Durchgängige Verschlüsselung für vertrauliche Videodaten – Dank vimacc auch auf kostengünstiger Hardware

Viele Videoüberwachungsanlagen übertragen und speichern Videodaten unverschlüsselt. Das birgt Risiken für die Datensicherheit.

Mögliche Angriffspunkte sind das Netzwerk, dessen Datenverkehr mit Tools wie etwa WireShark mitgeschnitten werden kann, oder Festplatten bzw. Fileserver, auf die jeder Mitarbeiter mit Administratorrechten leicht zugreifen kann. Videos können auf diese Weise von Unbefugten exportiert und mit Standardtools wie etwa dem VLC-Player zur Anzeige gebracht werden.

In vielen Fällen ist deshalb eine durchgängige Verschlüsselung der Videodaten geboten, etwa um bei Verwendung von Speicher in der Cloud die Erfüllung von Datenschutzbestimmungen gewährleisten zu können, oder aber auch, wenn es um streng vertrauliche Daten - etwa interne Forschungsergebnisse großer Konzerne - geht, die auch von eigenen Mitarbeitern nicht unbefugt gesehen oder exportiert werden sollen.

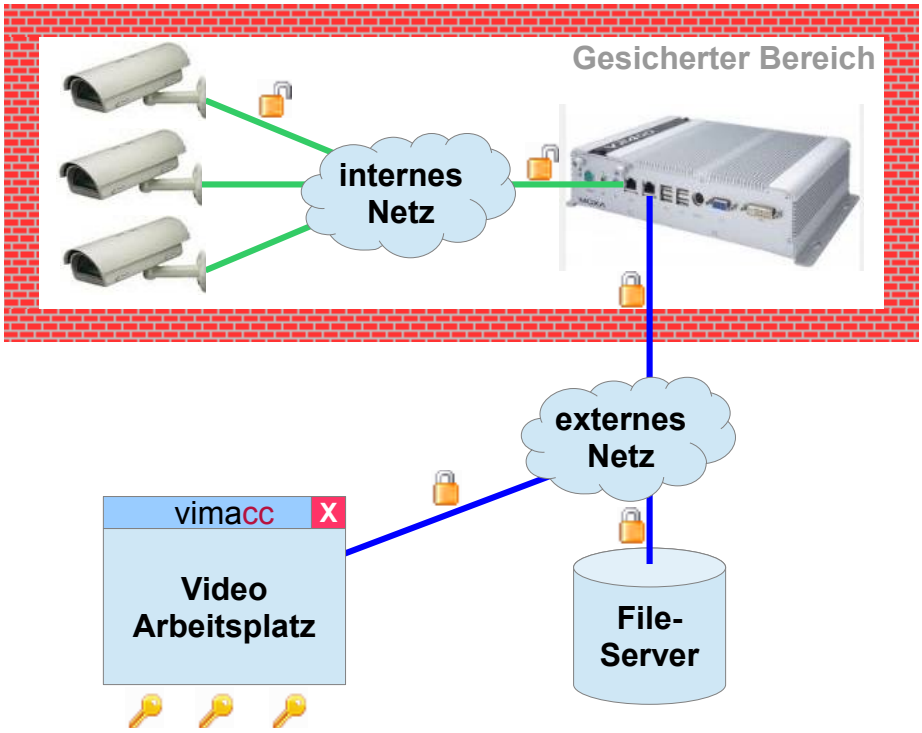
Es besteht die weit verbreitete Meinung, eine durchgängige Verschlüsselung aller Videodaten wäre viel zu aufwändig und teuer, benötige zu viel Rechenleistung. Deshalb lohnt sich ein Blick auf unsere Technologie:

Wir haben ein hybrides Verschlüsselungsverfahren, welches die hohe Sicherheit des asymmetrischen RSA für den Schlüsseltausch mit dem hohen Datendurchsatz von AES128 kombiniert, sehr effizient in optimiertem C++-Code implementiert. Auch bei begrenzter verfügbarer Rechenleistung können wir auf diese Weise eine derart gute Performance erzielen, dass eine konsequent durchgehende Verschlüsselung (end-to-end) vom gesicherten Bereich bis zum Arbeitsplatz des Betrachters bei minimalen Anforderungen an die Hardware möglich wird.

Nehmen wir als Beispiel den V2400 der Firma Moxa. Wir hatten dieses Gerät für ein Projekt gewählt, weil es unter anderem eine Bahnzulassung für den Einsatz in Schienenfahrzeugen besitzt:

Das Gerät verfügt über 2 Netzwerkanschlüsse, die wir zur Trennung des Kamera-Netzes vom Server-Netz nutzen. Auf der einen Seite schließen wir nur die IP-Kameras an, auf der anderen Seite geht es über LAN / WLAN zum Aufzeichnungsserver.

In der Praxis wird das so aufgebaut, dass diese Geräte in der benötigten Anzahl innerhalb des geschützten bzw. zu sichernden Bereichs (z.B. U-Bahn-Zug, Forschungslabor etc.) installiert werden, so dass von außen nicht auf die Kameras zugegriffen werden kann und **keine unverschlüsselten Daten den gesicherten Bereich verlassen**:



Nur wer über das Security-Token (wahlweise in Hard- oder Software) verfügt, kann das Videomaterial auswerten. Das Security-Token kann etwa in einem Schließfach hinterlegt werden, auf das nur unter ganz bestimmten Umständen mit exakt definierten Prozessen und Berechtigungen zugegriffen werden kann.

Die Freigabe kann zusätzlich an ein **4-, 6-, 8- ...-Augen-Prinzip** gekoppelt werden, d.h. nur alle Berechtigten gemeinsam (z.B. Sicherheitschef + Betriebsrat) können das Video-material zur Anzeige bringen und auswerten.

Unsere Software leitet gezielt nur die konfigurierten Videostreams weiter; alle anderen Datenströme und Zugriffe werden gesperrt.

Eine geeignete Hardware, auf der unsere Verschlüsselungs-Software läuft, kann je nach Systemauslegung z.B. wahlweise die Videostreams von bis zu

- 64 IP-Videokameras im PAL-Format oder
- 16 IP-Videokameras im Full-HD-Format

entgegennehmen, verschlüsseln, für die Aufzeichnung vorbereiten, paketieren und zum Server übertragen.

Als konkretes Beispiel maßen wir die CPU-Last, wenn auf einem Moxa V2400 gleichzeitig **60 Videostreams im PAL-Format** (4CIF@25fps = ca. 1Mbps) verarbeitet werden.

Die CPU-Last (Doppel-Atom-Prozessor N270@1,6GHz) beträgt dann

- ca. 40% ohne Verschlüsselung
- ca. 60% mit Verschlüsselung

Auf Client-Seite benötigen wir für die Anzeige verschlüsselter Videostreams nur ca. 30% mehr CPU-Leistung als für die Anzeige unverschlüsselter Videostreams. Verglichen mit dem Wettbewerb benötigen wir für die Anzeige verschlüsselter Videostreams sogar deutlich weniger CPU-Leistung als andere Produkte für die Anzeige unverschlüsselter Videostreams.

Unsere Software läuft sowohl Server- als auch Client-seitig sowohl unter Windows als auch unter Linux, gern auch auf der von Ihnen bevorzugten Plattform.

Eine sichere durchgängige Verschlüsselung ist also durchaus mit vertretbarem technischen Aufwand und zu überschaubaren Kosten machbar.

Falls Sie Interesse an diesem Thema haben, laden wir Sie herzlich zu einem Besuch bei uns ein, bei dem wir uns diese Möglichkeiten näher ansehen und darüber beraten können.

27.2.2014 Dipl.-Ing. Hardo Naumann