Networked AV in Depth: Securing AV Devices

TYPE: ARTICLE, REPORT OR

WHITEPAPER TOPICS: NETWORKED AV

SYSTEMS DATE: DECEMBER 2014

By Tim Kridel, Special to InfoComm
International®
Videoconferences frequently include confidential information, so the last thing clients want is someone eavesdropping (http://www.nbcnews.com /news/other/reportushackedunvideoconferencingspiedeuf8C10998104) . Meanwhile, digital signage done right can attract lots of eyeballs, which actually makes it attractive to hackers looking to embarrass a company by putting inappropriate content (http://www.themoscowtimes.com/news/article/hackerarrestedinbillboardpornstunt/399895.html) onscreen.

"Digital signage content is increasingly Webbased; the display is simply pointed toward a URL and shows the HTML5 content," says Michael O'Halloran, Smart Signage product manager in Samsung's enterprise business division. "While it may seem obvious, it's crucial to secure the display at the endpoint to ensure a hacker does not simply point the display at another, inappropriate URL."

People don't necessarily think of AV and hackers in the same sentence, but with more AV systems riding IP networks, securing AV devices — both physically and digitally — is critical.

Some lowtech hacks work because certain AV systems themselves are low tech. For example, bigbox retailers often use retail TVs to double as digital signage. That strategy backfired at a Fort Smith, Ark., Walmart when two men slipped a pornographic movie into the DVD player feeding the TVs. Not exactly networked AV (/cps/rde/xchg/infocomm/hs.xsl/39780.htm), but AV professionals point out that it would be a mistake to assume prograde signage networks can't also be exploited—and via sophisticated methods.

Cabinets and locks are as lowtech as security can get, but that doesn't mean they're ineffective. They're also just one layer in what needs to be a multilayered approach. And identifying what AV devices might be vulnerable is the first step.

"Oftentimes the network is 100 percent locked down, but the control system sits right on the table or credenza for anyone to reboot, reset, disconnect, etc.," says Toine Leerentveld, Crestron product line manager for control systems. "For a truly secure deployment, make sure your equipment is locked up and that only authorized personnel can get to it. With Ethernet control for most or all devices, it has become a reality to have the control system sit in an IT closet that is secured through keycard access."

Of course, not all AV gear can be locked away. For example, many enterprises now use iPads and Android tablets to run apps for control and videoconferencing. In those situations, the security focus should be on how those devices and apps are authenticated and whether their data traffic ought to be encrypted.

"We treat the control system app communication the same way we treat the control system touchpanel communication," Leerentveld says. "If you have authentication turned on, the apps use authentication. The level of security between both is the same."

IT Skills and Savvy Are Key

Control, digital signage and videoconferencing are a few examples of how AV traffic often piggybacks on a client's existing IT network. Such a design avoids the expense of building and maintaining a separate, AVonly network, but it also introduces the possibility that certain AV devices will create a back door into corporate servers and other IT systems.

To minimize such a security risk, AV professionals should consider partitioning the IT network so the AV traffic runs on a virtual local area network (VLAN). It also helps to place AV systems behind a firewall.

"Use access control lists, whitelists, blacklists, etc. in the firewall to limit access to intended parties only," says Allan Alford, director of Polycom's solutions security office. "On your videoconferencing systems, turn off unused management protocols and features in the systems themselves.

"Take advantage of the password features for both administrative and user roles," Allford continues. "Turn off application programming interfaces and Webbased management if not needed, and use complex passwords to protect them if they are. Change passwords regularly."

And don’t overlook a decidedly ITbased indicator of potentially illicit activity: system logs. Such logs should be inspected on a regular basis.

“This cannot be emphasized enough,” Alford says. “An administrator cannot be everywhere at once, and it is often after the fact that malicious actions are caught — but only if he or she monitors logs routinely. Good logs usually include sufficient information to close whatever hole was being exploited: Which user account was used? What is the IP address of the bad guy? Was something on the network left unprotected?”

When it comes to securing AV control systems, Leerentveld recommends focusing on:

Snooping: Hackers can tap into network traffic and gather important information. To prevent this, traffic between devices should be encrypted.

Management access: Control systems typically have an Ethernet management console that allows the user to upload programs, change configurations, etc. This management access (console, or webbased) is often wide open to anyone on the network, so adding a layer of authentication, requiring a user to log in before getting management access, is important. Integration with enterprise, Active Directory access control is ideal. This way, when the IT department removes a user, their user’s account is also automatically removed from the control system.

Network access: Many companies don’t take adequate steps to prevent unauthorized devices from accessing the network. One way to control this is to implement MAC filtering, by which network switches check a master list of MAC (media access control) addresses before granting access. But because such addresses can be spoofed, a better option may be to implement 802.1 x, which is a certificatebased authentication protocol for ensuring devices can’t be impersonated.

Crossnetwork access: If control systems and enterprise computers live on the same network, a control system could theoretically gain access to computer data. One best practice would be to implement multiple VLANs with specific routing rules, allowing only the necessary ports to open between the two networks.

Device access: Another way someone can attack a control system is by impersonating a UI device. It’s important to ensure that such devices are required to authenticate themselves to the control system. This way, the hacker would need to know a username and password, or be a member of the right Active Directory group to gain access.

Securing the Ecosystem

Sometimes, AV systems integrate with nonAV systems. And if either is vulnerable, they both could be.

“If your digital signage network interfaces with enterprise data, such as a pointofsale system, consider creating a mirror [server] so that you narrow the gateway through which the signage network interfaces with confidential data,” says Samsung’s O’Halloran.

Admittedly, the ability to implement such security measures depends, in part, on whether the client’s IT department will allow an integrator to do so. As with all things AV/IT, it’s important to coordinate with the IT department.

Moreover, AV integrators should make sure their own houses are in secure order. For example, some offer content creation and management as a managed service to digital signage customers. Unless the signage is on its own network, a hack into the integrator could offer a back door into the client’s IT systems. The Target credit card breach a year ago illustrates why that scenario isn’t as far-fetched as it might sound. Those hackers got in through an HVAC contractor that had a data connection to Target. The moral of the story: Make sure you practice the security best practices you preach.

Make Security Visible and Multilayered

Is an AV system secure? Sometimes users can tell just by looking.

“Spying requires secrecy, and secrecy can only happen if call participants are not alerted to the presence of the malicious party,” Alford says. “Deploy endpoints and infrastructure products that provide various means to alert participants to possible surveillance: LEDs on cameras and microphones, visual and auditory alerts when a call is joined, etc. Not all videoconferencing products support these features.”

Encrypting traffic is also wise, as is educating clients to look for an encryption indicator before launching into sensitive discussions. “Polycom systems all support call encryption, and the legitimate conference attendees will see an icon that indicates that the call is successfully encrypted,” Alford says.

For videoconferences and other AV traffic, certain physical security can provide another layer of protection, such as by running copper cables through conduit. Some government AV applications require fiber because copper cables can radiate enough signals to enable eavesdropping. Putting copper cables in conduit can minimize that risk. But even fiber is vulnerable to taps. If that’s a concern, consider periodically sweeping the network with a fiberoptic power meter to identify reflections. If they’re in places they shouldn’t be, it could indicate taps.

Overkill? Not necessarily. The more layers of security — physical or not – that hackers have to go through, the more likely they’ll be caught or give up. In the IT world, this strategy is known as “defense in depth,” and it applies to AV, too.

“If the intruder gets past the firewall, now he has to get past the call encryption or the passwordprotected accounts,” Alford says. “Build an environment where the next innermost ring is there to foil them. No defensive scenario can ever be considered perfect, but the goal is to implement as much as possible, and to supplement all technical settings with consistent and regular security process.”

For all security strategies, it’s important to consider how they’ll affect end users. If they’re overly complex, some users may look for ways to circumvent them, which can create even bigger risks.

“That’s the ageold battle: to make something really secure it typically becomes really userunfriendly,” Leerentveld says. “What we’ve done is put the security all in the dealer setup, so the end user walking into the room has no concept of what’s happened behind the scenes to make that a secure implementation. It should add no inconvenience to the user.”