WHITE PAPER

Axis 네트워크 오디오의 사이버 보안

9월 2025

요약

오늘날과 같이 모든 것이 연결된 세상에서 오디오 통신 시스템의 보안은 민감한 정보를 보호하고 운영 효율성을 유지하는 데 매우 중요합니다. 네트워크 오디오 시스템은 무단 액세스, 도청, 서비스 거부 공격, 악성코드, 소프트웨어 취약점 악용 등 수많은 위협에 직면해 있습니다. Axis는 기존 인프라와 원활하게 통합되는 최첨단 보안 솔루션을 통해 이러한 위험에 대응하며, 신뢰성, 확장성 및 강력한 보호 기능을 제공합니다.

Axis는 보안 내재화 접근 방식을 채택하여 암호화, 인증, 보안 소프트웨어 업데이트, 접근 제어, 시스템 보안 강화, 이벤트 로깅 기능을 통합합니다. SIPS, SRTP, HTTPS, IEEE 802.1AE와 같은 보안 프로토콜을 통해 안전한 통신 및 데이터 전송을 지원합니다.

Axis 오디오 관리 소프트웨어는 역할 기반 접근 제어, 보안 온보딩, 포괄적인 이벤트 로깅 기능을 제공하며 온프레미스 및 클라우드 기반 구축 환경을 모두 지원합니다.

이러한 다층적 보안을 활용하여 Axis 네트워크 오디오 시스템은 사이버 위협에 대한 엔드 투 엔드 보호 기능을 제공합니다.

목차

1 서론 4
2 위험 이해하기 4
3 Axis 네트워크 오디오의 이점 4
4 스피커 및 시스템 보안의 핵심 기능 4
5 시스템 전반에 걸친 보안 5
5.1 장치 보안 5
5.2 보안 프로토콜 5
5.3 오디오 관리 소프트웨어의 보안 7
5.3.1 온프레미스 솔루션 7
5.3.2 클라우드 기반 솔루션 7

1 서론

오디오 시스템은 리테일, 운송, 공공 안전, 교육 등 다양한 산업에서 통신, 보안, 운영 효율성에 핵심적인 역할을 합니다. 이러한 시스템은 사이버 공격의 표적이 되기 쉬우므로 강력한 보안 조치가 필수적입니다. 오디오 시스템이 손상되면 심각하고 광범위한 결과를 초래할 수 있습니다.

이 백서에서는 이러한 과제를 해결하기 위해 Axis 스피커 및 오디오 시스템이 사용하는 주요 보안 계층에 대해 자세히 살펴봅니다.

2 위험 이해하기

다양한 산업 분야에서 네트워크 오디오 솔루션 도입이 증가함에 따라, 보안이 확보되지 않은 시스템과 관련된 잠재적 위험 또한 크게 증가했습니다.

네트워크 오디오 시스템은 여러 유형의 위협에 노출될 수 있습니다.

- 무단 액세스입니다**.** 보호되지 않는 오디오 장치는 악의적인 공격자가 원격으로 액세스할 수 있으며, 이 경우 스피커 제어권 탈취, 무단 안내 방송 송출 또는 운영 방해 등이 발생할 수 있습니다.
- 도청 및 데이터 가로채기**.** 네트워크 오디오 시스템은 유선 또는 무선 네트워크를 통해 민감한 음성 데이터를 전송하는 경우가 있습니다. 암호화가 없으면 공격자가 대화를 가로채 녹음할 수 있으며, 이는 개인정보 침해, 산업 스파이 활동, 기밀 정보 오용 등으로 이어질 수 있습니다.
- 서비스 거부**(DoS)** 공격**.** 공격자는 네트워크 스피커나 오디오 서버에 과도한 트래픽을 유발하여 시스템 과부하 및 서비스 중단을 초래할 수 있습니다. 이러한 공격은 결정적인 순간에 비상 통신 시스템을 작동 불능 상태로 만들 수 있습니다.
- 악성코드 및 랜섬웨어 공격**.** 기존 IT 인프라와 마찬가지로 네트워크 오디오 장치도 악성코드나 랜섬웨어에 의해 손상될 수 있습니다. 공격자는 장치를 잠그고 금품을 요구하거나, 손상된 시스템을 더 광범위한 네트워크 공격을 위한 진입점으로 사용할 수 있습니다.
- 소프트웨어 및 공급망의 취약점 악용 보안 패치가 적용되지 않은 구형 운영 체제는 오디오 장치의 제어권을 탈취하는 데 악용될 수 있습니다. 또한, 안전하지 않은 공급망 관행은 배포 이전 단계에서부터 취약점을 야기하여 시스템을 초기부터 위험에 노출시킬 수 있습니다.

3 Axis 네트워크 오디오의 이점

Axis는 기존 인프라와 원활하게 통합되는 최첨단 스피커 및 시스템 보안 솔루션을 제공합니다. 개방형 아키텍처는 다양한 시스템 및 프로토콜과의 호환성을 제공합니다. Axis 시스템은 소규모 구축 환경부터 엔터프라이즈급 대규모 네트워크에 이르기까지, 조직의 요구 사항에 맞춰 유연하게 확장할 수 있도록 설계되었습니다. Axis는 온프레미스 및 클라우드 기반 오디오 관리 시스템을 모두 제공합니다.

Axis는 소프트웨어 개발에 보안 내재화 접근 방식을 적용합니다. Axis의 ASDM(Axis Security Development Model) 프레임워크는 전체 소프트웨어 개발 수명 주기에 걸쳐 보안을 통합하고 취약점 발생 위험을 줄이기 위한 프로세스와 도구를 정의하며, 지속적으로 개선되고 있습니다.

이러한 개선 작업의 일환으로, 다양한 보안 관련 표준을 정기적으로 평가하고 이를 ASDM에 반영합니다. Axis 소프트웨어는 EU의 GDPR(개인정보 보호 규정)을 포함하여 데이터 개인정보 보호 및 보안에 관한 엄격한 업계 표준을 준수합니다.

4 스피커 및 시스템 보안의 핵심 기능

Axis 네트워크 오디오는 장치는 물론 관리 시스템에도 보안 기능이 내장되어 있습니다.

암호화 및 인증

- 암호화는 TLS 1.2 및 1.3을 통해 오디오 데이터를 안전하게 전송하여 권한 없는 제3자의 정보 가로채기 및 액세스를 방지합니다.

- 인증을 통해 권한이 있는 장치와 사용자만 해당 장치뿐만 아니라 전체 솔루션에 액세스할 수 있도록 보장합니다.

안전한 장치 소프트웨어 업데이트

- Secure boot(대부분의 제품에 해당) 및 디지털 서명된 패치를 통해 검증된 장치 소프트웨어만 설치되도록 보장합니다. 이를 통해 악성 코드로부터 시스템을 보호합니다.

접근 제어

- AXIS Audio Manager Pro 및 AXIS Audio Manager Center는 역할 기반 접근 제어(RBAC)를 사용하여 시스템 접근 권한을 승인된 담당자로만 제한합니다.
- 중앙 집중식 관리를 통해 IT 관리자는 권한을 효과적으로 모니터링하고 제어할 수 있습니다.

시스템 보안 강화

- 기본 설정이 출고 시부터 보안에 최적화되어 있어 취약점을 줄여줍니다.
- 추가 구성 옵션을 통해 특정 사용 사례에 맞춰 맞춤 설정이 가능합니다. AXIS OS 보안 강화 가이드(*help.axis.com/axis-os-hardening-guide*)에서 기술 관련 조언을 제공합니다.

이벤트 로깅 및 모니터링

- 포괄적인 로깅 기능을 통해 시스템 활동에 대한 가시성을 확보할 수 있습니다. 이를 통해 실시간 위협 탐지 및 포렌식 분석에 도움을 받을 수 있습니다.

5 시스템 전반에 걸친 보안

Axis 네트워크 오디오는 장치와 관리 시스템 자체에 보안 기능이 내장되어 있습니다. 보안 프로토콜은 장치와 관리 소프트웨어 간 통신에서 높은 수준의 보안을 보장합니다.

5.1 장치 보안

모든 Axis 스피커는 Axis 장치 전용으로 개발된 소프트웨어인 AXIS OS에서 작동합니다. 이를 통해 장기적인 가치, 사이버 보안 및 세계적 수준의 통합을 지원합니다. AXIS OS를 통해 모든 Axis 스피커는 Axis 생태계의 강력한 보안 기능을 그대로 이어받습니다. 이를 통해 모든 장치에서 일관성과 신뢰성을 확보하고, 모든 구축 환경에 대해 엔드 투 엔드 보호 기능을 제공합니다. 보안 기능에는 암호화된 파일 시스템과 하드웨어 기반 사이버 보안 플랫폼인 Axis Edge Vault(*axis.com/solutions/edge-vault*)가 포함됩니다.

Axis Edge Vault는 Axis 장치의 무결성을 보호하고 암호화 키를 기반으로 한 보안 작업 실행을 지원합니다. 이 기능은 IEEE 802.1AR을 준수하는 Axis 장치 ID를 확인하고 이를 활용하여 IEEE 802.1X 및 HTTPS를 통해 제로 트러스트 네트워크에 장치를 안전하게 온보딩할 수 있도록 지원합니다. Axis Edge Vault를 사용하면 장치를 안전하게 부팅하고 시스템에 통합할 수 있으며, 암호화 키와 같은 민감한 정보가 안전하게 보호된다는 것을 신뢰할 수 있습니다.

Axis Edge Vault를 통해, 공급망을 거쳐 수령한 Axis 장치가 물리적으로 변조되거나 손상되지 않았음을 신뢰할 수 있습니다. Axis Edge Vault는 신뢰 체인을 구축하고, 암호화 방식으로 검증된 소프트웨어 체인이 중단 없이 유지되도록 보장합니다. 예를 들어, *Signed OS* 기능은 장치 소프트웨어가 Axis 정품임을 보장하며 Axis의 서명이 있는 업데이트만 설치되도록 합니다.

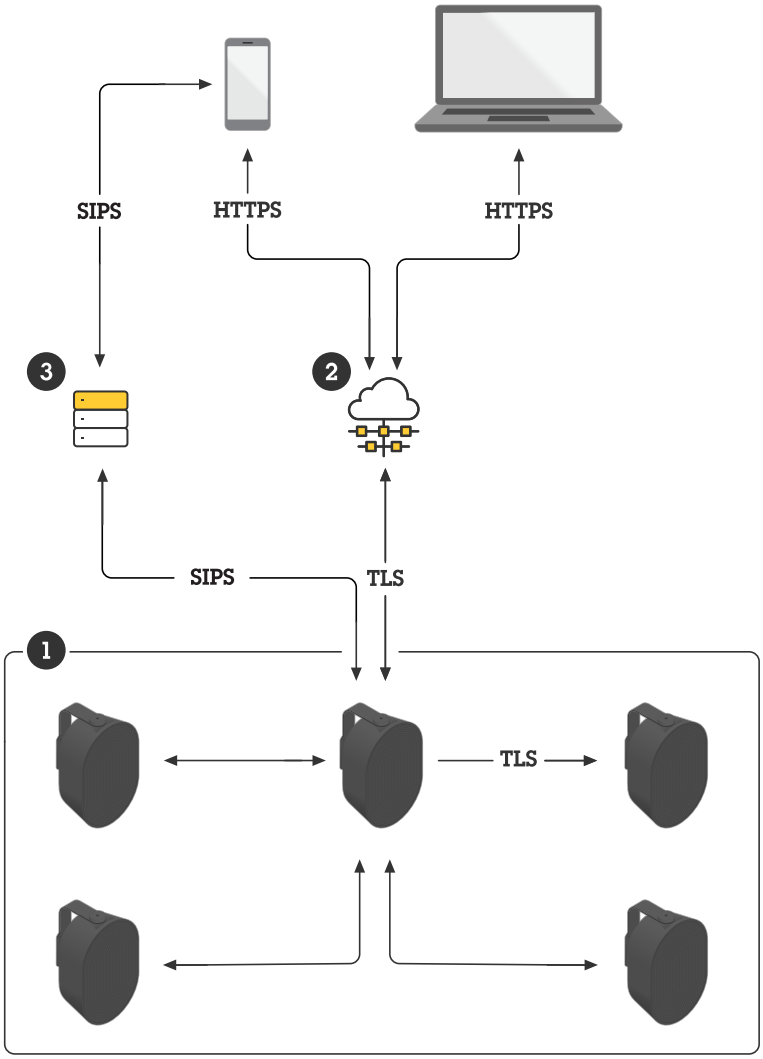
5.2 보안 프로토콜

Axis 장치 및 시스템은 개방형 프로토콜을 사용하여 안전한 통신, 전송, 스트리밍을 보장합니다.

- **SIPS** (SIP Secure): TLS(Transport Layer Security)를 통합하여 표준 SIP(Session Initiation Protocol)의 보안을 강화합니다. 이를 통해 IP PBX와 VoIP 전화기 간에 보안 연결이 설정됩니다. 보안 연결이 설정되면, SRTP(Secure Real-Time Transport Protocol)는 음성 데이터를 안전한 IP 패킷으로 암호화하여 인터넷을 통해 전송합니다. 이를 통해 송신 장치(IP 전화 시스템)에서 수신 장치(스피커)까지 엔드 투 엔드 암호화가 제공됩니다.

Axis 시스템은 SIPS와 SRTP를 활용하여 오디오 데이터는 물론 연결 설정 과정 자체를 안전하게 보호합니다. 이는 오디오 스트림과 연결 세부 정보(발신자 ID, 수신자 등)가 완벽하게 암호화되고 P2P(피어 투 피어) 보안 통신 채널이 강력하게 유지됨을 의미합니다.

- **멀티캐스트 컨트롤러**: Axis 스피커의 멀티캐스트 컨트롤러 기능은 SRTP를 통해 전송되는 멀티캐스트 오디오 스트림을 안전하게 수신하도록 지원하여 그룹 통신의 암호화를 보장합니다.
- **Transmit.cgi** 및 **receive.cgi**: 이 VAPIX API는 HTTPS를 통해 암호화된 P2P(Point-to-Point) 통신으로 오디오 스트림을 안전하게 송수신하는 방법을 제공합니다. CGI(Common Gateway Interface)는 웹 서버와 외부 프로그램 간의 통신을 정의하는 표준 프로토콜입니다.
- **RTSPS**(Real-Time Streaming Protocol Secure): 서버와 클라이언트 간의 실시간 미디어 스트림을 설정하고 관리하는 데 사용되는 네트워크 제어 프로토콜입니다. 암호화를 활용하여 무단 액세스를 방지하고, 보안 오디오 스트리밍을 지원합니다.
- **HTTPS**: 모든 API는 HTTPS로 보호되어 모든 통신의 기밀성과 무결성을 유지합니다.
- **IEEE 802.1AE**: MACsec(Media Access Control Security)이라고도 하는 이 프로토콜은 네트워크 계층 2에서 네트워크 통신을 AES-128로 암호화합니다. HTTPS, RTSPS, SIPS와 결합하면 네트워크 트래픽이 실질적으로 이중 암호화되어 네트워크 보안이 크게 향상됩니다.



여러 개방형 프로토콜을 통해 안전한 통신을 구현하는 네트워크 오디오 시스템.

1 *AXIS Audio Manager Edge: Axis* 스피커에 내장된 온프레미스 오디오 관리 솔루션
2 *AXIS Audio Manager Center:* 하이브리드 클라우드 기반의 중앙 집중식 오디오 관리 솔루션
3 파트너 *PBX*

5.3 오디오 관리 소프트웨어의 보안

5.3.1 온프레미스 솔루션

Axis 온프레미스 솔루션은 현장의 여러 스피커에 대한 구역 설정, 우선순위 지정, 보안 통신을 관리하도록 고안되었습니다.

AXIS Audio Manager Edge. 이 관리 소프트웨어는 Axis의 모든 네트워크 오디오 스피커에 내장되어 있습니다. 각 스피커를 별도의 관리 소프트웨어 서버 없이 완벽한 올인원 사운드 시스템으로 만들어 줍니다. AXIS Audio Manager Edge는 최대 20개 구역에 걸쳐 최대 200개 장치로 구성된 비교적 단순한 프로젝트를 관리하는 데 적합합니다.

- 장치 간 암호화를 지원합니다. 기본 암호화 방식은 자체 서명 인증서를 사용하는 TLS이지만, 장치에 신뢰할 수 있는 인증서를 설치하고 사이트의 시스템 설정에서 TLS 인증을 활성화할 것을 권장합니다. 이를 통해 중간자 공격을 방어할 수 있습니다.
- 로컬 사이트에 장치를 안전하게 온보딩할 수 있도록 지원합니다. 초기 설정은 장치 자격 증명을 사용하여 HTTPS를 통해 수행됩니다. 이후 장치 간 통신에는 MQTT(TLS-PSK)가, 장치 간 오디오 스트림과 같은 암호화된 RTP 데이터를 전송하는 데에는 SRTP가 사용됩니다.
- HTTPS API를 통해 운영 용도의 외부 시스템 액세스를 제공합니다.

AXIS Audio Manager Pro. 이 관리 소프트웨어는 더 큰 규모의 고급 프로젝트를 위한 것입니다. 단일 인터페이스에서 수많은 구역(500개 이상)과 수천 대의 장치(5000대 이상)를 처리할 수 있습니다. AXIS Audio Manager Pro는 장기 스케줄링과 고급 우선순위 설정을 용이하게 합니다.

- 역할 기반 접근 제어 기능을 포함하며, 이는 시스템 접근 권한을 승인된 담당자로만 제한하고 Active Directory 통합을 지원합니다.
- 장치의 보안 온보딩을 지원합니다.
- 상세한 이벤트 및 감사 로그를 포함합니다. 이는 시스템 활동에 대한 포괄적인 기록을 제공하여 관리자가 변경 사항을 추적하고, 동작을 모니터링하며, 문제를 해결하는 데 도움을 줍니다.

5.3.2 클라우드 기반 솔루션

AXIS Audio Manager Center는 몇 개의 사이트에서 수천 개의 사이트로 확장되는 다중 사이트 시스템의 원격 관리 및 모니터링을 위한 서비스입니다. 각 로컬 사이트에서 AXIS Audio Manager Edge와 함께 사용됩니다. 클라우드 기반 및 온프레미스 구성 요소를 모두 사용하는 이 솔루션은 편리하고 안정적인 하이브리드 클라우드 솔루션입니다.

AXIS Audio Manager Center는 관리를 간소화하고 중앙 집중식 제어를 제공하며, 장치의 보안 온보딩을 처리합니다. 싱글 사인온으로 선택된 사이트나 구역에 대한 안내 방송, 배경 음악, 광고 등을 예약할 수 있어 사용자 작업 부하가 크게 줄어듭니다. 주요 보안 기능은 다음과 같습니다.

- 역할 기반 접근 제어(RBAC): 시스템 접근 권한을 승인된 담당자로만 제한합니다.
- 중앙 집중식 사용자 관리: *My Axis* 또는 Active Directory 사용자/그룹을 지원하여 관리 업무를 간소화합니다. 로컬 사용자를 생성할 필요가 없습니다.
- 보안 온보딩: 각 장치에 설치된 고유 인증서를 사용하여 클라우드에서 신뢰를 확보함으로써 장치의 보안 온보딩 과정을 간소화합니다.
- 안전한 E2E 구성 간소화: 인증서 처리를 포함한 SIPS의 안전한 구성을 지원합니다.
- 상태 모니터링 및 알림: 시스템 상태에 대한 중앙 집중식 모니터링과 잠재적 문제에 대한 즉각적인 알림을 제공합니다.
- 보안 통신: 클라우드와 장치 간의 모든 통신은 TLS를 통해 암호화되며, 상호 TLS(양방향 인증)로 강력한 보안을 보장합니다.
- 원격 액세스: 어디서든 로컬 사이트에 안전하게 원격으로 액세스할 수 있습니다.

T10225475_KO/KO/M1.13/2509

Axis Communications에 대하여

Axis는 보안, 안전, 운영 효율성 및 비즈니스 인텔리전스를 향상시켜 더 스마트하고 더 안전한 세상을 실현합니다. 네트워크 기술 회사이자 업계 선도 기업인 Axis는 영상 감시, 접근 제어, 인터콤 및 오디오 솔루션을 제공합니다. 이러한 솔루션은 지능형 분석 애플리케이션으로 보완되고 고품질 교육을 통해 지원됩니다.

50개 이상의 국가에서 약 5,000명의 Axis 임직원이 전 세계의 기술 및 시스템 통합 파트너와 협력하여 고객에게 최적의 솔루션을 제공하고 있습니다. Axis는 1984년에 설립되었으며 본사는 스웨덴 룬드에 있습니다.