

Introduction to LAN

TDC 363

Lecture 09

Network Security (Chap. 14)

03/06/08

TDC363-09

1

Course Outline

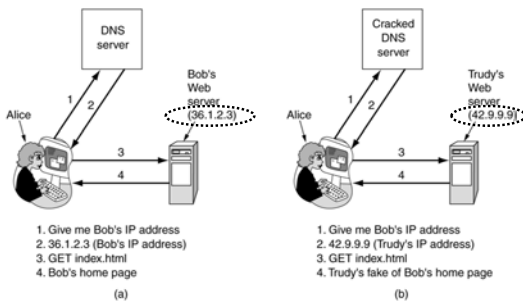
- Identifying security risks in the network
 - People, Hardware, Software, and Internet
 - Examples of security attacks
- Addressing security risk
 - Security policy
 - Firewall, Proxy Server, RAS, and RADIUS
 - User Authentication
 - Encryption
 - Private Key and Public Key
 - Kerberos
 - PGP
 - SSH
 - IPSec

03/06/08

TDC363-09

2

Example of Security Problem



03/06/08

TDC363-09

3

Terminology

- A **hacker** is someone who masters the inner workings of operating systems and utilities in an effort to gain inside/private information. (ref. p. 711)
- A **cracker** is someone who uses his or her knowledge of operating systems and utilities to intentionally damage or destroy data or systems
- **root** account (UNIX) and **administrator** account (Windows)
- **Authentication – Who are you?**
 - The process of reliably determining the genuine identity of the communicating nodes or users.
- **Authorization – What can you do?**
 - The process of determining the access rights of authenticated users.

03/06/08

TDC363-09

4

Need for Security

Some people who cause security problems and why.

- Student: have fun snooping on the network (reading others' e-mails)
- Cracker: Test/attack the security of the system.
- Business: industry espionage
- Ex-employee: get revenge
- Accountant: embezzle \$\$\$ from a company
- Con man: steal credit card info for sale
- Spy:
- Terrorist:

Ref. Tanenbaum p. 722

03/06/08

TDC363-09

5

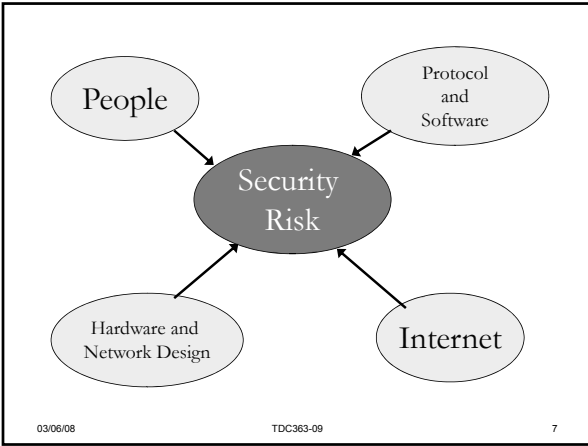
Security Audits

- Security audit is an activity that assesses an organization's security risks
- When
 - Regular: annual or quarterly
 - Irregular: conduct a security audit after making any major changes to the network
- It is common to hire a hacker to conduct a security audit.

03/06/08

TDC363-09

6



Security Risks w/ People

- Network administrators overlooking security flaws in topology or hardware configuration
- Network administrators overlooking security flaws in operating system or application configuration
- Lack of proper documentation and communication of security policies
- Dishonest or disgruntled employees abusing their file and access rights
- An unused computer or terminal being left logged into the network

03/06/08 TDC363-09 8

Security Risks w/ People (cont.)

- Users or administration choosing easy-to-guess passwords
- Authorized staff leaving computer room doors open or unlocked
- Staff discarding disks or backup tapes in public waste containers
- Administrators neglecting to remove access files and rights for former employees
- Users leaving passwords out in open spaces

03/06/08 TDC363-09 9

Risks Associated with Hardware and Network Design

- Wireless transmission can typically be intercepted
- Network hubs broadcast traffic over the entire segment, vulnerable to **sniffing**.
- Unused ports on hubs, switches, routers, or servers can be exploited.

03/06/08

TDC363-09

10

Risks Associated with Hardware and Network Design (cont.)

- If routers are not properly configured, outside users can sneak into the private network.
- Dial-in access servers used by telecommuting or remote staff may not be carefully secured and monitored.
 - No modem connection on desktop.
- Computers hosting very sensitive data may coexist on the same subnet with computers open to the general public.

03/06/08

TDC363-09

11

Risks Associated with Protocols and Software

- TCP/IP contains several security flaws
 - IP Addresses can be falsified (spoofing)
 - UDP requires no authentication.
- Trust relationships between one server and another may allow a cracker to access the entire network because of a single flaw
- Network operating system software typically contains “backdoors” or security flaws

03/06/08

TDC363-09

12

Risks Associated with Protocols and Software (cont.)

- Command line interface is convenient for administrators, and it is also convenient for intruders who could run destructive programs in a batch/background mode.
- Administrators might accept the default security options after installing an operating system or application
 - You may be surprised how many routers (or even servers) on the public network are using the default login and password.
- Transactions that take place between applications may be left open to interception

03/06/08

TDC363-09

13

Risks Associated with Internet Access

- **IP spoofing**
 - Outsiders obtain internal IP addresses, then use those addresses to pretend that they have authority to access your internal network from the Internet
- When a user Telnets or FTPs to your site over the Internet, his or her user ID and password will be transmitted in plain text. (subject to **sniffing**)
- Attackers may obtain information about your user ID from newsgroups, mailing lists, or forms filled out on the Web

03/06/08

TDC363-09

14

Risks Associated with Internet Access (cont.)

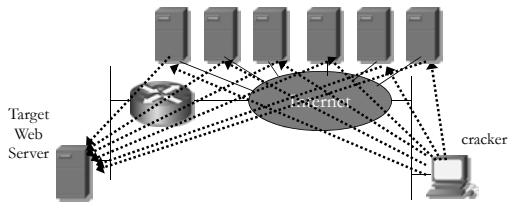
- **Flashing:** Internet user send commands to another Internet user's machine that cause the screen to fill with garbage characters
 - Example, pop-up menu
- **Denial-of-service (DOS)** attack
 - Occurs when a system becomes unable to function because it has been deluged with messages or otherwise disrupted

03/06/08

TDC363-09

15

DoS - ping



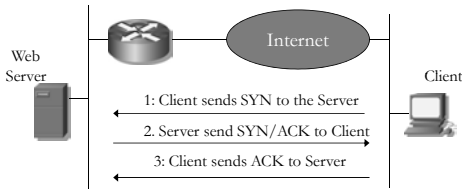
A cracker sends millions ICMP packets from his workstation to different machines on the Internet, where the source IP address of the packet is falsified (spoofed) as the web server. All machines then echo the ICMP message to the web server. As the web server is flooded with ICMP messages, it will not have the capability to process real IP packets.

03/06/08

TDC363-09

16

TCP SYN

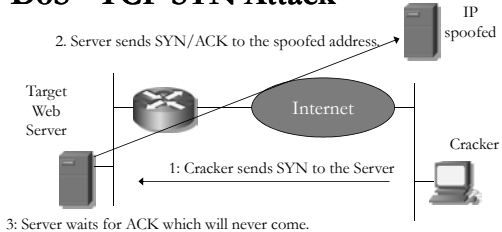


03/06/08

TDC363-09

17

DoS - TCP SYN Attack



If a cracker continuously sends SYN message with a falsified (spoofed) source IP address, the server would never get an ACK message back from the cracker. All SYN requests are put in the TCP buffer. When the buffer is full, the server cannot accept any more TCP requests.

03/06/08

TDC363-09

18

Addressing Security Risk

03/06/08

TDC363-09

19

Security Policy

- Why do you need a security policy?
 - Provide authorized users to access to the resources.
 - Protect unauthorized users from gaining access to the network, systems, programs, or data
 - Prevent accidental damage to hardware or software
 - Prevent intentional damage to hardware or software
 - Create an environment to withstand and quickly recover from any type of threat
 - Communicate employee's responsibilities with respect to maintaining data integrity and system security

03/06/08

TDC363-09

20

Security Policy - Passwords

- What you can enforce in NOS:
 - Password cannot be derived from user information
 - Password cannot be found in a dictionary
 - Password must be longer than n ($n > 8$) characters
 - Password must contain both letters and numbers
 - Password must be changed every n ($n < 30$) days
 - Password cannot be changed within n ($n < 24$) hours
 - New password must be significantly different ($> 50\%$) from the last n ($n > 2$) passwords.
- What you cannot enforce in NOS:
 - Do not write down your password or share it with others
 - Do not send passwords in an "unencrypted" way over the network.

03/06/08

TDC363-09

21

Physical Security

- Physical access to the network device
 - Computer room
 - Control room
 - Storage room
- Access control
 - Key
 - Badge or smart cards
 - Bio-recognition

03/06/08

TDC363-09

22

Addressing Risks Associated with Hardware and Design

- Firewall
 - Specialized device that selectively filters or blocks traffic between networks

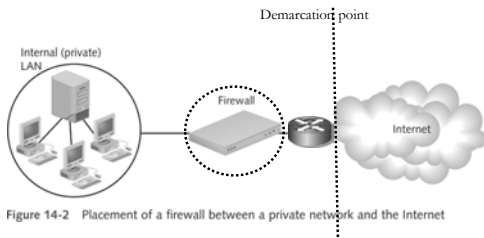


Figure 14-2 Placement of a firewall between a private network and the Internet

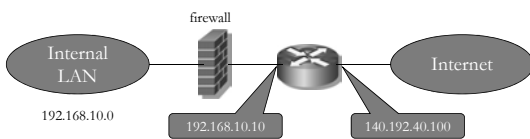
03/06/08

TDC363-09

23

Firewall

- It is a function, and can be on software or hardware.
- It can be a bridge or a router.
- Packet filtering is the standard feature of firewall
 - Most routers support packet filtering.
- NOS (Windows and UNIX) can also be configured to provide the firewall function.



03/06/08

TDC363-09

24

Packet Filtering

- Criteria that a firewall might use to accept or deny data:
 - Source and destination IP addresses
 - Use subnet mask to accept or deny a subnet
 - Source and destination ports
 - TCP, UDP, or ICMP protocols

03/06/08

TDC363-09

25

Proxy Service

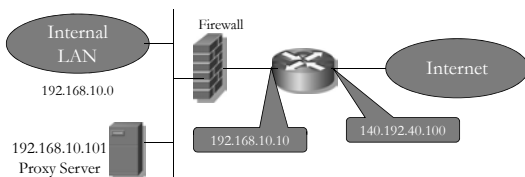
- Proxy service
 - It is at the application layer.
 - Software application on a network host that acts as an intermediary between external and internal networks
 - Network host that runs the proxy service is known as a **proxy server**, or gateway

03/06/08

TDC363-09

26

Firewall and Proxy Server



The firewall accepts Internet traffic only to/from the proxy server.

Cf. Figure 14-4

03/06/08

TDC363-09

27

Remote Access

- Capability for traveling employees, telecommuters, or distant vendors to access an organization's private LAN or WAN through specialized remote access servers
- Examples:
 - dial-up
 - VPN

03/06/08

TDC363-09

28

Dial-Up Networking

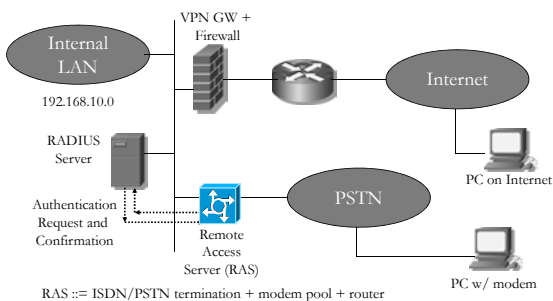
- User authentication and Authorization:
 - Login ID and password authentication
 - Ability to log all dial-up connections, their resources, and their connection times
 - Ability to perform callbacks to users who initiate connections
 - Centralized management of dial-up users and their rights on the network

03/06/08

TDC363-09

29

Remote Access Networks



03/06/08

TDC363-09

30

RADIUS

(show **the errors** in this diagram)

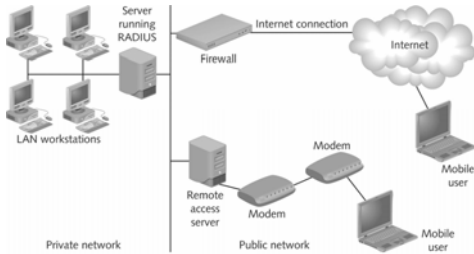


Figure 14-8 A RADIUS server providing centralized authentication

User Access Control

- Restriction that network administrators can use to strengthen the security of their networks
 - Some users may be valid only during specific hours
 - Some user IDs may be restricted to a specific number of hours per day of logged-in time
 - You can specify that user IDs can log in only from certain workstation or certain areas of the network
 - Set a limit on how many unsuccessful login attempts from a single user the server will accept before blocking that ID from even attempting to log on

Encryption

- Use of an algorithm to scramble data into a format that can be read only by reversing the algorithm
- In order to protect data, encryption provides the following assurances:
 - Data were not modified after the sender transmitted them and before receiver picked them up
 - Data can only be viewed by their intended recipient (or at their intended destination)
 - All of the data received at intended destination were truly issued by the stated sender and not forged by an intruder

Encryption

- The most popular kind of encryption weaves a **key** (random string of characters) into the original data's bits to generate a unique data block
 - The scrambled data block is known as **cipher text**
 - The longer the key, the more difficult the cipher text can be decrypted by an unauthorized system

03/06/08

TDC363-09

34

Encryption

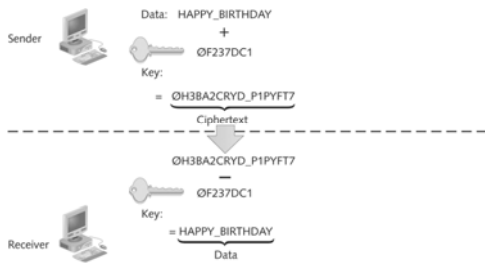


Figure 14-5 Key encryption and decryption

03/06/08

TDC363-09

35

Private Key Encryption

- Data are encrypted using a single key that only the sender and receiver know
- Also known as **symmetric encryption**
- The most popular private key encryption is the **data encryption standard (DES)**

03/06/08

TDC363-09

36

Private Key Encryption

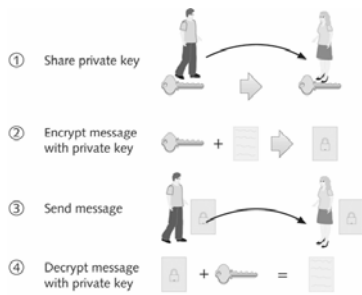


Figure 14-6 Private key encryption

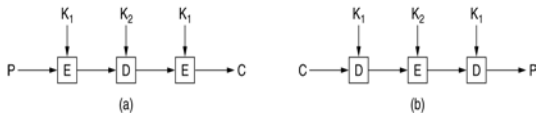
03/06/08

TDC363-09

37

Triple DES

- (a) Triple encryption using DES.
- (b) Decryption.



03/06/08

TDC363-09

38

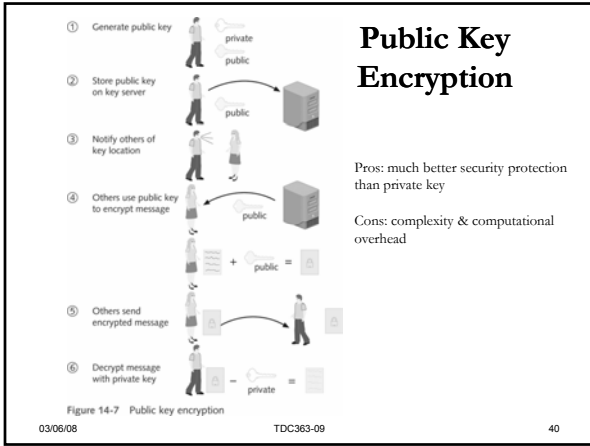
Public Key Encryption

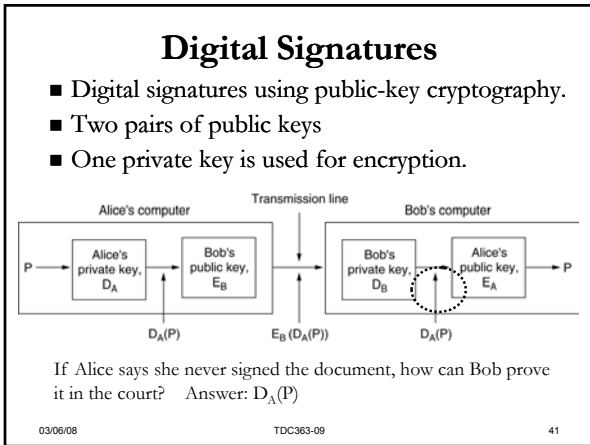
- Public key encryption
 - Data are encrypted using two keys
 - Also known as **asymmetric encryption**
- Public-key server
 - Provides a list of users' public keys
- Combination of public key and private key is known as **key pair**

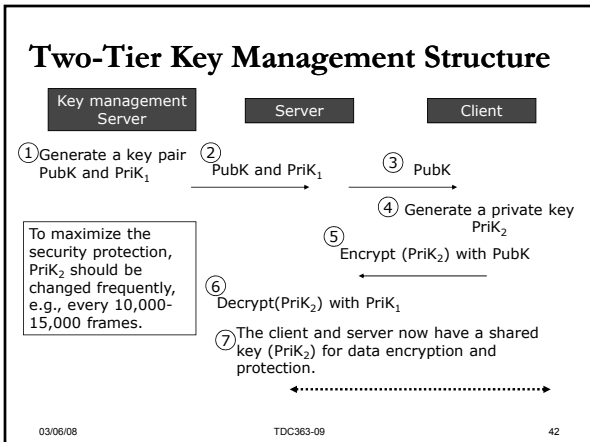
03/06/08

TDC363-09

39







Encryption Protocols

- Kerberos – Cross-Platform Authentication
- Pretty Good Privacy (PGP) – E-Mail
- Secure Sockets Layer (SSL) – TCP/IP
 - Secured HTTP, Telnet, FTP
- Internet Protocol Security (IPSec)

03/06/08

TDC363-09

43

Kerberos

- Cross-platform authentication protocol using key encryption to verify identity of clients and to securely exchange information once a client logs onto a system
- A **private key** encryption service.
- The server issuing keys to clients during initial client authentication is known as a **key distribution center (KDC)**
- In order to authenticate a client, KDC runs an **authentication service (AS)**
 - An AS issues a **ticket** (temporary set of credentials)
- A kerberos client, or user, is known as a **principal**

03/06/08

TDC363-09

44

Kerberos (cont.)

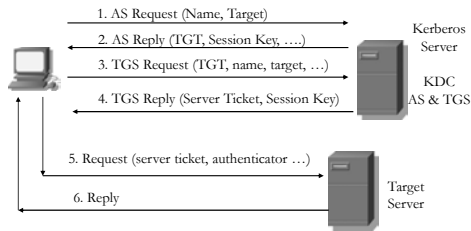
- Session key
 - Issues to both client and server by authentication service that uniquely identifies their session
- Authenticator
 - User's timestamp encrypted with the session key.
 - To help the service verify that a ticket is associated with an authenticated user
- Ticket granting service (TGS)
 - To solve the problem that a user has to request a separate ticket for a difference service.
 - Application separate from AS that also runs on the KDC
 - TGS issues client a ticket **granting ticket (TGT)**

03/06/08

TDC363-09

45

Kerberos Authentication Process



03/06/08

TDC363-09

46

Applications of Encryption

- Pretty Good Privacy (PGP)
 - **Public key** encryption system that verifies authenticity of an e-mail sender and encrypts e-mail data in transmission
- Secure Sockets Layer (SSL)
 - Method of encrypting TCP/IP transmissions en route between client and server using **public key** encryption technology

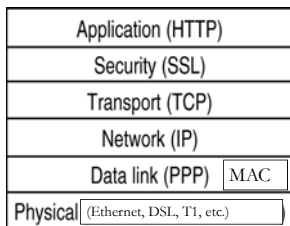
03/06/08

TDC363-09

47

SSL—The Secure Sockets Layer

- Layers (and protocols) for a home user browsing with SSL.



03/06/08

TDC363-09

48

Secure Sockets Layer (SSL)

- HTTPS
 - URL prefix indicating a Web page requires its data to be exchanged between client and server using SSL encryption
- SSL session
 - Association between the client and server identified by an agreement on a specific set of encryption techniques
- Note: ssh (vs. telnet) and sftp (vs. ftp) are not using SSL.

03/06/08

TDC363-09

49

SSL (cont.)

- Handshake protocol
 - Allow the client and server to authenticate each other
 - Client_hello
 - Message issued from the client to the server
 - Server_hello
 - Message issues from the server to the client
 - Server issues a public key or a digital certificate.
- Transport Layer Security (TLS)
 - Version of SSL being standardized by the IETF
 - RFC 2246

03/06/08

TDC363-09

50

Internet Protocol Security (IPSec)

- Defines encryption, authentication, and key management for TCP/IP transmissions
- Encrypts data by adding security information to the IP header.
- Operates at the Network layer (layer 3).
- IPSec accomplishes authentication in two phases:
 - Key management
 - Key encryption

03/06/08

TDC363-09

51

Internet Protocol Security (IPSec)

- Encrypt data by adding security information into the IP packet header.
- Key management
 - IPSec relies on Internet Key Exchange (IKE) for its key management
- In IPSec, two type of encryption may be used:
 - Authentication header (AH)
 - Encapsulation security payload (ESP)

03/06/08

TDC363-09

52

Review Questions

- What is a security audit? When shall you conduct a security audit?
- What is the difference between sniffing (snooping) and spoofing on the network?
- What is the risk of unused port in an office?
- Write a security policy for password (at least five items)

03/06/08

TDC363-09

53

Review Questions (cont.)

- Discuss the differences of NAT, Firewall, and Proxy server. Where do they locate at the OSI model?
 - Draw a network diagram for each one.
- Describe two methods where you can use private IP addresses to surf the public Internet.
- List four data fields in IP datagram that firewall may use to filter the packets.
- RADIUS: What is RADIUS? Draw a network diagram to show how it works? How is used to support VPN?

03/06/08

TDC363-09

54

Review Questions (cont.)

- What is the major difference between private key encryption and public key encryption? Which one is symmetric? Which one is more secure?
- Give a security protocol using private key.
- Give a security protocol using public key.
- What is Kerberos? Why do we need Kerberos?
- The CTI staff decide to disable telnet and FTP to the TDC Linux machines. Why? Without telnet and FTP, how can we access these machines?
- What is a digital signature? As a vendor, how can you prove that the signature is indeed from a customer?

03/06/08

TDC363-09

55

Review Questions (cont.)

- What is a DoS attack? Give an example of a DOS attack (describing the protocol messages used in such an attack).
 - What is TCP SYN attack? Draw a diagram to illustrate it.
- What are the encapsulation and encryption schemes used in IPSec?

03/06/08

TDC363-09

56

Final Exam

- Date: 03/17 (Monday), 11:45 – 02:00pm
- Same format as the midterm exam.
- Close book, close notes
- 2 pages of study notes (double side)
- Calculator is allowed, but no PDA.
- Seating – same as midterm
- Coverage: Lecture 05 – Lecture 09

03/06/08

TDC363-09

57
