West Texas Cyber Security Consortium

Cybersecurity Researchers Roll Out A New Heartbleed Solution

Technique Called 'Red Herring' Creates Decoy Servers, Entraps, Monitors Hackers Who Think They're Stealing Data

April 14, 2014

Dr. Kevin Hamlen

As companies scrambled in recent days to address the latest cybersecurity bug known as Heartbleed, researchers at The University of Texas at Dallas had a solution that fixes the vulnerability, and also detects and entraps hackers who might be using it to steal sensitive data.

The advanced technique — dubbed Red Herring — was created by a team led by Dr. Kevin Hamlen, an associate professor of computer science in the Erik Jonsson School of Computer Science and Engineering. It automates the process of creating decoy servers, making hackers believe they have gained access to confidential, secure information, when in fact their deeds are being monitored, analyzed and traced back to the source.

“Our automated honeypot creates a fixed Web server that looks and acts exactly like the original — but it’s a trap,” said Hamlen, a member of the UT Dallas Cyber Security Research and Education Institute (CSI). “The attackers think they are winning, but Red Herring basically keeps them on the hook longer so the server owner can track them and their activities. This is a way to discover what these nefarious individuals are trying to do, instead of just blocking what they are doing.”

The Heartbleed bug affects about two-thirds of websites previously believed to be secure. These are websites that use the computer code library called OpenSSL to encrypt supposedly secure Internet connections that are used for sensitive purposes such as online banking and purchasing, sending and receiving emails, and remotely accessing work networks. Heartbleed became public last week.

In 2012, a new feature named Heartbeat was added to software primarily for slow Internet connections. Heartbeat allowed connections to be held open, even during idle time. A flaw in the implementation allowed confidential information to be passed through the connection, hence the name Heartbleed.

Even though Heartbleed is now in the process of being fixed, victims face the challenge of not knowing who may already be exploiting it to steal the information, and what information they may be going after. A common fix for this type of problem is to create a trap, a honeypot that lures and exposes attackers. Typically this can involve setting up another Web server somewhere else.

Protecting Yourself from Heartbleed

It is estimated to take up to several weeks for some organizations to fully protect against Heartbleed. Until then, Dr. Kevin Hamlen recommends not signing into any security-sensitive servers for the next few days in an effort to reduce exposure to Heartbleed.

“Avoid entering your password into anything online for the next few days, and [after that] change all your online passwords,” Hamlen said.

“There are all sorts of ad hoc solutions where people try to confuse the attacker by deploying fake servers, but our solution builds the trap into the real server so that attacks against the real server are detected and monitored,” Hamlen said. “Our research idea can build this honeypot really quickly and reliably as new vulnerabilities are disclosed.”

The Red Herring algorithm created by Hamlen automatically converts a patch — code widely used to fix new vulnerabilities like Heartbleed — into a honeypot that can catch the attacker at the same time.

“When Heartbleed came out, this was the perfect test of our prototype,” Hamlen said.

Red Herring doesn’t stop at being a decoy and blocker; it can also lead to catching the attacker. As the attacker thinks he or she is stealing data, an analyst is tracking the attack to find out what information the attacker is after, how the malicious code works and who is sending the code.

“In their original disclosure, security firm Codenomicon urged experts to start manually building honeypots for Heartbleed,” Hamlen said. “Since we already had created algorithms to automate this process, we had a solution within hours.”

When news of Heartbleed became public on April 8, software engineering doctoral student Frederico Araujo started researching the vulnerability and had implemented Red Herring by 2:30 a.m. April 9.

“I was very proud that he had taken the initiative before I’d even gotten to it,” Hamlen said. “Normally, I personally would have started working on it sooner, but I’d been up all night grading papers the night before.”

Media Contact: LaKisha Ladson, UT Dallas, (972) 883-4183, lakisha.ladson@utdallas.edu
or the Office of Media Relations, UT Dallas, (972) 883-2155, newscenter@utdallas.edu.