New approach allows for faster ransomware detection

16 May 2022, by Matt Shipman

Credit: Pixabay/CC0 Public Domain

Researchers have developed a new approach for implementing ransomware detection techniques, allowing them to detect a broad range of ransomware far more quickly than using previous systems.

Ransomware is a type of malware. When a system is infiltrated by ransomware, the ransomware encrypts that system's data—making the data inaccessible to users. The people responsible for the ransomware then extort the affected system's operators, demanding money from the users in exchange for granting them access to their own data.

Ransomware extortion is hugely expensive, and instances of ransomware extortion are on the rise. The FBI reports receiving 3,729 ransomware complaints in 2021, with costs of more than $49 million. What's more, 649 of those complaints were from organizations classified as critical infrastructure.

"Computing systems already make use of a variety of security tools that monitor incoming traffic to detect potential malware and prevent it from compromising the system," says Paul Franzon, co-author of a paper on the new ransomware detection approach. "However, the big challenge here is detecting ransomware quickly enough to prevent it from getting a foothold in the system. Because as soon as ransomware enters the system, it begins encrypting files." Franzon is Cirrus Logic Distinguished Professor of Electrical and Computer Engineering at North Carolina State University.

"There's a machine-learning algorithm called XGBoost that is very good at detecting ransomware," says Archit Gajjar, first author of the paper and a Ph.D. student at NC State. "However, when systems run XGBoost as software through a CPU or GPU, it's very slow. And attempts to incorporate XGBoost into hardware systems have been hampered by a lack of flexibility—they focus on very specific challenges, and that specificity makes it difficult or impossible for them to monitor for the full array of ransomware attacks."

"We've developed a hardware-based approach that allows XGBoost to monitor for a wide range of ransomware attacks, but is much faster than any of the software approaches," Gajjar says.

The new approach is called FAXID, and in proof-of-concept testing, the researchers found it was just as accurate as software-based approaches at detecting ransomware. The big difference was speed. FAXID was up to 65.8 times faster than software running XGBoost on a CPU and up to 5.3 times faster than software running XGBoost on a GPU.

"Another advantage of FAXID is that it allows us to run problems in parallel," Gajjar says. "You could devote all of the dedicated security hardware's resources to ransomware detection, and detect ransomware more quickly. But you could also allocate the security hardware's computing power to separate problems. For example, you could

devote a certain percentage of the hardware to ransomware detection and another percentage of the hardware to another challenge—such as fraud detection."

"Our work on FAXID was funded by the Center for Advanced Electronics through Machine Learning (CAEML), which is a public-private partnership," Franzon says. "The technology is already being made available to members of the center, and we know of at least one company that is making plans to implement it in their systems."

The paper, "FAXID: FPGA-Accelerated XGBoost Inference for Data Centers using HLS," is being presented at the 30th IEEE International Symposium on Field-Programmable Custom Computing Machines (FCCM), being held in New York City from May 15-18.

More information: Conference: www.fccm.org/technical-program-2022/

Provided by North Carolina State University