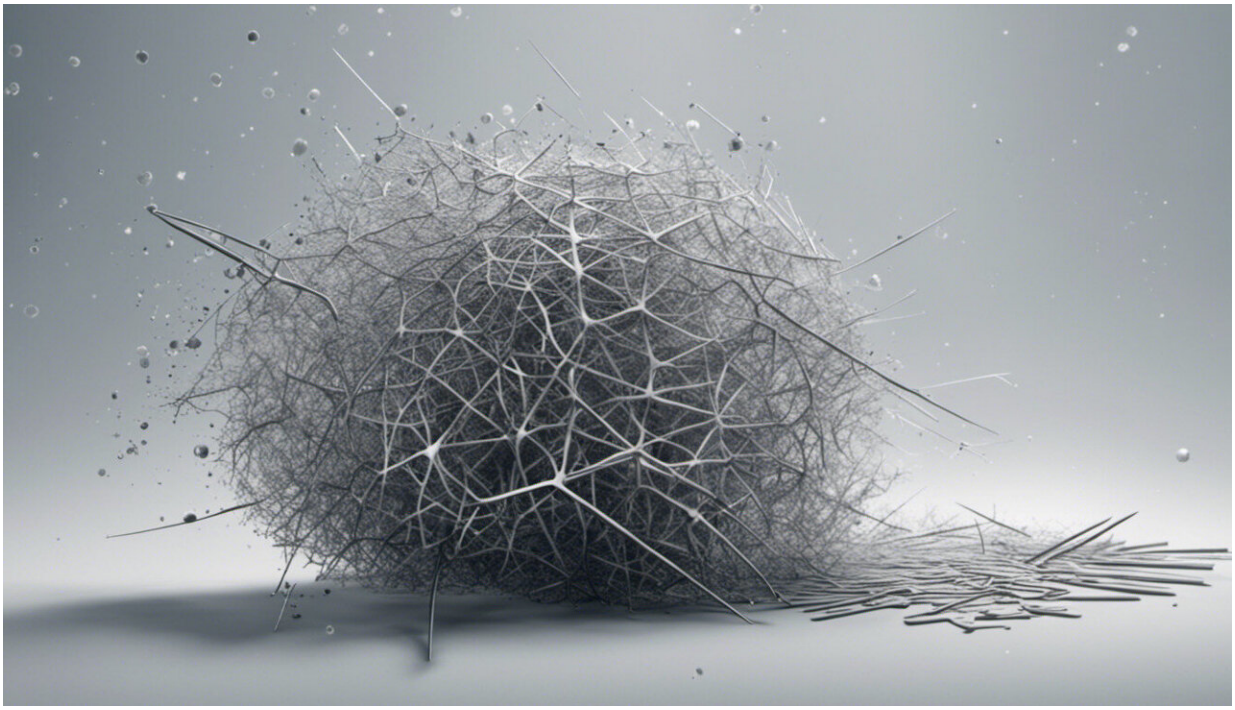
Logjam isn't the only reason your computer might be more vulnerable to internet threats

May 25 2015, by Andrew Smith



Credit: AI-generated image (disclaimer)

There's a hole in the protection surrounding some of the internet's supposedly secure websites. A group of researchers has discovered that cyber criminals and other hackers can attack websites that use the "https" security encryption using a method known as "Logjam". This attack, which is thought to work on around 8% of the top one million

websites, allows hackers to see important information that should be protected, such as payment details or private communication.

Encryption is a way of turning information into a secret code in order to stop others from eavesdropping on your internet conversations. Every time you see a padlock or then letters "https" in the address bar of your web browser, everything being sent between your computer and the remote web server where the website you are viewing is stored is encrypted and should be secret. The discovery of the Logjam attack, which is possible because of a flaw in the security software, means this may not always be the case.

Logjam works by attacking a part of the security process called the "Diffie-Hellman key exchange". This is a way of creating and securely sending the key that unlocks the encryption and allows you to read the information. This key is formed using two very large, complex and random prime numbers (numbers that can only be divided by themselves or the number one), which cannot easily be predicted. The larger the key, the stronger the encryption.

Older keys are saved with 1024 bits of computer memory, meaning each one has 2^{1024} possible combinations. But computers are now powerful enough to work out what the right combination is. The Logjam attack involves capturing the key data and then using computational power to crack its code. As a result, security experts are advising web sites that still use these keys to move to much longer versions that are harder to predict.

Hackers can also use something called a rainbow table to look up pre-cracked codes and use their computer to match the key against them. The more power a computer has, the faster it can work through the database of pre-cracked codes. There are still multiple combinations to check, but the work has in part already been done for them.

The growing power of computers means many existing security measures are increasingly likely to become obsolete and need replacing. However, it's not just companies failing to keep up with the latest advances that could leave internet users more vulnerable. Most technology companies are trying to create stronger security for their products because we (their customers) demand it. But there is also a trade-off between national security and personal security they have to be aware of.

Agencies such as the FBI have stated that some methods of encryption are now too strong, meaning they want to be able to peek at people's communications. They want encryption to be strong but not impenetrable. This has become a frustrating dilemma and, as Logjam proves by exploiting weaker Diffe-Hellman keys, there are weaker servers at the lower end that may fall foul of this demand to balance the security expectations of their organisation with the policing demands of governmental bodies.

There is already a flurry of activity across the internet as server administrators are attempting to patch the Logjam problem and increase their security level for key exchanges. We'll just have to hope that they can accomplish this before someone compromises their servers. While only a proportional minority of websites are affected by Logjam, you can also check your web browser and see if it needs updating.

Source: The Conversation

vulnerable-internet-threats.html