BadBIOS: Frightening or Fake?
Assignment Due: 2/25/16

In October of 2013, a man named Dragos Ruiu claimed to have discovered a very interesting piece of malware. He claimed that the malware was able to infect multiple hardware architectures and operating systems, persisted through system reformats and hardware replacements, and even managed to spread from air-gapped systems in known clean environments. Ruiu had some theories on how the malware spread in such strange and terrifying ways, but could never provide definitive proof. Furthermore, no investigative team has been able to successfully detect the malignant code that supposedly hosts portions of BadBIOS, making it even more difficult to believe. That being said, the Heartbleed vulnerability existed for nine years before it was discovered, so perhaps in this one niche case, "the absence of evidence is not evidence of absence".

First, read this article: http://arstechnica.com/security/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/

Then, read this more recent article: http://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems/

After reading both of the articles, do a little more research; just Google "BadBIOS" and read more information you come across via additional articles, opinions, forum posts, etc. Once you feel like you've read enough information on both sides of the argument, answer the questions below and submit your responses via Blackboard using either the provided text response box or by uploading a PDF of your responses.

1. Do you think BadBIOS is/was real? Why or why not?

2. What does it mean for a system to be "air-gapped"?

3. Are there any well-known methods for defending against firmware attacks?

4. Do you consider the hardware you use on a daily basis to be secure? If so, what assurances do you have that your hardware is secure? If not, why?