Bridging the Gap Between SIPR and NIPR Using KVM Switches

debug net

April 24, 2018

Abstract

To use a Keyboard, Video, Mouse (KVM) switch to connect air gapped systems like Secret Internet Protocol Network (SIPRNet) and Non-secure Internet Protocol Network (NIPRNet).

Figure 1. KVM switch (Avocent, 2010, p. 1)

KVM switches (Avocent, 2010) are a typical interface used to quickly switch between systems such as SIPRNet and NIPRNet in a government setting. A keyboard, mouse, monitor (with some models supporting multiple), sound inline jack, and microphone inline jack is plugged into each slot of the console section on the back, then cables are connected to each lettered section that is designated for each machine depending on their classification. Once power is applied, the KVM allows the user to push a convenient button to switch the monitor, keyboard, mouse, and audio inputs/outputs to that specific machine without having to re-seat connections for an extended period. The intent is not to move connections around again unless something is not functioning due to normal wear and tear. Despite this intent, there are no tactics, techniques, and procedures in place to monitor their correct configuration and/or prevent cross contamination.

According to Michael Hanspach and Michael Goetz (2013), it is theorized that one could communicate between systems using speakers and microphones. Their method used a 'covert channel' to send ultrasonic frequency sound to play and record command and control data over the

air between systems that are infected on both sides (air gapped and exposed to the cloud). One could theorize that those same communication protocols used by them could be used to accomplish the same task with more effectiviness by using inline audio jacks to connect systems directly because the inline jacks are typically less resistant to interference due to their design; this also allows for a covert line without the necessity for ultrasonic sound, which inherently limits bandwidth, but one would not hear the sound unless the audio passes out the speakers at the same time.

The vulnerability one could exploit is to cross the lines between machines and more than likely avoid detection because of the lack of monitoring of those connections on the back of the KVM switch, therefore creating that 'covert channel' and pass information between air gapped systems. Specifically, one can swap the inline sound and microphone jacks with the console section and on one of the machine's cables. This is so that the microphone line is in the speaker jack and the speaker line is in the microphone jack of the console section and the button is pushed for the side which is still plugged in for the lettered section (see figure 2 for example). These particular switches may not be the only systems vulnerable to this method, however one could extrapolate how another model or make would follow the same procedure.

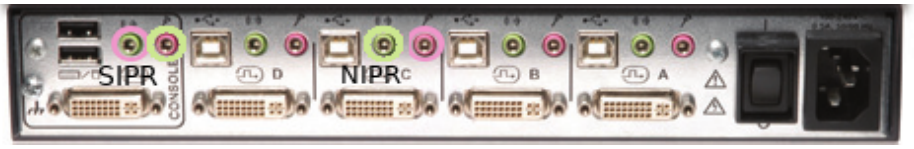

Figure 2. KVM (Avocent, p. 1) configuration example that exploits covert channel using colored circles to show respective jacks to use

Once the KVM switch is configured in this way, one can infect both sides (SIPRNet and NIPRNet) with a worm similar to badBIOS and then both systems will communicate whatever command and control data one could arbitrarily pass through (Goodin, 2013). Despite badBIOS' lack of proof, the potential for air gapping via modulated and demodulated audio between systems is still possible but it is a risk that is critical considering the sensitivity the kind of data that could be exposed from something like SIPRNet.

Security teams could implement the following mitigation techniques to prevent air gapping: monitoring cable connections on KVM switches to include checks by personnel whom possess air gapped systems like SIPRNet machines and comparing approved configurations with those actual configurations; enforcing policies that prevent the need for inline jacks on KVM switches except without information owner approval for mission critical needs; denying the need for microphone jacks for any reason, whether that is cutting the line or not using microphone cables at all; and/or implementing a software/hardware solution such as Data Loss Prevention (DLP) to prevent data transfer via audio systems.

Reference

Avocent. (2010). *SwitchView ® SC4 UAD KVM Switch*. Retrieved from http://www.avocent.com/Resources/Documents/Data_Sheets/Switch_View_SC4_UAD_KVM_Switch.aspx

Goodin, D. (2013). *Meet "badBIOS," the mysterious Mac and PC malware that jumps airgaps*. Retrieved from https://arstechnica.com/information-technology/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/

Hanspach, M. and Goetz, M. (2013). *On Covert Acoustical Mesh Networks in Air*. Retrieved from http://www.jocm.us/uploadfile/2013/1125/20131125103803901.pdf