Apple / iOS Access Control

SMD, May 29, 2023

Agenda

Overview of iOS

Access Control

iOS Access Control

iOS

popular mobile OS solution

iOS1 - 2007

yearly release

iOS16 - 2022

custom hardware, custom OS, security features

AppStore

Security in iOS

https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf

app sandboxing (MAC)

privacy settings

access control

app signing, app encryption

SEP, SepOS

TouchID, FaceID

iOS Components

firmware image

OTA updates

kernel cache

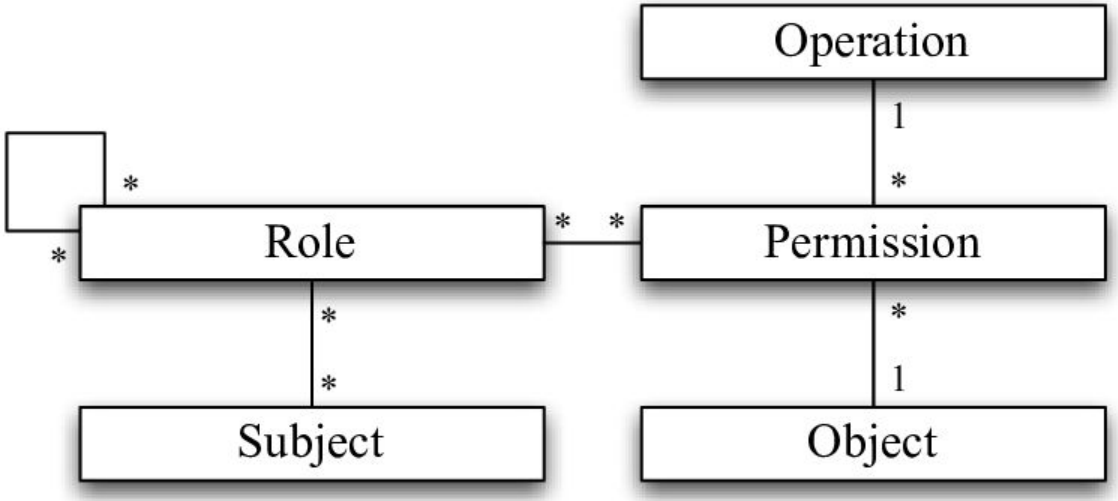
- extensions

dyld shared caches

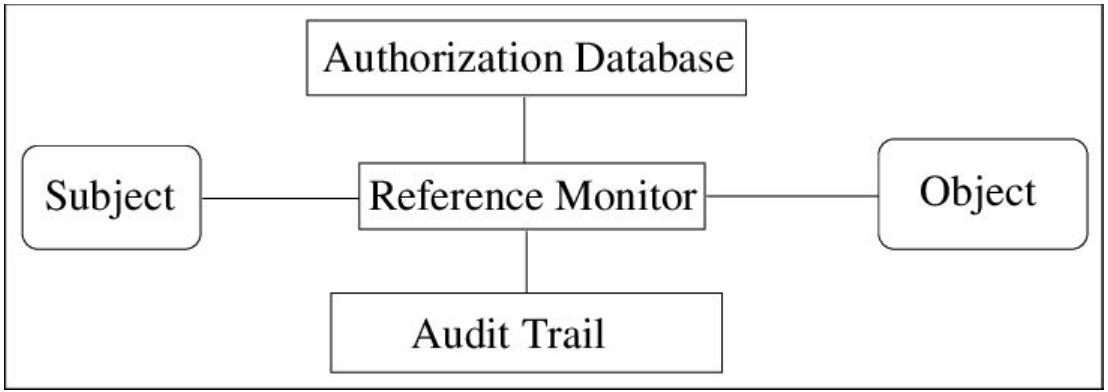
system applications

system configurations

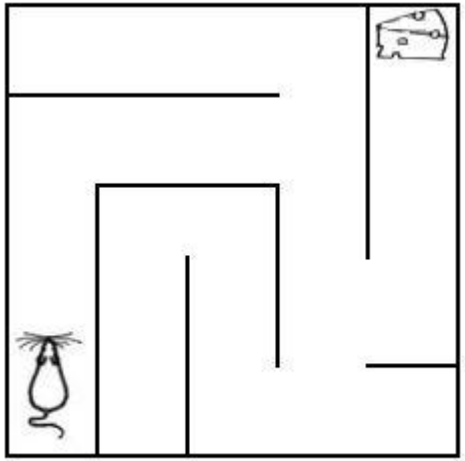
Subject-Object Model

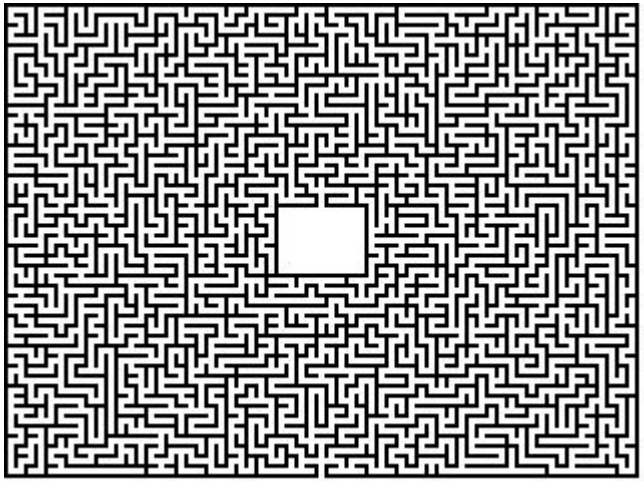


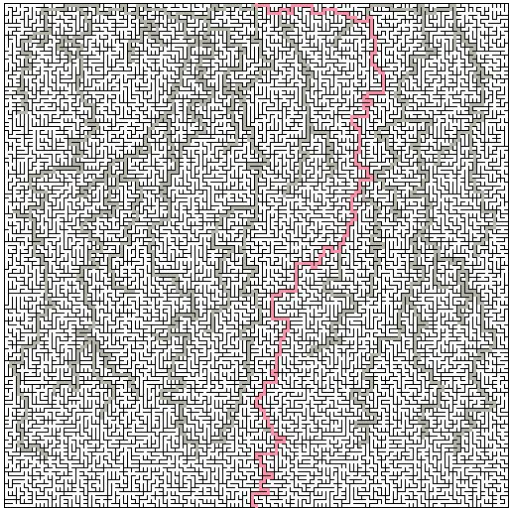
Reference Monitor

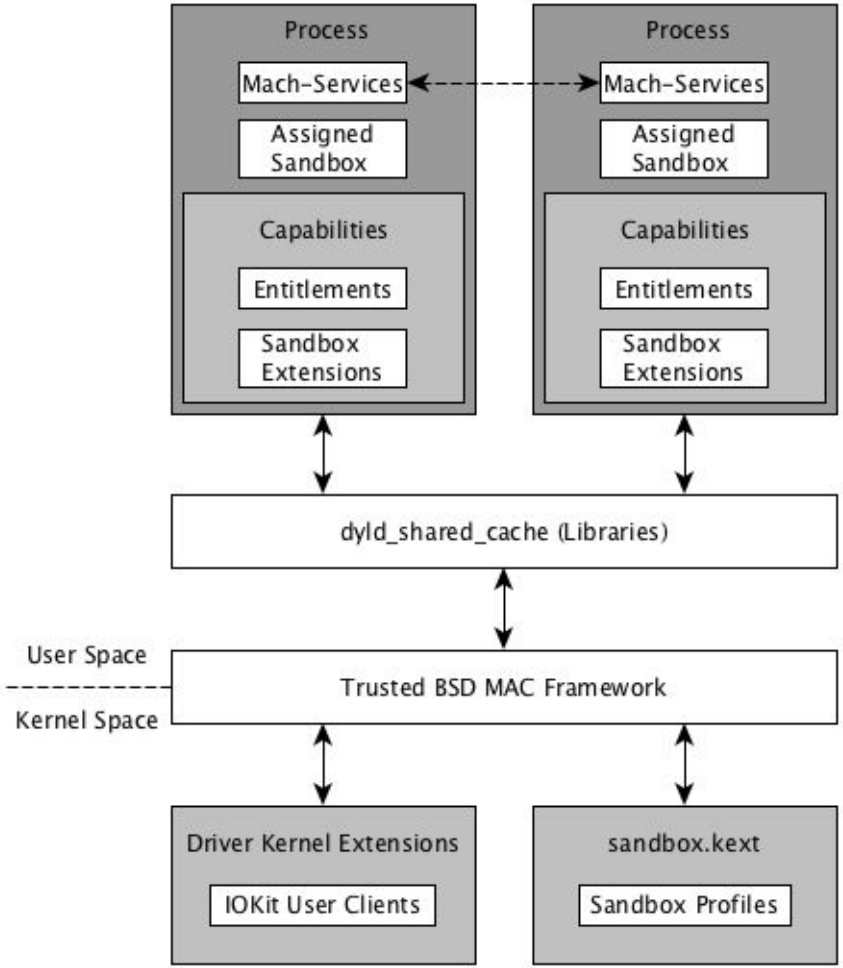


The Problem with Access Control Policies





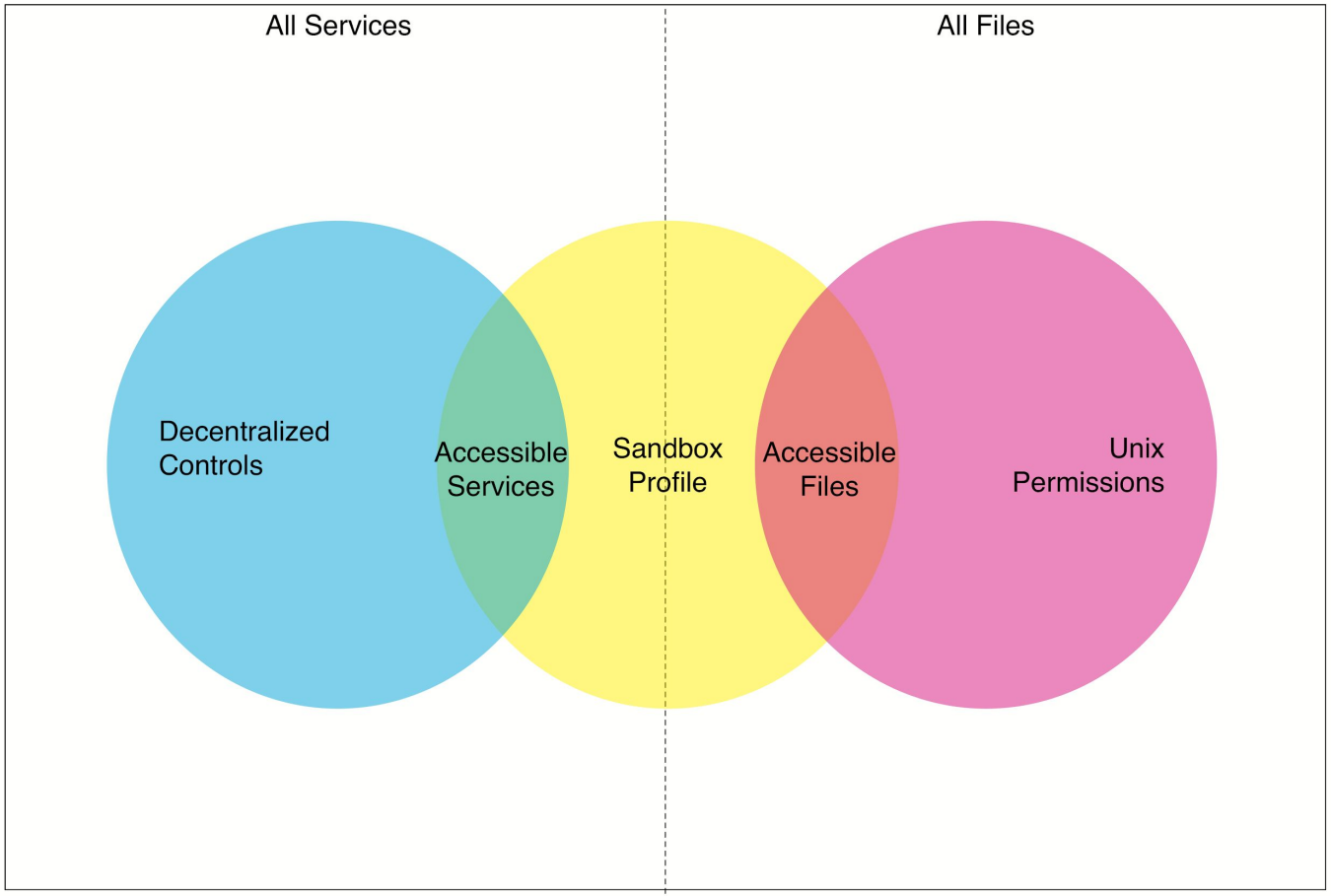



Process
Mach-Services
Assigned Sandbox
Capabilities
Entitlements
Sandbox Extensions
Process
Mach-Services
Assigned Sandbox
Capabilities
Entitlements
Sandbox Extensions
dyld_shared_cache (Libraries)
User Space
Kernel Space
Trusted BSD MAC Framework
Driver Kernel Extensions
IOKit User Clients
sandbox.kext
Sandbox Profiles

3 Major Access Control Policies

- Terminology
  - A policy determines whether a subject can perform an action on an object.
  - iOS policies make decisions based on attributes of the subject and object
- Sandbox Profiles
  - Action: System calls
  - Process runs unsandboxed or is assigned one of many predefined sandbox profiles
  - Sandbox profile rules can be conditioned on attributes of subject and object
  - Almost Mandatory Access Control (MAC)
- Unix File Permissions
  - Object: File
  - Traditional read, write, execute Discretionary Access Control (DAC)
  - Subject is a user, but concrete subject is a process
- Decentralized Access Checks
  - Object: Service (e.g., getting user's GPS coordinates)
  - Conditional logic inside of system processes that provide services

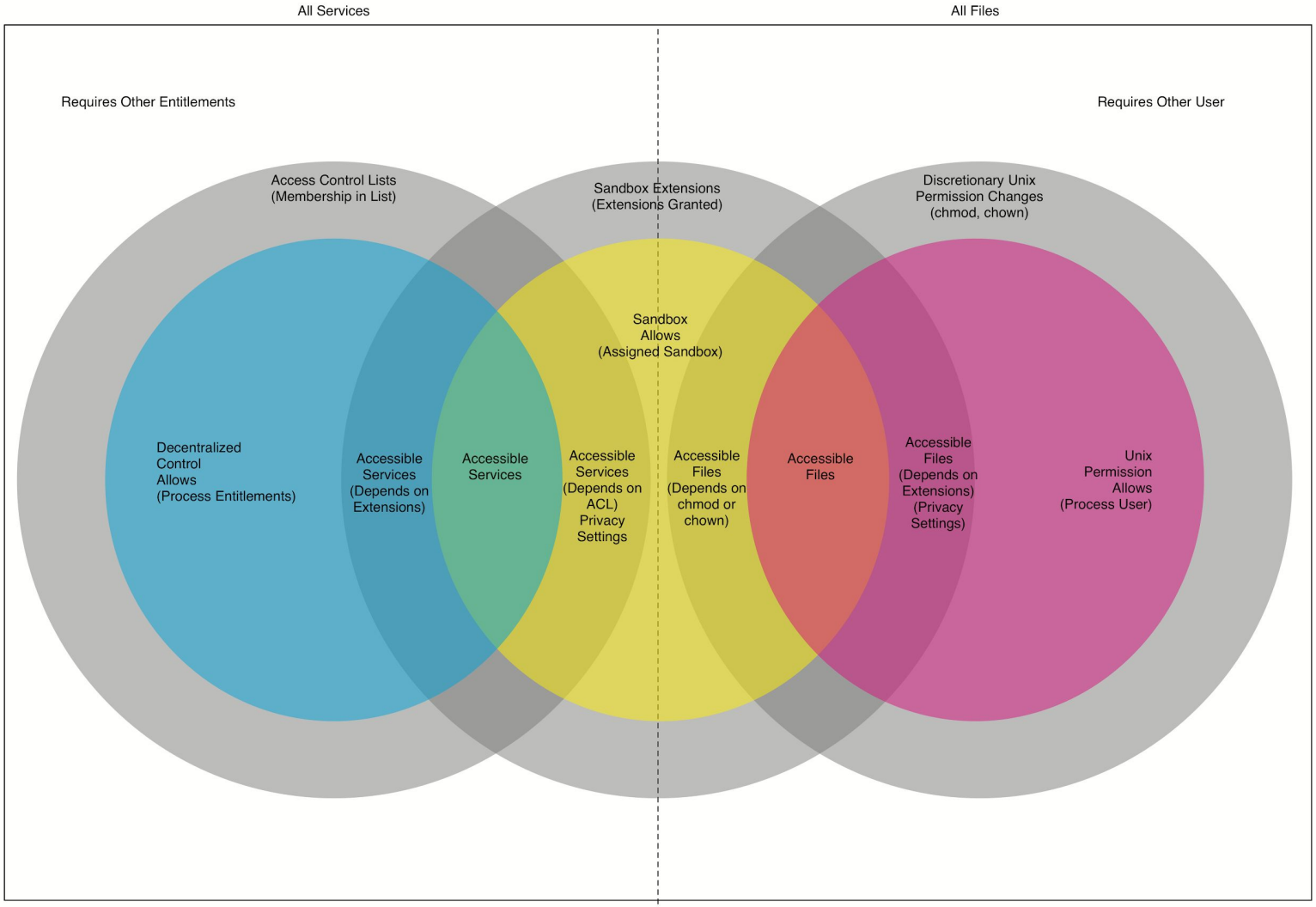
Protection Domain of a Process



Mandatory vs. Discretionary

Each policy type in iOS can be dynamically modified

- Privacy Settings
  - Sandbox Extensions
  - Access Control Lists
- Modifying file permissions or ownership


All Services
All Files
Requires Other Entitlements
Requires Other User
Access Control Lists
(Membership in List)
Sandbox Extensions
(Extensions Granted)
Discretionary Unix
Permission Changes
(chmod, chown)
Sandbox
Allows
(Assigned Sandbox)
Decentralized
Control
Allows
(Process Entitlements)
Accessible
Services
(Depends on
Extensions)
Accessible
Services
Accessible
Services
(Depends on
ACL)
Privacy
Settings
Accessible
Files
(Depends on
chmod or
chown)
Accessible
Files
Accessible
Files
(Depends on
Extensions)
(Privacy
Settings)
Unix
Permission
Allows
(Process User)

Jailbreaking Bypasses All of These Policies

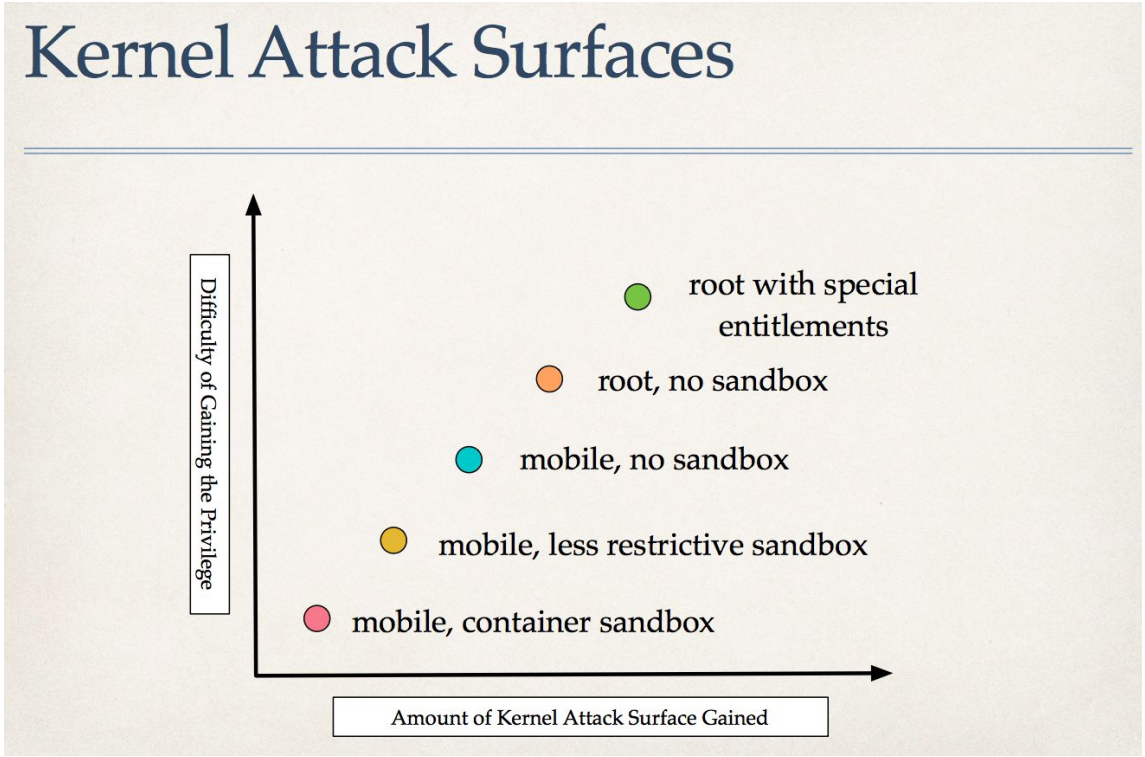
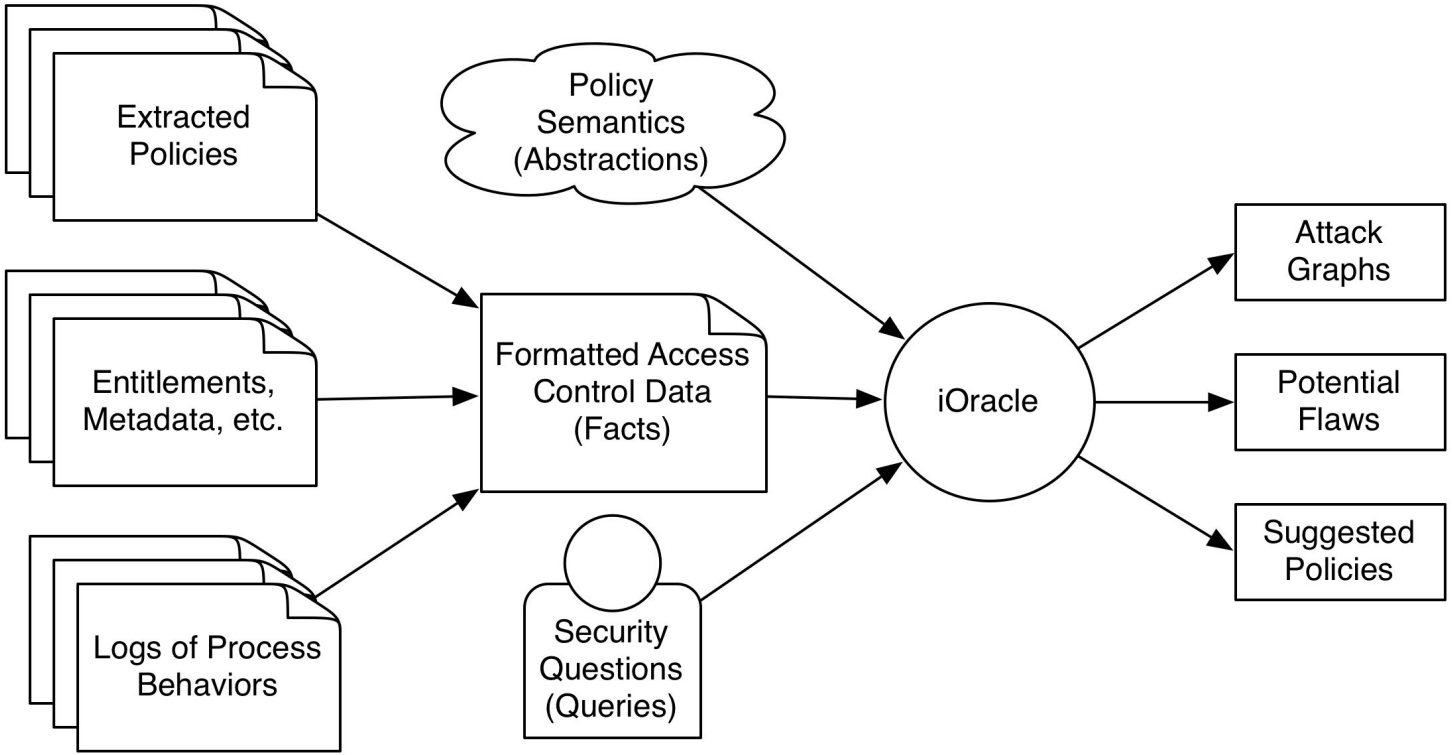


Image from: https://www.blackhat.com/docs/us-16/materials/us-16-Wang-Pangu-9-Internals.pdf

iOracle Overview

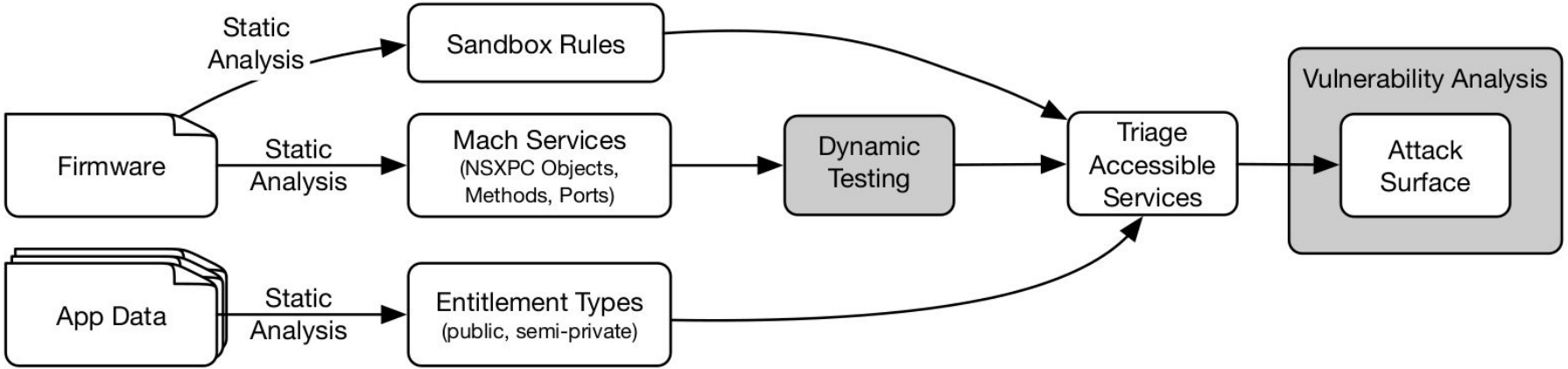


iOracle

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

iOracle is a fairly complex framework that combines the output of multiple static and dynamic analysis tools into Prolog facts which are used along with Prolog rules to answer queries about various qualities of iOS access control and runtime context.

Kobold: Overview



Kobold

`Evaluating Decentralized Access Control for Remote NSXPC Methods on iOS`

Kobold is a framework to study NSXPC-based system services using a combination of static and dynamic analysis. Using Kobold, we discovered multiple NSXPC services with confused deputy vulnerabilities and daemon crashes.

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

Findings

https://www.google.com/search?channel=fs&client=ubuntu&q=cve+ios+deshotels+deaconescu

submitted to Apple (responsible disclosure)

published as CVEs

CVE-2018-4446: https://support.apple.com/en-us/HT209340

CVE-2019-8698: https://support.apple.com/en-us/HT210346

Malus Security

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

https://discord.gg/m3gjuyHYw9