WHITE PAPER

Segurança na solução de uso corporal da Axis

Fevereiro 2024

Resumo

Apesar de ser baseado em uma plataforma aberta, o sistema de uso corporal da Axis possui um nível muito alto de segurança.

Para garantir a segurança em caso de perda da câmera, ela é baseada em uma plataforma mínima, sem componentes de software desnecessários. Em vez disso, mais recursos foram adicionados no controlador do sistema, que geralmente fica menos exposto a ameaças físicas. Além disso, o armazenamento interno da câmera é criptografado usando AES-256 para proibir o acesso não autorizado aos dados. A comunicação baseada em IPv6 e os certificados garantem que a câmera descarregará dados apenas no controlador de sistema específico ou no sistema ao qual pertence.

Quando os dados são descarregados da câmera para o controlador do sistema, é usada uma conexão HTTPS de rede criptografada. Os dados são armazenados por um breve período no dispositivo de armazenamento criptografado (com AES-256) do controlador do sistema, antes de serem transferidos usando outra conexão criptografada HTTPS para o destino do conteúdo.

A segurança e a integridade do controlador do sistema são reforçadas por um TPM (Módulo de plataforma confiável) compatível com FIPS 140-2. Outros recursos, que o sistema corporal compartilha com muitos outros dispositivos da Axis, são o firmware assinado, a inicialização segura e o vídeo assinado

Quando a filmagem é transmitida ao vivo por meio do AXIS Body Worn Live, os dados são criptografados em repouso, no transporte e no navegador da Web do visualizador. Também é criptografado de ponta a ponta com o protocolo XChaCha20-Poly1305. Além disso, o administrador controla quem pode visualizar a transmissão ao vivo dependendo do computador, do navegador da Web e das credenciais de usuário.

Índice

1 Siglas e terminologia

BWC. Câmera corporal

VMS. Sistema de gerenciamento de vídeo

EMS. Sistema de gerenciamento de evidências

Destino do conteúdo. Local que armazena gravações e dados de, por exemplo, câmeras corporais. Exemplos de destinos de conteúdo incluem sistemas de gerenciamento de vídeo, sistemas de gerenciamento de evidências e servidores de mídia.

2 Introdução

O sistema de uso corporal da Axis é baseado em uma plataforma aberta, o que facilita a integração com sistemas externos para gerenciamento de vídeo e gerenciamento de evidências. No entanto, possui um nível muito alto de segurança de sistema, pois esse foi o foco principal em todas as etapas da implementação do sistema.

Este white paper descreve o fluxo de dados entre os componentes do sistema corporal da Axis. Descrevemos especialmente as medidas tomadas para proteger o sistema e os dados, desde uma gravação da BWC até o destino do conteúdo. As diferentes mídias de armazenamento também estão destacadas, incluindo considerações adicionais de segurança.

3 Segurança em caso de perda da câmera

Por causa do uso diário, a câmera corporal (BWC) está fisicamente exposta a riscos de roubo e vandalismo. Vários recursos de design do sistema foram empregados para mitigar os efeitos de tais ameaças para que a segurança do sistema e dos dados seja mantida mesmo quando uma câmera é perdida.

Exemplo: a BWC baseia-se em uma plataforma de software mínima em comparação com outras câmeras Axis, e todos os componentes de software desnecessários foram removidos. A câmera e o controlador do sistema não suporta VAPIX nem protocolos como FTP, SSH ou SNMP. Além disso, a câmera não funciona como um servidor. A integração com outros sistemas, como VMS e EMS, é realizada pelo controlador do sistema, que geralmente é menos exposto a ameaças físicas do que as câmeras.

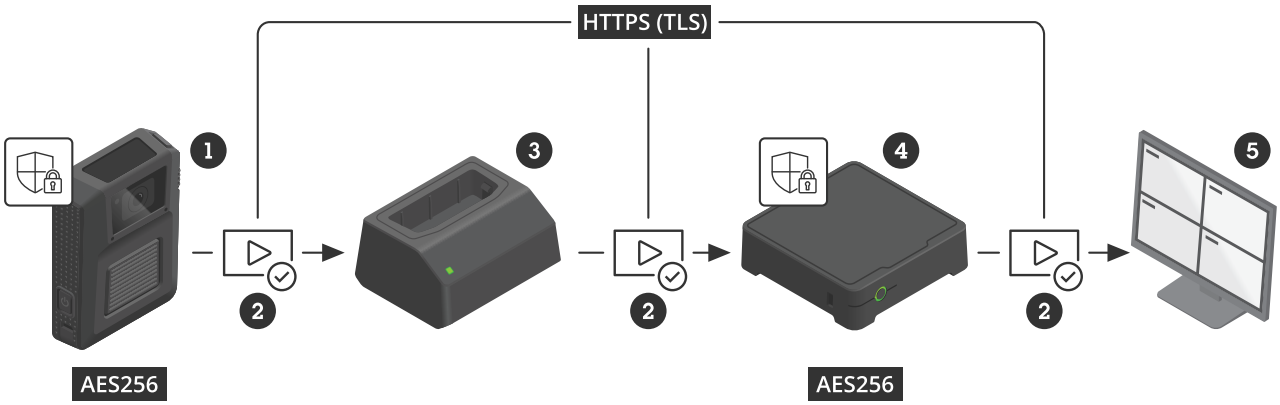
O armazenamento interno da BWC é criptografado usando AES-256 para proibir o acesso não autorizado aos dados em caso de perda da câmera.

A câmera descarregará os dados apenas para o controlador de sistema específico ou o sistema ao qual ela pertence. Isso ocorre porque a BWC e o controlador do sistema se comunicam com IPv6 e usam certificados. Os certificados são renovados automaticamente para corresponder ao mais recente do controlador do sistema toda vez que a câmera é acoplada na dock.

Caso a câmera fique desacoplada e fora do sistema por mais de quatro semanas, o controlador do sistema aceitará certificados mais antigos por oito semanas (período de tolerância). Caso a câmera fique inativa por mais tempo, ela precisará ser aceita novamente no sistema de forma manual, usando a senha da chave mestra. Isso é feito para garantir que a câmera perdida ou inativa por um longo período não seja adicionada novamente sem que seja notada, pois pode representar um risco de segurança.

4 Segurança na transferência de dados

Geralmente, após o turno, a BWC (contendo vídeos e metadados) é acoplada à dock station. Todos os dados são descarregados através da dock station para o controlador do sistema usando uma conexão de rede criptografada com HTTPS (HTTP com TLS). Os dados são armazenados no controlador do sistema por um breve período no dispositivo de armazenamento SSD e criptografado usando AES-256. O controlador do sistema então transfere os dados, usando HTTPS, para o destino do conteúdo.



Armazenamento e transferência de dados com segurança da BWC (1) para o destino do conteúdo (5).

1 *BWC com Axis Edge Vault*
2 *Vídeo assinado (recurso de segurança cibernética)*
3 *Estação de carregamento*
4 *Controlador de sistema com o Axis Edge Vault*
5 *Destino do conteúdo*

Também há suporte para usar uma chave de criptografia do destino do conteúdo para criptografar os dados na BWC e no controlador do sistema caso o destino do conteúdo forneça uma chave de criptografia pública. Nesse caso, os dados terão uma camada extra de criptografia ao serem enviados para o destino do conteúdo.

5 Outros recursos de segurança

A segurança e a integridade do controlador do sistema são reforçadas por um TPM (Módulo de plataforma confiável) compatível com FIPS 140-2.

Tanto o BWC quanto o controlador do sistema são equipados com o Axis Edge Vault, uma plataforma de segurança cibernética baseada em hardware que protege todos os dados nos dispositivos e ativa diversos recursos de segurança. Por exemplo, o sistema de arquivos é criptografado e a chave é protegida pelo Axis Edge Vault. *A inicialização segura* garante que os dispositivos possam inicializar apenas com firmware autorizado. O *firmware assinado* faz com que eles rejeitem atualizações de firmware se a integridade do firmware estiver comprometida. O *vídeo assinado* cria uma camada extra de proteção ao adicionar uma soma de verificação criptográfica ao stream de vídeo. Isso permite que o vídeo seja rastreado de forma confiável até a câmera exclusiva da Axis em que foi produzido, verificando se a filmagem não foi violada.

Consulte *www.axis.com/developer-community/signed-video* para obter mais detalhes sobre vídeo assinado ou *www.axis.com/solutions/built-in-cybersecurity-features* para saber mais sobre os recursos de segurança cibernética da Axis.

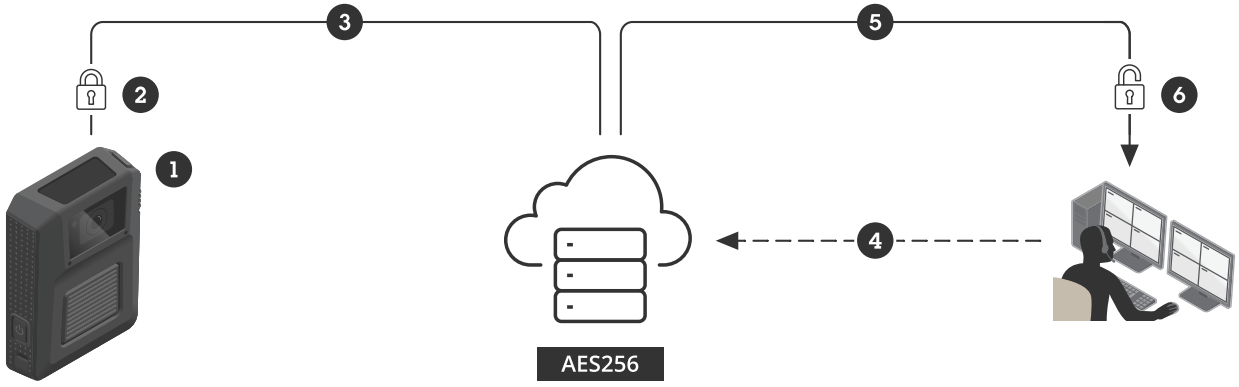
A única maneira de o usuário da câmera visualizar o vídeo gravado em campo é por meio do aplicativo AXIS Body Worn Assistant. Se o aplicativo estiver habilitado, a BWC transmitirá o vídeo diretamente para o aplicativo, mas nenhum material do vídeo será armazenado para acesso posterior no cache ou na memória do dispositivo que executa o aplicativo. Também haverá uma sobreposição no fluxo de vídeo para impedir o uso de dispositivos de gravação secundários para capturar o vídeo. Se ainda assim, isso for feito, o videoclipe poderá ser rastreado até o usuário da BWC por meio da sobreposição. O conector compatível com USB-C da BWC não pode ser usado de forma alguma para visualizar, excluir ou descarregar o vídeo.

6 Segurança com AXIS Body Worn Live

O AXIS Body Worn Live é um aplicativo que permite o acesso em tempo real aos dados das câmeras corporais da Axis. Ao fornecer aos usuários uma transmissão ao vivo de vídeo, áudio e outros dados, como coordenadas de localização, o AXIS Body Worn Live permite uma percepção situacional incomparável de um incidente em andamento. Ele é inicialmente fornecido como um serviço baseado em nuvem.

Com o AXIS Body Worn Live, os dados são criptografados não apenas em repouso (no armazenamento) e em trânsito, mas também totalmente criptografados de ponta a ponta entre a câmera e o navegador da Web do visualizador.

Todos os dados e arquivos hospedados no AXIS Body Worn Live são criptografados usando AES-256 em repouso. Todos os canais de comunicação são protegidos usando HTTPS com TLS, empregando certificados assinados por autoridades de certificação confiáveis. O AXIS Body Worn Live também adiciona outra camada de criptografia verdadeira de ponta a ponta com o protocolo XChaCha20-Poly1305.



Streaming ao vivo seguro com criptografia de ponta a ponta no AXIS Body Worn Live

1 *A BWC coleta vídeo ao vivo e outros dados.*
2 *Os dados são criptografados na BWC.*
3 *Os dados são transmitidos da BWC para o AXIS Body Worn Live.*
4 *O visualizador solicita dados do AXIS Body Worn Live.*
5 *Os dados são transmitidos do AXIS Body Worn Live para o visualizador.*
6 *Os dados são descriptografados no navegador do visualizador.*

O administrador do sistema da câmera corporal tem controle total sobre quem pode visualizar a transmissão em tempo real. Os dados são criptografados de forma que apenas os visualizadores aprovados pelo administrador possam descriptografar e visualizar o vídeo. Além disso, o administrador também revogar o acesso. O visualizador deve usar o computador certo, o navegador da Web certo e as credenciais de usuário certas. Ninguém mais, nem mesmo a Axis, pode acessar a transmissão em tempo real. A Axis não tem acesso às chaves de criptografia de ponta a ponta criadas pelo usuário.

Sobre a Axis Communications

A Axis promove um mundo mais inteligente e seguro, melhorando a segurança, a proteção, a eficiência operacional e a inteligência empresarial. Como empresa de tecnologia de rede e líder de mercado, a Axis disponibiliza soluções de videovigilância, controlo de acessos, sistemas de intercomunicação e de áudio. Estas são potenciadas por aplicações de análise inteligentes e apoiadas por uma formação de alta qualidade.aboutaxis_text

A Axis conta com cerca de 5000 empregados dedicados em mais de 50 países e colabora com parceiros tecnológicos e de integração de sistemas em todo o mundo para fornecer soluções aos clientes. A Axis foi fundada em 1984 e está sediada em Lund na Suécia.