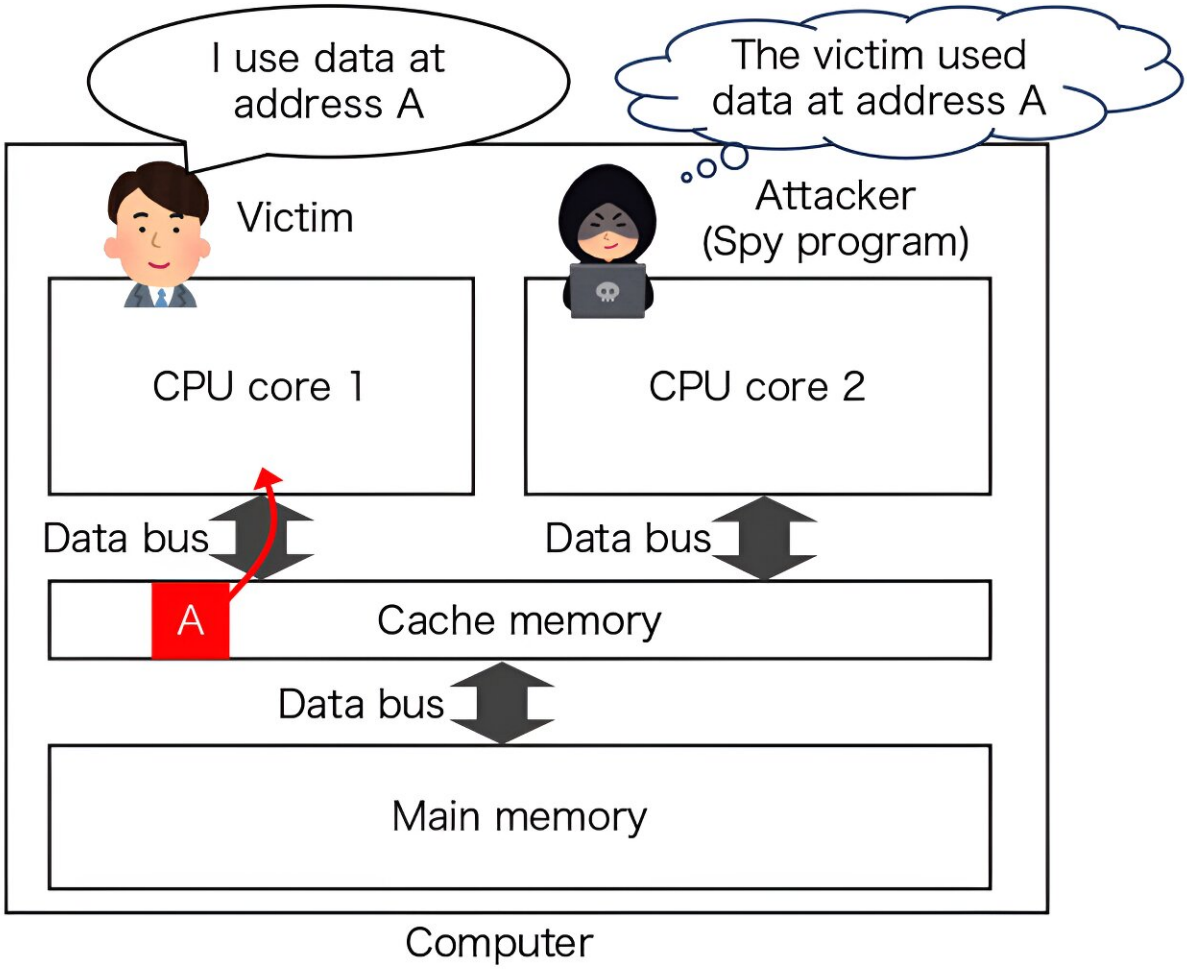
Researchers unveil new cipher system that protects computers against spy programs

August 1 2023



A schematic outlining how a hacker uses cache side-channel attacks. Credit: Rei Ueno

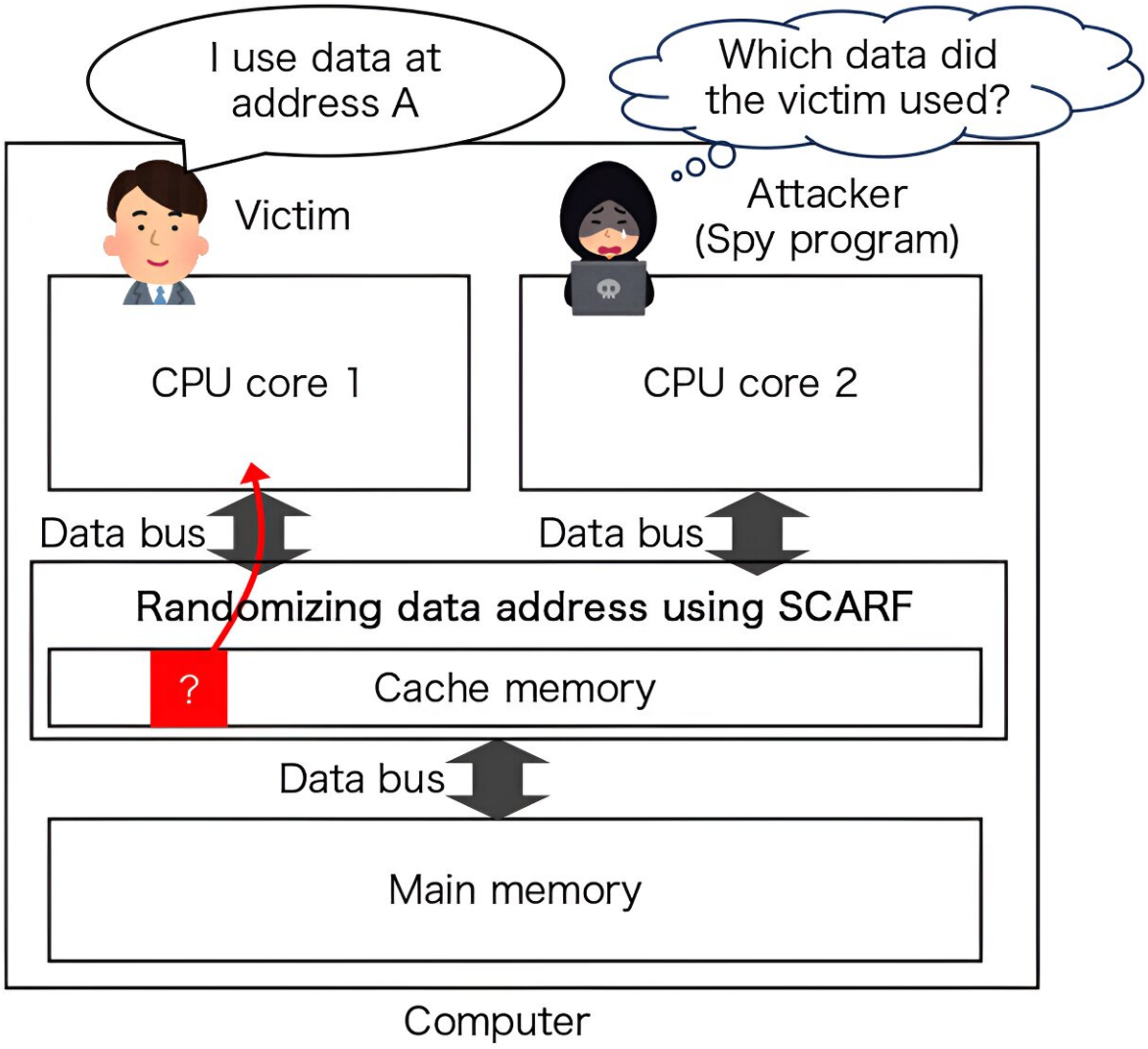
A group of international researchers has achieved a breakthrough in computer security with the development of a new and highly efficient cipher for cache randomization. The innovative cipher, designed by Assistant Professor Rei Ueno from the Research Institute of Electrical Communication at Tohoku University, addresses the threat of cache side-channel attacks, offering enhanced security and exceptional performance.

Cache side-channel attacks pose a significant threat to modern computer systems, as they can stealthily extract sensitive information, including secret keys and passwords, from unsuspecting victims. These attacks exploit vulnerabilities in the operating principles of contemporary computers, making their countermeasures extremely challenging.

Cache randomization has emerged as a promising countermeasure; however, identifying a secure and effective mathematical function for this purpose has been a lingering challenge.

To overcome this, Ueno and his colleagues created SCARF. SCARF is based on a comprehensive mathematical formulation and modeling of cache side-channel attacks, offering robust security. Moreover, SCARF exhibits remarkable performance, completing the randomization process with only half the latency of existing cryptographic techniques. The cipher's practicality and performance were thoroughly validated through rigorous hardware evaluations and system-level simulations.

The team comprised members from Tohoku University, CASA at Ruhr University Bochum, and NTT Social Informatics Laboratories at Nippon Telegraph and Telephone Corporation.



A schematic outlining how the new SCARF system operates. Credit: Rei Ueno

"We are thrilled to announce SCARF, a powerful tool in enhancing computer security," said Ueno. "Our innovative cipher is engineered to be compatible with various modern computer architectures, ensuring its widespread applicability and potential to bolster computer security significantly."

SCARF's potential impact extends beyond individual computers, as its implementation has the capacity to contribute to building a more secure information society. By mitigating cache side-channel attack vulnerabilities, SCARF takes a critical step towards safeguarding sensitive data and user privacy.

The paper detailing the development will be presented at the USENIX Security Symposium on August 9, 2023.

Provided by Tohoku University