CORR 2002-31

Controlled Proxy-assisted Secure End-to-End Communication

Hung-Yu Lin*

Abstract Current status on communication security
Communication security has always been one of the major concerns in network applications. Many mechanisms have been developed to improve the security of communications over the Internet. For example, IP Security (IPSec) implements security mechanisms in IP to provide a general-purpose transparent solution to upper layer applications. Secure Socket Layer (SSL) or Transport Layer Security (TLS) implements security mechanisms on top of TCP for HTTP, SMTP, and FTP. Other application-specific protocols, like PGP, PEM, and S/MINE for secure emails, Kerberos for authentication service, and Secure Electronic Transaction (SET), etc, are also available to provide application-specific security services for their users [1].

Note that these security services mainly are designed for TCP/IP networks and the client-server computation paradigm. Also they assume that users have adequate computation resource, including hardware, software, and communication bandwidth, to carry out the required operations. For wireless networks users who communicate through simple handheld devices or mobile users who travel away from their computer/network, they may not have adequate computation resource and could therefore temporarily lose the support of these security services. In fact, there is no support yet for two users, either on Mobile IP networks or commercial wireless networks, to conduct a secure communication. Commercial support for the secure end-to-end Voice over IP (VoIP) is not yet available either.