DOCUMENTO TÉCNICO

Ciberseguridad con audio en red de Axis

Septiembre 2025

Resumen

En el mundo interconectado actual, proteger los sistemas de comunicación de audio es vital para proteger la información confidencial y mantener la eficiencia operativa. Los sistemas de audio en red afrontan numerosas amenazas, como el acceso no autorizado, las escuchas clandestinas, los ataques de denegación de servicio, el malware y las vulnerabilidades de software. Axis enfrenta estos riesgos con avanzadas soluciones de seguridad que se integran a la perfección con las infraestructuras existentes, ofreciendo fiabilidad, escalabilidad y una protección muy sólida.

Axis adopta un enfoque de seguridad desde el diseño, que incorpora cifrado, autentificación, actualizaciones de software seguras, control de acceso, refuerzo del sistema y registro de eventos. Protocolos seguros como SIPS, SRTP, HTTPS e IEEE 802.1AE permiten mantener una comunicación y transmisión de datos seguras.

El software de gestión de audio Axis ofrece un control de acceso basado en roles, integración segura y el registro completo de eventos, resultando perfecto tanto para implementaciones locales como en la nube.

Al aprovechar estas capas de seguridad, los sistemas de audio en red Axis ofrecen una protección integral contra las ciberamenazas.

Índice

1 Introducción 4
2 Comprender los riesgos 4
3 Ventajas del audio en red Axis 4
4 Características clave de la seguridad de los altavoces y el sistema 5
5 Seguridad en todo el sistema 5
5.1 Seguridad del dispositivo 5
5.2 Protocolos de seguridad 6
5.3 Seguridad en el software de gestión de audio 7
5.3.1 Soluciones locales 7
5.3.2 Solución en la nube 8

1 Introducción

Los sistemas de audio desempeñan un papel crucial para la comunicación, seguridad y eficiencia operativa en distintos sectores, como el comercio minorista, el transporte, la seguridad pública y la educación. Estos sistemas resultan igualmente atractivos para los ciberataques, por lo que es esencial adoptar medidas de seguridad fiables. Un sistema de audio comprometido puede tener consecuencias graves y de gran alcance.

Este documento técnico explora las principales capas de seguridad que emplean los altavoces y sistemas de audio Axis para abordar estos desafíos.

2 Comprender los riesgos

Dada la creciente implementación de soluciones de audio en red en todas las industrias, los riesgos potenciales asociados con los sistemas inseguros han aumentado significativamente.

Los sistemas de audio en red pueden estar expuestos a distintos tipos de amenazas.

- **Acceso no autorizado.** Agentes malintencionados pueden acceder remotamente a dispositivos de audio sin protección, pudiendo llegar a tomar el control de los altavoces, emitir anuncios no autorizados o interrumpir las operaciones.
- **Escuchas ilegales e intercepción de datos.** En ocasiones, los sistemas de audio en red transmiten datos de voz confidenciales a través de redes cableadas o inalámbricas. Sin el cifrado, los atacantes podrían interceptar y grabar conversaciones, pudiendo derivar en violaciones de la privacidad, espionaje industrial o un uso indebido de información confidencial.
- **Ataques de denegación de servicio (DoS).** Los atacantes pueden llegar a saturar los altavoces o servidores de audio en red con un tráfico excesivo, conllevando la sobrecarga del sistema y la interrupción de los servicios. Este tipo de ataques podrían dejar inoperativos los sistemas de comunicación de emergencia en momentos críticos.
- **Ataques de malware y ransomware.** Al igual que la infraestructura informática tradicional, los dispositivos de audio en red pueden verse comprometidos por malware o ransomware. Los atacantes podrían bloquear dispositivos, exigir el pago de rescates o utilizar el sistema comprometido como punto de entrada para atacar la red en general.
- **Ataques de software y vulnerabilidades de la cadena de suministro.** Los sistemas operativos obsoletos con fallos de seguridad sin corregir pueden explotarse para hacerse con el control de los dispositivos de audio. Además, las prácticas inseguras en la cadena de suministro pueden introducir vulnerabilidades antes de la implementación, provocando que los sistemas resulten vulnerables desde el principio.

3 Ventajas del audio en red Axis

Axis ofrece soluciones de seguridad de sistemas y altavoces de última generación que se integran a la perfección en las infraestructuras existentes. Su arquitectura abierta proporciona compatibilidad con distintos sistemas y protocolos. Los sistemas Axis son flexibles y están diseñados para adaptarse a las necesidades de su organización, desde pequeñas implementaciones hasta redes empresariales. Axis ofrece sistemas de gestión de audio tanto locales como en la nube.

Axis aplica un enfoque de seguridad por diseño para el desarrollo de software.re. Nuestro marco de trabajo, el Modelo de desarrollo de seguridad de Axis (ASDM), define procesos y herramientas que garantizan la integración de la seguridad en todo el ciclo de vida del desarrollo de software y reducen el riesgo de vulnerabilidades. El ASDM recibe mejoras continuamente.

Uno de los muchos factores que contribuyen a su mejora es que realizamos evaluaciones periódicas de distintos estándares de seguridad y los adaptamos al ASDM. Nuestro software satisface los exigentes estándares del sector en materia de privacidad y seguridad de datos, incluido el RGPD (Reglamento General de Protección de Datos) de la UE.

4 Características clave de la seguridad de los altavoces y el sistema

Con el audio en red de Axis, la seguridad está integrada tanto en los dispositivos como en los sistemas de gestión.

Cifrado y autentificación

- El cifrado contribuye a una transmisión segura de datos de audio mediante TLS 1.2 y 1.3, impidiendo además que terceros no autorizados intercepten y accedan a la información.
- La autentificación garantiza que únicamente los dispositivos y usuarios autorizados puedan acceder a los dispositivos, así como a la solución general.

Actualizaciones seguras del software del dispositivo

- El inicio seguro (en la mayoría de los productos) y los parches firmados digitalmente garantizan que únicamente se instale software de dispositivos verificados. De esta forma se protegen los sistemas de códigos maliciosos.

Control de acceso

- AXIS Audio Manager Pro y AXIS Audio Manager Center utilizan control de acceso basado en roles (RBAC), que limita el acceso al sistema exclusivamente al personal autorizado.
- La gestión centralizada permite a los administradores de TI supervisar y controlar los permisos con gran eficacia.

Refuerzo del sistema

- La configuración predeterminada está optimizada para la seguridad desde el primer momento, lo que permite reducir las vulnerabilidades.
- Las opciones de configuración adicionales permiten la personalización según casos de uso específicos. La Guía de refuerzo de AXIS OS en *help.axis.com/axis-os-hardening-guide* ofrece asesoramiento técnico.

Registro y supervisión de eventos

- El registro completo proporciona visibilidad de las actividades del sistema. Esto puede resultar útil para la detección de amenazas en tiempo real y durante los análisis con captura forense.

5 Seguridad en todo el sistema

Con el audio de red de Axis, la seguridad está integrada en los dispositivos y sistemas de gestión. Los protocolos seguros confieren un alto nivel de seguridad en la comunicación entre dispositivos y software de gestión.

5.1 Seguridad del dispositivo

Todos los altavoces Axis funcionan con el AXIS OS, nuestro software diseñado específicamente para dispositivos Axis. Este ofrece valor a largo plazo, ciberseguridad e integración de primer nivel. Con el AXIS OS, todos nuestros altavoces incorporan sólidas funciones de seguridad del ecosistema Axis. Esto proporciona consistencia y fiabilidad a todos los dispositivos y ofrece protección integral para cada implementación. Las funciones de seguridad incluyen sistemas de archivos cifrados y la plataforma de ciberseguridad basada en hardware Axis Edge Vault (*axis.com/solutions/edge-vault*).

Axis Edge Vault protege la integridad de los dispositivos de Axis y habilita la ejecución de operaciones seguras en función de claves criptográficas. Permite verificar y aprovechar el IEEE 802.1AR-compliant Axis device ID para la integración segura del dispositivo en redes de confianza cero mediante IEEE 802.1X y HTTPS. Con Axis Edge Vault, puede iniciar el dispositivo de forma segura, integrarlo y tener la seguridad de que la información confidencial, como las claves criptográficas, queda protegida.

Con Axis Edge Vault, puede estar seguro de que el dispositivo Axis que ha recibido no ha sido manipulado ni se ha visto comprometido en la cadena de suministro física. Axis Edge Vault establece una cadena de confianza y

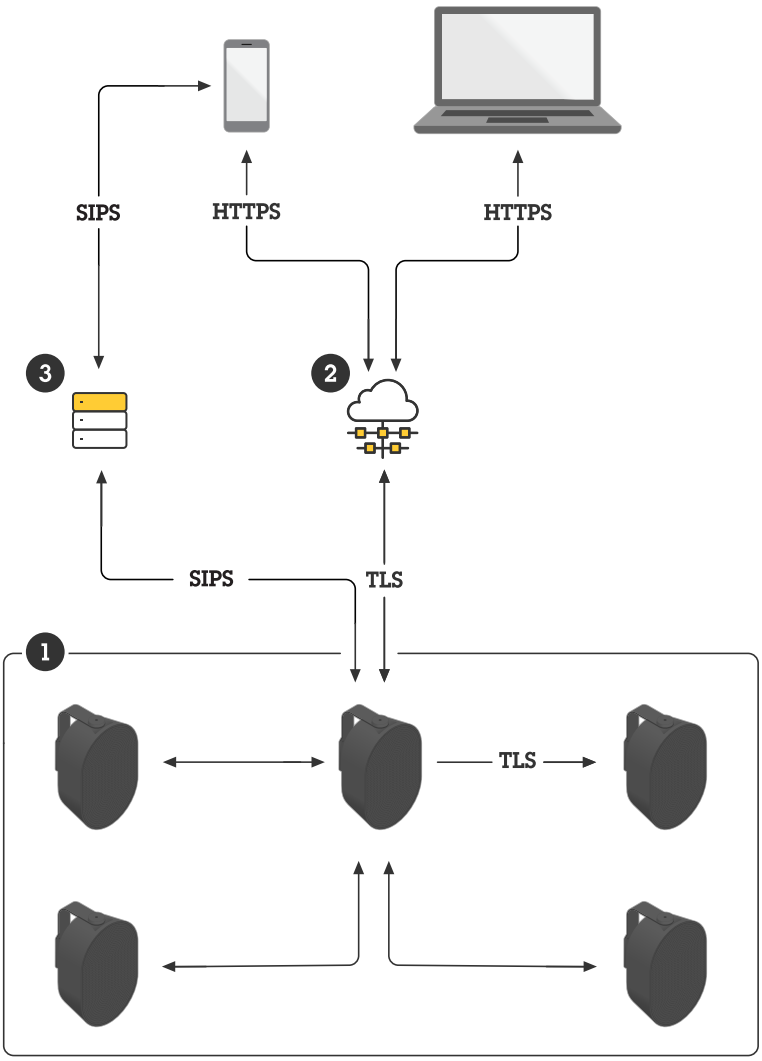
garantiza una cadena ininterrumpida de software validado criptográficamente. Por ejemplo, la función *signed OS* garantiza que el software del dispositivo es de Axis y que solo se pueden instalar actualizaciones firmadas por Axis.

5.2 Protocolos de seguridad

Los dispositivos y sistemas Axis utilizan protocolos abiertos para garantizar comunicaciones, transmisiones y flujos seguros.

- **SIPS** (SIP Secure): mejora el estándar SIP (protocolo de inicio de sesión) al incorporar TLS (capa de transporte seguro). Esto permite establecer una conexión segura entre una IP PBX y un teléfono VoIP. Una vez configurada la conexión segura, el SRTP (protocolo de transporte seguro en tiempo real) cifra los datos de voz en paquetes IP seguros para su transmisión por Internet. Esto se traduce en un cifrado de extremo a extremo desde el transmisor (sistema telefónico IP) hasta el receptor (altavoz).

  Mediante el uso de SIPS y SRTP, los sistemas Axis protegen tanto los datos de audio como la propia configuración de la conexión. Esto significa que el flujo de audio y los detalles de la conexión (como la identidad del emisor y el receptor) están completamente cifrados y que el canal de comunicación seguro punto a punto es sólido.
- **Controlador de multidifusión**: una función de controlador de multidifusión en los altavoces Axis permite la recepción segura de flujos de audio multidifusión enviados mediante SRTP. Esto garantiza que la comunicación grupal esté cifrada.
- **Transmit.cgi** y **receive.cgi**: estas API VAPIX representan un método seguro para enviar y recibir flujos de audio en comunicaciones cifradas punto a punto mediante HTTPS. La CGI (interfaz de puerta de enlace común) es un protocolo estándar que especifica la comunicación entre un servidor web y programas externos.
- **RTSPS** (Protocolo seguro de transmisión en tiempo real): un protocolo de control de red empleado para establecer y gestionar transmisiones multimedia en tiempo real entre un servidor y un cliente. Esto es compatible con la transmisión segura de audio, empleando el cifrado para evitar accesos no autorizados.
- **HTTPS**: todas las API están protegidas con HTTPS para asegurar la confidencialidad e integridad de todas las comunicaciones.
- **IEEE 802.1AE**: también conocido como MACsec (seguridad de control de acceso a medios), un protocolo de red que cifra la comunicación de red con AES-128, fundamentalmente en la capa 2. Al combinarse con HTTPS, RTSPS y SIPS, el tráfico de red se cifra doblemente y la seguridad de la red mejora de forma notable.



Un sistema de audio en red con comunicación segura gracias a varios protocolos abiertos.

1 *AXIS Audio Manager Edge: gestión de audio local integrada en altavoces Axis*
2 *AXIS Audio Manager Center: gestión de audio centralizada en la nube híbrida*
3 *PBX para socios*

5.3 Seguridad en el software de gestión de audio

5.3.1 Soluciones locales

Las soluciones locales de Axis están diseñadas para gestionar la zonificación, la priorización y la comunicación segura entre múltiples altavoces in situ.

AXIS Audio Manager Edge. Este software de gestión está integrado en todos los altavoces de audio en red de Axis. Convierte cada altavoz en un sistema de sonido completo e integral, sin necesidad de un servidor de gestión de software independiente. AXIS Audio Manager Edge está diseñado para gestionar proyectos de baja complejidad que constan de hasta 200 dispositivos en hasta 20 zonas.

- Compatible con el cifrado entre dispositivos. El método de cifrado predeterminado es TLS con certificados autofirmados, pero recomendamos instalar certificados de confianza en sus dispositivos y habilitar la autentificación TLS en la configuración del sistema del sitio. Esto proporciona protección contra ataques de intermediarios.
- Permite la integración segura de dispositivos al sitio local. La configuración inicial se realiza mediante HTTPS con las credenciales del dispositivo. Posteriormente, se utiliza MQTT (TLS-PSK) para la comunicación entre dispositivos y SRTP para enviar datos RTP cifrados, como transmisiones de audio, entre ellos.

- Proporciona acceso externo al sistema para casos de uso operativo mediante la API HTTPS.

AXIS Audio Manager Pro. Este software de gestión está pensado para proyectos más complejos y avanzados. Puede gestionar un gran número de zonas (más de 500) y miles de dispositivos (más de 5 000) en una única interfaz. AXIS Audio Manager Pro facilita la programación a largo plazo y la configuración avanzada de prioridades.

- Incluye el control de acceso basado en roles, que limita el acceso al sistema únicamente al personal autorizado, con compatibilidad con la integración de Active Directory.
- Permite la integración segura de dispositivos.
- Incluye un registro detallado de eventos y auditorías. Esto permite realizar un registro completo de la actividad del sistema, lo que puede ayudar a los administradores a realizar un seguimiento de los cambios, supervisar el comportamiento y resolver problemas.

5.3.2 Solución en la nube

AXIS Audio Manager Center es un servicio para la gestión y supervisión remotas de sistemas de varias instalaciones, que puede ampliase de varios emplazamientos a varios miles. Se utiliza junto con AXIS Audio Manager Edge en cada instalación local. Se trata de una solución práctica y estable de nube híbrida con componentes locales y de nube.

AXIS Audio Manager Center simplifica la gestión, ofrece un control centralizado y gestiona la integración segura de dispositivos. La carga de trabajo del usuario se reduce notablemente gracias a un inicio de sesión único para programar comunicados, música de fondo, publicidad y más para sitios o zonas seleccionados. Las principales funciones de seguridad incluyen:

- Control de acceso basado en roles (RBAC): limita el acceso al sistema únicamente al personal autorizado.
- Gestión centralizada de usuarios: admite usuarios/grupos de *My Axis* o Active Directory para una administración optimizada. No se necesitan usuarios locales.
- Integración segura: simplifica la incorporación segura de dispositivos con confianza desde la nube, mediante certificados únicos instalados en cada dispositivo.
- Simplifica las configuraciones E2E seguras: permite la configuración segura de SIPS, incluida la gestión de certificados.
- Supervisión de estado y notificaciones: ofrece supervisión centralizada del estado del sistema y alertas inmediatas ante posibles problemas.
- Comunicación segura: toda la comunicación entre la nube y los dispositivos se cifra mediante TLS, con autentificación bidireccional mutua que garantiza una seguridad fiable.
- Acceso remoto: permite el acceso remoto seguro al sitio local desde cualquier lugar.

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro mejorando la seguridad, la operatividad de las empresas y la inteligencia empresarial. Como líder del sector y empresa especializada en tecnología de redes, Axis ofrece videovigilancia, control de acceso, intercomunicadores y soluciones de audio. Su valor se multiplica gracias a las aplicaciones inteligentes de analítica y una formación de primer nivel.

Axis cuenta aproximadamente con 5.000 empleados especializados en más de 50 países y proporciona soluciones a sus clientes en colaboración con sus socios de tecnología e integración de sistemas. Axis fue fundada en 1984 y su sede central se encuentra en Lund (Suecia).aboutaxis_text2