Contribution ID: **216** Type: **Paper presentation**

Improving iOS Sandbox Profile Decompilation Accuracy

Thursday 18 September 2025 16:00 (15 minutes)

Mobile devices have become ubiquitous, with Apple owning more than 25% of the market. One method by which iOS ensures the security of its apps is through sandboxing. This mechanism is implemented as a set of rules compiled into binary files that lie inside the OS firmware that isolate applications within controlled environments to prevent unauthorized operations. The contents of these profiles are not made public by Apple. Thus, security engineers require third-party tools to decompile and then visualize the contents of the profiles mentioned above.

This paper presents a validation framework for iOS sandbox profile decompilers, specifically targeting the SandBlaster tool. Our approach represents sandbox profiles as dependency graphs and compares decompiled profiles with reference implementations compiled from Sandbox Profile Language (SBPL) representations using SandScout. The validator employs a graph-based comparison algorithm that identifies discrepancies in the operation rules and filter paths between the representations of the binary and SBPL profiles.

We evaluated our framework in iOS versions 7-10, analyzing both individual profiles and bundled profile collections. The results demonstrate perfect accuracy (100\% precision and recall) for iOS 7-8 profiles, while revealing systematic errors in iOS 9-10 decompilation, including missing or confused filters, incorrect string literals, and missing inter-process communication operations. Path-level accuracy ranges from 90-100% for iOS 9 and 75-100% for iOS 10, indicating version-specific degradation in decompilation quality. Additionally, we identified and resolved a critical performance bottleneck in SandBlaster's node matching algorithm, reducing decompilation time from over 7 hours to under 5 minutes for iOS 10 bundled profiles through algorithmic optimization from $\Theta(n^2)$ to $\Theta(n)$ complexity.

Author: DUȚU, Teodor-Ștefan (National Unviersity of Science and Technology Politehnica Bucharest)

Co-authors: DEACONESCU, Răzvan (University Politehnica of Bucharest); ALEXANDRESCU, Andrei (Nvidia Corporation)

Presenter: DUȚU, Teodor-Ștefan (National Unviersity of Science and Technology Politehnica Bucharest)

Session Classification: Security & Resilience in Cyber-Physical Systems

Track Classification: Security & Resilience in Cyber-Physical Systems