백서

AXIS 신체 착용 카메라

시스템 보안

2월 2024

요약

개방형 플랫폼에 기반하고 있음에도 불구하고 Axis 신체 착용 시스템은 매우 높은 수준의 시스템 보안을 자랑합니다.

카메라 분실 시 보안을 보장하기 위해 카메라는 불필요한 소프트웨어 구성 요소가 없는 최소화된 플랫폼에 기반을 두고 있습니다. 대신 물리적 위협에 덜 노출되는 시스템 컨트롤러에 더 많은 기능이 배치되어 있습니다. 또한 카메라의 내부 스토리지는 데이터에 대한 무단 액세스를 금지하기 위해 AES-256 암호화되어 있습니다. IPv6 및 인증서에 기반한 통신은 카메라가 특정 시스템 컨트롤러 또는 카메라가 속한 시스템으로만 데이터를 오프로드하도록 보장합니다.

카메라에서 시스템 컨트롤러로 데이터가 오프로드될 때 HTTPS 암호화된 네트워크 연결이 사용됩니다. 데이터는 시스템 컨트롤러의 AES-256 암호화 저장 장치에 잠시만 저장된 후, 다른 HTTPS 암호화 연결을 통해 콘텐츠 대상으로 전송됩니다.

시스템 컨트롤러의 보안과 무결성은 FIPS 140-2를 준수하는 TPM(Trusted Platform Module)을 통해 더욱 강화됩니다. 신체 착용 시스템이 다른 많은 Axis 장치와 공유하는 다른 기능으로는 signed firmware, secure boot, signed video가 있습니다.

AXIS Body Worn Live를 통해 영상을 라이브 스트리밍할 때, 데이터는 대기 상태에서, 전송 중에 그리고 뷰어의 웹 브라우저에서 암호화됩니다. 또한 XChaCha20-Poly1305 프로토콜을 사용하여 엔드 투 엔드 암호화됩니다. 이외에도 관리자가 특정 컴퓨터, 웹 브라우저 및 사용자 자격 증명을 포함해 라이브 스트림을 볼 수 있는 사람을 관리할 수 있습니다.

목차

1 약어 및 용어

BWC. 신체 착용 카메라(body worn camera)

VMS. 영상 관리 시스템(video management system)

EMS. 증거 관리 시스템(evidence management system)

콘텐츠 목적지. 예를 들어 신체 착용 카메라의 녹화 및 데이터를 저장하는 위치입니다. 콘텐츠 대상의 예로는 영상 관리 시스템, 증거 관리 시스템, 미디어 서버 등이 있습니다.

2 서론

Axis 신체 착용 시스템은 개방형 플랫폼을 기반으로 하므로 영상 관리 및 증거 관리를 위해 외부 시스템과 쉽게 통합할 수 있습니다. 그럼에도 불구하고 시스템 구현의 모든 단계에서 보안에 중점을 두었기 때문에 매우 높은 수준의 시스템 보안을 자랑합니다.

이 백서에서는 Axis 신체 착용 시스템의 구성 요소 간의 데이터 흐름을 설명합니다. 특히 BWC 녹화에서 콘텐츠 대상에 이르기까지 시스템과 데이터를 보호하기 위해 취한 조치에 대해 설명합니다. 추가 보안 고려 사항을 포함하여 다양한 저장 매체에 대해서도 강조합니다.

3 카메라 분실 시 보안

신체 착용 카메라(BWC)는 일상적인 사용 과정에서 도난 및 파손의 위험에 물리적으로 노출됩니다. 이러한 위협의 영향을 완화하기 위해 카메라가 분실되더라도 시스템 및 데이터 보안이 유지될 수 있도록 몇 가지 시스템 설계 기능이 적용되었습니다.

한 가지 예로, BWC는 다른 Axis 카메라에 비해 최소화된 소프트웨어 플랫폼을 기반으로 하며 불필요한 소프트웨어 구성 요소가 모두 제거되어 있습니다. 카메라와 시스템 컨트롤러는 VAPIX를 지원하지 않으며 FTP, SSH 또는 SNMP와 같은 프로토콜도 지원하지 않습니다. 이외에도, 카메라에는 서버 기능이 없습니다. 대신에 카메라에 비해 물리적 위협에 덜 노출되는 시스템 컨트롤러가 VMS 및 EMS와 같은 다른 시스템과의 통합을 처리합니다.

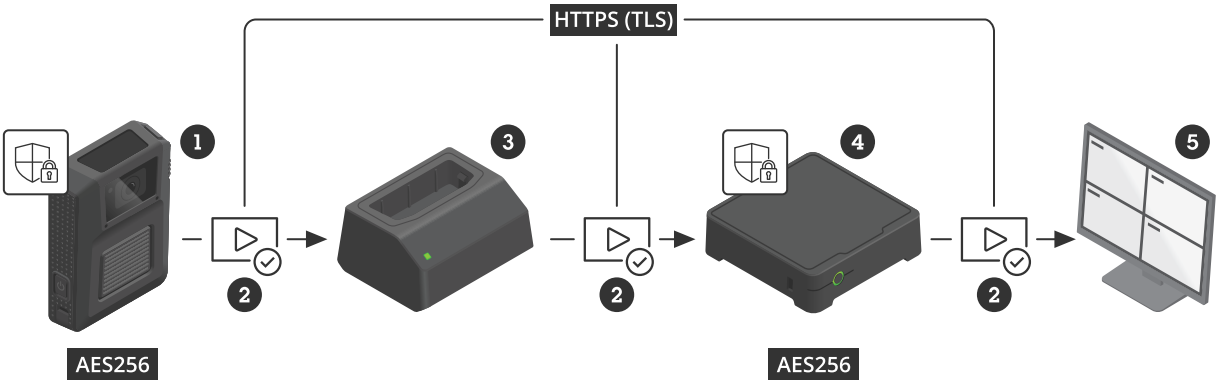
카메라 분실 시 데이터에 대한 무단 액세스를 방지하기 위해 BWC의 내부 스토리지는 AES-256을 사용하여 암호화됩니다.

카메라는 카메라가 속한 특정 시스템 컨트롤러 또는 시스템으로만 데이터를 오프로드합니다. 이는 BWC와 시스템 컨트롤러가 IPv6와 인증서를 사용하여 통신하기 때문입니다. 인증서는 카메라가 도킹될 때마다 시스템 컨트롤러의 최신 인증서에 맞게 자동으로 갱신됩니다.

카메라가 도킹 해제되어 4주 이상 시스템에서 떨어져 있는 경우, 시스템 컨트롤러가 8주 동안의 이전 인증서를 수락하는 유예 기간이 있습니다. 카메라가 그보다 더 오래 분리될 경우, 마스터 키 암호를 사용하여 시스템에서 다시 수동으로 승인해야 합니다. 이는 카메라를 분실했거나 오랫동안 분리된 카메라가 사용자가 인지하지 못하는 사이에 다시 추가되는 것을 방지하기 위한 것입니다. 사용자가 인지하지 못하는 사이에 추가되면 보안 위험을 초래할 수 있습니다.

4 데이터 전송 보안

일반적인 사용 시, 비디오와 메타데이터가 포함된 BWC를 교대 근무가 끝난 후 도킹합니다. 모든 데이터는 도킹 스테이션을 통해 HTTPS(TLS가 포함된 HTTP)로 암호화된 네트워크 연결을 사용하여 시스템 컨트롤러로 오프로드됩니다. 데이터는 시스템 컨트롤러에 잠시만 저장되며, AES-256으로 암호화된 SSD 저장 장치에 저장됩니다. 그런 다음 시스템 컨트롤러는 HTTPS를 사용하여 데이터를 콘텐츠 대상에 전송합니다.



BWC(1)에서 콘텐츠 목적지(5)로 안전한 데이터 전송 및 저장.

1. *Axis Edge Vault 탑재 BWC*
2. *Signed video(사이버 보안 기능)*
3. *도킹 스테이션*
4. *Axis Edge Vault 탑재 시스템 컨트롤러*
5. *콘텐츠 목적지*

콘텐츠 목적지가 공개 암호화 키를 제공하는 경우 콘텐츠 목적지의 암호화 키를 사용하여 BWC 및 시스템 컨트롤러의 데이터를 암호화하는 기능도 지원됩니다. 이 경우 데이터는 콘텐츠 대상에 전송될 때 추가 암호화 계층을 갖게 됩니다.

5 기타 보안 특성

시스템 컨트롤러의 보안과 무결성은 FIPS 140-2를 준수하는 TPM(Trusted Platform Module)을 통해 더욱 강화됩니다.

BWC와 시스템 컨트롤러 모두에는 장치의 모든 데이터를 보호하고 여러 보안 기능을 활성화하는 하드웨어 기반 사이버 보안 플랫폼 Axis Edge Vault가 탑재되어 있습니다. 예를 들어, 파일 시스템은 암호화되고 키는 Axis Edge Vault로 보호됩니다. *Secure Boot*는 인증된 펌웨어로만 장치를 부팅할 수 있도록 합니다. *Signed firmware*는 펌웨어 무결성이 손상된 경우 펌웨어 업그레이드를 거부하도록 합니다. *Signed video*는 비디오 스트림에 암호화 체크섬을 추가하여 추가적인 보호 계층을 생성합니다. 이를 통해 영상이 생성된 고유 Axis 카메라를 신뢰성 있게 추적할 수 있어 영상이 변조되지 않았는지 확인할 수 있습니다.

Signed video에 대한 자세한 내용은 *www.axis.com/developer-community/signed-video*를 참조하고, Axis 사이버 보안 특성에 대한 자세한 내용은 *www.axis.com/solutions/built-in-cybersecurity-features*를 참조하십시오.

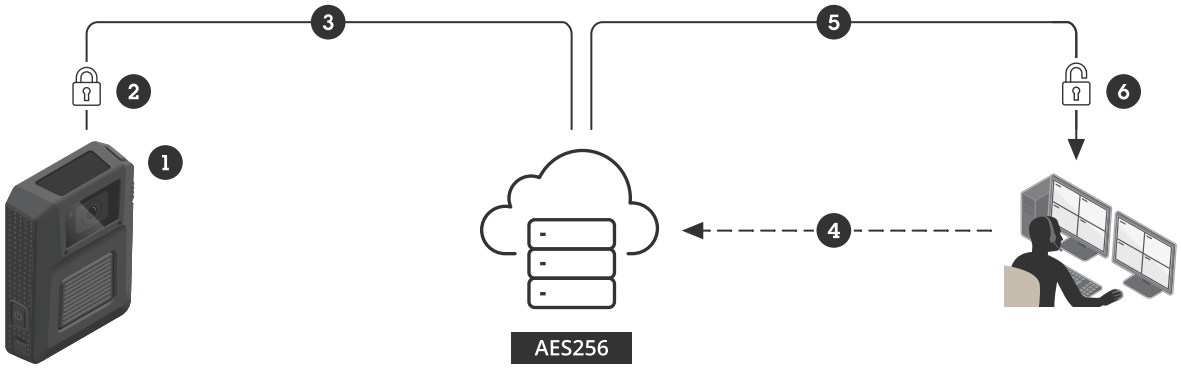
카메라 사용자가 사이트에서 녹화된 비디오를 볼 수 있는 유일한 방법은 AXIS Body Worn Assistant 애플리케이션을 사용하는 것입니다. 애플리케이션이 활성화된 경우, BWC는 애플리케이션으로 직접 비디오를 스트리밍하지만, 애플리케이션을 실행하는 장치의 캐시나 메모리에 비디오 자료가 나중에 액세스할 수 있도록 저장되지 않습니다. 비디오 스트림에는 비디오 캡처를 위한 보조 녹화 장치의 사용을 막기 위한 오버레이도 있습니다. 설화 녹화가 되어도, 비디오 클립에 대해 오버레이를 통해 BWC 사용자를 추적할 수 있습니다. BWC의 USB-C 호환 커넥터는 어떤 방식으로도 비디오를 보거나 삭제하거나 오프로드하는 데 사용할 수 없습니다.

6 AXIS Body Worn Live의 보안

AXIS Body Worn Live는 Axis 신체 착용 카메라의 실시간 데이터에 액세스할 수 있도록 하는 애플리케이션입니다. AXIS Body Worn Live는 사용자에게 비디오, 오디오 및 위치 좌표와 같은 기타 데이터의 실시간 스트림을 제공함으로써 진행 중인 사고에 대한 탁월한 상황 인식을 가능하게 합니다. 초기에는 클라우드 기반 서비스로 제공됩니다.

AXIS Body Worn Live를 사용하면 데이터가 대기 중(스토리지에서)과 전송 중일 때뿐만 아니라 카메라와 뷰어의 웹 브라우저 간에 완전히 엔드 투 엔드 암호화됩니다.

AXIS Body Worn Live에서 호스팅되는 모든 데이터와 파일은 미사용 시 AES-256을 사용하여 암호화됩니다. 모든 통신 채널은 신뢰할 수 있는 인증 기관에서 서명한 인증서를 사용하며, HTTPS와 TLS를 사용하여 보호됩니다. AXIS Body Worn Live는 XChaCha20-Poly1305 프로토콜을 사용하여 진정한 엔드 투 엔드 암호화의 또 다른 계층을 추가하기도 합니다.



AXIS Body Worn Live의 엔드 투 엔드 암호화를 통한 안전한 라이브 스트리밍

1 *BWC는 실시간 비디오와 기타 데이터를 수집합니다.*
2 *데이터는 BWC에서 암호화됩니다.*
3 *데이터는 BWC에서 AXIS Body Worn Live로 전송됩니다.*
4 *뷰어가 AXIS Body Worn Live에 데이터를 요청합니다.*
5 *데이터는 AXIS Body Worn Live에서 뷰어에게 스트리밍됩니다.*
6 *데이터는 뷰어의 웹 브라우저에서 복호화됩니다.*

신체 착용 카메라 시스템의 관리자는 라이브 스트림을 볼 수 있는 사람을 완전히 관리할 수 있습니다. 데이터는 관리자가 승인한 뷰어만 암호를 해독하고 비디오를 볼 수 있도록 암호화되어 있으며, 관리자는 접근 권한을 취소할 수도 있습니다. 관제원은 올바른 컴퓨터, 올바른 웹 브라우저 및 올바른 사용자 자격 증명을 가지고 있어야 합니다. Axis를 포함한 다른 누구도 라이브 스트림에 액세스할 수 없습니다. Axis는 사용자가 생성한 엔드 투 엔드 암호화 키에 액세스할 수 없습니다.

T10155258/KO/M4.2/2402

Axis Communications 정보

Axis는 보안 및 새로운 비즈니스 성과를 개선하기 위한 솔루션을 창조하여 더 스마트하고 안전한 세상을 가능하게 합니다. 네트워크 기술 회사이자 업계 리더인 Axis는 비디오 감시, 접근 제어, 인터콤, 오디오 시스템 솔루션을 제공합니다. 이러한 솔루션은 지능형 분석 애플리케이션으로 향상되고, 고품질 교육의 지원을 받습니다.

Axis에서는 50개 이상의 나라에 약 4,000명의 전담 직원이 있으며 전 세계 기술 및 시스템 통합 파트너와 협력하여 고객 솔루션을 제공합니다. Axis는 1984년에 설립되었으며 본사는 스웨덴 룬드에 있습니다