Data Encryption Algorithms for Internet-based Real-Time Systems

Li Hongyan [1,2], Shuang H. Yang[1,3], and Tan LianSheng [1]
[1]Department of Computer Science, Central China Normal University, Wuhan, China.
[2] Department of Computer and Electronic Science, Hubei University of Economics, Wuhan, China
[3]Department of Computer Science, Loughborough University, Loughborough, Leicestershire LE113TU, UK
Email: lhywawa@sohu.com, s.h.yang@lboro.ac.uk, 1.tan@ccnu.edu.cn

ABSTRACT

In recent years, the Internet has proved to be a powerful tool for real-time applications. However, security risk of the Internet communication still stops people to bring the real-time application into a reality. Little work has so far been done in developing a data encryption algorithm for Internet-based real-time applications. In order to satisfy the security requirements of Internet-based real-time systems, two hybrid data encryption algorithms are proposed. One is the combination of the Advanced Encryption Standard (AES) and the most popular public-key cryptography (RSA); the other is the combination of the AES and Secure Sockets Layer (SSL). The end-to-end encryption latency of different algorithms is investigated to show the efficiency of the two new algorithms for Internet-based real-time applications.

Keywords: real-time Systems, Encryption Algorithm, AES, RSA, SSL.

* Corresponding author, Hong-Yan Li, master in Computer Science Department at Central China Normal University.