FORBSBC

Directory and File Transfer Services

- Chapter 7

Learning Objectives

- Explain benefits offered by centralized enterprise directory services such as LDAP over traditional authentication systems
- Identify major vulnerabilities of the FTP method of exchanging data
- Describe S/FTP, the major alternative to using FTP, in order to better secure your network infrastructure
- Illustrate the threat posed to your network by unmonitored file shares

Directory Services

- Network services that uniquely identify users and can be used to authenticate and authorize them to use network resources
- Allow users to look up username or resource information, just as DNS does

Lightweight Directory Access Protocol (LDAP)

- Accesses directory data based on ISO's X.500 standard, but includes TCP/IP support and simplified client design
- Exchanges directory information with clients (is *not* a database that stores the information)
- Allows users to search using a broad set of criteria (name, type of service, location)

FORBSBC

continued…

LDAP

- Provides additional features including authentication and authorization
  - Each person uses only one username and password regardless of client software and OS
- Key feature and benefit
  - Versatile directory system that is standards based and platform independent

FORESEC

Major LDAP Products

Table 7-1 Major LDAP products

Vendor	Product
Microsoft	Active Directory
Sun	ONE Integration Server (formerly Netscape iPlanet)
IBM	Directory Server
Novell	eDirectory
MessagingDirect	M-Vault
Opensource	OpenLDAP

Common Applications of LDAP

- Single sign-on (SSO)
- User administration
- Public key infrastructure (PKI)

LDAP Operations

Table 7-2 Summary of LDAP operations

LDAP Operation	Description
Open	Establish a connection with one of a list of hostnames or IP addresses on the target LDAP servers; connection attempts are executed sequentially until one is successful
Bind	Authenticate a client to the LDAP server; three types of bind are supported: no authentication, simple authentication, and Simple Authentication and Security Layer (SASL)
Search	Search the directory, with a filter if desired. Returns matching entries for each requested attribute. Wildcards allow you to simulate the ability to list the children of an entry
Modify	Modify an existing LDAP entry
Add	Add entries to the directory; if necessary, the add operation creates an attribute that does not already exist in the directory
Delete	Delete entries from the directory
Modify DN	Change distinguished names
Abandon	Discontinue an operation that is in progress

LDAP Framework

- Directory Information Tree (DIT)
  - Data structure that actually contains directory information about network users and services
  - Hierarchical structure

Directory Information Tree

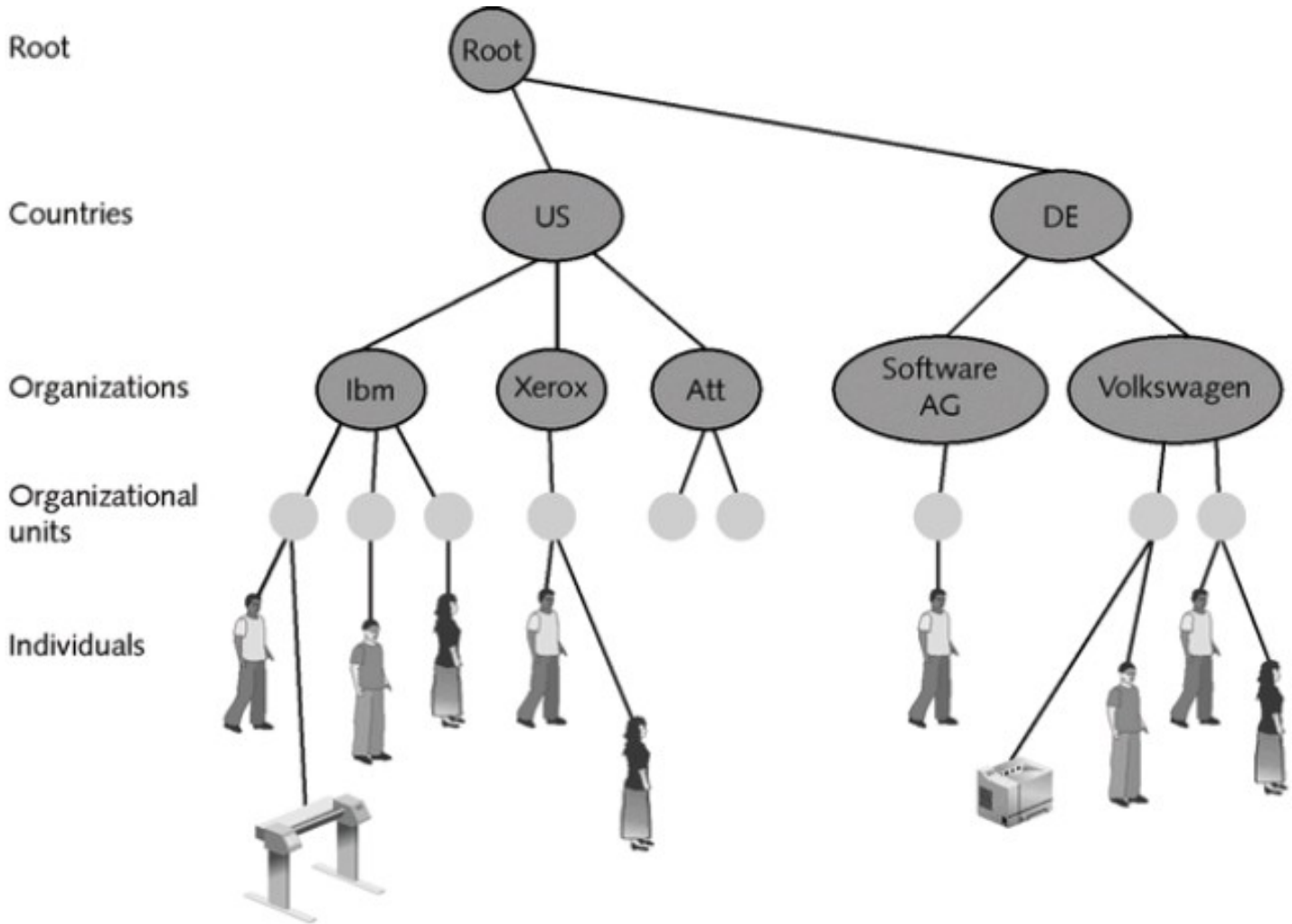

Figure 7-1 Directory Information Tree

LDAP Framework

- DN example
  - cn=Jonathan Q Public
  - ou=Information Security Department
  - o=XYZ Corp.
  - c=United States

Table 7-3 Some LDAP/X.500 abbreviations

DN	Distinguished name
CN	Common name
C	Country
O	Organization
OU	Organizational unit
DC	Domain name component

LDAP Security Benefits

- Authentication
  - Ensures users' identities
  - Three levels
    - No authentication
    - Simple authentication
    - Simple Authentication and Security Layer (SASL)
- Authorization
  - Determines network resources the user may access
  - Determined by access control lists (ACLs)
- Encryption
  - Utilizes other protocols through (SASL)

LDAP Security Vulnerabilities

- Denial of service
- Man in the middle
- Attacks against data confidentiality

File Transfer Services

- Ability to share programs and data around the world is an essential aspect of the Internet
- Critical to today's networked organizations

File Transfer Protocol (FTP)

- Commonly used but very insecure
- Two standard data transmission methods – active FTP and passive FTP
  - In both, client initiates a TCP session using destination port 21 (command connection)
  - Differences are in the data connection that is set up when user wants to transfer data between two machines

Setup of FTP Control Connection

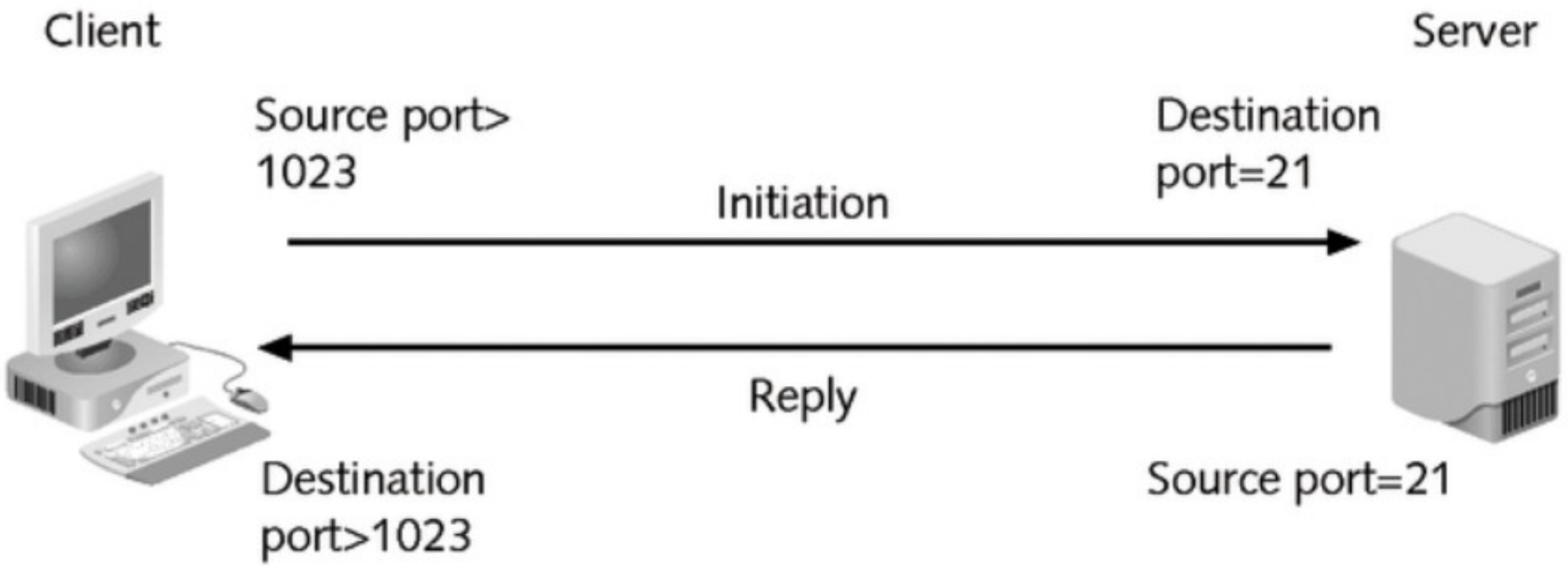

Figure 7-2 Setup of the FTP Control Connection

Active FTP

- FTP's default connection
- FTP server creates data connection by opening a TCP session using source port of 20 and destination port greater than 1023 (contrary to TCP's normal operation)

Setup of the Active FTP Data Connection

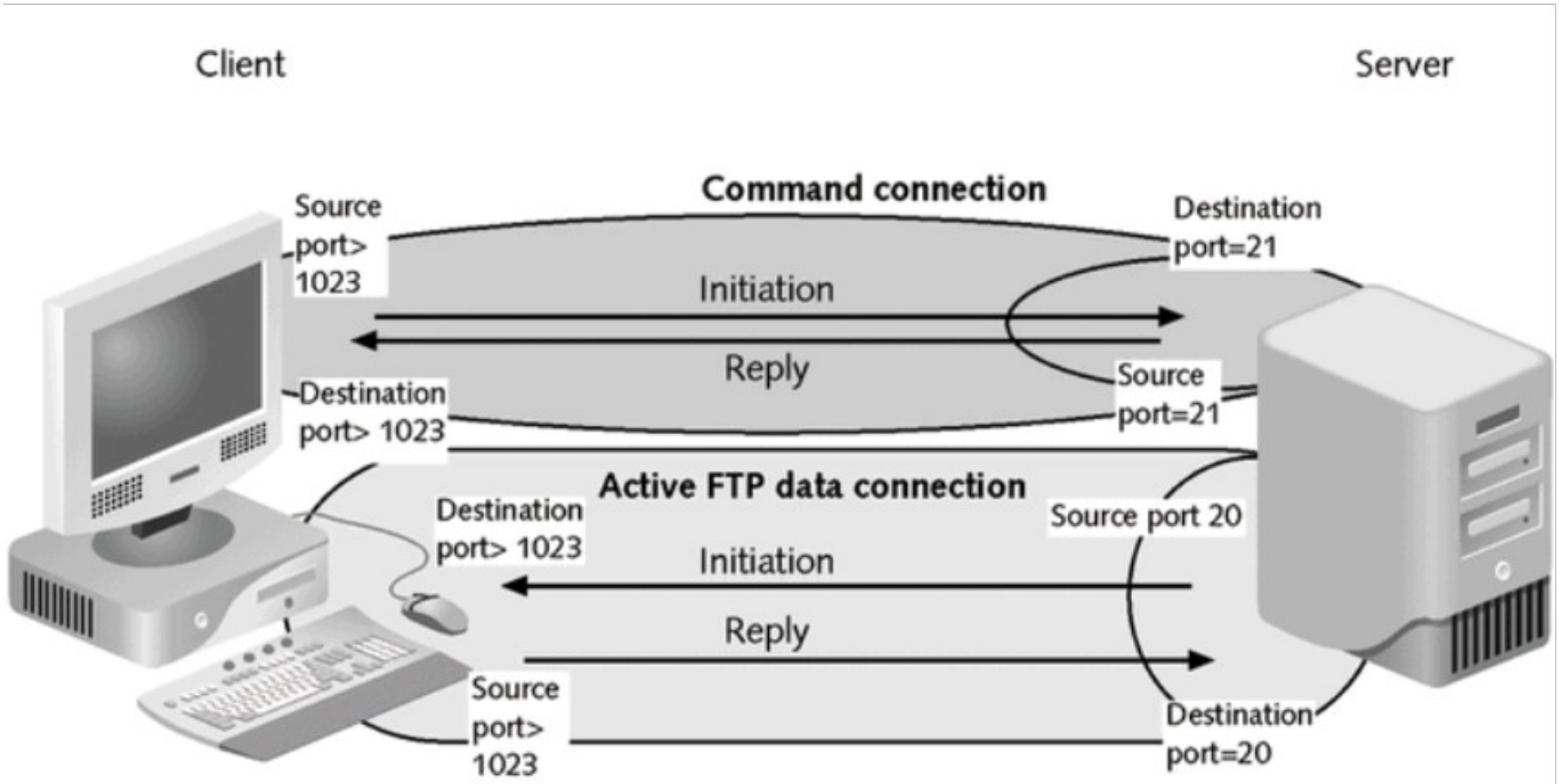

Figure 7-3 Setup of the active FTP data connection

Passive FTP

- Not supported by all FTP implementations
- Client initiates data connection to the server with a source and destination port that are both random high ports

Setup of the Passive FTP Data Connection

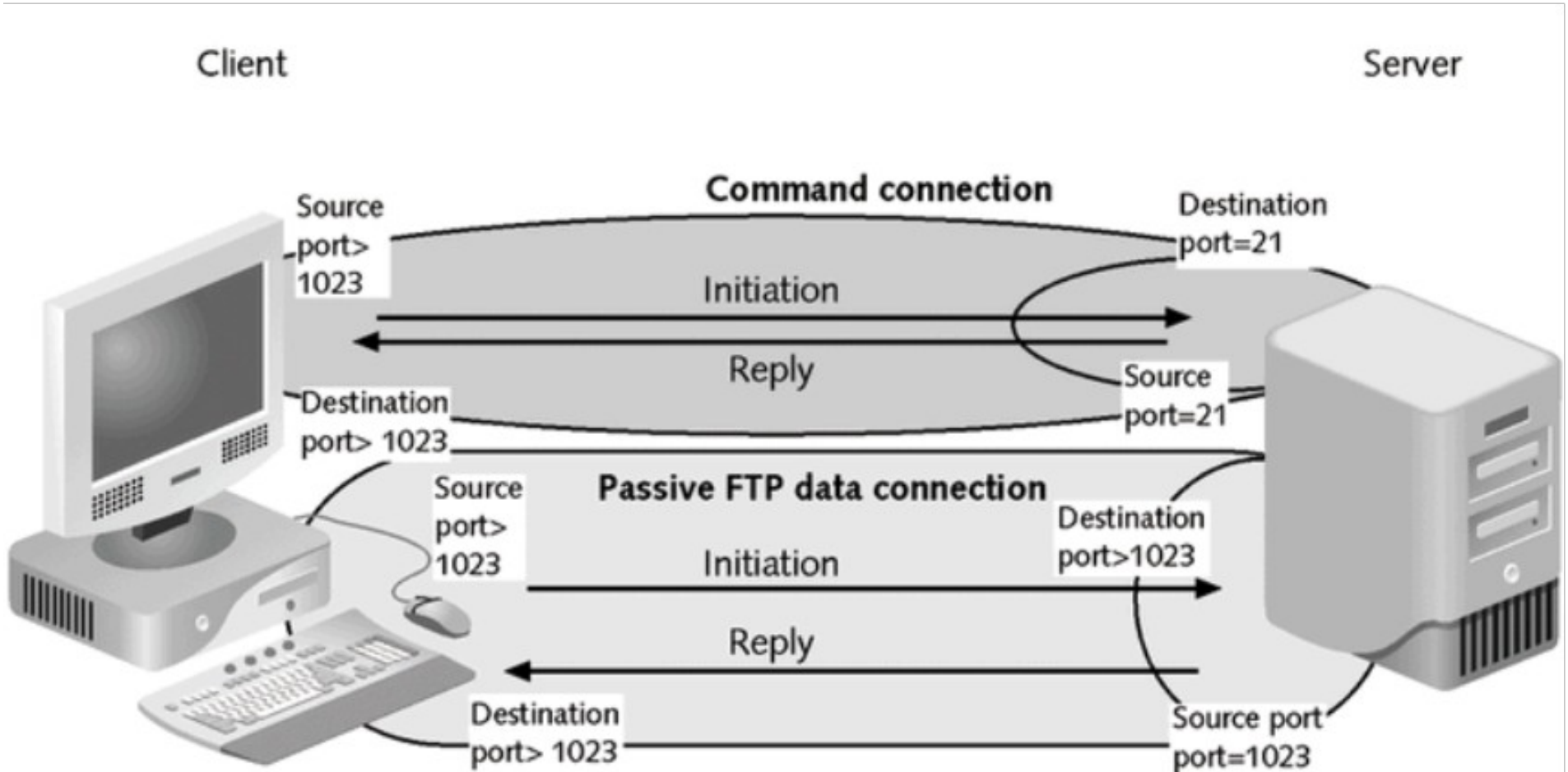

Figure 7-4 Setup of the passive FTP data connection

FORESEC

FTP Security Issues

- Bounce attack
- Clear text authentication and data transmission
- Glob vulnerability
- Software exploits and buffer overflow vulnerabilities
- Anonymous FTP and blind FTP access

FTP Countermeasures

- Do not allow anonymous access unless a clear business requirement exists
- Employ a state-of-the-art firewall
- Ensure that server has latest security patches and has been properly configured to limit user access
- Encrypt data before placing it on FTP server

continued…

FTP Countermeasures

- Encrypt FTP data flow using a VPN connection
- Switch to a secure alternative

FORESEC

Secure File Transfers

- Secure File Transfer Protocol (S/FTP)
  - Replacement for FTP that uses SSH version 2 as a secure framework for encrypting data transfers

Benefits of S/FTP over FTP

- Offers strong authentication using a variety of methods including X.509 certificates
- Encrypts authentication, commands, and all data transferred between client and server using secure encryption algorithms
- Easy to configure a firewall to permit S/FTP communications (uses a single, well-behaved TCP connection)
- Requires no negotiation to open a second connection

FORESEC

SecureFTP Implementation Programs

Table 7-4 SecureFTP implementations

Program	Link	Note
SSH	*http://ssh.com/products/ssh/download.cfm*	The SSH product produced by the company of the same name, offering both server and client software
OpenSSH	*www.networksimplicity.com/openssh/*	An open source version of SSH, primarily operated by the OpenBSD group
TTSSH	*www.zip.com.au/~roca/ttssh.html*	A free SSH client implementation that requires the freeware TeraTerm terminal program
PuTTY	*www.chiark.greenend.org.uk/~sgtatham/putty/*	A freeware SSH client implementation for Windows operating systems

File Sharing

- Originally intended to share files on a LAN
- Easy to set up
- Uses Windows graphical interface
- Can be configured as peer-to-peer or as client/server shares

Figure 7-5 File sharing in Windows XP

File Sharing Risks

- Confidentiality of data
- Some viruses spread via network shares
- Other types of critical information beside user documentation could become compromised if files shares are misconfigured

Protecting Your File Shares

- Define and communicate a policy
- Conduct audits of file shares using commercial scanning and audit tools

Chapter Summary

- Key resources used to support mission-critical business applications
  - Directory services
    - LDAP
  - File transfer mechanisms
    - FTP
    - S/FTP