Inavate

EUROPE
MIDDLE EAST
& AFRICA



Topics: Audio (https://www.inavateonthenet.net/topics/Audio)
Projection (https://www.inavateonthenet.net/topics/Projection)
Smart-workspaces (https://www.inavateonthenet.net/topics/Smart-workspaces)
Software (https://www.inavateonthenet.net/topics/Software)



(https://gude-systems.com/en/products/expert-power-control-8291-2/)

Shoring up security in enterprise AV

FEATURES

27/07/2017

Kieran Walsh, senior technical solutions manager at Audinate outlines the top vulnerabilities in today's enterprise AV systems.



(https://www.shure.com/en-US/products/mixers/intellimix-foundation-system?variant=IMXF5&utm_source=inavate&utm_medium=display&utm_campaign=us-en-shu-oct25-awar-prosp&sfid=imxf5)

The top vulnerabilities in an AV system are very similar in a lot of ways to any other system (IT or otherwise). A general concept of security is "Access, Authentication and Auditing."

Preventing physical access is stage one in any arena (banks are good at physical security). The number of IT and AV systems that don't employ the most basic layer 1 security (if a wall port isn't used - unplug it at the patchbay), lock switches away from public areas, etc is surprising.

Working up the stack - the next stop is Authentication - even if a network port is terminated at a switch port – what's to stop me

plugging something else in? Well... actually quite a lot! Most enterprise switches come with an implementation of 802.1x - and this can be used to control whether the switch port allows you to electrically connect to the network. The number of IT networks that implement this (often comes as a feature of the switch hardware) is incredibly low, and less so in AV

Connecting via VPN with strong authentication and individual (revocable) certificates is one of a number of ways to keep the "outside out" of your network (as long as it hasn't been physically compromised of course)

The cautions and observations thus far all compliment the new features that have been introduced with Dante Domain Manager. Dante Domain Manager can encrypt connection management, network monitoring and control using a customers own standard security certificates. Without login credentials, devices enrolled in a domain are invisible to anyone that is not a securely authenticated authorized user, whilst the ability to physically move an enrolled device anywhere within the network (including in other IP subnets) is seamlessly maintained in the Plug n Play way that Dante users have become used to. A device cannot subscribe to audio from another device in a Dante network without being a member of the same domain - in practice this would require an authorized and authenticated user to add the device.

Read about potential security concerns for AV in Tim Kridel's article *'Security holes and how to avoid a fall'.*



(https://data.imlgroup.uk/iseshowtv/)



(https://www.genelec.com/ral?utm_source=inavate&utPrem_medium=banner&utm_campaign=ral_c