Identity Authentication for Open Network

廖國宏、顏嵩銘

E-mail: 8515721@mail.dyu.edu.tw

ABSTRACT

Nowadays, wider usage of computer networks makes the life more convenient. However, more and more attacks are happening in the network to threaten human privacy. If the network can not authenticate the users correctly, then anunauthorized user can impersonate a legal user to access system resources inspite of the presence of other security mechanisms (for example, access control or login log) in the system. Identity authentication is particularly important for an open network in which mutually untrusted nodes and insecure channels give malicious users more chances to impersonate other users. In this thesis, we first introduce the aspects of public key infrastructure including X.509, Certification Authority, Directory Service, PEM, PGP, and self-certified public key. A secure and efficient protocol -- Zeus is then proposed for identity authentication in the open network. Furthermore, an authentication device which can be shared by many users is proposed for general purpose one-time password system. Finally, we implement a PGPcTalk program to provide real-time communication in the UNIX enviroment. This program can not only protect the contents of talk but also authenticate each user''s identity.

Keywords : PEM ; PGP ; Public Key Infrastructure ; Privacy Enhanced Mail ; Pretty Good Privacy ; Hash Function ; Symmetric algorithm ; Asymmetric algorithm

Table of Contents