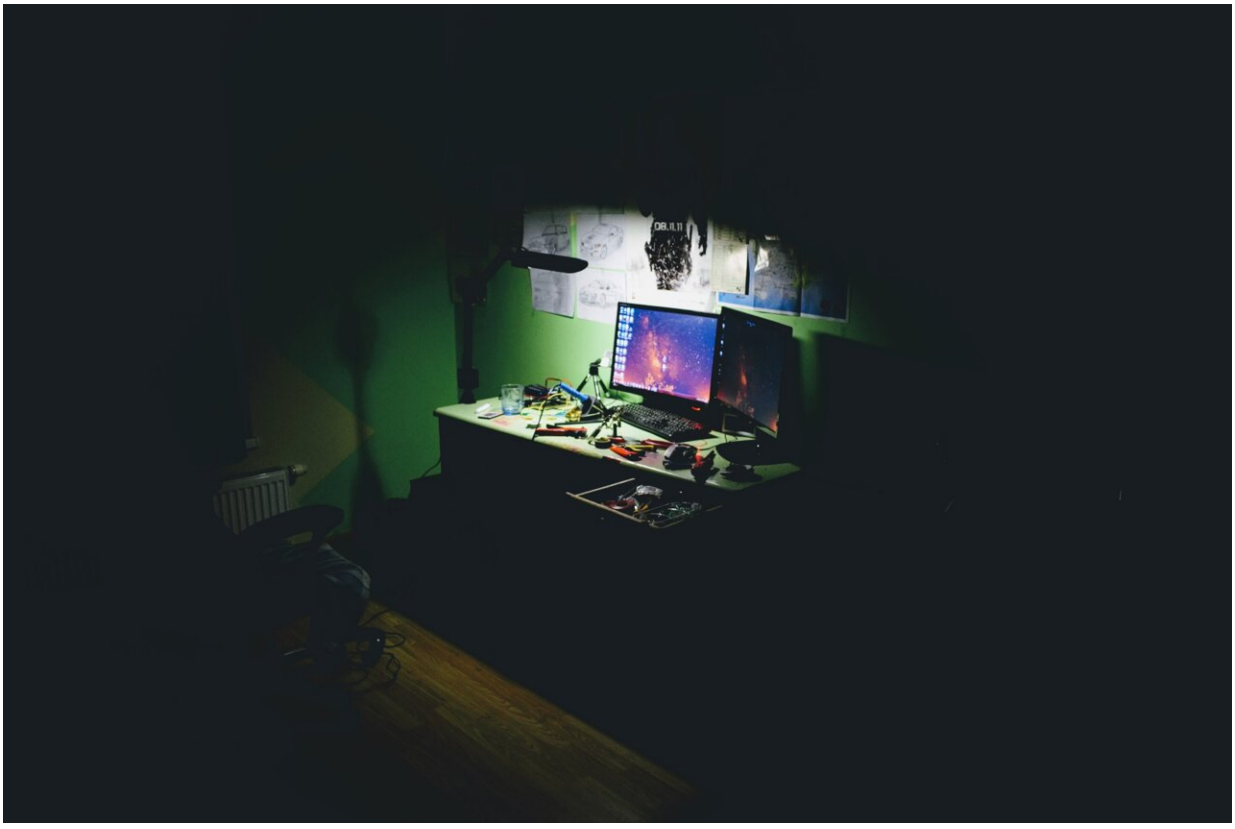
Researchers strengthen defenses against denial-of-service attack

August 3 2023, by Tom Rickey



Credit: Unsplash/CC0 Public Domain

Scientists have developed a better way to recognize a common internet attack, improving detection by 90 percent compared to current methods.

The new technique developed by computer scientists at the Department of Energy's Pacific Northwest National Laboratory works by keeping a watchful eye over ever-changing traffic patterns on the internet. The findings were presented on August 2 by PNNL scientist Omer Subasi at the IEEE International Conference on Cyber Security and Resilience, where the manuscript was recognized as the best research paper presented at the meeting.

The scientists modified the playbook most commonly used to detect denial-of-service attacks, where perpetrators try to shut down a website by bombarding it with requests. Motives vary: Attackers might hold a website for ransom, or their aim might be to disrupt businesses or users.

Many systems try to detect such attacks by relying on a raw number called a threshold. If the number of users trying to access a site rises above that number, an attack is considered likely, and defensive measures are triggered. But relying on a threshold can leave systems vulnerable.

"A threshold just doesn't offer much insight or information about what it is really going on in your system," said Subasi. "A simple threshold can easily miss actual attacks, with serious consequences, and the defender may not even be aware of what's happening."

A threshold can also create false alarms that have serious consequences themselves. False positives can force defenders to take a site offline and bring legitimate traffic to a standstill—effectively doing what a real denial-of-service attack, also known as a DOS attack, aims to do.

"It's not enough to detect high-volume traffic. You need to understand that traffic, which is constantly evolving over time," said Subasi. "Your network needs to be able to differentiate between an attack and a harmless event where traffic suddenly surges, like the Super Bowl. The

behavior is almost identical."

As principal investigator Kevin Barker said, "You don't want to throttle the network yourself when there isn't an attack underway."

Denial of service—denied

To improve detection accuracy, the PNNL team sidestepped the concept of thresholds completely. Instead, the team focused on the evolution of entropy, a measure of disorder in a system.

Usually on the internet, there's consistent disorder everywhere. But during a denial-of-service attack, two measures of entropy go in opposite directions. At the target address, many more clicks than usual are going to one place, a state of low entropy. But the sources of those clicks, whether people, zombies or bots, originate in many different places —high entropy. The mismatch could signify an attack.

In PNNL's testing, 10 standard algorithms correctly identified on average 52 percent of DOS attacks; the best one correctly identified 62 percent of attacks. The PNNL formula correctly identified 99 percent of such attacks.

The improvement isn't due only to the avoidance of thresholds. To improve accuracy further, the PNNL team added a twist by not only looking at static entropy levels but also watching trends as they change over time.

Formula vs. formula: Tsallis entropy for the win

In addition, Subasi explored alternative options to calculate entropy. Many denial-of-service detection algorithms rely on a formula known as

Shannon entropy. Subasi instead settled on a formula known as Tsallis entropy for some of the underlying mathematics.

Subasi found that the Tsallis formula is hundreds of times more sensitive than Shannon at weeding out false alarms and differentiating legitimate flash events, such as high traffic to a World Cup website, from an attack.

That's because the Tsallis formula amplifies differences in entropy rates more than the Shannon formula. Think of how we measure temperature. If our thermometer had a resolution of 200 degrees, our outdoor temperature would always appear to be the same. But if the resolution were 2 degrees or less–like most thermometers–we'd detect dips and spikes many times each day. Subasi showed that it's similar with subtle changes in entropy, detectable through one formula but not the other.

The PNNL solution is automated and doesn't require close oversight by a human to distinguish between legitimate traffic and an attack. The researchers say that their program is "lightweight"—it doesn't need much computing power or network resources to do its job. This is different from solutions based on machine learning and artificial intelligence, said the researchers. While those approaches also avoid thresholds, they require a large amount of training data.

Now, the PNNL team is looking at how the buildout of 5G networking and the booming internet of things landscape will have an impact on denial-of-service attacks.

"With so many more devices and systems connected to the internet, there are many more opportunities than before to attack systems maliciously," Barker said. "And more and more devices like home security systems, sensors and even scientific instruments are added to networks every day. We need to do everything we can to stop these attacks."

More information: Omer Subasi et al, Denial-of-Service Attack Detection via Differential Analysis of Generalized Entropy Progressions, *arXiv* (2021). DOI: 10.48550/arxiv.2109.08758

Provided by Pacific Northwest National Laboratory