International J. of Engg. Research & Indu. Appls. (IJERIA).
ISSN 0974-1518, Vol.1, No. III (2008), pp 51-59

A MODERN APPROACH FOR MULTI-KEY SECURE MULTIMEDIA PROXY USING ASYMMETRIC REVERSIBLE PARAMETRIC SEQUENCES

E. JAYABALAN, A. KRISHNAN & R. PUGAZENDI

Abstract

Because of limited server and network capacities for streaming applications, multimedia proxies are commonly used to cache multimedia objects such that, by accessing nearby proxies, clients can enjoy a smaller start-up latency and receive a better quality-of-service (QOS) guarantee – for example, reduced packet loss and delay jitters for their requests. However, the use of multimedia proxies increases the risk that intruders expose multimedia data to unauthorized access. In this paper, a framework for implementing a secure multimedia proxy system for audio and video streaming applications. The framework employs a notion of asymmetric reversible parametric sequence (ARPS) to provide the following security properties:

(i) Data confidentiality during transmission,

(ii) End-to-end data confidentiality,

(iii) Data confidentiality against proxy intruders,

(iv) Data confidentiality against member collusion.

Our framework is grounded on a multi-key RSA technique such that system resilience against attacks is provably strong given standard computability assumptions.

One important feature of our proposed scheme is that clients only need to perform a single decryption operation to recover the original data even though multiple proxies along the delivery path may have encrypted the data packets. On proposing the use of a set of encryption configuration parameters (ECP) to trade off proxy encryption throughput against the presentation quality of audio/video obtained by unauthorized parties. Implementation results show that we can simultaneously achieve high encryption throughput and extremely low video quality (in terms of peak signal-to-noise ratio and visual quality of decoded video frames) for unauthorized access.

Keyword: audio, asymmetric reversible, clients, encryption, multimedia data, multimedia object, multimedia proxy, packet, video, streaming, and server.