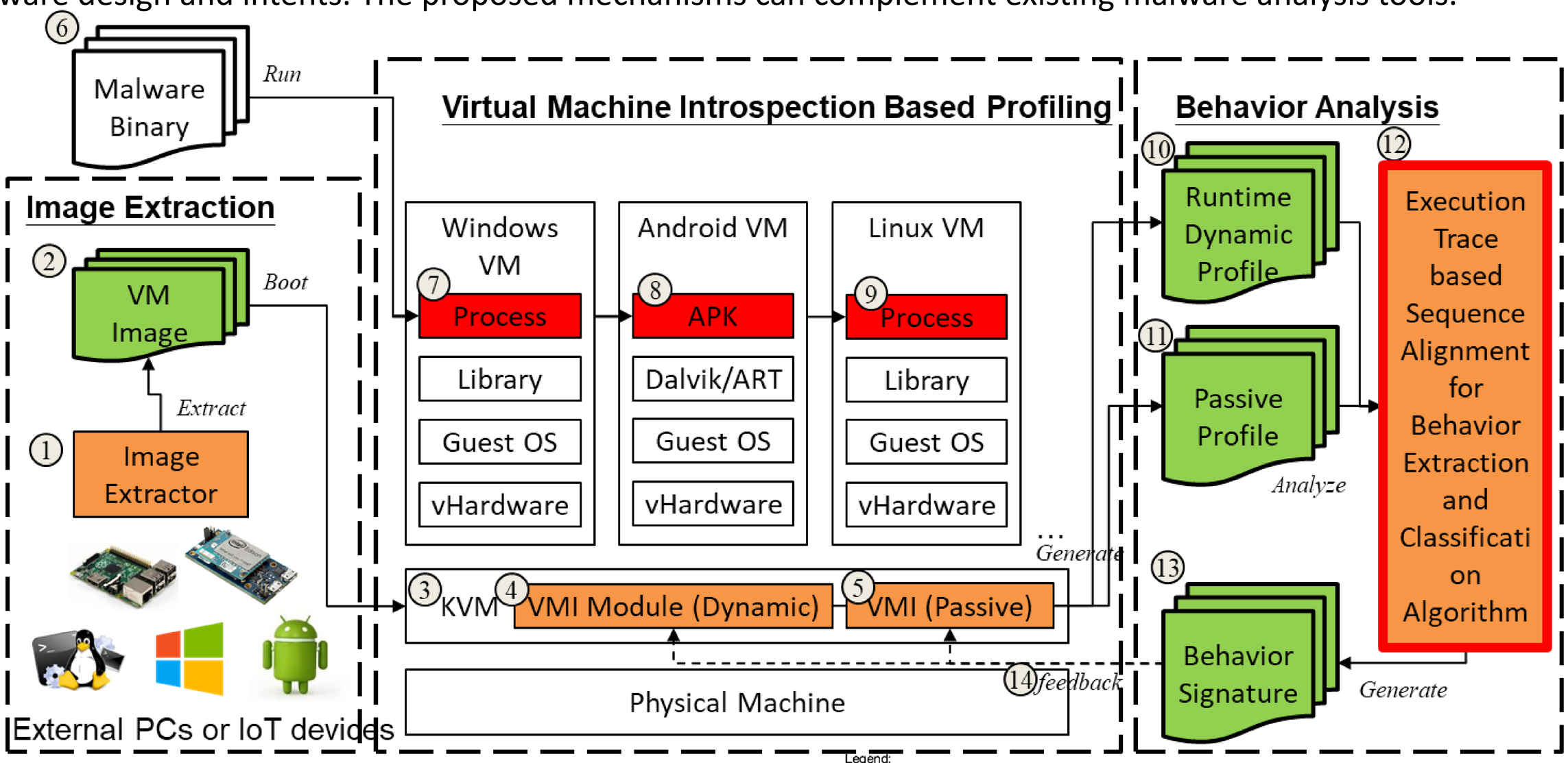
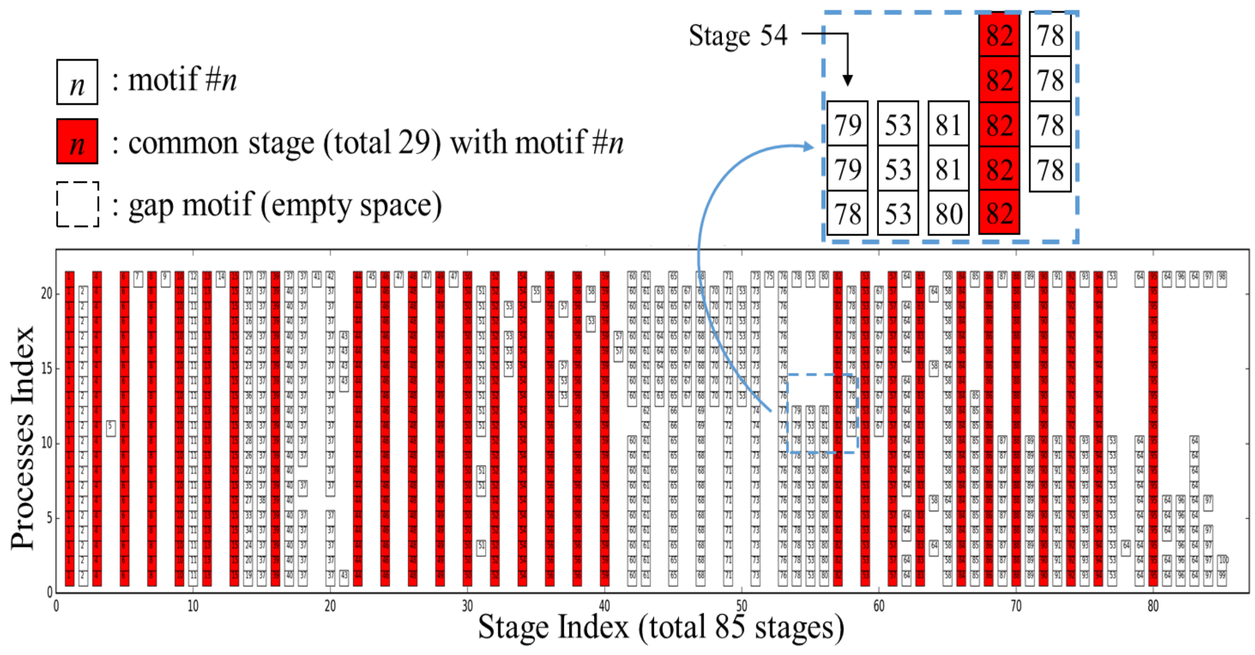
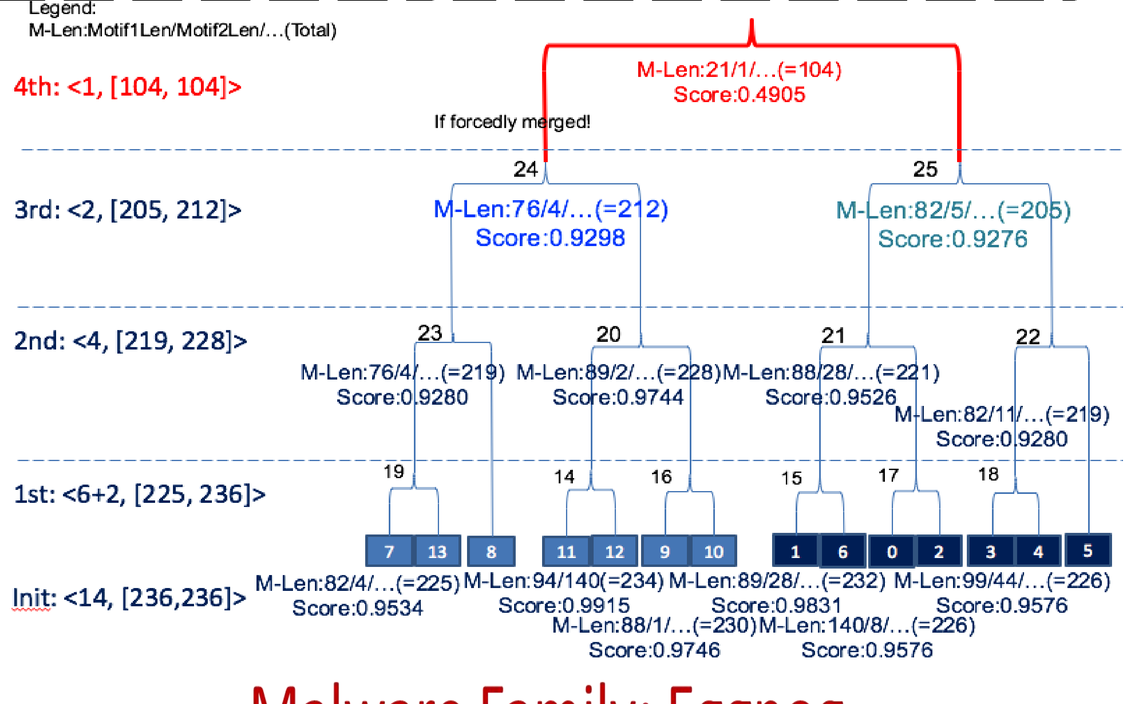
雲端與端點應用之連續資安防禦與分析系統
子計畫一:雲端應用暨IoT端點執行行為之資安分析與鑑識系統

執行單位：台灣大學資訊管理系
主持人：孫雅麗教授
計畫編號：MOST 106-2221-E-002-009

A malware family consists of a collection of variants, mostly owing to the obfuscation techniques, which may exhibit different appearance (e.g., binary, line order, code size, entropy, etc.), but they do possess common dynamic behaviors. Traditionally, malware detection lies on generating individual variants' signature and/or some ad-hoc behavior patterns. In this project, we propose a family-signature generation and detection method which focuses on common API sequence extraction from variants. We implemented an automated VMI-based high-level semantics profiling system and developed several execution sequence analysis algorithms to extract and generate malware family signature. We further implemented an automated tool to generate the lifecycle of the system-state-change activities of a malware family. The goal is to visualize how the harmful operations of a malware family undergoes, provide in-depth behavior investigation, and simplify malware analysis process in forensics to uncover malware design and intents. The proposed mechanisms can complement existing malware analysis tools.







Goals of Behavior Group Analysis

- Identify and classify extracted behavior group signatures which are used for malicious activity detection at runtime to achieve more effective and efficient detection of new variants of known malwares as well as unknown ones than conventional methods.
- Implement an Automated Dynamic Malware Profiling and Analysis System.

Malware Family: Eggnog