# Hackers in the Classroom:

## How to Secure Your AV Systems from Internal & External Threats

They're out there: Hackers and curious students who would love to break into your Classroom or Lecture room automation system and wreak havoc. This AMX White Paper explores the complex world of AV security and provides tips on how you can make your systems secure.

## INTRODUCTION: A VERY BAD DAY

The Dean of the School of Education is teaching her weekly class using a PowerPoint presentation and live feed from one of the early childhood development classrooms. The technology is working flawlessly and facilitating a wonderful discussion about teaching techniques for children with speech delay.

Meanwhile, hackers had discovered vulnerability in the system's web interface and compromised the system. They took control of a camera, recorded some of the audio and video and used the system as a jumping off point to hack into other critical systems. By the time the class concluded, it was too late.

Sound farfetched? Not at all. This is just one example of the damage that educational institutions face if they fail to implement strong security measures for their AV systems. Furthermore, external hackers are not the only security threat when it comes to AV systems - it's not uncommon for the threat to originate from the institutions student body, or for expensive AV equipment to "disappear" from a classroom ostensibly to show a movie at a fraternity party.

Now that individual AV components have become visible nodes on the overall IT network, it is imperative to recognize potential weaknesses and devise a plan for ensuring that your AV systems and assets remain secure.

### Snapshot: What damage can hackers inflict in a videoconferencing system?

| |
|---|
| Anonymously join VTC sessions |
| Upload malicious code to initiate Denial of Service attacks |
| Take control of cameras |
| Record audio and video streams and take snapshots |
| Establish a new session for eavesdropping |
| Use the system as a jumping off point and hiding place to exploit other systems |
| Edit configuration settings to make other features vulnerable |

## PROTECTING PHYSICAL ASSETS

### Physical asset Security

A typical classroom AV installation includes a touch panel for controlling the equipment and a controller or all-in-one presentation switcher for managing the audio and video inputs and outputs. The touch panel usually sits on the classroom table, while the controller or switcher sits in a cabinet or is installed in an equipment rack.

While IT organizations are fully aware of the implications of physically protecting IT assets such as laptops and servers, they sometimes forget that touch panels and controllers are expensive resources that reside in rooms that are frequently vacant. In short, they can disappear – or they can be used as an entry point into the IT network.

Fortunately, there are simple and effective ways to secure touch panels to a classroom wall, table or lectern. For example, AMX offers mount kits and/or Kensington locks that secure touch panels in the room without sacrificing aesthetics. This added level of physical security is but one of several reasons why AMX recommends dedicated touch panels over tablets like the iPad as a user interface in most types of classrooms.

AMX's NetLinx controllers and Enova DVX All-in-One Presentation Switchers have a small footprint that makes them suitable for locking in a small cabinet in the classroom itself. Additionally, most controllers and touch panels can be password protected to minimize the risk of unauthorized intrusion onto the network.

**Monitoring and maintaining AV assets**

AV and IT originated as separate silos. One of the major differences between the two disciplines was that the IT paradigm embraced real-time performance monitoring from a central location or network operations center, while AV assets were treated as stand-alone islands.

One obvious way of maintaining security is to monitor those assets in real time to detect when they might go offline or when their performance paramaters might abruptly change due to intrusion. AMX provides this capability via its Resource Management Suite (RMS) software, which enables real-time network visibility of all AV assets on the network.

## SECURING THE ROGUE ASSET: THE CLASSROOMROOM PC


One particular asset in the AV ecosystem deserves special mention: The dedicated classroom PC. Over the past few years, the PC has become a staple in the modern classroom, primarily as a tool for accessing the web and sharing content. Unfortunately, personal computers are not ideally suited for this purpose, as they require frequent software updates, take a long time to boot (thereby delaying the start of a meeting), and represent a significant security risk far beyond the typical risks of viruses and malware. That's why devices specifically designed for room collaboration, such as AMX's ENZO Cloud Presentation System, are expected to explode in popularity over the next several years.

Despite the widespread incidence of hackers and malware, sometimes the most significant threat to a network can come in the form of a curious student. In the case of the classroom PC, the threat can also arise when a meeting organizer fails to take the final step to purge the system of the information that was shared during the meeting.

**Logging Out**


Typically, meeting attendees will use the classroom PC to access files and other information over the corporate network by logging in under their corporate login credentials. One of the most common problems with shared PCs is that the user frequently forgets to log out, leaving the system open when the next person enters the classroom. While most systems are set up to automatically time out after the PC has been idle for a short time, there will always be incidences in which a session is still active when the next person accesses the PC.

**Purging Data and Files**

Another significant problem with classroom PCs is the fact that users frequently fail to purge the historical information relative to their session, including files and browsing history. This can be particularly troublesome when users use a room PC to access content from a file sharing application and then leave the session open. The easiest way to reduce the risk of users accessing confidential files is to use removable media such as USB drives, and to enforce a rule whereby users use a browser mode that does not retain browsing history.

## CONFIGURING AND CONTROLLING AV ASSETS


**Maintaining performance standards**

Like all other infrastructure assets, AV equipment needs to be optimally configured to successfully and reliably perform the complex functions required of it. IT departments need to safeguard that infrastructure from the unauthorized, untrained "helpful" user who wants to just log in quickly and customize a particular setting to their own liking. Campuses can handle this by instituting rigorous standards and authorization rules

relative to the operation and maintenance of their AV equipment, just like they do for their IT equipment.

**Eliminating meeting room disruptions**

Because equipment can be controlled over the network, Campuses need to limit access to prevent the disruptive joker who wants to anonymously log in and take control of cameras and lights. Many Campuses focus on establishing security safeguards against external threats while neglecting the attacks that can originate from inside the organization.

**Securing wireless technology**

In 2016, 90% of students will bring smartphones onto campus draining Wireless access. To respond to this demand, Campuses need to ensure that any wireless technology in use supports the latest security protocols to eliminate any unauthorized control of room technology. Wireless certifications such as CCXv4 should strongly be considered in sensitive wireless environments. Of course, wireless is never foolproof, so it's sometimes better to rely on a cabled solution when security is of utmost importance.


**Securing the AV controller / switcher**

The controller is typically a network-visible device that has a unique IP address. IT organizations understand how to protect these types of assets from intrusion, and most of them have built-in security capabilities to minimize risk of viruses.

That said, many controllers utilize "general purpose" operating systems like Microsoft Windows or UNIX that are significantly more susceptible to viruses than controllers that rely on proprietary or Linux-based operating systems. AMX controllers, for example, use a customized version of the VxWorks OS that is highly impervious to viral intrusions. Furthermore, it would be nearly impossible for a virus of any kind to propagate to an AMX system, since under normal operation an AMX controller does not dynamically load and execute code from the internet.

## SOLVING ISSUES WITH COMMUNICATION PRIVACY

Lectures and classes leverage a mix of public and propietary informationand it is imperative that such information remain private, both within and outside of the campus firewall.

We all know that Campuses are relying on IP-based communications (Video - h.323 and Voice - SIP) to carry conversations or information over networks. As is the case with any data that traverses a network, vulnerabilities can be exposed when the network is improperly managed. The hacker community has many data packet sniffing tools at their disposal that are capable of capturing and reconstructing those packets to allow them to "hear" all of the dialogue and information flow during a meeting.

As mentioned before, a common example of this phenomenon occurs through use of VTC systems. Widespread use of videoconferencing has positively impacted collaboration between users while significantly reducing travel costs for Campuses worldwide. At the same time, many Campuses have ignored the fact that deploying these systems with their default settings can leave an organization open to threats.

### Snapshot: Ways to avoid vulnerabilities in VTC systems

| |
|---|
| Change all default passwords and configurations |
| Enable / change encryption for VTC sessions |
| Disable broadcast streaming and the far-end camera control feature |
| Regularly update firmware and security patches |
| Disable the auto-answering feature |
| Separate VTC systems logically from the rest of the network using VLANs |
| If remote access is absolutely required, institute strict access controls (router access control lists, firewall rules) to limit privileged access to administrators only |

*Source: "Systems and Network Analysis Center Information Assurance Directorate: Video Teleconferencing," U.S. National Security Agency (www.nsa.gov/snac).*

## SOLVING ISSUES WITH INFORMATION PRIVACY

Along with the network access concerns noted above, a second security concern relates to how sensitive electronic information gets "cleansed" from that room so that users in an adjacent room user do not inadvertently have access to it.

In addition to protecting and purging sensitive data in documents and room PCs as discussed previously, there are also concerns about protecting sensitive activity data. For example, audio and video conference calls are often made between parties where the remote site being contacted should remain unknown to subsequent users of the meeting space. Many conference technologies keep call history for easy recall of previous sessions. Activity autonomy demands that the AV equipment can erase these transactional records and similar records in VTC and other systems.

## RECOGNIZING THE INTERNAL THREAT

IT organizations today have a plethora of tools to secure their networks from external threats. Unfortunately, sometimes a significant threat can originate from within a campus, either in the form of a disgruntled user or an user who innocently leaves a system open and vulnerable. This is definitely true in the case of classroom AV equipment, where users tend to leave systems running after they complete their meeting.

We hate to admit it, but sometimes Campuses find themselves dealing with unethical users who use the network for purposes of information theft or sabotage. This can be one of the most challenging issues an IT organization may face, since a disgruntled user has the advantage of working from within a campus firewall. This can be managed by configuring AV equipment so that users do not have access to administrative functions.

## CONCLUSION

IT organizations today are adept at securing their networks from threats. Unfortunately, sometimes the threats with AV equipment result from the fact that assets are not physically secure or centrally monitored. Other AV-specific threats are due to the fact that AV assets like controllers and touch panels are frequently left alone in a vacant room, providing an easy target for thieves or hackers.

Despite these threats, there are some clear, commonsense measures you can take to ensure that your AV system operates at the same level of security as your IT network:

**Conclusion: Some Ways to Secure Your AV Installation**

1. Consider a long-term strategy to replace room PCs with a device specifically designed for classroom collaboration such as AMX's ENZO Cloud Presentation System.
2. Monitor your AV assets in real time using software like AMX's Resource Management Suite (RMS)
3. Implement the same security measures for AV as you do for IT (VLANs, ICSP, passwords, firewalls, etc).
4. Physically secure touch panels using table and wall mount kits
5. Physically secure AV controllers in locked cabinets
6. Use dedicated touch panels rather than tablets or other mobile devices as the room's User Interface, as these are easier to secure
7. Consider a master controller that does not use a general purpose OS like Windows or UNIX – these are more susceptible to viruses and malware
8. Change system defaults, especially for VTC systems
9. If remote access is absolutely required, institute strict access controls (router access control lists, firewall rules) to limit privileged access to administrators only