

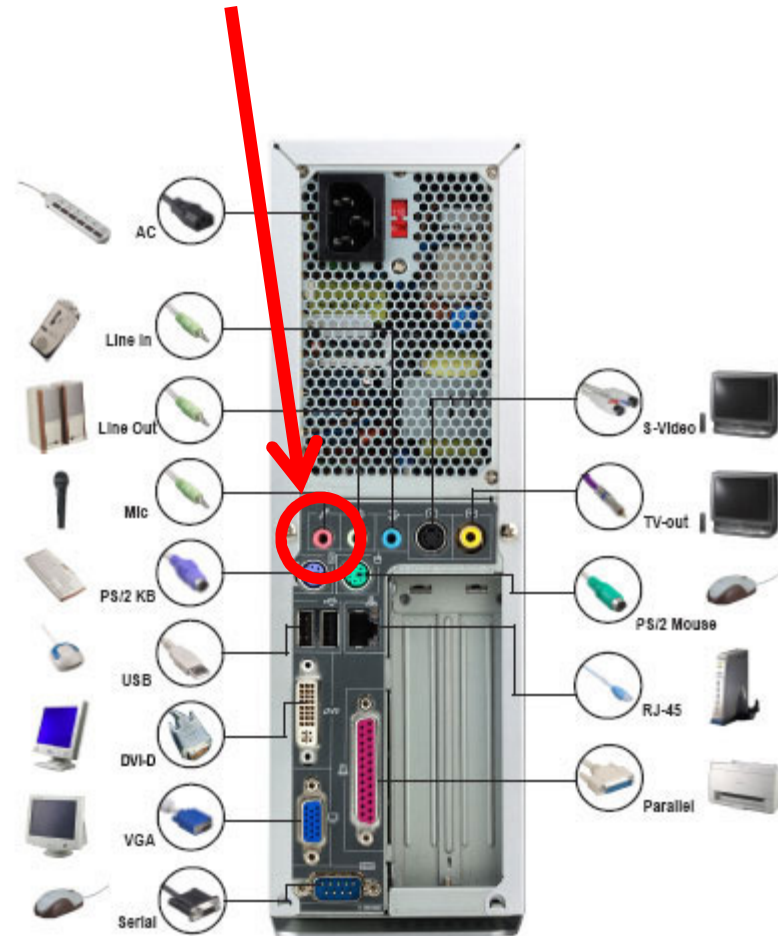
Training Module 5 - Audio Leakages and KVMs



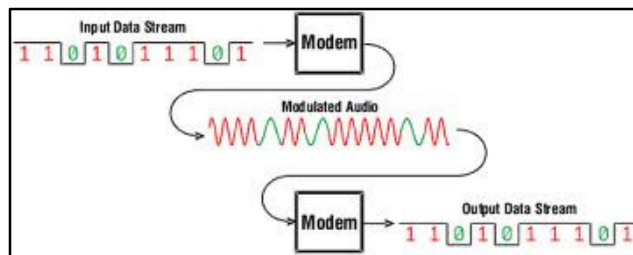
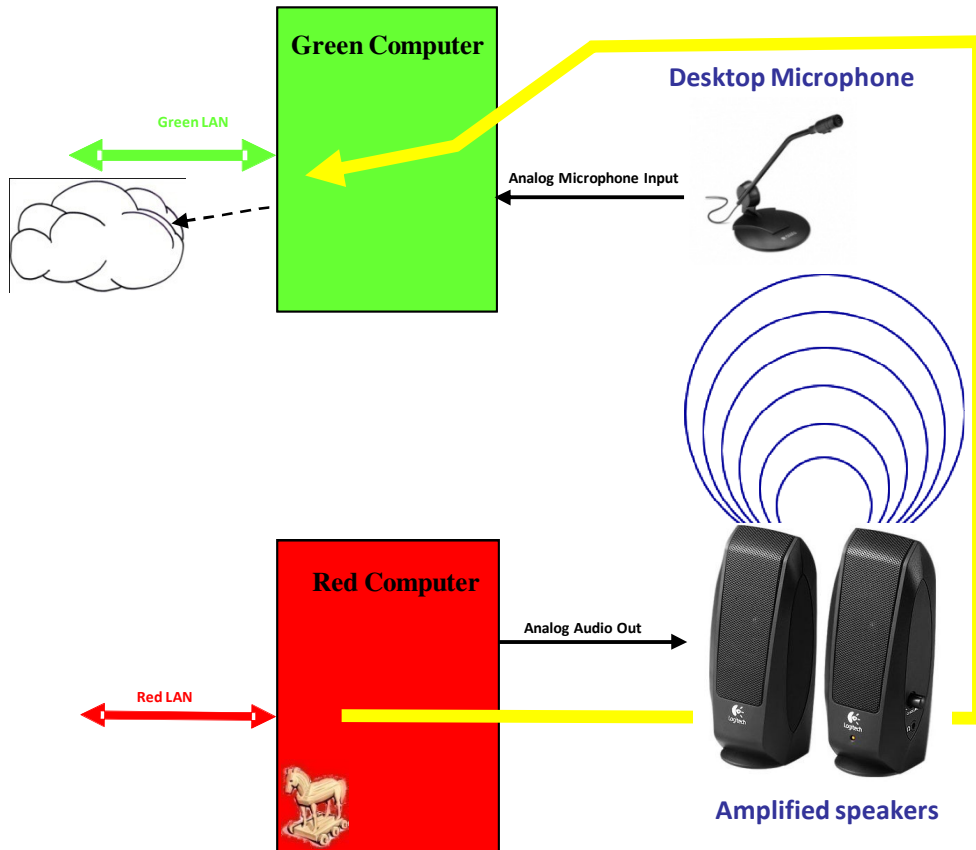
Introducing – The Microphone Input

The most **unsecure** port in any computer by far!

- Can be easily controlled and reprogrammed by any code, program or malicious code
- Very sensitive analog input – preamplifier can sense few mV signal!
- Referenced to chassis ground – can pickup many types of weak signals.
- Programmable gain and filters to clean unwanted noises.
- Vulnerable even when microphone is not connected!



Basic Acoustic Leakage Scenario



1. Hostile code in red computer takes secret file from Red LAN and converts it at night into a series of beeps to be played by Red Computer sound card (audio codec).
2. Another malicious code running in Green Computer opens the microphone with high gain and set filters to the beeps of Red Computer.
3. Red Computer play the file, Green computer decodes it and translates it back into a binary file.
4. Green Computer sends the leaked file over the internet to another happy customer...

<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.

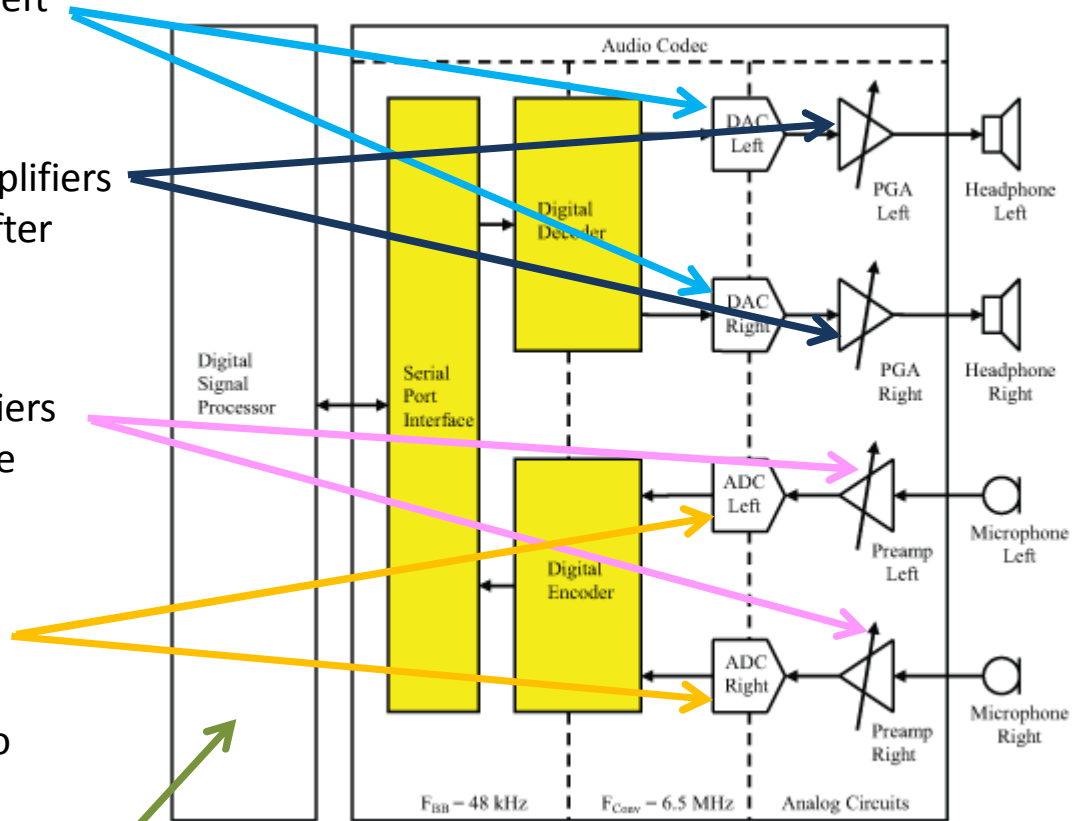
Support

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.

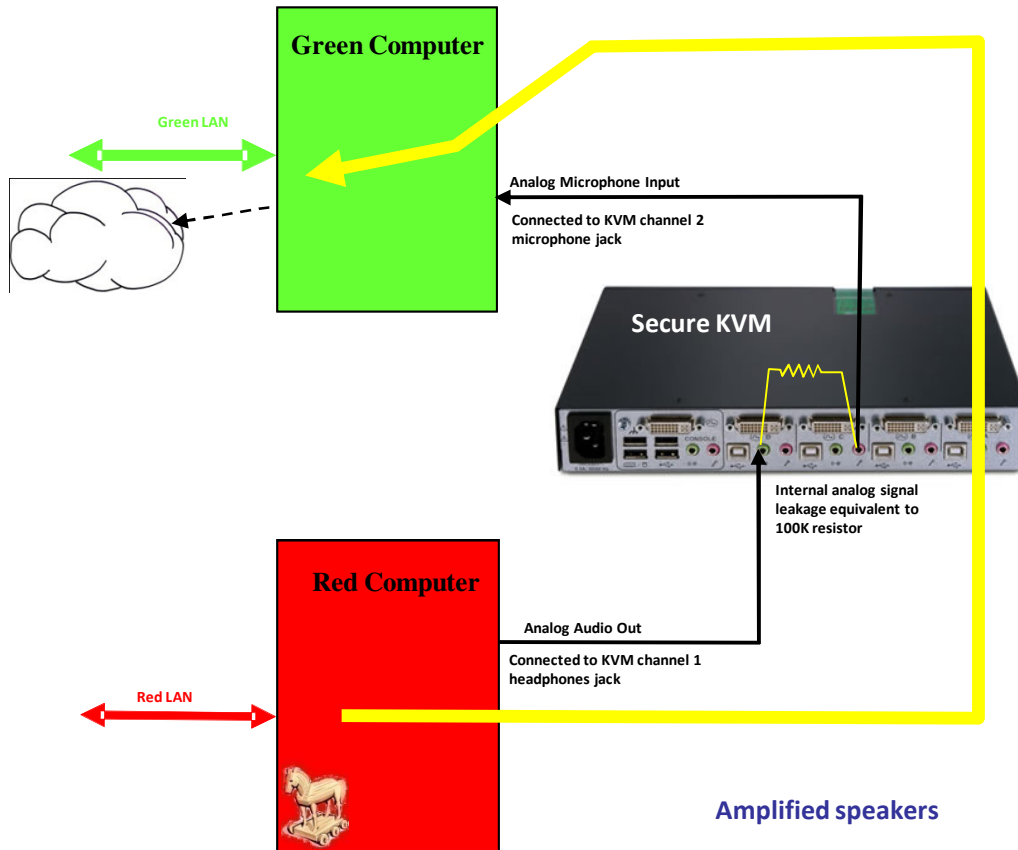
Serious misunderstanding – Audio input signals can be easily exploited through software attacks to analyze analog signal and to leak data between networks. The microphone port is VERY DIFFERENT from any other port in PC or KVM!

How Computer Sound Card Works?

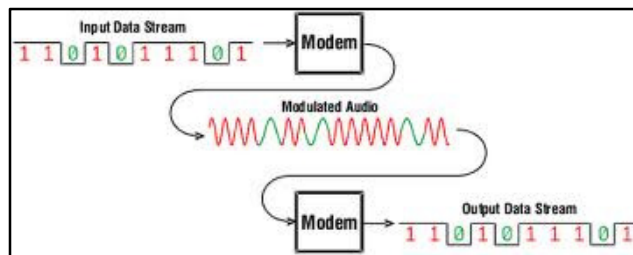
- Two DACs (Digital to Analog Converters) – converting the left and right digital streams into analog signal.
- Two Programmable Gain Amplifiers (PGA) amplifies the signals after the DACs to drive speaker / headset amplifiers.
- Two very sensitive preamplifiers connected to the microphone inputs (sometime only one – mono)
- Two ADCs (Analog to Digital Converters) takes the analog signals and convert them into digital streams.
- Software driver operating as DSP (Digital Signal Processor) and can perform filtering, FFT and any needed mathematic operation on these streams.



Audio Leakage Through KVM Scenario



1. Hostile code in red computer takes secret file from Red LAN and converts it at night into a series of beeps to be played by Red Computer sound card (audio codec).
2. Another malicious code running in Green Computer opens the microphone with high gain and set filters to the beeps of Red Computer. KVM may be off (unpowered) or on...
3. Red Computer play the file, Green computer receives it, amplifies it, decodes it and translates it back into a binary file.
4. Green Computer sends the leaked file over the internet to another happy customer...



Audio Leakages and KVMs

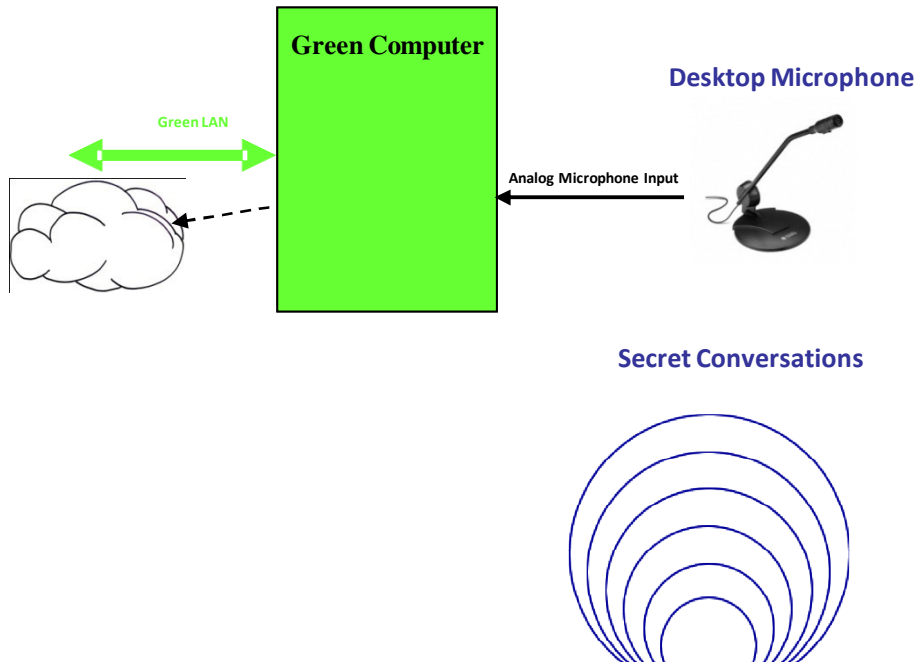


Signal inserted to:	Signal tested on:	KVM is	Isolation @28KHz
Channel 1 Ear	Channel 4 Mic	On, Channel 2 selected	48dB
Channel 2 Ear	Channel 3 Mic	Off	54dB
Channel 4 Ear	Channel 4 Mic	On, Channel 4 selected, no Mic	44dB
Console Mic	Channel 2 Mic	On, Channel 3 selected	45dB

Things that you need to know about computer sound cards and security

1. Can be easily programmed and controlled by any code running under the OS.
2. 50 lines of Visual Basic code can implement a primitive modem with good reliability and parity check.
3. Program can control output volume and microphone gain. Maximum volume in one computer and maximum microphone gain in the other one is good way to start audio leakages.
4. Even if you removed the actual microphone from the system – you still exposed to microphone input vulnerabilities.
5. Microphone input is not grounded or terminated. When microphone is not connected the input lines are floating and acting as a super sensitive antenna for low frequencies.
6. Sound card can generate and sample audio frequencies way beyond human hearing limitations (20KHz).
7. You can do audio leakages at 1200 Baud rate when you hold one computer audio cable plug tip at one hand and another computer microphone input cable at the other hand!
8. There are sound cards that enable code to change channels in a way that connected headset without microphone would become a microphone.

Acoustic Bug Leakage Scenario



1. Malicious code running in Green Computer opens the microphone with high gain to receive conversations in the room.
2. Audio recorded is compressed and encrypted by same code.
3. Green Computer sends the leaked file over the internet to another happy customer...



You can never know when your computer microphone is listening to you! Always disconnect the cable when not in use.

Summery – Do and Don't

1. Do not use commercial KVMs for isolated networks.
- 2. Never connect a microphone cables to a Secure KVM.**
3. Buy 3rd Generation Secure KVM that don't support microphone input when possible.
4. Never leave in same room microphone connected to one computer and amplified speakers to the other.
5. Do not allow headset connection that the headphones will be connected to one computer and the microphone to another!
6. Do not use PCs with special analog cards, video capture or audio cards with secure KVMs.
7. Do not connect microphone to internet connected computers.