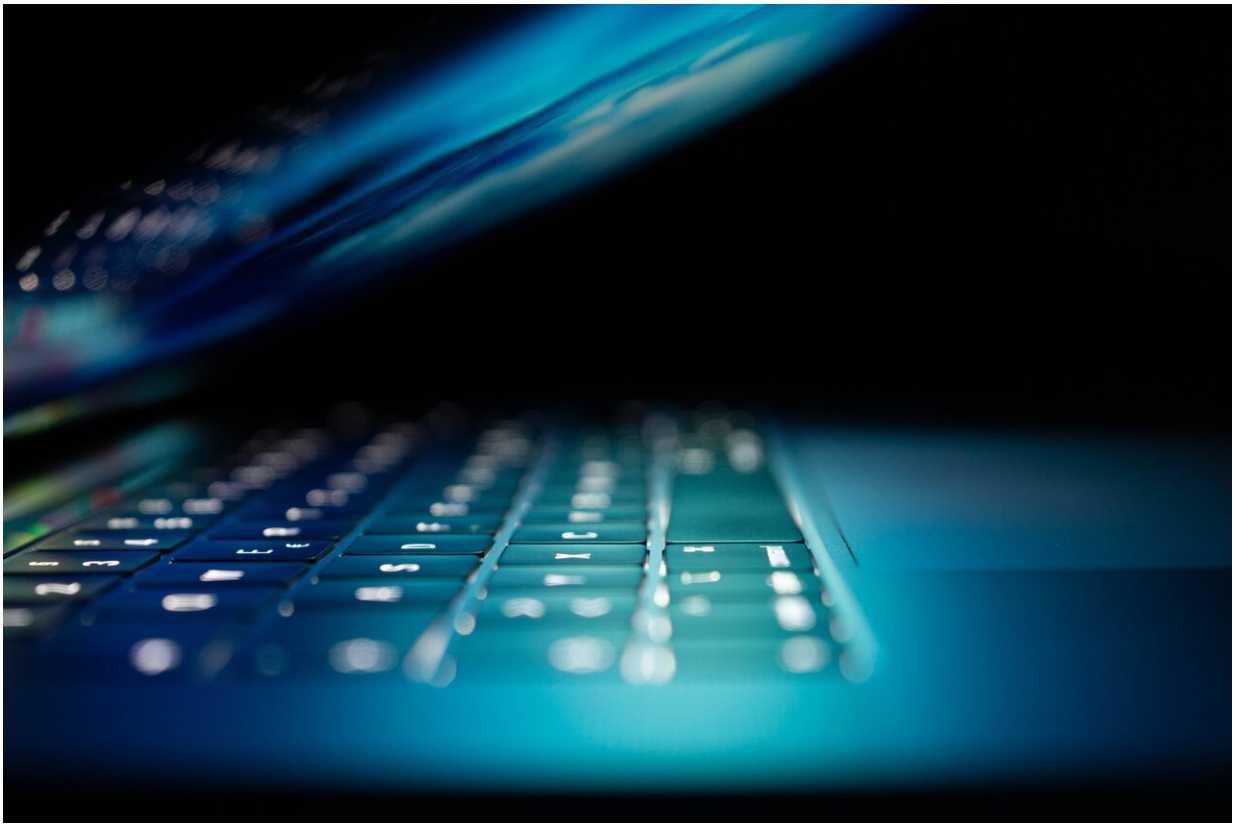
How randomized data can improve our security

August 9 2023



Credit: Unsplash/CC0 Public Domain

Huge streams of data pass through our computers and smartphones every day. In simple terms, technical devices contain two essential units to process this data: A processor, which is a kind of control center, and a

RAM, comparable to memory. Modern processors use a cache to act as a bridge between the two, since memory is much slower at providing data than the processor is at processing it.

This cache often contains private data that could be an attractive target for attackers. A team of scientists from Bochum, Germany, in cooperation with researchers from Japan, has now developed an innovative cipher that not only offers greater security than previous approaches, but is also more efficient and faster. They are presenting their work at the prestigious Usenix Security Symposium in Anaheim, California (U.S.).

The team includes Dr. Federico Canale and Professor Gregor Leander from the Chair of Symmetric Cryptography, Jan Philipp Thoma and Professor Tim Güneysu from the Chair of Security Engineering, all from Ruhr University Bochum, as well as Yosuke Todo from NTT Social Informatics Laboratories and Rei Ueno from Tohoku University (Japan).

Cache not well protected against side-channel attacks until now

Years ago, CASA PI Professor Yuval Yarom, who has been at Ruhr University since April 2023, discovered that the cache is not well protected against a certain type of attack. The serious Spectre and Meltdown vulnerabilities made headlines at the time because they affected all popular microprocessors as well as cloud services. Caches are unobtrusive, but they perform an important task: they store data that is requested very frequently. Its main function is to reduce latency.

If the CPU had to fetch from slower RAM every time it needed to access data, this would slow down the system. This is why the CPU fetches certain data from the cache. However, attackers can exploit this

communication between CPU and cache. Their method: They overwrite the cache's unsecured data. The system requests the data from main memory because it cannot find it in the cache. This process is measurably slower.

"In so-called timing side-channel attacks, attackers can measure the time differences and use them to observe memory accesses by other programs. Thus, they can steal private keys for encryption algorithms, for example," explains Jan Philipp Thoma from the Chair of Security Engineering.

Innovative mathematical solution

While patches have been developed to fix the vulnerability for certain attacks, they have failed to provide provable security. However, the team from Bochum and Japan has now come up with an innovative solution: "Our idea is to use mathematical processes to randomize the data in the cache," explains Gregor Leander, who recently received an ECR Advanced Grant for his research. This randomization in the CPU's caches can help prevent attacks by disabling attackers from removing data from the cache.

"The interdisciplinary approach of cryptography and hardware security considerations is a novelty in computer security. While there have been previous ideas for randomized cache architectures, none have been very efficient and none have been able to completely withhold strong attackers," said Tim Güneysu, who heads the Chair of Security Engineering. The new SCARF model uses block cipher encryption, a completely new idea for the field, according to the researchers.

"Normally, we encrypt data with 128 bits, in the cache we sometimes work with 10 bits. This is a complex process because it takes much longer to mix this data with a large key," said Gregor Leander. The large

key is needed because a shorter encryption of such small amounts of data could be more easily broken by attackers.

The aforementioned randomization usually takes a lot of time. This would limit the functionality of the cache. In contrast, SCARF uses block ciphers to operate faster than any previous solution. "SCARF can be used as a modular component in cache architectures and automatically ensures secure—i.e. unpredictable—randomization with simultaneously low latency, i.e. response time," explains Jan Philipp Thoma: "He concludes: "With SCARF, we offer an efficient and secure solution for randomization."

Double protection by combining with ClepsydraCache

The work done by the researchers can therefore have a fundamental impact on protecting sensitive data in the digital society. In addition, the researchers, in collaboration with other colleagues, present another work at this year's Usenix Security Symposium that can be combined with SCARF.

The paper, "ClepsydraCache—Preventing Cache Attacks with Time-Based Evictions," likewise introduces a new idea for cache security. Jan Philipp Thoma, Gregor Leander, Tim Güneysu and CASA PI Lucas Davi from the University of Duisburg-Essen are also involved.

It was also developed in close collaboration with researchers from the Department of Integrated Systems at RUB. "ClepsydraCache relies on cache decay combined with index randomization. Cache decay means that data that is not used for a longer period of time is automatically removed from the cache," explains Jan Philipp Thoma.

Data security benefits from such a mechanism, as it reduces the number of cache conflicts. Those conflicts would slow down the process and

might also lead to data leakage with the help of the side-channel attacks described above. The researchers were able to prove that their proposal can withstand known attack vectors and can be easily implemented in existing architectures.

Interdisciplinary work leads to successful research

The compatibility of the two "SCARF" and "Clepsydracache" works could therefore make future generations of caches more secure than ever before—without affecting their performance in any way. The teamwork thus shows that the interdisciplinary approach pursued by the Cluster of Excellence CASA "Cybersecurity in the Age of Large-Scale Adversaries" can lead to groundbreaking research results.

More information: CARF—A low-latency block cipher for secure cache-randomization, 32th USENIX Security Symposium, 2023, Anaheim, U.S., Pre-Print: www.usenix.org/system/files/us … ecurity23-canale.pdf

Preventing cache attacks with time-based evictions, 32th USENIX Security Symposium, 2023, Anaheim, U.S., Pre-Print: www.usenix.org/system/files/se … _48-thoma-prepub.pdf

Provided by Ruhr-Universitaet-Bochum