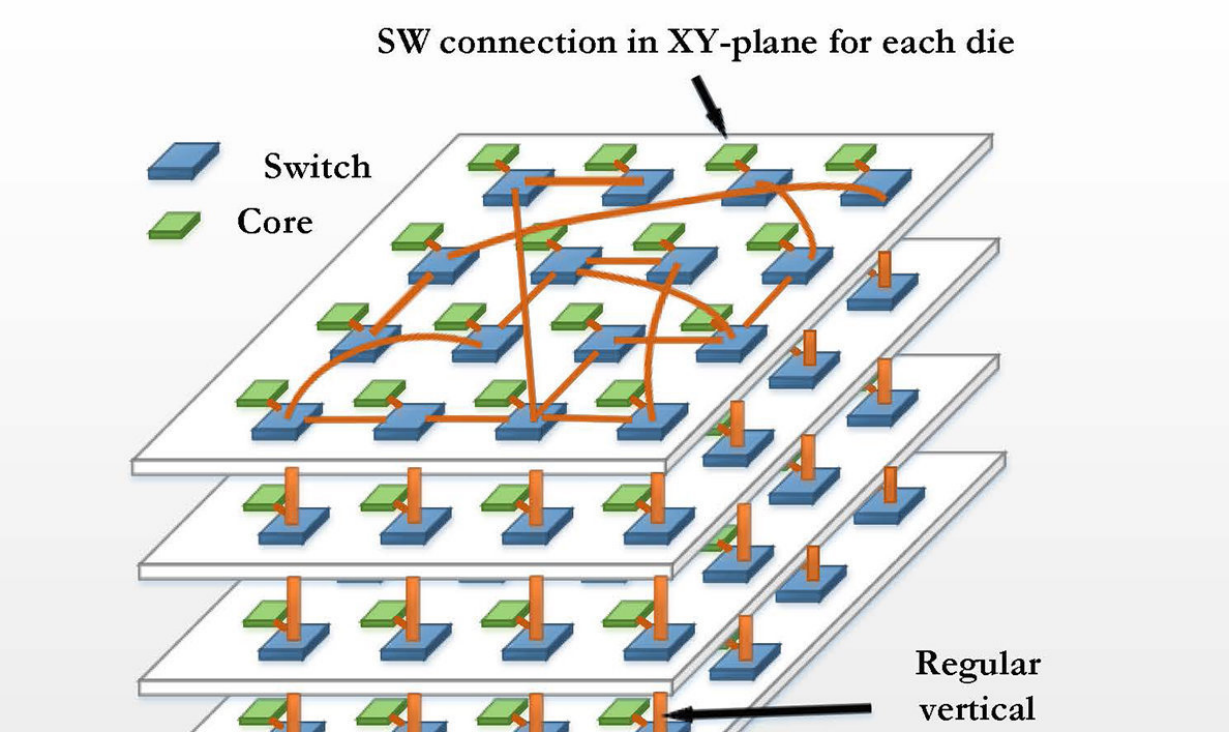
Researchers discover computer chip vulnerabilities

December 13 2018, by Tina Hilding



This figure shows a 3D manycore chip where the processing cores are connected through vertical links. Credit: Washington State University

A Washington State University research team has uncovered significant and previously unknown vulnerabilities in high-performance computer chips that could lead to failures in modern electronics.

The researchers found they could damage the on-chip communications system and shorten the lifetime of the whole computer chip significantly by deliberately adding malicious workload.

Led by Partha Pande, assistant professor in the School of Electrical Engineering and Computer Science, they reported on the work during the recent 2018 IEEE/ACM International Symposium on Networks-on-Chip.

Researchers have been working to understand the vulnerabilities of computer chips as a way to prevent malicious attacks on the electronics that make up everyday life. Some consumer electronics vendors, such as Apple and Samsung, have been accused of exploiting vulnerabilities in their own electronics and sending software updates that intentionally slow down earlier phone models to encourage consumers to purchase new products.

Previous researchers have studied computer chip components, such as the processors, computer memory and circuits for security vulnerabilities , but the WSU research team found significant vulnerabilities in the sophisticated communications backbone of high-performance computer chips.

"The communications system is the glue that holds everything together," said Pande. "When it starts to malfunction, the whole system is going to crumble."

High-performance computers use a large number of processors and do parallel processing for big data applications and cloud computing, and the communications system coordinates the processors and memory. Researchers are working to increase the number of processors and incorporate high-performance capabilities into hand-held devices.

The researchers devised three "craftily constructed deleterious" attacks to test the communications system. This additional workload enhanced electromigration-induced stress and crosstalk noise. The researchers found that a limited number of crucial vertical links of the communication system were particularly vulnerable to fail. Those links connect the processors in a stack and allows them to talk with each other.

"We determined how an agent can target the communication system to start malfunctions in the chip," said Pande. "The role of the communications and the threat had not been clear to the research community before."

The researchers will now be working to develop ways to mitigate the problem, such as automated techniques and algorithms to detect and thwart attacks.

More information: Sourav Das et al, Abetting Planned Obsolescence by Aging 3D Networks-on-Chip, *2018 Twelfth IEEE/ACM International Symposium on Networks-on-Chip (NOCS)* (2018). DOI: 10.1109/NOCS.2018.8512162

Provided by Washington State University