TU Graz

SCIENCE
PASSION
TECHNOLOGY

Kernel Security in the Wild:

Side-Channel-Assisted Exploit Techniques, Kernel-Level Defenses, and Real-World Analysis

Lukas Maar

September 26, 2025

PhD Defense

› isec.tugraz.at

Motivation

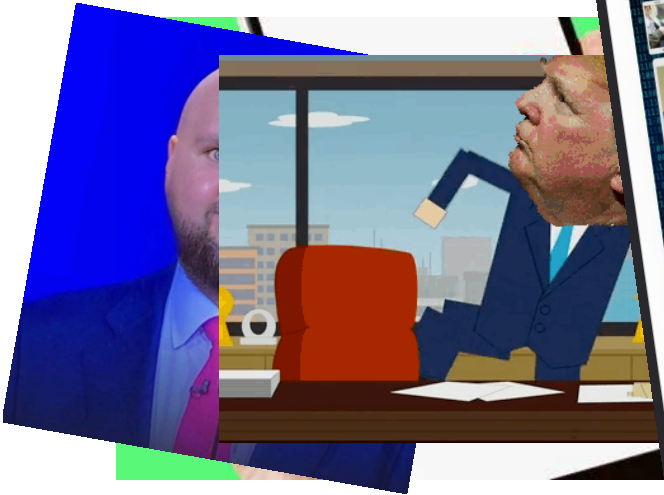
Motivation

Motivation

Motivation

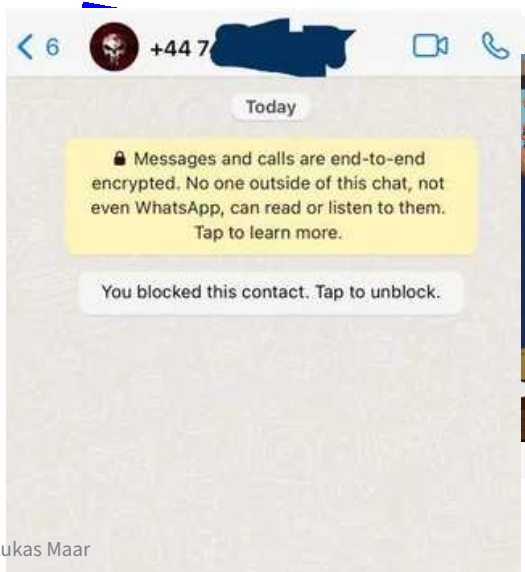
Motivation

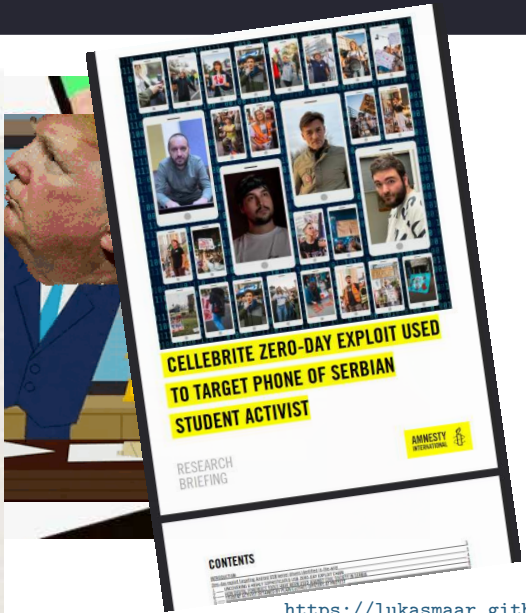
Motivation



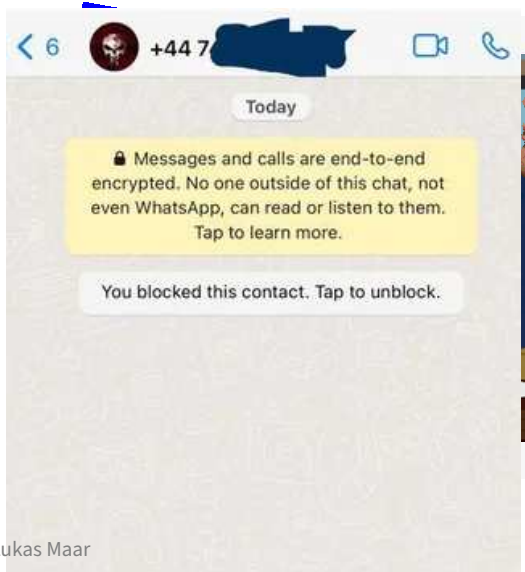
CELLEBRITE ZERO-DAY EXPLOIT USED TO TARGET PHONE OF SERBIAN STUDENT ACTIVIST
AMNESTY INTERNATIONAL
RESEARCH BRIEFING
CONTENTS

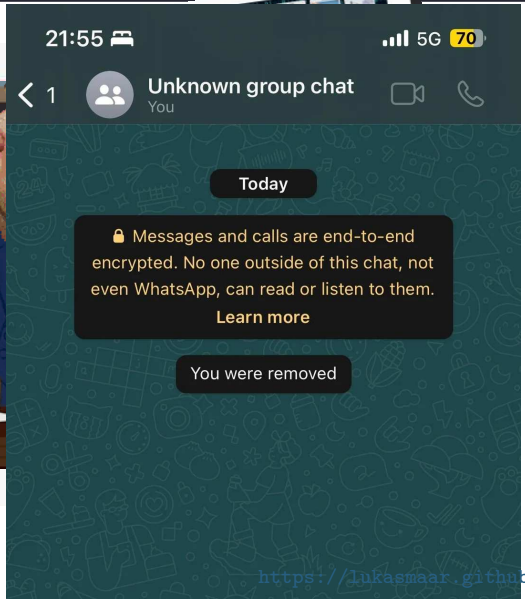
Motivation


6
+44 7
Today
Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.
You blocked this contact. Tap to unblock.

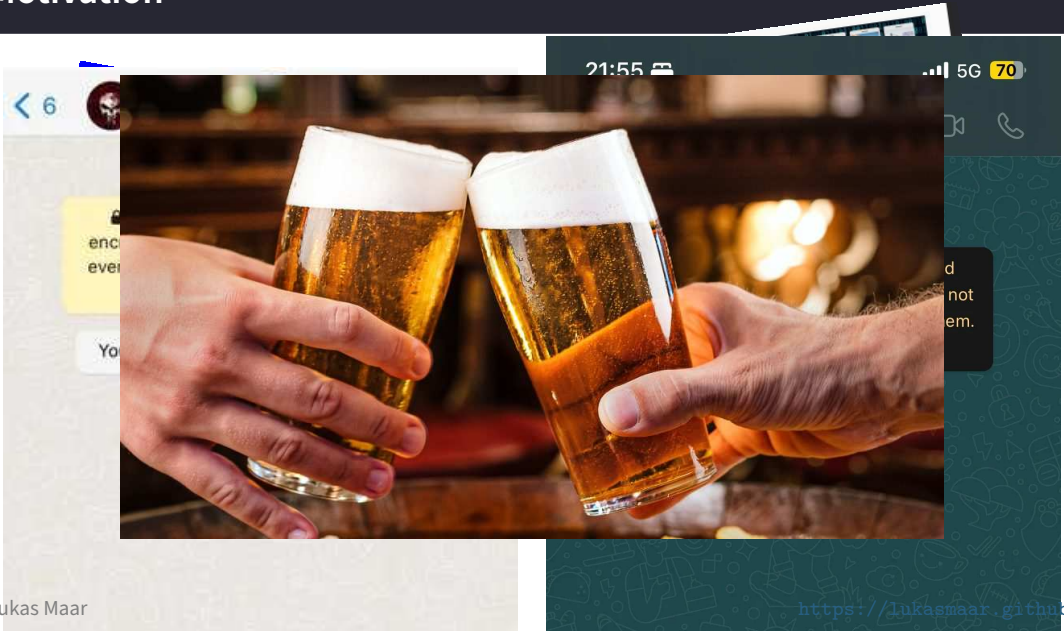

CELLEBRITE ZERO-DAY EXPLOIT USED TO TARGET PHONE OF SERBIAN STUDENT ACTIVIST
AMNESTY INTERNATIONAL
RESEARCH BRIEFING
CONTENTS

Motivation


6
+44 7
Today
Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.
You blocked this contact. Tap to unblock.


21:55
5G
70
1
Unknown group chat
You
Today
Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them.
Learn more
You were removed

Motivation



Motivation of Next Morning

Motivation of Next Morning

Motivation of Next Morning

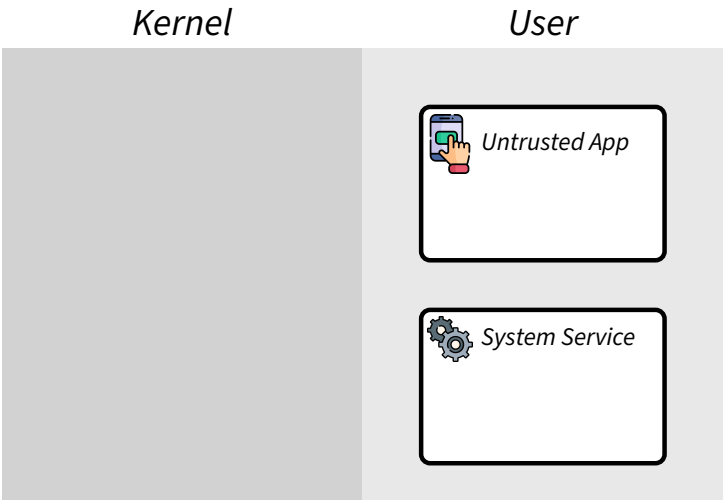
Motivation of Next Morning

Motivation of Next Morning

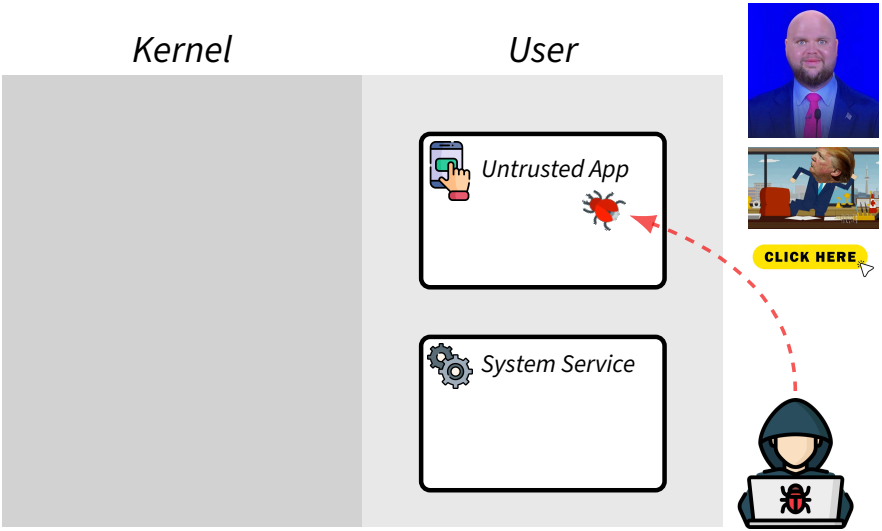
How to Exploit?

Kernel *User*

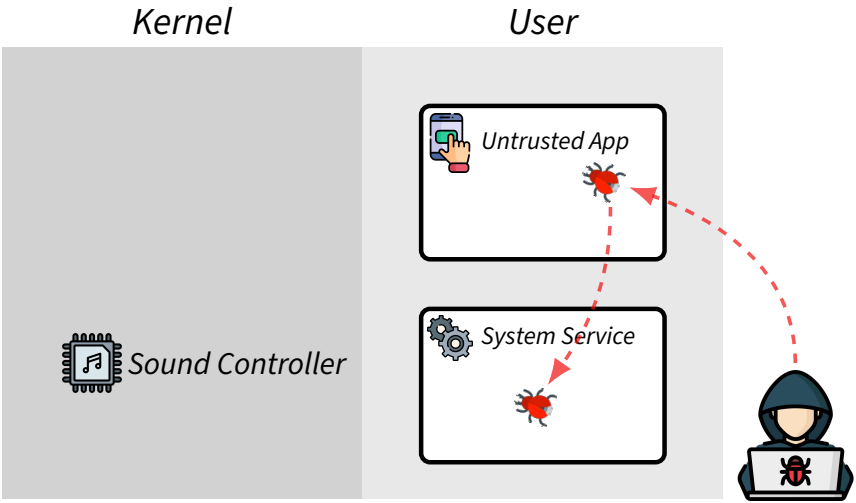
How to Exploit?



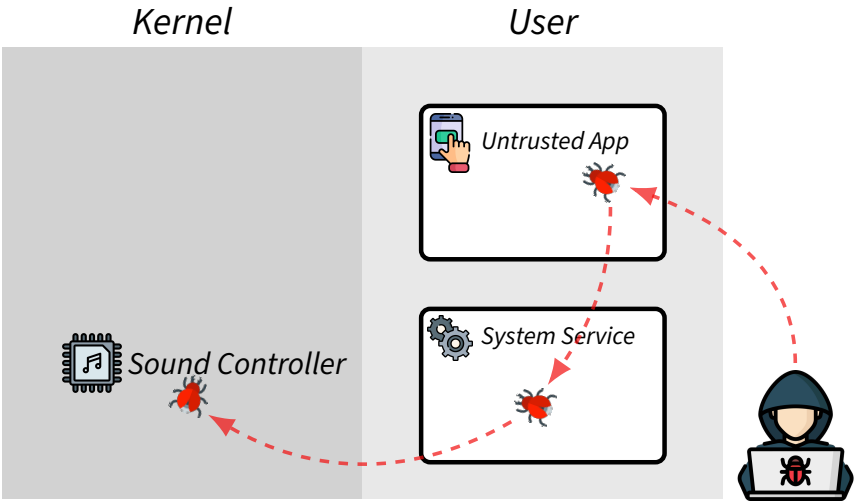
How to Exploit?



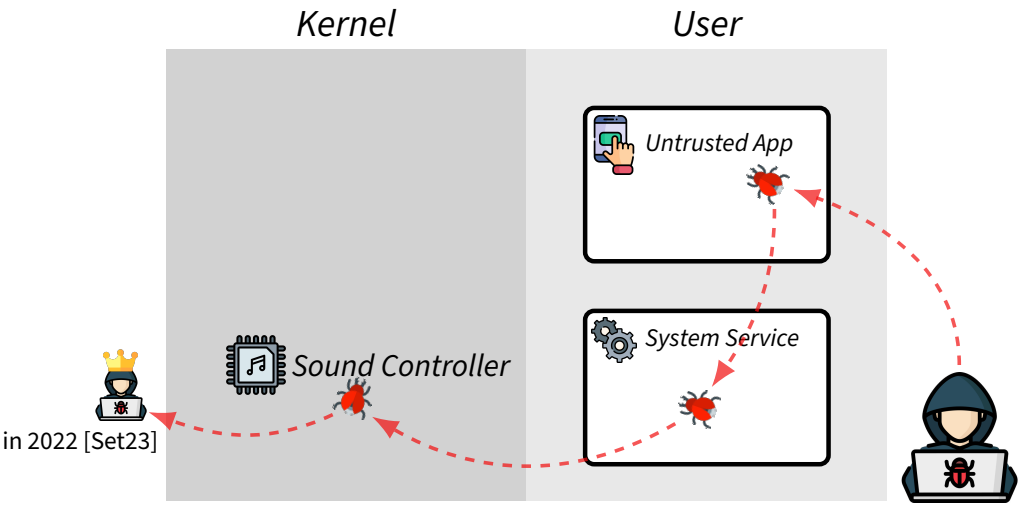
How to Exploit?



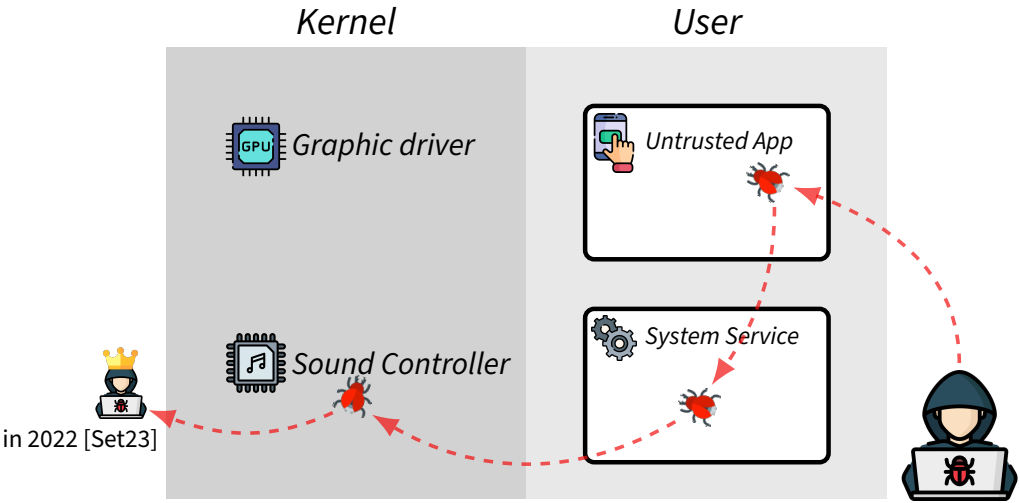
How to Exploit?



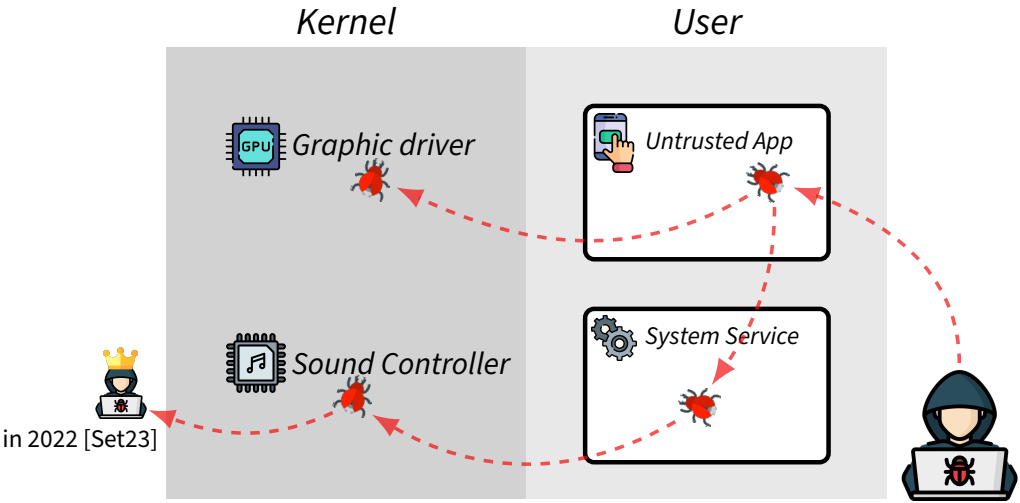
How to Exploit?



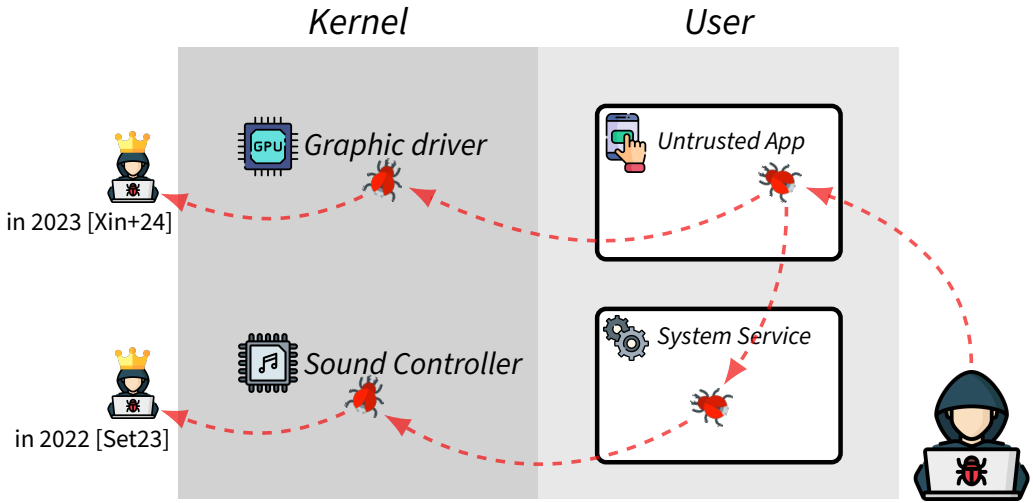
How to Exploit?



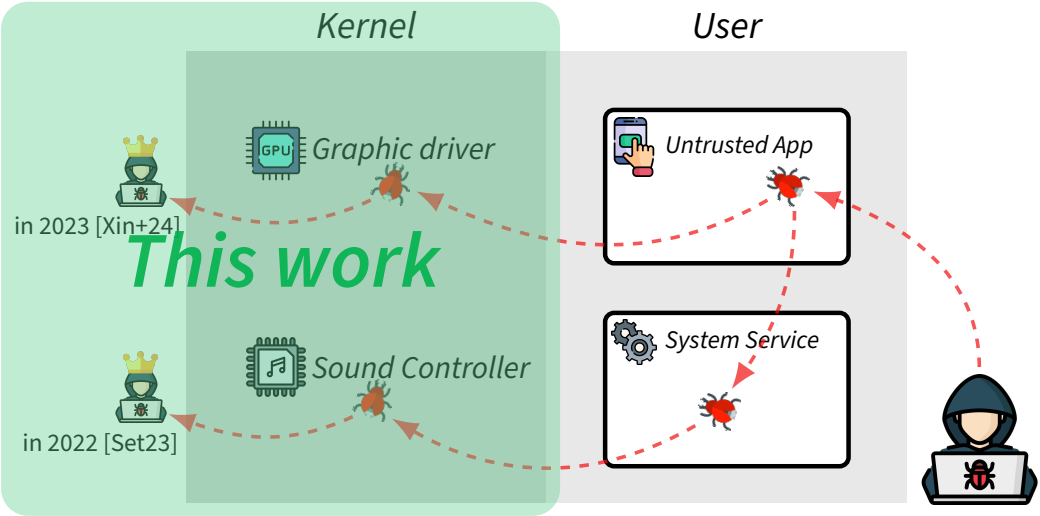
How to Exploit?



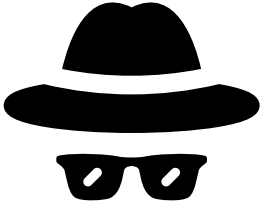
How to Exploit?



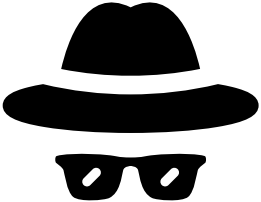
How to Exploit?



Threat Actor’s Goal



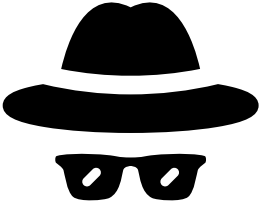
Threat Actor's Goal



- **Stealthy**

  Ensure exploits are reliable and undetected

Threat Actor's Goal

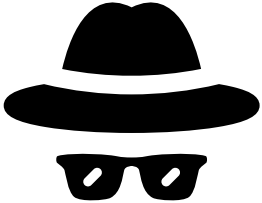


- **Stealthy**
  - Ensure exploits are reliable and undetected
- **Defenses**
  - Operate effectively despite security measures

Threat Actor's Goal

- **Stealthy**
  - Ensure exploits are reliable and undetected
- **Defenses**
  - Operate effectively despite security measures
- **Android Ecosystem**
  - Function across multiple devices

~~Threat Actor's~~ Defender's Goal



- **Stealthy**
  - Ensure exploits are reliable and undetected
- **Defenses**
  - Operate effectively despite security measures
- **Android Ecosystem**
  - Function across multiple devices

~~Threat Actor's~~ Defender's Goal

Stealthy

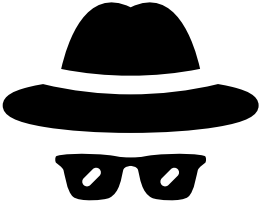
ed

usures

function across multiple devices

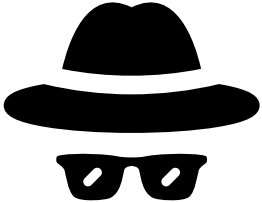
Make in-the-wild exploitation as hard as possible

My Main Contributions



- Stealthy
- Defenses
- Android Ecosystem

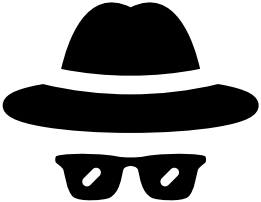
My Main Contributions



- **Stealthy**
  - *Enhance exploit reliability via side channels*
  - Goal: Push defender site
- **Defenses**

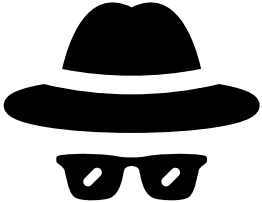
- **Android Ecosystem**

My Main Contributions



- **Stealthy**
  - *Enhance exploit reliability via side channels*
  - Goal: Push defender site
- **Defenses**
  - *Increase Defense Effectiveness*
  - Goal: Direct resiliance improvement
- **Android Ecosystem**

My Main Contributions



- **Stealthy**
  - *Enhance exploit reliability via side channels*
  - Goal: Push defender site
- **Defenses**
  - *Increase Defense Effectiveness*
  - Goal: Direct resiliance improvement
- **Android Ecosystem**
  - *Reveal Shortcomings in the Android Ecosystem*
  - Goal: Push vendors

Enhance Exploit Reliability via Side Channels

Systematization of my Kernel Side-Channel Contributions

Side Channel	Type	Target	Goal

Systematization of my Kernel Side-Channel Contributions

Side Channel	Type	Target	Goal
SLUBStick	Software	Slab allocator	Cross-cache reuse (heap manipulation)

Systematization of my Kernel Side-Channel Contributions

Side Channel	Type	Target	Goal
SLUBStick	Software	Slab allocator	Cross-cache reuse (heap manipulation)
KernelSnitch	Software	Kernel data structures	Leakage of heap object locations Covert channel Website fingerprinting

Systematization of my Kernel Side-Channel Contributions

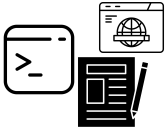
Side Channel	Type	Target	Goal
SLUBStick	Software	Slab allocator	Cross-cache reuse (heap manipulation)
KernelSnitch	Software	Kernel data structures	Leakage of heap object locations Covert channel Website fingerprinting
TLB disclosure	Hardware	TLB	Leakage of heap object locations Leakage of stack locations Leakage of page table locations

SLUBStick

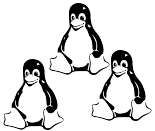
Kernel Memory Allocator

Kernel

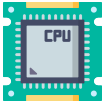
Applications



System Services



Hardware

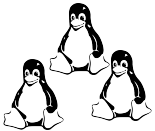


Kernel Memory Allocator

Kernel

Applications

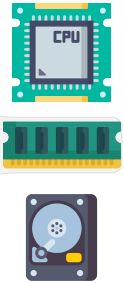
System Services



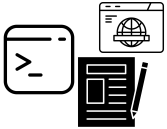
Slab

Buddy

Hardware

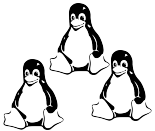


Kernel Memory Allocator



Applications

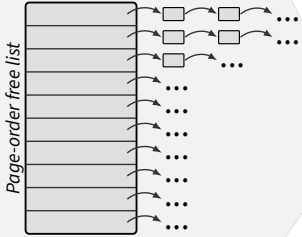
System Services



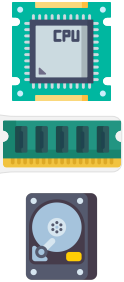
Kernel

Slab

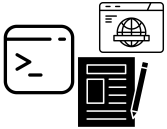
Buddy



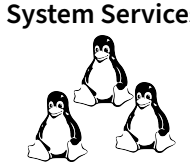
Hardware



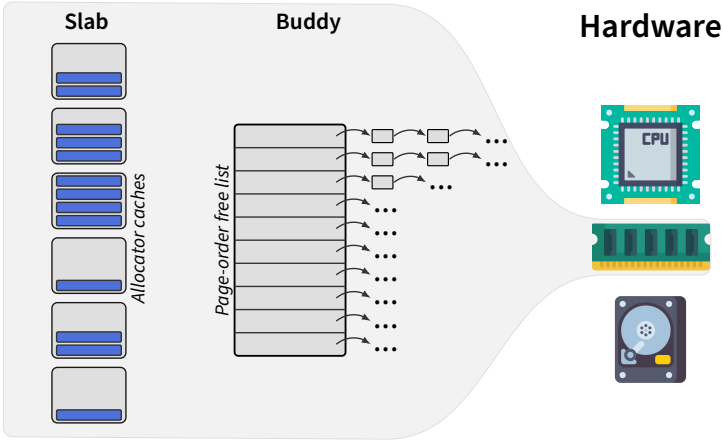
Kernel Memory Allocator



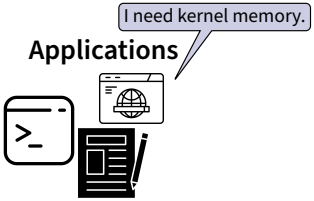
Applications

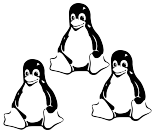


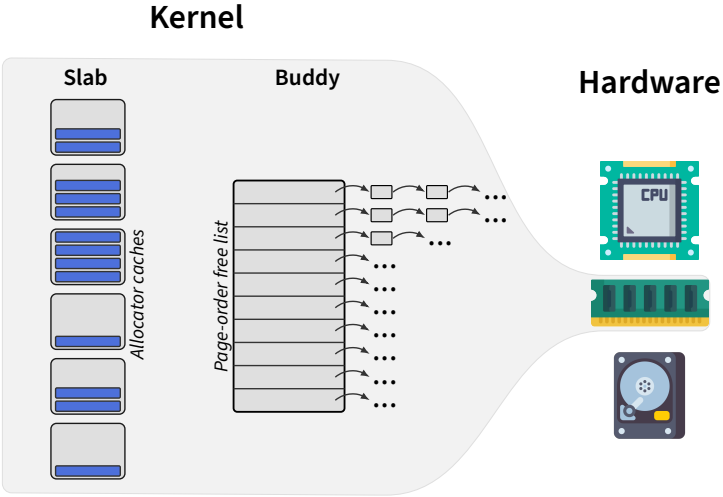
System Services



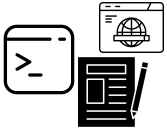
Kernel Memory Allocator



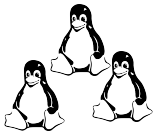




Kernel Memory Allocator



Applications

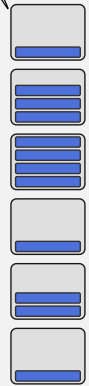


System Services

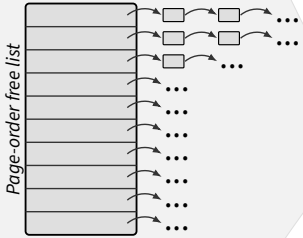
Kernel

Sure, here you go.

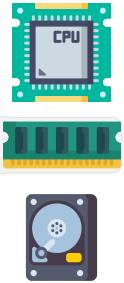
Slab



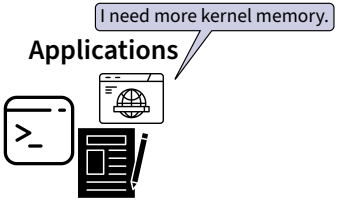
Buddy

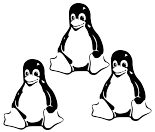


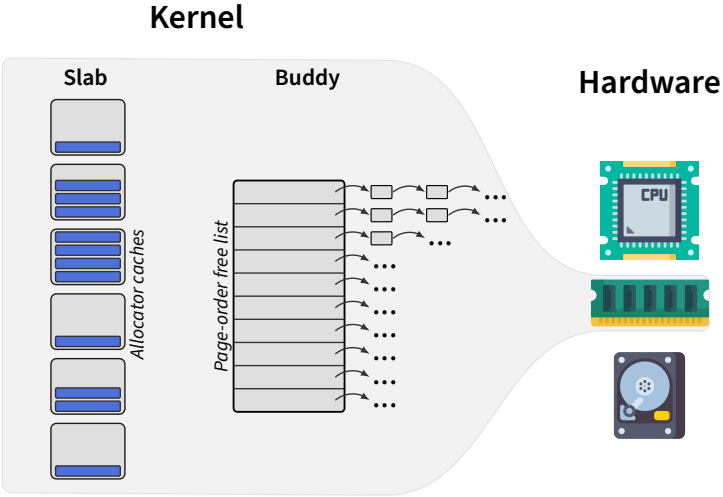
Hardware



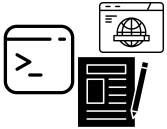
Kernel Memory Allocator





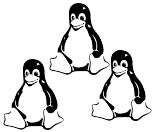


Kernel Memory Allocator

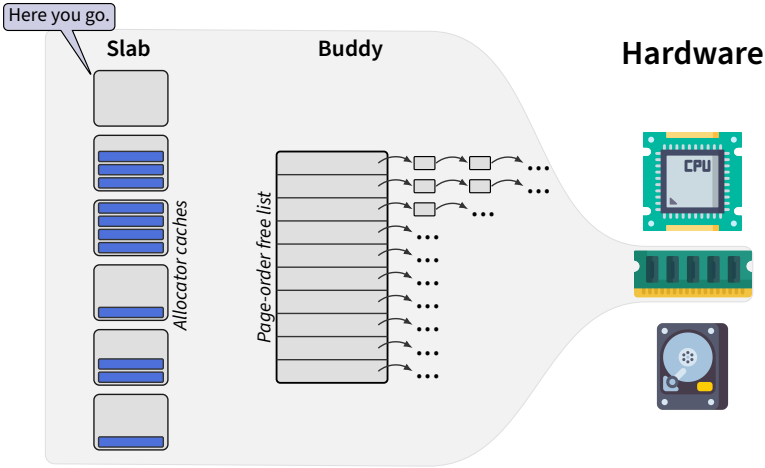


Applications

System Services

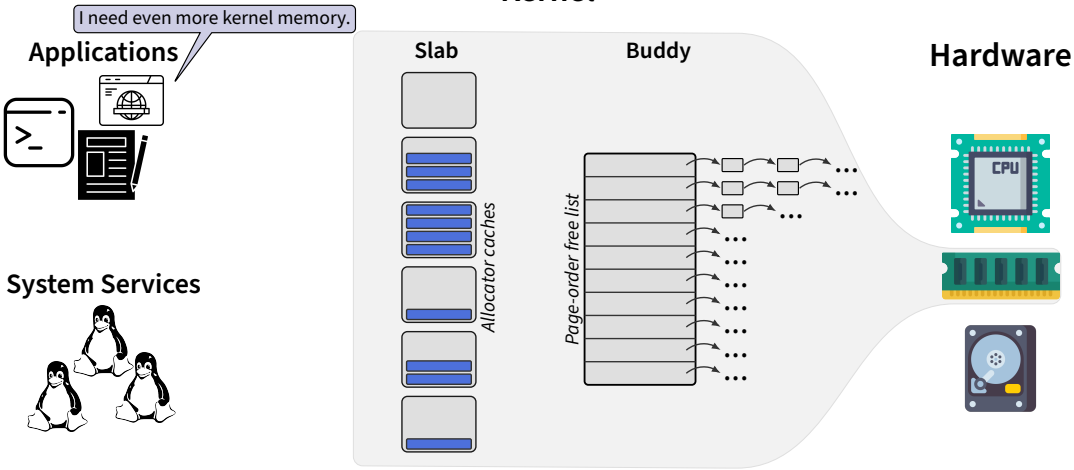


Kernel

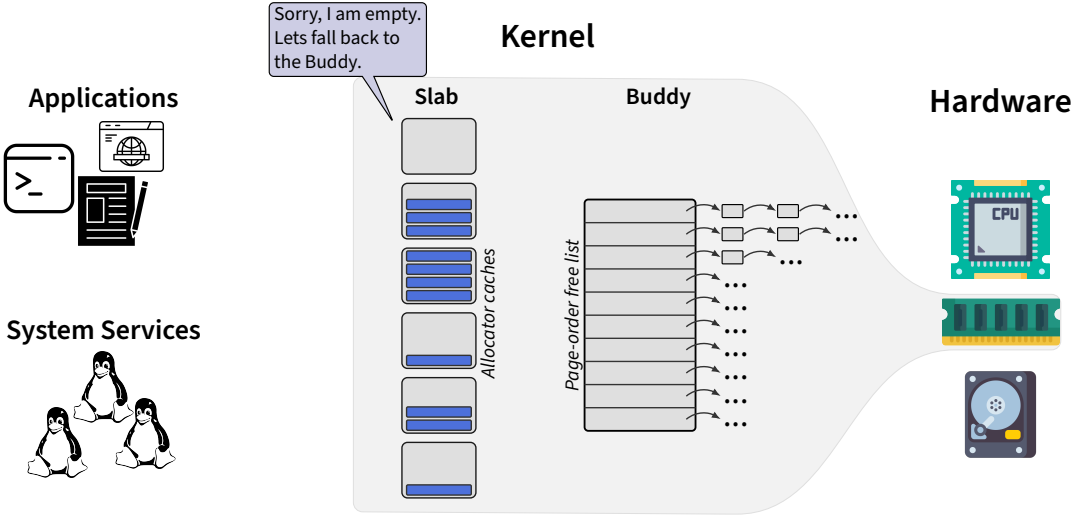


Hardware

Kernel Memory Allocator

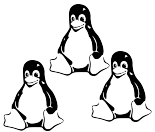


Kernel Memory Allocator

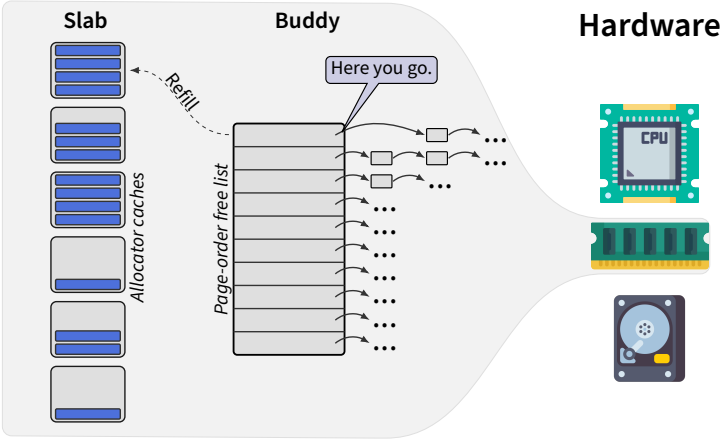


Kernel Memory Allocator

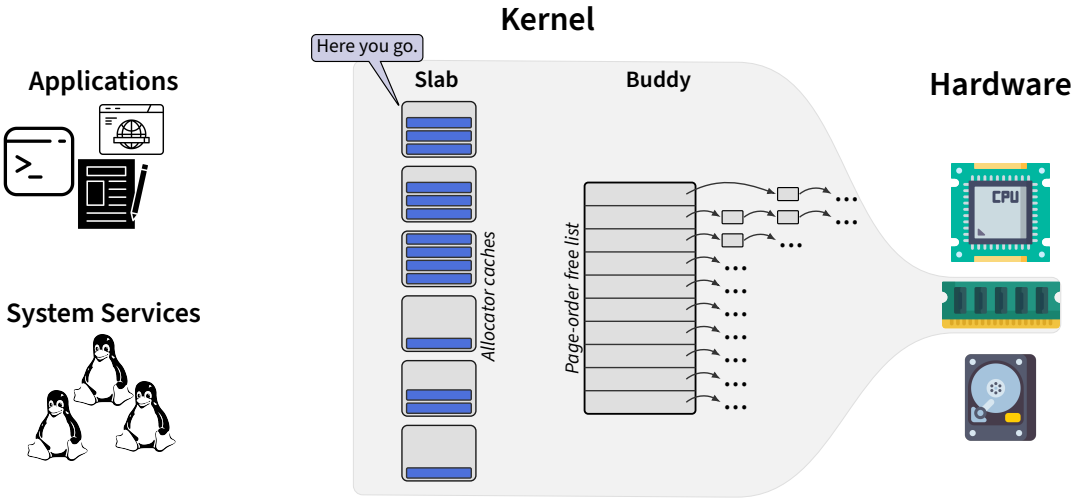
Applications



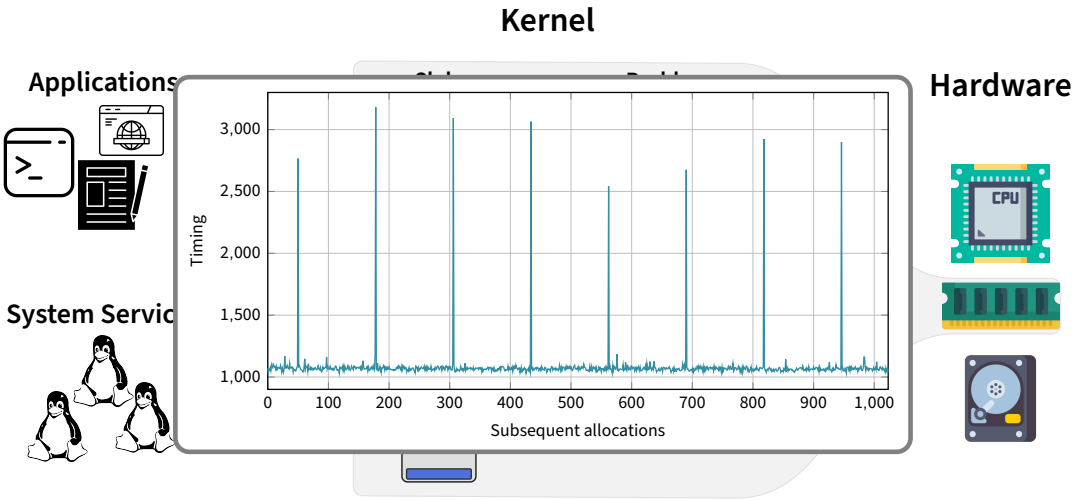
System Services



Kernel Memory Allocator



Kernel Memory Allocator



SLUBStick

Timing Allocator Side Channel:

- Measure syscall timing
- Increase reliability of heap manipulation

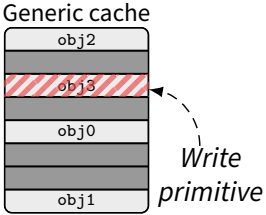
SLUBStick

- **Timing Allocator Side Channel:**
  - Measure syscall timing
  - Increase reliability of heap manipulation
- **Cross-Cache Reuse:**
  - Return slab page to buddy
  - Reclaim it for another object

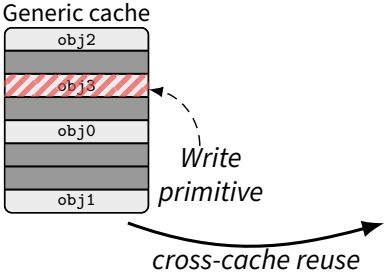
SLUBStick

- **Timing Allocator Side Channel:**
  - Measure syscall timing
  - Increase reliability of heap manipulation
- **Cross-Cache Reuse:**
  - Return slab page to buddy
  - Reclaim it for another object
- **High Reliability:**
  - $\geq$ 99.2 % for single slab pages

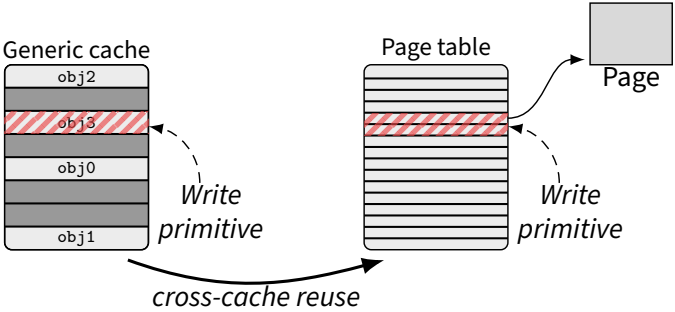
Cross-Cache Reuse to Arbitrary Read and Write



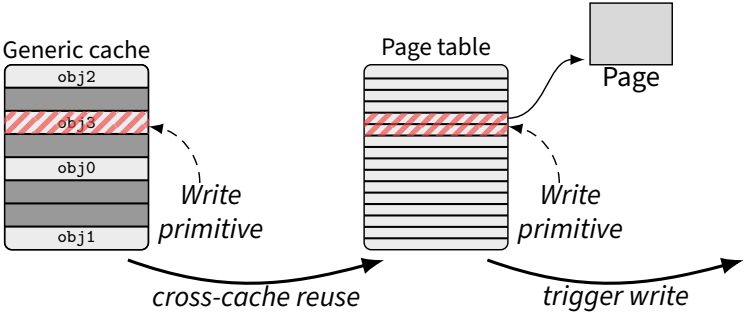
Cross-Cache Reuse to Arbitrary Read and Write



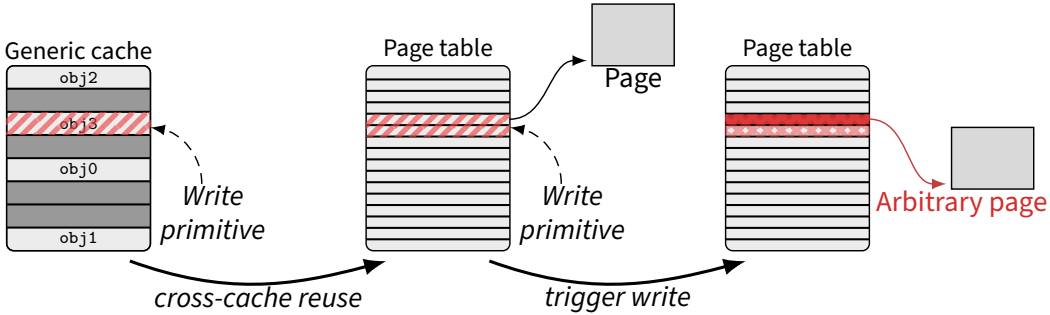
Cross-Cache Reuse to Arbitrary Read and Write



Cross-Cache Reuse to Arbitrary Read and Write



Cross-Cache Reuse to Arbitrary Read and Write



KernelSnitch

Linked List Access Timings

Empty list

List with
2 elements

List with
5 elements

Linked List Access Timings

Empty list

List with
2 elements

List with
5 elements

Fast access

Linked List Access Timings

Empty list

List with
2 elements

List with
5 elements

Fast access

Medium fast access

Linked List Access Timings

Empty list

List with
2 elements

List with
5 elements

Fast access

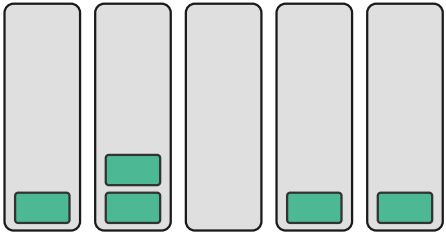
Medium fast access

Slow access

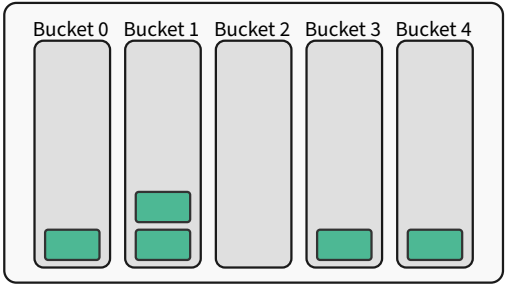
Hash Table Access Timings

Hash Table Access Timings

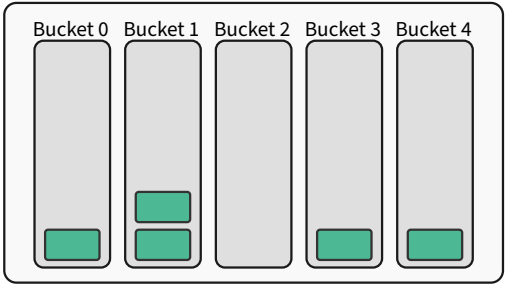
Hash Table Access Timings



Hash Table Access Timings

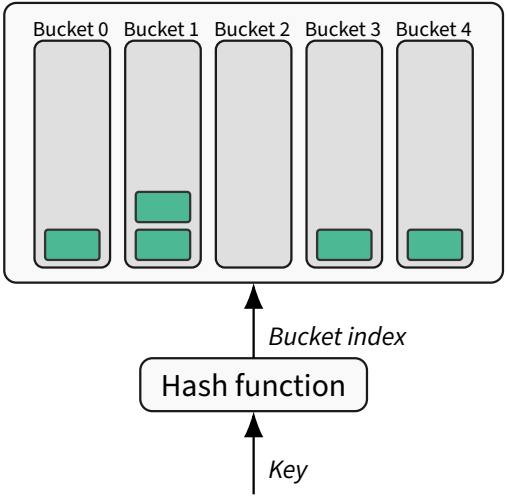


Hash Table Access Timings

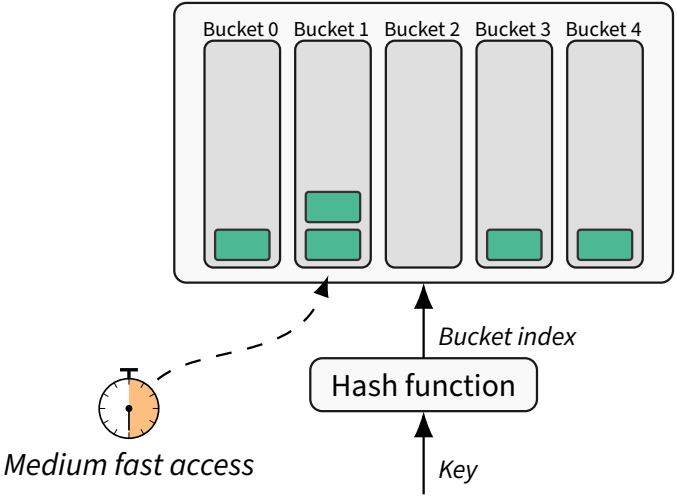


Hash function

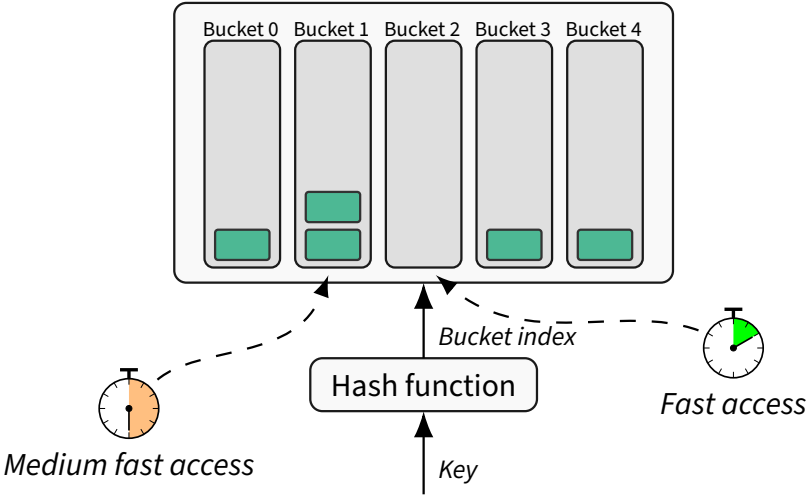
Hash Table Access Timings



Hash Table Access Timings



Hash Table Access Timings



Timing Histogram

Syscall $\rightarrow$ performs bucket access

Timing Histogram

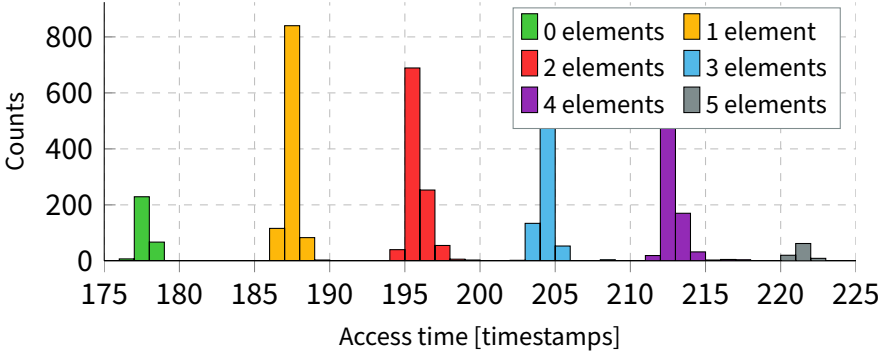
Syscall $\rightarrow$ performs bucket access

- Measure syscall timing
- Buckets between 0 and 5 elements

Timing Histogram

Syscall → performs bucket access

- Measure syscall timing
- Buckets between 0 and 5 elements



KernelSnitch

Covert Channel:

- *Sender:* Adjust occupancy level
  Receiver: Probes occupancy level

Covert Channel:

- *Sender:* Adjust occupancy level
  Receiver: Probes occupancy level
- Results: Up to 580 $\mathrm{kbit\,s^{-1}}$

KernelSnitch

Covert Channel:

- *Sender:* Adjust occupancy level
  Receiver: Probes occupancy level
- Results: Up to 580 $\mathrm{kbit\,s^{-1}}$

Website Fingerprinting:

- *Browser:* Adjust occupancy levels
  Spy: Probes occupancy levels

KernelSnitch

Covert Channel:

- *Sender:* Adjust occupancy level
  Receiver: Probes occupancy level
- Results: Up to 580 $\mathrm{kbit\,s^{-1}}$

Website Fingerprinting:

- *Browser:* Adjust occupancy levels
  Spy: Probes occupancy levels
- Results: F_1 of 89.3 %

KernelSnitch

Covert Channel:

- *Sender:* Adjust occupancy level
  Receiver: Probes occupancy level
- Results: Up to 580 $\mathrm{kbit\,s^{-1}}$

Website Fingerprinting:

- *Browser:* Adjust occupancy levels
  Spy: Probes occupancy levels
- Results: F_1 of 89.3 %

Kernel Heap Location Disclosure:

- Exploiting kernel's hash table indexing

KernelSnitch

Covert Channel:

- *Sender:* Adjust occupancy level
  Receiver: Probes occupancy level
- Results: Up to 580 $\mathrm{kbit\,s^{-1}}$

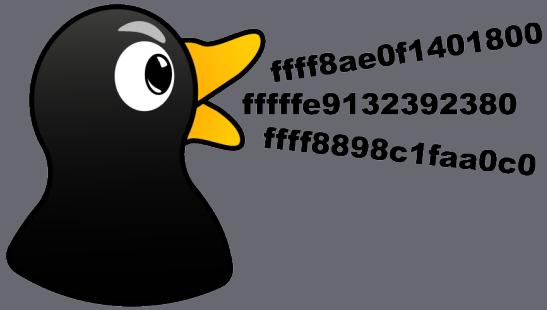
Website Fingerprinting:

- *Browser:* Adjust occupancy levels
  Spy: Probes occupancy levels
- Results: F_1 of 89.3 %

Kernel Heap Location Disclosure:

- Exploiting kernel's hash table indexing
- Results: Disclosure in under one minute

TLB Disclosure



Address Translation

virtual address:

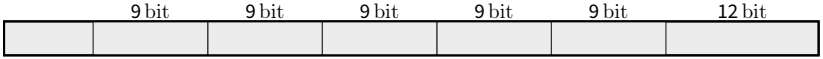
Address Translation

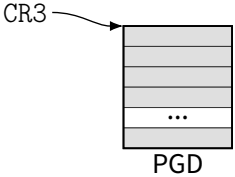
virtual address:

	9 bit	9 bit	9 bit	9 bit	9 bit	12 bit

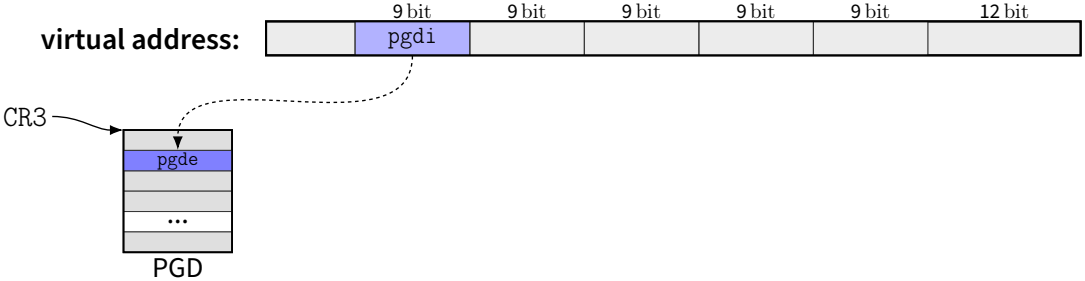
Address Translation

virtual address:

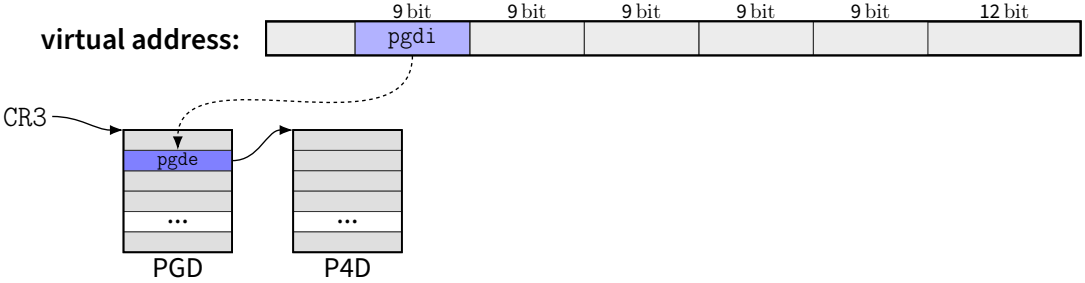




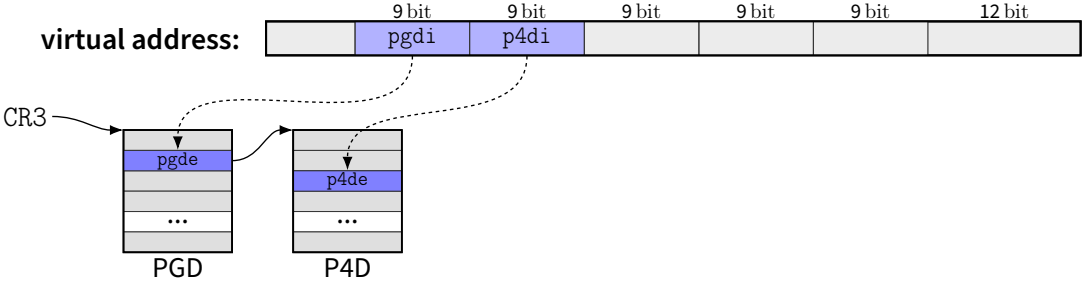
Address Translation



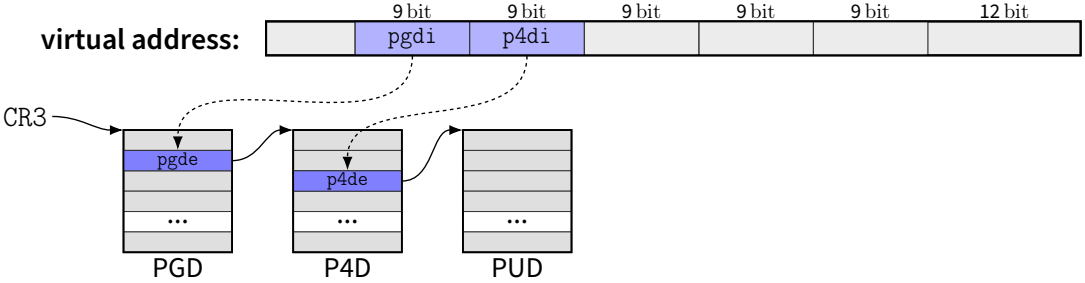
Address Translation



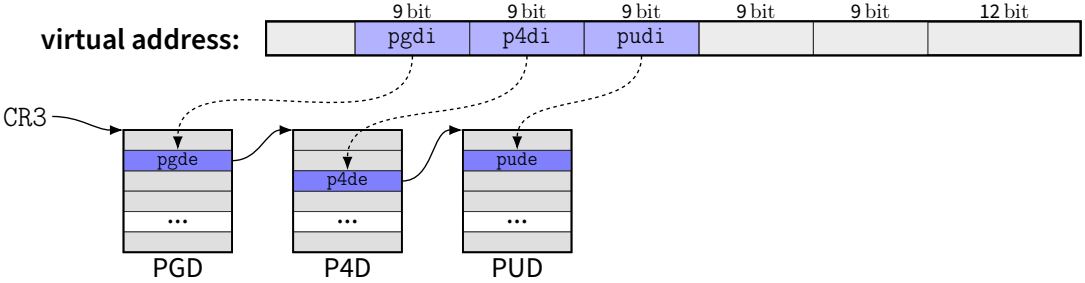
Address Translation



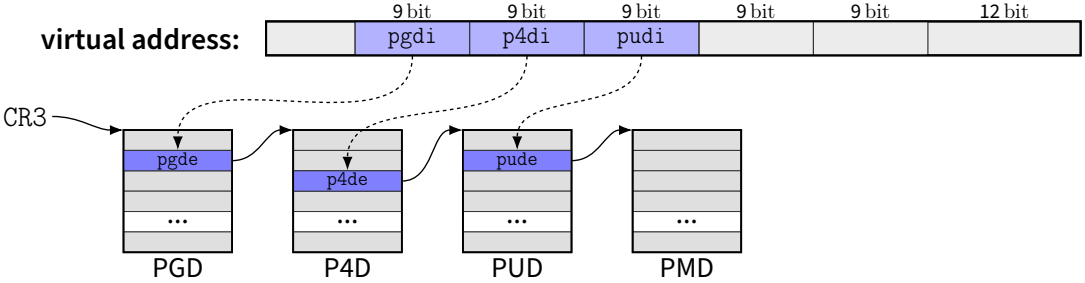
Address Translation



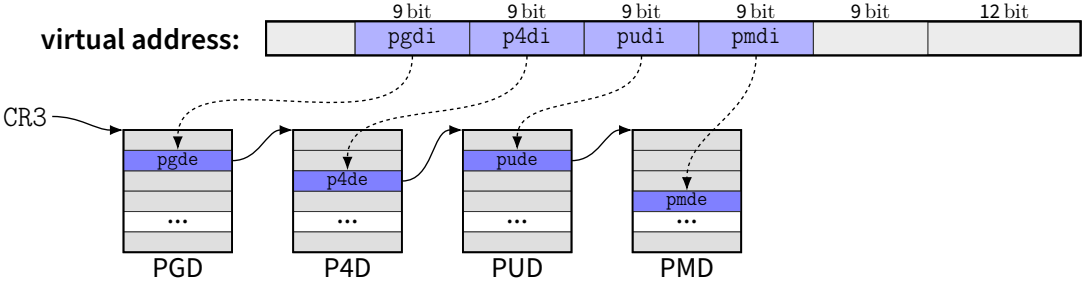
Address Translation



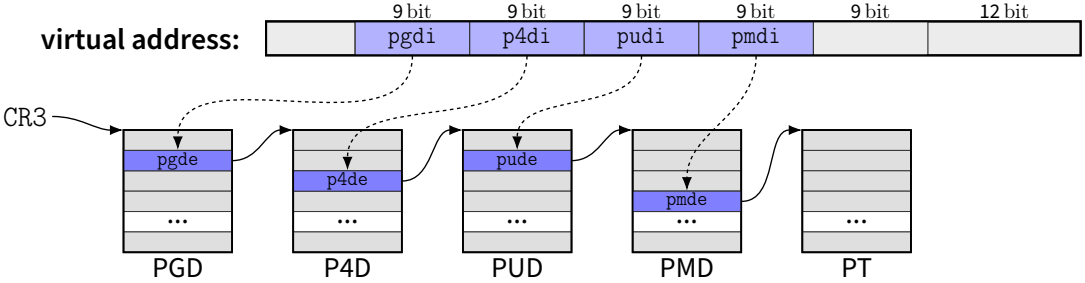
Address Translation



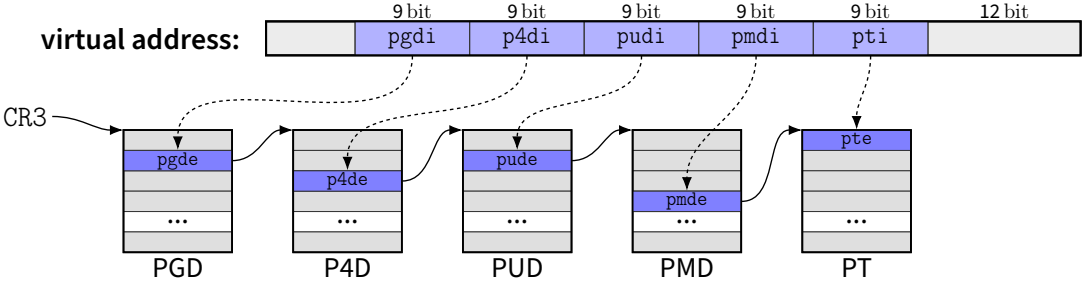
Address Translation



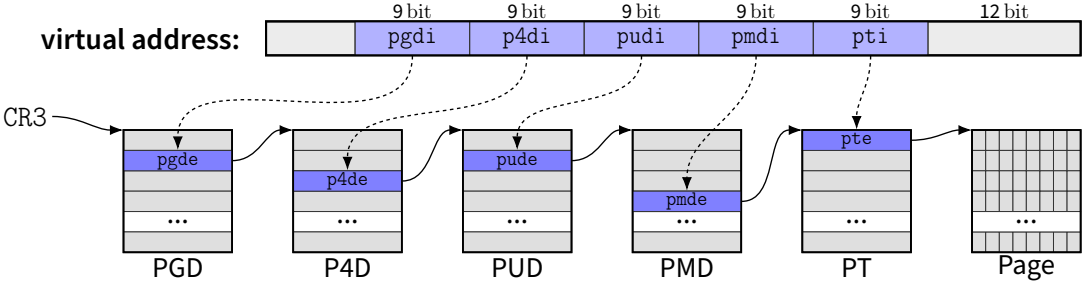
Address Translation



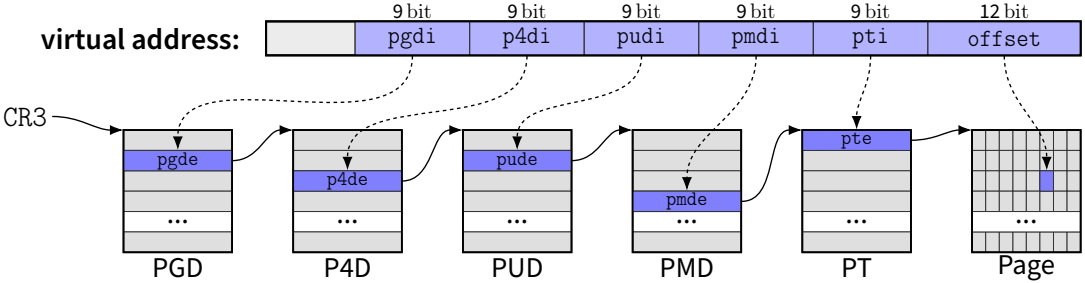
Address Translation



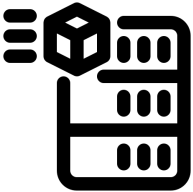
Address Translation



Address Translation

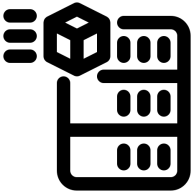


Translation Lookaside Buffer



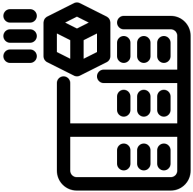
- Each page-table access → memory fetch
  - Slow!

Translation Lookaside Buffer



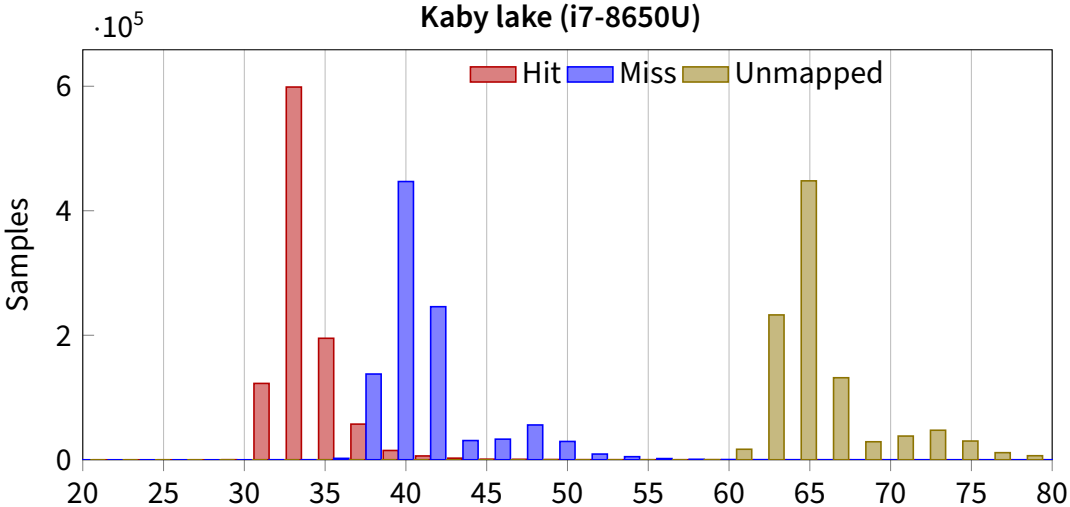
- Each page-table access → memory fetch
  - Slow!
- TLB
  - CPU cache
  - Stores page-table entries

Translation Lookaside Buffer

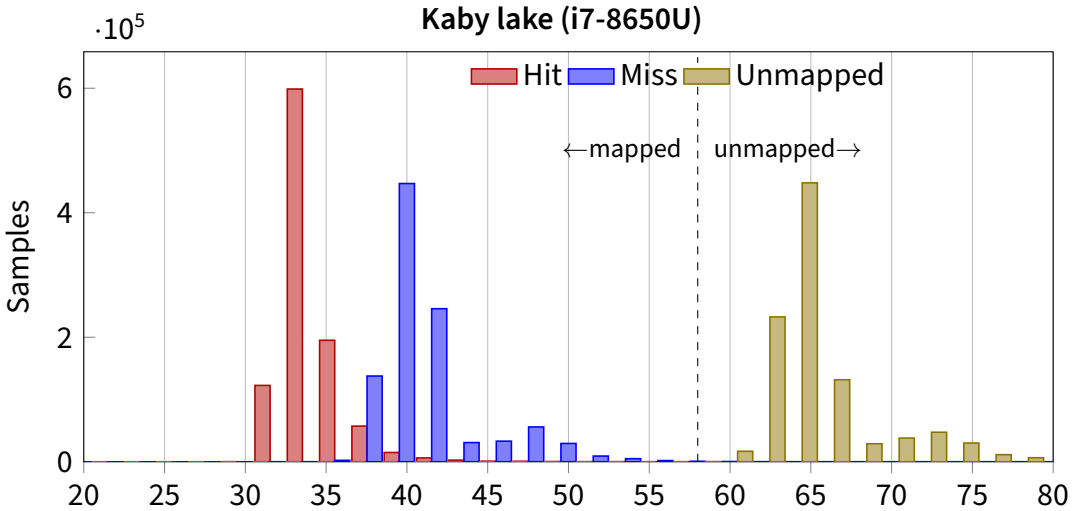


- Each page-table access → memory fetch
  - Slow!
- TLB
  - CPU cache
  - Stores page-table entries
- Faster!

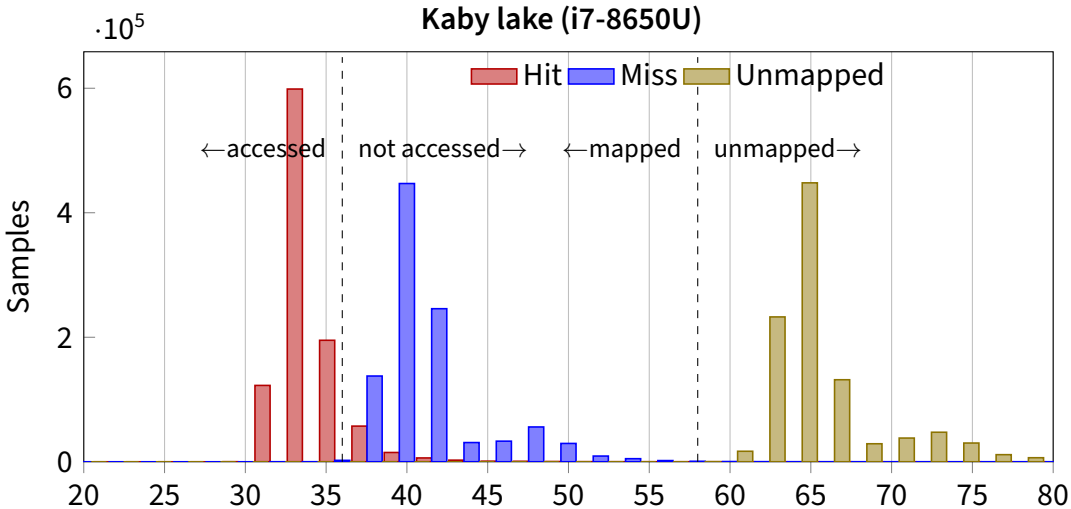
TLB Timing Histogram



TLB Timing Histogram

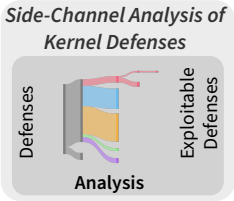


TLB Timing Histogram



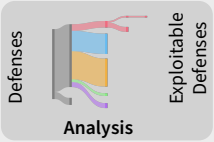
Advanced TLB Side Channel

Advanced TLB Side Channel



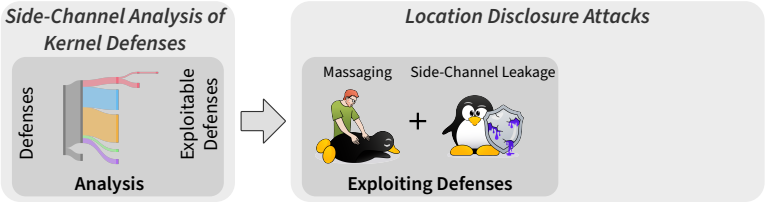
Advanced TLB Side Channel

Side-Channel Analysis of Kernel Defenses

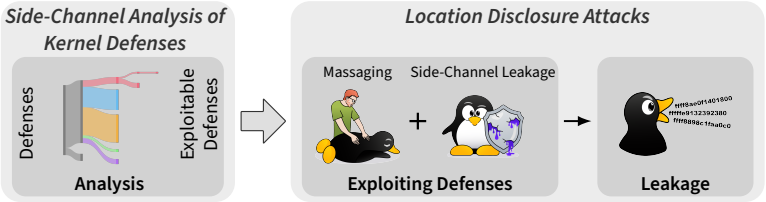


Location Disclosure Attacks

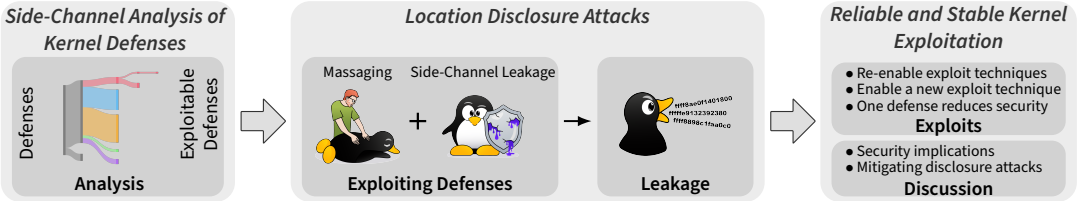
Advanced TLB Side Channel



Advanced TLB Side Channel



Advanced TLB Side Channel



Advanced TLB Side Channel Results

Advanced TLB Side Channel Results

- **Analysis:**
  - Virtualization of the kstack
  - Virtualization of the kheap
  - Strict memory permission enforcement

Advanced TLB Side Channel Results

- **Analysis:**
  - Virtualization of the kstack
  - Virtualization of the kheap
  - Strict memory permission enforcement
  - Additional allocator design decisions

Advanced TLB Side Channel Results

- **Analysis:**
  - Virtualization of the kstack
  - Virtualization of the kheap
  - Strict memory permission enforcement
  - Additional allocator design decisions
- **Evaluation:**
  - Intel CPUs from 8th to 14th gen
  - Generic Ubuntu kernels from v5.15 to 6.8

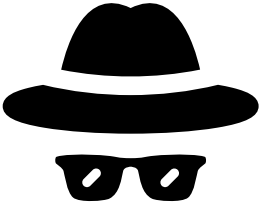
Advanced TLB Side Channel Results

- **Analysis:**
  - Virtualization of the kstack
  - Virtualization of the kheap
  - Strict memory permission enforcement
  - Additional allocator design decisions
- **Evaluation:**
  - Intel CPUs from 8th to 14th gen
  - Generic Ubuntu kernels from v5.15 to 6.8
- **Results:**
  - Three side-channel-assisted exploit techniques
  - Near 100 % reliability
  - No system crashes

Increase Defense Effectiveness

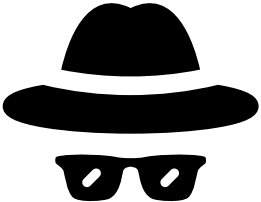
Attack Strategies

Attack Strategies



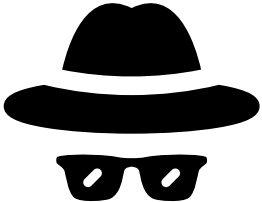
- **Control-Flow Hijacking Attacks:**

Attack Strategies



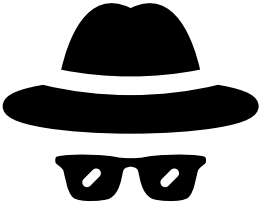
- **Control-Flow Hijacking Attacks:**
  - Manipulates control data
    - *such as function pointers*
  - Goal: Arbitrary code execution in the kernel

Attack Strategies



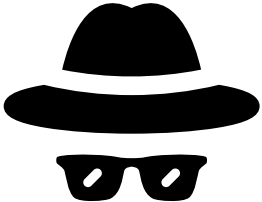
- **Control-Flow Hijacking Attacks:**
  Manipulates control data
  such as function pointers
  Goal: Arbitrary code execution in the kernel
- **Data-Oriented Attacks:**

Attack Strategies



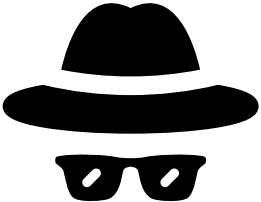
- **Control-Flow Hijacking Attacks:**
  - Manipulates control data
    - *such as function pointers*
  - Goal: Arbitrary code execution in the kernel
- **Data-Oriented Attacks:**
  - Manipulates non-control data
    - *such as data pointers*
  - Goal: Arbitrary read/write to kernel memory

~~Attack~~ Defense Strategies



- **Control-Flow Hijacking Attacks:**
  - Manipulates control data
    - *such as function pointers*
  - Goal: Arbitrary code execution in the kernel
- **Data-Oriented Attacks:**
  - Manipulates non-control data
    - *such as data pointers*
  - Goal: Arbitrary read/write to kernel memory

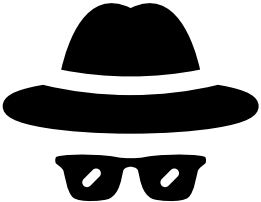
~~Attack~~ Defense Strategies



- **Control-Flow Hijacking Attacks:**
  - Manipulates data
    - *such as data pointers*
  - Goal: Arbitrary code execution in the kernel
- **Data-Oriented Attacks:**
  - Manipulates non-control data
    - *such as data pointers*
  - Goal: Arbitrary read/write to kernel memory

HEK-CFI

~~Attack~~ Defense Strategies

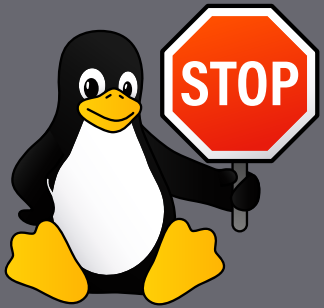


- **Control-Flow Hijacking Attacks:**
  - Manipulat ta
    - *su ters*
  - Goal: Ar code execution in the kernel
- **Data-Oriented Attacks:**
  - Manipula trol data
    - *such rs*
  - Goal: Arbit read/write to kernel memory

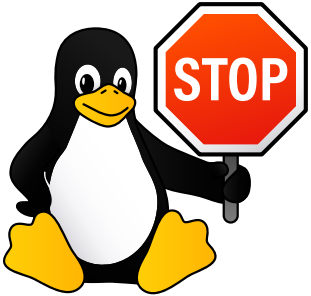
HEK-CFI

DOPE

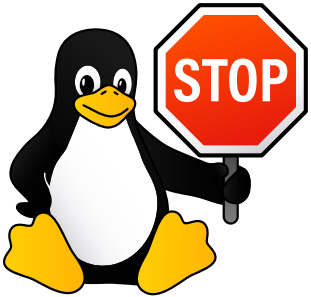
HEK-CFI



HEK-CFI

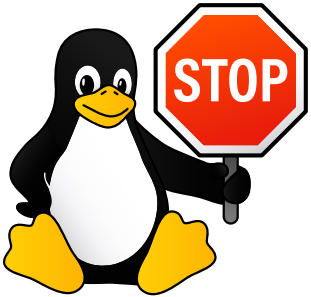


HEK-CFI



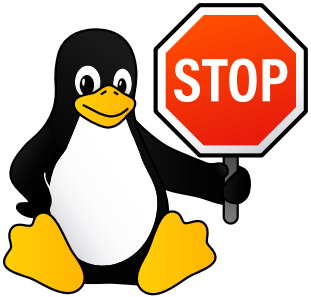
- **Hardware-Enforced Kernel Control-Flow Integrity:**
  - Intel CET, i.e., FineIBT and shadow stack
  - Safe areas

HEK-CFI



- **Hardware-Enforced Kernel Control-Flow Integrity:**
  - Intel CET, i.e., FineIBT and shadow stack
  - Safe areas
- **Protects Control Data:**
  - Function pointers, operation table pointers and return addresses
  - CPU registers during system events

HEK-CFI

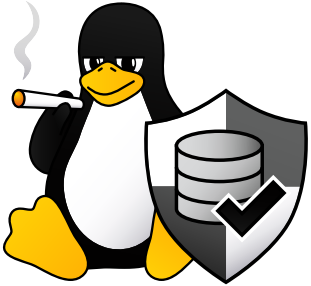


- **Hardware-Enforced Kernel Control-Flow Integrity:**
  - Intel CET, i.e., FineIBT and shadow stack
  - Safe areas
- **Protects Control Data:**
  - Function pointers, operation table pointers and return addresses
  - CPU registers during system events
- **POC:**
  - Linux kernel 5.18 with compiler pass
  - $\approx$ 1.85 % overhead

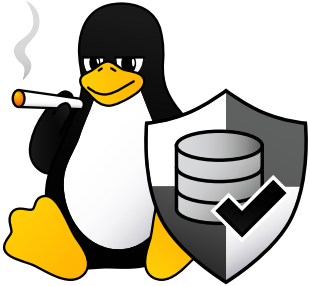
STOP

DOPE

DOPE

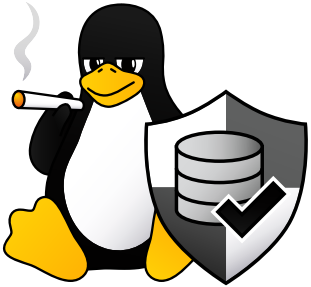


DOPE



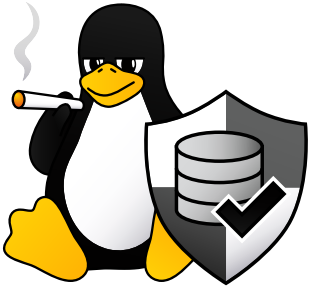
- **DOmain Protection Enforcement:**
  - Memory Protection Keys, i.e., Intel PKS
  - Principle of least privilege

DOPE



- **DOmain Protection Enforcement:**
  - Memory Protection Keys, i.e., Intel PKS
  - Principle of least privilege
- **Protects Non-Control Data:**
  - Credentials, page tables, ...

DOPE

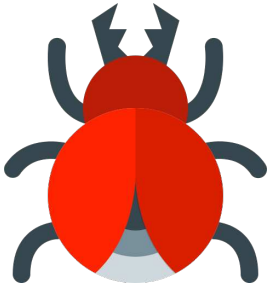


- **DOmain Protection Enforcement:**
  - Memory Protection Keys, i.e., Intel PKS
  - Principle of least privilege
- **Protects Non-Control Data:**
  - Credentials, page tables, ...
- **POC:**
  - Linux kernel 5.19 with compiler pass
  - $\approx$ 2.3 % overhead

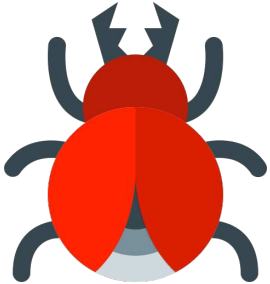
STOP

Reveal Shortcomings in the Android Ecosystem

In-the-Wild Exploits

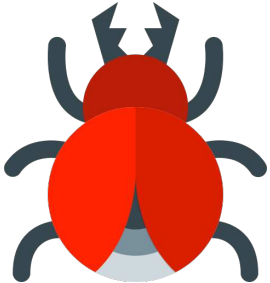


In-the-Wild Exploits



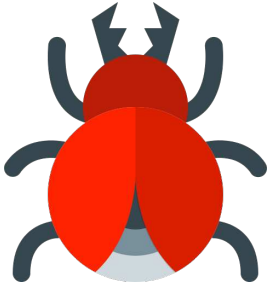
- Exploit vulnerabilities

In-the-Wild Exploits



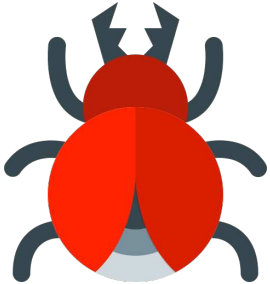
- Exploit vulnerabilities
- Escalate privileges

In-the-Wild Exploits



- Exploit vulnerabilities
- Escalate privileges
- Goal:
  - Compromise system
  - Install persistent spyware
  - ...

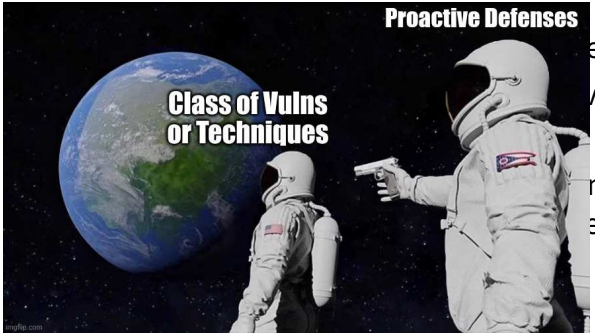
In-the-Wild Exploits



- Exploit vulnerab
- Escalate privileg
- Goal:
  - Compromis
  - Install persi
  - ...

In-the-Wild Exploits

How Well Protected are Devices against In-the-Wild Exploits



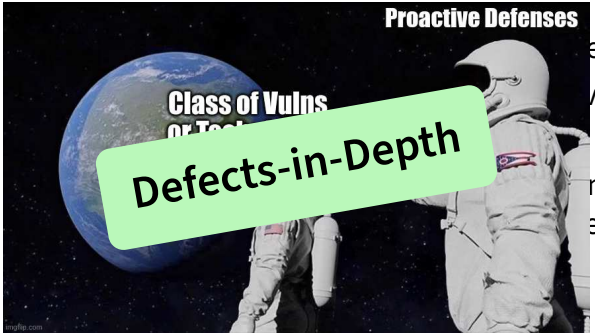
erab

vileg

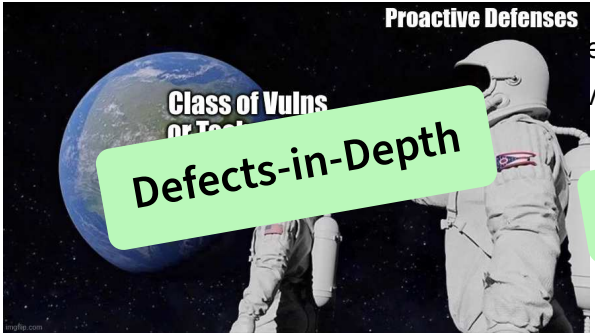
mis

ersi

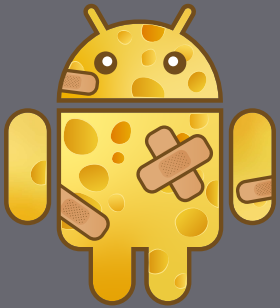
How Well Protected are Devices against In-the-Wild Exploits



How Well Protected are Devices against In-the-Wild Exploits



Defects-in-Depth



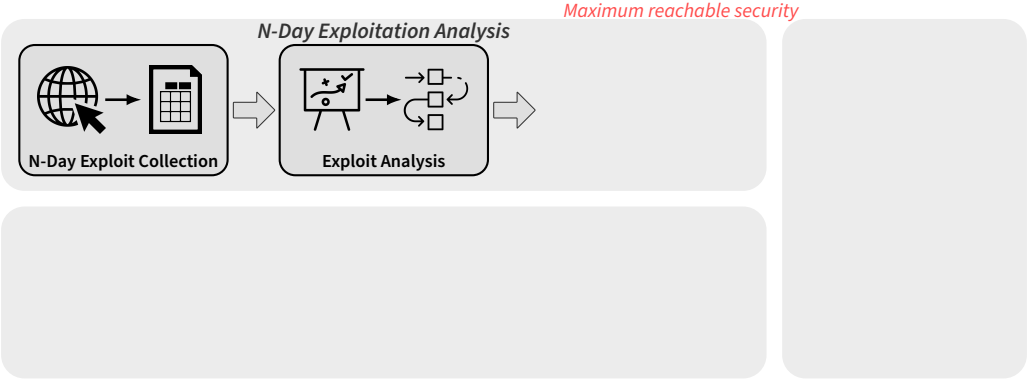
Defects-in-Depth

Defects-in-Depth

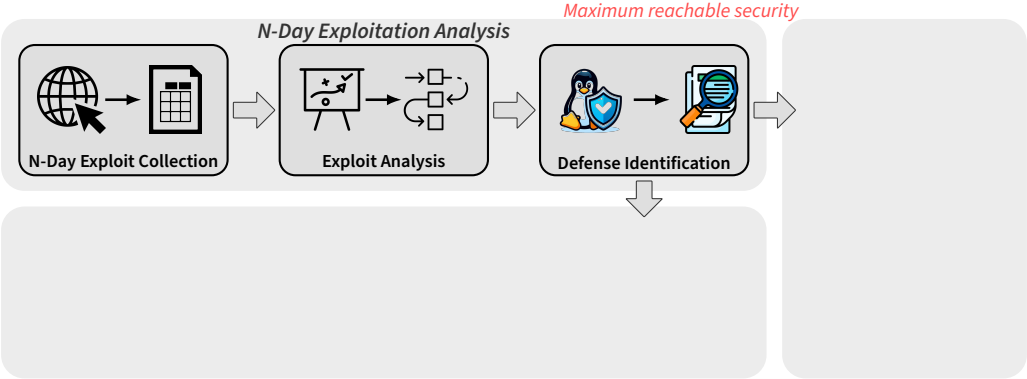
Maximum reachable security

N-Day Exploitation Analysis

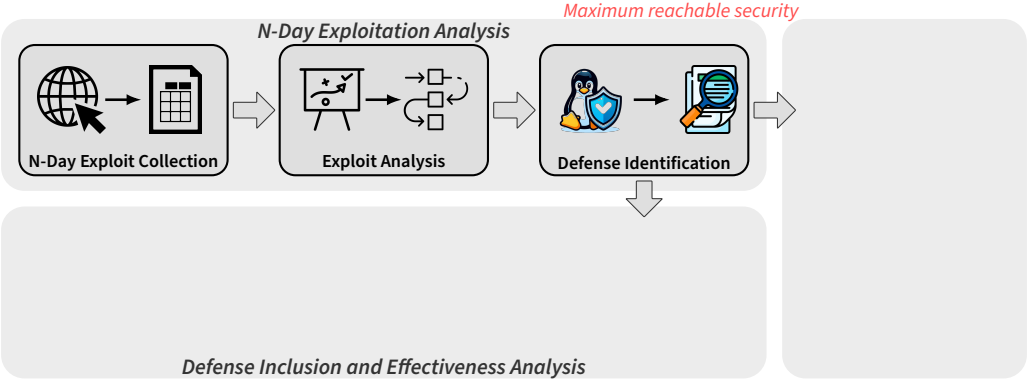
Defects-in-Depth



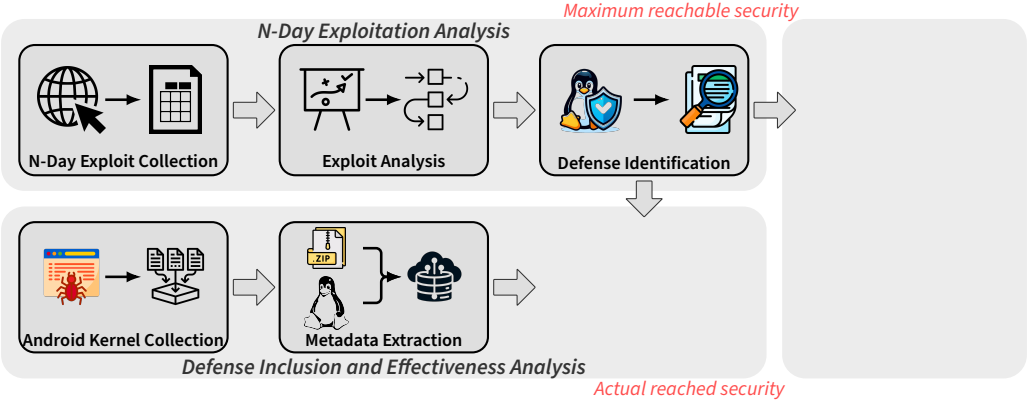
Defects-in-Depth



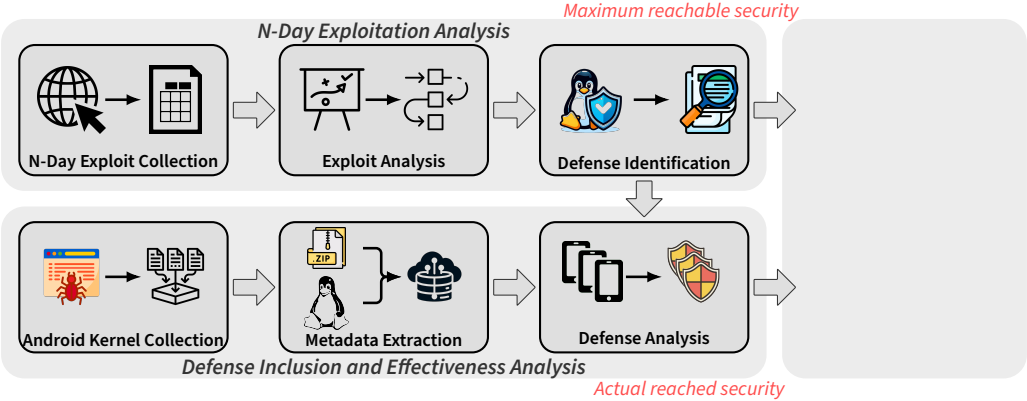
Defects-in-Depth



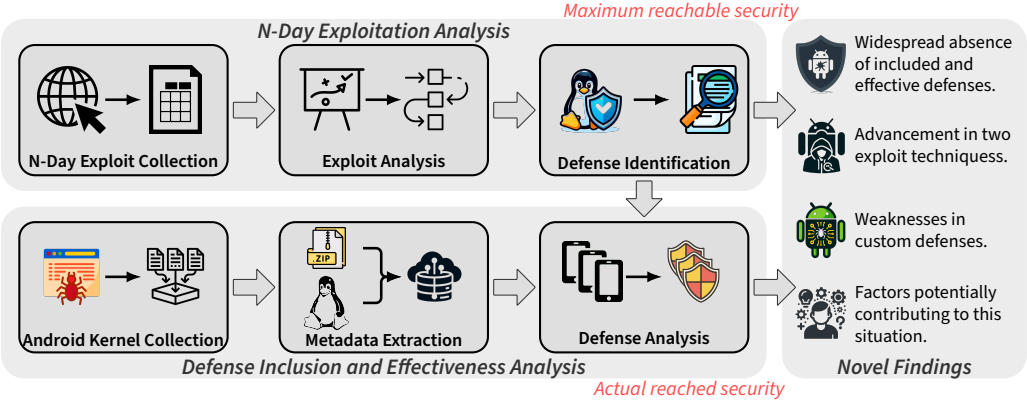
Defects-in-Depth



Defects-in-Depth



Defects-in-Depth



Maximum Reachable Security

Maximum Reachable Security

CVE	DM1	DM2	DM3	DM4	DM5	DM6	DM7	DM8	DM9	DM10
CVE-2019-2215	✓	✗	✓							✓
CVE-2019-2025	✓		✓							
CVE-2020-0030	✓	✗	✓							✓
CVE-2021-1968,-1969,-1940				✓	✓				✗	
CVE-2021-0920	✓		✓							
CVE-2021-1905				✓	✓				✗	
CVE-2022-22265			✓							
CVE-2021-25369,-25370		✗	✓	✗					✗	✓
CVE-2016-3809,-2021-0399			✓	✓	✓				✗	
CVE-2022-20409			✓							
CVE-2023-21400			✓						✶	✗
CVE-2022-28350									✶	✗
CVE-2020-29661									✶	✗
CVE-2021-22600			✓							
CVE-2020-0423	✓							✗	✓	✓
CVE-2022-22057						✓		✗	✓	✓
CVE-2023-26083,-0266				✗					✗	
CVE-2020-0041	✓		✓							
CVE-2019-2205	✓		✓							
CVE-2019-2025	✓		✓					✗	✓	✓
CVE-2020-3680	✓		✓					✗	✓	✓
CVE-2022-20421			✓							
CVE-2022-0847							✓			
CVE-2021-4154										
CVE-2021-38001				✓	✓				✗	
NO_NUMBER (∼2021)			✓			✓				

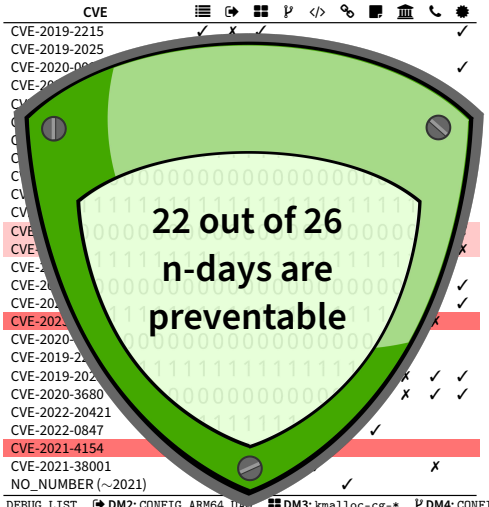
DM1: `CONFIG_DEBUG_LIST` **DM2:** `CONFIG_ARM64_UAO` **DM3:** `kmalloc-cg-*` **DM4:** `CONFIG_CFI_CLANG`
DM5: `CONFIG_BPF_JIT_ALWAYS_ON` **DM6:** `CONFIG_SLAB_FREELIST_HARDENED` **DM7:** `CONFIG_INIT_ON_ALLOC_DEFAULT_ON`
DM8: KSMA protection **DM9:** Samsung RKP **DM10:** Huawei HKIP

Maximum Reachable Security

CVE	DM1	DM2	DM3	DM4	DM5	DM6	DM7	DM8	DM9	DM10
CVE-2019-2215	✓	✗	✓							✓
CVE-2019-2025	✓		✓							
CVE-2020-0030	✓	✗	✓							✓
CVE-2021-1968,-1969,-1940				✓	✓				✗	
CVE-2021-0920	✓		✓							
CVE-2021-1905				✓	✓				✗	
CVE-2022-22265			✓							
CVE-2021-25369,-25370		✗	✓	✗					✗	✓
CVE-2016-3809,-2021-0399			✓	✓	✓				✗	
CVE-2022-20409			✓							
CVE-2023-21400			✓						✶	✗
CVE-2022-28350									✶	✗
CVE-2020-29661									✶	✗
CVE-2021-22600			✓							
CVE-2020-0423	✓							✗	✓	✓
CVE-2022-22057						✓		✗	✓	✓
CVE-2023-26083,-0266				✗					✗	
CVE-2020-0041	✓		✓							
CVE-2019-2205	✓		✓							
CVE-2019-2025	✓		✓					✗	✓	✓
CVE-2020-3680	✓		✓					✗	✓	✓
CVE-2022-20421			✓							
CVE-2022-0847							✓			
CVE-2021-4154										
CVE-2021-38001				✓	✓				✗	
NO_NUMBER (∼2021)			✓			✓				

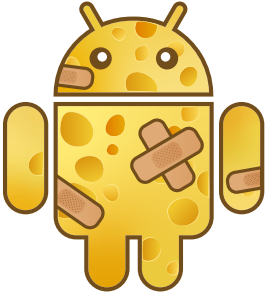
DM1: `CONFIG_DEBUG_LIST` **DM2:** `CONFIG_ARM64_UAO` **DM3:** `kmalloc-cg-*` **DM4:** `CONFIG_CFI_CLANG`
DM5: `CONFIG_BPF_JIT_ALWAYS_ON` **DM6:** `CONFIG_SLAB_FREELIST_HARDENED` **DM7:** `CONFIG_INIT_ON_ALLOC_DEFAULT_ON`
DM8: KSMA protection **DM9:** Samsung RKP **DM10:** Huawei HKIP

Maximum Reachable Security

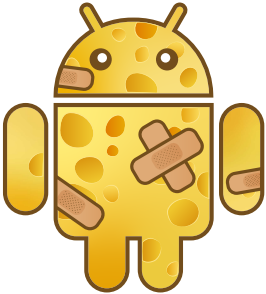


DM1: CONFIG_DEBUG_LIST **DM2:** CONFIG_ARM64_UAO **DM3:** kmalloc-cg-* **DM4:** CONFIG_CFI_CLANG
DM5: CONFIG_BPF_JIT_ALWAYS_ON **DM6:** CONFIG_SLAB_FREELIST_HARDENED **DM7:** CONFIG_INIT_ON_ALLOC_DEFAULT_ON
DM8: KSMA protection **DM9:** Samsung RKP **DM10:** Huawei HKIP

Actual Reached Security



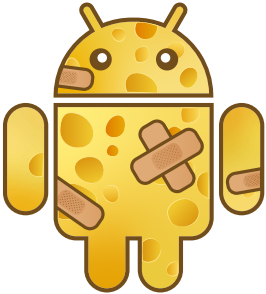
Actual Reached Security



Exploit Flows Still Feasible:

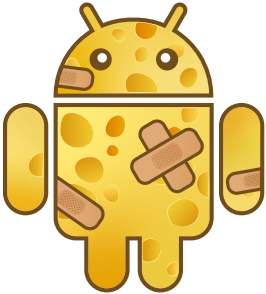
- *Ground Truth:* **4** of 26

Actual Reached Security



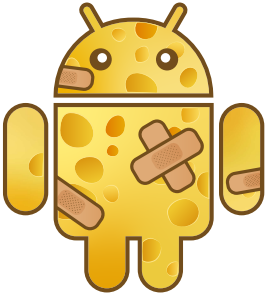
- **Exploit Flows Still Feasible:**
  - *Ground Truth:* **4** of 26
- **Evaluation:**
  - 994 devices
  - From 10 vendors

Actual Reached Security



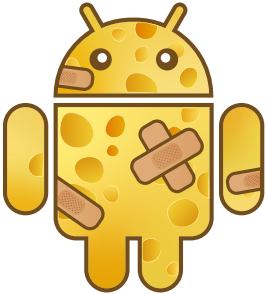
- **Exploit Flows Still Feasible:**
  - *Ground Truth:* **4** of 26
- **Evaluation:**
  - 994 devices
  - From 10 vendors
  - *Average:* **15.2** of 26

Actual Reached Security



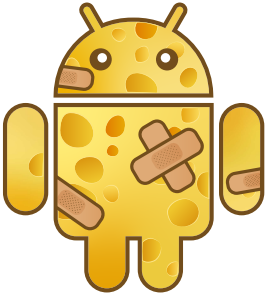
- **Exploit Flows Still Feasible:**
  - *Ground Truth:* **4** of 26
- **Evaluation:**
  - 994 devices
  - From 10 vendors
  - *Average:* **15.2** of 26
- **Notable Mentions:**

Actual Reached Security



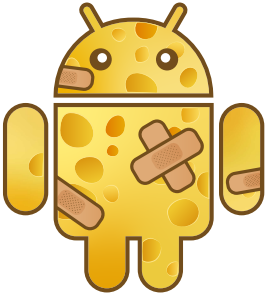
- **Exploit Flows Still Feasible:**
  - *Ground Truth:* **4** of 26
- **Evaluation:**
  - 994 devices
  - From 10 vendors
  - *Average:* **15.2** of 26
- **Notable Mentions:**
  - *Best:* Google with **11.8** of 26

Actual Reached Security



- **Exploit Flows Still Feasible:**
  - *Ground Truth:* **4** of 26
- **Evaluation:**
  - 994 devices
  - From 10 vendors
  - *Average:* **15.2** of 26
- **Notable Mentions:**
  - *Best:* Google with **11.8** of 26
  - *Worst:* Fairphone with **18.5** of 26

Actual Reached Security

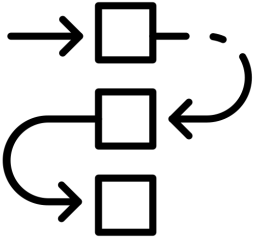


- **Exploit Flows Still Feasible:**
  - *Ground Truth:* **4** of 26
- **Evaluation:**
  - 994 devices
  - From 10 vendors
  - *Average:* **15.2** of 26
- **Notable Mentions:**
  - *Best:* Google with **11.8** of 26
  - *Worst:* Fairphone with **18.5** of 26
  - *Largest Marketshare:* Samsung with **16.1** of 26

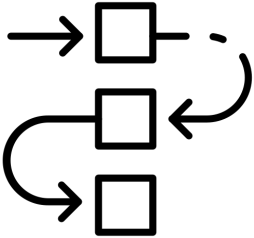
STOP

The Doom of Device Drivers

The Doom of Device Drivers

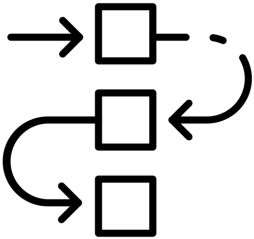


The Doom of Device Drivers



Identify N-Day Vulnerabilities:

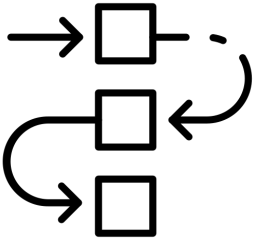
The Doom of Device Drivers



Identify N-Day Vulnerabilities:

- Accessible from untrusted security contexts.
- Affect a wide range of Android devices.

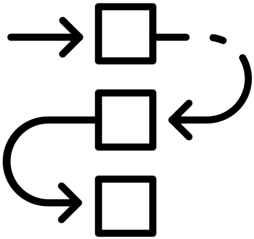
The Doom of Device Drivers



Identify N-Day Vulnerabilities:

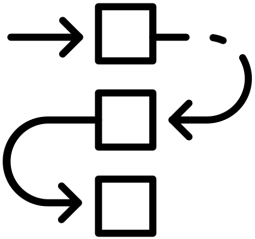
- Accessible from untrusted security contexts.
- Affect a wide range of Android devices.
- *Results:* **50 known** vulns in **11** drivers

The Doom of Device Drivers



- **Identify N-Day Vulnerabilities:**
  - Accessible from untrusted security contexts.
  - Affect a wide range of Android devices.
  - *Results:* **50 known** vulns in **11** drivers
- **Patch Inclusion Analysis:**

The Doom of Device Drivers



Identify N-Day Vulnerabilities:

- Accessible from untrusted security contexts.
- Affect a wide range of Android devices.
- *Results:* **50 known** vulns in **11** drivers

Patch Inclusion Analysis:

- 131 Android devices
- 7 device vendors
- 3 chipset vendors

Devices Susceptibility to at least 1 N-Day

Device Vendor	All Devices Analyzed	
	Crit Vuln	Any Vuln
	%	%
Samsung		
Xiaomi		
Asus		
Realme		
Vivo		
Oppo		
OnePlus		

in December 2024

Devices Susceptibility to at least 1 N-Day

Device Vendor	All Devices Analyzed	
	Crit Vuln	Any Vuln
	%	%
Samsung	45.5	45.5
Xiaomi	67.3	71.4
Asus	75.0	100.0
Realme	56.2	62.5
Vivo	40.0	40.0
Oppo	42.9	42.9
OnePlus	85.7	85.7

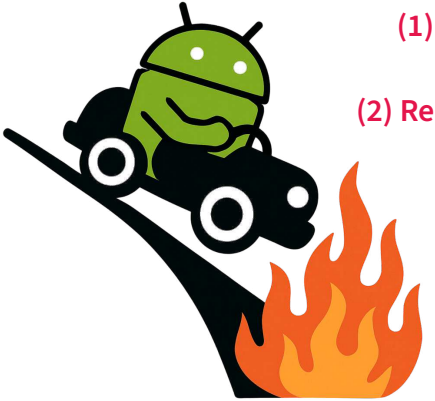
in December 2024

Key Findings

Key Findings

(1) Clustering: Devices susceptible to 1 n-day vuln are often susceptible to many.

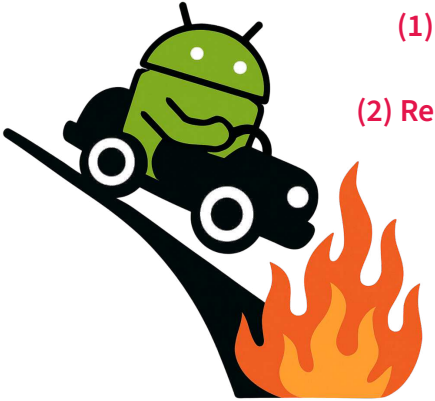
Key Findings



(1) Clustering: Devices susceptible to 1 n-day vuln are often susceptible to many.

(2) Replacement: Vulns are often fixed via new device models than updates.

Key Findings

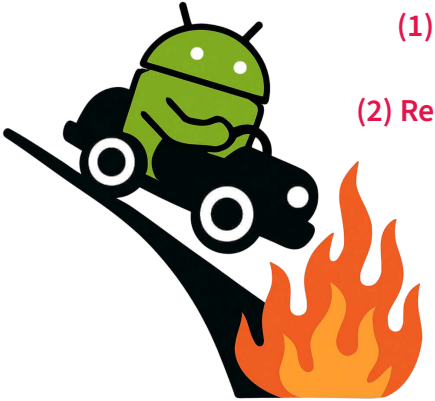


(1) Clustering: Devices susceptible to 1 n-day vuln are often susceptible to many.

(2) Replacement: Vulns are often fixed via new device models than updates.

(3) Delay: Patch times can exceed a year depending on vendors and vuln type.

Key Findings



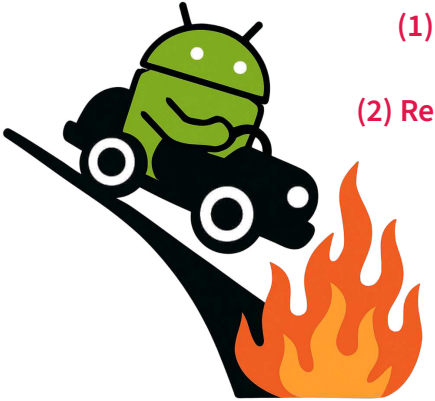
(1) Clustering: Devices susceptible to 1 n-day vuln are often susceptible to many.

(2) Replacement: Vulns are often fixed via new device models than updates.

(3) Delay: Patch times can exceed a year depending on vendors and vuln type.

(4) Reuse: PoCs for driver vulns work across devices and timeframes.

Key Findings



(1) Clustering: Devices susceptible to 1 n-day vuln are often susceptible to many.

(2) Replacement: Vulns are often fixed via new device models than updates.

(3) Delay: Patch times can exceed a year depending on vendors and vuln type.

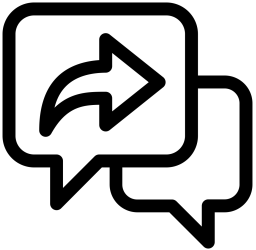
(4) Reuse: PoCs for driver vulns work across devices and timeframes.

(5) Exploit: Threat actors can weaponize n-day vulns, avoiding costly zero-days.

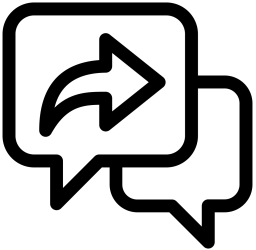
STOP

Outlook

Top Responses



Top Responses

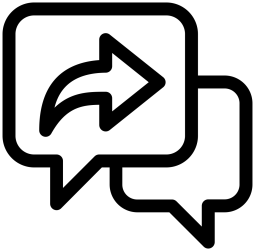


Top Responses

"What voodoo programming is this?"

response to KernelSnitch

Top Responses



"What voodoo programming is this?"

response to KernelSnitch

"It's the hardware vendors damn problem!"

response to the TLB side channel

Top Responses

"What voodoo programming is this?"

response to KernelSnitch

"It's the hardware vendors damn problem!"

response to the TLB side channel

Incorporates fewer security measures due to performance costs

response to Defects-in-Depth

Top Responses

"What voodoo programming is this?"

response to KernelSnitch

"It's the hardware vendors damn problem!"

response to the TLB side channel

Incorporates fewer security measures due to performance costs, particularly for low-end devices.

response to Defects-in-Depth

Top Responses

"What voodoo programming is this?"

response to KernelSnitch

"It's the hardware vendors damn problem!"

response to the TLB side channel

Incorporates fewer security measures due to performance costs, particularly for low-end devices.

response to Defects-in-Depth

Top Responses

"What voodoo programming is this?"

response to KernelSnitch

"It's the hardware vendors damn problem!"

response to the TLB side channel

Incorporates fewer security measures due to performance costs, particularly for low-end devices.

response to Defects-in-Depth

Kernel exploitation requires social hacking.

response to The Doom of Device Drivers

Top Responses

"What voodoo programming is this?"

response to KernelSnitch

"It's the hardware vendors damn problem!"

response to the TLB side channel

Incorporates fewer security measures due to performance costs, particularly for low-end devices.

response to Defects-in-Depth

Kernel exploitation requires social hacking.

response to The Doom of Device Drivers

We mostly patch recent (current generation) devices.

Summary

Summary

Contributions:

Summary

Contributions:

- 7 first-authored publications
  - *5 tier-one venues*
  - *2 tier-two venues*

Summary

Contributions:

- 7 first-authored publications
  - *5 tier-one venues*
  - *2 tier-two venues*
- CSAW and Pwnie Award nominees

Summary

Contributions:

- 7 first-authored publications
  - *5 tier-one venues*
  - *2 tier-two venues*
- CSAW and Pwnie Award nominees
- 12 authored publications

Summary

Contributions:

- 7 first-authored publications
  - *5 tier-one venues*
  - *2 tier-two venues*
- CSAW and Pwnie Award nominees
- 12 authored publications
- 3 Black Hat and 1 Nullcon talks

Summary

Contributions:

- 7 first-authored publications
  - *5 tier-one venues*
  - *2 tier-two venues*
- CSAW and Pwnie Award nominees
- 12 authored publications
- 3 Black Hat and 1 Nullcon talks
- Multiple vulnerabilities
  - *some of which needs to be disclosed*

Summary

Contributions:

- 7 first-authored publications
  - *5 tier-one venues*
  - *2 tier-two venues*
- CSAW and Pwnie Award nominees
- 12 authored publications
- 3 Black Hat and 1 Nullcon talks
- Multiple vulnerabilities
  - *some of which needs to be disclosed*

Teaching:

Summary

Contributions:

- 7 first-authored publications
  - *5 tier-one venues*
  - *2 tier-two venues*
- CSAW and Pwnie Award nominees
- 12 authored publications
- 3 Black Hat and 1 Nullcon talks
- Multiple vulnerabilities
  - *some of which needs to be disclosed*

Teaching:

- Secure Software Development VO/KU
- Pentesting Lab

Summary

Contributions:

- 7 first-authored publications
  - *5 tier-one venues*
  - *2 tier-two venues*
- CSAW and Pwnie Award nominees
- 12 authored publications
- 3 Black Hat and 1 Nullcon talks
- Multiple vulnerabilities
  - *some of which needs to be disclosed*

Teaching:

- Secure Software Development VO/KU
- Pentesting Lab

Others:

Summary

Contributions:

- 7 first-authored publications
  - *5 tier-one venues*
  - *2 tier-two venues*
- CSAW and Pwnie Award nominees
- 12 authored publications
- 3 Black Hat and 1 Nullcon talks
- Multiple vulnerabilities
  - *some of which needs to be disclosed*

Teaching:

- Secure Software Development VO/KU
- Pentesting Lab

Others:

- Multiple proposals
  - *some also got accepted*
- Supervised 2 Master and 1 Bachelor students

STOP

Enhance Exploit Reliability via Side Channels

Increase Defense Effectiveness

Reveal Shortcomings in the Android Ecosystem

Reveal Shortcomings
in the Android Ecosystem

Enhance Exploit Reliability
via Side Channels

Increase Defense
Effectiveness

TU Graz

SCIENCE
PASSION
TECHNOLOGY

Kernel Security in the Wild:

Side-Channel-Assisted Exploit Techniques, Kernel-Level Defenses, and Real-World Analysis

Lukas Maar

September 26, 2025

PhD Defense

› isec.tugraz.at

References I

[Gua25a] T. Guardian. **Ice obtains access to Israeli-made spyware that can hack phones and encrypted apps.** 2025. URL: https://www.theguardian.com/us-news/2025/sep/02/trump-immigration-ice-israeli-spyware.

[Gua25b] T. Guardian. **Owner of spyware used in alleged WhatsApp breach ends contract with Italy.** 2025. URL: https://www.theguardian.com/technology/2025/feb/06/owner-of-spyware-used-in-alleged-whatsapp-breach-ends-contract-with-italy.

[Int21] A. International. **Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally.** 2021. URL: https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project.

[Int25] A. International. **Europe: Paragon attacks highlight Europe's growing spyware crisis.** 2025. URL: https://www.amnesty.org/en/latest/news/2025/03/europe-paragon-attacks-highlight-europes-growing-spyware-crisis/.

References II

[Mar+25] B. Marczak, J. Scott-Railton, K. Robertson, A. Perry, R. Brown, B. A. Razzak, S. Anstis, and R. Deibert. **Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations**. 2025. URL: https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/.

[Omt23] P. Omtzigt. **Pegasus and similar spyware and secret state surveillance**. 2023. URL: https://pace.coe.int/en/files/33018/html.

[Set23] Seth Jenkins. **Analyzing a Modern In-the-wild Android Exploit**. 2023. URL: https://googleprojectzero.blogspot.com/2023/09/analyzing-modern-in-wild-android-exploit.html.

[Xin+24] X. Xing, E. Rodionov, J. Bottarini, A. Bacchus, A. Chaudhary, L. Fawcett, and J. Artgole. **Google & Arm - Raising The Bar on GPU Security**. 2024. URL: https://security.googleblog.com/2024/09/google-arm-raising-bar-on-gpu-security.html.