ATLAS Kobold

Online Platform for Binary Analysis

Modern mobile smartphones are powerful devices running full fledged operating systems. Features are enhanced by using rich applications typically located in an online store, easy to install and use.

A rich set of applications provided extended functionality for the user but also increase the likelyhood of security risks, such as leaking of private date, money loss or reputation damage.

Modern mobile OSes add security enhancements to reduce risks. Our aim is to provide developers and sofware vendors with solutions to assess the security of their products.

Kobold

Kobold is a framework for studying flaws in system services in Apple iOS. Kobold is open source software part of an ecosystem of solutions for assessing the security of Apple iOS. Kobold's targeting of Apple iOS is motivated by the comparatively reduced number of researcher involved in iOS, the requirement for binary analysis and reversing (most code is proprietary) and the security features presented by Apple to strenghen iOS.

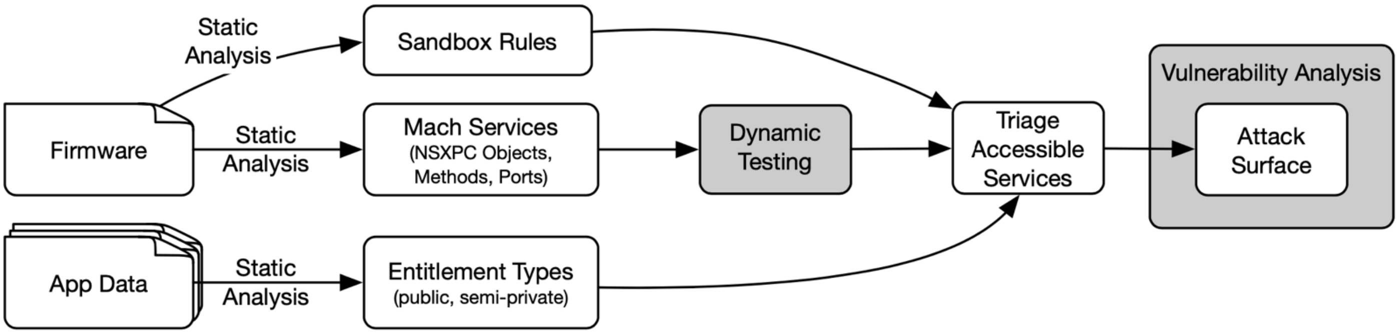
Kobold is used to investigate the IPC interface in Apple iOS: NSXPC.

Main features of ATLAS Kobold

- Apple iOS
- targets IPC (NSXPC)
- fuzzes methods in services
- static + dynamic analysis
- identifies flaws in system services

https://github.com/malus-security/kobold

Copyright (c) 2020 ATLAS



How Kobold Works

Kobold leverages two key insights. First, the standardized IPC interfaces (e.g., NSXPC) contain predictable patterns in compiled code that are identifiable via static analysis. Second, error messages returned by unauthorized attempts to access IPC services can provide a model of the iOS IPC access control policy. Using these insights, Kobold provides a pattern-based, static binary program analysis to enumerate NSXPC interfaces and then dynamically uses systematic probing to extract an approxi- mation of the access control policy encoded by conditional checks within a given service.

Kobold addresses challenges in determining which security and privacy sensitive NSXPC methods are accessible to third-party applications through a combination of static analysis and dynamic testing, Kobold's static analysis helps to enumerate the attack sur face, while the dynamic analysis allows an analyst to triage which NSXPC services are likely to contain vulnerabilities.

Kobold is divided into three tasks. First, it performs a survey of the entitlements available to third party applica- tions. Second, it enumerates the NSXPC services accessible to third party applications. Third, we evaluate the security sensitivity of accessible NSXPC services in order to highlight services likely to allow confused deputy attacks.

The first and second tasks are automated. We developed scripts and integrated existing tools to extract application entitlements and enumerate NSXPC services. The third task uses fuzzing and manual analysis to investigate NSXPC service methods that are accessible and security sensitive.

Kobold is known to work on Apple iOS 9, 10 and 11. It has lead to the release of 3 CVEs by Apple.

About ATLAS

The ATLAS project ("Hub inovativ pentru tehnologii avansate de securitate cibernetică") plans on improving research and collaboration performances in the cyber-security domain, by addressing themes of high interest: security of applications, operating systems, IoT and cloud.

The ATLAS project is financed through a research grant from the Romanian Ministry of Research and Innovation, CCCDI - UEFISCDI, project no. PN-III-P1-1.2-PCCDI-2017-0272, in the PNCDI III programme.