USE CASE

Secure live video without compromise

Ultra-low latency with live video encryption.

Key Customer Concerns

- Secure live video streams without loss of quality, latency, or compression
- Embed/integrate security at time of manufacture (OEM)
- Secure video both in-transit and at-rest
- Apply stronger security solutions, as existing protocols (TLS) have been proven flawed and subject to vulnerabilities
- Reduce cost and overhead of engineering security into devices and/or applications
- Apply security on extremely low power devices

Ubiq Benefits

- Any data can be protected including live streams
- Almost zero latency with Full HD video delays < 500 microseconds
- Low CPU overhead, even works on something as small as a Raspberry Pi
- Multithreaded to maximize bandwidth utilization
- Device authentication via pre-installed certificates
- Keys are rotated every 100KB to maximize security

Contact us to learn more!
www.ubiqsecurity.com

THE SITUATION

The global video streaming market size is anticipated to reach USD124.57 billion by 2025. This trend will escalate through the growing adoption of smartphones and devices, in combination with extensive range of high-speed Internet technologies such as 5G, has resulted in increasing data growth. Video streaming, more than any other communications tool, has the power to convey messages faster and more effectively to any accessible audience across the world.

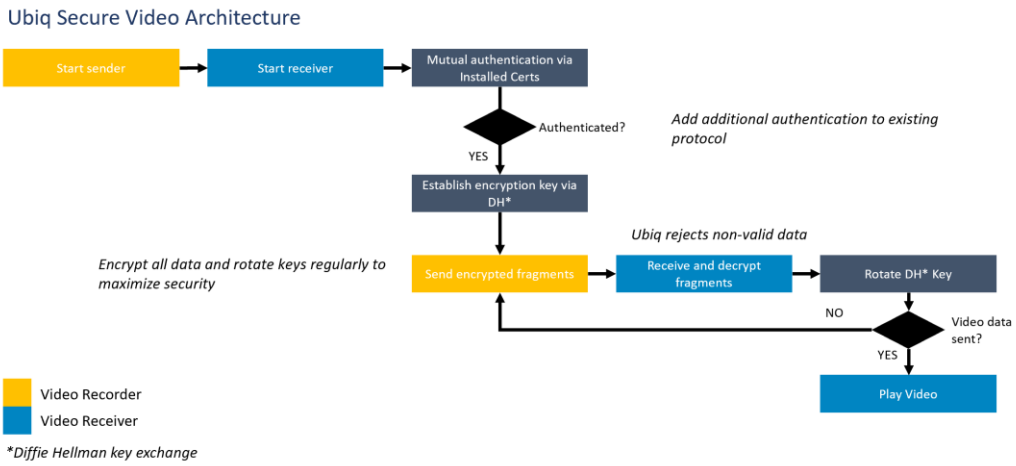
Video has also extended beyond a means communications and content delivery; businesses are starting to rely on video as an important source of business intelligence. Video feeds can be used for video analytics to trigger actions as part of a smart building or smart city. More often than not, the footage contains faces of people like you and I. Consumer privacy is an ever-growing concern, and has to be respected even before new regulations come in.

Streaming video and real-time surveillance are also used in situations which have serious consequences – in military and police field operations, natural disaster and emergency situations, providing medical guidance in remote locations, sending data to autonomous vehicles, the list is endless. If the streaming data is compromised by hackers in these instances, it could mean life or death. Whatever risks or stakes, the ability to better secure and transmit real-time data is essential.

CHALLENGES

Most of today's video streams are either unsecured or secured by TLS. While TLS provides authentication and encrypted transport, it comes with a price. The TLS protocol has been proven flawed and subject to vulnerabilities, allowing hackers to find their way into the private connection and exploit the data in numerous ways.

UBIQ



Even the latest version of TLS 1.3 is known to have major vulnerabilities allowing hackers to potentially eavesdrop on encrypted traffic, which is clearly a big risk for organizations.

Many modern applications also require ultra-low latency to maximize customer experience and ensure real-time operations of critical tasks. The problem will only grow as 5G networks eliminate the network bottleneck. Due to remote or isolated deployments the only solution to secure the video stream is to implement software directly onto the recording device such as an IP-enabled camera. These devices are extremely low power and cannot handle CPU intensive tasks like current encryption techniques.

HOW UBIQ (SDK) HELPS

Instead of using protocols such as TLS, which simply creates a private connection (or tunnel), Ubiq secures the data itself. We can use the same technology to secure data while in transit and when it's being stored (for archiving/replay) – as shown in the diagram above. Ubiq provides accelerated protected data transmission to ensure sensitive data gets to its intended destination.

- Any data can be protected including live HD streams
- Extremely low latency under < 500 microseconds
- Low CPU overhead, even works on something as small as a Raspberry Pi
- Multithreaded to maximize bandwidth utilization
- Device authentication via pre-installed certificates
- Keys are rotated every 100KB to maximize security

UBIQ SDK VERSUS TLS/SSL COMPARISON TABLE

Features	UBIQ SDK	TLS/SSL
Certificate-based authentication	✔	✔
Secure data in rest	✔	
Secure data immediately upon capture	✔	
Secure data in motion	✔	✔
Optional multi-path transmission	✔	
Encryption key rotation scheme	Every 100KB	Every session
Patching cycle	As and when vulnerabilities are discovered	Only upon major TLS updates
Library size*	10MB	50MB
Latency overhead	<1ms	>10ms

*Comparison of windows libraries

REAL-WORLD APPLICATIONS

Real time surveillance and monitoring of key locations and activities.

Real time streaming of patient data and VR imaging.

Real time transmission of car sensor data.

Maximize customer privacy and get data back in real time.

To find out more about Ubiq or to request a demo, visit www.ubiqsecurity.com

UBIQ