Defects-in-Depth

Analyzing the Integration of Effective Defenses against One-Day Exploits in Android Kernels

Lukas Maar, Florian Draschbacher, Lukas Lamster, and Stefan Mangard

August 15, 2024

Graz University of Technology

Who am I?

Lukas Maar

PhD candidate @ Graz University of Technology

Improve system security

https://lukasmaar.github.io

lukas.maar@iaik.tugraz.at

Defects-in-Depth

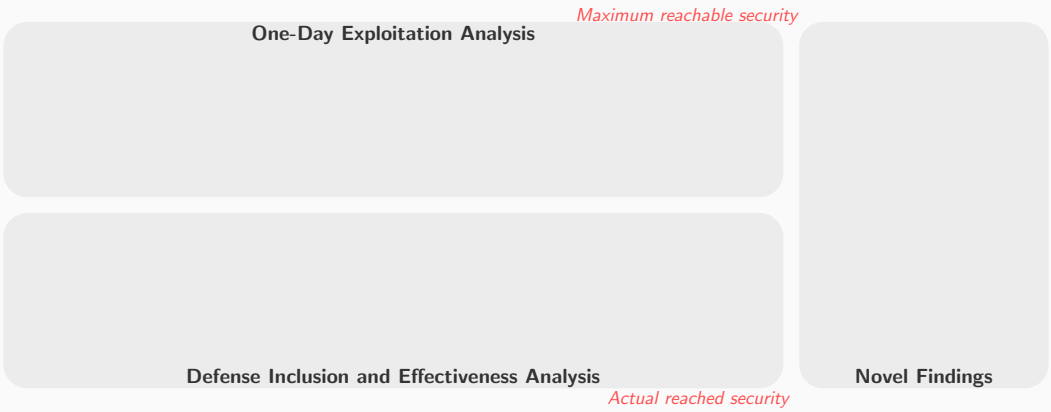
High-Level Workflow

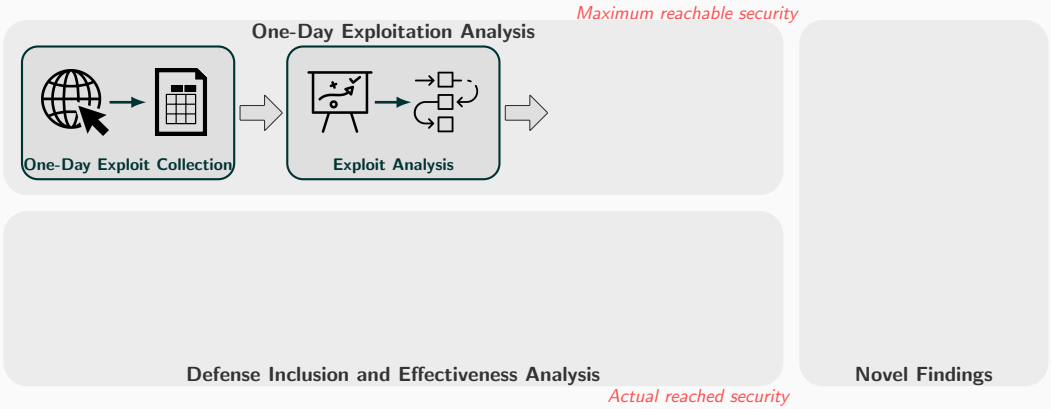
One-Day Exploitation Analysis

Defense Inclusion and Effectiveness Analysis

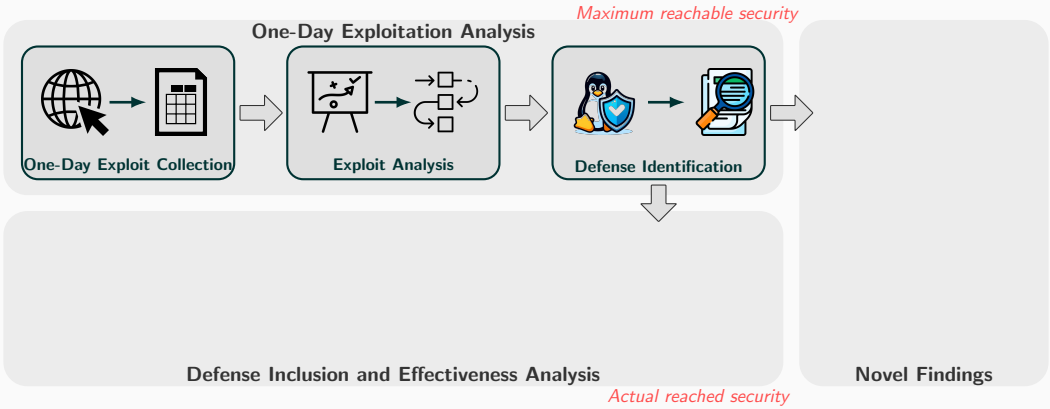
Novel Findings

High-Level Workflow

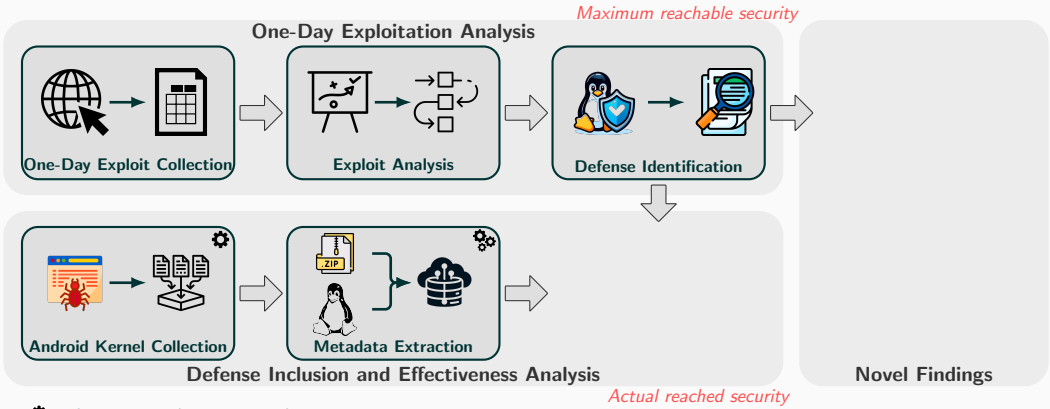



Maximum reachable security
One-Day Exploitation Analysis
One-Day Exploit Collection
Exploit Analysis
Defense Inclusion and Effectiveness Analysis
Novel Findings
Actual reached security

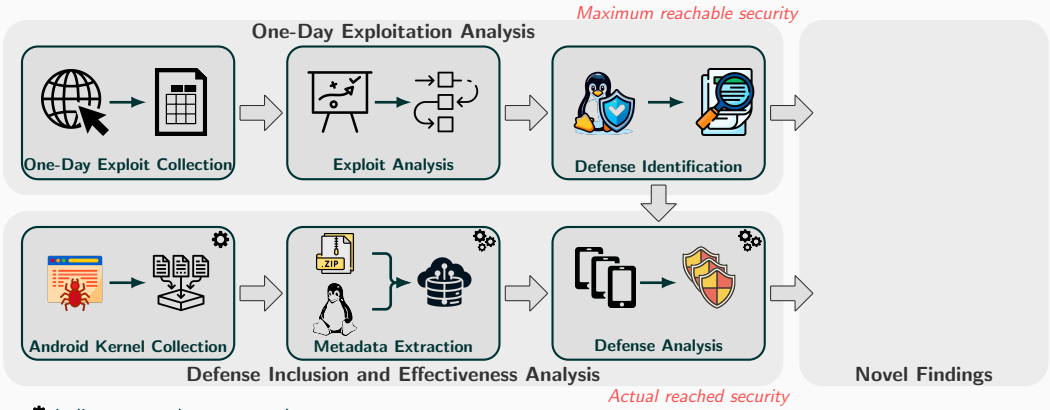
High-Level Workflow



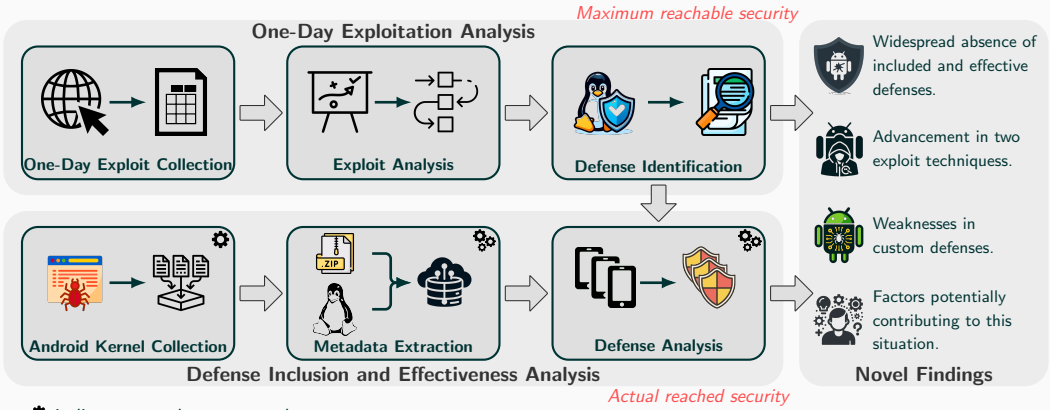
High-Level Workflow



High-Level Workflow

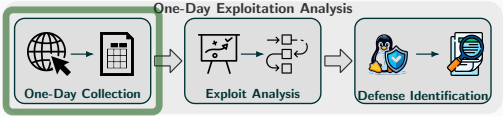


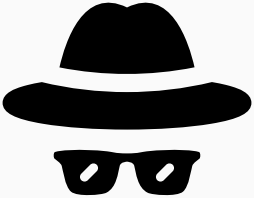
High-Level Workflow

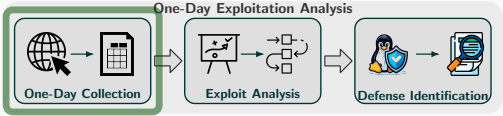


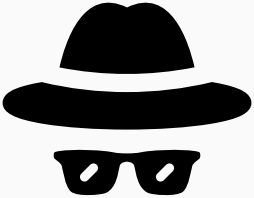
One-Day Exploitation Analysis

One-Day Exploit Collection

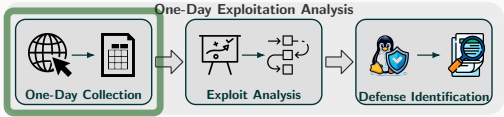


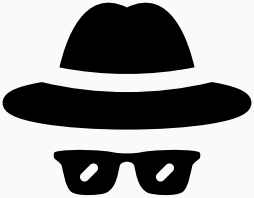






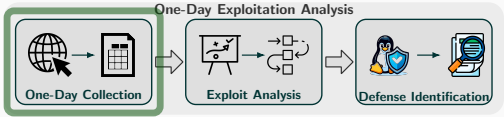
- **One-day exploits:**
  - "One-day vulnerabilities are known vulnerabilities for which a patch or mitigation is available."

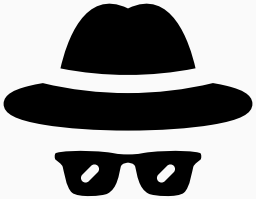




- **One-day exploits:**
  - "One-day vulnerabilities are known vulnerabilities for which a patch or mitigation is available."
  - "N-days function like 0-days on Android due to long patching times [Sto23]."

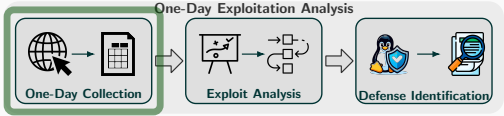
One-Day Exploit Collection

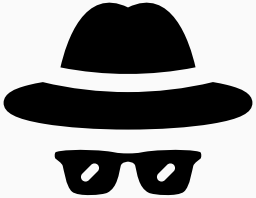




- **One-day exploits:**
  - "One-day vulnerabilities are known vulnerabilities for which a patch or mitigation is available."
  - "N-days function like 0-days on Android due to long patching times [Sto23]."
- **All one-days exploiting memory-safety vulnerabilities**
  - Between 2021 and 2023

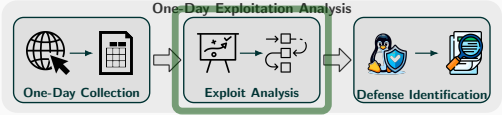
One-Day Exploit Collection

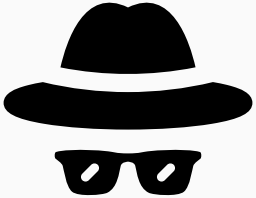


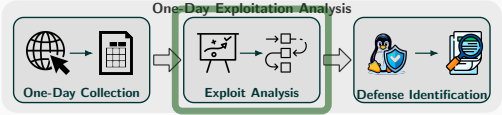


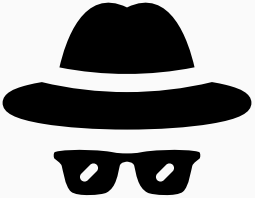
- **One-day exploits:**
  - "One-day vulnerabilities are known vulnerabilities for which a patch or mitigation is available."
  - "N-days function like 0-days on Android due to long patching times [Sto23]."
- **All one-days exploiting memory-safety vulnerabilities**
  - Between 2021 and 2023
- **Sources:**

Exploitation Flow Analysis

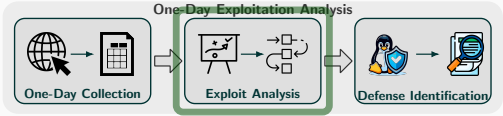


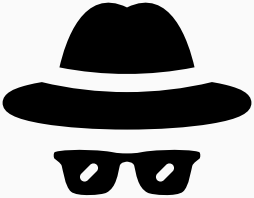






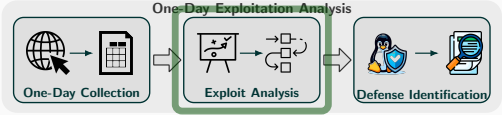
- **One-day exploitation flow [Aza20]:**
  - Vulnerability-agnostic chain of exploit techniques
  - One technique elevates a primitive to a more powerful form
  - Leverages the capabilities of a vulnerability to gain root privileges

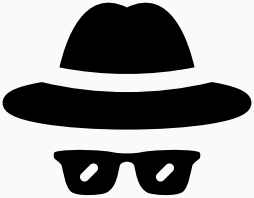




- **One-day exploitation flow [Aza20]:**
  - Vulnerability-agnostic chain of exploit techniques
  - One technique elevates a primitive to a more powerful form
  - Leverages the capabilities of a vulnerability to gain root privileges
  - E.g. for primitives: UAF write, PC control, or arbitrary r/w.

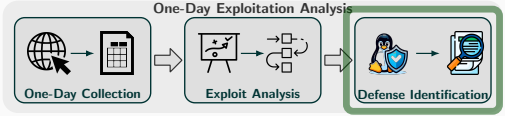
Exploitation Flow Analysis





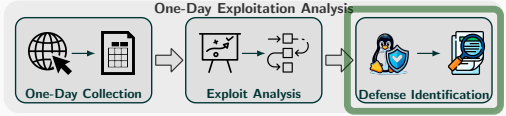
- **One-day exploitation flow [Aza20]:**
  - Vulnerability-agnostic chain of exploit techniques
  - One technique elevates a primitive to a more powerful form
  - Leverages the capabilities of a vulnerability to gain root privileges
  - E.g. for primitives: UAF write, PC control, or arbitrary r/w.

- **Analyze 26 one-day exploitation flows**
  - 10 exploit techniques


One-Day Exploitation Analysis
One-Day Collection
Exploit Analysis
Defense Identification

Maximum Reachable Security

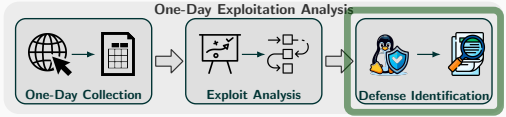
CVE	DM1	DM2	DM3	DM4	DM5	DM6	DM7	DM8	DM9	DM10
CVE-2019-2215	✓	✗	✓							✓
CVE-2019-2025	✓		✓							
CVE-2020-0030	✓	✗	✓							✓
CVE-2021-1968,-1969,-1940				✓	✓				✗	
CVE-2021-0920	✓		✓							
CVE-2021-1905				✓	✓				✗	
CVE-2022-22265			✓							
CVE-2021-25369,-25370		✗	✓	✗					✗	✓
CVE-2016-3809,-2021-0399			✓	✓	✓				✗	
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)			✓			✓				

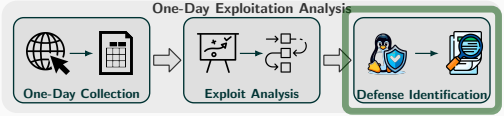


DM1: CONFIG_DEBUG_LIST DM2: CONFIG_ARM64_UAO DM3: kmalloc-cg-* DM4: CONFIG_CFI_CLANG
DM5: CONFIG_BPF_JIT_ALWAYS_ON DM6: CONFIG_SLAB_FREELIST_HARDENED DM7: CONFIG_INIT_ON_ALLOC_DEFAULT_ON
DM8: KSMA protection DM9: Samsung RKP DM10: Huawei HKIP

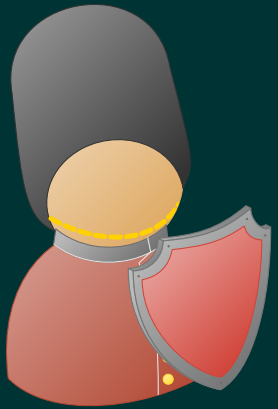
Maximum Reachable Security

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,-2021-03										
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)			✓			✓				

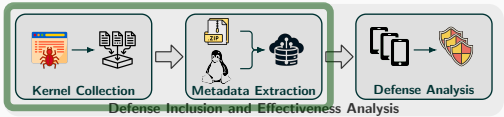
22 out of 26 one-days are preventable



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

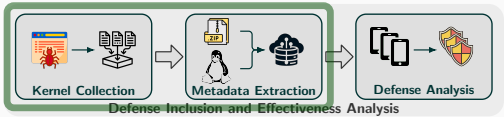


Defense Inclusion and Effectiveness Analysis

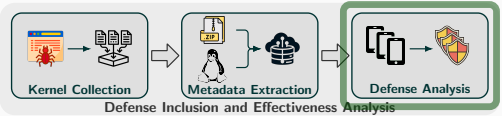


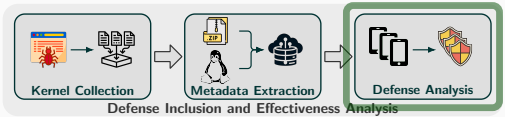
- **Goal:**
  - Determine actual security reached
  - By downstreamed Android kernels

Android Kernel Collection & Metadata Extraction

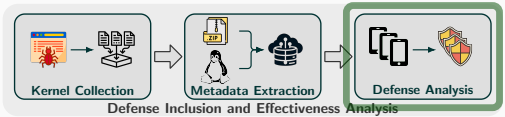


- **Goal:**
  - Determine actual security reached
  - By downstreamed Android kernels
- **Android devices:**
  - 10 vendors:
    - SAMSUNG, mi, oppo, vivo, HUAWEI, R, Motorola, Google, 1+, FAIRPHONE
  - 1698 devices released between 2018 and 2023
  - We extracted 994 device kernels


Kernel Collection
Metadata Extraction
Defense Analysis
Defense Inclusion and Effectiveness Analysis



- **Source code analysis:**
  - *Manual analysis* of all kernel defenses
  - Determine their effectiveness



- **Source code analysis:**
  - *Manual analysis* of all kernel defenses
  - Determine their effectiveness
- **Kernel binary analysis:**
  - *Automatic analysis* of all kernel defenses
  - Depending whether the kernel includes crucial routines

    E.g., check or permission setting function
  - Determine their inclusion

Novel Findings

Level of Security reached Severely Lacking

Widespread absence of included and effective defenses.

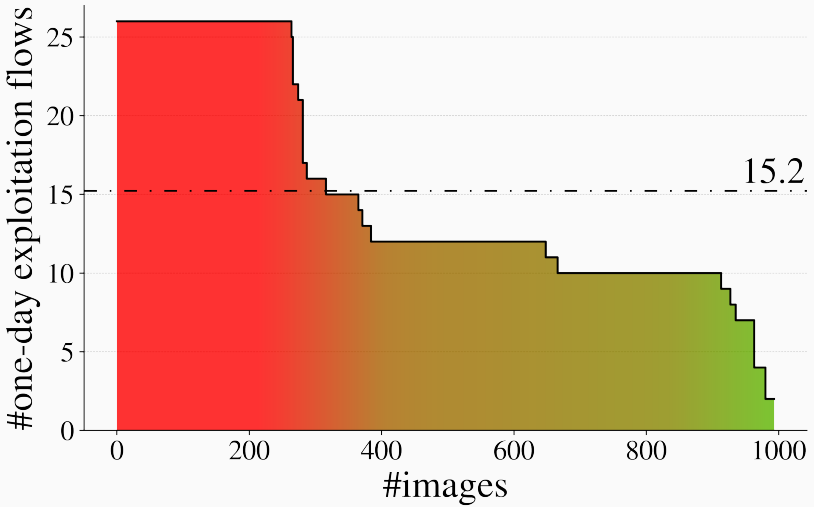
Advancement in two exploit techniquess.

Weaknesses in custom defenses.

Factors potentially contributing to this situation.

Novel Findings

Level of Security reached Severely Lacking



Widespread absence of included and effective defenses.

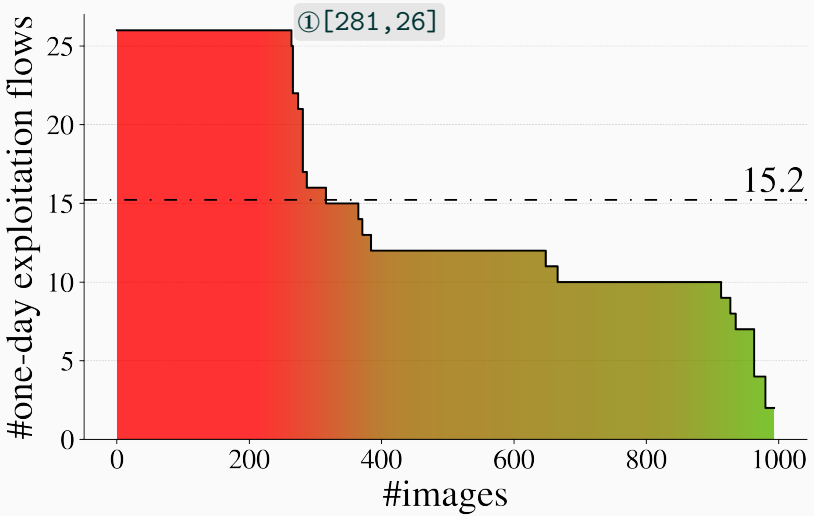
Advancement in two exploit techniquess.

Weaknesses in custom defenses.

Factors potentially contributing to this situation.

Novel Findings

Level of Security reached Severely Lacking



Widespread absence of included and effective defenses.

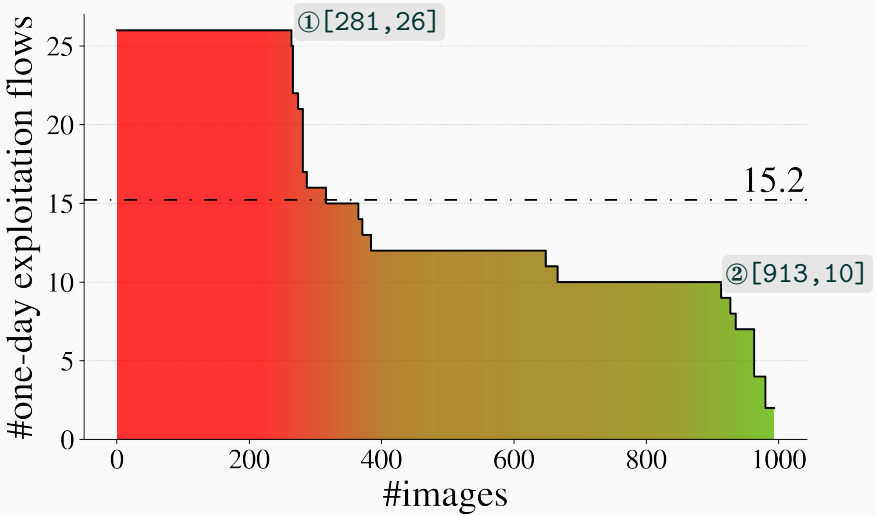
Advancement in two exploit techniquess.

Weaknesses in custom defenses.

Factors potentially contributing to this situation.

Novel Findings

Level of Security reached Severely Lacking



Widespread absence of included and effective defenses.

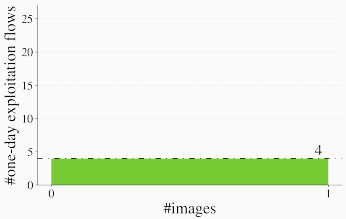
Advancement in two exploit techniquess.

Weaknesses in custom defenses.

Factors potentially contributing to this situation.

Novel Findings

Level of Security reached Severely Lacking contd



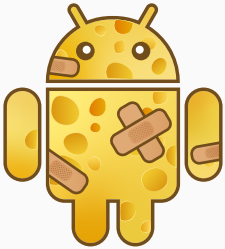
(a) Ground truth **(b)** Google

(c) Samsung **(d)** Fairphone

- Widespread absence of included and effective defenses.
- Advancement in two exploit techniquess.
- Weaknesses in custom defenses.
- Factors potentially contributing to this situation.

Novel Findings

Factors Potentially Contributing to this Situation



Widespread absence of included and effective defenses.

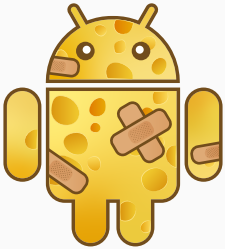
Advancement in two exploit techniquess.

Weaknesses in custom defenses.

Factors potentially contributing to this situation.

Novel Findings

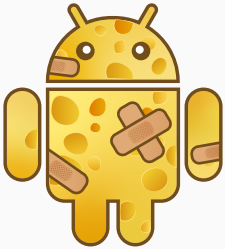
Factors Potentially Contributing to this Situation



1. Correlation between older kernels and more susceptibility
   - *The use of older kernels*

Widespread absence of included and effective defenses.
Advancement in two exploit techniquess.
Weaknesses in custom defenses.
Factors potentially contributing to this situation.
Novel Findings

Factors Potentially Contributing to this Situation

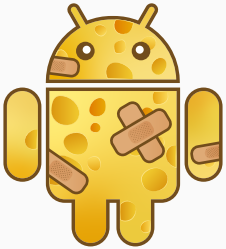


1. Correlation between older kernels and more susceptibility
   - *The use of older kernels*
2. Well configured v3.10 provides more security than 38.1 % of vendor-supplied kernels
   - *Lack of importance regarding security-relevant features*

Widespread absence of included and effective defenses.
Advancement in two exploit techniquess.
Weaknesses in custom defenses.
Factors potentially contributing to this situation.

Novel Findings

Factors Potentially Contributing to this Situation



1. Correlation between older kernels and more susceptibility
   - *The use of older kernels*
2. Well configured v3.10 provides more security than 38.1 % of vendor-supplied kernels
   - *Lack of importance regarding security-relevant features*

"Implementing certain security mitigations can lead to significant **performance costs**, e.g., `CONFIG_DEBUG_LIST` was enforced in the past but OEMs complaint about the performance hit."

Widespread absence of included and effective defenses.

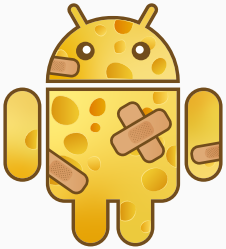
Advancement in two exploit techniquess.

Weaknesses in custom defenses.

Factors potentially contributing to this situation.

Novel Findings

Factors Potentially Contributing to this Situation



1. Correlation between older kernels and more susceptibility
   - *The use of older kernels*
2. Well configured v3.10 provides more security than 38.1 % of vendor-supplied kernels
   - *Lack of importance regarding security-relevant features*

- "Implementing certain security mitigations can lead to significant **performance costs**, e.g., `CONFIG_DEBUG_LIST` was enforced in the past but OEMs complaint about the performance hit."
- "However, considering the fact that the majority of Android devices are **low-end devices**, it's generally not possible to apply all mitigations due to the performance reasons."

Widespread absence of included and effective defenses.

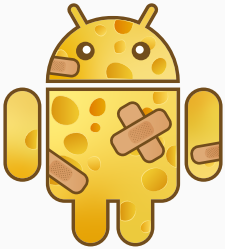
Advancement in two exploit techniquess.

Weaknesses in custom defenses.

Factors potentially contributing to this situation.

Novel Findings

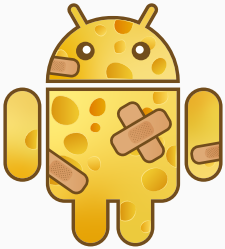
Factors Potentially Contributing to this Situation contd



- "However, few models are still checking the feasibility of applying RKP due to chipset's **limited performances**".

Widespread absence of included and effective defenses.
Advancement in two exploit techniquess.
Weaknesses in custom defenses.
Factors potentially contributing to this situation.
Novel Findings

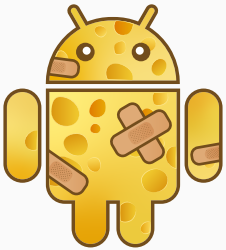
Factors Potentially Contributing to this Situation contd



- "However, few models are still checking the feasibility of applying RKP due to chipset's **limited performances**".
- "As you mentioned, consider the **significant performance cost**, currently HKIP does not protect page tables for user address translation."

Widespread absence of included and effective defenses.
Advancement in two exploit techniquess.
Weaknesses in custom defenses.
Factors potentially contributing to this situation.
Novel Findings

Factors Potentially Contributing to this Situation contd



- "However, few models are still checking the feasibility of applying RKP due to chipset's **limited performances**".
- "As you mentioned, consider the **significant performance cost**, currently HKIP does not protect page tables for user address translation."
- **Evaluation:** Difference between low and high-end devices

Widespread absence of included and effective defenses.

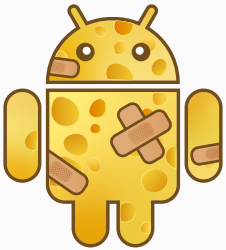
Advancement in two exploit techniquess.

Weaknesses in custom defenses.

Factors potentially contributing to this situation.

Novel Findings

Factors Potentially Contributing to this Situation contd



- "However, few models are still checking the feasibility of applying RKP due to chipset's **limited performances**".
- "As you mentioned, consider the **significant performance cost**, currently HKIP does not protect page tables for user address translation."
- **Evaluation:** Difference between low and high-end devices

3. 23.8 % susceptibility gap between high and low-end devices

Performance cost, especially for less powerful low-end devices

Widespread absence of included and effective defenses.

Advancement in two exploit techniquess.

Weaknesses in custom defenses.

Factors potentially contributing to this situation.

Novel Findings

Conclusion

https://lukasmaar.github.io

- **Analyzed 26 one-days targeting the Android kernel**
- **Identified defenses mitigating most of these one-days**
- **Performed a defense inclusion and effectiveness analysis**
- **Presented novel findings:**
  1. Absence of effective defenses in vendor-provided kernels
  2. Advancement in two exploitation techniques
  3. Weaknesses in defenses
  4. Potential factors that contribute to this situation

References

[Aza20] B. Azad. A survey of recent iOS kernel exploits. 2020. URL: https://googleprojectzero.blogspot.com/2020/06/a-survey-of-recent-ios-kernel-exploits.html.

[Sto23] M. Stone. The Ups and Downs of 0-days: A Year in Review of 0-days Exploited In-the-Wild in 2022. 2023. URL: https://security.googleblog.com/2023/07/the-ups-and-downs-of-0-days-year-in.html.