ホワイトペーパー

Axis装着式カメラ

システムセキュリティ

2月 2024

概要

Axisの装着式システムは、オープンプラットフォームをベースにしているにもかかわらず、非常に高いレベルのシステムセキュリティが備わっています。

カメラ紛失時のセキュリティを確保するため、このカメラは不要なソフトウェアコンポーネントを排除し、最小限のプラットフォームに基づいて構築されています。その代わりに、通常は物理的な脅威にさらされにくいシステムコントローラーに多くの機能を搭載しています。カメラの内部ストレージはAES-256で暗号化されており、データへの不正アクセスを防止しています。証明書を使用したIPv6経由の通信により、カメラは特定のシステムコントローラーまたはシステムのみにデータをオフロードします。

カメラからデータがシステムコントローラーにオフロードされる際は、HTTPSで暗号化されたネットワーク接続が用いられます。データはAES-256で暗号化されたシステムコントローラーのストレージデバイスに一時的に保存され、その後別のHTTPS暗号化接続を通じて、コンテンツ送信先に転送されます。

システムコントローラーのセキュリティと完全性は、FIPS 140-2準拠のTPM（Trusted Platform Module）によってさらに強化されます。装着式システムが他の多くのAxisデバイスと共通するその他の機能としては、署名付きファームウェア、セキュアブート、署名付きビデオなどがあります。

AXIS Body Worn Liveを通じて映像をライブストリーミングする際には、保存中・転送中のデータおよび閲覧者のWebブラウザにあるデータが暗号化されます。また、XChaCha20-Poly1305プロトコルを使用して、エンドツーエンドで暗号化されます。さらに、特定のコンピューター、Webブラウザ、ユーザー認証情報など、ライブストリームを視聴できるユーザーを管理者が制御することができます。

目次

1 頭字語と用語

BWC：装着式カメラ（Body Worn Camera）

VMS：ビデオ管理システム（Video Management System）

EMS：証拠管理システム（Evidence Management System）

コンテンツ送信先：装着式カメラなどからの録画とデータを保存する場所。コンテンツ送信先の例として、ビデオ管理システム、証拠管理システム、メディアサーバーなどがあります。

2 はじめに

Axis装着式システムはオープンプラットフォームに基づいて構築されているため、外部のビデオ管理システムや証拠管理システムと容易に統合することができます。一方で、非常に高レベルのシステムセキュリティを備えています。これは、システム実装のあらゆる段階において、このセキュリティに主要な焦点が当てられているためです。

本ホワイトペーパーでは、Axis装着式システムのコンポーネント間のデータフローの概要についてご説明します。特に、BWCでの録画からコンテンツ送信に至るまで、システムとそのデータを保護するために講じられている対策について説明します。さまざまなストレージメディアについても、セキュリティ上の留意点を含めて紹介しています。

3 カメラ紛失時のセキュリティ

日常的に使用されるBWC（装着式カメラ）は、常に盗難や破壊行為といった物理的な危険性に曝されます。このような脅威の影響を軽減するために、いくつかのシステム設計機能が採用されており、カメラを紛失した場合でもシステムとデータのセキュリティを維持することができます。

一例として、BWCは他のAxisカメラと比較して、最小限のソフトウェアプラットフォームに基づいて構築されており、不要なソフトウェアコンポーネントはすべて削除されています。カメラとシステムコントローラーはVAPIXをサポートしておらず、FTP、SSH、SNMPといったプロトコルもサポートしていません。また、カメラにはサーバー機能がありません。VMSやEMSといった他のシステムとの統合は、システムコントローラーで処理します。システムコントローラーは通常、カメラほど物理的な脅威にさらされることはありません。

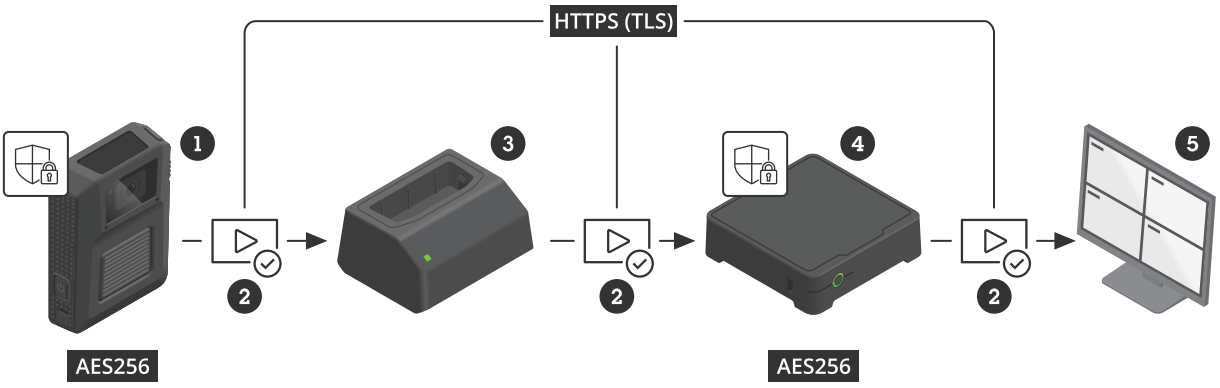
BWCの内部ストレージは、AES-256で暗号化されています。これにより、カメラ紛失時におけるデータへの不正アクセスを防止することができます。

カメラは、カメラが属する特定のシステムコントローラーまたはシステムのみにデータをオフロードします。これは、BWCとシステムコントローラーがIPv6で通信し、証明書を使用するためです。証明書はカメラがドッキングするたびに、システムコントローラーからの最新のものと一致するように自動的に更新されます。

カメラがドックから外され、システムから4週間以上離れている場合、システムコントローラーは猶予期間として8週間、古い証明書を受け入れます。カメラそれ以上離れている場合は、マスターキーのパスフレーズを使用して、手動でシステムに再度接続する必要があります。これは、セキュリティ上のリスクを引き起こす可能性がある、紛失していたカメラや長期間ドッキングされていなかったカメラが気づかぬうちに再び追加されてしまうことのないようにするためです。

4 転送中のデータのセキュリティ

通常の使用では、BWCは任務終了後にドッキングされます。BWCには、ビデオとメタデータが格納されています。カメラをドッキングすると、HTTPS（TLSによるHTTP）接続による暗号化ネットワーク経由で、ドッキングステーションを介してすべてのデータがシステムコントローラーにオフロードされます。データは、AES-256により暗号化されたシステムコントローラーのSSDストレージデバイスに一時的に保存されます。次に、HTTPS接続経由で、システムコントローラーからデータがコンテンツ送信先に転送されます。



BWC (1) からコンテンツ送信先 (5) への安全なデータ転送と保管

1 *Axis Edge Vault搭載のBWC*
2 *署名付きビデオ（サイバーセキュリティ機能）*
3 *ドッキングステーション*
4 *Axis Edge Vault搭載のシステムコントローラー*
5 *コンテンツ送信先*

コンテンツ送信先が公開暗号化キーを提供している場合、コンテンツ送信先の暗号化キーを使用してBWCとシステムコントローラーのデータを暗号化する機能もサポートしています。この場合、コンテンツ送信先に送信されるデータに追加の暗号化レイヤーが加わります。

5 その他のセキュリティ機能

FIPS 140-2認証TPMを搭載していることで、システムコントローラーのセキュリティと整合性がより強化されます。

BWCとシステムコントローラーは、ハードウェアベースのサイバーセキュリティプラットフォームであるAxis Edge Vaultが搭載されており、デバイス上のすべてのデータを保護し、いくつかのセキュリティ機能を実現します。例えば、ファイルシステムは暗号化され、キーはAxis Edge Vaultによって保護されます。*セキュアブート*は、承認されたファームウェアでのみデバイスがブートできることを保証します。*署名付きファームウェア*は、ファームウェアの完全性が損なわれた場合、ファームウェアのアップグレードを拒否します。*署名付きビデオ*は、ビデオフレームに暗号化チェックサムを追加することで、追加の保護レイヤーを構築します。これにより、ビデオが録画された特定のAxisカメラまで遡って確実に追跡することができるため、映像が改ざんされていないことを確認することが可能となります。

署名付きビデオの詳細については、*www.axis.com/developer-community/signed-video*、Axisのサイバーセキュリティ機能の詳細については、*www.axis.com/solutions/built-in-cybersecurity-features*をご覧ください。

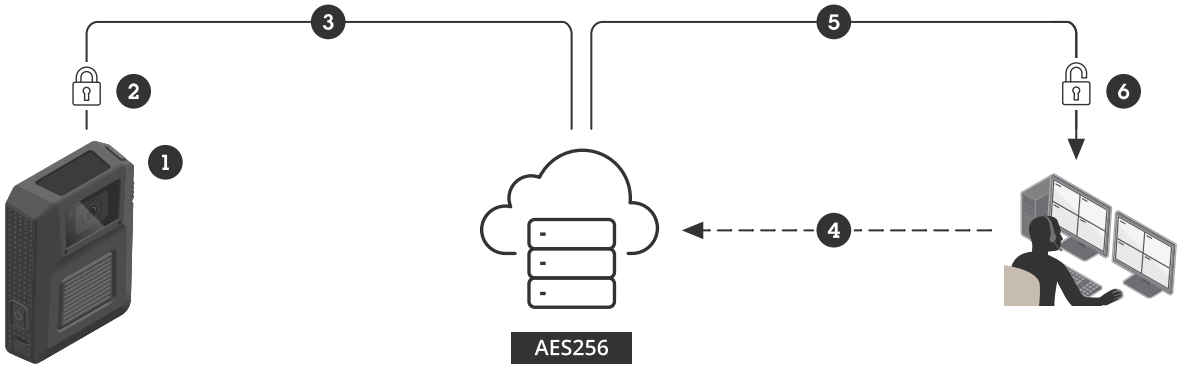
カメラユーザーが現場で録画ビデオを表示するには、AXIS Body Worn Assistantアプリケーションを使用しなければなりません。アプリケーションが有効になっている場合、BWCはアプリケーションに直接ビデオをストリーミングしますが、アプリケーションを実行しているデバイスのキャッシュやメモリーにビデオ素材を保存することはありません。また、ビデオストリームにはオーバーレイが表示され、二次的な録画デバイスによるキャプチャを抑止します。それでも録画が行われた場合、オーバーレイを介して、BWCユーザーまで遡ってビデオクリップを追跡することが可能となります。BWCのUSB-C対応コネクターは、ビデオの表示、削除、オフロードに使用することはできません。

6 AXIS Body Worn Liveによるセキュリティ

AXIS Body Worn Liveは、Axis装着式カメラのライブデータにアクセスできるアプリケーションです。AXIS Body Worn Liveは、映像、音声、位置座標などのデータのライブストリームをユーザーに提供することで、進行中のインシデントに関する比類ない状況認識を可能にします。最初はクラウドベースのサービスとして提供されます。

AXIS Body Worn Liveを使用すると、データは保存中（保管中）および転送中だけでなく、カメラと閲覧者のWebブラウザ間もエンドツーエンドで完全に暗号化されます。

AXIS Body Worn Liveでホストされるデータとファイルはすべて、保存時にAES-256で暗号化されます。すべての通信チャンネルは、信頼された認証局によって署名された証明書を使用し、TLSによるHTTPSで保護されます。また、AXIS Body Worn Liveは、XChaCha20-Poly1305プロトコルによる、真のエンドツーエンド暗号化のもう1つのレイヤーも追加します。



AXIS Body Worn Liveにおけるエンドツーエンド暗号化による安全なライブストリーミング

1. *BWCで、ライブビデオやその他のデータが収集されます。*
2. *データはBWCで暗号化されます。*
3. *データはBWCからAXIS Body Worn Liveに送信されます。*
4. *閲覧者はAXIS Body Worn Liveからのデータを要求します。*
5. *データはAXIS Body Worn Liveから閲覧者にストリーミングされます。*
6. *データは閲覧者のWebブラウザで復号化されます。*

装着式カメラシステムの管理者は、誰がライブストリームを視聴できるかを完全に制御することができます。暗号化されたデータを復号化して動画を視聴できるのは、管理者が承認した閲覧者のみとなります。また、管理者はアクセス権を取り消すこともできます。閲覧者は、適切なコンピューター、適切なWebブラウザ、適切なユーザー認証情報を備えている必要があります。他の誰も、Axisでさえもライブストリームにアクセスすることはできません。Axisは、ユーザーが作成したエンドツーエンドの暗号化キーにはアクセスできません。

Axis Communicationsについて

Axisはセキュリティとビジネスパフォーマンスを向上させるソリューションを生み出すことで、 よりスマートで安全な世界の実現を目指しています。 ネットワークテクノロジー企業として、 また業界のリーダーとして、Axisはビデオ監視、 アクセスコントロール、インターコム、音声システムなどのソリューションを提供しています。 これらのソリューションは インテリジェントな分析アプリケーションによって強化され、高品質のトレーニングに支えられています。

Axisは50ヶ国以上に約4,000人の熱意にあふれた従業員を擁し、 世界中のテクノロジーおよびシステムインテグレーションパートナーと連携することで、 カスタマーソリューションをお届けしています。 Axisは1984年に設立され、本社は スウェーデンのルンドにあります。