Publication: Asian Scientist
Date: 31 May 2016
Headline: The Internet Defender

The Internet Defender

Surprising insights into the role of high frequency traders and short sellers revealed by SMU Professor of Finance Ekkehart Boehmer's research.

PUBLISHED ON MAY 31, 2016

AsianScientist (May 31, 2016) - By Sim Shuzhen - Distributed Denial-of-Service (DDoS) attacks are increasingly in the news, and are becoming ever more sophisticated and larger in scale. In these attacks, an adversary tries to overwhelm and crash important services such as government websites, bank servers and credit card payment gateways by flooding them with messages that originate from thousands of different Internal Protocol (IP) addresses.

Leading the fight against this scourge is computer security expert Virgil Gligor, visiting professor at the Singapore Management University (SMU) School of Information Systems (SIS).

On sabbatical from Carnegie Mellon University in the United States, where he is a professor in the Department of Electrical and Computer Engineering, Professor Gligor is no stranger to Singapore. He first visited in the early 1980s to deliver lectures on computer security at the invitation of then-National Computer Board. Since then, he has also served on the advisory board of SIS. This time, he hopes to establish collaborations with local researchers in the areas of trustworthy computing systems and applied cryptographic protocols.

Finding and thwarting DDoS attacks

“As technology advances, and as the Internet connects more people and more services, the possibility and real examples of DDoS have increased in number,” says Professor Gligor.

Besides their potential to disrupt important services, there may also be a more insidious side to these attacks, Professor Gligor notes. The use of DDoS as a threat to extort payments from companies is on the rise, and there is evidence that some countries have launched politically-motivated attacks against services in other nation states.

Professor Gligor is working to anticipate and discover new classes of DDoS attacks that could potentially target vulnerable spots on the Internet.

“In order to look for defences against new problems, you have to find the new problems,” he explains.

He has shown, for example, that routing bottlenecks—key routers with links to many hosts—arise as a natural property of the Internet. Their highly connected nature, however, makes them an ideal target for DDoS attacks. The research has been published in a conference paper “Routing Bottlenecks in the Internet: Causes, Exploits, and Countermeasures” in the *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*.

.

In scenarios known as crossfire attacks—discovered by Professor Gligor and students and published in a conference paper “The Crossfire Attack” in the *2013 IEEE Symposium on Security and Privacy*—the adversary attempts to flood and crash these routers by sending them traffic from tens of thousands of bots

under its control. Such attacks have the potential to disrupt communications on a large scale—an entire city, state or small country could be cut off from the outside world.

Probing the Internet’s weak spots

DDoS attacks are relatively new problems that are extremely difficult to prevent or resolve, says Professor Gligor.

“Twenty years ago, there were very few instances of distributed computations that could attack a particular website. An adversary could not gather so much computing capacity,” he explains. Now, however, economics is on the side of the adversary, who can buy bots by the thousand on the “bot market”—likely an offshoot of the spamming industry—at very low prices. In contrast, it costs a lot more for the defender to increase the bandwidths of key routers, which would help mitigate the flooding.

DDoS attacks also tend to be stealthy. Bot networks generate low-intensity traffic that is indistinguishable from legitimate traffic, making attacks hard to detect until it is too late. In addition, bottleneck routers often belong to different Internet service providers (ISPs). Since bot traffic on an individual router is often not intense enough to raise an alarm, the only way to detect an attack is for ISPs to communicate with each other. In practice, however, these companies are more likely to compete than to collaborate.

Possible solutions, says Professor Gligor, include reversing the cost asymmetry, or forcing the adversary into a conflict-of-interest situation. The latter option might involve having the attacked router instruct its sources to reroute their traffic. If the adversary complies, the attack is unsuccessful; if it does not, then the traffic stands out as adversarial.

Such deterrents, however, only work if the adversary is rational. This may not always be the case—political attacks, for example, might involve irrational or cost-insensitive adversaries.

In addition to theoretical analysis, Professor Gligor and his colleagues also use simulations and real Internet measurements to test their hypotheses and propose solutions. Tracing packet routes from presumed locations of bots, for example, allows them to detect routing bottlenecks in the network of a bank’s website. In the laboratory, they then simulate attacks on these routers, working out important parameters such as bottleneck size, cost, impact and overall feasibility.

The future of computer security

A major threat that users will continue to face in the future, says Professor Gligor, is the presence of security loopholes in computer software. While it costs little for software makers to enter the market, there are no regulations stipulating basic levels of security for their products. Software makers also absolve themselves of liability through End User License Agreements.

This combination of factors has had a tremendous effect on software innovation, says Professor Gligor. Further compounding the problem, there are also no incentives for programmers to produce secure software—an undertaking which requires much more time and effort.

“Security is going to remain a problem of fundamental importance for many years to come. It’s not something we can solve with a silver bullet,” he says. “As technology advances and becomes more complex—and more useful in many ways—there will be more avenues of attack.”

Asian Scientist Magazine is a media partner of the Singapore Management University Office of Research.