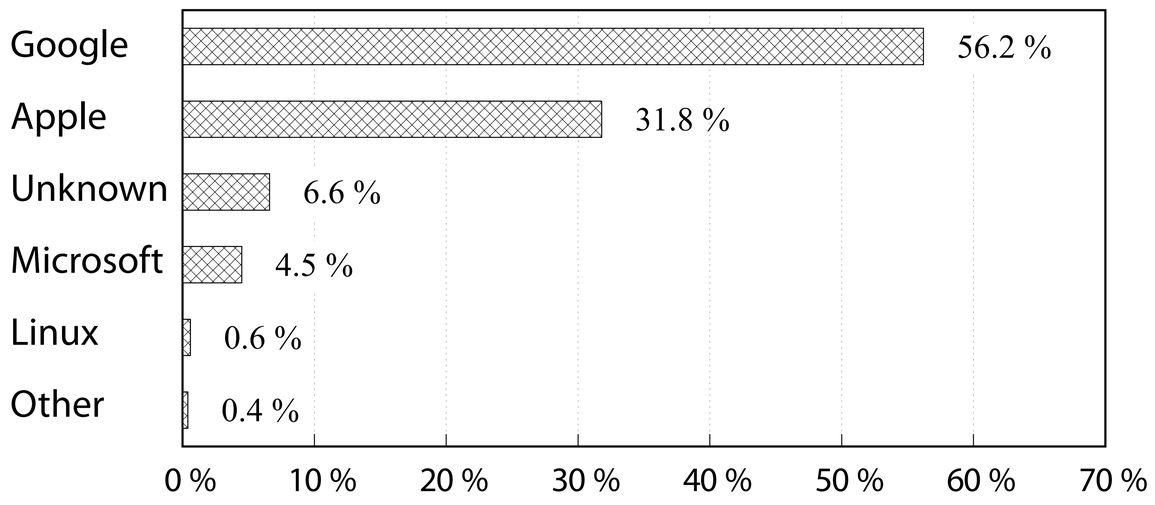
Scheduler – controlling component which invokes data analysis. It is important to schedule the analysis to match collector data storage interval so that each run of analysis has new data to process.

Analyser – main data processing unit. upon receiving data, an operating system is determined for every active IP address in the network according to the methods introduced in technical session [1].

Graph Database – information storage for further processing and visualisations.

Web Interface – a central point for data access and manipulation. Must provide big picture of operating systems in the network and individual host details

Operating System Vendor Usage Share



The market share of vendors based on results from the our measurement of our Wi-Fi network. Mobile devices such as phones and tablets dominate the dynamic network whereas traditional operating systems currently have decreasing popularity. *Unknown* means that the method could not determine the OS, *Other* category is the rest of operating systems with low market share (e.g., BlackBerry).

Source codes and testing datasets are available at:
https://github.com/CSIRT-MU/PassiveOSFingerprint

[1] Laštovička, Martin and Jirsík, Tomáš and Čeleda, Pavel and Špaček, Stanislav and Filakovský, Daniel. Passive OS Fingerprinting Methods in the Jungle of Wireless Networks. In 2018 IEEE/IFIP Network Operations and Management Symposium. Taipei, Taiwan: IEEE, 2018.

This research was supported by the Security Research Programme of the Czech Republic 2015 – 2020 (BV III / 1 VS) granted by the Ministry of the Interior of the Czech Republic under No. VI20172020070 Research of Tools for Cyber Situation Awareness and Decision Support of CSIRT Teams in the Protection of Critical Infrastructure.
Martin Laštovička is Brno Ph.D. Talent Scholarship Holder – Funded by the Brno City Municipality.

Brno **Ph.D.** Talent