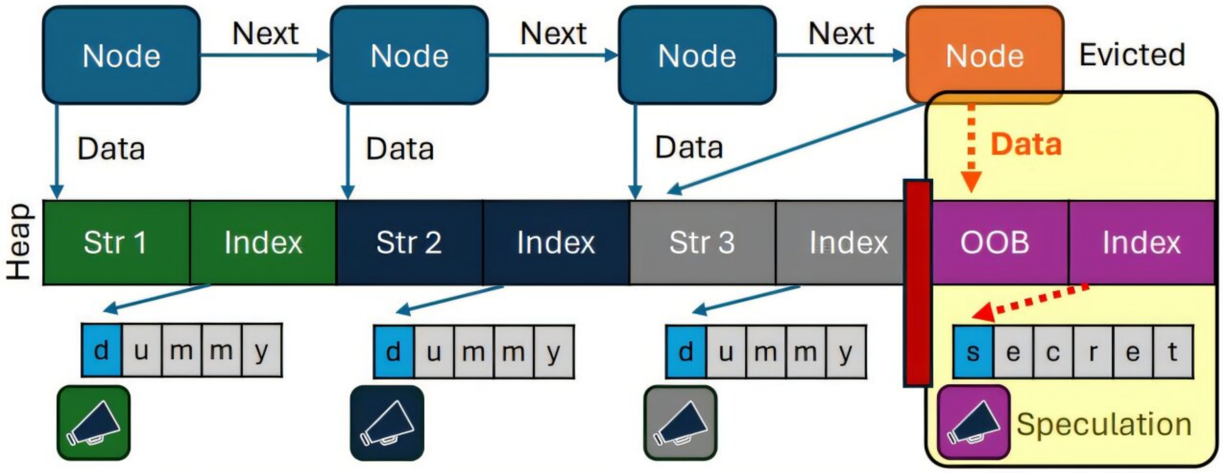
TechXplore

Security vulnerabilities discovered in Apple processors

January 29 2025



Graphical overview of the browser-based version of our LAPtraining gadget. Architectural execution is shown in blue arrows, while speculative execution is shown in red arrows and the highlighted region. Credit: SLAP: Data Speculation Attacks via Load Address Prediction on Apple Silicon. https://predictors.fail/files/SLAP.pdf

The US tech giant Apple has always advertised security assurances alongside ever faster processor performance for its products.

Now an international team of cybersecurity researchers, including Yuval Yarom, principal investigator at the cluster of excellence CASA and Professor of Computer Security at the Faculty of Computer Science and the Horst Görtz Institute for IT Security at Ruhr University Bochum, Germany, has discovered at least two security vulnerabilities.

The research results will be presented at the IEEE SP 2025 and USENIX Security 2025 conferences. Further information can be found on their website.

To identify vulnerabilities in existing systems, cybersecurity experts must examine real-world attack scenarios. In their paper "FLOP: Breaking the Apple M3 CPU via False Load Output Predictions," researchers Jason Kim, Jalen Chuang, and Daniel Genkin (all from Georgia Institute of Technology) along with Yuval Yarom (Ruhr University Bochum) analyzed Apple's M- and A-series processors in detail.

Manufacturers continually develop optimization techniques to enhance processor speed and performance. "Unfortunately, we keep realizing that security often gets the short end of the stick," explains Yuval Yarom.

The team examined Apple's Load Value Predictor (LVP), designed to accelerate computing by predicting computational steps and anticipating data retrieval from memory. The processor performs calculations based on these predictions and compares the results when the actual data arrives. If the prediction is incorrect, the processor discards the results and recomputes using the correct data.

Sensitive data can be spied out

The researchers demonstrated that Apple's LVP is prone to errors. "If the LVP guesses incorrectly, the CPU can perform arbitrary calculations with incorrect data under speculative execution. This can lead to critical checks in the program logic for memory security being bypassed, creating attack surfaces for spying on secrets stored in memory," the scientists warn.

Their findings show that attacks on web browsers such as Safari and Chrome are possible, potentially exposing sensitive information like credit card details, search histories, and calendar events.

A second paper by the same research team titled "SLAP: Data Speculation Attacks via Load Address Prediction on Apple Silicon" reveals another security vulnerability in Apple processors. Similar to "FLOP," the researchers examined a specific unit in the processor: the central processing unit (CPU)—the "brain" of a computer responsible for most calculations and tasks.

Starting with the M2/A15 series, all Apple processors are equipped with a Load Address Predictor (LAP), which predicts the next memory address from which the CPU will retrieve data. The research shows that when the LAP makes incorrect predictions, arbitrary calculations can be initiated, creating a significant security risk.

"This enables an end-to-end attack on the Safari browser, allowing attackers to spy on email content or browser activity," the team explains.

The researchers reported these vulnerabilities to the Apple Product Security Team in May and September last year as part of Responsible Disclosure, providing ample time for countermeasures.

More information: Jason Kim et al. FLOP: Breaking the Apple M3 CPU via False Load Output Predictions. predictors.fail/files/FLOP.pdf

Jason Kim et al. SLAP: Data Speculation Attacks via Load Address Prediction on Apple Silicon. predictors.fail/files/SLAP.pdf

Provided by Ruhr-Universitaet-Bochum

Citation: Security vulnerabilities discovered in Apple processors (2025, January 29) retrieved 31 January 2025 from https://techxplore.com/news/2025-01-vulnerabilities-apple-processors.html