AVI SPL®

THE STATE OF VIDEO CONFERENCING SECURITY

IDENTIFY WEAK POINTS AND ELIMINATE THE RISK

INTRODUCTION: THE THREAT IS REAL

Video conferencing equipment, found in almost every boardroom around the world, may be opening up companies and government entities to serious security breaches.

To prove this point, HD Moore, chief security officer at Rapid7, a Boston-based company that looks at security holes in computer systems, recently scanned the Internet and discovered, in less than two hours, over 5000 companies, including law firms, universities, pharmaceutical companies, oil refineries, and medical centers,[1] whose video conference systems were wide-open and could be easily hacked.

How did he do it? By writing a code that scanned the Internet for video conference systems outside the firewall that are configured to auto-answer calls—a common default feature that makes it easier to accept inbound calls.[2]

> In less than two hours, the chief security officer at Rapid7 discovered over 5000 companies, including law firms, universities, pharmaceutical companies, oil refineries, and medical centers, whose video conference systems were wide-open and could be easily hacked.[1]

Even more disturbing, however, may be the recent presentation at Black Hat Europe, by Moritz Jodeit, "Hacking Video Conferencing Systems." While Moore's research illustrated the need to securely configure video conferencing systems, Jodeit took it one step further. He demonstrated how to get root access into a popular video conference device and then remotely compromise the device in its most secure configuration.[3]

In both instances, once the devices were hacked, Moore and Jodeit had the ability to control the device's peripherals like recording audio using the microphone[4] and zooming the camera in and out, with the ability to see small objects up to 50 yards away.[5] These demonstrations proved that there is a myriad of information that can be gleaned—from confidential discussions to the ability to zoom in and read top-secret documents—once a video conference system is compromised.

CORPORATE ENTITIES ARE DESIRABLE TARGETS

Unauthorized viewing, content snooping, session recording, and retransmission are potentially grave threats to organizations. The stakes are especially high with companies that frequently use video conferencing to get immediate operational feedback for real-time decision making.

To help organizations combat this threat, this paper takes an in-depth look at some of the most critical video conference equipment security risks and offers actionable suggestions to help mitigate them.

WHAT INCREASING VIDEO CONFERENCE USE MEANS

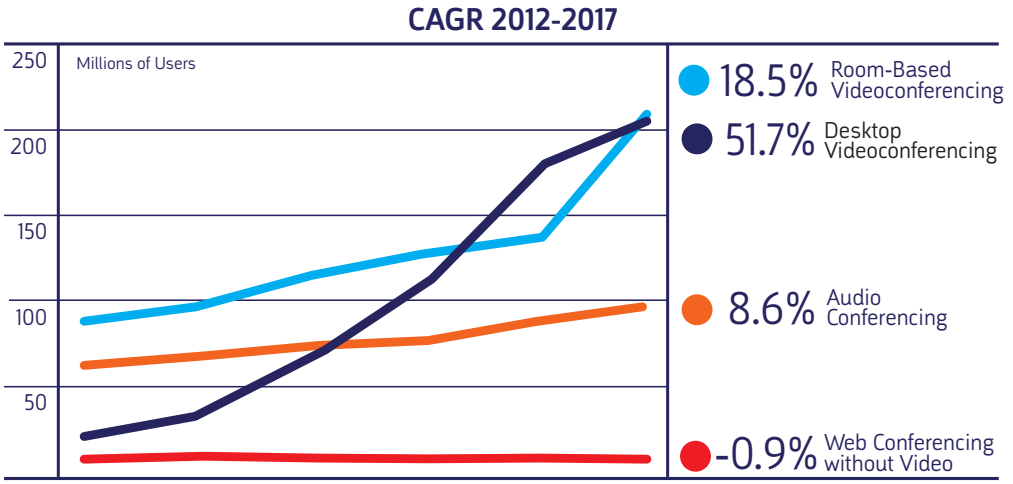
WE'RE SECURE. HOW CAN OTHERS PUT US AT RISK?

THE WORKPLACE IS GROWING MORE GEOGRAPHICALLY DISPERSED

Nowadays videoconferencing systems are widely deployed in companies. Whether it's working with other partners, vendors and contractors, or remote employees, more and more companies are adopting video conferencing as a way to stay connected on a day-to-day basis. Organizations also make heavy use of video conferencing in more high-level situations, such as conducting meetings between executives or negotiating with potential clients.[6]

The increased acceptance of telecommuting and flexible working schedules will increase digital communication. In addition to reducing the cost and personal burden of travel, video conferencing allows immediate interaction. And unlike an audio-only conference call, a live video meeting promotes relationship building by bringing in non-verbal cues that enhance communication and understanding.

As prices have come down and availability of video-capable devices has gone up, video conference calls may soon be as universal as telephone calls. The number of desktop video conferencing users is expected to grow eightfold, from about 27 million in 2012 to about 213 million by 2017. And, by 2015, there will be more desktop video conferencing users than audio conferencing users.[7]



Video conferencing growth in users compared to audio. Source: Cisco VNI Service Adoption Forecast, 2012-2017

AS POPULARITY AND USAGE GROWS, SO DO SECURITY RISKS

As video conferencing becomes mainstream, the risk of an impactful breach increases. Unfortunately, verified reports are rare since video conference breaches often go unnoticed.

The obvious risk with video conferencing is an uninvited guest joining the video conference and gaining access to the conversations and screen shares. However, there are additional risks with unauthorized

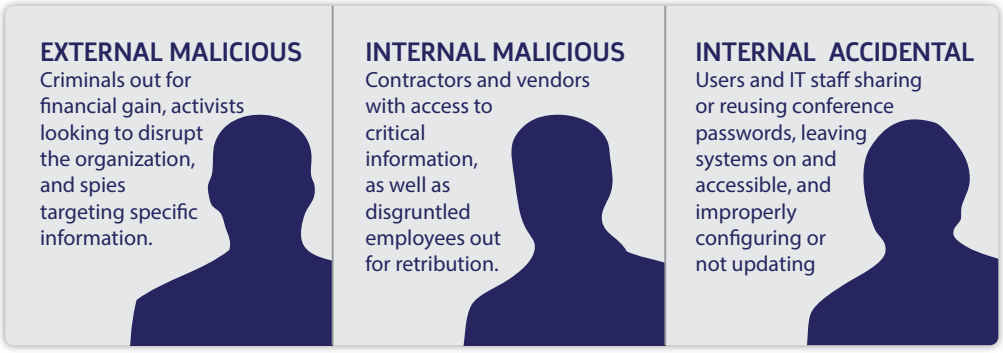
access. These risks include audio-only or content-only snooping, session recording, and retransmitting and re-streaming to unauthorized participants.

Another often overlooked risk is data leaks. Hackers can steal the IP addresses of other conference rooms and lists of frequently called phone numbers right off the video conferencing module.[8] In fact, in his boardroom snooping session, HD Moore found that he could leap from one open system into its address book and dial into the conference rooms of other companies, even those companies, such as Goldman Sachs, that put their system behind the firewall.[9]

> "The companies that really have to worry about breaches—the Department of Defense, banks—put their systems behind the firewall, but that doesn't mean there aren't exceptions. If you talk to outside companies, you need to decide if you want to be accessible or totally secure."
>
> – Ira M. Weinstein, senior analyst at Wainhouse Research[10]

WHO ARE THEY?

The simple answer is that the intruders can be anybody. They can be the Chinese hackers who recently attempted to hack into the computers of an audio visual conference equipment maker in a likely attempt to tap into boardroom and other high-level remote meetings[11], or they can be the forgetful or disorganized employee down the hall. Security breaches happen as a result of people in different categories—those external and internal to your organization—and they create intentional and accidental results.



WE ALWAYS USE THE LATEST SECURITY PROTOCOLS

AS LONG AS THE DATA IS ENCRYPTED, WON'T WE BE FINE?

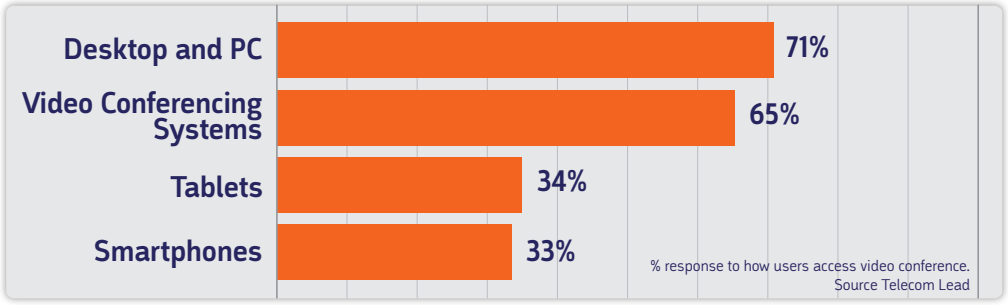
IT'S ONLY AS GOOD AS THE WEAKEST LINK

As a general rule, all standards-based video conferencing systems use 128-bit AES encryption. This secures the audio and video data being sent back and forth between users. However, even though the video conferencing system is very secure, there may be weaknesses in the connection points, such as hand offs to the network or the specific user devices.

Intruders don't need to break the video encryption code when they can just hack into these connection points before or after the data has been encrypted. The recent and well-publicized credit card breach at Target was done through the stolen credentials of a heating and refrigeration contractor. Once inside, they were able to gain access to customers' personal information.[12]

POTENTIAL WEAK POINTS WHERE VIDEO CONFERENCING TAKES PLACE

More and more agencies and organizations are allowing users to be productive wherever they are: their desk, another company, their home, or even a client or vendor site. They are embracing the BYOD (bring your own device) strategy in order to increase productivity and decrease costs.



Infonetics, a communications research firm, surveyed 115 organizations in the U.S. and Canada and found nearly all of them reported (or had users report) that malicious apps had been downloaded onto a device. Sixty-four percent of the respondents said that users' devices containing sensitive or proprietary data had been lost or stolen.[13] These are security issues that leave open the possibility of unintended access. But endpoints are only one potential area of weakness in video conferencing security. Many popular video conferencing services, like WebEx and Google Hangouts, send the data through a router or middleman server where it is decrypted and stored before being delivered to the user's device. With so much traffic, they are also desirable targets.

HOW CAN SOMETHING SO GOOD BE SO BAD?

Routers and firewalls are tremendously valuable in securing network traffic, but they can make managing video communications extremely difficult. Video conferencing performance can be degraded as each packet is inspected as it traverses the firewall. These ordinarily helpful technologies can cause trouble by hiding the network addresses of internal devices and even block all incoming calls and session requests.

In order to get around these video-related firewall issues, network administrators often disable the firewall or place the video system in the network DMZ. Alternatively, a video-specific firewall solution can be deployed. But an architecture using custom solutions for every video and audio connection will end up creating a number of communication silos.

IT CAN HAPPEN TO THE BEST OF US

Even the United Nations architecture may be vulnerable. The NSA was accused of tapping into the UN's video conference calls in the summer of 2012.[14] The documents leaked by NSA contractor Edward Snowden showed that the NSA gained access to the internal video conferencing system of the UN by bypassing encryption. One document brags about the access while also saying the number of communications decoded rose from 12 to 458 in just three weeks.[15]

WE HAVE COMPREHENSIVE NETWORK AND INFRASTRUCTURE SECURITY

OUR ARCHITECTURE IS FIRST CLASS. WHAT COULD GO WRONG?

LOOK FOR USER-INTRODUCED WEAKNESSES

Even the best video conferencing system deployed on well-designed architecture can still experience security breaches. The final weak link in the security chain is people. Although people generally do their best, they make mistakes, and they are only as good as what they know.

> Demonstrations have proved that there is a myriad of information that can be gleaned—from confidential discussions to the ability to zoom in and read top-secret documents—once a video conference system is compromised.

DEFAULT CONFIGURATION ISSUES

It's easy to accept the configuration defaults that come with any new system. After all, the vendor knows best, right? Most of the time, when implementing any new system, like video conferencing, users and administrators are in learning mode and are fearful of changing any default settings. It's not until they are more familiar and comfortable that they begin to customize the system.

Unfortunately, as HD Moore pointed out, some default settings can dramatically increase vulnerability, such as the default setting that automatically accepts inbound calls. That way, users do not have to press an "accept" button every time someone dials in. Today, many video conferencing systems come with that setting turned on by default. This means anyone can join the conference, often undetected.

SOCIAL ENGINEERING, THE HUMAN FACTOR

Social engineering is a term defined as a means of tricking other people into breaking normal security procedures. This may come in the form of an email attachment containing malware, phishing scams to induce users to provide sensitive information like passwords, and what is called "scareware," which frightens people into running software that is potentially dangerous.

For example, a hacker could send a phishing email asking to verify video system IP addresses or user account information. An employee could reply to this email, possibly providing access to an outsider. Access to recorded video meetings should be subject to the same stringent security checks as those to restricted physical documents and files.

Social engineers also leverage the fact that most people are not aware of the value of information and are not careful in protecting it, including recorded video sessions.

EVEN A SECURE ARCHITECTURE MIGHT NOT BE ENOUGH

In early 2012, the Internet hacker group Anonymous released a 16-minute recording of an audio call between Scotland Yard and the FBI discussing the activities of Anonymous. They also released an email that included the conference dial-in number and passcode.[16]

A 19-year old Irish student, associated with Anonymous, joined and recorded the call after hacking into an Irish police officer's Gmail account. This is a case where a series of human errors, and not the technology itself, caused the breach.[17]

RECOMMENDATIONS

EVEN THOUGH ATTACKS ARE GETTING MORE COMPLEX, MOST BREACHES CAN BE EASILY PREVENTED

ADDRESS THE EASY AND OBVIOUS

Agencies can increase the security of their video conferencing systems tremendously for little to no cost. The following are recommendations based on best practices:

- Require users to have complex passwords for the system and require them to be changed often.
- Require every participant to have a PIN when entering a video conferencing session.
- Train users to look for signs of hacked video conferencing equipment, such as equipment lights or moving cameras before a call is underway.
- Continuously conduct architecture reviews to ensure all connected components support and employ current security measures.
- Use a session border controller with SIP to secure IP-connected video equipment in order to restrict only authorized traffic.
- Learn and control the auto-answer feature. When possible, set to OFF so that no uninvited guests can participate without being announced.
- After a video conferencing call is connected, put the system on mute. That way, an intruder can't hear or see the conference until someone inside un-mutes the call.
- Change the default encryption settings from 'On (If Available)' to 'On (Required)' to require encryption for every call.
- Disable the remote camera control so that only the moderator can control the camera.
- Always close the camera shutter when the system is not in use.

REDUCE RISK, TAKE MORE CONTROL

Creating and enforcing policies and procedures can bring a company closer to being more secure, but there are additional solutions available that make this process easier and offer extra protection for video conferencing systems.

Sometimes, absolute privacy assurance is needed in a conference room that offers video conferencing. AVI-SPL's Block ME™ offers a simple way to prevent unauthorized video calls from launching in meeting rooms. Block ME puts controls in the hands of users who can press a button to prevent calls from being initiated or received. When enabled, Block ME prevents video-specific traffic to and from the network.

Many companies find they need greater control over the administration of a video conferencing system, but do not have the staff to provide it. AVI-SPL's VNOC Symphony® is a platform that automates the complex, backend processes needed to schedule, monitor, and manage video conferencing and AV resources. Symphony works with over 3,000 AV devices from leading manufacturers. The integrated Business Process Automation Module uses customized rules and policies determined by both the customer and AVI-SPL's staff to govern VNOC Symphony.

Symphony helps users and administrators greatly reduce user-induced security risks. For example, not all users know how to disconnect or whether the system did in fact hang up. Symphony assures that the call is disconnected without the user needing to do anything.

AVI-SPL offers a complete video conferencing architecture review to help identify security gaps and weaknesses in the network as it relates to the video conferencing solution. Our team of experts are trained in the latest security methods and technologies, and are knowledgeable in all of the latest security threats related to video conferencing.

Conclusion

Documented attacks on video conferencing systems aren't common, but that doesn't mean they aren't out there. Due to their nature, most video conferencing breaches go undetected. But government agencies should be prepared. The risks will rise as more agencies use video conferencing for meetings with remote workers, other agencies, customers, and suppliers.

Every agency is different and must walk the fine line between functionality and increased security. Locking access down to the internal network makes the system very secure but reduces the benefit of easily connecting to users outside the network. However, allowing access outside the network introduces both security and privacy risks. Fortunately, with AVI-SPL, there is a way to mitigate many of the security risks while still offering the functionality users require.

About AVI-SPL

AVI-SPL has a team of experts with the experience needed to meet the most technically advanced needs of our clients. We can help you design, build, and support the systems and environments that enable your video communication and collaboration. Our engineers are certified to ensure they have the skills and knowledge necessary to manage projects of all scopes.

AVI-SPL works with Cisco to provide solutions for different markets, including healthcare, education, hospitality, and many more. From integration and fabrication through installation, documentation, training, and support, the team at AVI-SPL is equipped to be your partner every step of the way.

We're ready to help you better understand how video collaboration can fit into your organization. To learn more about video collaboration solutions for midmarket companies, contact us at (866) 559-8197 or visit www.avispl.com.

About Cisco

Cisco is a worldwide manufacturer of video collaboration and video-sharing solutions. Cisco's networkcentric platform is changing the nature of work and the way we live. AVI-SPL works with Cisco to provide solutions for different markets, including healthcare (Moffitt Cancer Center), education (Rialto Unified School District), hospitality (Fleming's Steakhouse), and many more. Learn more about Cisco on avispl.com.

References:

[1] Perlroth, Nicole. “Cameras May Open Up the Board Room to Hackers.” New York Times. January 22, 2012.
[2] ibid.
[3] Storm, Darlene. “Black Hat Europe: Hacking to Spy and Remotely Control Video Conferencing Systems.” ComputerWorld. March, 2013. http://blogs.computerworld.com/cybercrime-and-hacking/21930/black-hat-europe-hacking-spy-remotely-control-video-conferencing-systems
[4] Ibid.
[5] Perlroth. “Cameras May Open.”
[6] Jodeit, Moritz. “Hacking Video Conferencing Systems.” Presented at BlackHat Europe. 2013. https://media.blackhat.com/eu-13/briefings/Jodeit/bh-eu-13-hacking-video-jodeit-wp.pdf
[7] Cisco. “Cisco VNI Service Adoption Forecase, 2012-2017.” http://www.cisco.com/c/en/us/solutions/collateral/service-provider/vni-service-adoption-forecast/Cisco_VNI_SA_Forecast_WP.html
[8] Sampson. Lisa.”Secure Video Conferencing: Auto-answer Can Be Risky.” http://searchunifiedcommunications.techtarget.com/feature/Secure-video-conferencing-Auto-answer-can-be-risky
[9] Perlroth. “Cameras May Open.”
[10] Perlroth. “Cameras May Open.”
[11] “Chinese hackers target remote conferencing gear: Dell researchers.” Reuters. July 31, 2013. http://www.reuters.com/article/2013/07/31/us-china-hacking-idUSBRE96U0YI20130731
[12] Bjorhus, Jennifer and Spencer, Jim. “Growing Computer Connections Between Vendors and Businesses Give Hackers Many Points of Entry.” Star Tribune. Feb. 11, 2014. http://www.startribune.com/business/244819221.html
[13] Wilson, Jeff. “ Enterprises rate mobile device security vendors, reveal BYOD concerns.” March 8, 2012. http://www.infonetics.com/pr/2012/Enterprise-Mobile-Security-Strategies-Survey-Highlights.asp
[14] Weinsteim, Ira M. and Davis, Andrew W. “Keeping Video Conferencing Security in Perspective.” Nojitter. Spet. 2, 2013. http://www.nojitter.com/post/240160666/keeping-video-conferencing-security-in-perspective-8230
[15] RT. “UN ‘aware of the reports’ of NSA hacking into diplomatic communications.” August 27, 2013. http://rt.com/news/un-communications-nsa-leak-scandal-026/
[16] Webtorials.”Videoconferencing Security.” http://www.webtorials.com/content/2012/10/videoconferencing-security.html
[17] Ibid.