World's fastest open-source intrusion detection is here

November 5 2020, by Daniel Tkacik

An FPGA integrated circuit (Intel's Stratix 10 FPGA shown here) is essential to the performance of the CMU team's intrusion detection system. Credit: Intel

Intrusion detection systems are the invisible intelligence agencies in

computer networks. They scan every packet of data that is passed through the network, looking for signs of any one of the tens of thousands of different types of cyberattacks they're aware of.

As Internet speeds continue to increase, so too does the amount of data that passes through. To keep up, intrusion detection systems have grown into giant racks and stacks of servers, driving energy costs up for organizations that rely on them for protection.

That's all about to change. Researchers in Carnegie Mellon University's CyLab have developed the fastest-ever open-source intrusion detection system—one that achieves speeds of 100 gigabits per second using a single server.

"What was previously possible with 100-700 processor cores and a whole rack of machines, we can now do with five processor cores in a single server," says CyLab's Justine Sherry, an assistant professor in the Computer Science Department (CSD) in the School of Computer Science.

The researchers are presenting their work at this week's USENIX Symposium on Operating Systems Design and Implementation.

Key to the researchers' success is the use of a field-programmable gate array (FPGA), an integrated circuit for which users can write code and customize, hence "field-programmable." The researchers programmed the FPGA to be tailored for the sole job of intrusion detection and wrote that algorithms which can't run on traditional processors and are significantly faster.

When placed in a network, Sherry says that an average of 95 percent of data packets are processed by the FPGA on its own, while the other five percent are passed on to central processing units when it becomes

overwhelmed, hence the necessity of five processor cores in their system.

"The FPGA does most of the work, but some of it still goes to the processors," Sherry says.

The result in energy-savings is enormous: their intrusion detection system uses 38 times less power using an FPGA than hundreds of processing cores would in performing the same work.

"It's like your electricity bill used to be $100, and now it's $3," says Sherry. "We created one pizza box-sized machine to do the work of a whole room of servers."

The researchers' code is open-sourced and available for download on GitHub.

More information: www.usenix.org/conference/osdi … ntation/zhao-zhipeng

Provided by Carnegie Mellon University