Project code: BCSDS-13

Proposed title: ***Secure Stream (or Video) Authentication***

Supervisor and/or client(s): UOW

Project supervisor: Mr. Lai Soon Phin

Project description:

Summary

Video streaming technologies are becoming immensely important with the growth of the multimedia technology. With streaming or videos, the end user can start watching the file almost as soon as it begins downloading with a specific player. Security becomes a key problem to be handled when your valuable multimedia assets are floating over the network, simply because of the unsecured player beign used for the steaming of videos. This situation has increase the idea of stream alteration which has become very common in the IT world. This has created some concerns about how most web users want to secure their steams or videos. Most IT or computer users have used the advantage of the fact that streams or videos which are posted either on the net or being played by a specific player can be easily altered there by breaching its authentication rules. The parties that are affected are mostly advertisements by businesses, organizations and personal videos that are posted on the web for end users. With the consideration of this issue, there is the need to create a player that will help check the alteration of images. Therefore the above project title to be implemented can be summarized as a software project which can protect or secure a stream. For example, a movie in AVI format from any alterations that is no changes to be made. The idea behind the project depicts the main task of the project as well. It is to create a player which can be a specific player for a specific format and a converter that will convert an AVI or any other format to a specific format, then sign it to secure it. In addition to that, the created player should be able to carry out this task: If someone alters the file, then the player will show that the stream is no longer authentic. That means if one is able to apply a subtitle or add or remove a couple of frames from the stream, then these functions should lead to a correct detection of alterations.

Implementation:

The emphasis of this project is to develop an environment with security infrastructure that performs secure video streaming to users for the prevention of security threats through a player. Different techniques, algorithms and protocols to be are put together in such a way that they are providing a best security solution to the stream or video to make it authentic. The process of authenticatio, as the main concern of the project is done by allowing the network access to only authorized users, keys are generated through DH (Diffie-Hellman) key exchange mechanism, AES (Advance Encryption Standard) algorithm is used for data encryption, and then encrypted data is embedded into the SRTP (Secure Real-Time Transport Protocol) header. The SRTCP (Secure Real-Time Transport Control Protocol) Sender and Receiver reports are also generated for data acknowledgement. A keyed-hash algorithm is used to generate the MAC (Message Authentication Code) for every SRTP packet. After undergoing all these processes, the data is finally traveling over the network media.

A computer security standard Advance Encryption Standard (AES) is used for the encryption and decryption of data where the cryptography scheme is a symmetric block cipher that encrypts and decrypts data using 128 bit key. As an efficient encryption standard, it is currently being deployed on a large scale.

SRTP (Secured Real-Time Transport Protocol) is used for packetization of data as well as to enhance its security. In this scheme we first construct the SRTP packets by embedding the video data and then transmit them on the network media. SRTP (a profile of RTP) which can provide confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic of RTP(Real-Time Transport protocol) and RTCP (Real-Time Transport Control protocol) keyed-hash function is used to compute the MAC (Message Authentication Code) for every SRTP packet to authenticate the data traveling across the network. To achieve non-repudiation and real authentication, we would be relying on a conventional signature scheme, for example RSA [27] or Rohatgi's ktimes signature scheme.

Resources:

The necessary resources may include; A PC or a laptop. The preferred programming language to be used is the Java programming language. The hardware built in resources like the notepad and command prompt will be necessary. In addition an internet will be useful as well and will be needed.

Project Developers:

Francis Kyereh Twumasi (BCSUW) - Leader/Programmer

Abdulhayyu Lawal Hamisu (BCSDS) - Designer/Writer/Secretary

Chima Emmanuel (BCSDS) - Analyst/Tester