Department of Computer Science and Engineering
University of Moratuwa

Computer, Network and Web Security
A preliminary introduction

Shantha Fernando & Gihan Dias

Department of Computer Science and Engineering

University of Moratuwa

shantha@cse.mrt.ac.lk

Topics

- Computer Security
- Network Security
- Web Trust?
- Web Assurance?
- Internet Security

- Using the Computer and Internet / web in a secure manner

Why Internet Security?

- Internet is an essential part of doing business today
- Connecting to the Internet exposes us to some dangers
- We need to identify, understand and control the risks
- Similar to any other risks of doing business

Computer security

- What is Computer Security?

"A computer system is secure
if you can depend upon it
to behave as you expect"

Computer Security Objectives

- To protect the resources of your computer system

Resources

- Physical Assets
- Data / software
- Personnel
- Trust

Where do Security Threats come from?

- Insiders
  - Users
  - System administrators / programmers
- Outsiders
  - Associates (customers, contractors)
  - Former employees
  - Others
- Most incidents are due to insiders

Network Security

- Why is network security problematic?
- Network is dispersed
  - not all nodes may be visible
- Many heterogeneous parts
  - hardware, software
- Lack of central control
- Many avenues of attack

Internet Security

- Security risks multiply when you connect to the Internet
- Why?
  - Your system is accessible to millions of people
  - You have no control on them
- Vulnerabilities are discovered and exploited almost instantaneously
  - Before you can act

Electronic Commerce Security

- You are doing business

but

- You are dealing with an unseen party

- Issues:
  - authentication
  - confidentiality and Integrity
  - accountability
  - non repudiation

Computer System Security

Types of Computer Systems

- Hosts
  - Unix
  - mainframes
  - PCs
- Networks
  - servers
  - workstations
  - network hardware
    - routers, switches, etc.

How can a System be Attacked?

- By impersonating a valid user
  - human engineering
  - wiretapping
  - searching
- By exploiting a bug in the system
  - hardware
  - operating system
  - applications

Achieving System Security

- Access control
- File and data control

Access Control

- The “front door” of the computer
- Admit those who require access
  - identification and authentication
- Lock out those who don’t

Complete security can be achieved by denying all access

But then the system will be of no use

User Privileges

- Principle of minimum privilege

"A user should be given all the privileges he needs to do his work and no more."

- Normal users
- Privileged users
  - Administrators
  - Managers
  - Programmers

Authentication

- Proving you are who you say you are

- Authentication Methods
- by Something you have
  - e.g., token
- by Something you know
  - e.g., password
- by Something you are
  - e.g., fingerprint

Data Security

- Integrity
  - Data remains unaltered
  - Identity of creator / modifier is known
- Confidentiality
  - Data is not disclosed to unauthorised parties

File security

- Access rights
- Set for each user or group of users
- For each file or directory
- Specify if the file can be
  - read
  - written
  - modified
  - deleted
  - etc. ...

Bugs in a System

- All systems have bugs
- Some bugs allow system security to be breached
- Some security holes are “features”
  - trade-off between usability and security

Protecting Yourself from Bugs

- Use minimum components needed
  - each component may have bugs
  - interactions among components may cause bugs
- Use reliable components
  - designed with security in mind
  - with a history of reliable operation
  - with expectation of quick bug fixes

Protecting Yourself (cont.)

- Install latest security updates
  - include in service contract
- Monitor security lists
  - e.g. www.cert.org
- You will never be 100% safe!

Network Security

Types of Network

- Departmental network
  - within a room
- Local network
  - within a building
- Corporate network
  - worldwide
- Public network
  - worldwide
- Security problems multiply as network becomes larger

Network Security

- Host security
  - servers
  - clients
  - network hardware
- Data transmission security

Host security (on a network)

- Access to host is via services provided
  - can ensure security by not providing any services
  - but then the system is of no use!
- Provide only necessary services
- Ensure provided services are secure

Access control

- Since access is over a network, plaintext passwords are unsafe
  - may be wiretapped
- Cryptographic Access Control
  - e.g., secure shell
- Challenge - Response mechanism
  - Manual
  - Computer
  - Time-based
  - Smart card

Server Security

- Use a secure operating system
- Enable security features
  - Ensure sysadmin is competent!
- Disable unneeded features
- Install security updates
  - O.S. and *all* applications!

Client Security Problems

- Some O.S.'s (e.g. Win 9x) are not designed for security
- Some applications (e.g. MS Office) are not designed for security
- Clients are controlled by users
- Users favour features over security

Implementing Client Security

- Use a more secure O.S. (e.g. Win 2000 or Linux)
- Use a client management system (e.g. ZenWorks)
- Control software installed on clients
  - users may resist
- Educate users

Viruses

- Caused by lack of security features on PCs
- Spread mainly by carelessness and lack of policy
- A good security policy helps to check viruses
- Set up virus scanners and virus guards

Network Infrastructure Security

- Hubs, switches, routers, etc.
  - same vulnerabilities as other hosts
  - located in various places
- Network cabling and outlets
  - Who can access them?
- Wide-area networks
  - not under your control

Data Transfer Security

- Confidentiality
  - ensures data is not revealed to in transit
- Integrity
  - ensures data is not modified in transit
- Authentication
  - ensures you are talking to whom you think you are

Data transfer security

- Encryption of Data Stream
- Authentication of both parties

Encryption

- Single-key encryption
  - same key shared by sender and receiver
  - provides both privacy and integrity
- Dual (public) key encryption
  - each user has both a private and public key
- Difficulty of breaking is related to key length
  - export restrictions

Public key encryption

- Privacy
  - encrypt using public key
  - decrypt only by private key
  - no-one else can decrypt
- Integrity
  - encrypt using private key
  - decrypt only by public key
  - no-one else can encrypt

Security on the Internet

Types of Internet Connections

- Dial-up (single Computer)
- Dial-up (network)
- Dedicated (network)

When you connect to the Internet ...

- You can access the Internet

  and

- The Internet can access you

- The Internet is a two-way network
- There are lots of people out there
- Some of them may be after you

Why worry about it?

- Privacy
  - you have information on your system you need to keep private and secure
- Commerce
  - the Internet is used for conducting business
- Reputation
  - an attack on your system may diminish your reputation

Implementing Internet Security

- Secure your servers
- Secure your clients
- Secure your network
- Implement a firewall

- A firewall is not a cure-all

Firewalls

- Separate a more secure network from a less secure one
  - Typically, a corporate network from the Internet
- Why use a firewall?
  - easier to secure a network using a single firewall than trying to secure every machine in the network

Functions of a Firewall

- Deny unauthorised access
  - from outside to inside
  - from inside to outside
- Control access to authorised services
- Log accesses and access attempts
- Raise alarm if suspicious activity occurs

Types of Firewalls

- Packet filters
  - network layer
- Application gateways

- Configuring a firewall is not trivial
  - need to update the configuration as the world changes

Web Security

Web Security Problems

- Securing the web server
- Securing the web client
- Securing information that travels between the web server and the user

Web Server Security

- O.S. and application security
- Security of interface between web server and database
  - it's all that stands between your data and the world
  - generally implemented by scripting languages such as Perl and ASP
- Security of interface to the web
  - can it be hacked?

What is a Secure Web Server?

- A server which implements an encrypted protocol such as SSL
- Not necessarily more secure than any other server

Web Client Security

- A web browser (e.g. Internet Explorer) is a large software with $many$ features
- Each feature is a potential security hole

Web Client Security Problems

- Downloaded files
  - may contain viruses and trojan horses
  - some files are signed for authentication
- Helper applications and plug-ins
  - may run programs on your machine
- Javascript
  - has security model
- Java
  - has security model

Client Security Problems (Cont.)

- ActiveX, etc.
  - many security problems
- Cookies
  - Allow sites to track usage
- Browser bugs
  - many reported
  - many will remain

Securing Data Transfer

- Secure Socket Layer (SSL)
- Encrypts data transferred between browser and server
- Identifies server
- (optionally identifies user - rarely used)
- Does not secure data once on the server (or client)

Types of Encryption

- Typically defined by key length
- 40-bit encryption
  - till recently, all that was allowed to be exported from the U.S.
  - not sufficient for any valuable information
- 128-bit encryption
  - now available for export (under certain conditions)
  - generally sufficient
  - are you *sure* you can trust your software vendor?

Conclusion

- Secure all your machines
- Keep up-to-date
- Make sure you have a recovery plan