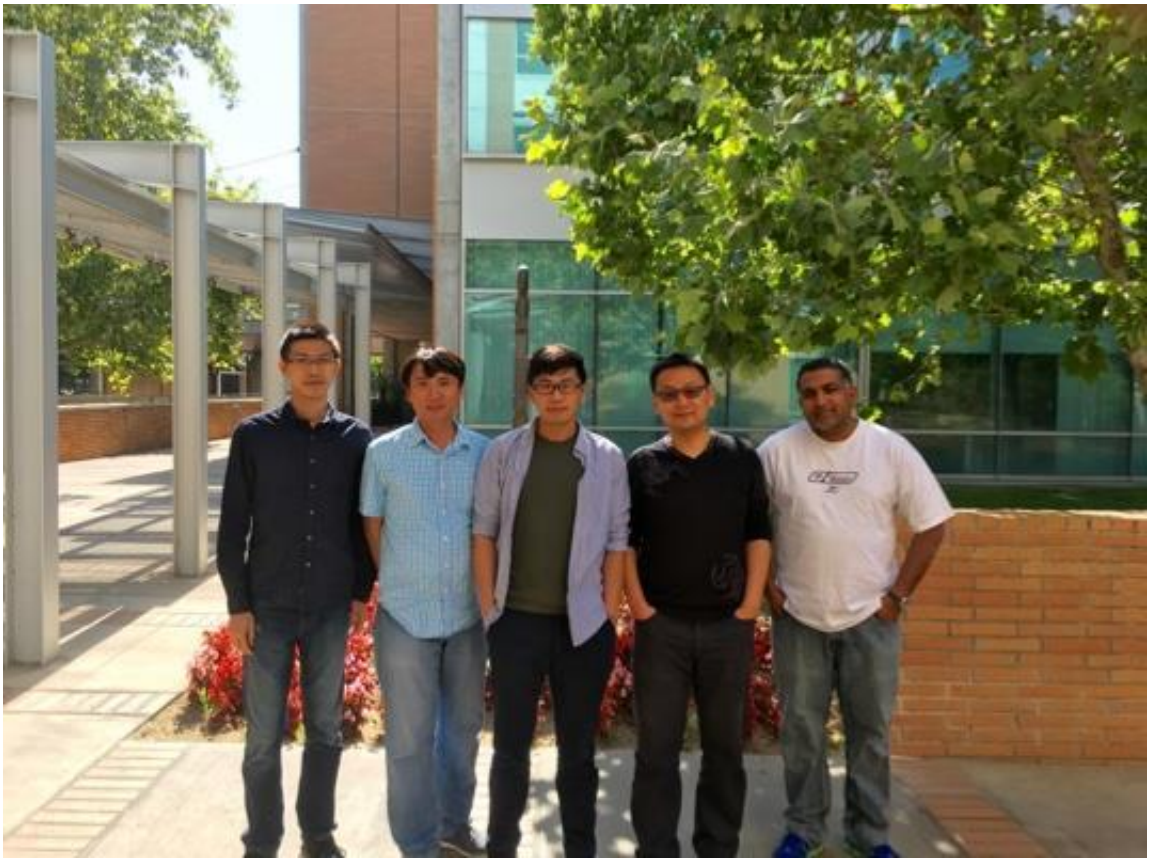
Study highlights serious security threat to many internet users

August 9 2016



Research team (left to right): Zhongjie Wang, Tuan Dao, Yue Cao, Zhiyun Qian and Srikanth V. Krishnamurthy. Credit: UC Riverside

Researchers at the University of California, Riverside have identified a weakness in the Transmission Control Protocol (TCP) of all Linux operating systems since late 2012 that enables attackers to hijack users'

internet communications completely remotely.

Such a weakness could be used to launch targeted attacks that track users' online activity, forcibly terminate a communication, hijack a conversation between hosts or degrade the privacy guarantee by anonymity networks such as Tor.

Led by Yue Cao, a computer science graduate student in UCR's Bourns College of Engineering, the research will be presented on Wednesday (Aug. 10) at the USENIX Security Symposium in Austin, Texas. The project advisor is Zhiyun Qian, an assistant professor of computer science at UCR, whose research focuses on identifying security vulnerabilities to help software companies improve their systems.

While most users don't interact directly with the Linux operating system, the software runs behind-the -scenes on internet servers, android phones and a range of other devices. To transfer information from one source to another, Linux and other operating systems use the Transmission Control Protocol (TCP) to package and send data, and the Internet Protocol (IP) to ensure the information gets to the correct destination.

For example, when two people communicate by email, TCP assembles their message into a series of data packets—identified by unique sequence numbers—that are transmitted, received, and reassembled into the original message. Those TCP sequence numbers are useful to attackers, but with almost 4 billion possible sequences, it's essentially impossible to identify the sequence number associated with any particular communication by chance.

The UCR researchers didn't rely on chance though. Instead, they identified a subtle flaw (in the form of 'side channels') in the Linux software that enables attackers to infer the TCP sequence numbers associated with a particular connection with no more information than

the IP address of the communicating parties.

This means that given any two arbitrary machines on the internet, a remote blind attacker without being able to eavesdrop on the communication, can track users' online activity, terminate connections with others and inject false material into their communications. Encrypted connections (e.g., HTTPS) are immune to data injection, but they are still subject to being forcefully terminated by the attacker. The weakness would allow attackers to degrade the privacy of anonymity networks, such as Tor, by forcing the connections to route through certain relays. The attack is fast and reliable, often taking less than a minute and showing a success rate of about 90 percent.

Qian said unlike conventional cyber attacks, users could become victims without doing anything wrong, such as downloading malware or clicking on a link in a phishing email.

"The unique aspect of the attack we demonstrated is the very low requirement to be able to carry it out. Essentially, it can be done easily by anyone in the world where an attack machine is in a network that allows IP spoofing. The only piece of information that is needed is the pair of IP addresses (for victim client and server), which is fairly easy to obtain," Qian said.

Qian said the researchers have alerted Linux about the vulnerability, which has resulted in patches applied to the latest Linux version. Until then, Qian recommends the following temporary patch that can be applied to both client and server hosts. It simply raises the `challenge ACK limit' to an extremely large value to make it practically impossible to exploit the side channel. This can be done on Ubuntu, for instance, as follows:

1. Open /etc/sysctl.conf, append a command

"/net.ipv4/tcp_challenge_ack_limit = 999999999".

2. Use "sysctl -p" to update the configuration.

Provided by University of California - Riverside