SYSTEM SECURITY

FOR TRADITIONAL AND WEB BASED SYSTEMS

Dr. Krishnendu Guha

Assistant Professor (On Contract)

National Institute of Technology (NIT), Jamshedpur

Email: krishnendu.ca@nitjsr.ac.in

INTRODUCTION

- With increasingly complex transactions and many innovative exchanges, the Web has brought heightened security concerns to the professional's world.
- Total System Security is a MYTH
- The actions analysts and users take are meant to move systems toward the secure end of the continuum by lessening the system's vulnerability.
- It should be noted that as more people in the organization gain greater computer power, gain access to the Web, or connect to intranets and extranets, security becomes increasingly difficult and complex.
- Security has three interrelated aspects: physical, logical, and behavioral.
- All three must work together if the quality of security is to remain high.

PHYSICAL SECURITY

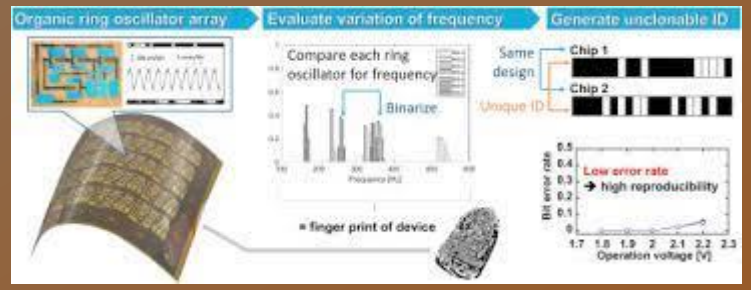
- Physical security refers to securing the computer facility, its equipment, and software through physical means.
- It can include controlling access to the computer room by means of
- machine readable badges,
- biometric systems, or
- a human sign-in/sign-out system,
- using closed circuit television cameras to monitor computer areas,
- backing up data frequently, and storing backups in a fireproof, waterproof area, often at a secure off-site location.
- In addition, small computer equipment should be secured so that a typical user cannot move it, and it should be guaranteed uninterrupted power.

- Alarms that notify appropriate people of
- fire,
- flood, or
- unauthorized human intrusion

- Decisions about physical security should be made along with users when the analyst is planning for computer facilities and equipment purchases.

- Obviously, physical security can be much tighter if anticipated in advance of actual installation and if computer rooms are specially equipped for security when they are constructed rather than outfitted as an afterthought.

LOGICAL SECURITY

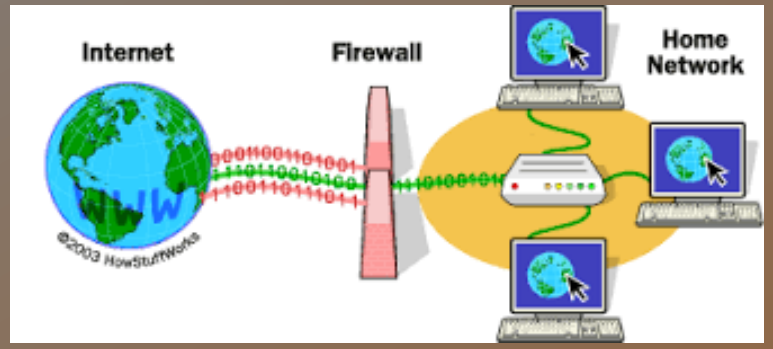


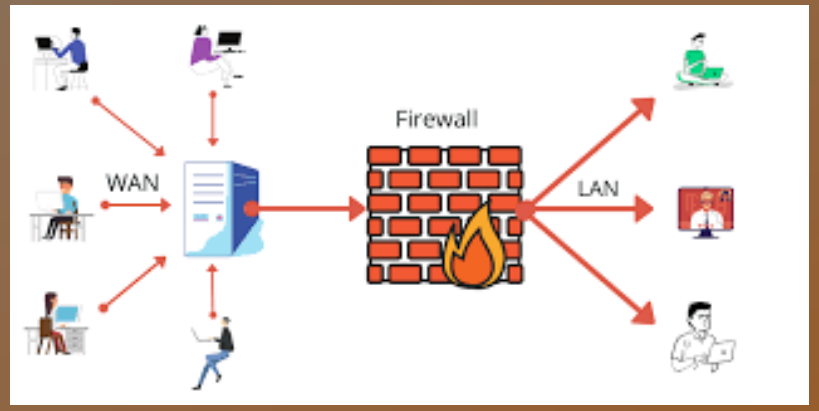
- Logical security refers to logical controls in the software itself.
- The logical controls familiar to most users are passwords or authorization codes of some sort.
- When used, they permit the user with the correct password to enter the system or a particular part of a database.

- Passwords, however, are treated cavalierly in many organizations.
- Employees have been overheard yelling a password across crowded offices,
- taping passwords to their display screens, and
- sharing personal passwords with authorized employees who have forgotten their own.

- Special encryption software has been developed to protect commercial transactions on the Web, and business transactions are proliferating.

- Internet fraud is also up sharply, however, with few authorities trained in catching Internet criminals and a “wild west,” or “last frontier,” mentality clearly evidenced in those instances when authorities have been able to apprehend Web criminals.

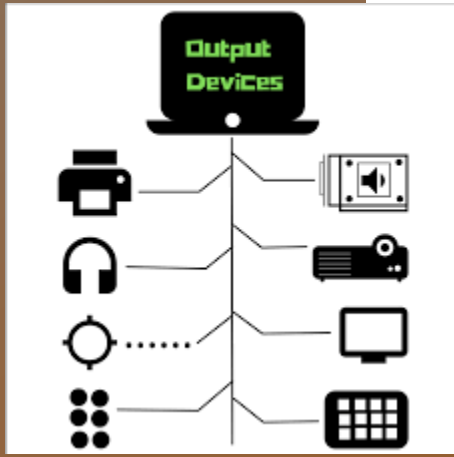




- One way for networks to cut down on the risk of exposure to security challenges from the outside world is to build a firewall or firewall system.
- A firewall constructs a barricade between an internal organization's network and an external (inter)network, such as the Internet.
- The internal network is assumed to be trustworthy and secure, whereas the Internet is not.
- Firewalls are intended to prevent communication into or out of the network that has not been authorized and that is not wanted.
- A firewall system is not a perfect remedy for organizational and Internet security; it is, however, an additional layer of security that is now widely endorsed.

BEHAVIOURAL SECURITY

- The behavioral expectations of an organization are implicit in its policy manuals and even on signs posted in work rooms and lunch rooms
- Security can begin with the screening of employees who will eventually have access to computers, data, and information, to ensure that their interests are consistent with the organization's interests and that they fully understand the importance of carrying through on security procedures.
- Policies regarding security must be written, distributed, and updated so that employees are fully aware of expectations and responsibilities.
- It is typical that the systems analyst will first have contact with the behavioral aspects of security.
- Some organizations have written rules or policie prohibiting employees from surfing the Web during work hours, or even prohibiting Web surfing altogether, if company equipment is involved.
- Other corporations use software locks to limit access to Web sites that are judged to be objectionable in the workplace, such as game, gambling, or illegal sites.



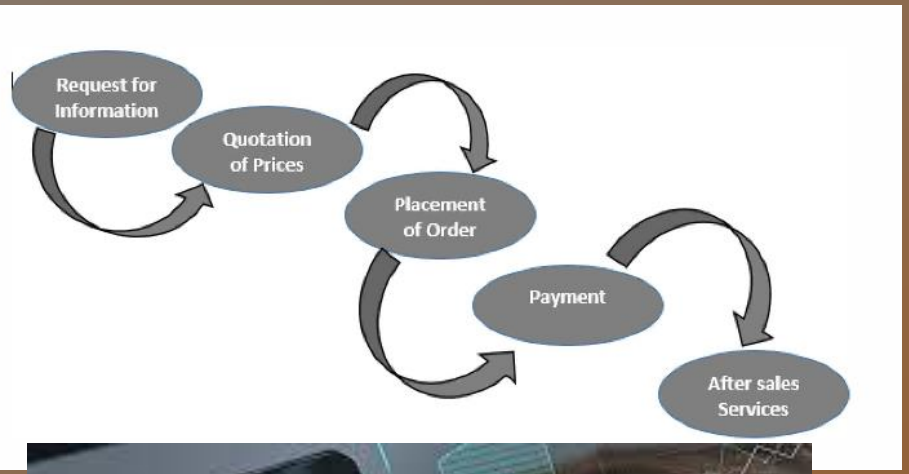
- Part of the behavioral facet of security is monitoring behavior at irregular intervals to ascertain that proper procedures are being followed and to correct any behaviors that may have eroded with time.
- Having the system log the number of unsuccessful sign-on attempts of users is one way to monitor whether unauthorized users are attempting to sign on to the system.
- Periodic and frequent inventorying of equipment and software is desirable.
- In addition, unusually long sessions or a typical after-hours access to the system should be examined.
- Employees should clearly understand what is expected of them, what is prohibited, and the extent of their rights and responsibilities.
- In the United States and European Union, employers are legally obligated to disclose all monitoring that is being done or that is being contemplated, and they must supply the rationale behind it.
- Such disclosure should include the use of video cameras, software, and phone monitoring.
- Output generated by the system must be recognized for its potential to put the organization at risk in some circumstances.
- Controls for output include displays that can only be accessed via password, the classification of information (that is, to whom it can be distributed and when), and secure storage of printed and stored documents, no matter what their format.

SPECIAL SECURITY CONSIDERATIONS FOR ECOMMERCE

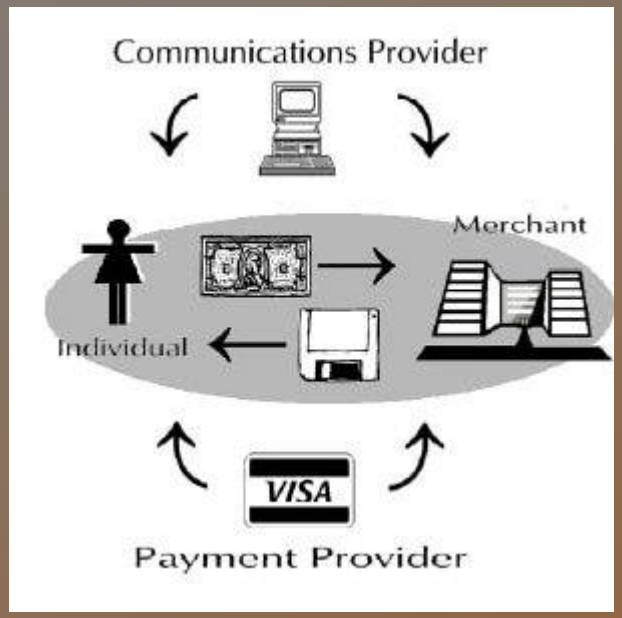
- It is well known that intruders can violate the integrity of any computer system.
- The analyst needs to take a series of precautions to protect the computer network from both internal and external Web security threats.
- A number of actions and products can help you:
- **1.** Virus protection software.
- **2.** Email filtering products that provide policy-based email and email attachment scanning and filtering to protect companies against both incoming and outgoing email.
  - Incoming scanning protects against spam (unsolicited email such as advertising) attacks, and outgoing scanning protects against the loss of proprietary information.
- **3.** URL filtering products that provide employees with access to the Web by user, by groups of users, by computers, by the time, or by the day of the week.

- **4.** Firewalls, gateways, and virtual private networks that prevent hackers from gaining backdoor access to a corporate network.
- **5.** Intrusion detection and anti-phishing products that continually monitor usage, provide messages and reports, and suggest actions to take.
- **6.** Vulnerability management products that assess the potential risks in a system and discover and report vulnerabilities. Some products correlate the vulnerabilities to make it easier to find the root cause of the security breach.
  - Risk cannot be eliminated, but this software can help manage the risk by balancing security risk to the financial bottom line.
- **7.** Security technologies such as secure socket layering (SSL) for authentication.
- **8.** Encryption technologies such as secure electronic translation (SET).
- **9.** Public key infrastructure (PKI) and digital certificates (obtained from a company such as VeriSign). Use of digital certificates ensures that the reported sender of the message is really the company that sent the message.

PRIVACY CONSIDERATIONS FOR ECOMMERCE

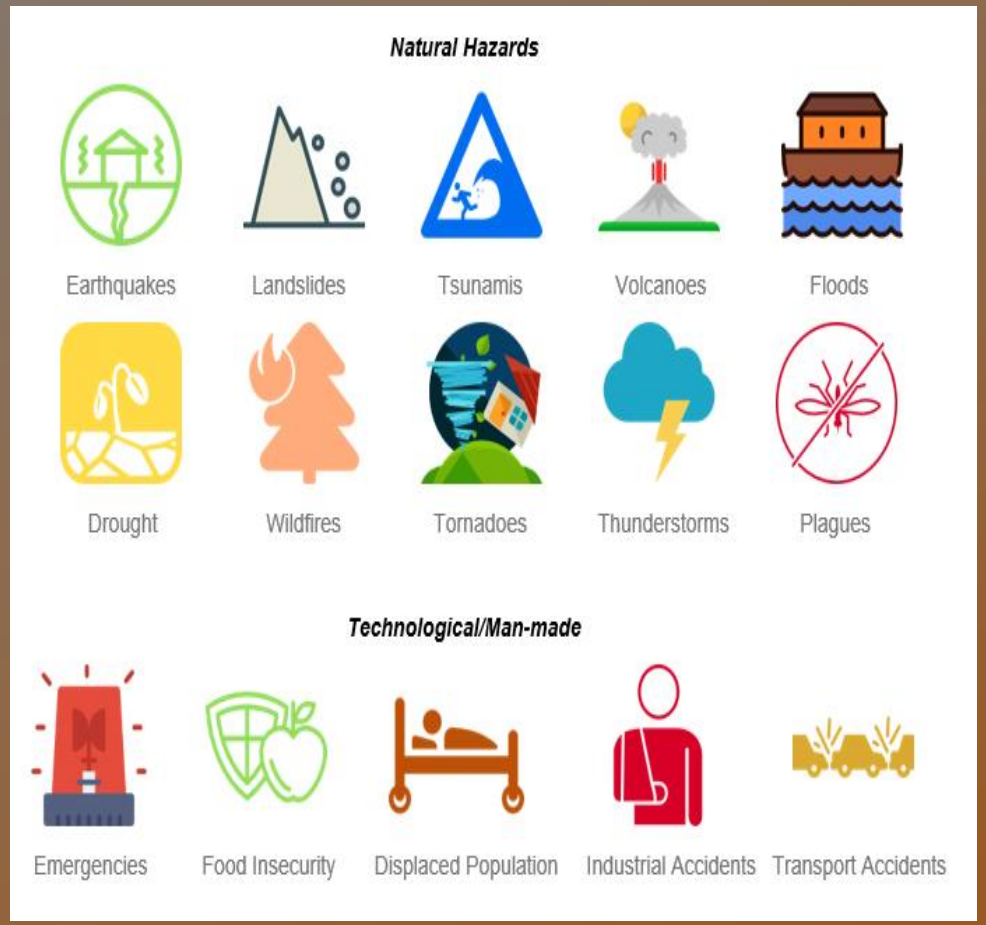


- The other side of security is privacy.
- To make your Web site more secure, you must ask the user or customer to give up some privacy.
- As a Web site designer, you will recognize that the company for which you design exercises a great deal of power over the data its customers are providing.
- The Web, however, allows the data to be collected faster and allows different data to be collected (such as the browsing habits of the customer).
- In general, information technology makes it possible to store more data in data warehouses, process that data, and distribute the data more widely.
- Every company for which you design an ecommerce application should adopt a privacy policy. Here are some guidelines:
- **1.** Start with a corporate policy on privacy. Make sure it is prominently displayed on the Web site so that all customers can access the policy whenever they complete a transaction.



- **2.** Only ask for information the application requires to complete the transaction at hand.
  - For example, is it necessary to the transaction to ask a person's age or gender?
- **3.** Make it optional for customers to fill out personal information on the Web site.
  - Some customers do not mind receiving targeted messages, but you should always give customer an opportunity to maintain the confidentiality of their personal data by not responding.
- **4.** Use sources that allow you to obtain anonymous information about classes of customers.
  - There are companies that offer audience profiling technology and technology solutions for management of advertisements, their targeting, and their delivery.
  - They do so by maintaining a dynamic database of consumer profiles without linking them to individuals, thereby respecting customers' rights to privacy.
- **5.** Be ethical.
  - Avoid the latest cheap trick that permits your client to gather information about the customer in highly suspect ways.
  - Tricks such as screen scraping (capturing remotely what is on a customer's screen) and email cookie grabbing are clear violations of privacy, and may prove to be illegal as well.

DISASTER RECOVERY PLANNING



- Some disasters are quite common, such as power outages, and we can assess the probability of some disasters occurring, such as a hurricane or an earthquake.
- However many disasters are unexpected in their timing or their severity, perhaps even causing loss of life, creating chaos for people and the organization itself.
- The fields of disaster preparedness and disaster recovery are interdependent, and they build on each other.
- Disaster preparedness includes what a company should do if it encounters a crisis.
- The field of disaster recovery is focused on how a business can continue in the aftermath of a disaster and how it can restore essential systems in the IT infrastructure.
- The traditional disaster recovery process consists of planning, a walkthrough, practice drills, and recovery from the disaster.

- When hit with a disaster, a company stands to lose people, money, reputation, and their own assets, as well as those of their clients.
- It is important to do the right things to minimize potential losses.
- The key questions that analysts must ask early on are
- (1) whether employees know where to go, and
- (2) what to do in the face of a disaster.

- Conventional wisdom provides seven elements to consider during and after a disaster.
- **1.** Identify the teams responsible for managing a crisis.
- **2.** Eliminate single points of failure.
- **3.** Determine data replication technologies that match the organization's timetable for getting systems up and running.
- **4.** Create detailed relocation and transportation plans.
- **5.** Establish multiple communication channels among employees and consultants who are onsite, such as analyst teams.
- **6.** Provide recovery solutions that include an off-site location.
- **7.** Ensure the physical and psychological well-being of employees and others who may be physically present at the work site when a disaster hits.

- The disaster preparedness plan should identify who, in the event of a disaster, is responsible for making several pivotal decisions.
  - These include decisions about whether business operations will continue; how to support communications (both computer and voice); where people will be sent if the business is uninhabitable; where personnel will go in an emergency; seeing to the personal and psychological needs of the people present in the business and those who might be working virtually; and restoring the main computing and work environments.
- Redundancy of data provides the key for eliminating single points of failure for servers running Web applications.
- Some businesses are moving to storage area networks (SANs) to get away from some of the unreliability associated with physical tape backups and storage.
- Synchronous remote replication, also called data mirroring, gets affected if companies are farther than 100 miles away from the site,.
- The three common choices are either to send employees home, to have them remain onsite, or to relocate them to a recovery facility that is set up to continue operations.
- The American Red Cross Website (www.redcross.org), which provides details for supporting humans during disasters and providing for them in the aftermath.


obrigado
Dank U
Merci
mahalo
Köszi
спасибо
Grazie
Thank you
mauruuru
Takk
Gracias
Dziękuję
Děkuju
danke
Kiitos