Computer Science
& Engineering
Department

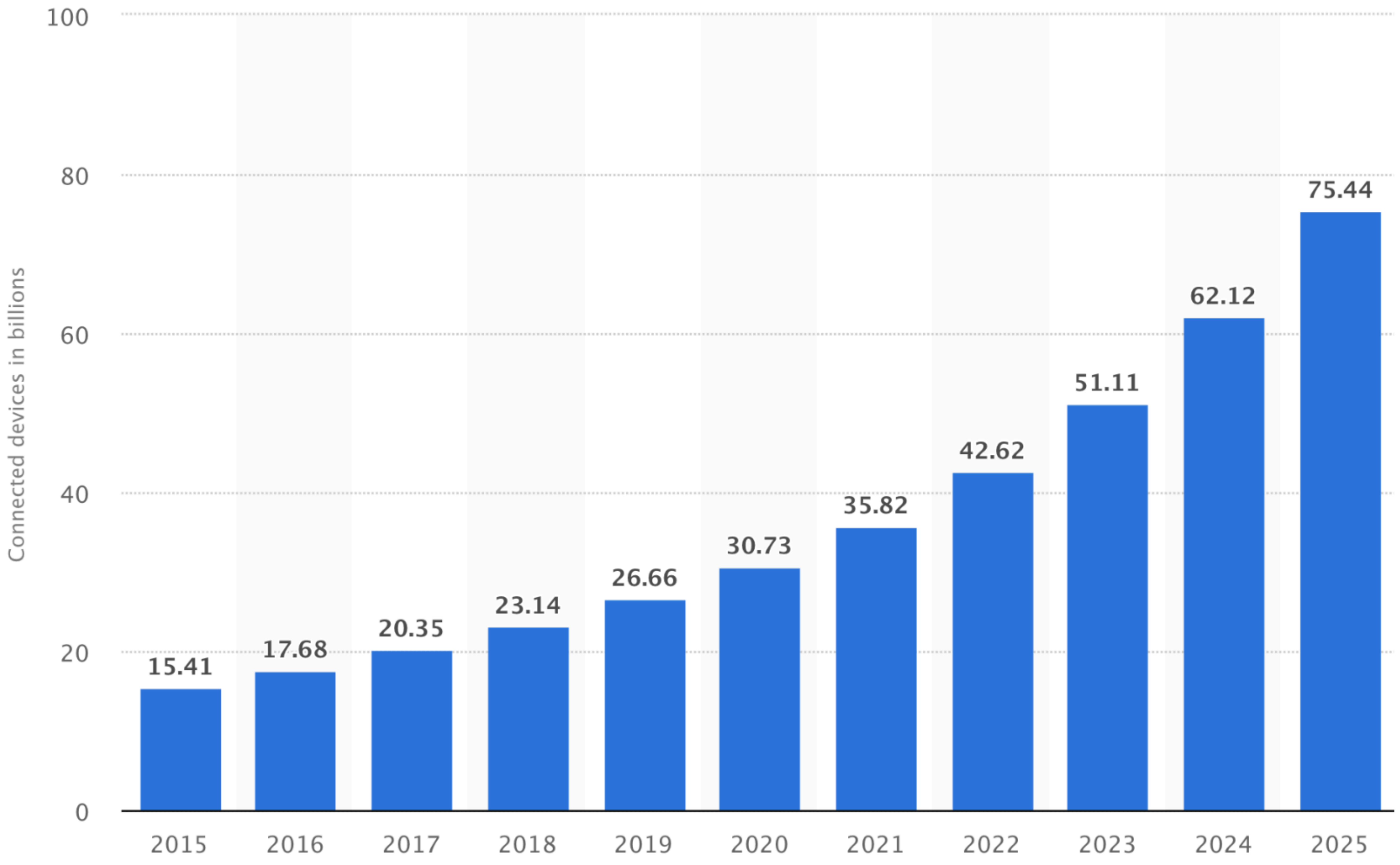
Improving the Security of Embedded Operating Systems

drd. ing. Costin Carabaș
Advisor: Prof. Dr. Ing. Nicolae Țăpuș
16 December 2021

University Politehnica of Bucharest

Context

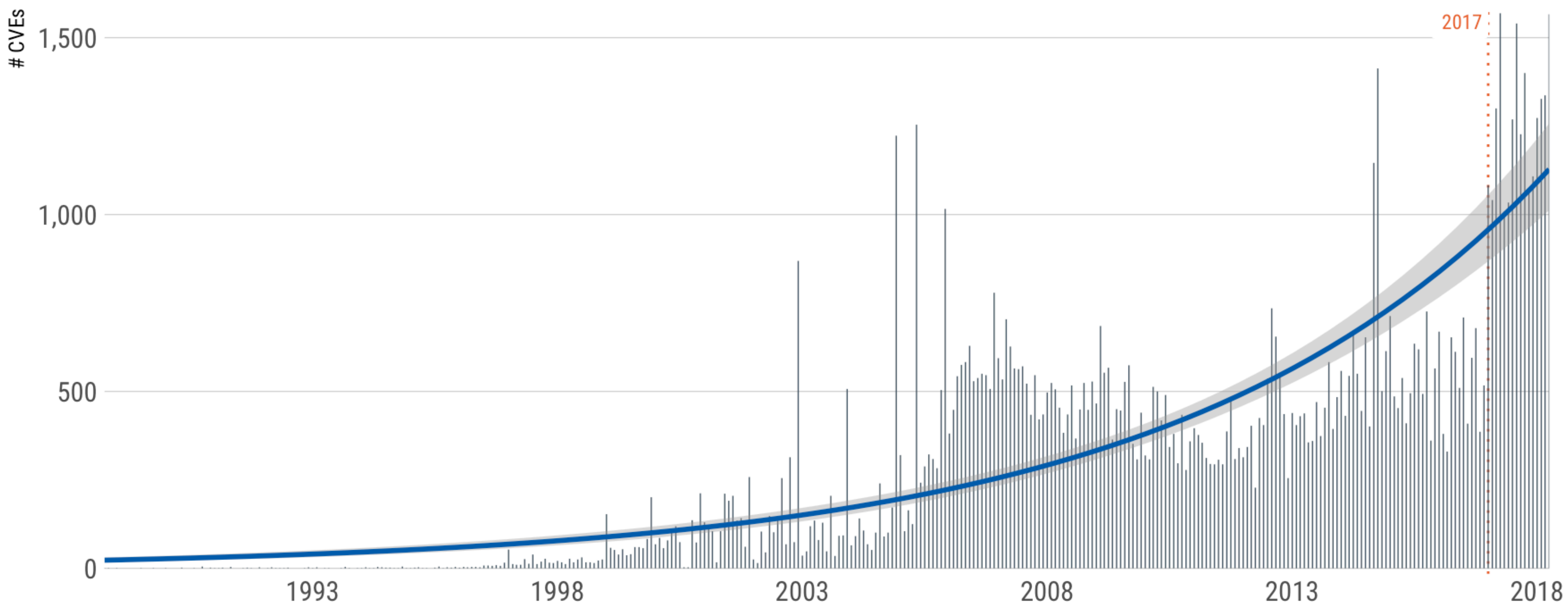
- Rapid evolution of embedded devices
- Rapid evolution of software solutions



https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Context

- Rapid evolution of embedded devices
- Rapid evolution of software solutions
- Rapid evolution of CVE (Common Vulnerabilities and Exposures)
- Security — critical component



CVE's per year/month

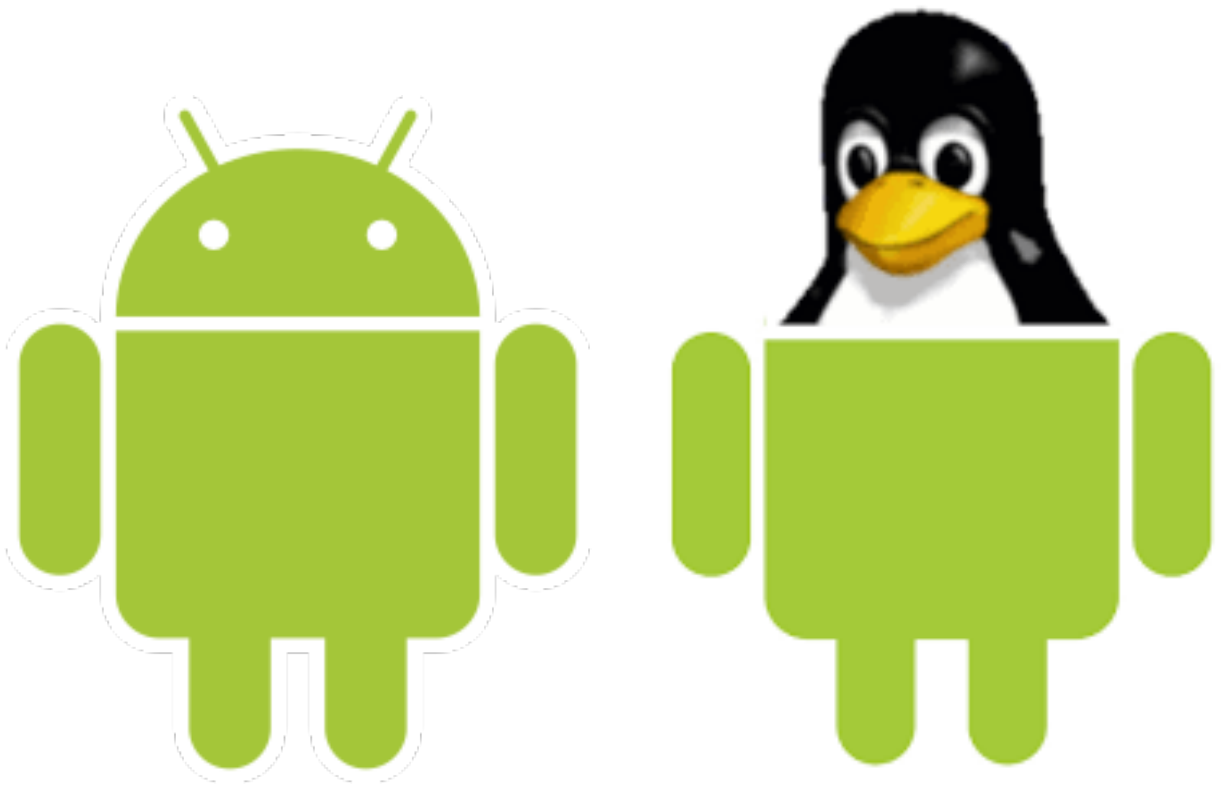
Data compiled from MITRE, NVD and Rapid7

Scope

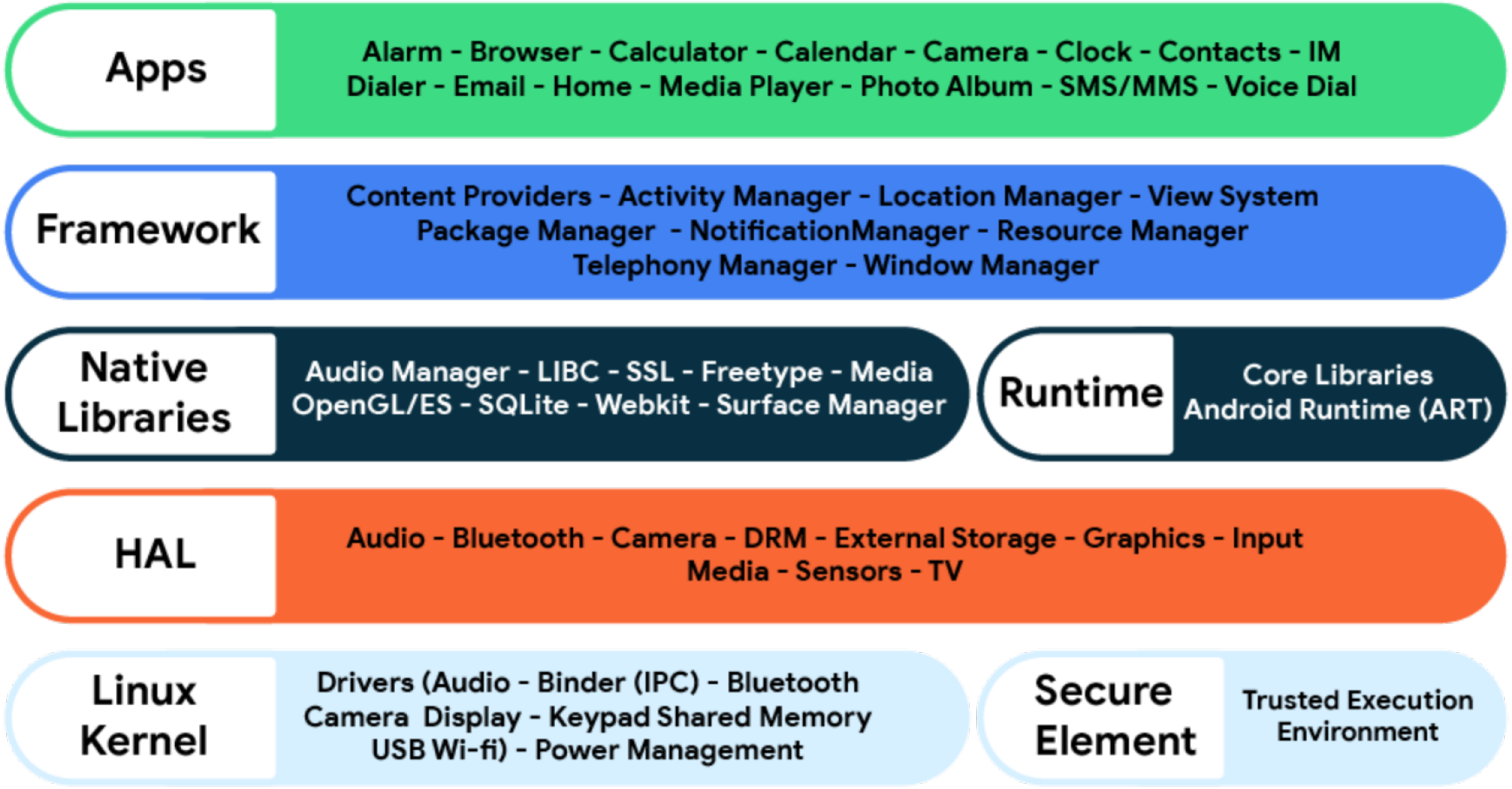
Open source

Closed source

Scope - Android



- Libraries
- Android Kernel



Apps

Alarm - Browser - Calculator - Calendar - Camera - Clock - Contacts - IM
Dialer - Email - Home - Media Player - Photo Album - SMS/MMS - Voice Dial

Framework

Content Providers - Activity Manager - Location Manager - View System
Package Manager - NotificationManager - Resource Manager
Telephony Manager - Window Manager

Native Libraries

Audio Manager - LIBC - SSL - Freetype - Media
OpenGL/ES - SQLite - Webkit - Surface Manager

Runtime

Core Libraries
Android Runtime (ART)

HAL

Audio - Bluetooth - Camera - DRM - External Storage - Graphics - Input
Media - Sensors - TV

Linux Kernel

Drivers (Audio - Binder (IPC) - Bluetooth
Camera Display - Keypad Shared Memory
USB Wi-fi) - Power Management

Secure Element

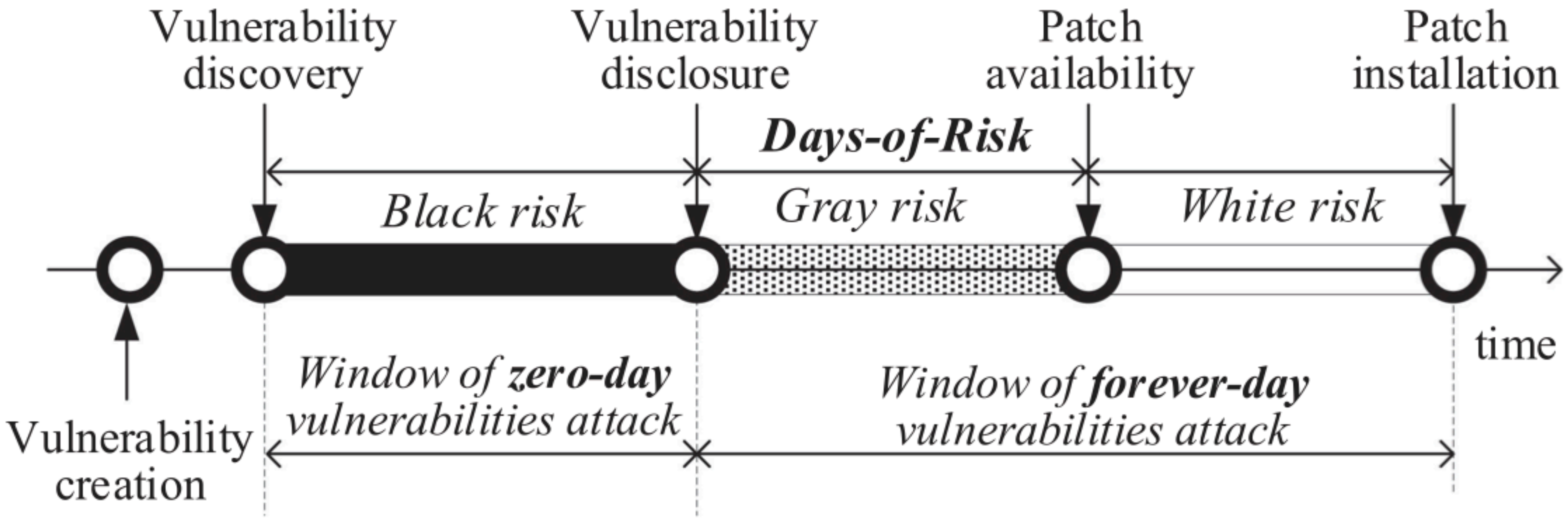
Trusted Execution
Environment

Scope - iOS

- Code Signing Protection Mechanism
- Unix Permissions
- Sandbox Framework
- Capabilities
  - Entitlements
  - Sandbox Extensions

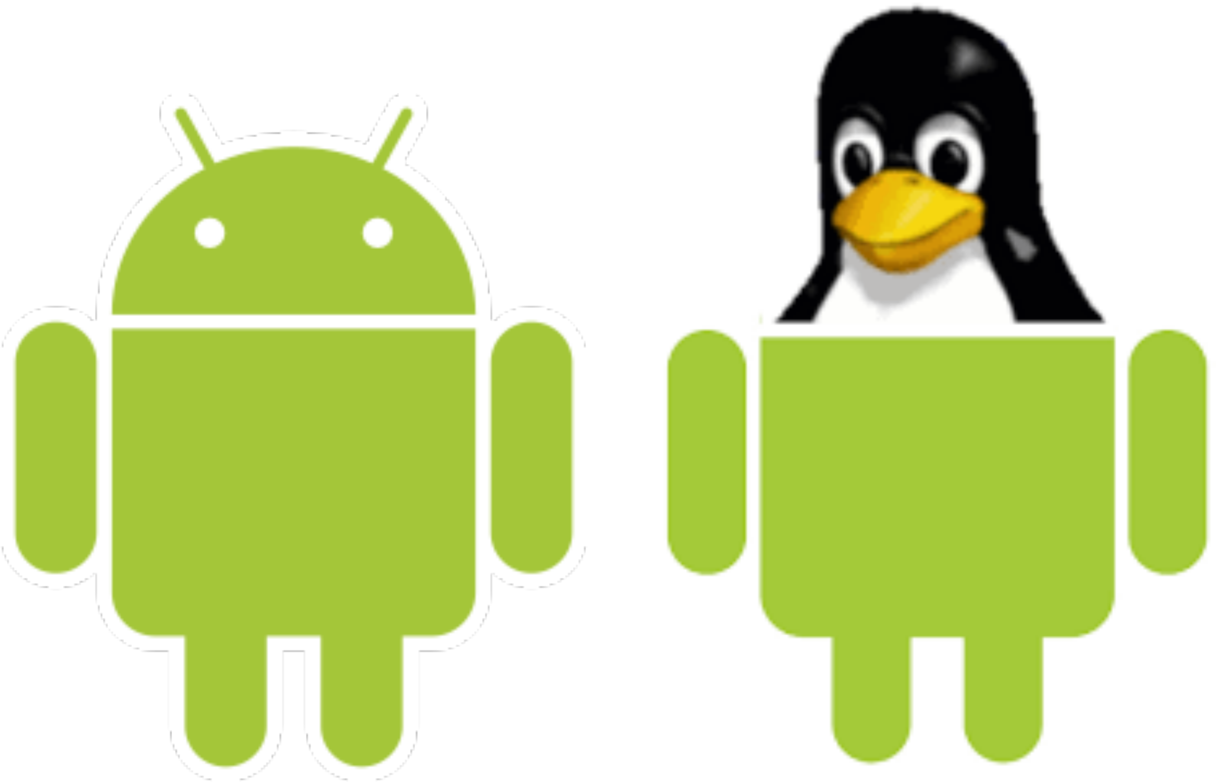
Objectives

- Improve vulnerability detection
- Discover zero-day vulnerabilities



Objectives - Android

- Implement method to discover vulnerabilities in:
  - Android Libraries (1)
  - Linux Kernel (2)



Objectives - iOS

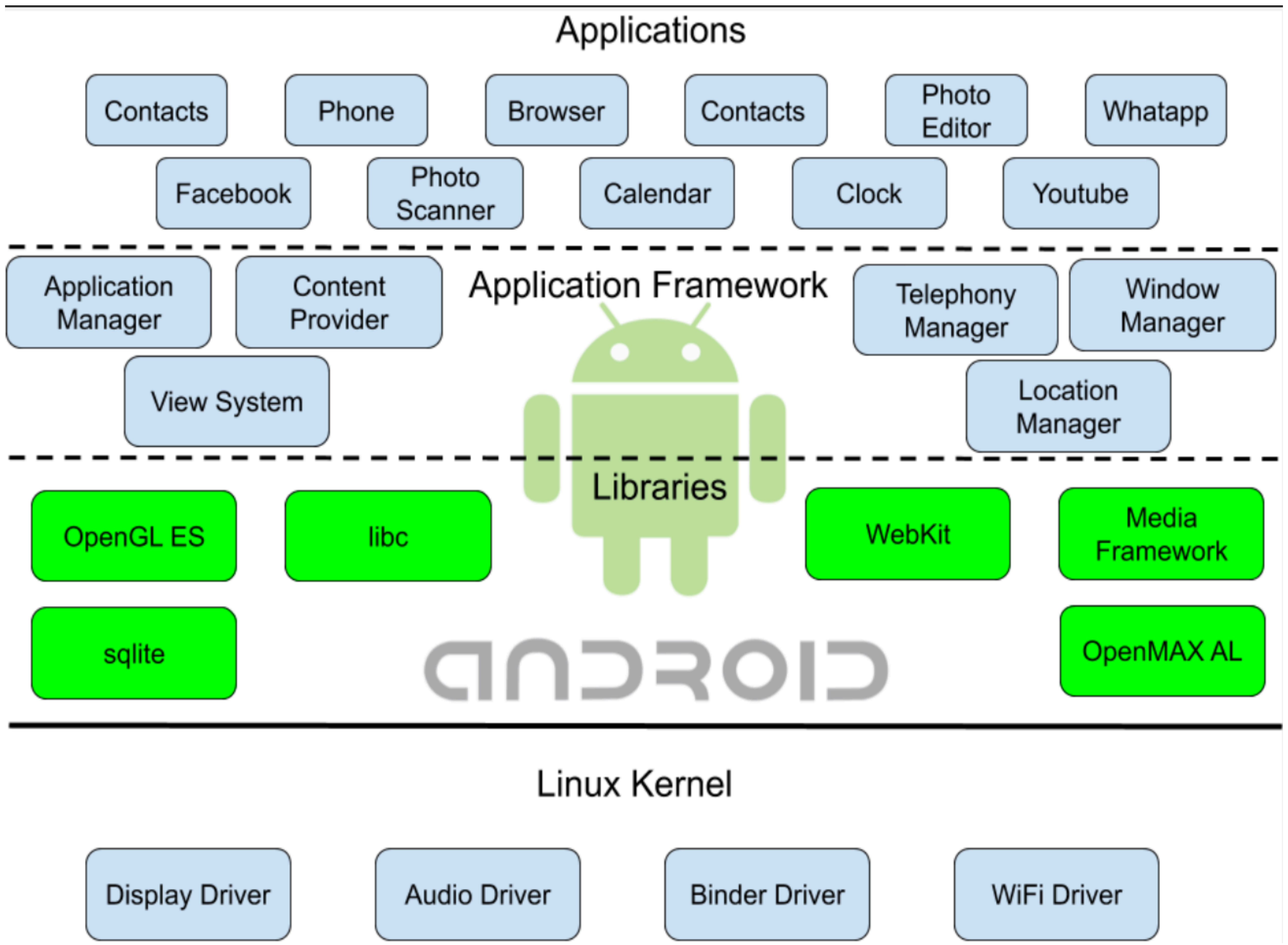
- Discover policy flaws in iOS protection system (3)
- Improve Apple Sandbox System (4)
- Discover vulnerabilities in the iOS IPC system (5)
- Discover programming errors during development phase (6)

Computer Science
& Engineering
Department

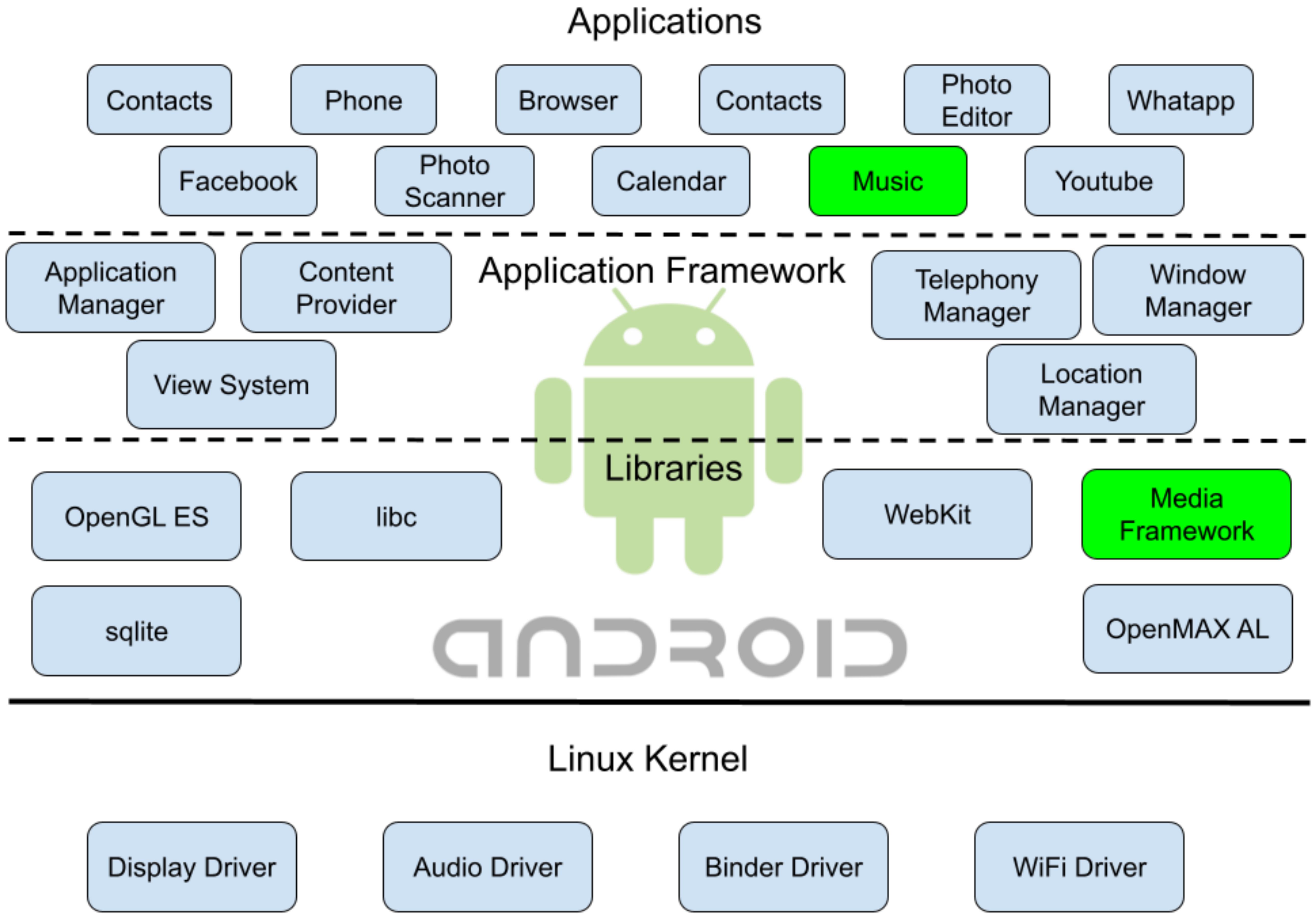
FUZZINGSTER - DETECTING AND ANALYZING ANDROID VULNERABILITIES IN USER SPACE (1)

UNIVERSITATEA POLITEHNICA DIN BUCURESTI 1818

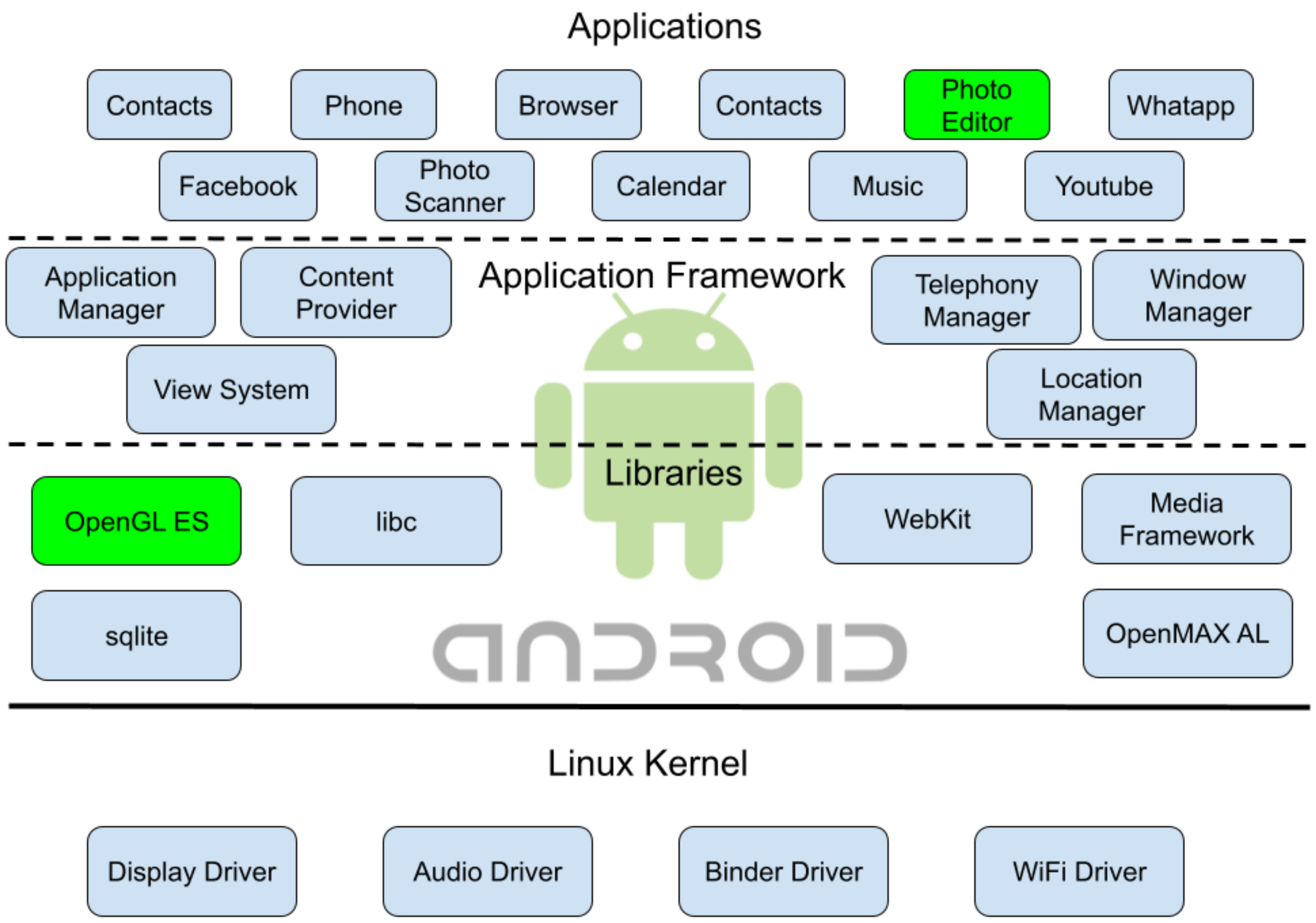
Scope


Applications
Contacts
Phone
Browser
Contacts
Photo Editor
Whatapp
Facebook
Photo Scanner
Calendar
Clock
Youtube
Application Manager
Content Provider
Application Framework
Telephony Manager
Window Manager
View System
Location Manager
Libraries
OpenGL ES
libc
WebKit
Media Framework
sqlite
android
OpenMAX AL
Linux Kernel
Display Driver
Audio Driver
Binder Driver
WiFi Driver

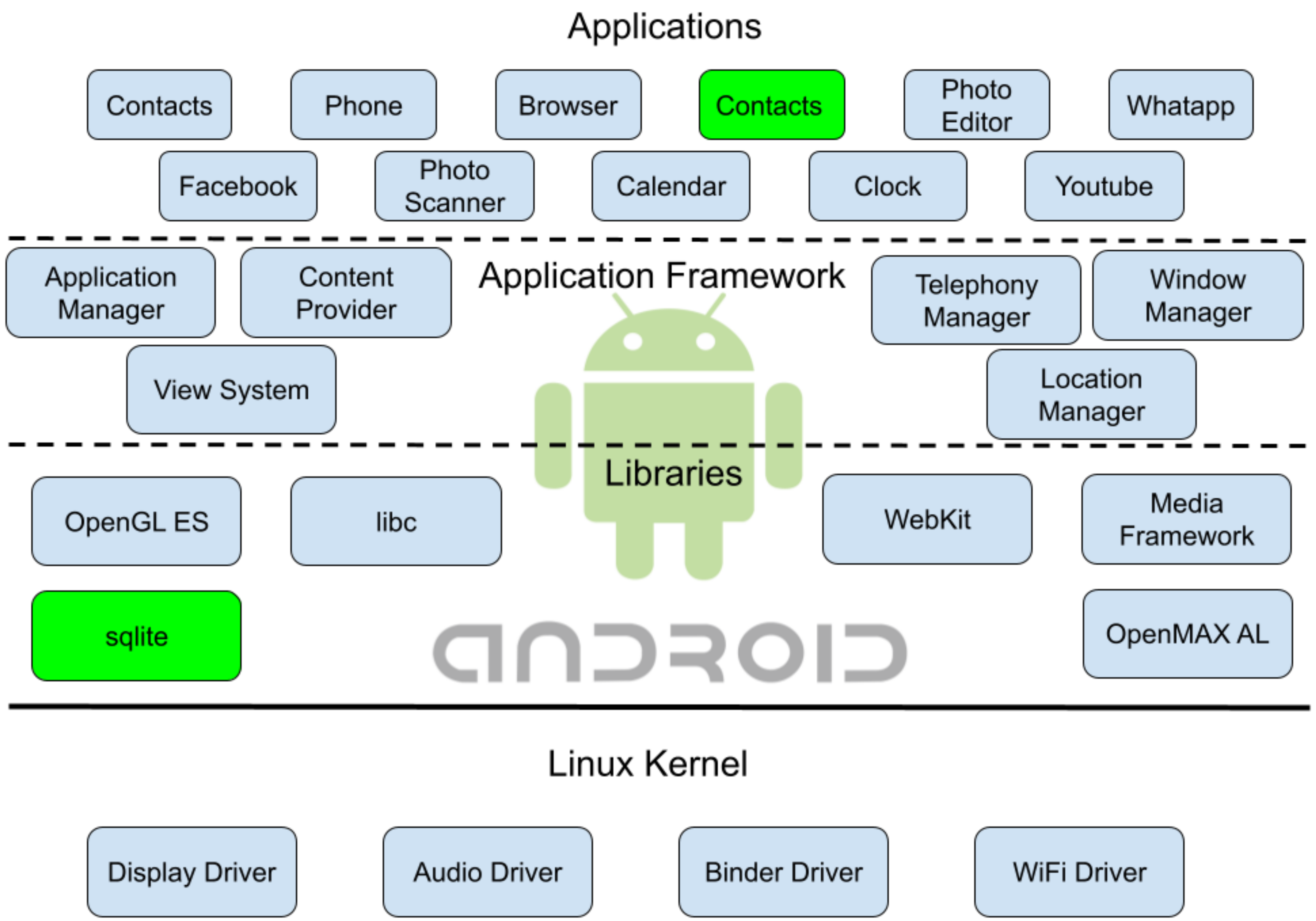
Android Applications



Android Applications



Android Applications

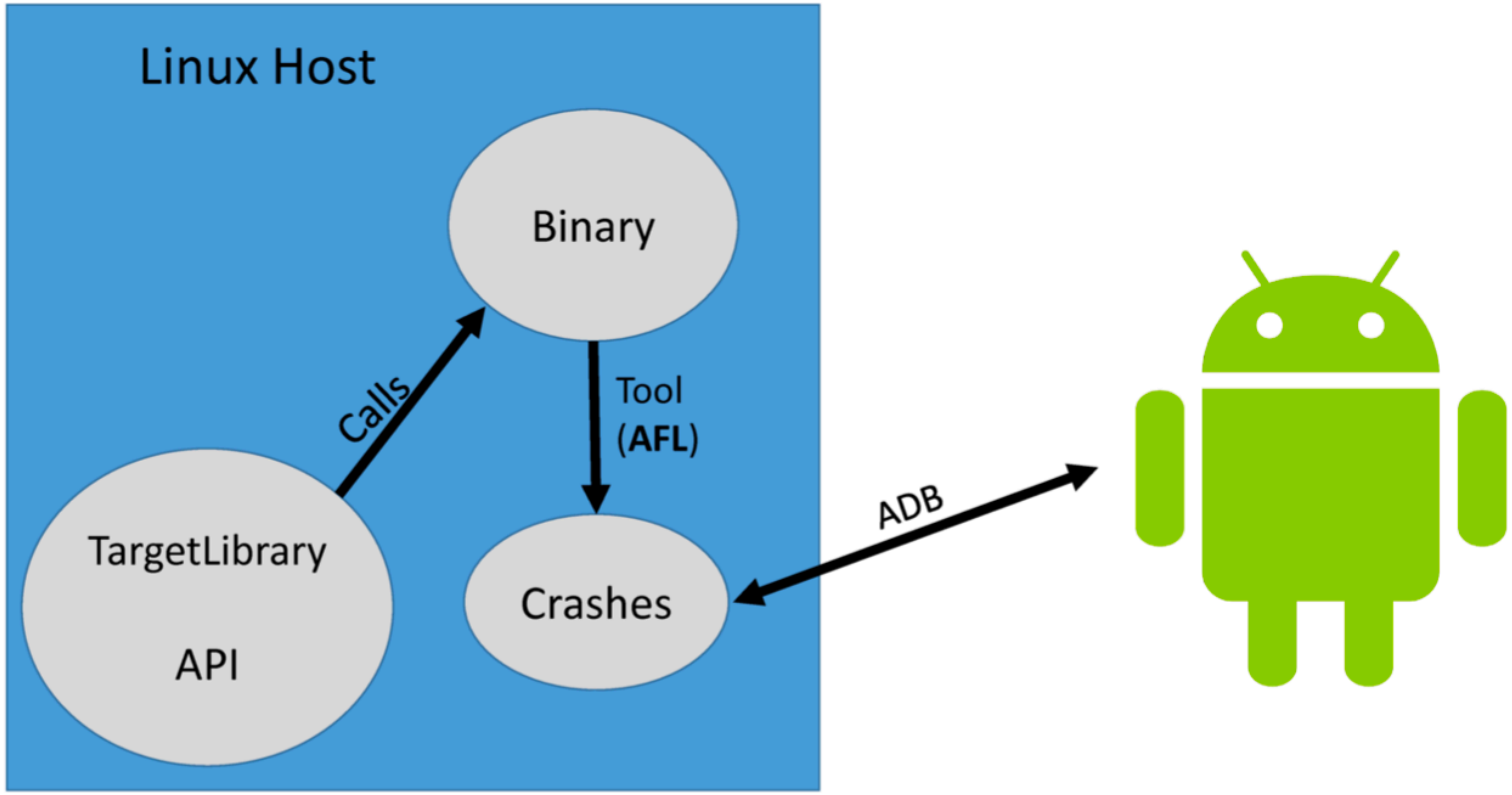


Terminology

- Cross compiled
- Fuzzing
- Binary instrumentation

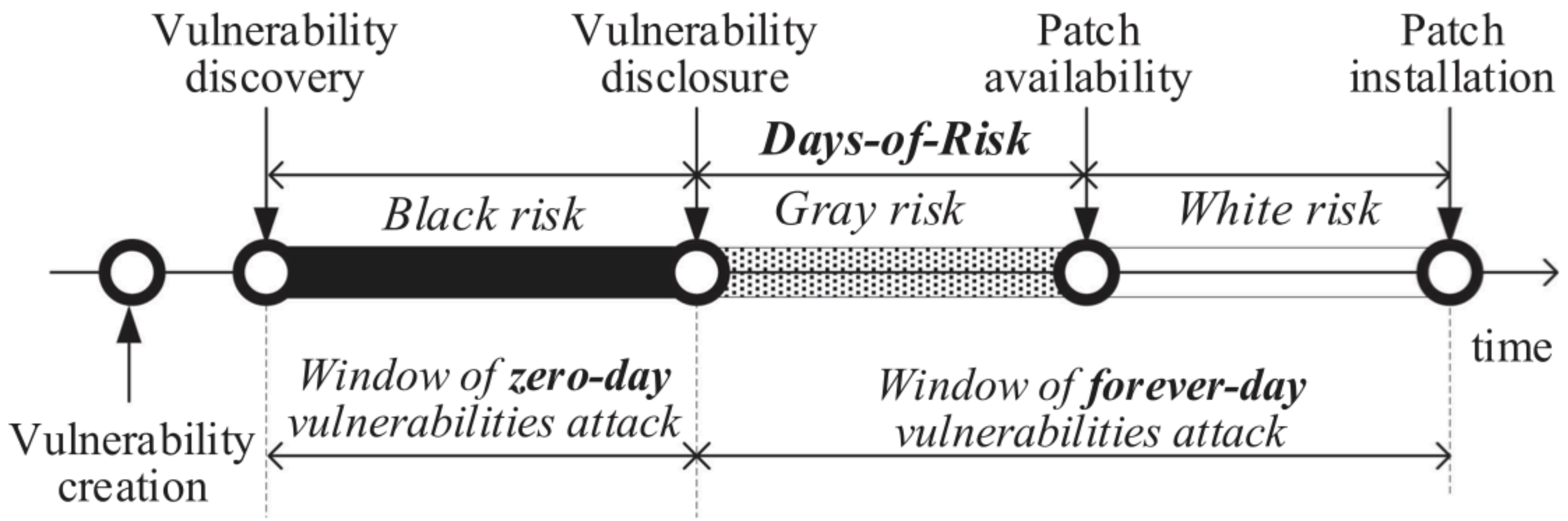
Fuzzing Android Libraries

- Cross compiled on Linux Host
- Coverage-Guided Fuzzing
- Binary Instrumentation
- Several fuzzing campaigns on PC and UPB cluster
- Target libraries: sqlite and gzip



Vulnerability Life-cycle

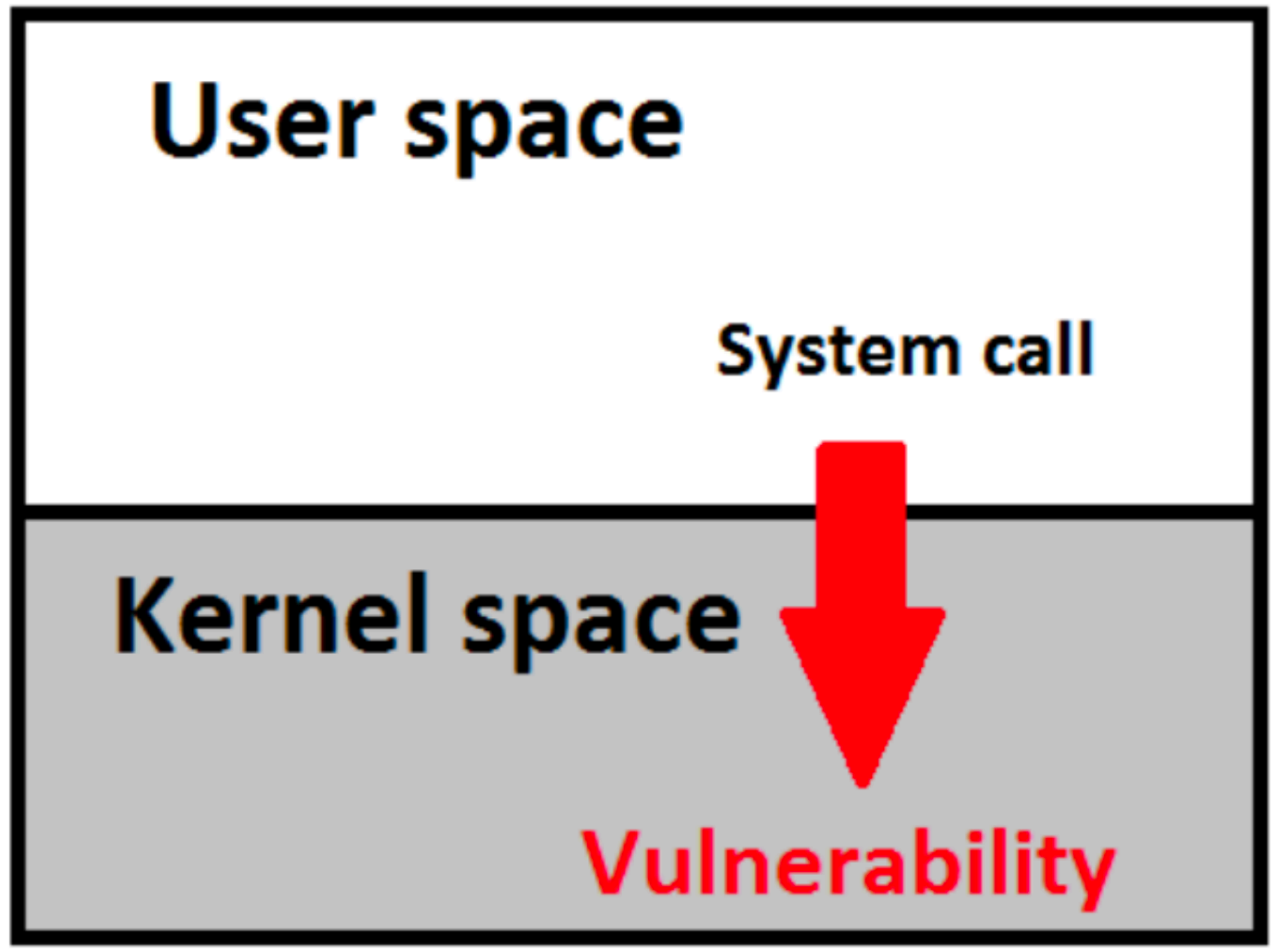
- Double Free (CWE 415)
- Gray risk vulnerability



FUZZING-KS - DETECTING AND ANALYZING VULNERABILITIES IN KERNEL SPACE (2)

Fuzzing via System Calls

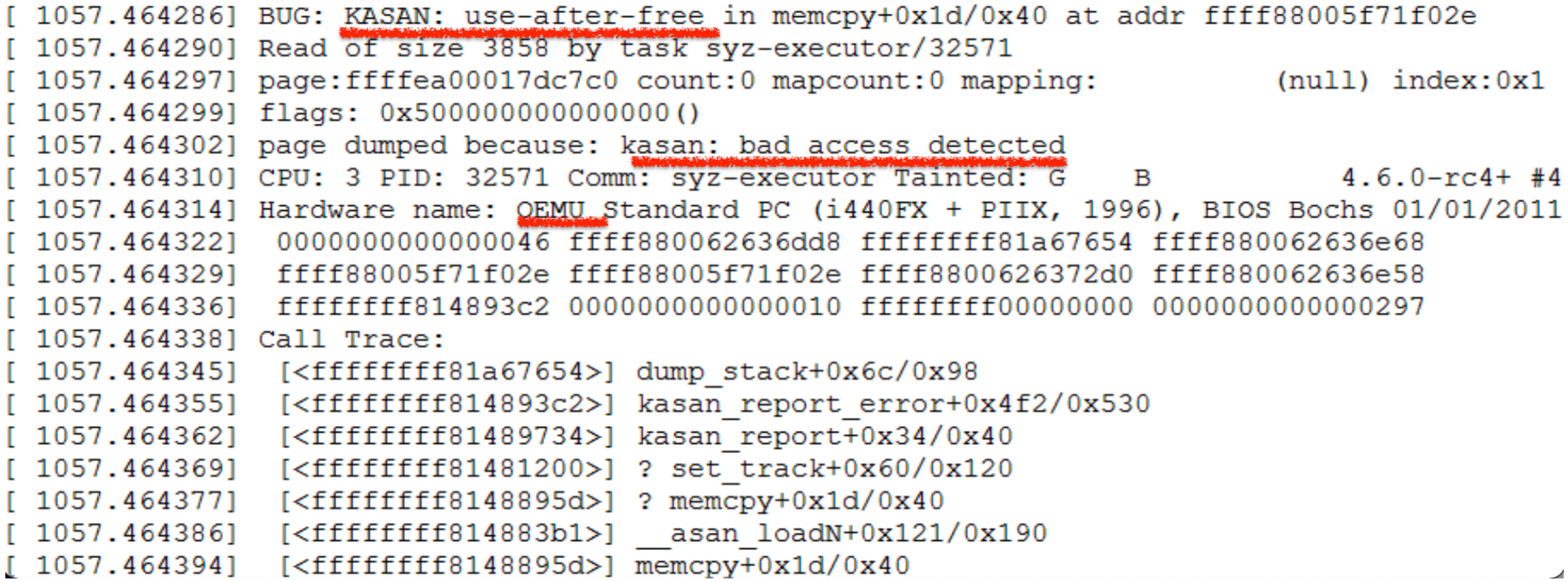
- Compile-time instrumentation on Linux Kernel
- KASAN - checks memory access
  - out-of-bounds, use-after-free, race conditions
- Kcov - kernel code coverage
- Coverage-Guided Fuzzing
- QEMU VMs



Fuzzing campaigns

- Several fuzzing campaigns on PC and UPB cluster
- Result: thousands of potential crashes
- Triage module for validating and minimising each crash

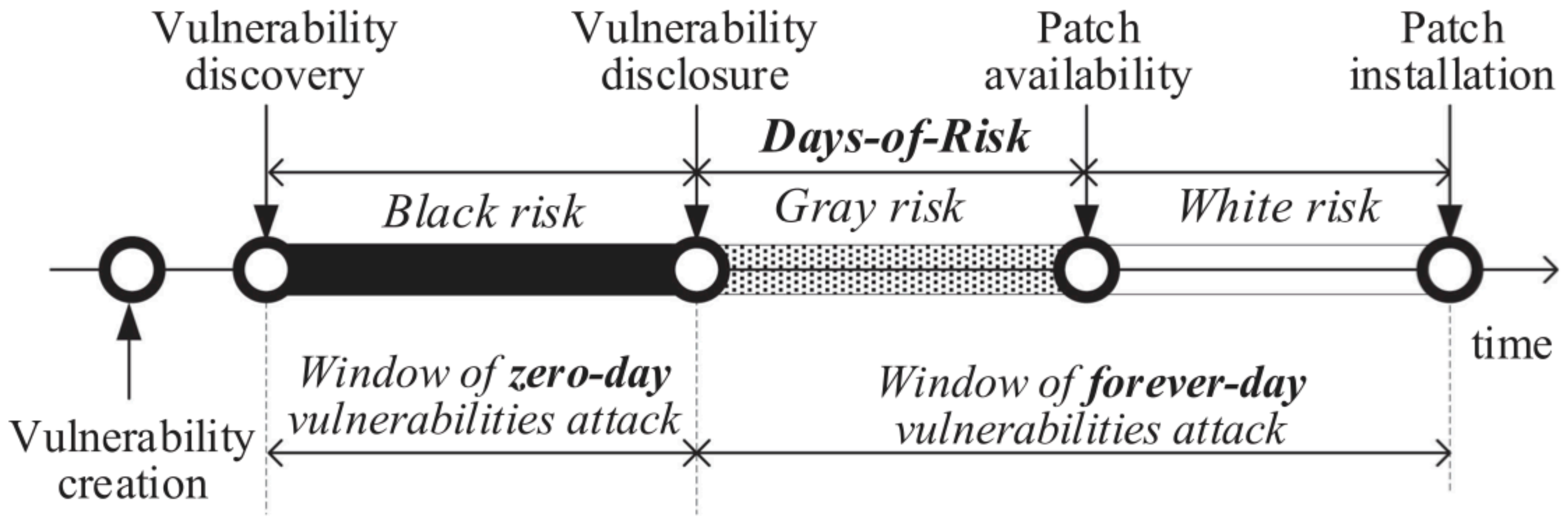
Fuzzing campaigns



```
[ 1057.464286] BUG: KASAN: use-after-free in memcpy+0x1d/0x40 at addr ffff88005f71f02e
[ 1057.464290] Read of size 3858 by task syz-executor/32571
[ 1057.464297] page:ffffea00017dc7c0 count:0 mapcount:0 mapping:          (null) index:0x1
[ 1057.464299] flags: 0x500000000000000()
[ 1057.464302] page dumped because: kasan: bad access detected
[ 1057.464310] CPU: 3 PID: 32571 Comm: syz-executor Tainted: G    B           4.6.0-rc4+ #4
[ 1057.464314] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS Bochs 01/01/2011
[ 1057.464322]  0000000000000046 ffff880062636dd8 ffffffff81a67654 ffff880062636e68
[ 1057.464329]  ffff88005f71f02e ffff88005f71f02e ffff8800626372d0 ffff880062636e58
[ 1057.464336]  ffffffff814893c2 0000000000000010 ffffffff00000000 0000000000000297
[ 1057.464338] Call Trace:
[ 1057.464345]  [<ffffffff81a67654>] dump_stack+0x6c/0x98
[ 1057.464355]  [<ffffffff814893c2>] kasan_report_error+0x4f2/0x530
[ 1057.464362]  [<ffffffff81489734>] kasan_report+0x34/0x40
[ 1057.464369]  [<ffffffff81481200>] ? set_track+0x60/0x120
[ 1057.464377]  [<ffffffff8148895d>] ? memcpy+0x1d/0x40
[ 1057.464386]  [<ffffffff814883b1>] __asan_loadN+0x121/0x190
[ 1057.464394]  [<ffffffff8148895d>] memcpy+0x1d/0x40
```

Vulnerability Life-cycle

- Use After Free (CWE 416)
- Gray risk vulnerability



iOracle: Automated Analysis of iOS Access Control Policies (3)

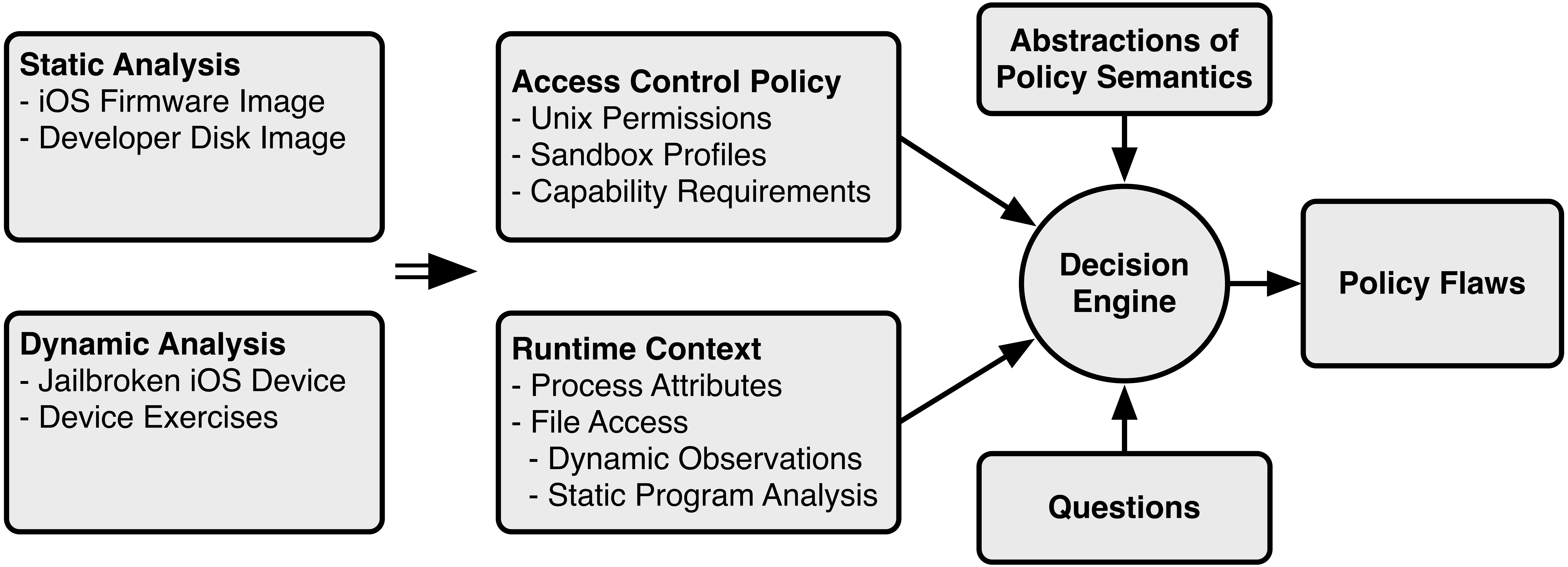
Terminology

- Policy — determines whether a subject can perform an action on an object
- Entitlements — a right that grants a privilege (key-value pair)
- Sandbox extensions - tokens passed from a process to another
- Apple Sandbox — restricts access based on a sandbox profile
- Jailbreak - privilege escalation exploit

Decentralised Policies

- Sandbox profiles (container profile)
- Unix File Permissions (read/write/execute)
- Code Protection Mechanism (signed executables)
- iOS Capabilities:
  - Entitlements (key-value pairs)
  - Sandbox extensions

Overview of iOracle



Static Analysis
- iOS Firmware Image
- Developer Disk Image

Dynamic Analysis
- Jailbroken iOS Device
- Device Exercises

Access Control Policy
- Unix Permissions
- Sandbox Profiles
- Capability Requirements

Runtime Context
- Process Attributes
- File Access
  - Dynamic Observations
  - Static Program Analysis

Abstractions of Policy Semantics

Decision Engine

Questions

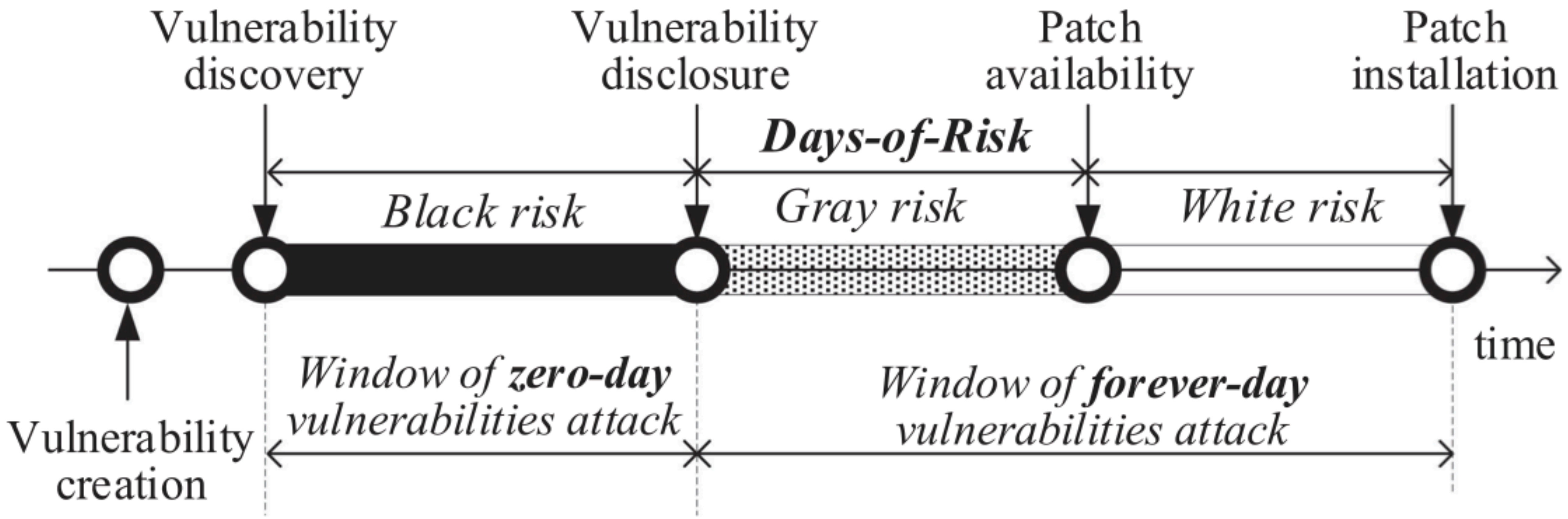
Policy Flaws

Abstractions & Questions

- Model data in Prolog
- ?- access(process(Proc),operation(“file-read”),file(“superSecret.txt”))

Evaluate iOracle

- Previously known vulnerabilities (jailbreaks)
- Previously unknown policy flaws:
  - Self-granted capabilities
  - Capability redirection
  - Keystroke exfiltration
  - Chown redirection



SANDTAILOR - ADDING CUSTOM SANDBOX PROFILES TO IOS APPS (4)

Overview

- Scope: Apple Sandbox
- All 3rd party apps — container profile
- Doesn't follow the least privilege principle
- Objective: Every 3rd party application different sandbox profile

Challenges

- Attach a custom profile sandbox
  - Enforcement
- Create a custom profile sandbox
  - Application Inspection
  - Tracing - create a profile sandbox custom tailored

Computer Science & Engineering Department

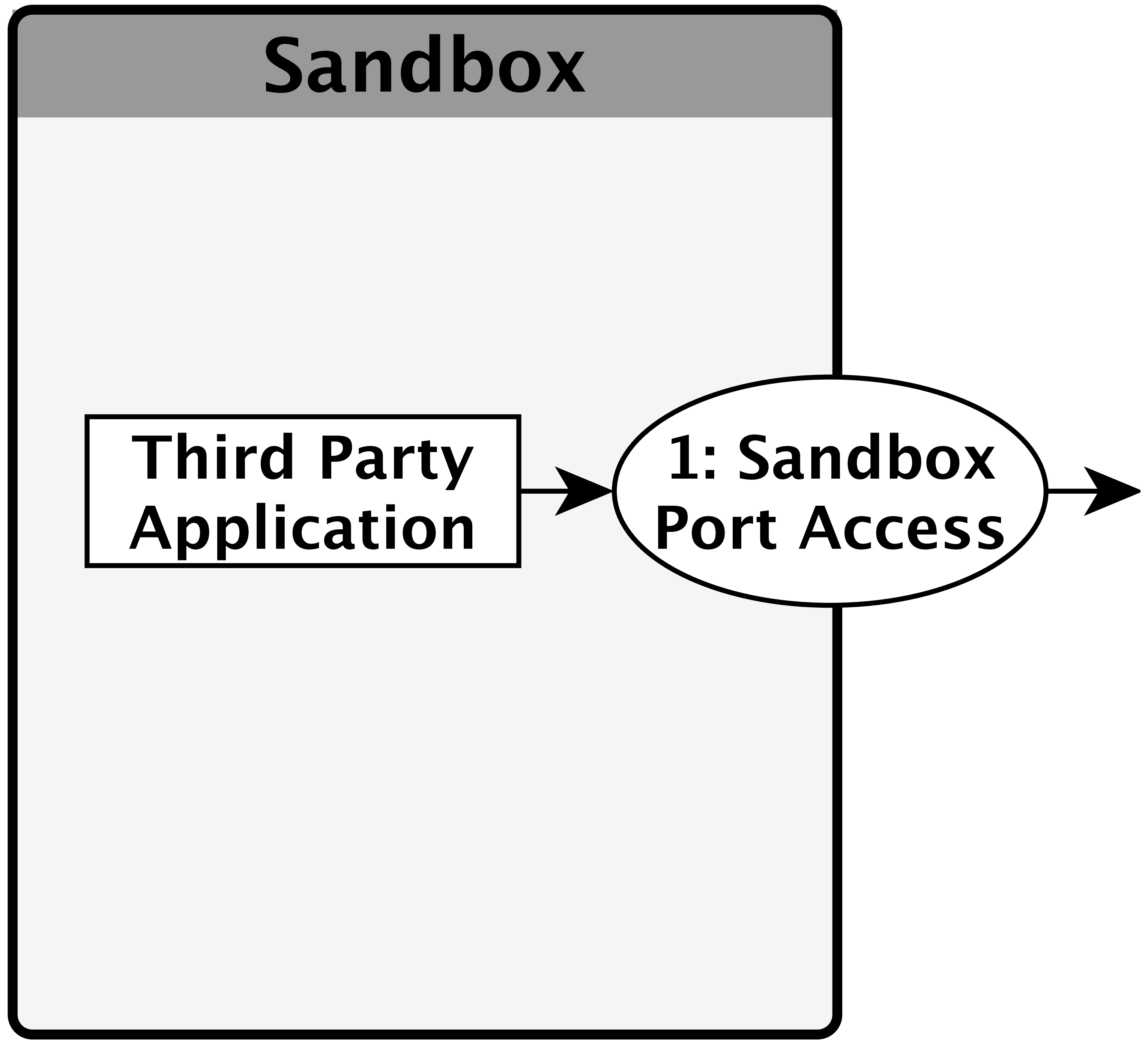
Kobold: Evaluating Decentralized Access Control for Remote NSXPC Methods on iOS (5)

UNIVERSITATEA POLITEHNICA DIN BUCURESTI 1818

Defining the Attack Surface

- Which entitlements are available to third party apps?
    - Entitlement: a privilege embedded in an app’s signature
- Which NSXPC methods are accessible to third party apps?
    - NSXPC: An object oriented IPC mechanism, which may require entitlements
- Of these accessible NSXPC methods, which are dangerous?

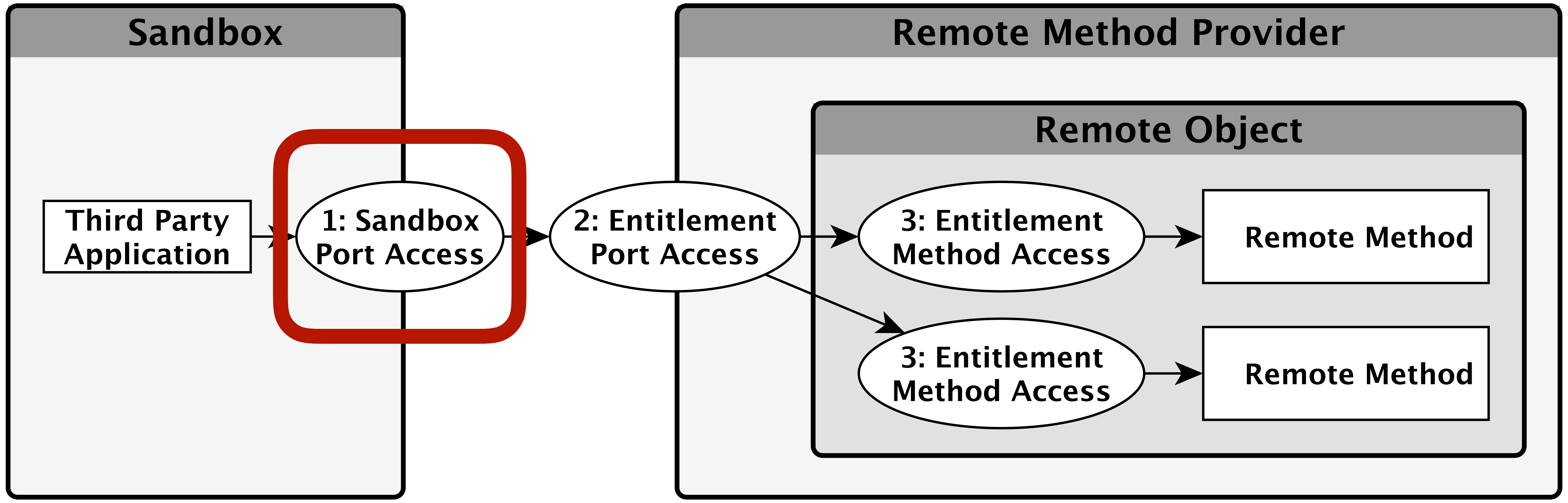
NSXPC Access Control



Mach Port: an IPC abstraction allowing communication between two processes.
With NSXPC, a port can map to multiple remote methods.

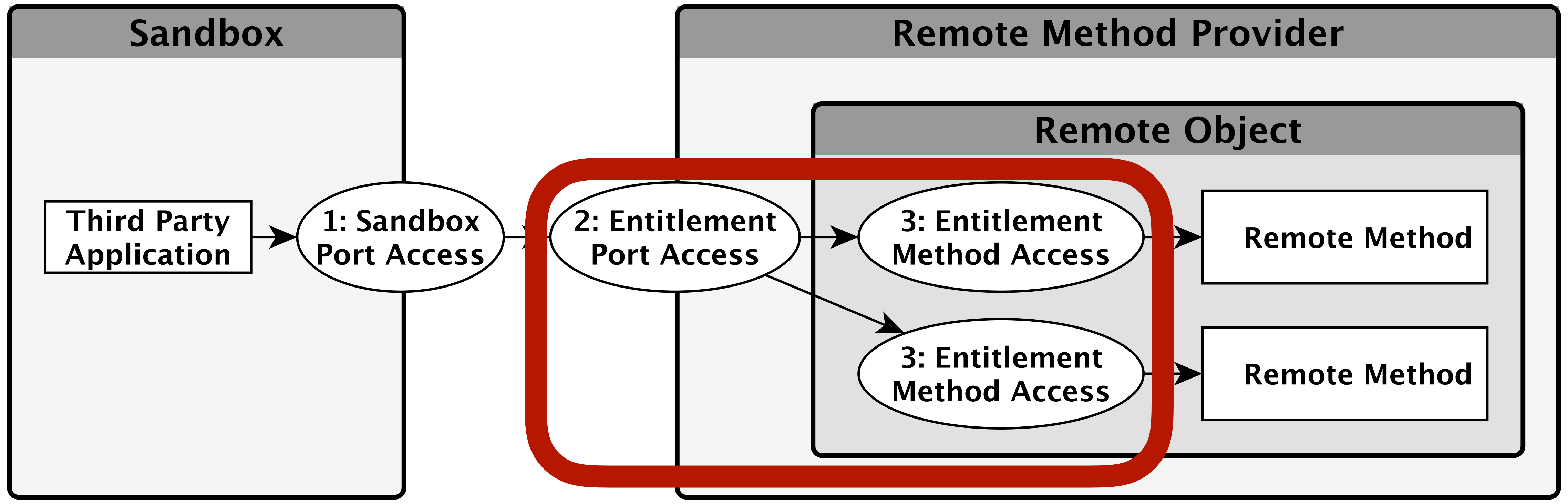
Sandbox Mach-Lookup Rules

```
(allow mach-lookup(
  require-all
   (global-name "siri.vocabularyupdates")
   (require-entitlement “com.apple.developer.siri”)
  )
)
```



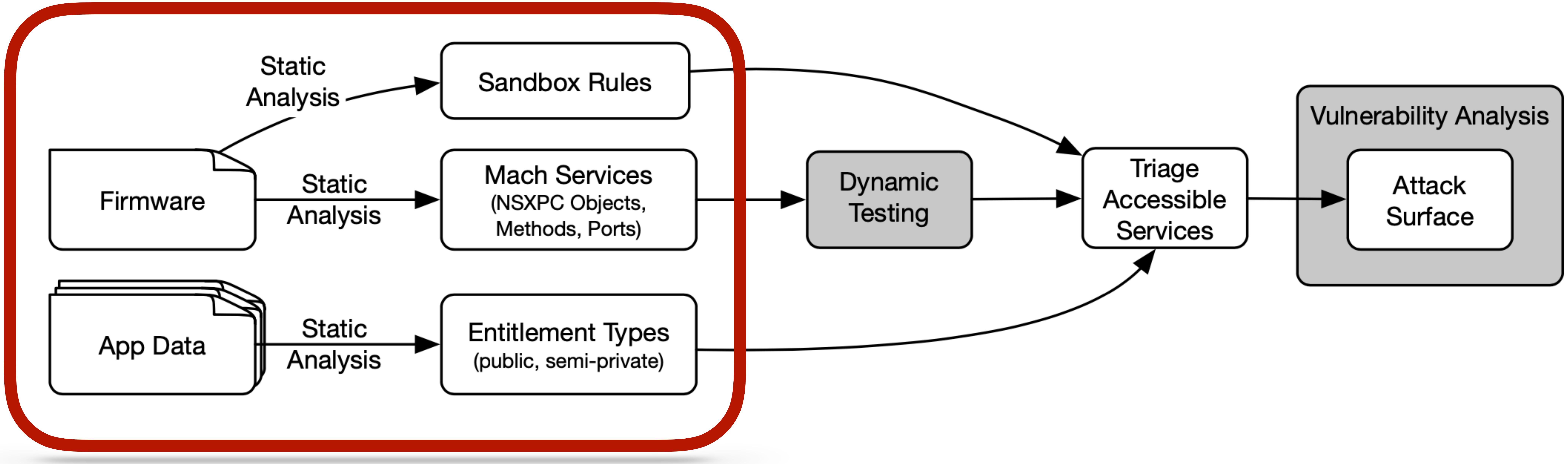
Daemon Entitlement Requirements

- Remote method providers (Daemons) check entitlements
    - On Port Access
    - On API (Method) Access

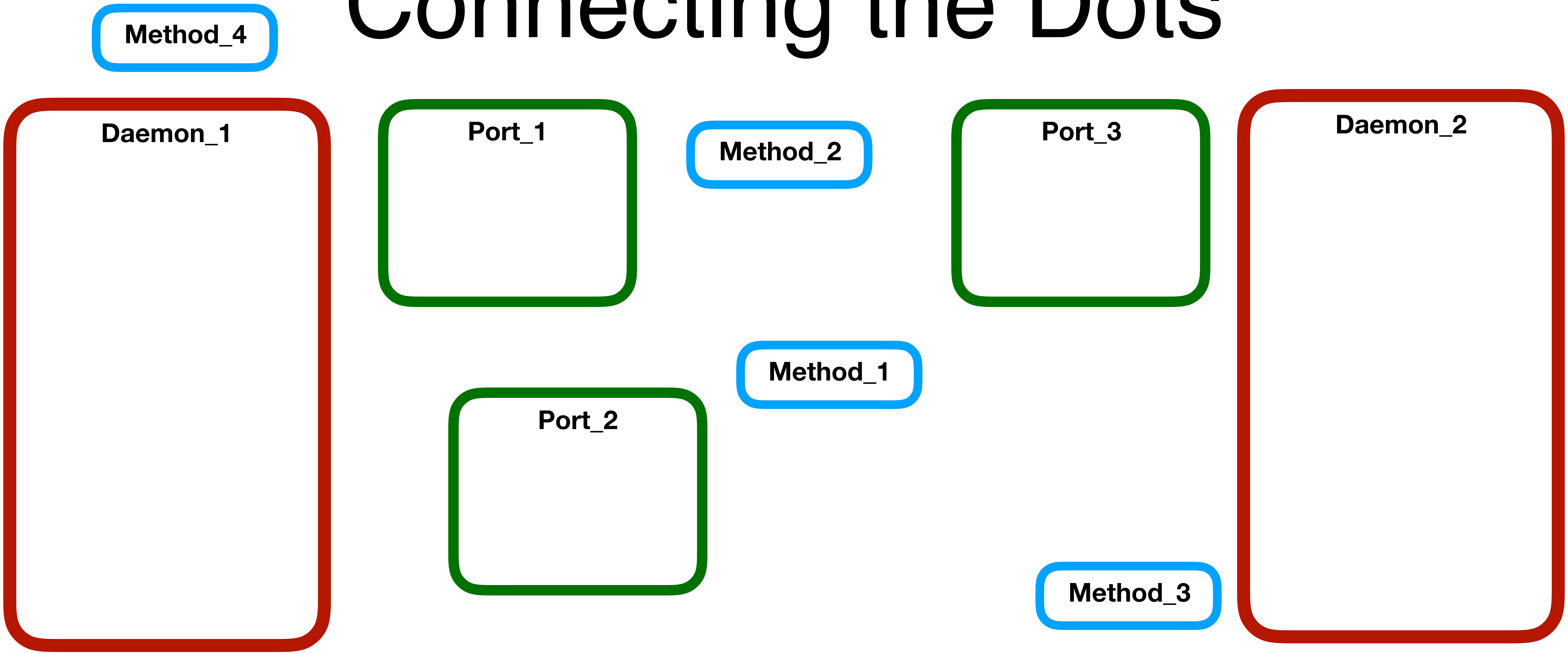


```
//psuedocode for entitlement check in daemon logic

entitlement_key = “health.stats”

entitlement_value = “weight”

if check_value(entitlement_name, client) == entitlement_value:

    send_weight(client)

else:

    send_error(client, “missing entitlement”)
```

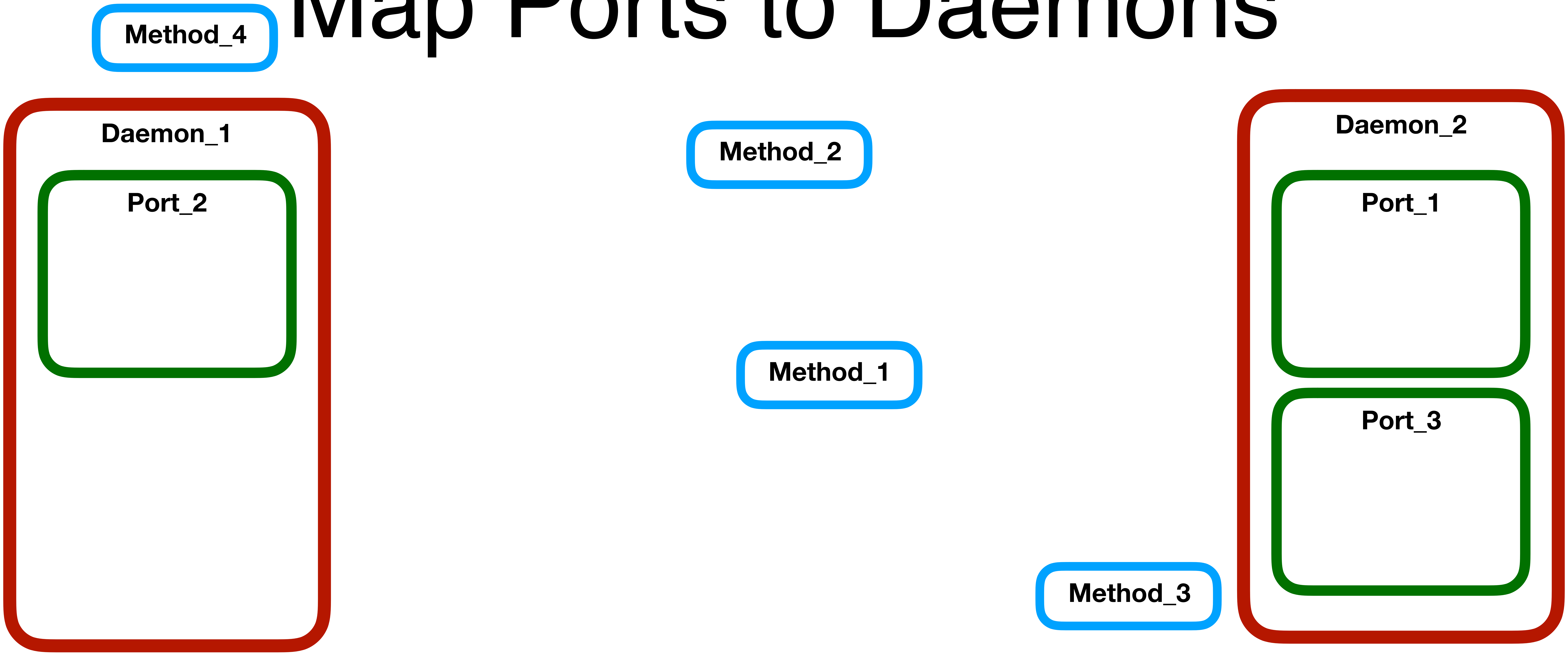
Kobold Overview



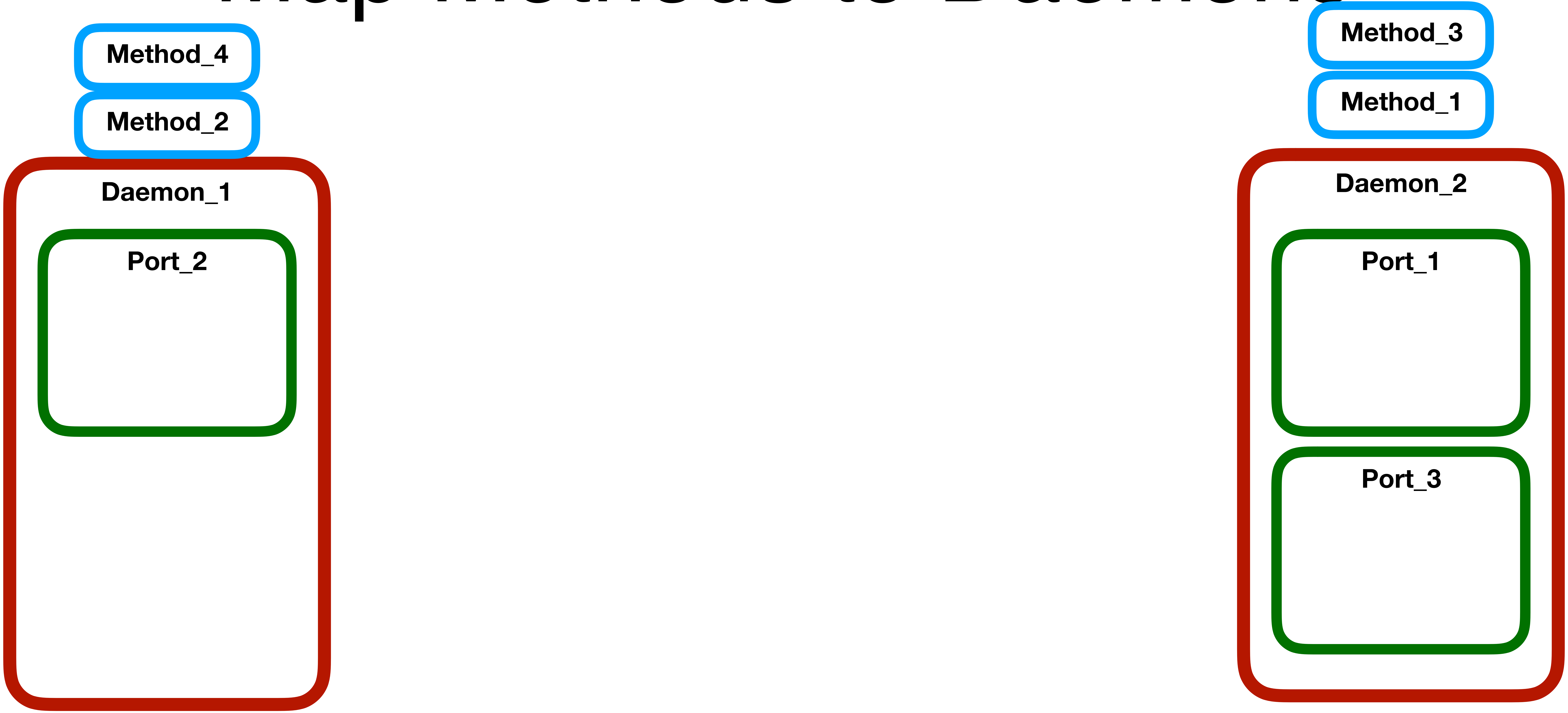
Connecting the Dots



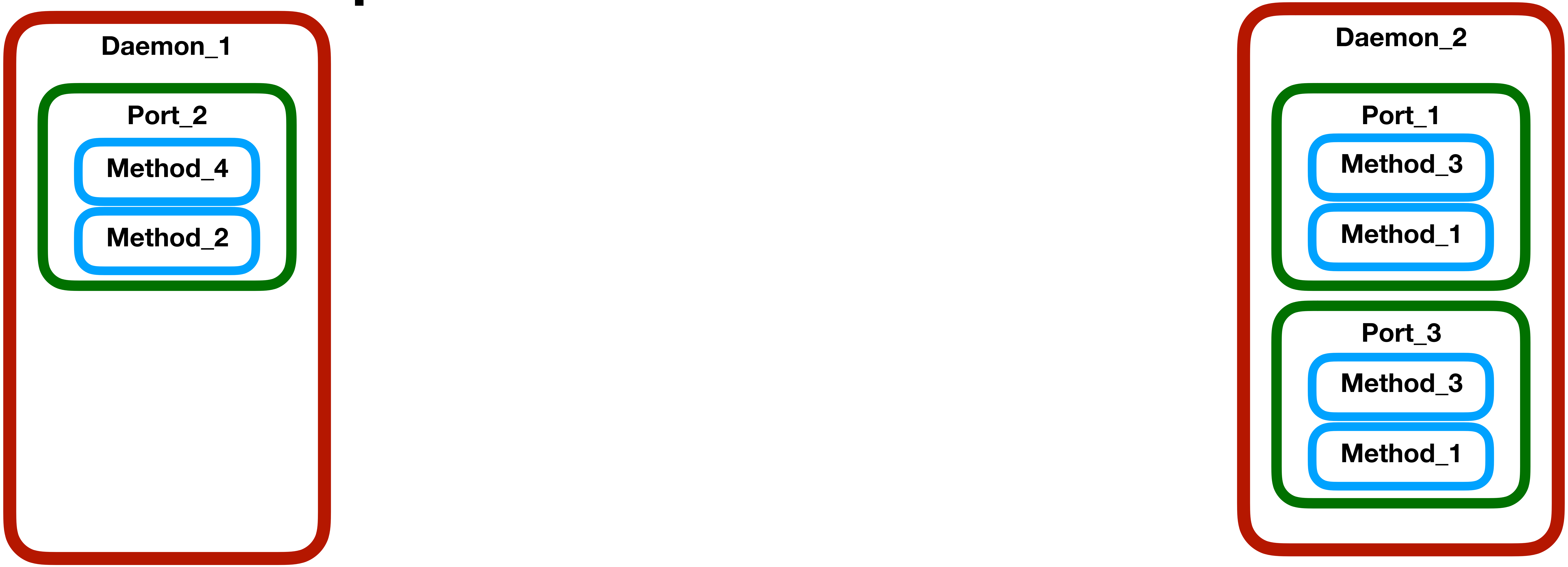
Map Ports to Daemons



Map Methods to Daemons



Map Methods to Daemons



Daemon_1

Port_2

Method_4

Method_2

Daemon_2

Port_1

Method_3

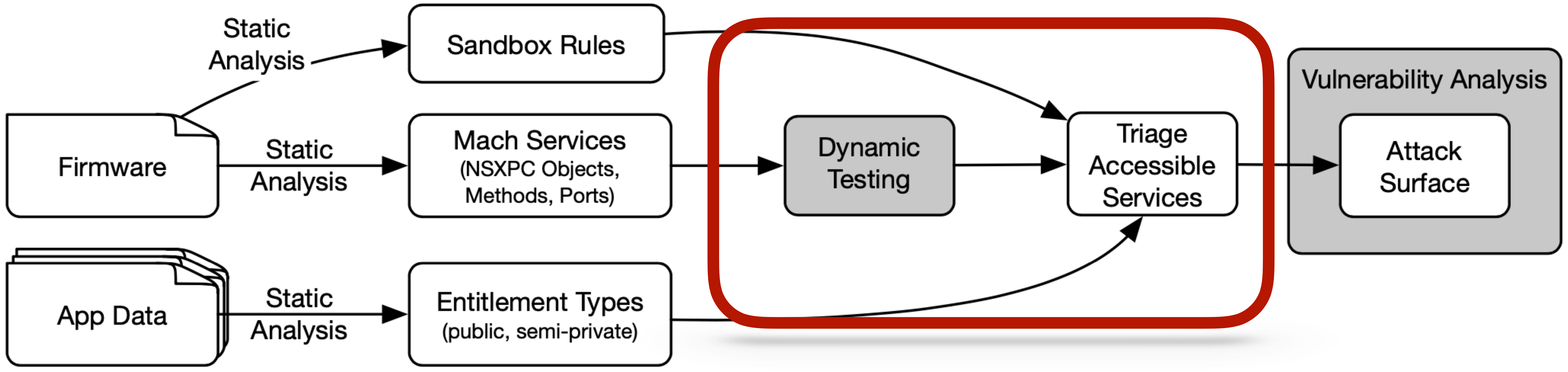
Method_1

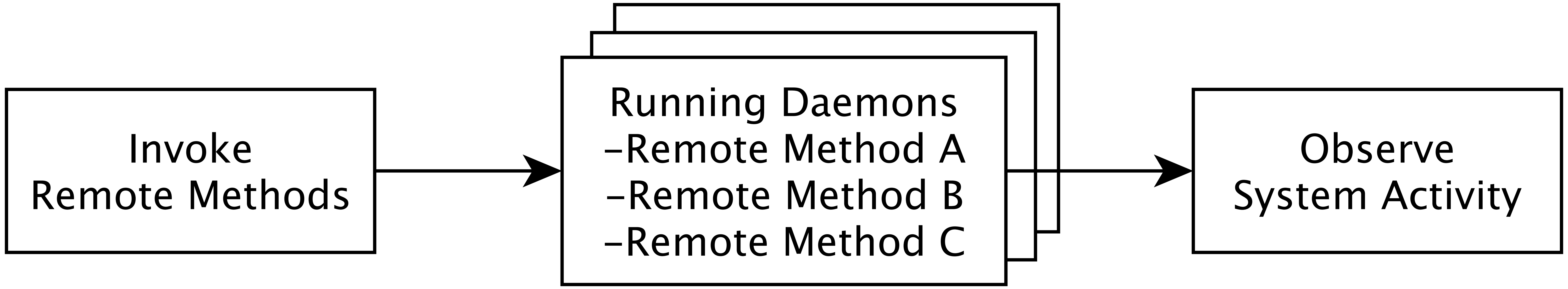
Port_3

Method_3

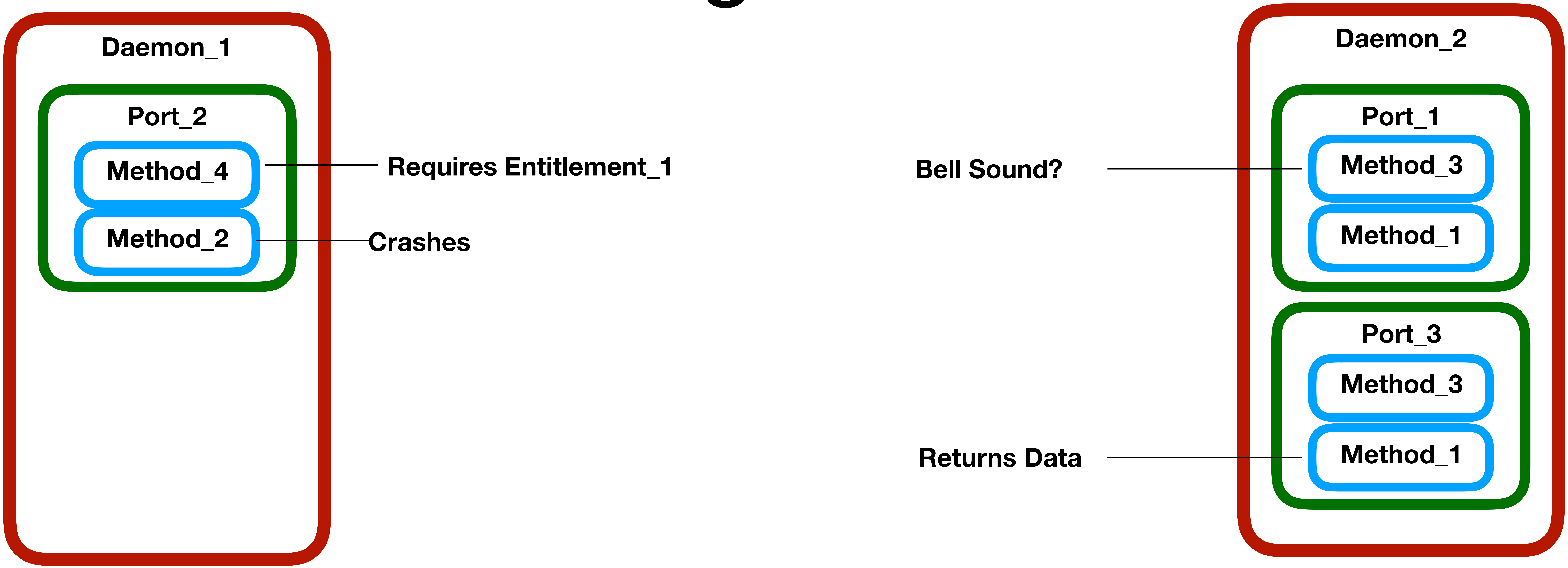
Method_1

What’s Accessible?



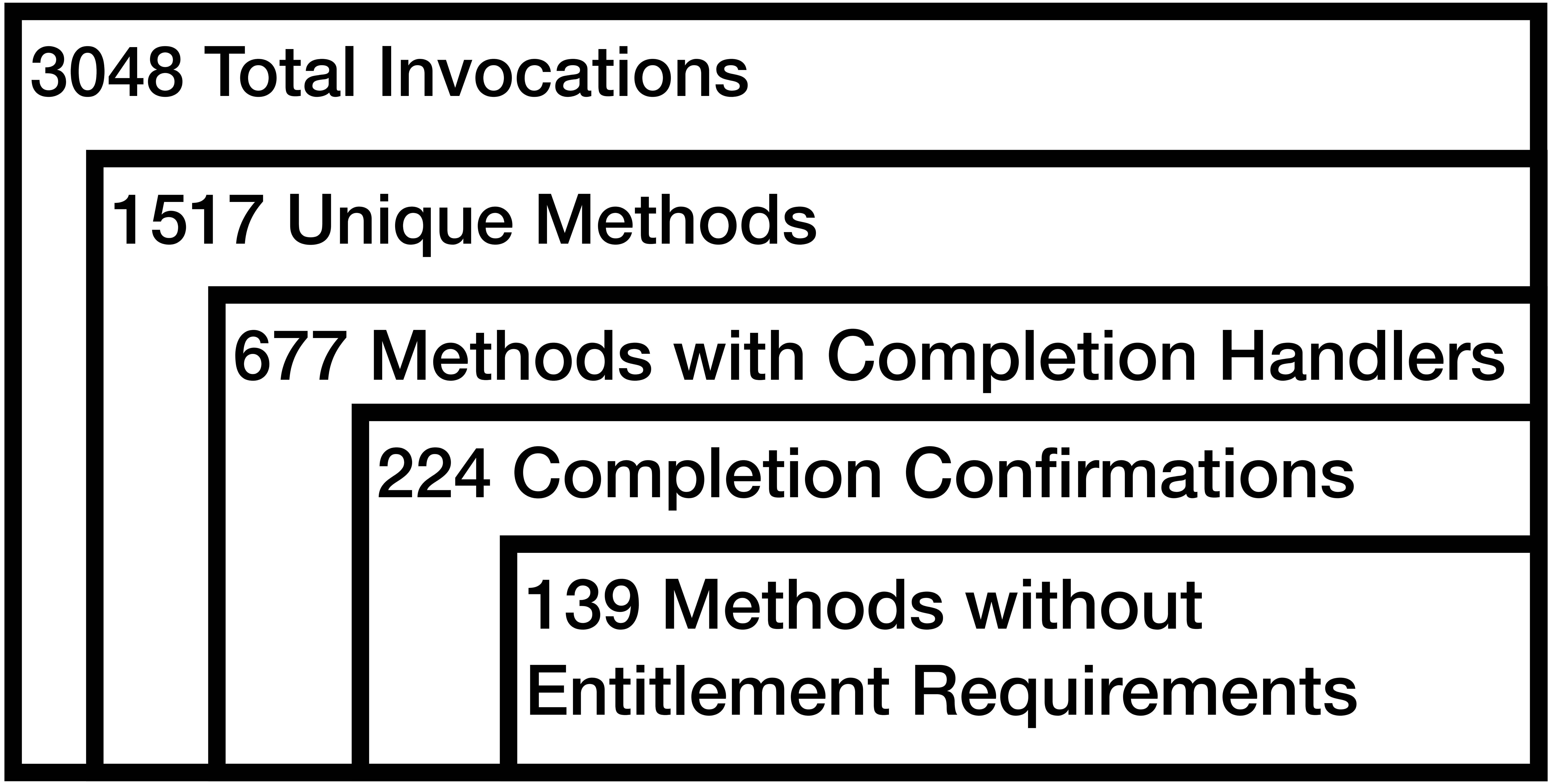


Running the Code



What did we find?

Remote Method Enumeration



3048 Total Invocations

1517 Unique Methods

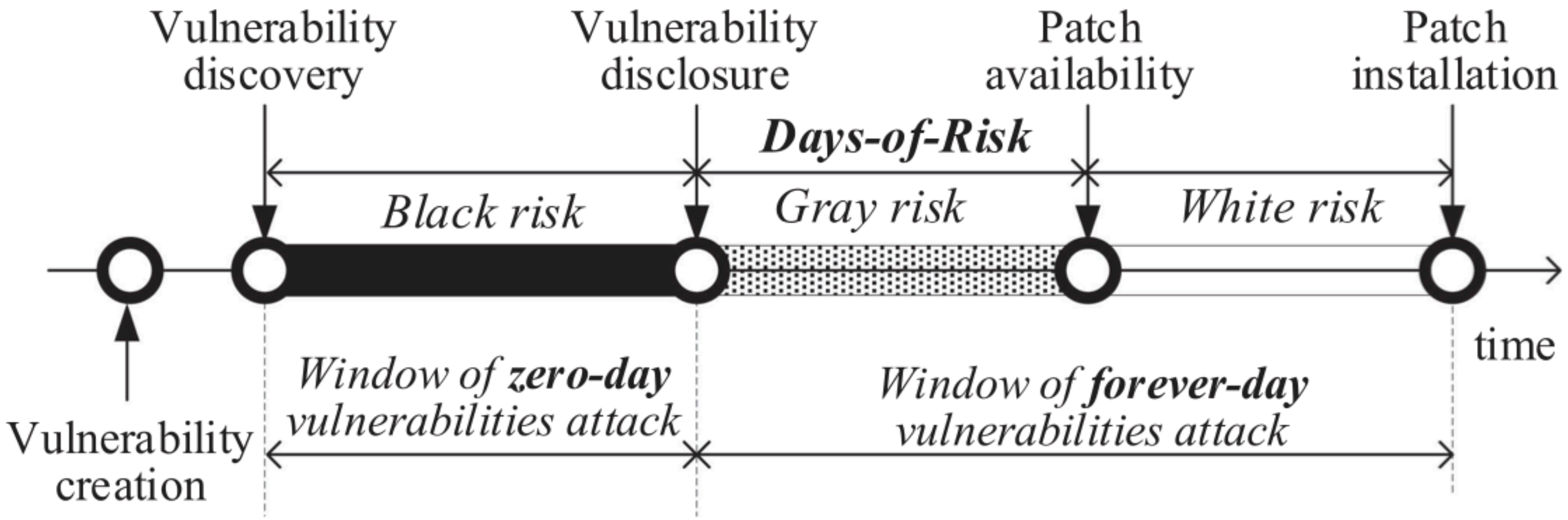
677 Methods with Completion Handlers

224 Completion Confirmations

139 Methods without
Entitlement Requirements

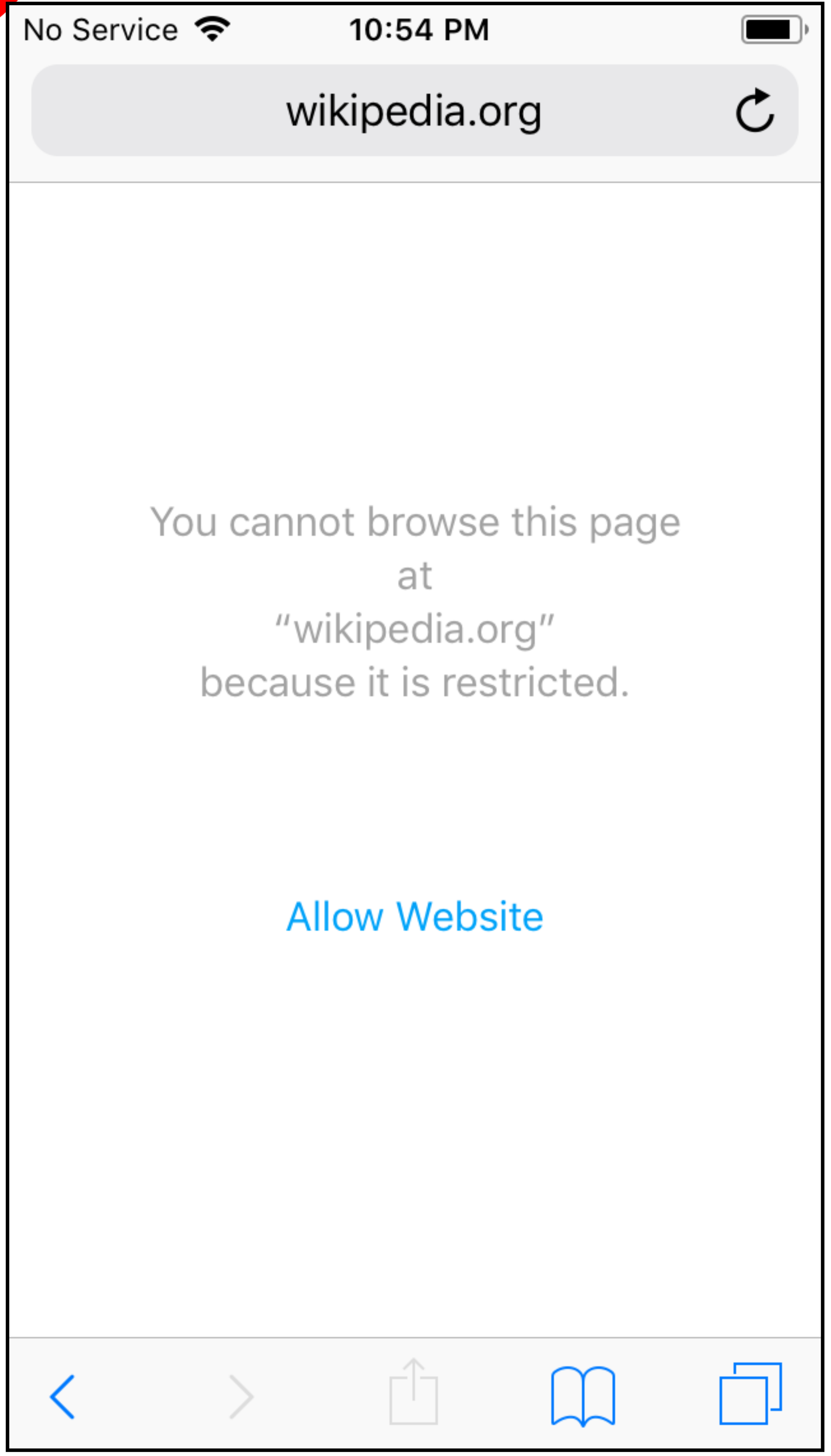
Discovered Vulnerabilities

- CVE-2019-8698: Block access to all websites
- CVE-2019-8502: Activate microphone in dictation request
- CVE-2018-4446: Leak File Provider information
- Daemon crashes



Blocking all websites through confused deputy

Safari



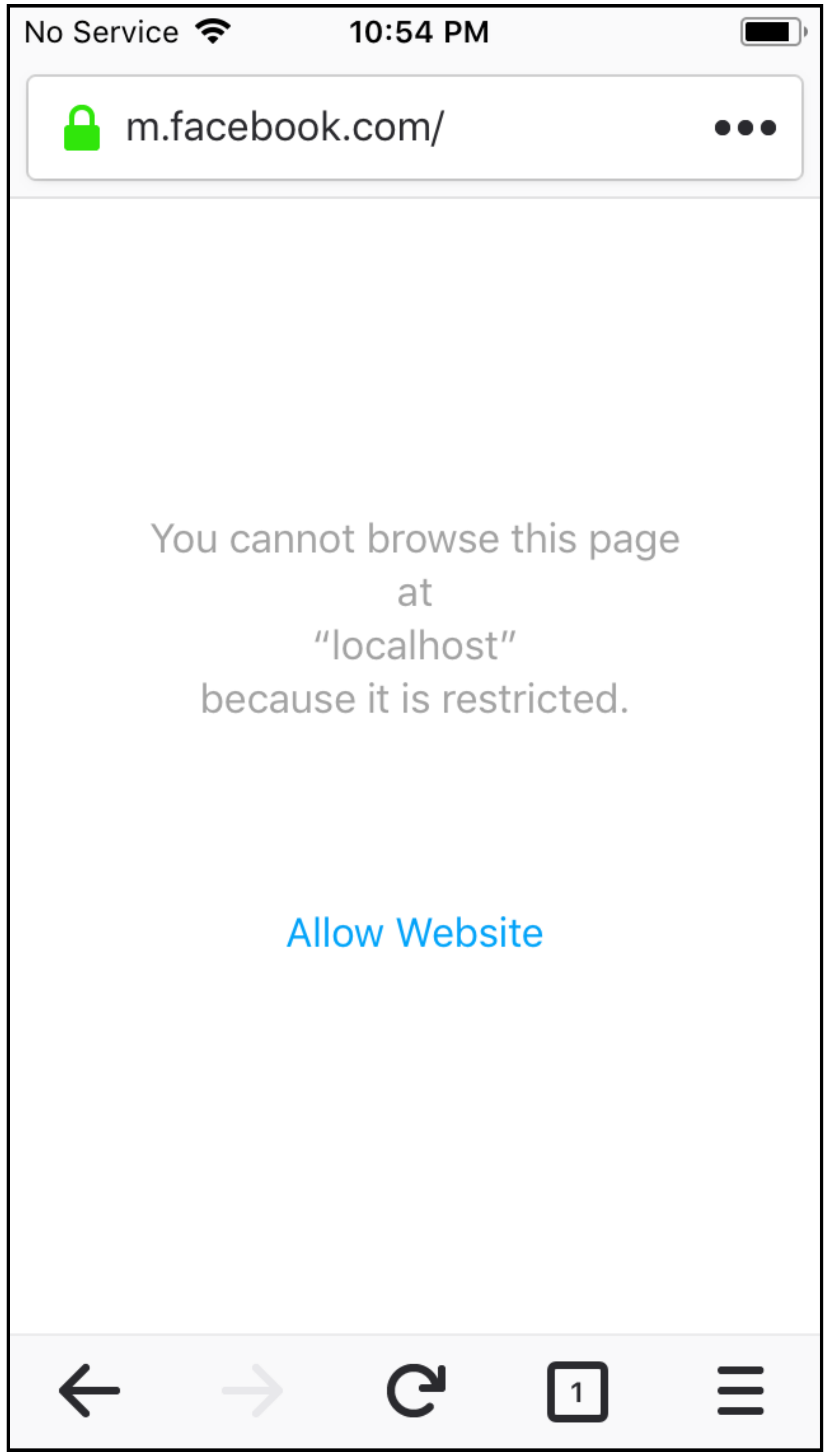
No Service 10:54 PM

wikipedia.org

You cannot browse this page at "wikipedia.org" because it is restricted.

Allow Website

Firefox

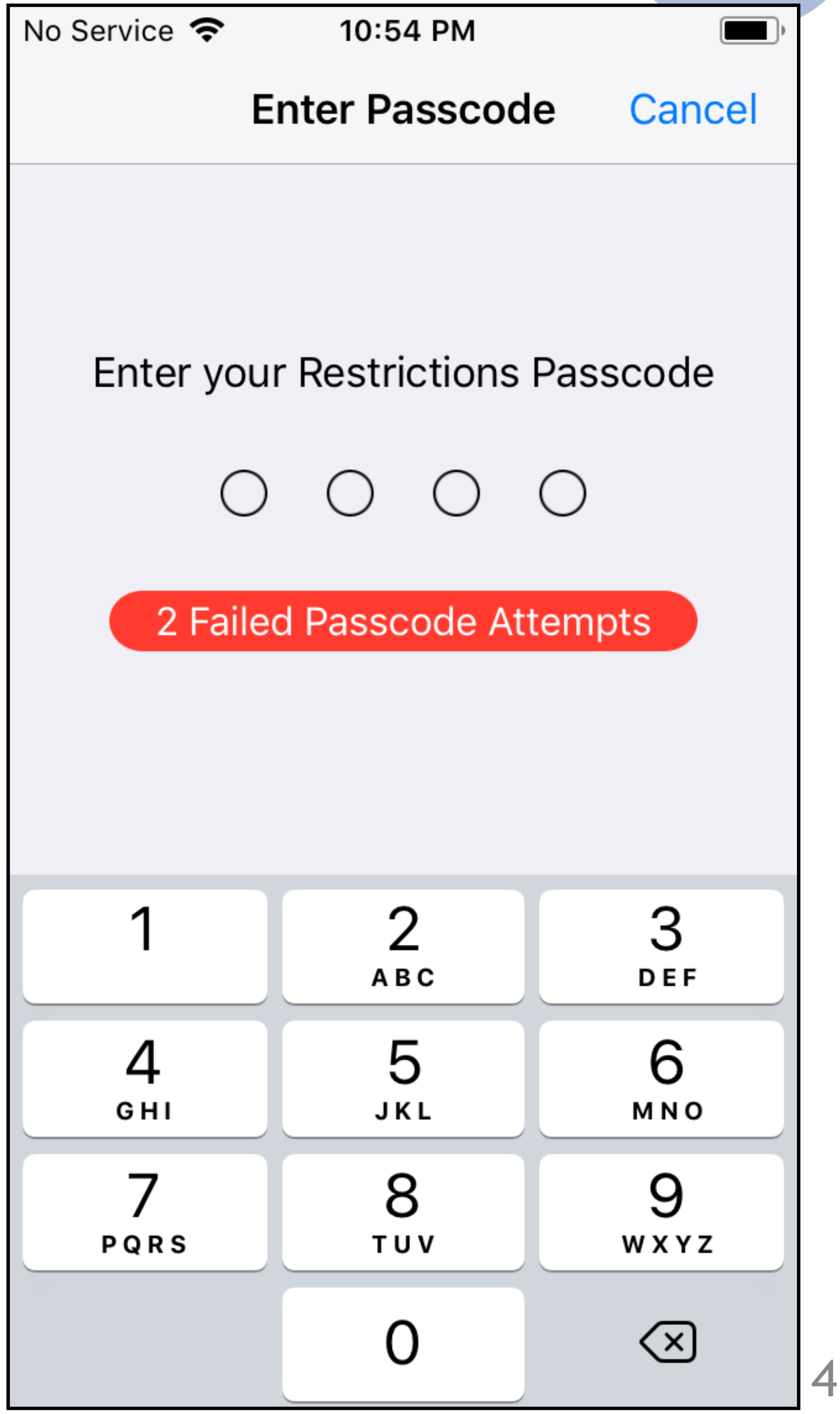


No Service 10:54 PM

m.facebook.com/

You cannot browse this page at "localhost" because it is restricted.

Allow Website



No Service 10:54 PM

Enter Passcode Cancel

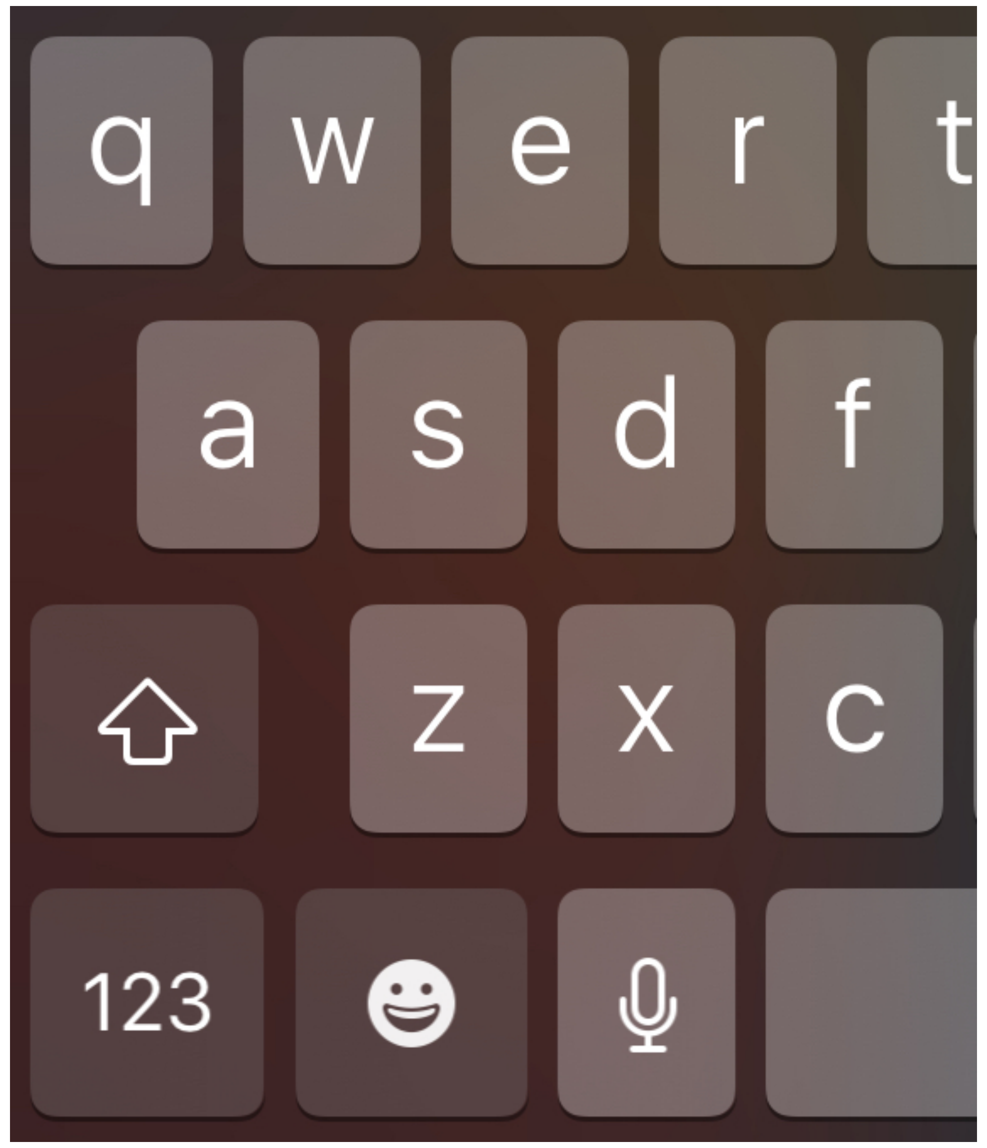
Enter your Restrictions Passcode

○ ○ ○ ○

2 Failed Passcode Attempts

Start Dictation Session

- Bells ringing during fuzzing
- Muting phone does not stop bells
- Evidence of microphone activation
  - Port: *com.apple.assistant.dictation*
  - Method: *startRecordingForPendingDictation*
  - Bell interrupts Voice Recording
  - Same bell as keyboard dictation prompt
  - Feedback on noise cancelling headphones



File Provider File Name Inference

- State dump allows inferring file names in File Provider directories
- UUID and domain should prevent file guessing attack
- State dump leaks the UUIDs and domains

```
“com.microsoft.skydrive.onedrivefileprovider"

documentStorageURL = “file:///private/var/mobile/Containers/Shared/AppGroup/
C4F93D7B-B6B4-498B-A747-47198D89C1D2/File%20Provider%20Storage/";

domains = {2645129dbb71cb32 = "<NSFileProviderDomain: 0x131e24fd0>";
```

```
Error reading metadata: The file "user.settings.bak" couldn't
be opened because you don't have permission to view it.
```

```
Error reading metadata: The file "user.settings.bak" couldn't
be opened because there is no such file.
```

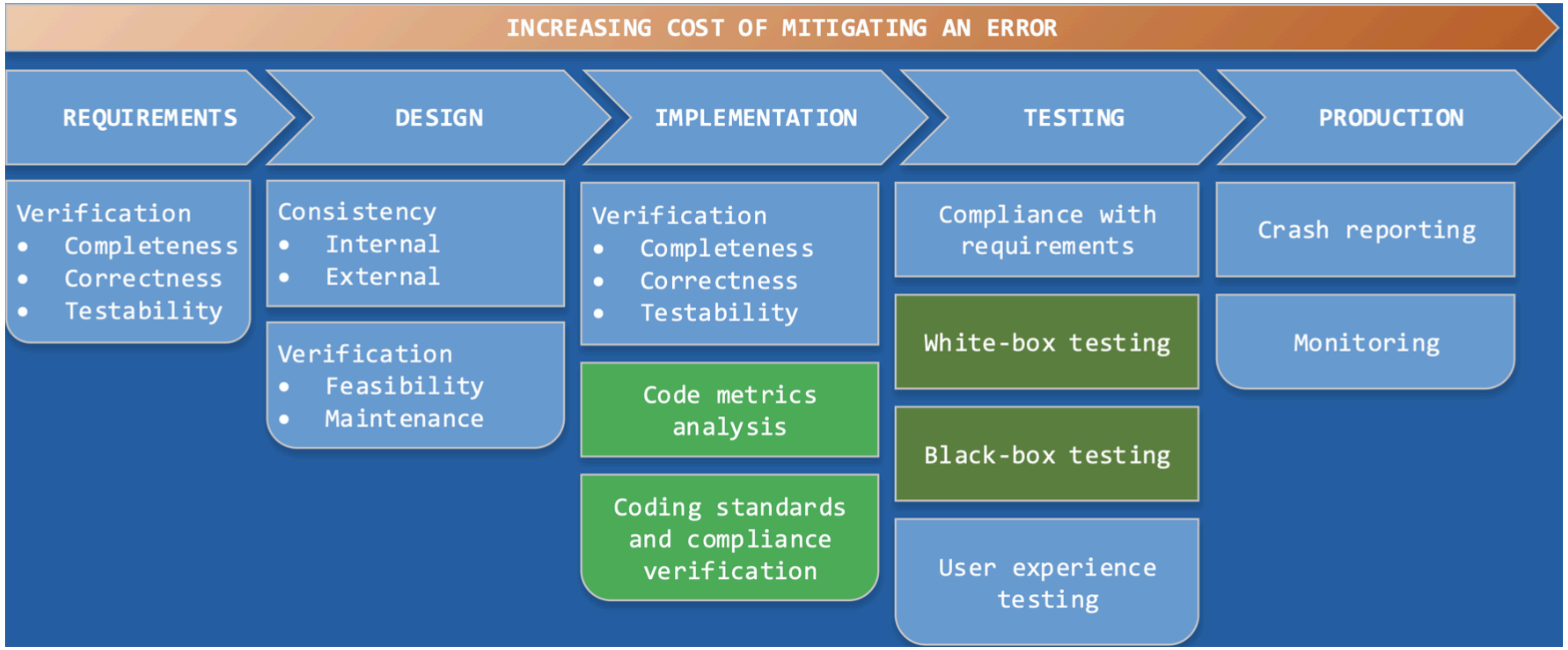
Computer Science
& Engineering
Department

PSCODING - PROACTIVE SECURE CODING FOR IOS APPLICATIONS (6)

POLITEHNICA
UNIVERSITATEA DIN BUCURESTI
1818

Objectives

- Static analysis
- Code verifier
- Best practices during implementation phase
- Swift programming language



INCREASING COST OF MITIGATING AN ERROR

REQUIREMENTS

Verification
- Completeness
- Correctness
- Testability

DESIGN

Consistency
- Internal
- External

Verification
- Feasibility
- Maintenance

IMPLEMENTATION

Verification
- Completeness
- Correctness
- Testability

Code metrics analysis

Coding standards and compliance verification

TESTING

Compliance with requirements

White-box testing

Black-box testing

User experience testing

PRODUCTION

Crash reporting

Monitoring

Issues Tackled

- Reference Cycle
- Use of NSUserDefaults instead of Keychain
- Sync Operation on Main Thread
- Use of NSCoding
- Access control (private/public variables)
- Unsecure communication (HTTP vs HTTPS)

Contributions (1)

- (1) Fuzzingster — Detecting and Analyzing Android Vulnerabilities in User Space
    - Method for finding vulnerabilities in Android Libraries
- (2) Fuzzing-KS — Detecting and Analyzing Vulnerabilities in Kernel Space
    - Method for finding vulnerabilities in Android/Linux Kernel
- (3) iOracle — Automated Evaluation of Access Control Policies in iOS
    - Created a Centralised Model for Apple policy System
    - Discover known and unknown policy flaws

Contributions (2)

- (4) SandTailor — Adding Custom Sandbox Profiles to iOS Applications
    - Improve Apple Sandbox System by enforcing a different sandbox profile to each application
- (5) Kobold — Evaluating Descentralized Access Control for Remote NSXPC Methods on iOS
    - Framework that discovers and invokes daemons’ methods via NSXPC
    - Confused deputy attacks; 3 CVEs
        - CVE-2019-8698: Block access to all websites
        - CVE-2019-8502: Activate microphone in dictation request
        - CVE-2018-4446: Leak File Provider information

Contributions (3)

- (6) PSCoding — Proactive Secure Coding for iOS Applications
  - Static analysis tool
  - Discover programming errors during implementation

Publications (1)

- C. Carabas and M. Carabas, "Fuzzing the Linux kernel," 2017 Computing Conference, 2017, pp. 839-843, doi: 10.1109/SAI.2017.8252193V. Corneci, C. Carabaş, R. Deaconescu and N. Ţăpuş, "Adding Custom Sandbox Profiles to iOS Apps," 2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet), 2019, pp. 1-5.

- A. Surdu, C. Carabas and M. Carabas, "Designing a Framwork for Creating CLIs," 2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet), 2018, pp. 1-6.

- M. Carabas, C. Carabas, L. Gheorghe, R. Deaconescu and N. Tapus, "Monitoring and auditing mobile operating systems." 2016 International Journal of Space-Based and Situated Computing, 6(1), 54-63, doi: 10.1504/IJSSC.2016.076571

- C. Carabas, I. Patru, M. Carabas, L. Gheorghe and N. Tapus, "Error Monitoring for Mobile Operating Systems," 2015 Ninth International Conference on Complex, Intelligent, and Software Intensive Systems, 2015, pp. 302-307, doi: 10.1109/CISIS.2015.42.

- C. Carabaș, N. ȚĂPUȘ, “Embedded Devices Overview: Does Security Match The Evolution Of Technology”. International Journal of Progressive Sciences and Technologies, [S.l.], v. 24, n. 1, p. 510-519, jan. 2021. ISSN 2509-0119.

- V. Zamfir, M. Carabas, C. Carabas and N. Tapus, "Systems Monitoring and Big Data Analysis Using the Elasticsearch System," 2019 22nd International Conference on Control Systems and Computer Science (CSCS), 2019.

Publications (2)

- L. Deshotels, C. Carabas, J. Beichler, R. Deaconescu and W. Enck, "Kobold: Evaluating Decentralized Access Control for Remote NSXPC Methods on iOS," 2020 IEEE Symposium on Security and Privacy (SP), 2020, pp. 1056-1070.
- V. Corneci, C. Carabaş, R. Deaconescu and N. Ţăpuş, "Adding Custom Sandbox Profiles to iOS Apps," 2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet), 2019, pp. 1-5.
- M. A. Marin, C. Carabas, R. Deaconescu and N. Tăpus, "Proactive Secure Coding for iOS Applications," 2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet), 2019, pp. 1-5.
- M. Carabas and C. Carabas. "Instruction caching for bhyve", 2019 In Proceedings of the 6th Conference on the Engineering of Computer Based Systems (ECBS '19). Association for Computing Machinery, New York, NY, USA, Article 17, 1–5.
- G. Mocanu, C. Carabaş and N. Ţăpuş, "Fuzz testing in AWS Firecracker hypervisor," 2021 20th International Symposium on Parallel and Distributed Computing (ISPDC), 2021, pp. 130-137, doi: 10.1109/ISPDC52870.2021.9521598.
- L. Deshotels, R. Deaconescu, C. Carabas, I. Manda, W. Enck, M. Chiroiu, N. Li, and A. Sadeghi, "IOracle: Automated Evaluation of Access Control Policies in iOS", 2018 In Proceedings of the 2018 on Asia Conference on Computer and Communications Security (ASIACCS ’18).

Thank you for your attention.

UNIVERSITATEA POLITEHNICA DIN BUCURESTI 1818

Computer Science
& Engineering
Department

costin.carabas@upb.ro

Backup slides

UNIVERSITATEA POLITEHNICA DIN BUCUREȘTI 1818

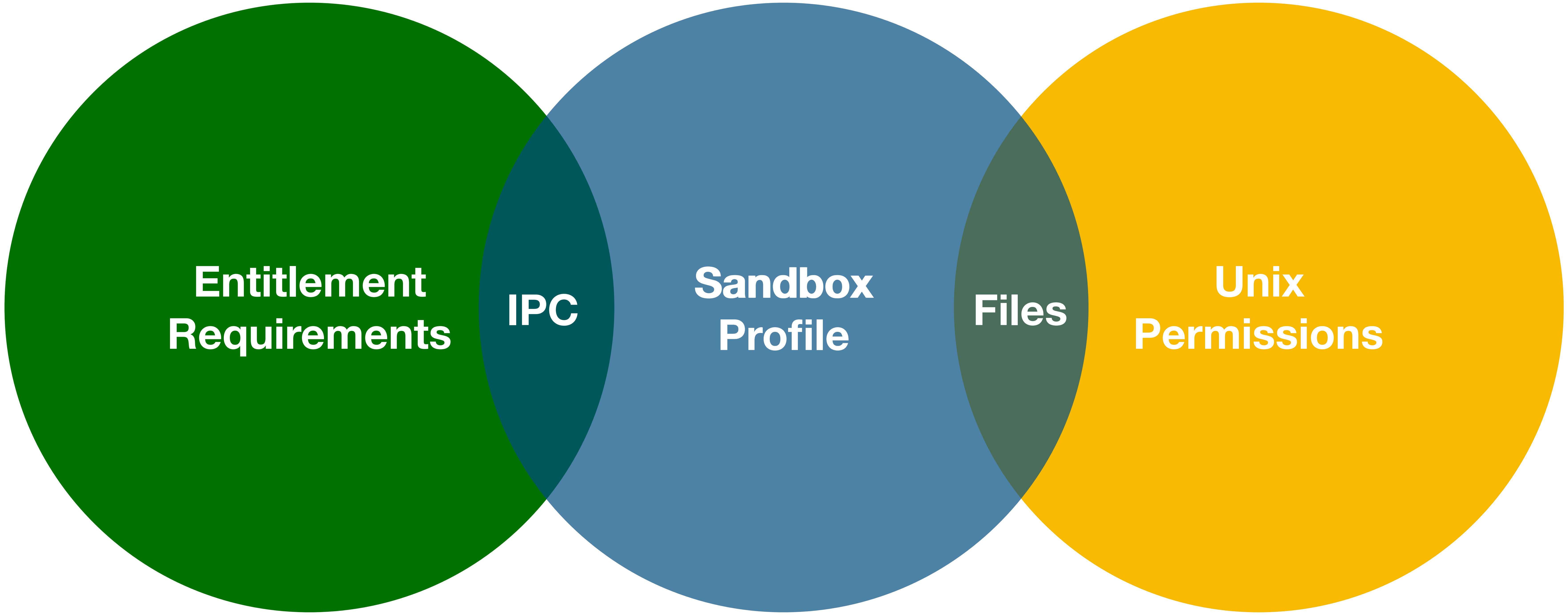
Computer Science
& Engineering
Department

iOracle -Prolog implementation

- Define tables of facts
  - parent(alice,bob)
  - parent(bob,charlie)
- Define rules that abstract those facts
  - grandparent(A,C):- parent(A,B), parent(B,C).
- Make queries about facts and rules
  - ?- grandparent(alice,X).

- Define tables of facts
  - allow(policy(unixPerm),process(Proc),operation(Op),file(File))
  - allow(policy(sandbox),process(Proc),operation(Op),file(File))
- Define rules that abstract those facts
  - access(process(Proc),operation(Op),file(File)):- allow(policy(sandbox),process(Proc),operation(Op),file(File)), allow(policy(unixPerm),process(Proc),operation(Op),file(File))
- Make queries about facts and rules
  - ?- access(process(X), operation("read"), file("/etc/passwd")).

Analysis of iOS Access Control



Entitlement Requirements

IPC

Sandbox Profile

Files

Unix Permissions

Kobold (IEEE S&P 2020)

SandScout (CCS 2016)

iOracle (AsiaCCS 2018)

iOracle -Data extraction

- Static data:
  - sandbox profiles
  - File Metadata and Unix Configurations
  - Program Attributes: symbols, code signatures
- Dynamic data: file changes, process accesses
  - File accessed
  - Process/File ownership
  - Sandbox Extensions