Research Statement of LO Swee Won

sweewon.lo.2009@smu.edu.sg

The pervasiveness of multimedia applications, and hence the large-scale dissemination of multimedia content through the public and open networks have drawn security concerns for both the users as well as the media owners. In particular, the authenticity of the disseminated multimedia content - whether it has been maliciously tampered with (by modifying, deleting or inserting media data) when in transit - is in question. Verifying the authenticity of the disseminated multimedia content will thwart tampering motivated by political, social, commercial or even personal purposes.

The design of an efficient authentication scheme for modern multimedia streams is met with the following challenges: (1) The inherent structure (i.e. the type of encoding) of the multimedia stream to be protected; (2) The lossy nature of the wired or wireless networks; (3) The need of the authentication scheme to be transparent to any intermediary proxies performing transcoding operations.

The structure of a multimedia stream is affected by the type of encoding used. The fact that a multimedia stream should cater for heterogeneous receivers, each with different decoding capability and on different network bandwidth motivates the standardization of "scalable multimedia encoding" standards. The widely used JPEG-2000 and MPEG-4 as well as the recently standardized H.264/Scalable Video Coding (SVC) standards are examples of scalable encoding standards for multimedia streams. These standards achieve the property of "encode once, decode many ways" to support heterogeneous user device capabilities and network conditions, i.e. a subset of the multimedia stream forms another valid stream that requires less decoding complexities and consumes lower bandwidth. As such, an efficient authentication scheme must be able to "scale" with the multimedia stream.

Secondly, the authenticity of multimedia stream should remain verifiable even when under packet loss condition of the network. The authentication scheme should ensure that packets that are received be verifiable (and hence contribute to the overall reconstructed quality of the multimedia content. Hence, the authentication scheme must be tolerant to packet loss. Note that the case of packet loss is different from the proxy transcoding operations where an intermediate proxy discards a portion of the multimedia stream for receivers with lower decoding capabilities.

Finally, it is a common practice that within a network, there exist intermediate proxies that are performing transcoding to the multimedia stream to suit the decoding capabilities of end devices or adding content such as subtitles or company logo for video streams. Such legitimate modification, insertion or deletion of multimedia content should be accommodated by the authentication scheme. For an intermediate proxy serving a large number of receivers, it is important to design an authentication scheme that is transparent to the proxy to facilitate the transcoding operations.