白皮书

安讯士网络音频的网络安全

9月 2025

概述

在当今互联互通的世界中，保障音频通信系统的安全对于保护敏感信息和维持运营效率至关重要。网络化音频系统面临诸多威胁，包括未经授权的访问、窃听、拒绝服务攻击、恶意软件和软件漏洞利用。安讯士利用具备尖端技术的安全解决方案应对这些风险，这些方案能与现有基础设施无缝集成，提供可靠性、可扩展性和强大的保护。

安讯士采用安全设计理念，整合了加密、身份验证、安全软件更新、访问控制、系统加强及事件日志记录等措施。安全协议（如SIPS、SRTP、HTTPS和IEEE 802.1AE）启用安全的通信与数据传输。

安讯士音频管理软件提供基于角色的访问控制、安全接入和全面事件日志记录功能，同时支持内部部署与基于云端的部署。

利用这些安全层，安讯士网络音频系统为抵御网络威胁提供端到端保护。

目录

1 引言

音频系统在零售、交通运输、公共安全和教育等多个行业中，对沟通、安全保障及运营效率起着至关重要的作用。这些系统也是网络攻击的常见目标，因此必须采取强有力的安全措施。音频系统一旦遭到破坏，可能产生严重且深远的影响。

本白皮书探讨了安讯士扬声器和音频系统为应对这些挑战所采用的主要安全层。

2 理解风险

随着网络化音频解决方案在各个行业的日益普及，不安全系统带来的潜在风险也显著增加。

网络化音频系统可能面临多种类型的威胁。

- **未被授权的访问。** 未受保护的音频设备可能被恶意攻击者远程访问，从而控制扬声器、发布未经授权的公告或干扰操作。
- **窃听和数据拦截。** 网络化音频系统有时会通过有线或无线网络传输敏感语音数据。若数据未加密，攻击者可能截获并录制对话内容，导致隐私泄露、工业间谍活动或机密信息被滥用。
- **拒绝服务 (DoS) 攻击。** 攻击者可向联网扬声器或音频服务器发送海量流量，导致系统过载并中断服务。此类攻击可能在关键时刻导致紧急通信系统瘫痪。
- **恶意软件和勒索软件攻击。** 与传统IT基础设施一样，网络化音频设备也可能受到恶意软件或勒索软件的攻击。攻击者可能锁死设备、勒索赎金，或利用受感染的系统作为跳板攻击更大范围的网络。
- **软件漏洞利用和供应链漏洞。** 存在未修复安全漏洞的过时操作系统可能被利用，攻击者因此可获得对音频设备的控制。此外，不安全的供应链业务可能在部署前就引入了漏洞，导致系统从一开始就存在安全隐患。

3 安讯士网络音频的益处

安讯士提供采用最先进技术的扬声器和系统安全解决方案，可与现有基础设施无缝集成。开放式架构可兼容多种系统和协议。安讯士系统具有高度灵活性，可随着您组织的需求而扩展，从小规模部署到企业级网络均能满足。安讯士提供内部部署和基于云端的音频管理系统。

安讯士采用安全设计理念进行软件开发。我们的框架——安讯士安全开发模型 (ASDM)——定义了确保在整个软件开发生命周期中融入安全措施并降低漏洞风险的流程与工具。ASDM持续改进。

改进的方法之一是：定期评估各类安全相关标准，并将它们映射到ASDM框架。我们的软件符合数据隐私与安全方面的严格行业标准，包括欧盟的《通用数据保护条例》(GDPR)。

4 扬声器与系统安全的核心特性

安讯士网络音频设备将安全性内置于设备和管理系统中。

加密与认证

- 加密技术通过TLS 1.2和1.3协议实现音频数据的安全传输，防止未经授权的第三方截获和访问信息。
- 身份验证确保只有经过授权的设备和用户才能访问设备，同时也能访问整体解决方案。

安全设备的软件更新

- 安全启动（适用于多数产品）与数字签名补丁 确保仅安装 经验证的 设备软件。这可保护系统免受恶意代码的侵害。

门禁控制

- AXIS AudioManager Pro和AXIS AudioManager Center使用基于角色的访问控制 (RBAC)，仅允许授权人员访问系统。

- 集中管理使IT管理员能够有效监控和控制权限。

系统加强

- 开箱使用时，默认设置已针对安全性进行优化，从而降低了漏洞风险。
- 额外的配置选项支持根据具体使用场景进行定制化设置。AXIS OSHardening Guide（可在*help.axis.com/axis-os-hardening-guide*上查看）提供技术建议。

事件日志记录与监控

- 通过全面的日志记录，可看到系统活动。这有助于实时威胁检测和取证分析。

5 贯穿系统的安全性

安讯士网络音频设备将安全性内置于设备和管理系统中。安全协议启用了设备与管理软件之间的高通信安全性。

5.1 设备安全性

所有安讯士扬声器均采用AXIS OS系统，这是我们为安讯士设备量身打造的软件。它可实现长期价值、网络安全以及享誉世界的集成。借助AXIS OS，我们所有的扬声器都继承了安讯士生态系统的强大安全特性。这确保了所有设备的一致性和可靠性，并为每次部署提供端到端的保护。安全特性包括加密文件系统以及基于硬件的网络安全平台Axis EdgeVault (*axis.com/solutions/edge-vault*)。

AXIS Edge Vault保障安讯士设备的完整性，并启用基于加密密钥执行安全操作。 它通过 IEEE 802.1X 及HTTPS，验证并利用符合 IEEE 802.1AR 安讯士设备ID ，实现设备在零信任网络中的安全接入。借助 Axis Edge Vault，您可安全启动设备、集成设备，并确保加密密钥等敏感信息获得有效保护。

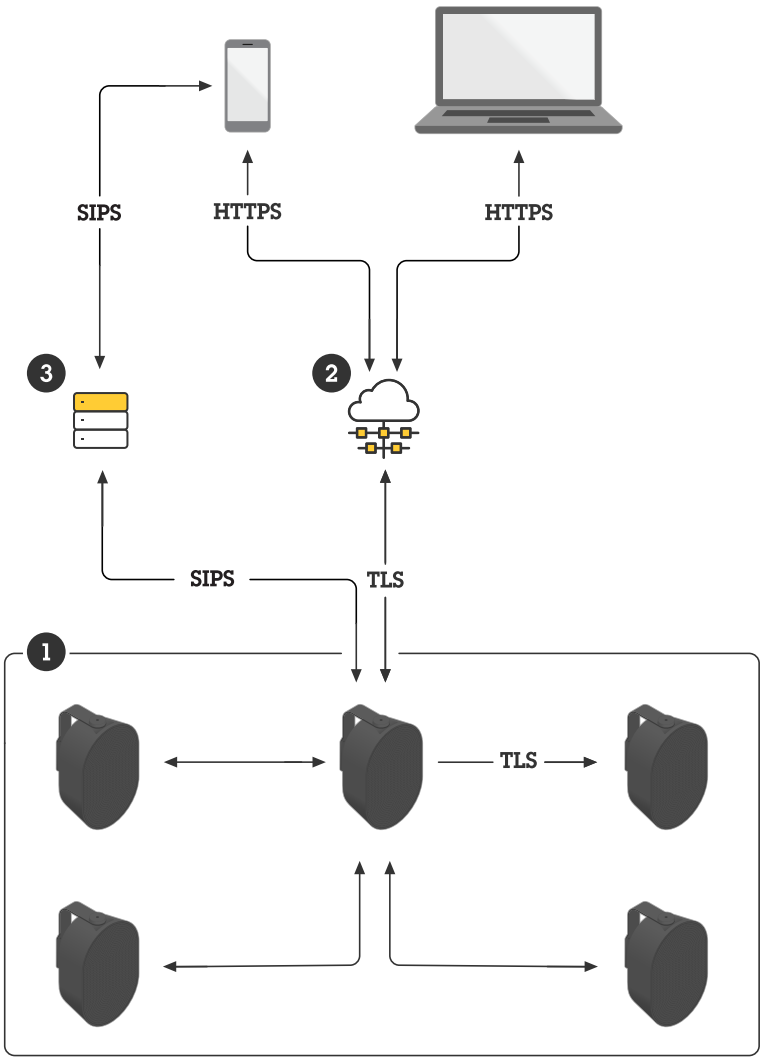
使用Axis Edge Vault，您可确保收到的安讯士设备在物理供应链中未被篡改或破坏。AXIS Edge Vault建立信任链，确保加密验证软件的完整性。例如， 功能*签名操作系统* 可确保 设备软件 来自 安讯士，且仅能安装由安讯士签名的更新。

5.2 安全协议

安讯士设备和系统采用开放协议，实现安全通信、传输和流媒体传输。

- **SIPS**（SIP安全）：通过整合TLS（传输层安全协议）来增强标准SIP（会话初始协议）。这在IP PBX和VoIP电话之间建立了一条安全连接。安全连接设置后，SRTP（安全实时传输协议）将语音数据加密为安全的IP数据包，通过互联网传输。这提供了从发送端（IP电话系统）到接收端（扬声器）的端到端加密。

  通过利用SIPS和SRTP协议，安讯士系统同时保障了音频数据传输与连接设置过程的安全性。这意味着，音频流和连接详细信息（例如，呼叫方身份和接受者）均获得全面加密，点对点安全通信通道具有强大的安全性。
- **多播控制器**：安讯士扬声器中的多播控制器功能可安全接收通过SRTP传输的多播音频流，确保群组通信经过加密处理。
- **Transmit.cgi**和**receive.cgi**： 这些VAPIX API通过HTTPS提供加密点对点通信的安全音频流收发方法。CGI（通用网关接口）是规范网页服务器与外部程序通信的标准协议。
- **RTSPS（实时流协议安全版）**： 一种网络控制协议，用于在服务器与客户端之间建立和管理实时媒体流。该功能支持安全的音频流传输，通过加密技术防止未经授权的访问。
- **HTTPS**：所有API均通过HTTPS加密，以确保所有通信的保密性和完整性。
- **IEEE 802.1AE**：又被称为MACsec（媒体访问控制安全），是一种基于AES-128加密的网络协议，能在第二层网络层实现基本网络通信加密。若与HTTPS、RTSPS和SIPS结合使用，网络流量将获得双重加密保护，显著提升网络安全性。



得益于多个开放协议，实现安全通信的网络音频系统。

1 *AXIS AudioManager Edge*：**集成在安讯士扬声器中的内部部署音频管理解决方案**
2 *AXIS AudioManager Center*：**混合云集中式音频管理解决方案**
3 合作伙伴*PBX*

5.3 音频管理软件中的安全性

5.3.1 内部部署解决方案

安讯士内部部署解决方案专为管理现场多扬声器的分区、优先级设置以及安全通信而设计。

AXIS Audio Manager Edge。安讯士网络音频扬声器都内置这种管理软件。安装管理软件后，每个扬声器都成为完整的多功能音响系统，不再需要单独的软件管理服务器。 AXIS Audio Manager Edge旨在管理复杂度较低的项目，最多支持20个区域内的200台设备。

- 支持设备间的加密通信。默认加密方式是使用自签名证书的TLS协议，但我们建议您在设备上安装受信任的证书，并在站点系统设置中启用TLS身份验证。这可防止中间人攻击。
- 启用设备安全接入本地站点。初始设置通过具备设备凭证的HTTPS完成。之后，在设备之间采用MQTT (TLS–PSK) 协议进行通讯， 使用SRTP协议在设备之间传输加密的RTP数据（例如，音频流）。
- 通过HTTPS API为可操作的使用场景提供外部系统访问权限。

AXIS Audio Manager Pro。该管理软件设计用于规模更大、更复杂的项目。它能在单一接口中管理大量区域 (500+) 和几千台设备 (5000+)。 AXIS Audio Manager Pro支持长期调度和高级优先级设置。

- 包含基于角色的访问控制，仅允许授权人员访问系统，并支持Active Directory集成。
- 启用设备的安全接入。
- 包含详细的事件和审计日志。这为系统活动提供了全面记录，可帮助管理员追踪变更、监控行为并排查问题。

5.3.2 基于云端的解决方案

AXIS Audio Manager Center是一项用于远程管理和监控多站点系统的服务，可从几个站点扩展到数千个站点。它在每个本地站点与 AXIS Audio Manager Edge 一起使用。同时使用基于云的和内部部署的组件，这是便利且稳定的混合型解决方案。

AXIS Audio Manager Center简化管理流程，提供集中控制功能，并支持设备的安全接入。用户工作负载极大减少，对所选场所或区域进行单点登录以安排通知、背景音乐、广告等。主要安全特性包括：

- 基于角色的访问控制 (RBAC)： 仅允许授权人员访问系统。
- 集中式用户管理： 支持*My Axis*或Active Directory用户/组，实现高效管理。无需本地用户。
- 安全接入： 通过在每台设备上安装独一无二的证书，借助云端信任机制简化设备的安全接入流程。
- 简化安全的E2E配置： 启用SIPS安全配置，包括证书处理。
- 健康监控和通知： 提供集中式系统健康监控，并在潜在问题出现时立即发出警报。
- 安全通信： 云端与设备间的所有通信均通过TLS加密传输，双向TLS（双向认证）机制确保了更强大的安全性。
- 远程访问： 实现从任何地点安全地远程访问本地站点。

关于安讯士 (Axis Communications)

安讯士通过打造各种解决方案，提高安全水平和企业效益，旨在创造一个高度智能、更加安全的世界。作为一家网络技术公司和行业领导者，安讯士致力于推出视频监控、访问控制、内部通信和音频系统解决方案。安讯士通过智能分析应用程序增强解决方案，并提供高质量培训支持。

安讯士在全球50多个国家和地区设有办事机构，拥有超过5,000名尽职的员工，并与遍布世界各地的技术和系统集成合作伙伴携手并进，为客户带来高价值的解决方案。安讯士创立于1984年，总部位于瑞典。