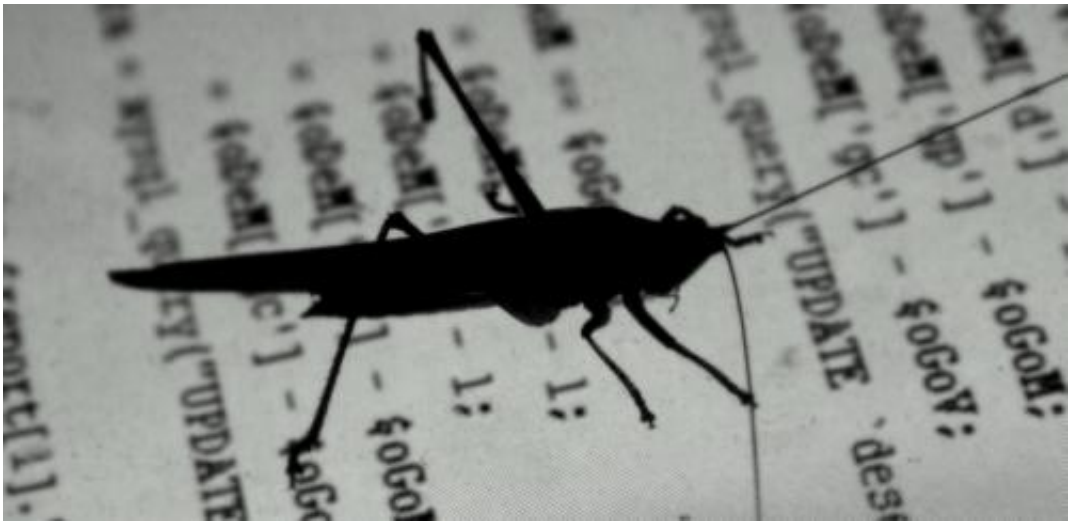
New vulnerability discovered in common online security

March 2 2016, by David Ellis



New bugs in the code for OpenSSL. Credit: Flickr/Guilherme Tavares, CC BY-NC

One of the world's most common security software packages – used as the basis of protection for many web browsers – has been found to be vulnerable to a specific form of attack, according to research led by the University of Adelaide.

OpenSSL provides encryption protection for a range of applications on most types of computers and is similar to the encryption packages used by the web browsers Google Chrome (BoringSSL) and Firefox (Mozilla's Network Security Service (NSS)).

Dr Yuval Yarom, Research Associate at the University of Adelaide's School of Computer Science, says he and colleagues Daniel Genkin (Tel Aviv University) and Dr Nadia Heninger (University of Pennsylvania) have discovered that OpenSSL is vulnerable to a type of attack known as a "side channel attack".

A side channel attack enables a hacker to take important information about software by examining the physical workings of a computer system – such as minute changes in power usage, or observing changes in timing when different software is being used.

Dr Yarom has found that it is possible to "listen in" to the workings of the OpenSSL encryption software. In the team's case, they measured highly sensitive changes in the computer's timing – down to less than one nanosecond (one billionth of a second). From these measurements they recovered the private key which OpenSSL uses to identify the user or the computer.

"In the wrong hands, the private key can be used to 'break' the encryption and impersonate the user," Dr Yarom says.

"At this stage we have only found this vulnerability in computers with Intel's 'Sandy Bridge' processors. Computers with other Intel processors may not be affected in the same way."

Dr Yarom says the likelihood of someone hacking a computer using this method is slim: "We seem to be the first to have done it, and under controlled conditions.

"Servers, particularly Cloud servers, are a more likely target for this side-channel attack. It's less likely that someone would use it against a home computer. There are so many easier-to-exploit vulnerabilities in home computers that it's unlikely someone would try to do this in the real

world – but not impossible."

Dr Yarom says there have been debates about this form of attack on OpenSSL for more than 10 years now, with some manufacturers claiming it couldn't be done. "But we have proven the vulnerability exists," he says.

"With OpenSSL being the most commonly used cryptographic software in the world right now, it's important for us to stay vigilant against any possible attack, no matter how small its chances might be.

"Once we discovered the vulnerability, we contacted the developers of OpenSSL and have been helping them to develop a fix for the problem," he says.

Provided by University of Adelaide