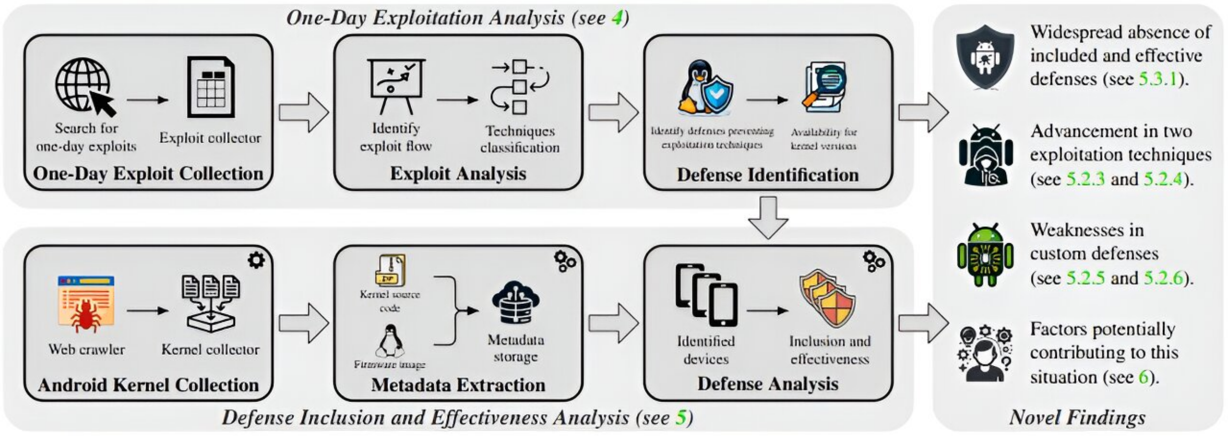
TechXplore

Numerous manufacturers use insecure Android kernels, analysis shows

August 16 2024


One-Day Exploitation Analysis (see 4)
Search for one-day exploits
Exploit collector
One-Day Exploit Collection
Identify exploit flow
Techniques classification
Exploit Analysis
Identify defenses preventing exploitation techniques
Availability for kernel versions
Defense Identification
Web crawler
Kernel collector
Android Kernel Collection
Kernel source code
Firmware image
Metadata storage
Metadata Extraction
Identified devices
Inclusion and effectiveness
Defense Analysis
Defense Inclusion and Effectiveness Analysis (see 5)
Widespread absence of included and effective defenses (see 5.3.1).
Advancement in two exploitation techniques (see 5.2.3 and 5.2.4).
Weaknesses in custom defenses (see 5.2.5 and 5.2.6).
Factors potentially contributing to this situation (see 6).
Novel Findings

The high-level workflow of the study. Credit: https://www.usenix.org/system/files/usenixsecurity24-maar-defects.pdf

In an analysis of smartphones from 10 manufacturers, researchers at TU Graz have found that the Android kernels used are vulnerable to known attacks—so-called one-day exploits—despite existing protection mechanisms.

Smartphones are a constant companion and important work tool for many people. In addition to contacts, appointments and emails, the devices are increasingly being used for sensitive tasks such as online banking or official matters. This increases the safety requirements.

As Lukas Maar, Florian Draschbacher, Lukas Lamster and Stefan Mangard from the Institute of Applied Information Processing and Communications at Graz University of Technology (TU Graz) have discovered in a comprehensive analysis of the Android kernels of the 10 largest and most well-known smartphone manufacturers, there are numerous flaws here that allow one-day exploits using already known attack methods. The researchers presented their findings on 15 August at the Usenix Security Symposium in Philadelphia.

Depending on the manufacturer and model, only between 29% and 55% of the 994 smartphones tested by the research team were able to prevent attacks. In contrast, the Generic Kernel Image (GKI) version 6.1 provided by Google would be able to prevent around 85% of attacks.

Compared to the GKI, the manufacturer kernels performed up to 4.6 times worse in defending against attacks. The research team analyzed devices from these manufacturers that came onto the market between 2018 and 2023 (listing from the most secure to the least secure): Google, Realme, OnePlus, Xiaomi, Vivo, Samsung, Motorola, Huawei, Oppo and Fairphone.

The Android versions used on these smartphones ranged from versions 9 to 14, while the kernels covered the range from versions 3.10 to 6.1, with manufacturers who rely on lower kernel versions also offering less security.

Effective defense mechanisms rarely activated

Another key point of the analysis is that there are already effective defenses for a number of the known attack methods, but they are either rarely activated in the manufacturers' kernels or the kernels are configured incorrectly. As a result, even kernel version 3.1 from 2014 with all security measures activated could provide better protection against known attacks than about 38% of the kernels configured by the manufacturers themselves.

The researchers also found that manufacturers' low-end models were about 24% more at risk than high-end models. One important reason for this is the loss of performance that additional security measures can cause, which is why they are often deactivated in low-end models to conserve resources.

"We hope that our results will help to ensure that more effective security measures can be found in manufacturers' kernels in the future, making Android more secure," says Maar. "We also shared our analysis with the manufacturers investigated and Google, Fairphone, Motorola, Huawei and Samsung have taken note—some have even released patches.

"We have also suggested that Google update the Android Compatibility Definition Document (CDD), which sets out the framework of requirements for devices to be compatible with Android.

"Google itself has emphasized that it is aware of the problem and wants to strengthen the integration of kernel security measures step by step. However, it is up to the manufacturers whether they want to sacrifice performance for this."

More information: Defects-in-Depth: Analyzing the Integration of Effective Defenses against One-Day Exploits in Android Kernels. www.usenix.org/conference/usen … ntation/maar-defects

Provided by Graz University of Technology

Citation: Numerous manufacturers use insecure Android kernels, analysis shows (2024, August

16) retrieved 16 August 2024 from https://techxplore.com/news/2024-08-numerous-insecure-android-kernels-analysis.html