Trusted Information Systems

Secure External Access and Service

Providing Protection for the Network

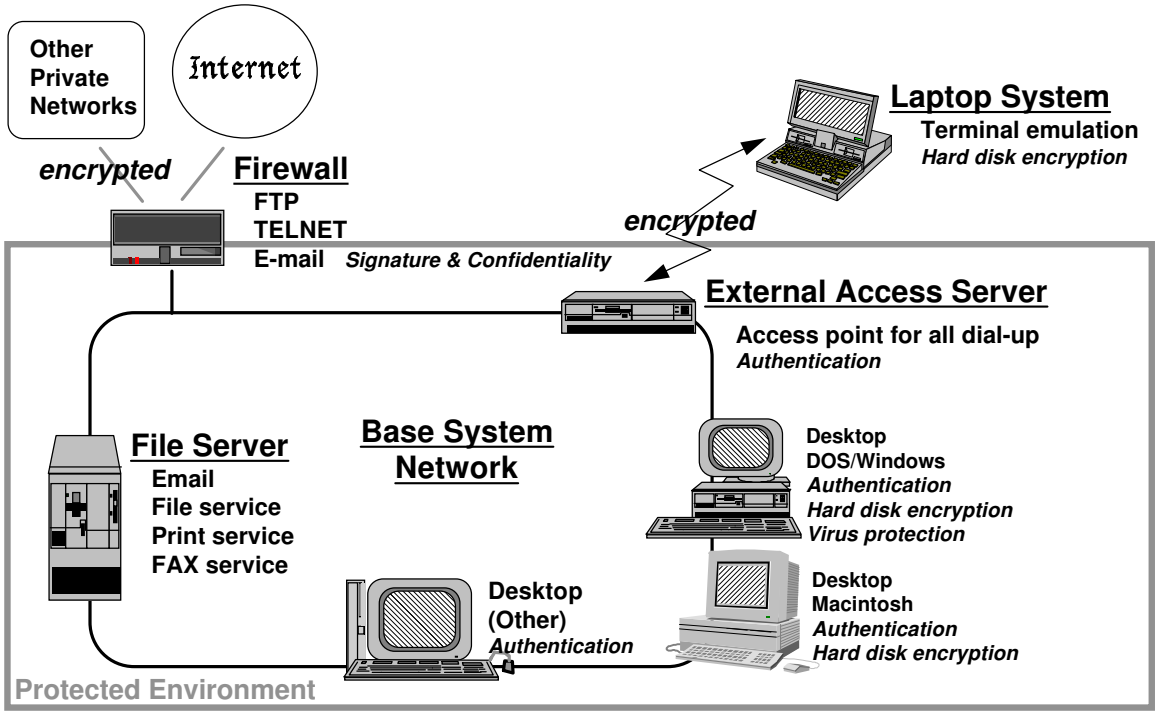
The Requirement

A private network that carries sensitive data among local computers requires proper security measures to protect the privacy and integrity of the traffic. When such a network is connected to other networks, or when telephone access is allowed into that network, the remote "terminals," phone lines, and other connections become extensions to that private network and must be protected accordingly. In addition, the private network must be protected from outside attacks that could cause loss of information, breakdowns in network integrity, or breaches in security.

The Problem

While security is important, security measures that are onerous or cumbersome often end up being circumvented by legitimate users of the network in order to get their work done. Because of this, usability — or "user friendliness" — in security features is of the utmost importance.

The Solution



The Solution

Trusted Information Systems, Inc. (TIS) has extensive experience in providing solutions that provide for strong user authentication, access control, and integrity protection for data on private (isolated) networks (or collections of networks). These solutions also support the secure connection of private networks to external internetworks, as well as dial-up network connections, via firewalls and secured links, with authentication and encryption of traffic. We use a combination of commercial off-the-shelf (COTS) software, as well as software we developed for this purpose.

Secure Internet Connection: the TIS Firewall Toolkit. TIS has developed a toolkit for building secure, but flexible, Internet firewalls in a variety of configurations. Built into the firewall is logging, electronic mail gateway services, Domain Name Service, an FTP gateway proxy, a TELNET gateway proxy, an internet service access control server, and a generic pass-through plug gateway.

User Authentication. The National Computer Security Center's "red book" defines authentication as "(1) to establish the validity of a claimed identify or (2) to provide protection against fraudulent transactions by establishing the validity of ... an individual..." Identification of a user is often accomplished on computers through the use of a user name and password pair. More secure solutions usually include one-time passwords and challenge/response systems. These methods should be used for all applications requiring strong user authentication.

File Integrity and Protection. Through the use of encryption and access control based on strong user authentication, computer and file access may be limited and controlled.

Secure Electronic Mail. To secure e-mail, additional security measures are desirable, especially for official business. Privacy Enhanced Mail (PEM) provides three essential features necessary for official business: integrity, authentication and non-repudiation, and privacy. Trusted Mail® is available for individual use, or to run on mail gateways.

Encrypted Remote Communications. Protection of remote connections to the campus network can be done in several ways, all involving encryption: encrypted TELNET, encrypted terminal emulation, encrypted Serial Line IP, and point-to-point network encryption.

For further information please send electronic mail to *netsec@TIS.COM*, call (301) 854–6889, Fax to (301) 854–5363, or write to: Trusted Information Systems, Inc., ATTN: Network Security, 3060 Washington Road, Glenwood, MD 21738.