RIGA TECHNICAL UNIVERSITY

1862

RĪGAS TEHNISKĀ
UNIVERSITĀTE

Telecommunications Software

„VIDEO STREAMING APPLICATION ENCRYPTION SECURITY”

Practical work

Student: [Pedro Manuel Da Silva Vieira, 190ADB151]

Instructor: Mr. Viktors

Rīga, 2019.g.

Introduction

As time goes on, the streaming video market increases dramatically.

As a result, several security issues have begun to emerge due to the high number of existing piracy, hacking and other types of cyber attacks that are increasing year after year.

As video streaming tools evolved, new methods to preserve their security were emerging with the aim of ending possible virtual attacks.

There are currently some solutions, one of which is AES video encryption.

What is AES Video Encryption?

AES stands for Advanced Encryption Standard.

When the video is encrypted, a special key scrambles the video content. Unless the viewer has the correct access key, they can’t watch the video. Furthermore, if they try to intercept it, all they’ll see is a scrambled mess of useless data.

Encryption works by taking plain text and converting it into cipher text, which is made up of seemingly random characters. Only those who have the special key can decrypt it.

The encryption process is invisible, but provides a significant layer of protection against interception and piracy.

Who Needs AES Video Encryption?

AES video encryption can be extremely valuable to anyone who needs to keep video private. AES works in combination with password protection and signed keys to keep your videos as secure as possible.

Normally this type of tool is quite required in agencies like the government or enterprises, as there is extremely confidential information and therefore need to be protected so that no one can have access unless they have the appropriate information to do it.

However, anyone will be able to use these tools, as some content creators that sell online courses, need these videos to be unique to those who paid to watch them, so basically anyone who wants to keep their video content from being copied should consider AES video encryption.

This type of service is not cheap either. Piracy costs the U.S. economy more than $20 billion per year. The price tag internationally, however, is even bigger

Here are some examples that using AES Video Encryption:

- Government
- Enterprise
- SMB
- OTT and entertainment
- Education and eLearning
- Lawyers

Benefits of AES Video Encryption

AES video encryption prevents “Man-in-the-Middle” (MITM) style hacking attacks. In this type of attack, someone intercepts network traffic maliciously. They’re trying to steal sensitive data.

This type of cyber-attack often happens when we connect to a public Wi-Fi network and simply log in to some account, for example a bank account. This type of hacker can through this unprotected Wi-Fi network and get all the user data, so then you have exposed your financial details to this hacker.

AES video encryption allows you to halt these types of attacks completely. Anyone snooping on your streams will be stymied by AES encryption. This provides protection against piracy, data theft, intellectual property appropriation, and more.

Conclusion

We can conclude that with the advancement and popularization of video streaming, new security protection methods began to emerge, among them AES Video Encryption.

Through these new tools, it is becoming increasingly difficult to make virtual attacks on these devices that are now protected, further enhancing security through encryption of video streaming.

References

https://www.counterpath.com/security-encryption/

https://www.dacast.com/blog/aes-video-encryption/

https://www.ibm.com/downloads/cas/XWMNBMBV

https://www.atpinc.com/blog/what-is-aes-256-encryption

https://www.iconfinder.com/icons/527327/electronic_electronics_encryption_lock_secure_security_system_icon