By now most of you have heard of the OpenSSL vulnerability issue code named HeartBleed. Below is more information on the issue and a test site to test any servers you may have using OpenSSL.

You may wish to forward the below advisory to faculty and staff within your individual units.

TEST SITE:  http://filippo.io/Heartbleed/

2014-04-09: Understand "Heartbleed" and Protect Yourself

• **What is Heartbleed.** Heartbleed is a critical security vulnerability in a widely-used piece of Internet software called OpenSSL. The vulnerability has been around since at least March 2012, but was only recently published. It is unclear whether attackers have been exploiting this vulnerability in the past.

• **What OpenSSL does.** OpenSSL typically is used on Internet servers to encrypt. For example, when you connect to a web server and you see the little padlock icon in your browser bar that indicates a secure session, that’s often OpenSSL. Think about your secure sessions with banks, credit cards, Google, Facebook, Yahoo, you name it.

• **What can an attacker do using OpenSSL?** Simply put, the attacker can read the data you exchange with that website, including, for example usernames and passwords.

• **So do the attackers have my username and password?** Possibly. There’s no way to be sure.

• **So what do I do?** First, computer servers worldwide need to be patched, but that needs to be done by the companies that own the websites – there is nothing you can or need to do with your computer, smartphone, etc. at this moment. This is a big deal, so companies are patching their webservers right now. In the meantime, pay close attention to your bank accounts, credit cards, etc. and be on the lookout for suspicious activity. Then, on Thursday or Friday, **change each and every one of your computer passwords, everywhere.** This means your University passwords, your online banking, Facebook, Yahoo, Google, Dropbox – everything.

• **Have AgriLife or University Systems been affected?** As discussed above, there is no way to tell if a webserver has been attached. AgriLife IT is updating any servers that may be impacted. Individually operated unit or agency systems should be reviewed by their respective owners.

• **Where do I learn more?** Just Google “heartbleed”
Alan Kurk
Director/CIO
Texas A&M AgriLife Communications & Information Technology
Phone: 979.845.9343  Email: akurk@tamu.edu