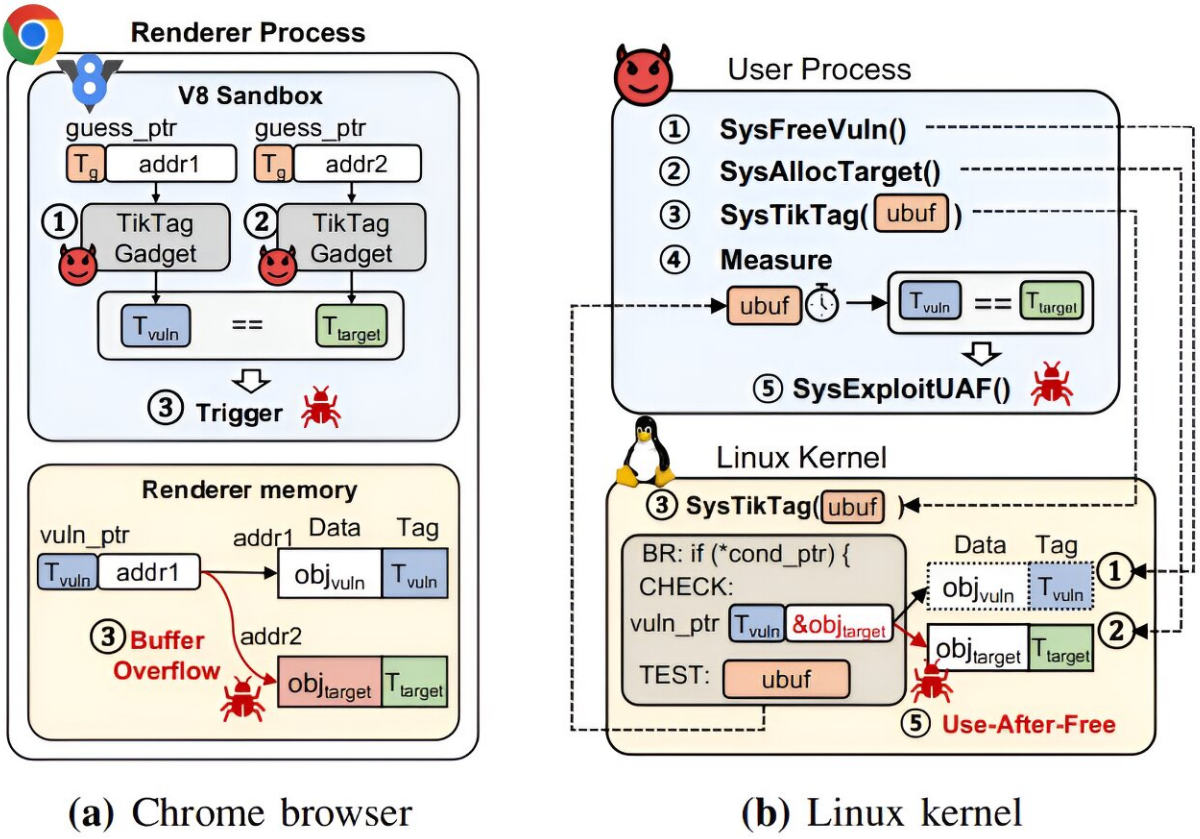
Security experts find vulnerability in ARM's memory tagging extensions

June 19 2024, by Bob Yirka



(a) Chrome browser (b) Linux kernel

MTE bypass attacks. Credit: *arXiv* (2024). DOI: 10.48550/arxiv.2406.08719

A combined team of security experts from Seoul National University and Samsung Research has found a vulnerability in memory tagging extensions (MTEs) employed by ARM processors as a means of protection from memory leaks. The group has published a paper describing their findings on the *arXiv* preprint server.

In 2018, Arm, Ltd., introduced a new hardware feature for advanced reduced instruction set computer (RISC) machines (ARMs) that could be used by software makers to detect memory violations. MTEs tag blocks of physical memory with metadata.

When software makes a memory call within a tagged region, generally using a pointer, the new hardware looks to see if the pointer holds a matching key for the referenced memory block. If not, an error is returned, preventing data from being written where it is not supposed to happen—such as during buffer overflows.

The introduction of MTE has been considered an attractive addition to the ARM architecture because it helps programmers prevent memory corruption and possible vulnerabilities such as hackers accessing data in unsecured areas. Unfortunately, it appears that the introduction of MTEs has also led to the introduction of a new vulnerability.

In this new work, the research team developed two techniques they call TIKTAG-v1 and -v2 that they claim are capable of extracting MTE tags for random memory address areas. They explain that both techniques involve the use of software to watch as speculative operations influence the way that data is pre-fetched.

Software systems use pre-fetching to speed up operations, preventing lag times associated with waiting for data retrieval. Speculative executions

work in much the same way, executing code in advance that might be useful at a future point, sometimes using pre-fetched data and writing to memory. If the results of such executions are not needed, they are simply discarded. The vulnerabilities the team found involved taking advantage of such pre-fetched and/or discarded information.

The research team found that they were able to extract MTE tags in 95% of their attempts, which, they note, could lead to exploitation. They also proposed multiple possible solutions to fix the problem, which they sent to Arm, Ltd.

More information: Juhee Kim et al, TikTag: Breaking ARM's Memory Tagging Extension with Speculative Execution, *arXiv* (2024). DOI: 10.48550/arxiv.2406.08719

Citation: Security experts find vulnerability in ARM's memory tagging extensions (2024, June 19) retrieved 20 June 2024 from https://techxplore.com/news/2024-06-experts-vulnerability-arm-memory-tagging.html