Robert Fink
rwfwcb
BadBIOS Answers

1. I do not think that BadBIOS is or was real. I have a couple reasons for thinking this way. My first suspicion is Ruiu's claim that the air-gapped machines were maintaining connections via high frequencies sent and received from the computer speakers and microphone. This seems unlikely since computer speakers are not usually made with the range for ultrasonic sounds, and I also think it is unlikely for the average microphone to pick them up as well. Another reason I argue against the existence of BadBIOS is that Ruiu claims it could hide itself from being analyzed. Even the NSA's malware can be detected and removed. The fact that nobody in the security world can detect BadBIOS makes me believe that it does not exist.

2. When a system is "air-gapped" it means that the system is not connected to any unsecure network like the Internet or an unsecure local area connection.

3. Yes there are methods for defending against firmware attacks. It is important to do OS updates, BIOS updates, and other updates as they become available to stay patched against known vulnerabilities. Hard drives and important data should be encrypted. Email filters should be setup to block phishing campaigns. Have updated anti-malware shielding and eliminating any malicious attachments or downloads. Web traffic should be scanned for malware. UEFI 2.3.1 standards defenses are also made to protect the integrity of the firmware. There is also Microsoft BitLocker with Trusted Platform Module that check the integrity of firmware.

4. Yes I consider the hardware I use on a daily basis to be secure. I make sure I install updates as they become available. My firewall is set to prevent unauthorized incoming connections. I use Avast anti-virus and it updates its definitions a couple times a day. My MacBook SSD is encrypted with FileVault2. Most importantly I follow safe user practices and don't do any risky downloading or Internet browsing.