

Training Module 4 - Analog Leakages and Isolation in Secure KVM System

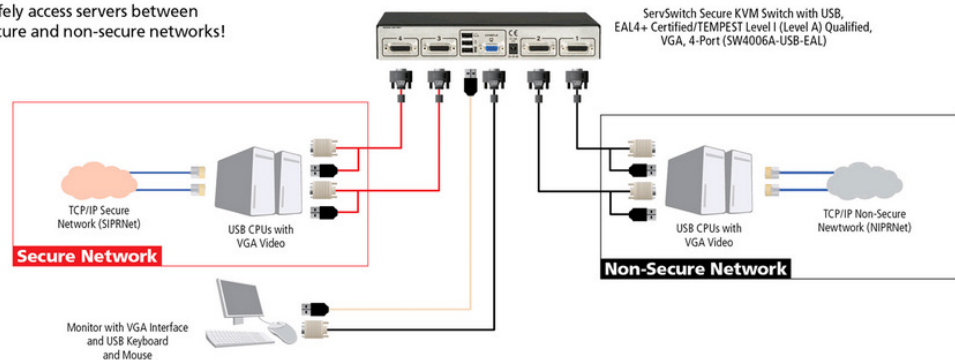


KVM Isolation – Common Misconception

Secure KVMs are adding security risks through analog signal leakages.

- A TEMPEST / Cold-War era claim often heard from customers and certification bodies.
- Vendors claiming high isolation between this and this...
- Tests conducted or required by agencies worldwide to certify KVMs.

Safely access servers between
secure and non-secure networks!



The [ServSwitch Secure KVM Switch with USB](#) uses Black Box's exclusive hardware-based data isolation to ensure unidirectional data flow with hardware data diodes to provide robust security against port-to-port data leakage. Channel-to-channel crosstalk isolation greater than 80-dB virtually eliminates cross-port signal sniffing.

"Other solutions on the market use software-based data isolation technology, which introduces the risk of hacking or malware threats," said Mike McCurry, ServSwitch Product Manager at Black Box. "Our hardware-based technology eliminates the risk of both intentional and unintentional software corruption that might expose sensitive data."

KVM Isolation – NIAP Misconception

<http://www.niap-ccevs.org/PD/0166.html>

PD166

Effective Date:2011-05-19

Last Modified2011-05-19

Issue

What additional peripherals may be switched under the Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile (PP)? In particular, can audio signals or CAC cards be covered by the switch?

Resolution

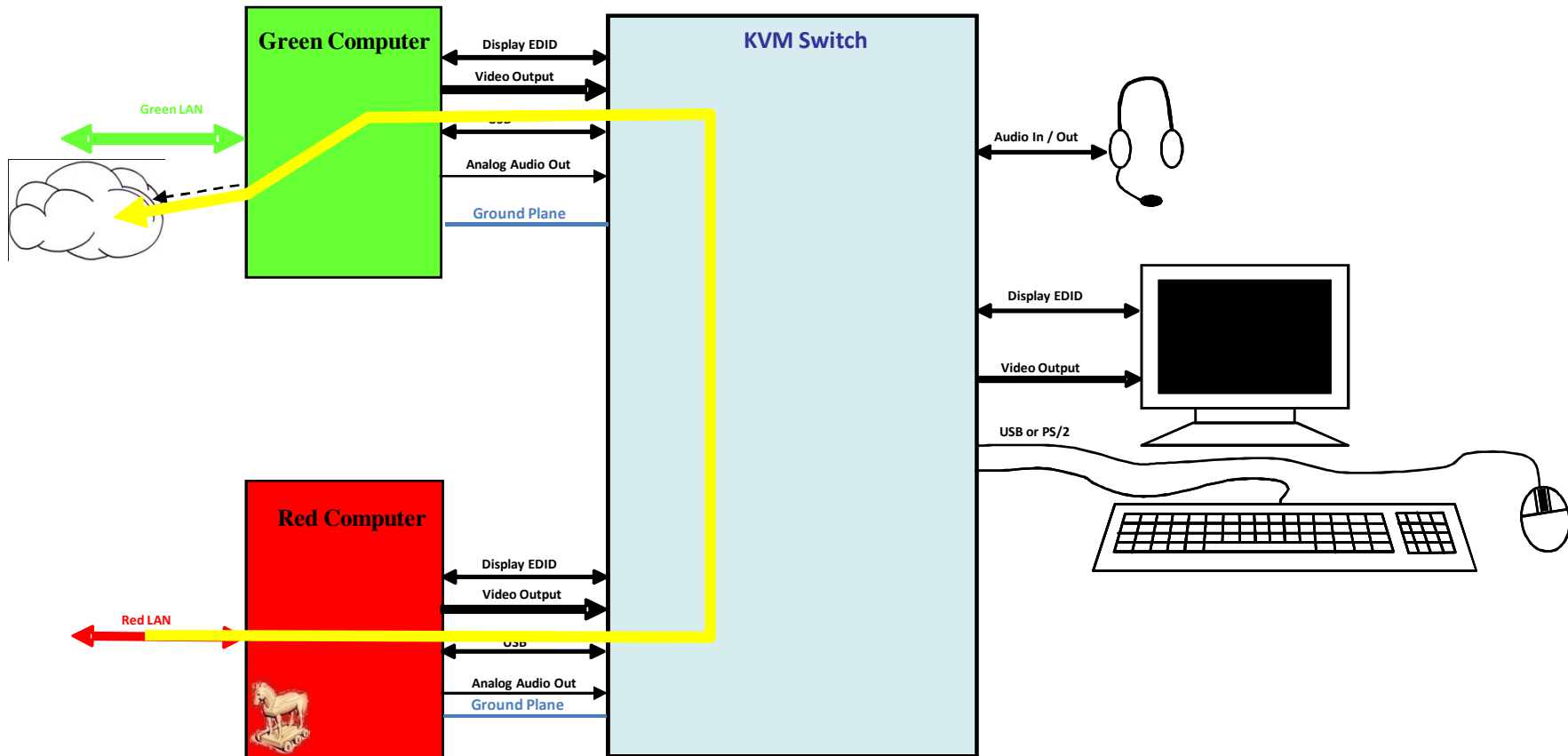
Analog audio devices (those typically connected through a 3.5mm Stereo Mini Jack) MAY be switched through a peripheral sharing switch. Devices that connected through a USB port, with the exception of the already approved keyboards and mice, **MUST NOT** be switched through a peripheral sharing switch.

Support

Switching audio devices provides the ability to switch two audio ports (input and output) between attached computers and audio devices. This additional support permits connections for speakers and a microphone to be shared between the computers along with the keyboard, video display, and mouse (KVM). These devices are permitted because the audio ports are transducers between human actions/senses and the computer; as such, they present the same type of interface as the keyboard, mouse, and video output that are identified acceptable in the PP. Note that the only acceptable audio devices covered by this PD are simple electro-mechanical transducers (e.g., microphones, speakers) that incorporate no digital signals whatsoever. It must be noted that more complex audio devices and/or those that connect through the USB port are prohibited in a TOE conforming to the PSS PP. Administrative guidance and the Validation Report must specify the acceptable audio devices and connections.

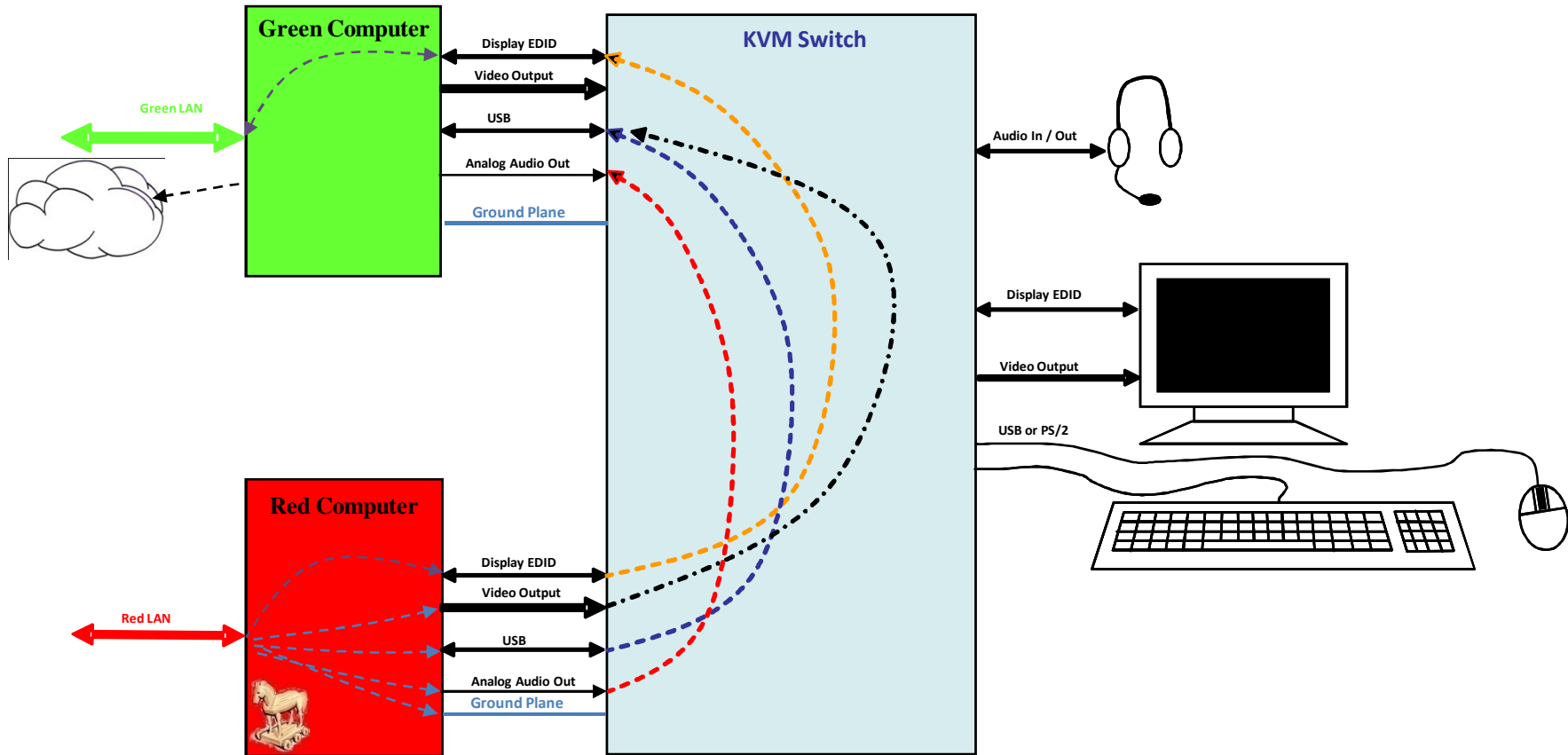
Serious misunderstanding – Audio input signals can be exploited through software attacks to analyze analog signal and to leak data between networks.

The Analog Leakage Scenario



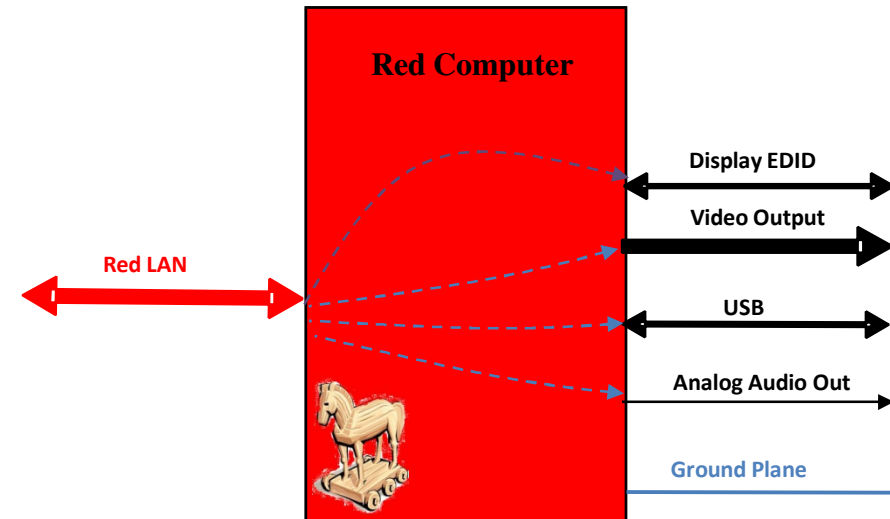
Target digital data must be converted to analog / digital signal in Red Computer, leak through the KVM and then converted back into digital data at the Green Computer to exit through Green LAN to the Internet.

KVM Potential Analog Signal Leakage Paths



Assumptions – Red Computer Side

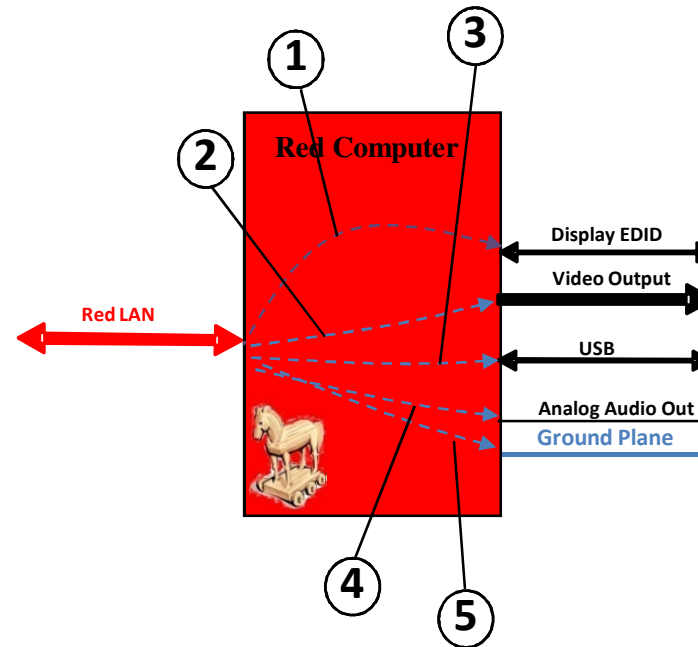
1. Primary attacker target is information on the Red LAN
2. Secondary attacker target is local information on Red Computer
3. Attack goal – export data from Local / Red LAN
4. Attacker was able to infect Red Computer with undetectable malicious code capable of using all Red Computer resources
5. Attacker aware of the specific KVM connected to the Red Computer



To fulfill his goals – attacker must find a way to pass Red LAN or Red Computer local digital data into one / more of the 5 external interfaces as analog signal.

Red Computer Side Data Conversion

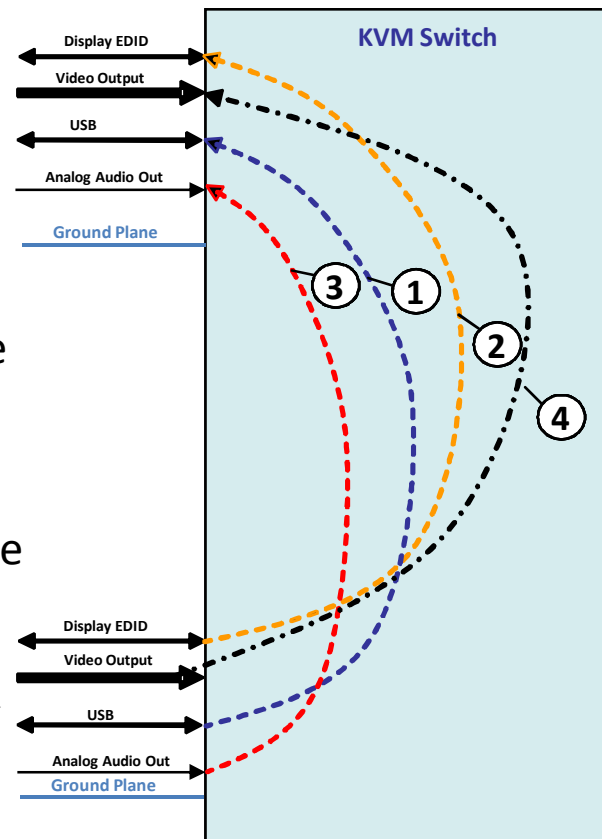
- ① From LAN to EDID transmitted signal – **Easy** using malicious code
- ② From LAN to Video transmitted signal – **Easy** using malicious code
- ③ From LAN to USB transmitted signal – **Easy** using malicious code
- ④ From LAN to audio transmitted signal – **Easy** using malicious code



Following the Red Computer side assumption – attacker can easily use Red Computer to transmit Red LAN or local data into encoded audio, video, EDID or USB data.

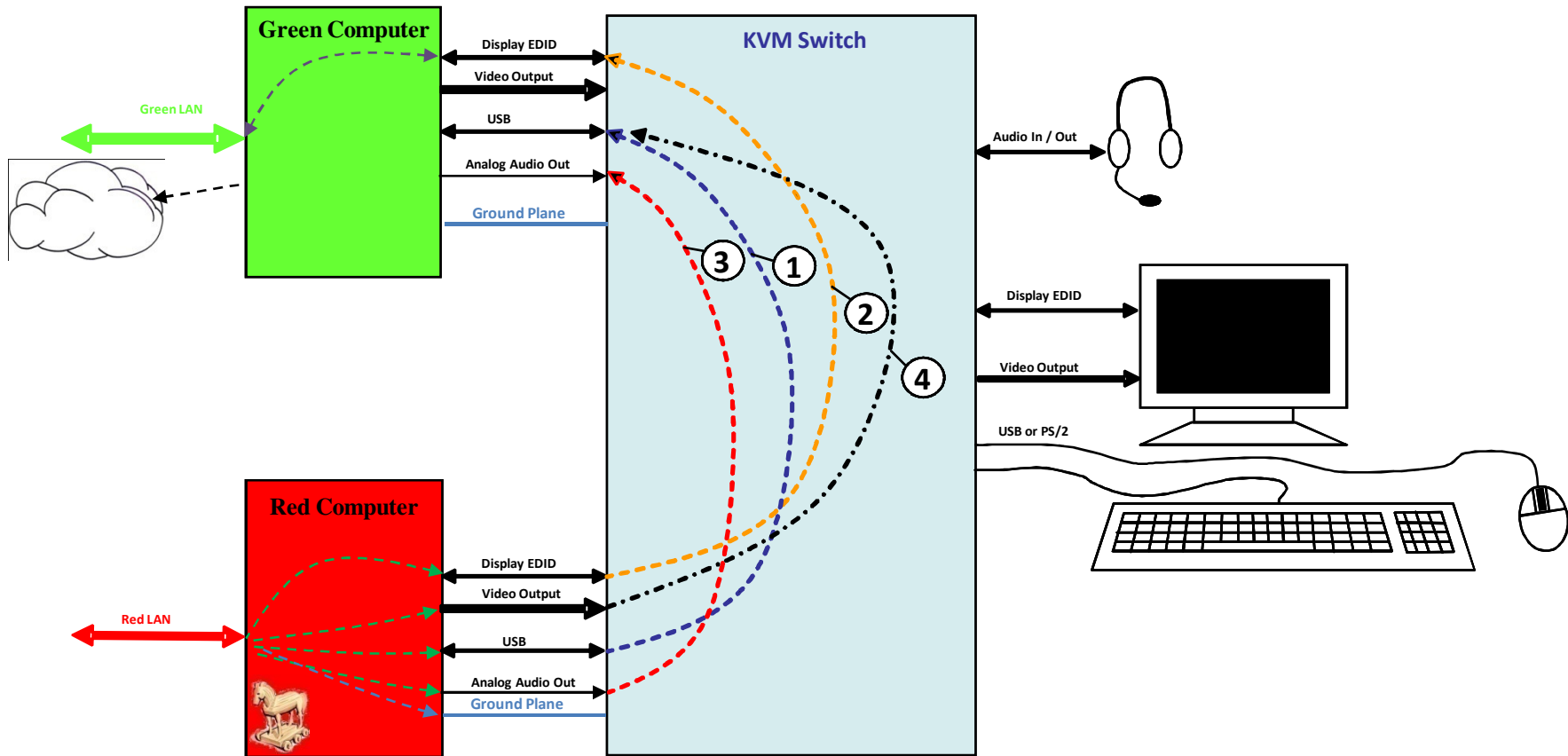
Assumptions – KVM Analog Leakages

- KVM is Secure type and was not tampered by attacker
 - KVM Isolation is better than -10dB
- ① Residual USB digital signal may leak between Red Computer USB interface and Green Computer USB interface
 - ② Residual EDID digital signal may leak between Red Computer EDID interface and Green Computer EDID interface
 - ③ Residual audio analog signal may leak between Red Computer audio interface and Green Computer audio interface
 - ④ Residual audio analog signal may leak between Red Computer audio interface and Green Computer audio interface



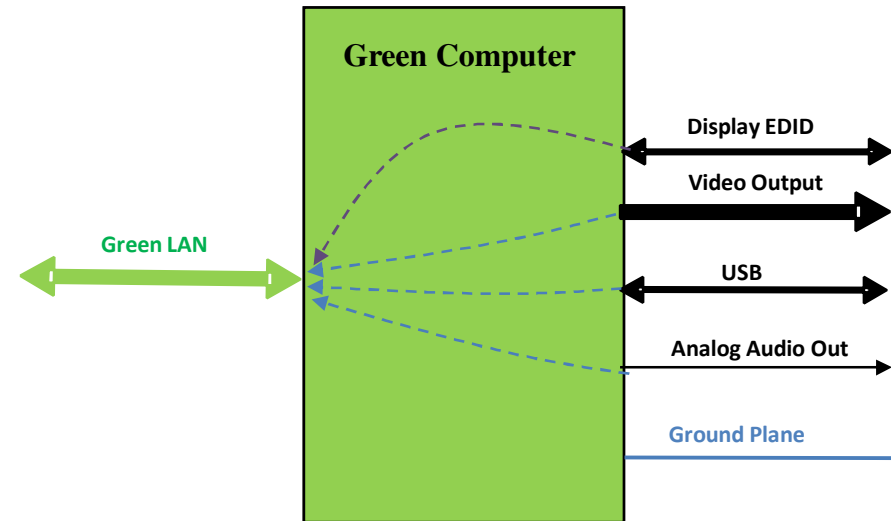
Red Computer generated analog / digital signal may be present on KVM Green Computer interfaces.

KVM Potential Analog Signal Leakage Paths



Assumptions – Green Computer Side

1. Attacker may gain full remote access to the Green Computer. Attacker may load any malicious code.
2. Attack goal – export residual data riding on the KVM interfaces into the Green LAN and the internet
3. Attacker aware of the specific KVM connected to the Red Computer
4. Green Computer does not have analog cards and was not physically tampered
5. Microphone input is not connected to the KVM



To fulfill his goal – attacker must find a way to convert the weak residual signal on KVM interfaces into digital data exported to the Green LAN.

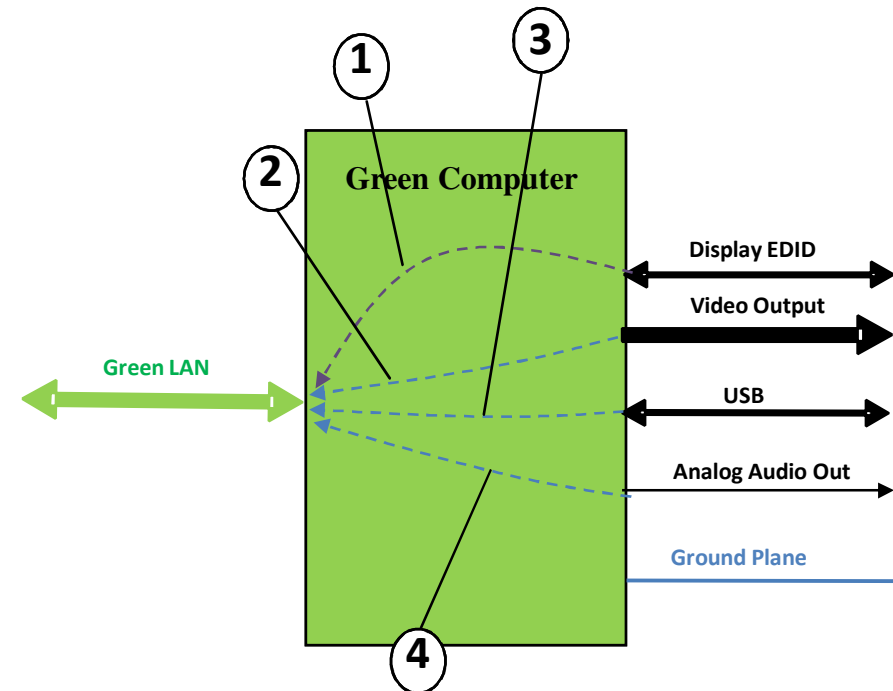
Green Computer Side Analog Conversion

- ① From EDID residual digital signal to Green LAN – **No path!** Video card EDID cannot analyze this signal.
- ② From Video residual digital signal to Green LAN – **No path!** Video card output cannot analyze this signal.
- ③ From USB residual digital signal to Green LAN – **No path!** USB host circuitry cannot analyze this signal.

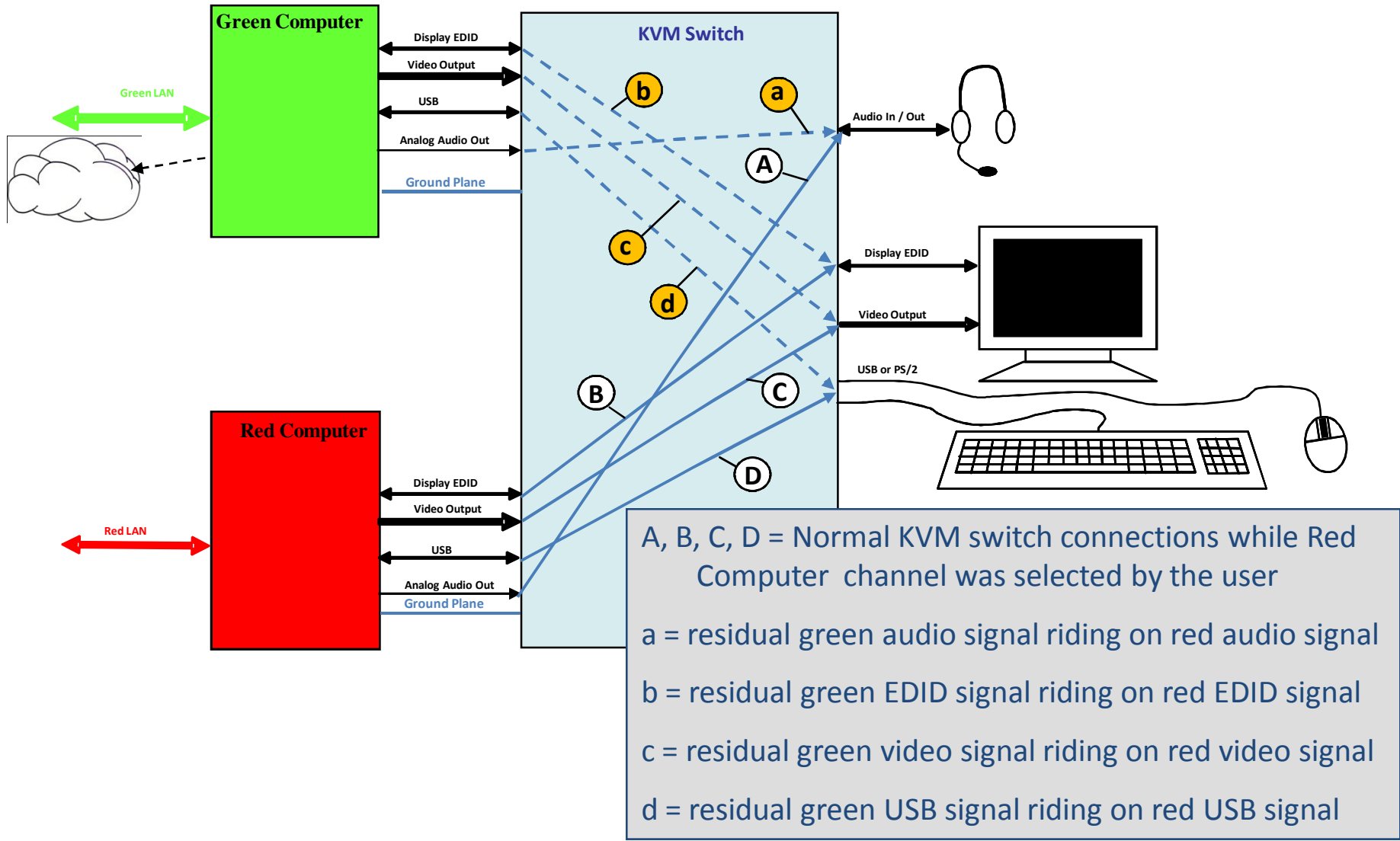
④ From Audio residual digital signal to Green LAN – **Potential path through Audio Codec.**



The only path that attacker may use is the audio path. No other circuitry in a standard PC may be abused to detect weak residual signals. The only analog leakage need to be tested for analog isolation is the analog audio path.

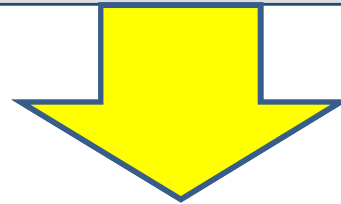


Why we are not concerned with Console side leakages?



Why we are not concerned with Console side leakages?

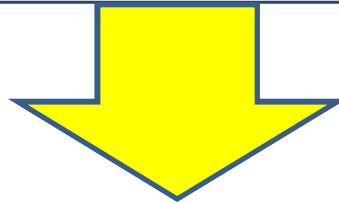
1. Assumption that user is not hostile (not cooperating with the attacker)
2. Assumption that user console equipment was not sabotaged / modified by the attacker
3. User console equipment does not have the technical capabilities to analyze / detect weak analog signals
4. User is allowed to listen / see all connected channels anyway! Even when KVM channel is not selected (it is user decision).



Conclusion: Console side signal leakages through KVM are not considered as a significant security risk.

Why we are not concerned with Ground and power leakages?

1. Assumption that both Red Computer and Green Computer are connected to the same mains power system and same ground anyway.
2. Attacker does not have any remote capabilities to analyze and filter the ground noise.
3. The LAN shield does not carry any significant signal leakages.
4. The KVM itself injects to the ground less than 10% of the signals injected by the non-TEMPEST PCs



Conclusion: KVM signal leakages through ground is the same as without KVM.

Summery – Do and Don't

1. Do not use commercial KVMs for isolated networks.
- 2. Never connect microphone cables to Secure KVMs.**
3. Do not use PCs with special analog cards, video capture or audio cards with secure KVMs.
4. Test for analog signal isolation across audio outputs only. Nothing else is critical for security.
5. Don't invest in TEMPEST KVMs if your site and computers are not TEMPEST.
6. Digital remote attacks on Secure KVMs are much higher risk compared to analog leakages.