TRULY SECURE? NOT NECESSARILY SO.
You keep unique passwords. Run the latest anti-virus software. Order only from the most trusted online vendors. Your online information is secure, right? Maybe not.

In April 2014, millions of Internet users were forced to face the harsh reality that their most valuable information—Social Security numbers, credit card information, email passwords, and more—potentially had been compromised, all because of a simple, overlooked software programming bug called Heartbleed.

The flaw had exposed a loophole in the OpenSSL security protocol, a type of encryption software that provides security among devices connecting over a network. For hackers, the bug created an easy entry point for acquiring passwords that ostensibly protect such sensitive information as financial records, healthcare databases, and email communication.

In the weeks and months that followed the revelation, software developers seeking to protect the estimated two-thirds of web servers susceptible to Heartbleed released software patches and implored users to change their passwords. Unfortunately, the potential for damage had already been unleashed. As The Washington Post's Lindsey Bever put it, “It’s as if someone went on vacation not knowing the lock on the front door was broken. Could someone walk in? Yes. Will they? Did they? Who knows?”

C O L L A B O R A T I N G T O T H W A R T V U L N E R A B I L I T I E S

The Internet, often analogized to the Wild West, thrives in a largely unregulated infrastructure that has spawned countless valuable technological innovations. Too often, however, security considerations have come as an afterthought—something McCormick researchers hope to change.

More than a year before the public became aware of the Heartbleed bug, Yan Chen, professor of electrical engineering and computer science, and his research team had set out to develop an automated approach that could locate similar security vulnerabilities in other SSL encryption protocols like OpenSSL.

“Almost all Internet authentication systems are based on SSL, which means these vulnerabilities are inherent to the Internet as a whole,” Chen says.

Collaborating with researchers at the University of Illinois at Chicago, Columbia University, and Zhejiang University in China, Chen’s team created and implemented SSLint, a programming tool that can accurately and efficiently scan a security software’s source code and detect vulnerabilities.

To test SSLint, the researchers spent two years analyzing millions of lines of code within 485 different SSL and TLS security programs. They uncovered 27 previously unknown vulnerabilities.

“Previous studies had failed to reveal the scale of SSL vulnerabilities. The sheer number we found indicates either widespread inexperience or unwitting carelessness of some developers,” says Vaibhav Rastogi, a PhD candidate in Chen’s group and co-author of the study. “SSL and its successor TLS form the security backbone of the Internet, and vulnerabilities betray the trust people place in it. Users are left exposed to spying and modification of their communications.”

Similar to Heartbleed, the vulnerabilities Chen’s team found came from security packages already in use, including some that have been downloaded hundreds of thousands of times. The researchers approached the developers of the programs in question and pinpointed the exact location of the vulnerabilities so patches could be built to treat them.

“A lot of the developers took our advice,” Rastogi says, noting that the team received at least 14 confirmations of patches in development. “Security techniques still need a fundamental redesign, but there has been improvement.”

T O P - O F - M I N D , N O T S E C O N D T H O U G H T

For Aleksandar Kuzmanovic, associate professor of electrical engineering and computer science at McCormick, the Heartbleed bug symbolizes a broader trend. He observes that developers often push new software or mobile apps to market as quickly as possible, content to react to security breakdowns as they occur instead of addressing cyber security threats proactively.

“A Facebook application may make sense from a system design perspective, but not from a security perspective,” says Kuzmanovic, whose recent research quantified the privacy leaks present when using social networks on mobile devices. “As soon as the app works, there’s a rush to put it online. If something goes wrong, they’ll deal with it then.”

One lesson that Heartbleed has taught: no matter how tough your security protocol, vulnerabilities exist, and information placed online has the potential to be compromised. That uneasiness won’t go away anytime soon.

“Security is improving,” says Chen. “But there’s still a long way to go before we can truly call the Internet secure.”

ALEX GERAGE