



Training Module 3 - Display-KVM Vulnerabilities

Version B
July 27, 2011

Targeted attacks on KVM?

What is a targeted attack?

Some IT attacks are random. The attacker scans large number of unknown computers to find specific vulnerabilities and then use that vulnerability to attack one or more computers. A targeted attack is an attacker or a group of attackers that specifically targeting your organization. They may spend months or even years in targeted and structured attempts to gain access to your networks.

Why targeted attack using a KVM?

Just because they are there – one leg in a classified network and another leg in non-classified network. It is just bad timing and location...

What is the target on the attack using a KVMs?

Most users think that the goal of such attacker is to capture the information that the user types. This is definitely not the case today! Most targeted attacks using KVMs are intended to create a bridge or leak between classified isolated network and non-classified network.

How would I know that my KVMs are being attacked?

You will not know.

Targeted attacks on KVM?

What else can be attacked to leak?

Nothing. Just the KVMs. There is no other equipment with the potential to leak. Attackers would never target a network diode or a pump as they know that it would be an impossible task.

Where is the attacker located?

Typically in a remote site (different country, different continent). The magic of the internet...

Who is the potential attacker?

Depending on the value of your classified information. It can range from one or two team members to large number of specialized experts working in an agency in a hostile or friendly country. It is definitely not a bored student in California...

How long does it take?

Anything from weeks to years depending on how important is the information and how vulnerable your organization.

Targeted attacks on KVM?

Is the attack is KVM model specific?

There are many similarities and common vulnerabilities across different product. Still when secure KVMs involved the attack must be very much model dependant.

How would the attacker know what KVM models I have?

Sometimes he / she can find that information on the internet (bids, solicitations). Sometime he / she will guess and try. In most cases the attacker will run an agent that will detect the footprint of the KVM and report back the findings.

What security vulnerability exists in a display?

Display in normal use – does not have any security vulnerabilities. Only a shared display is having some critical security vulnerabilities. The difference that cause the problems – the sharing. Shared resource = big risks.

Can I avoid shared display security issues by disconnecting EDID?

In most cases it is not possible – EDID is needed to get proper display settings from video driver, OS and applications.

Targeted attacks on KVM?

So what is the attack concept?

1. Typically the attacker gains access to the non-classified network that is connected to the internet. This is done through firewall penetration. Not too complex for professional attackers.
2. Next step is to inject some code into the classified network. As this network is isolated – the attacker typically uses some type of social attack. The code that injected is used to provide signaling to the other side of the KVM.
3. The attacker scans the non-classified network with an attempt to receive the signaling.
4. Once signaling is received, the attacker knows that that KVM is located in the critical position. The leakage starts from that point.

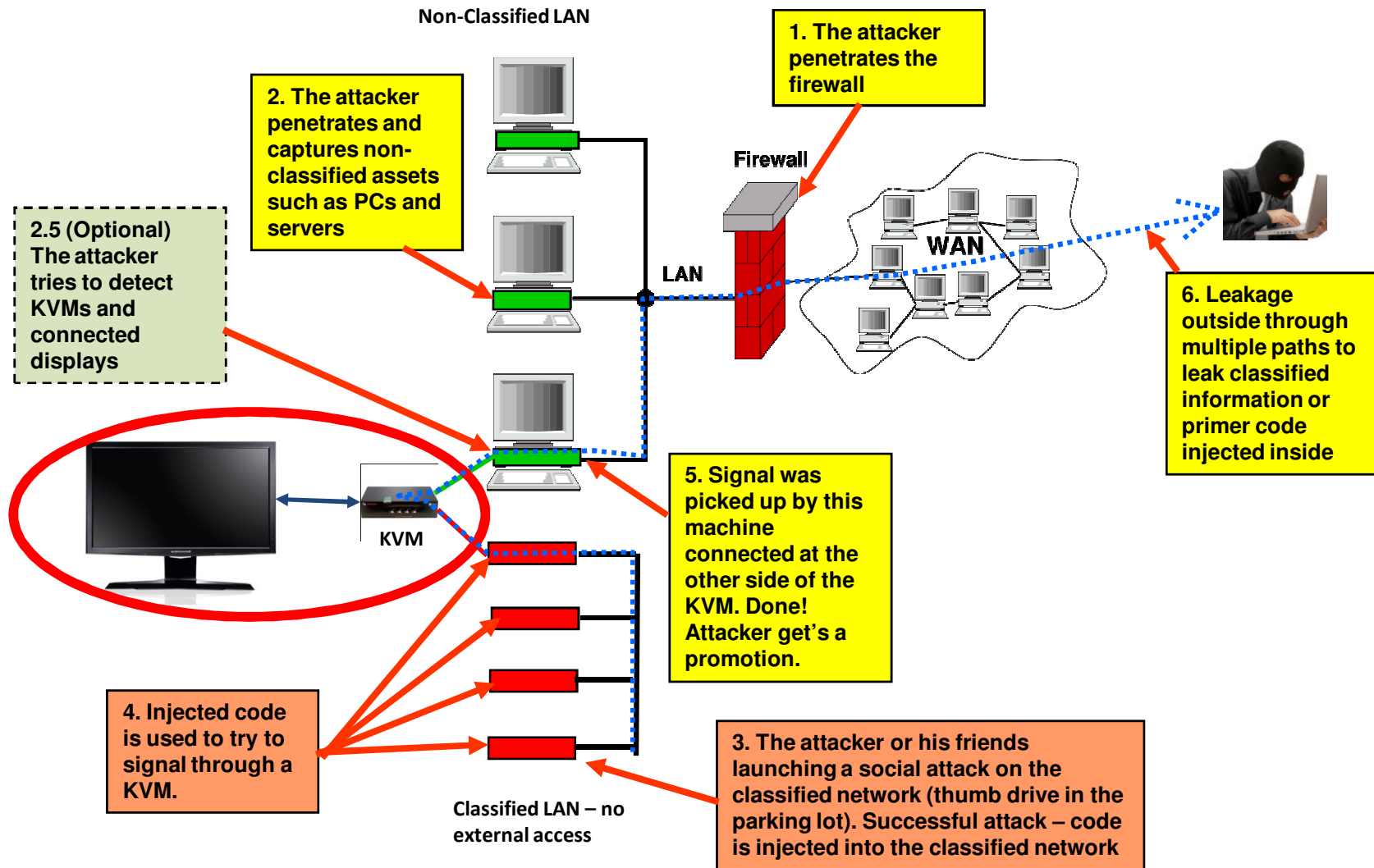
Any specific displays that are more vulnerable?

Displays that their EDID lines are used to control the display through VESA Monitor Control Command Set (MCCS).

How would the attacker know what KVM models I have?

Sometimes he / she can find that information on the internet (bids, solicitations). Sometime he / she will guess and try. In most cases the attacker will run an agent that will detect the footprint of the KVM and report back the findings.

KVM + Display Remote attack and leakage scenario



Targeted attacks on KVM?

Can I use IDS or anti-virus software to detect this attack?

No. The malicious code involved in these attacks are not well detected and profiled. This is a custom code made by professionals with very specific intentions. They know all about your IDS. Even if you can detect one code, there is a high chance that you will not detect the next one.

How the KVM user is involved in such attack?

Typically the user is not involved at all. The attack is abusing his / her equipment. Nothing else. In most cases the user is not aware of the attack or the resulted leak.

What can I do to protect from such attack?

1. Use latest high security KVMs only. Remove everything else.
2. Segment your networks.
3. Protect your organization from social attacks by proper training and tools.

How often attacks like that happens?

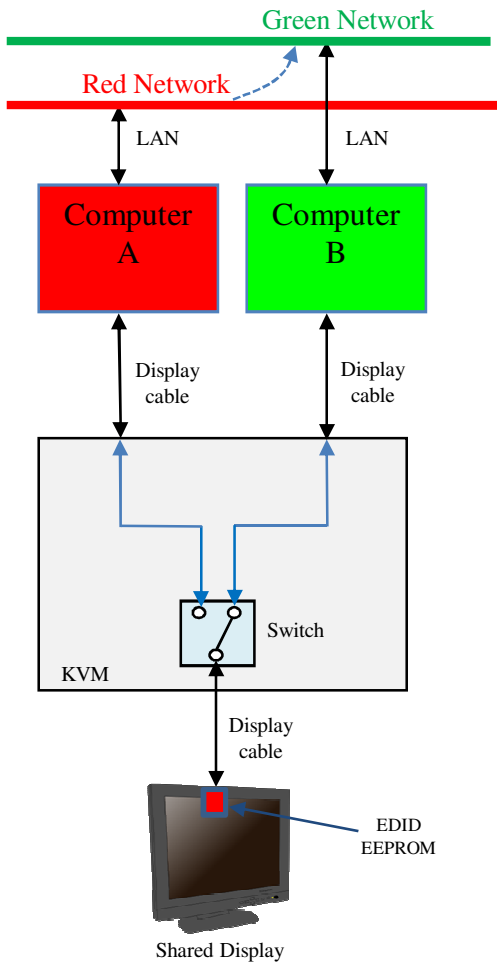
No one knows...

Most of them are undetected.

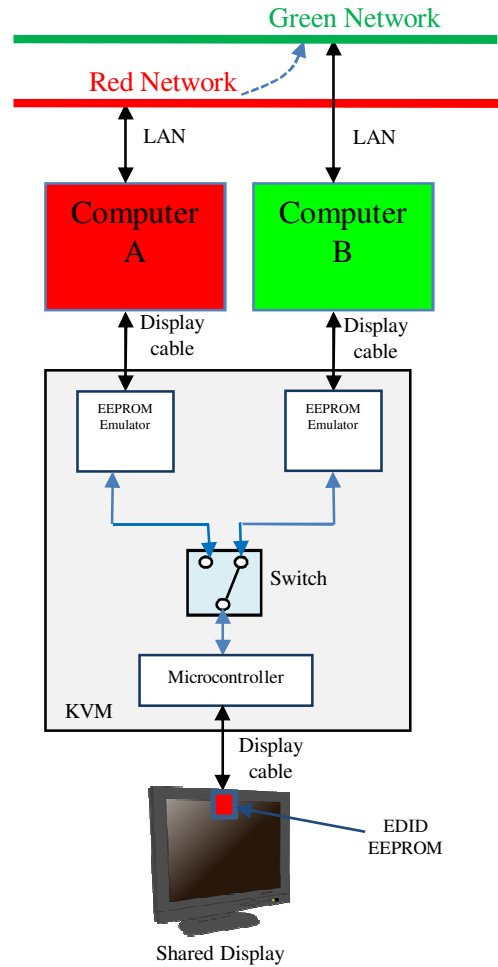
The common assumption in the Cyber defense community is: *"If the can – they will!"*

Display-KVM Vulnerabilities

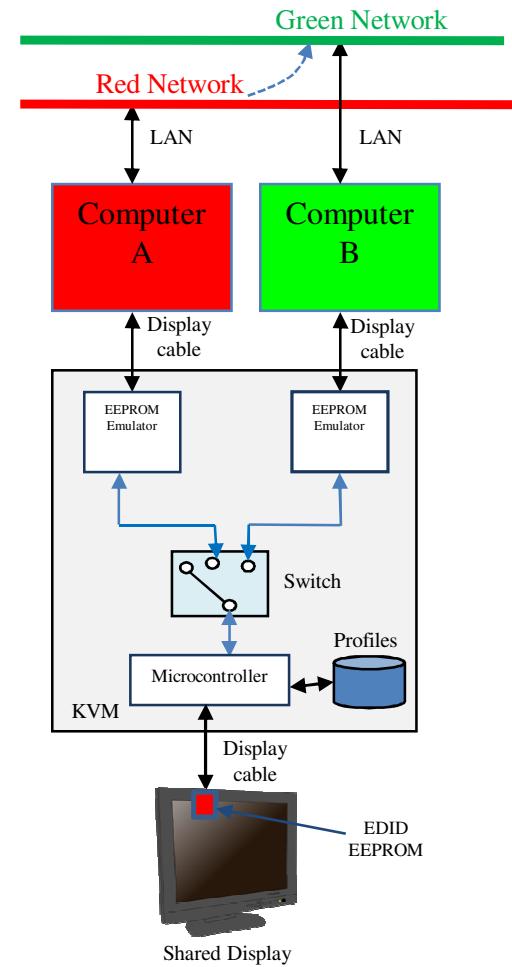
Commercial KVM



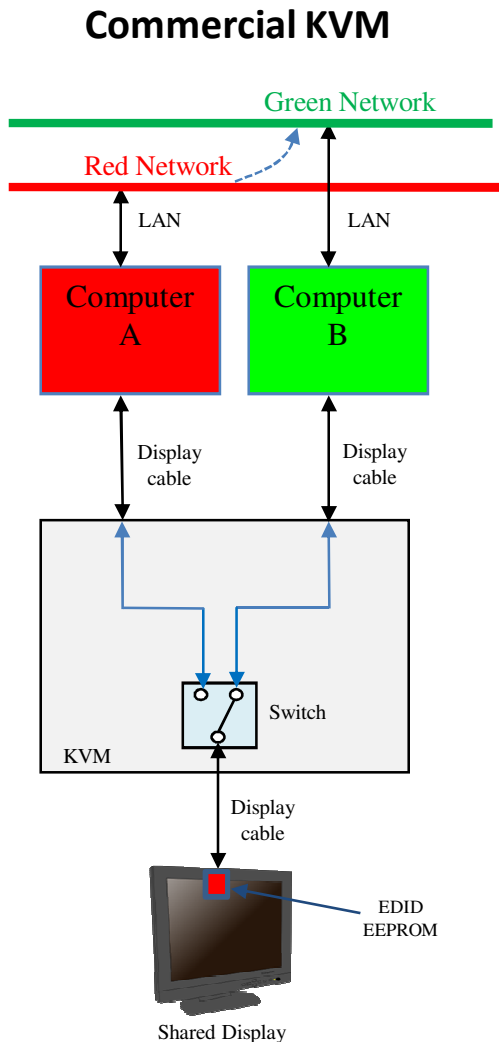
2nd Gen Secure KVM



3rd Gen Secure KVM



Display-KVM Vulnerabilities – Commercial KVM



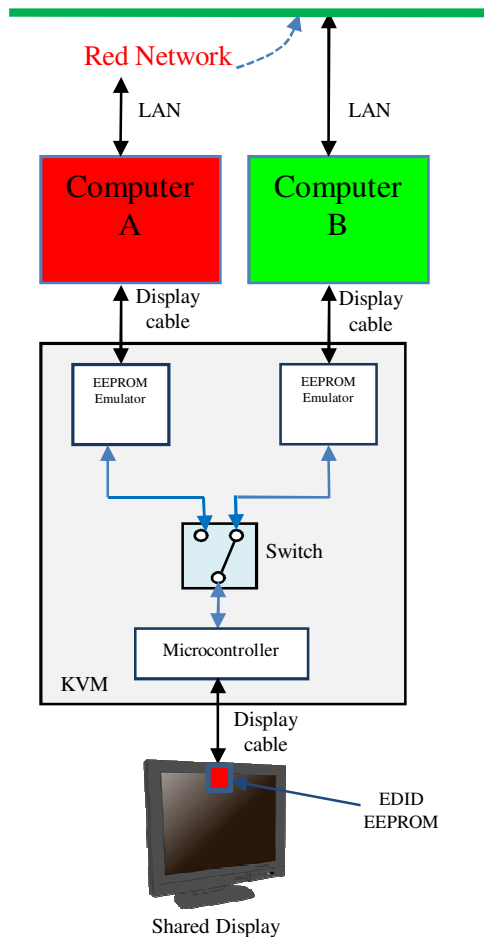
Attacker uses certain memory effects in the shared display to leave messages (signal) from computer A to computer B:

1. Hostile code injected into computer A is continuously toggling EDID CLK signal to deliver '1' or stop toggling to signal '0'
2. At each KVM switching the malicious code running in PC B immediately analyzing the EDID chip state if it is in transition state then it records '1', if it is in idle state then it records '0'.
3. At the end of the day there are several bytes that passed. Things can go much faster at night as the KVM switching may be controlled by PC A and this will allow several Megabytes of data to leak between computer A and B.
4. Computer B sends the received information to the attacker using various deception techniques to prevent detection. Usually using mailboxes.

Note: there are many other EDID signaling methods other than the one mentioned here. All using some type of residual state memory to cause single bit flow at a time (signaling)

2nd Gen SKVM – EDID operation

2nd Gen Secure KVM



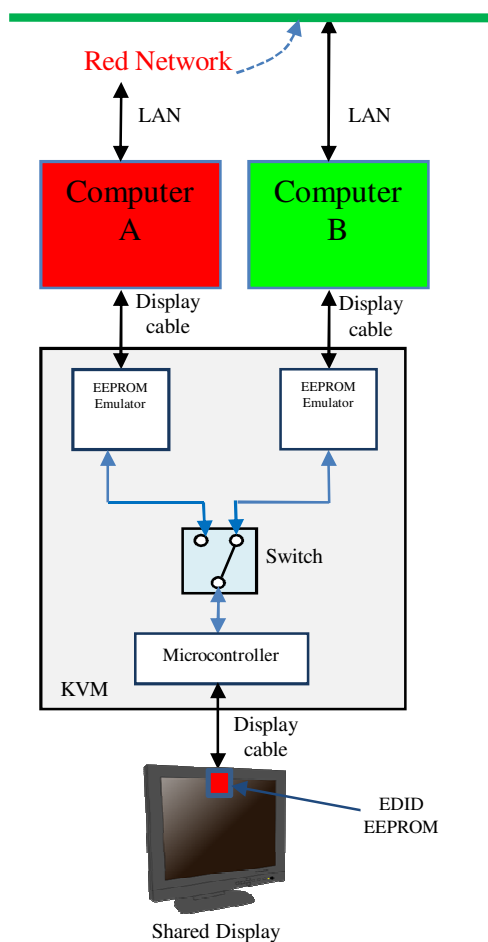
1. During KVM boot or power up the shared display EDID content is read by microcontroller.
2. Following that read the copied content is written into the 2 or more EEPROM emulators (one for each channel).
3. Once completed writing, the microcontroller places the two EEPROM emulators in write protected mode.
4. When KVM starts normal operation, computers A and B accessing their respective EEPROM emulators to copy shared display EDID content.

This implementation preventing direct access of the connected computers into a shared resource and thus can prevent most Display-KVM attacks. Still there are several vulnerabilities that may be abused to signal bits across this system as will be shown in the next slide.

Another possible form of attack is on the KVM microcontroller. By modifying its code, it is possible to use EEPROM emulators to copy large set of data from computer A to computer B.

Display-KVM Vulnerabilities – 2nd Gen SKVM

2nd Gen Secure KVM

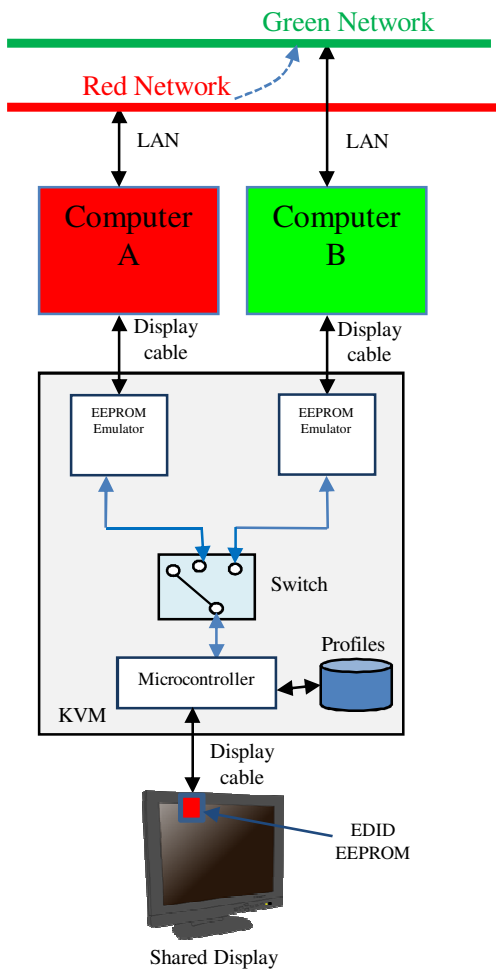


Similar to the previous scenario but here the attacker is limited to much smaller number of potential signals as EDID emulators are blocking many “real-time” signaling options. Still there are several good options.

1. Hostile code injected into computer A is causing the EDID EEPROM chip to enter a factory test mode to signal ‘1’ immediately after KVM reading.
2. At each KVM power up the malicious code running in PC B can check the display EDID chip state. If it is in factory test mode then it records ‘1’, if it is in other state then it records ‘0’.
3. At the end of the month there are several bytes that passed from A to B. Things can go much faster at night as the KVM reboots may be controlled by using USB power signaling. This signaling will cause the KVM to reboot repeatedly and hence signal at much faster rate.
4. Computer B sends the received information to the attacker using various deception techniques to prevent detection. Usually using mailboxes.

Note: Power signaling of 2nd generation KVM is typically possible through various software defined power interrupts. If not possible then alternative methods can be used to speed signaling rate through the use of several bits per re-boot.

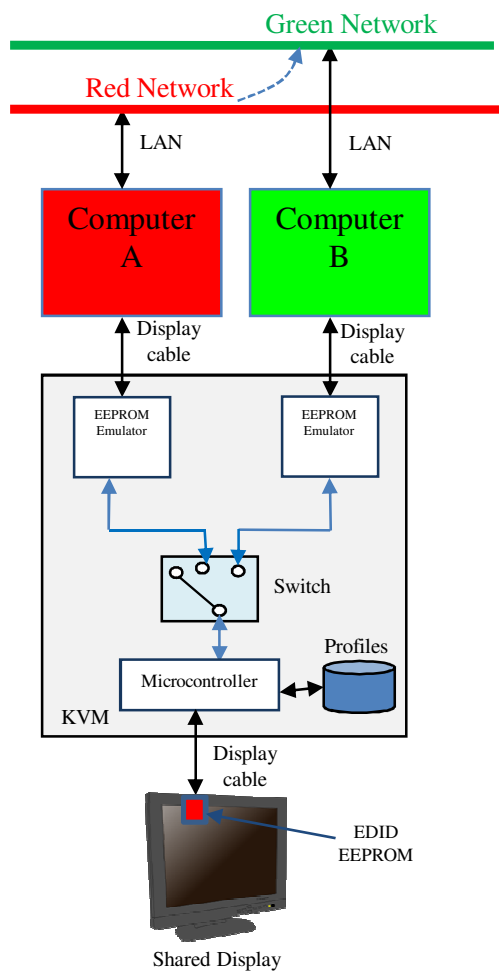
3rd Gen SKVM – Method of operation



There are several improvements compared to 2nd generation secure KVMs:

1. The microcontroller in the KVM checks and qualifies the EDID content copied from the shared display against profiles stored in its permanent memory. Only valid EDID content that passed this qualification will be copied to the EEPROM Emulators. If display failed to qualify display status LED will blink to provide user indication.
2. To prevent certain signaling attacks through the EEPROM emulators, when KVM is in operation mode, the EEPROM Emulators are electrically isolated from the microcontroller.
3. Display EDID content is static – it cannot be changed after initial KVM power up. Information is not latched. If shared display is disconnected from the KVM then video functions will be disabled until next power up cycle.

Display-KVM Vulnerabilities – 3rd Gen SKVM



There is no known EDID / Display attack method for this KVM.

- Even if the attacker successfully reprogrammed the KVM Microcontroller, he / she will not be able to leak data as EEPROM emulators are not writable by connected computers and microcontroller is not accessible to the computers in normal KVM use mode.
- Even complex attack scenarios evolving modified display firmware and attacks from both computers will not cause information leakage across the KVM as the modified display will be rejected.

Attack example: Making Display EDID Programmable

The strategy

Simple physical tampering of a standard display that will make its EDID memory chip rewriteable. This simple example assists later in KVM-Display leakage attack through EDID channel.

Implementation

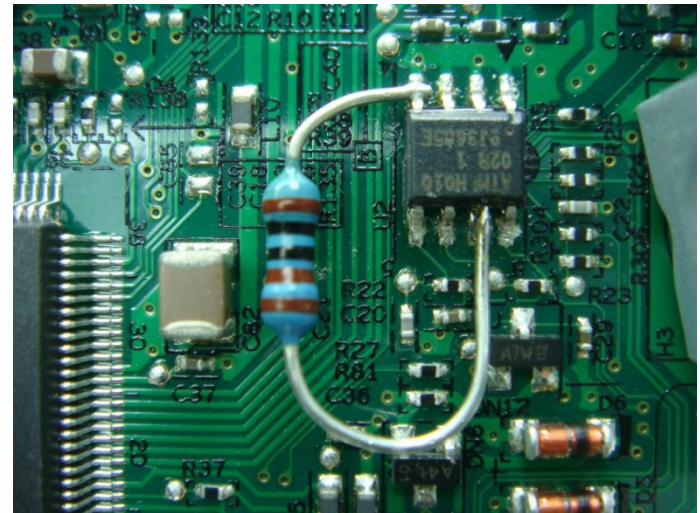
Attacker needs 5 minutes of uninterrupted access to the display, small Phillips screwdriver and soldering iron. Attacker will access the display controller board, find the EDID EEPROM and bridge the Write Protect pin (7) to the ground pin (4) using a short wire or 470 Ohm resistor. Attacker then launches a simple leakage attack by writing leaked data in the display EDID EEPROM unused data space.

Results

At least 256 Bytes of data can be leaked across the KVM at each channel switching. If attacker controls the KVM (at night) Mega Bytes of information can easily leak every night.

Prevention

3rd Generation secure KVM. Internal inspection of all displays.



Display-KVM Vulnerabilities

Protection Feature	Commercial KVM	2 nd Gen Secure KVM	3 rd Gen Secure KVM
EDID is emulated	No	Yes	Yes
EDID emulation is written only at boot (static)	No	Yes/No (some)	Yes
EDID circuitry is independently powered	No	Yes/No (some)	Yes
EDID emulators are isolated from microcontroller	No	No	Yes
EDID content is qualified against a pre-defined profile (firewall) + user indication	No	No	Yes
Products	All non Common Criteria products,	Avocent: SC420, SC440, SC540, SC4 PDV, SC4 UAD Belkin: F1DN102U Adder: SW200xA-USB-EAL, AVSD100x Argon: Ruggedized KVM (SC440 inside)	Belkin: New Advanced DVI-I Secure KVMs

KVM EDID Testing

Most KVM vendors would not tell you what protection methods they are using for EDID. Here are some simple methods / tests that will allow you to find out by yourself:

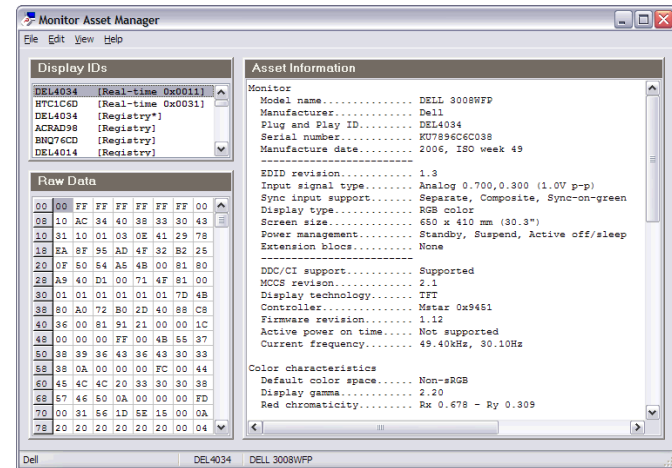
Does my KVM use emulators?

1. Check in NIAP web-site – validate product list <http://www.niap-ccavs.org/vpl/>. Download the Security Target and look for technical description of EDID circuitry.

2. Connect the KVM to a computer without connecting any display. Look at control panel display to see if display was detected. Most KVMs having emulators (2nd Gen) will show the parameters of the last display connected.

Does my KVM EDID design is static?

Change the shared display after KVM was turned on and see if computers will detect the new display. If new display was detected then – either the KVM does not have EDID emulation or the KVM EDID design is not static (2nd Generation Secure KVM).



KVM EDID Testing – cont.

How to test EDID firewall?

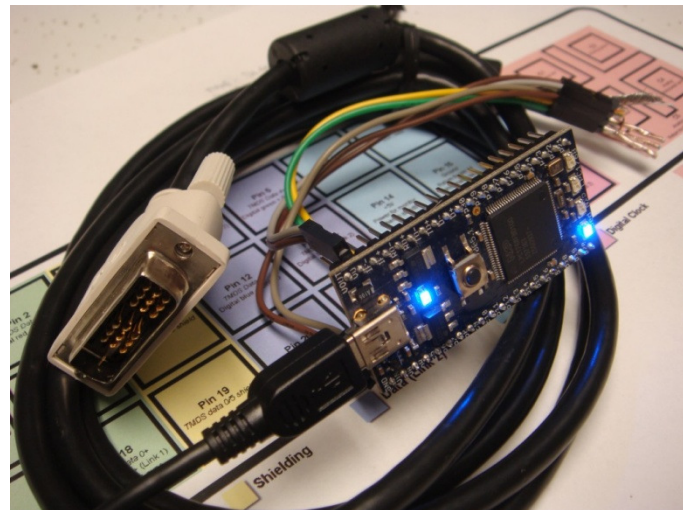
You will need to build a custom hardware / software environment to test this function.

Tools needed:

- USB I2C programmer (see http://www.diolan.com/i2c/i2c_interface.html)
- Display cable (DVI or VGA). One side need to be cut to connect the EEPROM chip.
- I2C 2KB memory chip (see Digi-key <http://search.digikey.com/scripts/DkSearch/dksus.dll?Detail&name=24VL024HT/SNCT-ND>)
- See cable connection details in <http://www.imsolidstate.com/archives/879>
- Download DDC viewer software (for example: http://programming.softlandmark.com/components_and_libraries/WinI2C_DDC_Lite_Info.html)

Test process

1. Build the special cable.
2. Capture real display EDID content and program into the emulated EDID chip that you assembled.
3. Test with the DDC viewer program to verify.
4. Modify the EDID content and check with a KVM. See if KVM will reject the display (3rd Generation Secure KVM only).



Display - KVM Vulnerabilities

Attack method	Commercial KVM	2 nd Gen Secure KVM	3 rd Gen Secure KVM
Signaling attack using display re-write hardware tampering	High Risk	Medium Risk	Low/No Risk
Signaling attack using EDID residual memory	High Risk	Low/No Risk	Low/No Risk
Mailbox attack through MCCS functions	High Risk	Medium Risk	Low/No Risk
Mailbox attack through firmware update	High Risk	Medium Risk	Low/No Risk
Display image capture attack	Low/No Risk	Low/No Risk	Low/No Risk
KVM code attack on EDID microcontroller	Low/No Risk	Medium Risk	Low/No Risk

Legend:

High Risk

Medium Risk

Low/No Risk

Attack Methods – Signaling attack using display re-write hardware tampering

The strategy

Attacker modifies the display hardware making the EDID EEPROM rewriteable.

Implementation

Attacker can first modify several displays before shipment to the customer. The rest of the attack can be done remotely: attacker will use infected network to search for these individual displays and link them to KVMs. Once suitable target is found – the signaling attack is done through the use of the shared display EDID chip as a mailbox. Every time the KVM switches from A to B, data stored in EDID chip is leaked from A to B.

Results

Fast signaling attack across the KVM. May be further accelerated if computer A is capable of controlling KVM switching at night.

Prevention

3RD Generation Secure KVM will efficiently block all known forms of this attack. 2nd Generation Secure KVM provides partial protection. Detection methods including EDID write read attempt scripts and DDC read – write programs.

Attack Methods – Signaling using EDID residual memory

The strategy

Attacker uses a malicious code in computer A to continuously / momentary interact with shared display EDID chip to signal '1' or otherwise to signal '0'. Once KVM switches over to computer B information can be read by modified display driver to extract the '0' and '1'. Bytes constructed by this process are sent to a remote location where the attacker can retrieve it.

Implementation

Attacker will detect KVMs and shared displays in network B to identify potential target. Attacker will install malicious code in computer A to interact with shared EDID using one or more methods of residual memory. The another code installed in computer B is used to collect this signaling and construct useful data. This data is then sent to the attacker using a method that would not leave a trace.

Results

Leakage of several bits or bytes per day. Can be accelerated if computer B is capable of controlling KVM switching at night.

Prevention

At least 2nd Generation Secure KVM.

Attack Methods - Mailbox attack through MCCS functions

The strategy

Use various programmable display settings as a mailbox to store bits / bytes of leaked data. For example: using Gama correction values attacker may leak 3 x 8 bits of data. Many of these settings would not be detectable by the user.

Implementation

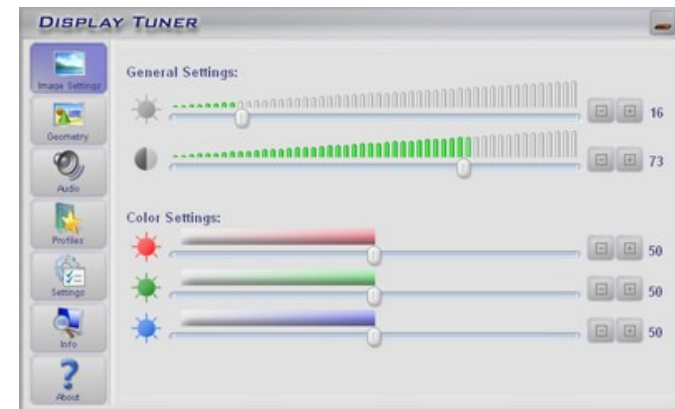
Attacker is using a modified MCCS display control utility code in computer A to store collected bits / bytes of data as various display settings. Another similar utility used by computer B to read this data after KVM switching and clear the settings. This process is repeated every time that the KVM is switching channels.

Results

Several KB of leaked data every day. Data transfer may be accelerated if computer B is capable of controlling KVM switching at night.

Prevention

3rd Generation Secure KVM.



An example of a freeware utility that can read – write display settings

Attack methods – Mailbox attack using Display Firmware Update

The strategy

Some displays enable firmware update through EDID / USB lines. For example most of iMac displays support this feature. Attacker may use this function:

1. As a mailbox to store large sets of data.
2. To program new firmware that will capture display images.

Note: Typical display controller is as powerful as intel x386 processor. Many teams tried to demonstrate a leakage through image capture using modified firmware. While capture itself was possible, no team was able to demonstrate the next step – how this image can be leaked into the other channel through the video port. Therefore strategy No. 2 here is currently impossible.

Most of these attacks were demonstrated using high-end displays such as Apple, Samsung and Eizo. Some displays support this function but it is undocumented.

Implementation

Attacker detect a display that support this feature coupled through a KVM (by scanning network A). Once found, data from network A is copied into the display controller flash using update utility code (USB or EDID). Once KVM switches the shared display into computer B, a malicious code in B uses a modified firmware update code to read that data stored in the display controller flash. If read is not possible then firmware version and date are used to leak at least 20 bytes of data at each switching.

Attack methods – Mailbox attack using Display Firmware Update – Cont.

Results

At least 512 Bytes of data can be leaked across the KVM at each channel switching. If attacker controls the KVM (at night) Mega Bytes of information can easily leak every night.

Prevention

2nd Generation secure KVM.

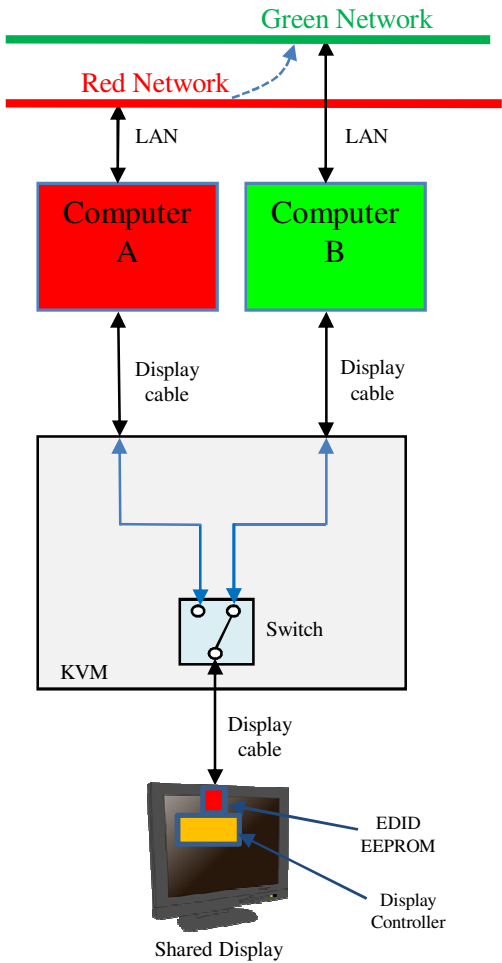
Note: Unfortunately there is no reliable database of display vulnerabilities that exist today.

As general rules:

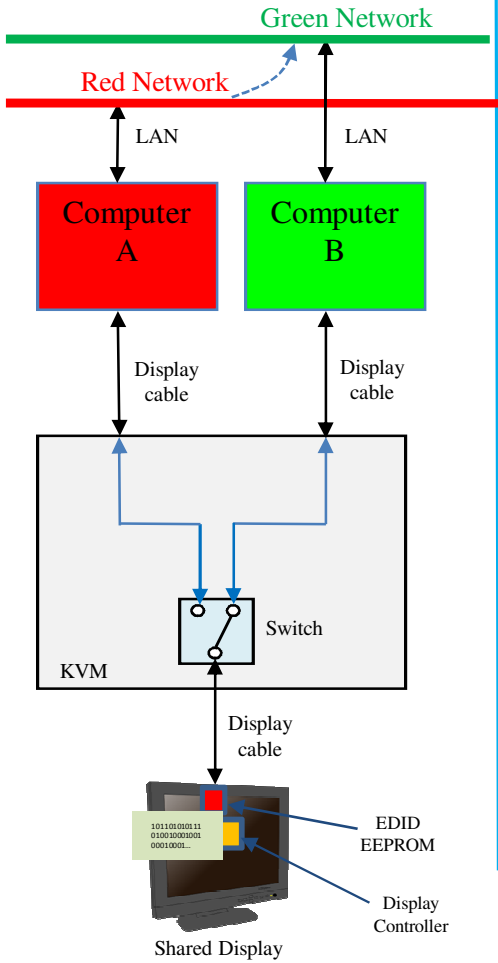
- Do not use high-end displays with non-secure KVMs.
- Do not connect display USB ports to anything!

Attack methods – Mailbox attack using Display Firmware Update – Cont.

Step 1 – critical data collected by computer A for delivery

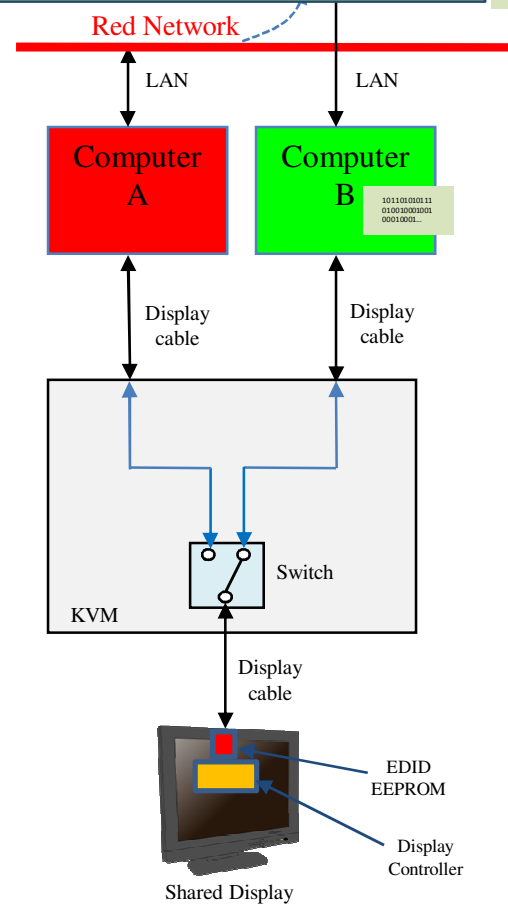


Step 2 – malicious code in computer A copies the leaked data as part of a display firmware update.



Step 3 – malicious code in computer B reads firmware update fields and reconstructs leaked data.

Step 4 – leaked data is transmitted to the remote attacker using an untraceable method.



Attack Methods – Display image capture attack

The strategy

Attacker recognize a target display with capture capability and uses this capability to capture classified images from one network (computer A) and release that data using USB interface at the other network (computer B).

Implementation

Complex and very much model dependant. Can be demonstrated in some Apple displays with USB ports. Relatively complex attack. Estimated 1 man/year to develop capture capabilities for one specific display model.

Results

Snapshots of user display or even artificial picture made of leaked data from computer A can be captured by display controller and linked through EDID or USB lines to computer B.

Prevention

Use 3rd Generation Secure KVM. Leave display USB ports unconnected.

Attack Methods – KVM code attack on EDID microcontroller

The strategy

Modify KVM functionality so it will leak data internally through the EEPROM Emulators. Attacker is aware of the microcontroller type in the KVM and tested many types of attacks on same KVM in his / her lab. Attacker will run necessary code on computer B to program required code change inside attacked KVM.

Implementation

Attacker is able to modify the code in KVM display microcontroller to disable the write protect and allow computer A to write leaked data on EEPROM Emulator. Then the modified microcontroller reads that code and write it into the second EEPROM Emulator. A malicious code installed in computer B can read this modified EDID content and record the leaked data bytes.

Results

Constant leakage of kilobytes or even megabytes of data through the KVM.

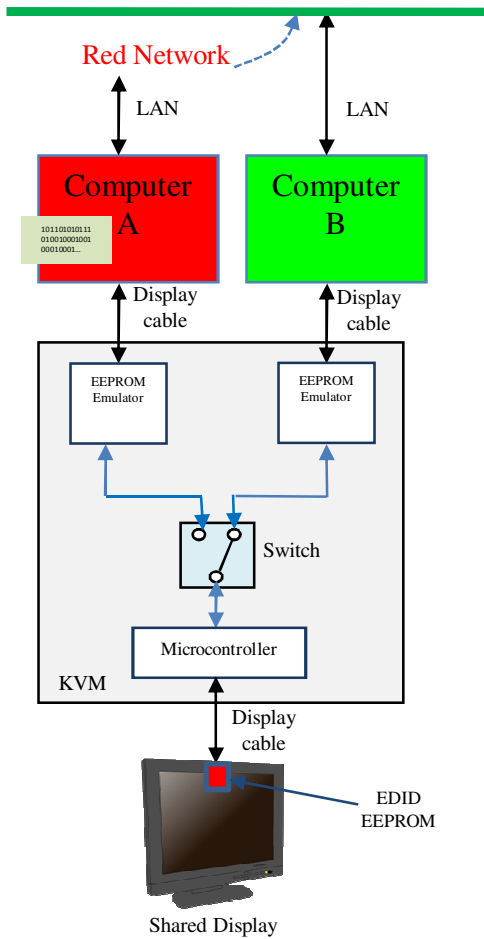
Prevention

Only 3rd Generation Secure KVM EDID Firewall functionality can prevent this form of attack.

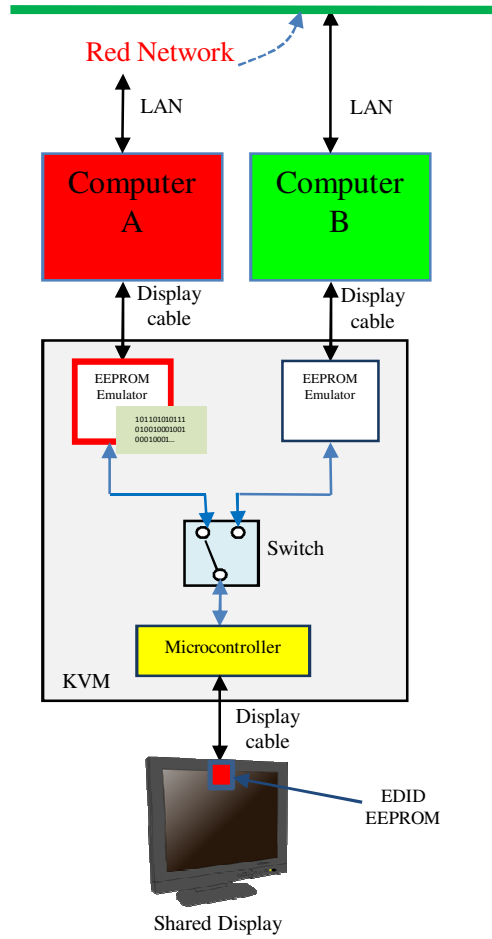
Attack Methods – KVM code attack on EDID microcontroller

Step 1 – critical data collected by computer A for delivery

2nd Gen Secure KVM

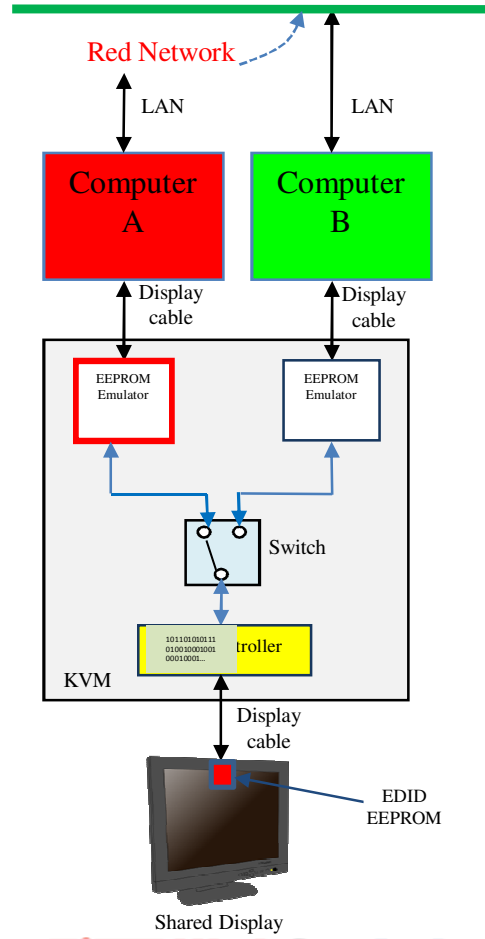


Step 2 – modified code in microcontroller disables the write protection of computer A EEPROM Emulator. Computer A malicious code writing leaked data into EEPROM



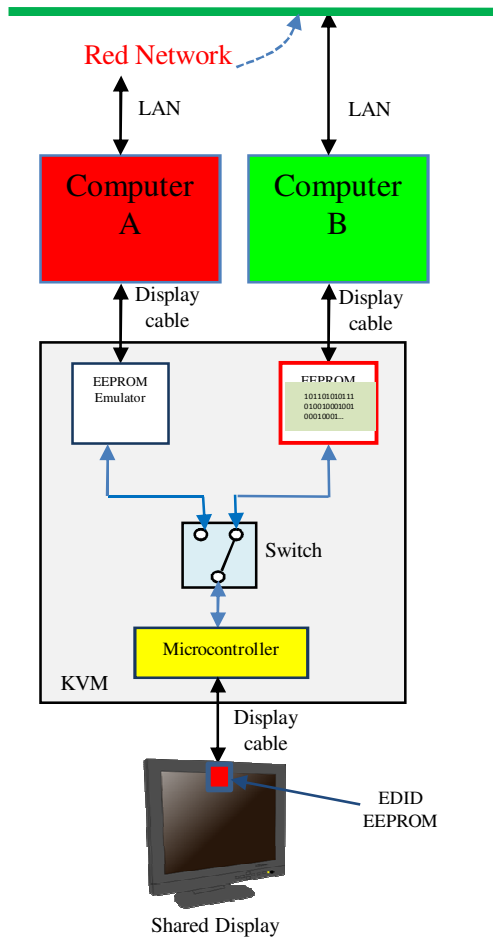
Step 3 – modified code in microcontroller reads the left side EEPROM Emulator content.

2nd Gen Secure KVM



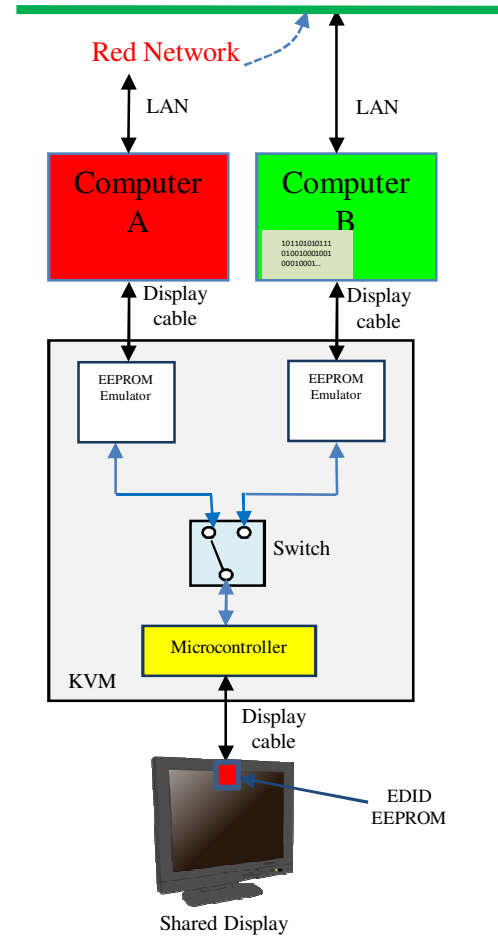
Attack Methods – KVM code attack on EDID microcontroller

Step 4 – once KVM is switched to computer B – modified code in microcontroller disables the EEPROM Emulator write protect and writes the leaked data into the chip



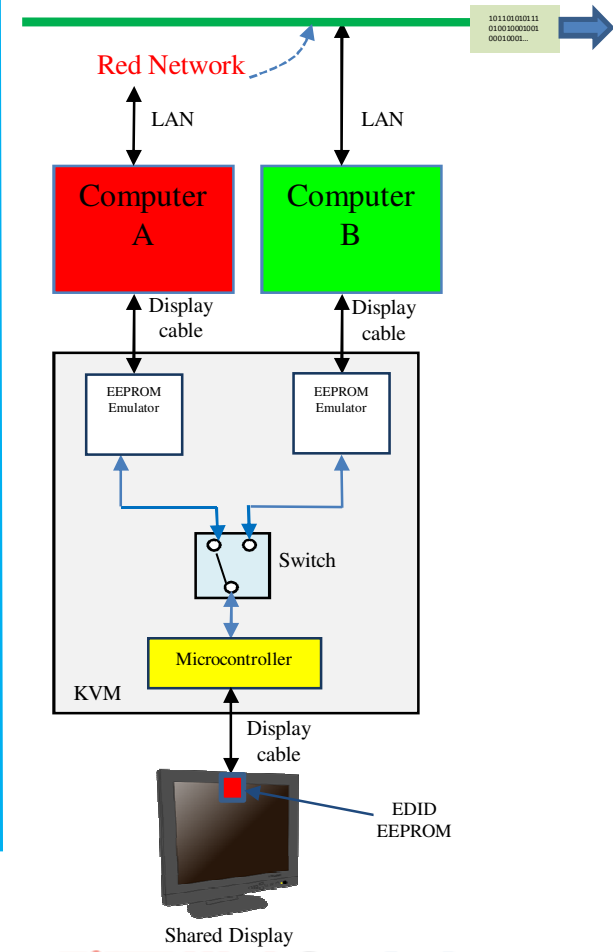
Step 5 – malicious code in computer B copies the EEPROM Emulator content and extract the leaked data.

2nd Gen Secure KVM



Step 6 – leaked data is transmitted to the remote attacker using an untraceable method.

2nd Gen Secure KVM



What the DOD think about this?

Official position:

“In 2005, the Defense Science Board of the Department of Defense expressed concerns about the migration of microelectronics foundries from the United States to foreign countries and its impact on the security of microchips and microelectronic components delivered to the government and military and used in critical infrastructure [3]. If an adversary is able to gain access to a microelectronic component during the design phase, then a clandestine modification will corrupt every unit manufactured and the confidentiality, integrity or availability of any system using such a component can be compromised. Moreover, given the complexity of modern systems, such a modification can be deeply embedded into a system and difficult to detect and attribute.”

For full document see: http://www.cra.org/govaffairs/images/2005-02-HPMS_Report_Final.pdf

The message here is clear – if you can't trust your peripherals – at least connect a secure KVM that will protect you from them. Secure KVMs are made in the US and you can trust them (at least some of them). 3rd Generation Secure KVMs are the only efficient protection method against all known KVM – Display vulnerabilities.

Additional information

Much of the information discussed here was collected by agencies and it is still classified. Still additional information can be found on the internet:

EDID EEPROM chips

<http://ww1.microchip.com/downloads/en/DeviceDoc/21682E.pdf>

Display firmware updates

- <http://support.apple.com/kb/TS3207>
- <http://support.apple.com/kb/DL1338>
- <http://www.fixdevice.com/firmwares/cat/monitor.html>

Display attacks

- <http://www.imsolidstate.com/archives/879>

MCCS

- http://en.wikipedia.org/wiki/Monitor_Control_Command_Set
- <http://www.bluechillies.com/details/41987.html>