Design and Implementation of Security Services for Computer Networks

By:

Mohammad Abdollahi Azgomi

Advisor:

Dr. Ali Movaghar

M.S. Thesis,

Department of Computer Engineering,

Sharif University of Technology, 1996

Abstract. Computer networks are the most susceptible to intrusions and illegal interceptions in the new technologies. Because of that, security and its fulfillment is of high importance in the operation of computer networks. One of the approaches for establishing security in networks is "to prepare security services in the application layer of the OSI reference model". This perspective has been nominated in this thesis as a privileged methodology on implementing security. The implementation of "security server in a security domain" is our practical solution for this purpose. In addition to implementation of the basic security mechanisms and services, a prototype of the *Kerberos* authentication model and secure versions for three major services of networks (e-mail, file transfer, and remote login) is developed. For the *secure e-mail*, the PAS* software is developed. PAS is on the basis of PEM standard, and prepares integrated mailing and privacy functionalities, with Farsi language support. A new protocol for *secure file transfer* is introduced and its development is based on client/server architecture. For *secure remote login*, a special authentication method is designed and implemented. Another notable result of this project is the development of a *secure application programs interface (API)* that could be used to develop other secure services and applications.

In this thesis, the fundamentals of security of the computer systems, as well as illegal interceptions and intrusions in computer networks, security models, evaluation of security in networks, and a new criteria for evaluation of secure services are also introduced.

Keywords. Computer networks, security, cryptography, authentication, digital signature, security services, security mechanisms, Kerberos, secure electronic mail, secure file transfer, secure remote login, security models, security evaluation.

* PAS is an abbreviation in Persian