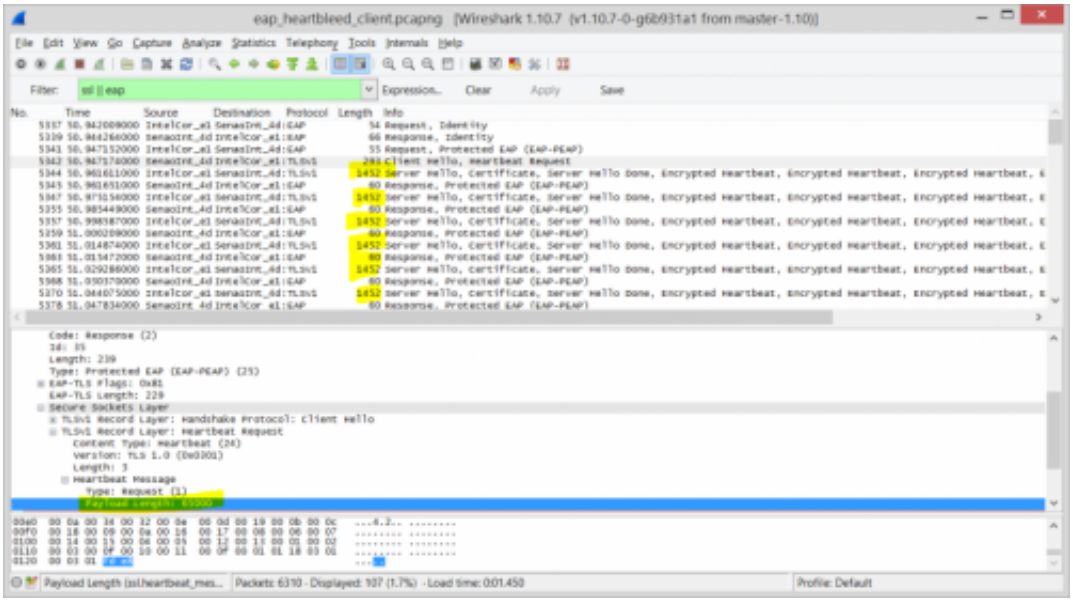
Heartbleed-like Cupid poses opportunity for wireless attack

June 3 2014, by Nancy Owano



The Cupid now being talked about in technology circles is hardly the sweet angel that aims a love arrow at innocents' hearts. This Cupid represents an attack vector threatening information security. Thanks to a Portuguese researcher, security watchers have been made more aware of yet another variation of the Heartbleed headache. This vulnerability, based on the same Heartbleed exploit, was discussed last month in detail by Luis Grangeia of information security company, Sysvalue. The researcher showed how the Cupid attack vector can do its mischief on

wireless networks and connected devices.

According to Grangeia, a presentation that he gave at a local event focused on an "attack vector for the Heartbleed bug, specifically on networks using EAP TLS tunneled authentication methods." (EAP stands for Extensible Authentication Protocol and-TLS, for Transport Layer Security.) He said, "I wrote a patch for hostapd and wpa_supplicant to provide a proof of concept of the attack."

Michael Mimoso, editor, Threatpost, the Kaspersky Lab security news service, explained that Grangeia built patches that modify the hostapd and wpa-supplicant, two programs acting as wireless access and authentication management points. Hostapd sets up a configurable access point; it's supported on Linux. Mimoso said that hackers could create a wireless network configuration of their choosing that would allow vulnerable clients to connect to it. Wpa_supplicant, supported on Linux and Android, is used to connect to wireless networks.

Dan Goodin, security editor at Ars Technica, noted that Cupid streamlines the process of exploiting devices connecting over wireless networks secured using the EAP, used by many large organizations to password-protect access.

Grangeia, meanwhile, talked about the process by which such an attack can occur. "This is basically the same attack as Heartbleed, based on a malicious heartbeat packet. Like the original attack which happens on regular TLS connections over TCP, both clients and servers can be exploited and memory can be read off processes on both ends of the connection. The difference in this scenario is that the TLS connection is being made over EAP, which is an authentication framework/mechanism used in wireless networks. It's also used in other situations, including wired networks that use 802.1x Network Authentication and peer to peer connections."

What software is affected? He noted, "I've done very limited testing on this. I have confirmed however that on Ubuntu, if you are using a vulnerable version of OpenSSL the default installations of wpa_supplicant, hostapd, and freeradius can be exploited. Android 4.1.0 and 4.1.1 use a vulnerable version OpenSSL. Also, all versions of Android use wpa_supplicant to connect to wireless networks, so I have to assume that these are probably vulnerable."

As for clients, he said that anyone with an Android device running 4.1.0 or 4.1.1 should avoid connecting to unknown wireless networks unless they upgrade their ROM. People using a Linux-system device to connect to wireless networks should make sure to upgrade their OpenSSL libraries, and, he added, "if you followed Heartbleed mitigation recommendations you should be fine."

Another reassuring comment is that those with home routers are probably safe from this attack vector, as most home routers use a single key for wireless security, not EAP authentication mechanisms. However, he said that "If you have a corporate wireless solution on your company you should look at this problem, since most of the managed wireless solutions use EAP based authentication mechanisms. And some companies use OpenSSL. You should look at having your equipment tested or contacting your vendor and ask for more information. You should also look at this issue if you have any type of EAP authentication mechanism on your corporate network. Note that 802.1x Network Access Controlled wired networks might also suffer from this problem."

More broadly, wrote Russell Brandom in The Verge, "it's a reminder that the security world is still working through the various effects of Heartbleed. Even after the central servers have been patched, researchers can discover more obscure attacks that go after less obvious targets."

More information: www.sysvalue.com/en/heartbleed-cupid-wireless/