

Training Module 1 – KVM Misconceptions

Rev B
July 27, 2011



Target audience:

1. End users - IT procurement
2. End users - IT manager / stuff
3. End users - IT Security officers
4. HSL sales people and key channels

Myth #1:“KVM is not connected to the network and therefore it shouldn’t be treated as network vulnerability”

The truth is:

KVM is an IT equipment that touches two computers. These two computers are typically touching two “isolated” networks. Therefore the KVM may be used to *leak information* between these two networks. Just like a firewall but much easier to break!

“KVM is as critical as any other piece of IT equipment having one leg in one network and another leg in another network.”

Myth #2: “It is always better without a KVM”

The truth is:

1. Ask your users. In many cases it may be impractical or inefficient to operate without KVMs.
2. What will you do with 3 or 4 networks without KVM?
3. There are major security concerns when users interacting with several computers without a KVM.

“In many real-world scenarios having multiple isolated networks – KVM is an essential and critical productivity and security tool”

Myth #3: “To cause a KVM to leak data one must physically tamper that KVM”

The truth is:

No no no! There are many possible attack scenarios that tampers the firmware or even leak data around the KVM without touching the KVM at all! Most known methods are double-sided remote attacks by two infected computers.

In fact the biggest vulnerability of a non-secure KVM is its capability to contain a hidden leakage or conditional leakage. These leakages are extremely hard to detect. Coupled with infected computer and secret networks may easily leak to the internet.

Physical KVM tampering is definitely not the common attack method today.

“The biggest risk of a KVM is the potential to leak data between channels. Use secure KVM if you want protection”

Myth #4: “PS/2 is safer than USB”

The truth is:

Not at all.

1. PS/2 peripherals are much more vulnerable to eavesdropping or electromagnetic leakages compared to USB. PS/2 is single-ended non-shielded signal while USB is balanced differential and shielded signal.
2. PS/2 data loggers and mass-storage devices can store secret data just like USB devices.
3. Most USB protection means are inefficient in protecting PS/2 port.

In any case PS/2 becomes an obsolete technology now. Hard to support in new PC platforms and OSs.

“Forget PS/2. Its history”

Myth #5: “Audio leakages can only leak audio content”

The truth is:

Audio signal leakages can cause severe data leakages between networks.

There are several well-known KVM attack scenarios that uses the internal audio channels just like old telephony modems – data stream converted to audio “beeps” and back to digital stream at the other end. The result is slow data leakage between networks.

“Treat audio channels as potential security vulnerability (with and without KVM)”

Myth #6: “Computer displays are not a security vulnerability. They are state-less and uni-directional by design ”

The truth is:

A single display shared between different networks is a major security concern. Modern display are digitally communicating with the coupled computers using bi-directional data flow. This communication channel is normally used for Plug and Play but can be easily abused for data leakages between computers.

You can't simply disable Plug and Play or cut these lines.

Many of the new computer displays are having a programmable microcontroller inside to support remote management.

Another area that can be abused for leakages.

“Treat shared display as a transparent data bridge”

Myth #7: “The primary concern with KVM use in classified networks is the electromagnetic leakages or TEMPEST”

The truth is:

During the cold-war, this statement was true. Today analog telephony, fax and telex are hardly used anymore. Most of the communications is done in the air (telephony, satellite, radio), another is in optical lines. Intelligence collection and attacks is primarily on the digital and encryption level. TEMPEST is now much smaller concern compared to digital attacks. Most KVMs are operating in a safe area just like the attached computers and peripherals.

“The odds that a black track is parking near your facility is much smaller compared to the odds that someone is trying to attack you remotely from the internet (100%)”

Myth #8: “Small data leakage is less dangerous than big files or stream coming out”

The truth is:

Definitely not true. If your administrator password is that leaked data? There are known cases where a single bit leaked caused massive damage (timing leakages for example).

Small data may enable much larger leakages afterwards. In general ANY leakage is a risk.

Over time – small (slow) leakages can add up to large data.

“In classified networks - Any leakage is critical”

Myth #9: “KVM cannot be detected on the network”

The truth is:

There are several known attacks that were designed to map coupled peripherals and KVMs. The purpose of this code is to perform “asset counting” before attacking particular KVMs. The first phase of any attack on KVM is to know that it is there. This can be easily done by software agents propagate like virus. Resulted information is stored or sent elsewhere for analysis and attack planning.

KVMs can be detected through USB device signatures and other unique characteristics. In most cases attacker can identify vendor and model.

“KVMs and connected peripherals are detectable targets”

Myth #10: “My secret network is an island. It is isolated”

The truth is:

Check if it is 3 networks away from Internet access or WAN. This means that attacking 3 KVMs in between will bridge between your secret network and the internet.

Isolation is an idealization. In reality the level of isolation depends on the level of attack invested. KVMs helping attackers to “jump” across isolated networks.

“With proper resources, most “islands” can leak. KVMs are primary targets for leaking internally. Firewalls are primary targets for leaking to the outside”

Myth #11: “The peripheral devices that we are using are safe”

The truth is:

No. They are not. Peripheral devices used with KVMs may have a memory effect that will be used by attacker to leak information. Examples are status LEDs in keyboards, Mouse resolution and settings, display settings etc.

Another issue – all peripheral devices are made in China today (including their chips). It is hard to trust these sources these day... [See US DoD opinion on this issue)

“Peripheral devices cannot be trusted. Especially when connected with a KVM”

Myth #12: “All Secure KVMs having Common Criteria certification offers the same security level”

The truth is:

Common Criteria certification provides a minimum standard.

Some products exceed that minimum by far. Some just comply with the standard.

In general KVMs that protected by physics (optical diodes) provides much higher security than KVMs with conventional electronics and firmware.

3rd generation Secure KVMs are well protected against new forms of KVM attack. In particular they are built with the assumption that one or more connected PCs are infected with malicious code and that one network has free access to the internet.

“If you are looking for security – Common Criteria is a good start. Then – check under the hood.”

Myth #13: “Active anti-tampering will prevent attacker from tamper with the KVM device”

The truth is:

It may (or may not) prevent physical tampering. Still most attacks on KVMs are done remotely on firmware of peripherals. Anti-tampering will not protect from these attacks.

Anti-tampering can be disabled by capable attacker (just like a safe). It designed to take time, knowledge, tools and effort and therefore to prevent an opportunistic attack.

Another goal is to prevent tampering while in transit or in storage.

“Anti-tampering is like protecting money in a safe - Someone may steal the whole safe.”

Myth #14: “Attacks on KVMs are being performed by hackers”

The truth is:

It is like saying that intelligence collection work is typically done by amateurs...

KVMs are primary targeted by well organized professionals / governments as part of large or focused intelligence effort to collect classified information.

Some smaller crime or terror organizations may use this strategy to assist in fraud or to cause damages.

Professional attacks may take months or years and may cost millions of dollars. Your classified information may worth millions of dollars to someone...

“KVM attacks are well sponsored and performed by highly knowledgeable professionals.”

Myth #15: “Attacks on KVMs are always attempting to leak data outside”

The truth is:

Not necessarily. Some attacks designed to import code that will damage the network or overload it once activated.

Another type of code called “primer code” may be used to create larger security breach at later time as part of multi-staged attack.

“Attacks on KVMs are equally dangerous due to potential data / code export and import.”

Myth #16: “I can detect successful attack on KVMs”

The truth is:

In many cases it is extremely hard. Leakages can happen on a random basis or even once in a life-time. If you can't find it – it doesn't mean that it is not there.

Many of the tested scenarios are requires extensive resources to detect. Standard tools will not help here. In fact in many cases it is cheaper to replace all un-trusted KVMs than to analyze their potential security risks.

“You may leak critical data from your classified networks through KVMs. You will not know it and you cannot stop it until you will replace them.” Prevention is much easier than detection.

Myth #17: “I don’t need physical isolation and secure KVMs between networks with same classification”

The truth is:

Yes you need! Think what will happen if you bridge these networks? Isolation of networks having similar or same classification is now common practice.

If someone successfully entered one network – you don’t want that the damage will soon propagate to the other network.

As security level goes up – networks much be divided properly to mitigate and contain penetration / leakage risks.

“Use network isolation and secure KVMs wherever you don’t want networks to leak to one another.”

Myth #19: “KVM is a simple hardware device”

The truth is:

Non-secure KVM is definitely a simple hardware and it can leak and abused by attackers. Secure KVM on the other hand is a sophisticated hardware – firmware device having multiple microprocessors (sometimes more than 20) that designed to protect your data.

“Secure KVMs are complex and sophisticated – same as the potential attackers .”

Myth #20: “I have few unsecure KVMs – most of my KVMs are secure. I am OK”

The truth is:

You are not OK. Your investment in the highest security KVM worth nothing once your attacker will find these weak links. Guess what – your attacker will not spend any time and effort on you secure KVMs – they will immediately focus on your old KVMs.

It may take them few minutes or hours to bridge one of these “few” older KVMs and the damage is done.

“All the attacker need is one bad KVM to target.”

Myth #21: “I can use virtual machines (VMWare) or Citrix to isolate between security levels instead of investing in KVMs”

The truth is:

Would you put your life on it? You better not...

Odds are that your potential professional attackers would not see these “soft isolation” methods as a real barrier.

In general – if your application is critical – don’t trust anything other than good old physics. Use physical separation, highly isolated KVMs, Optical data diodes and pumps etc.

“Trust only strong physical separation.”

Myth #22: “Even if my KVMs will leak – information will not reach the outside world”

The truth is:

Just like water flow – it will find its way out. It may not flow out through the internet. Creative ways to leak out data includes – people carrying data out (intentionally or unintentionally), using or abusing wireless LAN, using audio leakages, using video signaling, etc. (The list is very long).

Keep in mind that many of these attacks are using multiple stages or methods to create the required effect.

“You have to assume that any internal leakage will find its way out.”

Myth #23: “I can assume that PCs in my classified network are not infected”

The truth is:

Very small code imported into your classified network may cooperate with a tampered KVM, firewall or diode to leak data in a well hidden way.

There are known cases where highly audited “Golden Image” contained some seeds or pieces of hostile code.

Your users may find creative ways to carry infected code into your networks.

“Don’t trust your users. Don’t trust your classified networks just trust the barriers you put there.”

Myth #24: “Using multiple displays and peripherals is more secure than using a KVM”

The truth is:

Not correct. Several researches done by agencies showed that human errors involved with multiple displays and peripherals are much more frequent and dangerous compared to KVM setup. Additional workload always causing more errors.

New secure KVMs offering customization and indication options to further improve user situational awareness.

“Secure KVM is always more secure than a messy desktop.”

Myth #25: “I have other things to do with my IT security budget than spending them on KVMs”

The truth is:

Your whole annual investment in IT security will be worthless if you have one leaking KVM somewhere in your network...

You can spend millions of dollars in firewalls and anti-virus. Nothing will help you against internal leakage threats.

Today the #1 vulnerability target in defense organizations is the KVM. Protect your organization or prepare to leak...

“KVM removal / retrofit is critical and necessary investment – don’t wait for next year budget!”