ACADEMIA DE STUDII ECONOMICE - Bucureşti

Bucharest University Of Economic Studies

FACULTY OF BUSINESS ADMINISTRATION

(Facultatea de Administrare a Afacerilor cu predare în limbi străine)

Technologies on e-Business

-

Securing Data in Computer Networks and Internet

By: Professor Vasile AVRAM, PhD

- suport de curs destinat studenţilor de la sectia engleză - licenta-

(Lecture notes for 2nd year students of English division)

- anul II - Zi -

(last update: October, 2013)

Bucureşti 2013

Table of Contents

Chapter 3 Securing Data in Computer Networks and Internet

*) *Note! These course is based on the excerpt [AvDg-03-07] updated/ completed with information as indicated by references*

3.1 Internet vulnerabilities and security

The modern organizations (and even individuals) are more and more dependent on information technology (IT) in commercial (or personal), governmental operations, or generally, any kind of human activity. Today, in order to be competitive, we must receive, process, and send information as soon and safety as possible to all partners. Internet technologies dramatically increase the importance of IT to every business and professional concern. They emerge initially as an offshoot of traditional IT but spawn an entirely new concept of IT systems and become now dominant technologies.

If information is recorded electronically and is available on networked computers, it is more vulnerable than if the same information is printed on paper and locked in a file cabinet. Intruders do not need to enter an office or home, and may not even be in the same country. They can steal or tamper with information without touching a piece of paper or a photocopier. They can create new electronic files, run their own programs, and hide evidence of their unauthorized activity.

Because of the inherent openness of the Internet and the original design of the protocols, (earlier designed without security in mind) Internet attacks in general are quick, easy, inexpensive, and may be hard to detect or trace. An attacker does not have to be physically present to carry out the attack. In fact, many attacks can be launched readily from anywhere in the world - and the location of the attacker can easily be hidden. Nor is it always necessary to "break in" to a site (gain privileges on it) to compromise confidentiality, integrity, or availability of its information or service.

We consider here that the purpose of the computer security is to prevent unauthorized access to the operating system services and to protect the information from voluntary misuse or modification. Similarly, for Internet enabled/ based informatics systems or applications/ services where all functionality is based on message exchange, or better on communication, the purpose of the communication security is the protection of the data in a computer network or in a distributed system.

As the Internet has grown up as more and more systems were connected to. A variety of different external attacks were devised to threaten these plethora of systems and generating consequently many requirements for controlling access to information and functionality. These requests have manifested as a set of standards to address security concerns. Exposing more and more computing resources to build richer, more compelling interactions and applications means risking having these resources compromised. Security standards have therefore evolved in tandem with the Internet. The evolution of business systems toward e-business system request consider security as a fundamental aspect of their design, since the risk possessed by these e-business systems is considerably higher than for any other “classical” type of business model. That is happening because the activity of an e-business entity is strictly based on communication and exchange of information, therefore protecting it is crucial. “E-mail and interactive websites offered the prospect of a radical shift from traditional business models to transactions almost exclusively conducted electronically [RK-10]”.

It is now essential to design systems to withstand external attacks and to recover from such attacks. Without security precautions, it is almost inevitable that attackers will compromise a networked system. Security engineering is concerned with the development and evolution of systems that can resist malicious attacks, which are intended to damage the system or its data. Software security engineering is part of the more general field of computer security. This has become a priority for businesses and individuals as more and more criminals try to exploit networked systems for illegal purposes.[IS-11]

When you consider security issues related to informatics systems we have to consider both the application software and the infrastructure on which this system is built (Figure 3.1). On a layered model the infrastructure for complex applications running in the back-end systems section in Figure 3.1 or in any server/ client computer may include:

• a platform as combination between specific hardware and an operating system. The hardware today includes a variety memory circuits (having as ancestor the CMOS part) that can be written with a specific driver/ or part of a driver allowing to better adapt a motherboard or a device to the operating system. The operating system, such as Linux or Windows (generally server version on server computers and workstation version on client computers), must contains network services allowing the inclusion of the computer into a network and access to Internet;

• other generic applications/ services that run on that system (such as web browsers and e-mail clients, CGI, or, generally, any Web-service);

• a database management system or at least his sql-engine allowing access for consulting and maintaining databases;

• middleware that supports distributed computing and database access or allows the communication with/ within legacy systems. This level can ensure a wall-like for defense;

• libraries of reusable components that are used by the application software (they are generally available locally as services or modules offered by the operating system);

• Web-services repositories from where Web-services delivered at client request via service broker, to any computer access in "Web enabled" environments.

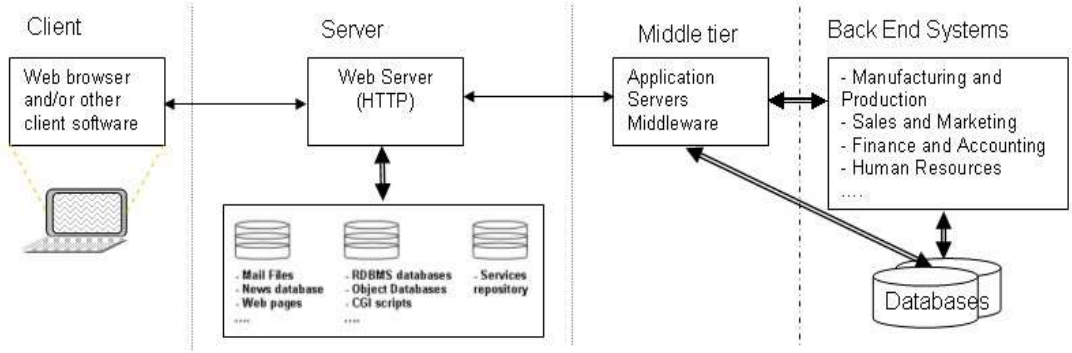

Figure 3.1 Client/server computing on the Internet (Source [ITech-09])

Most of external attacks focus on system infrastructures because infrastructure components are well known and widely available, even in source code. Attackers can probe these systems for known weaknesses or new weaknesses determined by missimplementations of different parts. They share to their attackers community information about vulnerabilities that they have discovered to obtain a better position or keep their existing one. As many people use the same software, attacks have wide applicability. The discovered/ known/ revealed infrastructure vulnerabilities may lead to attackers gaining unauthorized access to an application system and its data. [IS-11]

To understand how the usage of Internet for different activities evolves Figure 3.2 shows the evolution of number of mail messages delivered 'via' Internet from 1995 (before 1995 the

usage of same services is measured in thousands only and must be represented on a separate chart, but the trend is the same), where the trend established as exponential until today. Figure 3 shows the evolution of signaled incidents and vulnerabilities over Internet for the same timeline.

In 2013 the number of e-mail accounts is 3,9 billion and has a average growth rate 6% [IntStat-13-17]. Figure 4 shows an estimate of Business vs. Consumer e-mail accounts in the period 2013-2017 based on the growth rate determined analyzing the evolution based on source [IntStat-13-17]. A set of complex statistics information about traffic and many aspects of Internet can be found to the address http://www.internetworldstats.com/stats.htm.

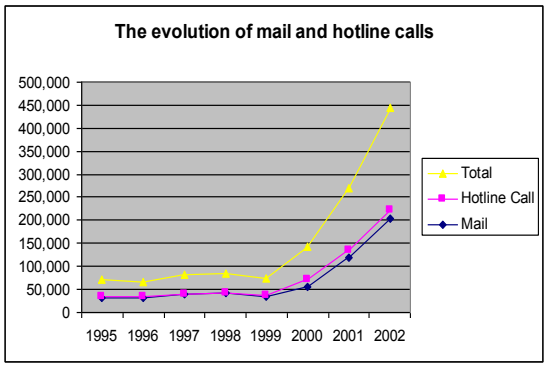

Figure 2 The evolution of number of mail messages (in thousands)

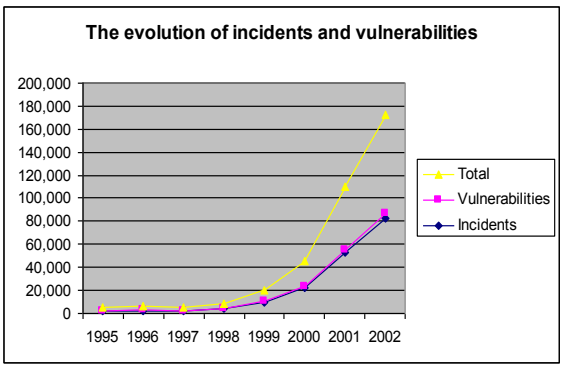

Figure 3 The evolution of number of signaled incidents and vulnerabilities (in thousands)

	2013	2014	2015	2016	2017
Worldwide Email Accounts (M)	3,899	4,116	4,353	4,626	4,920
Business Email Accounts (M)	929	974	1,022	1,078	1,138
% Business Email Accounts	*24%*	*24%*	*23%*	*23%*	*23%*
Consumer Email Accounts (M)	2,970	3,142	3,331	3,548	3,782
% Consumer Email Accounts	*76%*	*76%*	*77%*	*77%*	*77%*

Business vs. Consumer Email Accounts (M), 2013–2017

Figure 4 The Estimation 2013-2017 for Email Accounts (Source [IntStat-13-17])

3.2 Access Controls

The controls mitigate a wide variety of information security risks in the cyberspace. The term access control refere here to a broad range of controls that perform such tasks as ensuring that only authorized users can log on and preventing unauthorized users from gaining access to resources. Access controls are implemented using a defense-in-depth strategy, in which multiple layers or levels of access controls are deployed to provide layered security.

The main access control topics are:

Topic	Meaning
Permission	the access granted for an object which determine what you can do with it, such as read permission for a file that allows only to open it, or create, read, edit, or delete that allow you to completely manipulate the file;
Rights	the ability to take an action on an object, for example to modify the hour and date in in the system settings;
Privileges	the combination rights and permissions.

The primary access control types can be categorized as:

- **Preventive** – stop unwanted or unauthorized activity from occurring.
  Examples of preventive access controls include fences, locks, biometrics, mantraps, lighting, alarm systems, separation of duties, job rotation, data classification, penetration testing, access control methods, encryption, auditing, presence of security cameras or closed circuit television (CCTV), smart cards, callback procedures, security policies, security awareness training, antivirus software, firewalls, and intrusion prevention systems [CISSP-12].
- **Detective** – discover or detect unwanted or unauthorized activity;
  Examples of detective access controls include security guards, motion detectors, recording and reviewing of events captured by security cameras or CCTV, job rotation, mandatory vacations, audit trails, honeypots or honeynets, intrusion detection systems, violation reports, supervision and reviews of users, and incident investigations [CISSP-12].
- **Corrective** – modifies the environment to return systems to normal after an unwanted or unauthorized activity has occurred;
  They also include antivirus solutions that can remove or quarantine a virus, backup and restore plans to ensure that lost data can be restored, and active intrusion detection systems that can modify the environment to stop an attack in progress [CISSP-12].
- **Deterrent** – discourage violation of security policies.;
- **Recovery** – repair or restore resources, functions, and capabilities after a violation of security policies;
- **Directive** – direct, confine, or control the actions of subjects to force or encourage compliance with security policies;
- **Compensation** – provide various options to other existing controls to aid in enforcement and support of security policies.

3.3 Vulnerability and Attack

A **vulnerability** is a weakness that a person can exploit to accomplish something that is not authorized or intended as legitimate use of a network or system. When a vulnerability is exploited to compromise the security of systems or information on those systems, the result is a security incident. Vulnerabilities may be caused by engineering or design errors, or faulty implementation. An **attack** is any attempt to exploit the vulnerability of a system. Here we must consider two categories crackers and hackers. Crackers are malicious users intent on waging an attack against a person or system, so that they can be considered attackers. They may be motivated by greed, power, or recognition in their group. Some hackers are ‘professionals’ (generally technology enthusiasts with no malicious intent) while others are bored or disaffected personnell, or youths trying their “muscles”. Attackers aren't the only type of threat, they can be can be something natural or it could be accidental, but when considering access control, threats are primarily unauthorized individuals (commonly attackers) attempting unauthorized access to resources. Generally all are commonly refered by the term “hacker” and their actions by “hacking”.
Typical hacking activities might include:

- defacement of a website;
- obtaining access to and stealing information;
- corrupting data;
- the illicit use of credit cards in corporate payment systems.

Sony suffered multiple data breaches throughout 2011, an occurrence that severely tarnished its image.A massive data breach in April 2011 resulted in attackers stealing data from 77 million Sony PlayStation customer accounts. In May 2011, 24.5 million Sony Online Entertainment accounts were compromised. In June 2011, an attack on Sony Pictures compromised over one million user accounts, and the attackers bragged that they used a single SQL injection attack to retrieve data. In October 2011, when Sony locked almost 100 thousand PlayStation accounts, it said the credentials were stolen from other sites and sent email messages to users encouraging them to "choose unique, hard-to-guess passwords"—implying the problem was the customers' fault. Ironically, Sony may have been correct because many users have a single password they use for multiple online accounts. But coming after the recent spate of attacks, its advice was met with

skepticism.Losses from the April 2011 Sony PlayStation breach are estimated at 171 million dollars, but losses from the other attacks haven't been publicized. Additionally, intangible losses aren't publicly available. It's highly likely that many gamers have chosen to quit using the PlayStation and/or purchase another competing product. Were these losses preventable? Many security professionals say yes. At the Black Hat conference in 2011, Sony was nominated for "Most Epic Fail" for these attacks and also for laying off numerous information security personnel months before the first cyber-attack. [CISSP-12]

The technical causes behind successful intrusion techniques are represented by the following (but not only) major technical vulnerabilities:

- flaws in software or protocol designs;
- weaknesses in how protocols and software are implemented;
- weaknesses in system and network configurations.

Figure 5 shows the existing dependencies between a coosen technology and security vulnerabilities of software.

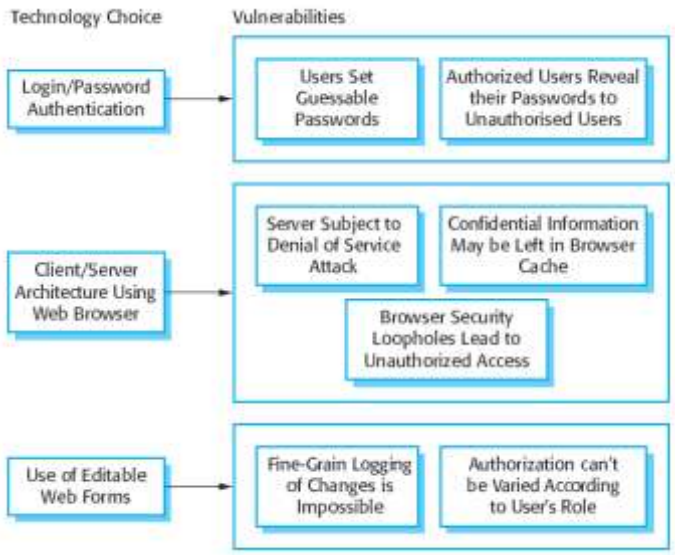

Figure 5 The Dependences Between Technology and Vulnerabilities (Source [IS-11])

3.4 Basic security concepts

The basic security concepts important to information on the Internet are confidentiality, integrity, and availability. Table 1 shortly describes these concepts.

Table 1. The concepts of confidentiality, integrity, and availability

Concept	Description
Confidentiality	When information is read or copied by someone not authorized to do so, the result is known as *loss of confidentiality*. For some types of information, confidentiality is a very important attribute. Examples include research data, medical and insurance records, new product specifications, and corporate investment strategies. For example, when the buyer makes a payment on the Internet and inserts the credit card number, the system encrypts it so that on its way from the buyer to the merchant and from the merchant to a transaction processing network, the access to the places where it is stored will be limited.

	Confidentiality can be thus described as protection of the privacy of the clients' personal information.
Integrity	Information can be corrupted when it is available on an insecure network. When information is modified in unexpected ways, the result is known as *loss of integrity*. This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting.
Availability	Information can be erased or become inaccessible, resulting in *loss of availability*. This means that people who are authorized to get information cannot get what they need. Availability is often the most important attribute in service-oriented businesses that depend on information (e.g., airline schedules and online inventory systems). Availability of the network itself is important to anyone whose business or education relies on a network connection. When a user cannot get access to the network or specific services provided on the network, they experience a *denial of service* (DoS).

Concepts relating to the people who use that information are authentication, authorization, and nonrepudiation. Table 2 shortly describes these concepts.

Table 2. The concepts of identification, authentication, authorization, nonrepudiation, and accountability

Concept	Description
Identification	*A subject* claims an identity. Is the process by which a subject professes an identity and accountability is initiated.
Authentication	*Authentication* is proving that a user is whom he or she claims to be, it proves a claimed identity. That proof may involve something the user knows (such as a password), something the user has (such as a "smartcard"), or something about the user that proves the person's identity (such as a fingerprint). Thus we consider that authentication is the process of verifying or testing that a claimed identity is valid. Identification and authentication always occur together as a single two-step process. The most common authentication technique is the use of password that is generally transmitted encrypted using hashing algorithms such as Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).
Authorization	*Authorization* is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program. Subjects are granted access to objects based on proven identities.
Nonrepudiation	Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted - the user cannot later deny that he or she performed the activity. This is known as *nonrepudiation.*
Accountability	When auditing is implemented subjects can be held accountable for their actions

Security professionals need to be aware of common attack methods so that they can take proactive steps to prevent attacks, recognize them when they occur, and respond appropriately. In any organization, communications are contained into a network that link all personnel internally and also link third parties (suppliers, stakeholders, strategic allies, agencies and even customers) externally. The business is now conducted globally (or migrate to be) and mobile workforce operate all over the world connected to the organization's network through mobile devices. In that context the exposure of the organization's communications (in all aspects, including remote or distributed processing) to network security incidents is higher.

A **network security incident** is any network-related activity with negative security implications. This usually means that the activity violates an explicit or implicit security policy (see the section on security policy). Incidents come in all shapes and sizes. They can come from anywhere on the Internet, although some attacks must be launched from specific systems or networks and some require access to special accounts. A typical attack pattern consists of gaining access to a user's account, gaining privileged access, and using the victim's system as a launch platform for attacks on other sites. The Table 3 shows the main categories of incidents and a brief description of each.

Table 3. Categories of incidents

Category	Description
Probe	A probe is characterized by unusual attempts to gain access to a system or to discover information about the system.
Scan	A scan is simply a large number of probes done using an automated tool.
Account Compromise	An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system-level or root-level privileges (privileges a system administrator or network manager has).
Root Compromise	A root compromise is similar to an account compromise, except that the account that has been compromised has special privileges on the system.
Packet Sniffer	A packet sniffer is a program that captures data from information packets as they travel over the network.
Denial of Service	The goal of denial-of-service attacks is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it.
Exploitation of Trust	Computers on networks often have trust relationships with one another and attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.
Malicious Code	Malicious code is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malicious code includes: Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Worms are self-replicating programs that spread with no human intervention after they are started. Generally they used as transport vector for viruses. Viruses are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems. These sorts of programs can lead to serious data loss, downtime, denial of service, and other types of security incidents.
Internet Infrastructure Attacks	These rare but serious attacks involve key components of the Internet infrastructure rather than specific systems on the Internet.

In the face of the vulnerabilities and incident trends, a robust defense requires a flexible strategy that allows adaptation to the changing environment, well-defined policies and procedures, the use of robust tools, and constant vigilance.

Figure 6 shows the types of attaks experienced an reported by the repondents of the survey realized in 2010 by Computer Crime Institute.

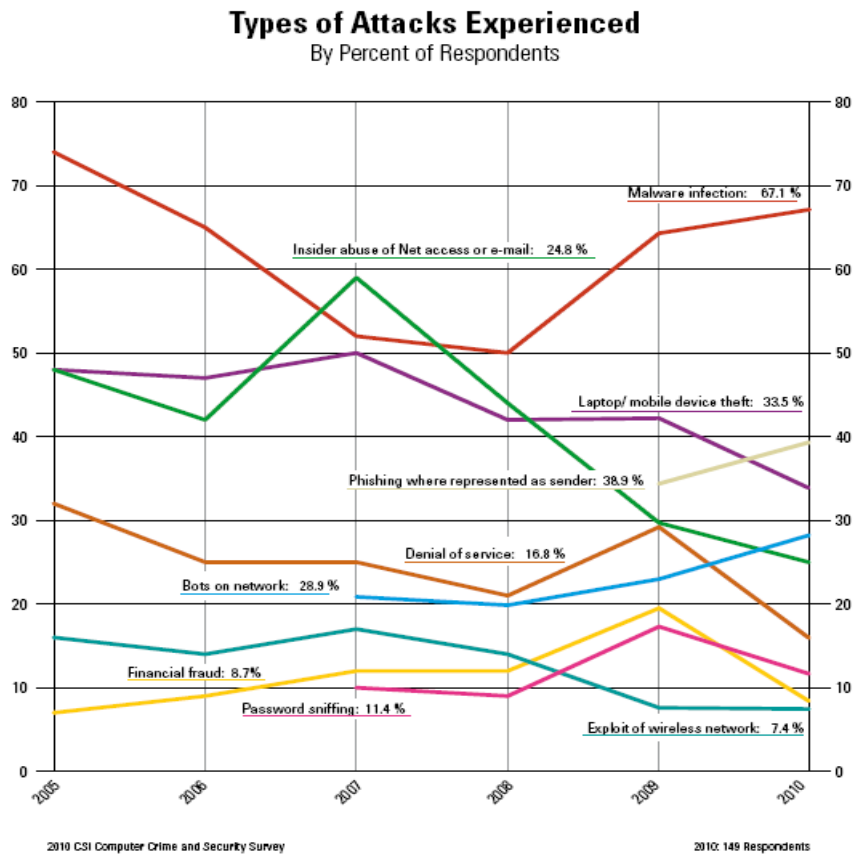

Figure 6 Types of Attacks Experienced (Source [CSI-10])

Social Engineering Attacks

Phishing	Attempts to trick users into giving up sensitive information, opening an attachment, or clicking a link. It often tries to obtain personally identifiable information such as usernames, passwords, or credit card details by masquerading as a legitimate company.
Spear Phishing	A form of phishing targeted to a specific group of users. It may appear to originate from a colleague or co-worker within the organization or from an external source.
Whaling	A variant of phishing that targets senior or high-level executives such as CEOs and presidents.
Vishing	A variant of phishing that uses the phone system or VoIP commonly to spoof the caller ID number to impersonate a valid bank or financial institution.
Smart Card Attacks	The attack is a side-channel attac it means is a passive, noninvasive attack intended to observe the operation of a device. When the attack is successful, the attacker is able to learn valuable information contained within the card, such as an encryption key and personal identification number (PIN).
Denial of Service Attacks (DoS)	DoS prevents a system from processing or responding to legitimate traffic or requests for resources.

3.5 Security policy

A **security policy** is a documented high-level plan for organization-wide computer and **information security**. It defines the security requirements for an organization, identifies assets that need protection and the extent to which security solutions should go to protect them, and provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. Because a security policy is a long-term document, the contents avoid technology-specific issues. The security policy document can be realized as a single document/ single policy or as multiple security policies with each one focused on a separate area. Typically the security policy is created or approved by senior leadership, and it provides a broad overview of an organization's security needs without going into details about how to fulfill the needs. The security policies are used by the professionals within organization as a guide to implement security requirements and even represent the source in developing standards. A security policy covers the following (among other topics appropriate to the organization):

- high-level description of the technical environment of the site, the legal environment (governing laws), the authority of the policy, and the basic philosophy to be used when interpreting the policy;
- risk analysis that identifies the site's assets, the threats that exist against those assets, and the costs of asset loss;
- guidelines for system administrators on how to manage systems;
- definition of acceptable use for users;
- guidelines for reacting to a site compromise.

Factors that contribute to the success of a security policy include management commitment, technological support for enforcing the policy, effective dissemination of the policy, and the security awareness of all users. Management assigns responsibility for security, provides training for security personnel, and allocates funds to security. Technological support for the security policy moves some responsibility for enforcement from individuals to technology. The result is an automatic and consistent enforcement of policies, such as those for access and authentication.

Technical options that support policy include (but are not limited to);

- challenge/response systems for authentication;
- auditing systems for accountability and event reconstruction;
- encryption systems for the confidential storage and transmission of data;
- network tools such as firewalls (Figure 7) and proxy servers.

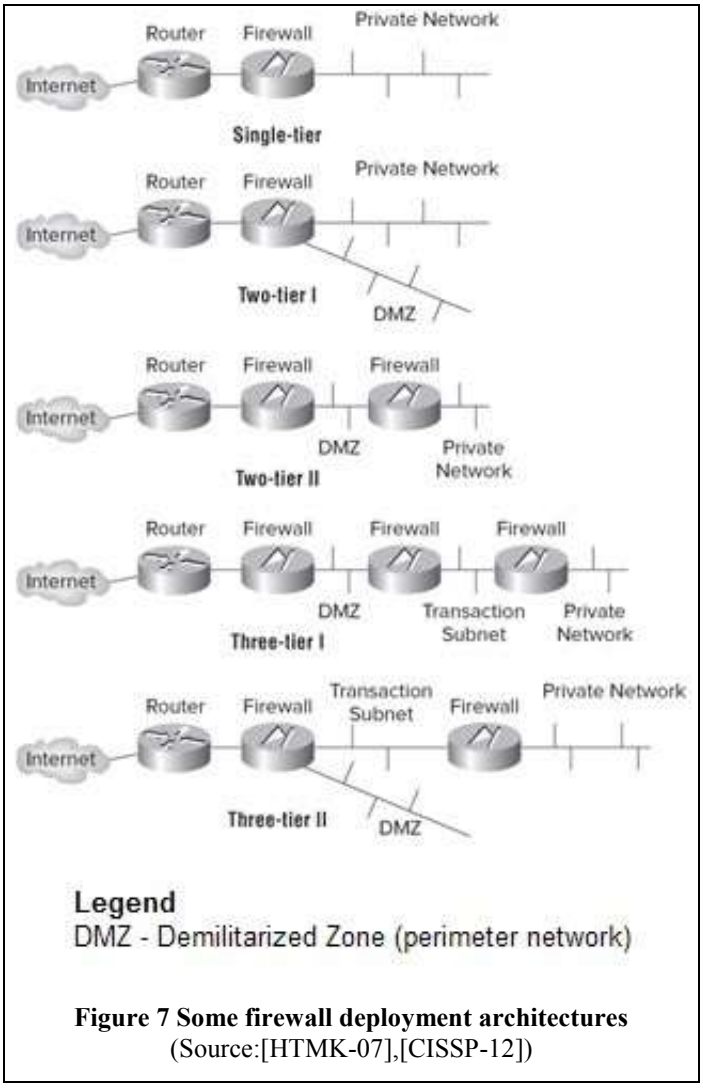

Figure 7 Some firewall deployment architectures
(Source:[HTMK-07],[CISSP-12])

A firewall (Figure 7) is a combination of hardware and software that serves as a gateway between the private network and the Internet.

In these architectures (Figure 7) the firewalls are used to guard access to network by preventing unwanted intrusion and block malicious files. They protect information entering and living the network and within the network itself.

The isolation area refered by demilitarized zone (DMZ) allow isolate the web server internally and externally.

Depending on the deployment architecture and configuration of the firewall, access can be allowed to certain internal information for certain external parties, and to internal parties for certain external information.

The firewall acts as a sole gateway with the purpose of identifying and dennying unauthorized intrusion. You must keep in your mind that inluding firewalls have their own limitations so that is not the panacea for all treats so that you must combine multiple security solutions.

The commonly recommended practices for improving security are represented by the following:

- all accounts must have a password and the passwords are difficult to guess (maybe, a one-time password system is preferable to other);
- the cryptographic techniques must be used to ensure the integrity of system software on a regular basis;
- apply secure programming techniques when writing software;
- must be vigilant in network use and configuration and all necessary changes must be realized as vulnerabilities become known;
- apply the latest available fixes and keep systems current with upgrades and patches as vendors deliver them;
- regularly check on-line security archives for security alerts and technical advice;
- audit systems and networks, and regularly check logs.

A 10 points security guideline that is helpful in designing system security (based on [IS-11]) is:

Nr.	Security Guideline	Explanation
1	Base security decisions on an explicit security policy	After the definition of security policy all security decisions must consider them
2	Avoid a single point of failure	The security must not be enshured by a single mechanism
3	Fail securely	Since system failures are inevitable in all systems security critical systems should always ‘failsecure’ (protect the system even when failling).
4	Balance security and usability	The demands of security and usability are often contradictory
5	Log user actions	Maintain a log of user actions
6	Use redundancy and diversity to reduce risk	Maintain more than one version of software or data in a system
7	Validate all inputs	
8	Compartmentalize your assets	Should not provide all-or-nothing access to information in a system
9	Design for deployment	System must be configured correctly when it is deployed in its operational environment
10	Design for recoverability	Design the system with the assumption that a security failure could occur

The security of a system must be checked on a scheduled basis and any time a suspicion appear in systems behaviour. The check of the security of a system can be realized by using a combination of testing, toolbased analysis, and formal verification:
- Experience-based testing - system is analyzed against types of attack that are known to the validation team;
- Tool-based testing – usage of various security tools to analyze the system;
- Formal verification – verify system against a formal security specification.
The Figure 8 shows the protection applied on a Patient system at infrastructure levels.

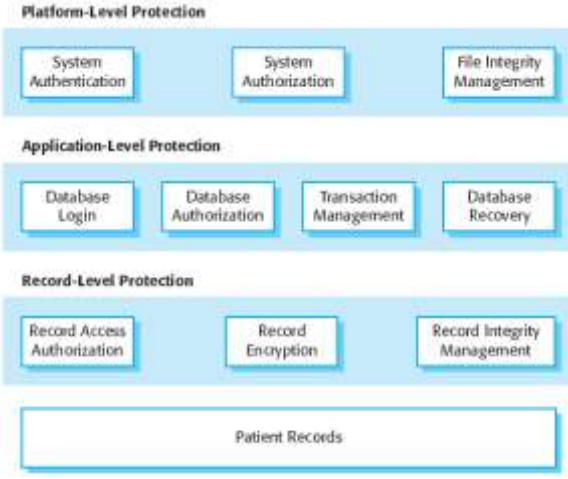

Figure 8 Protection Levels for a Patient Application (Source [IS-11])

Preventing Access Control Attacks. The protection against access control attacks requires a rigid adherence to a strong security policy and to take numerous security precautions such as:
- Control physical access to systems;
- Control electronic access to password files;
- Encrypt password files;
- Create a strong password policy;
- Offer tips to users on how to create strong passwords;
- Use password masking;
- Deploy multifactor authentication;

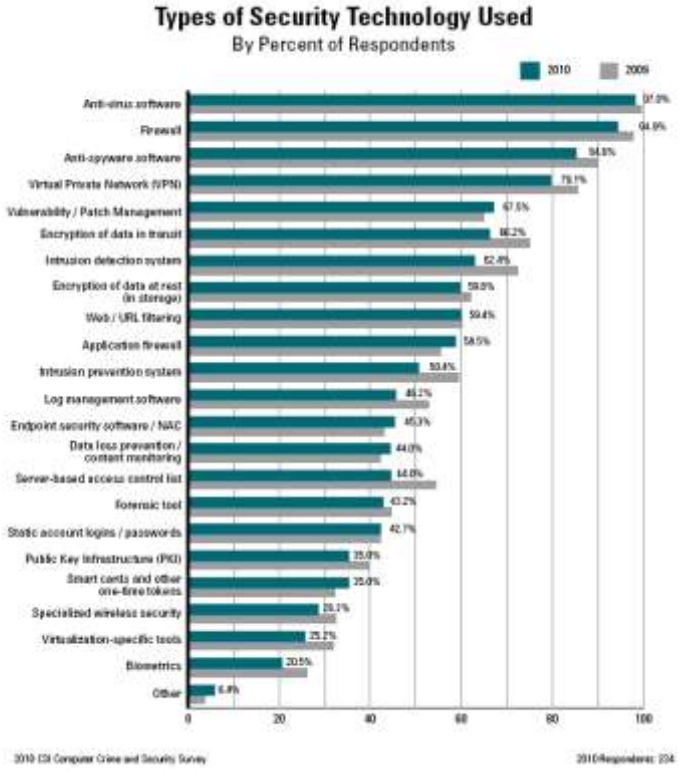

Figure 9 Type of Security Technology Used (Source [CSI-10])

- Use account lockout controls;
- Use last logon notification;
- Educate users about security;
- Audit access controls;
- Actively manage accounts;
- Use vulnerability scanners.

Figure 9 shows the percentage of the type of technology used to apply security policies by IT and Figure 10 the degree of satisfacion of the security solution designers with the choosen technology.

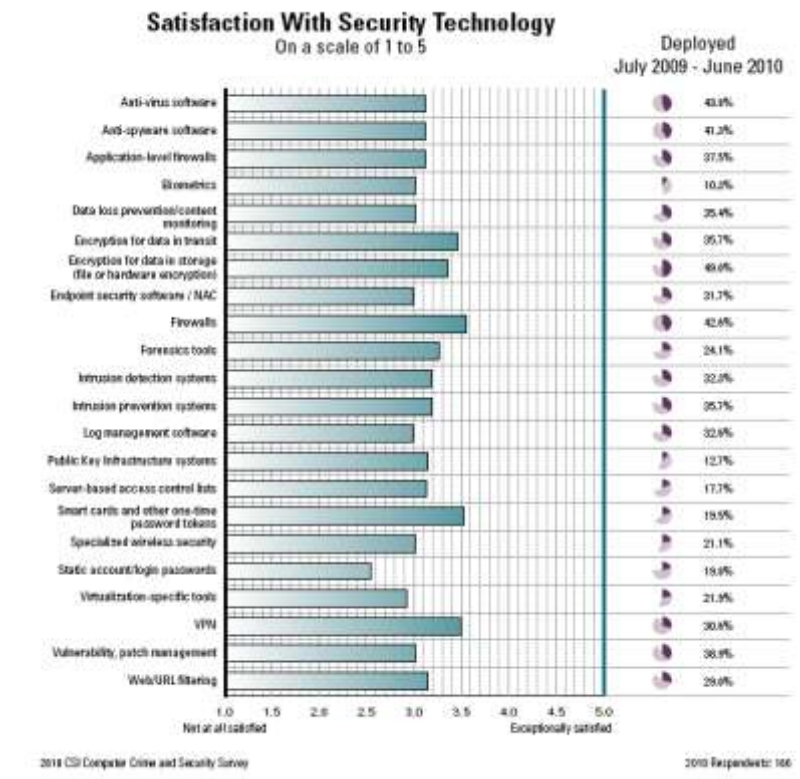

Figure 10 Satisfaction With Security Technology (Source [CSI-10])

3.6 The Top-Down Approach to Security

The initiation, support, and direction come from top management, work their way through middle management, and then reach staff members so that a security program must be designed and implemented based on a top-down approach. A top-down approach makes sure the people actually responsible for protecting the company's assets (senior management) are driving the program [HS-10].

The approach includes two phases:

1. **Design and implement a security program**. When designing and implementing a security program, the security professionals must determine the functionality and realize the end result expected. Many times, companies just start locking down computers and installing firewalls without taking the time to understand the overall security requirements, goals, and assurance levels they expect from security as a whole within their environment. The team involved in the process should start from the top with very broad ideas and terms and work its way down to detailed configuration settings and system parameters. At each step, the team should keep in mind the overall security goals so each piece it adds will provide more granularity to the intended goal.

2. **Develop and implement procedures, standards, and guidelines that support the security policy** and to identify the security countermeasures and methods to be put into place. Once these items are developed, the security program increases in granularity by developing baselines and configurations for the chosen security controls and methods.

Annex 1. Some security considerations

A. Potential E-Commerce Threats

Natural disasters	Other disasters
Cold weather	Blackouts
Earthquakes	Fires
Floods	Gas leaks
Hot weather	Neighborhood hazards
Hurricanes	Nuclear attacks
Ice storms	Oil leaks
Ocean waves	Power failure
Severe dust	Power fluctuations
Snow	Radioactive fallout
Tornadoes	Structural failure

B. Intentional Computer and E-Commerce Threats

Intentional computer and e-commerce threats usually fall into one of the following categories:

- Computer viruses;
- Trojan horses;
- Logic bombs;
- Trap doors;
- Denial-of-access attacks.

C. Computer Virus Symptoms

Some computer virus symptoms are represented by:

- Certain programs are bigger than normal;
- Data disintegrates;
- Data or programs are damaged;
- Hard disk space diminishes significantly;
- Keyboard locks;
- Memory becomes constrained;
- Screen freezes (no cursor movement);
- Sluggish disk access;
- Unexpected disk activity;
- Unusual messages appear on the screen;
- The computer takes too much time to boot.

D. Biometric Security Measures

- Fingerprint
- Hand geometry
- Palmprint
- Retinal scanning
- Signature analysis
- Voice recognition

E. The functional architecture for e-commerce

(excerpt from reference [ITech-09] pages 142-144)

Systems for Internet commerce have many masters. For analysis of architecture we consider four primary components of Internet commerce system (figure 3.12): customer, seller, transaction system, and payment gateway. For each one we present some security considerations.

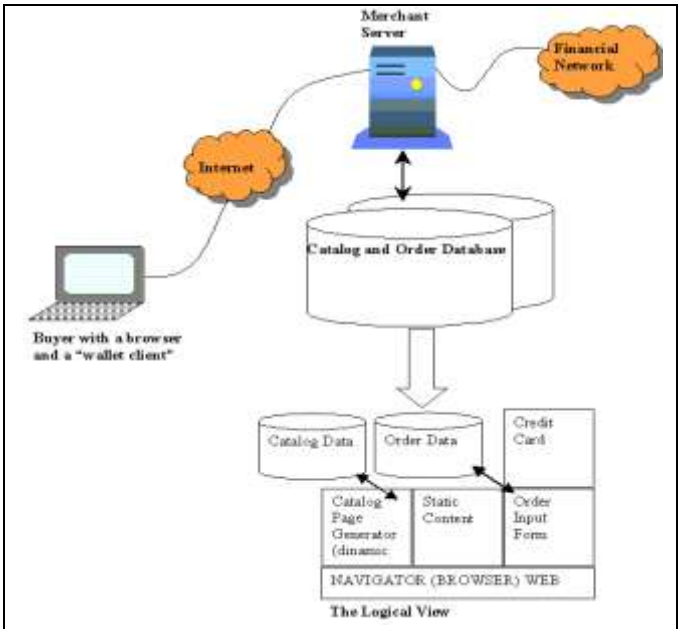

Figure 3.1 The functional architecture for e-commerce

1) **Customers** (Buyer, Clients) – The client is a computer system, typically a PC, connected directly to Internet via an ISP (Internet Service Provider), or indirectly via a corporate network. The primary tool for using www is a browser (a Web client). It is possible also to access www via specialized applications designed for e-commerce (particular for payments) called wallets. The buyer can be represented by:
   - **Retail customer** – the buyer that use the system for business-to-consumer commerce. This category of customers would like to retain their privacy, releasing as little information as possible to sites on the Net. Generally due to commercial interests this information is combined with other sources of data to build up a very detailed picture of the costumer. A major interest of this category of customers refers to the security. They want to be assured that their credit card numbers and other sensitive information are adequately protected;
   - **Business customers** – the buyers that use Internet commerce systems in the course of their daily jobs (i.e. an administrator reordering office suppliers). For this customers the security required refers to keep their competitors from finding out what they are doing and assuring the integrity of business records in company computer systems;
2) **Seller** (Merchant, Vendor) – The computer system or systems containing the merchant's electronic catalog or products. Sellers include merchants engaged in business-to-business or business-to-consumer commerce or publishers and content providers engaged in information commerce. The seller's are extremely interested in the integrity of their marketing presence, their prices, their customer records, and their business records;
3) **Transaction system** – the computer system or systems that process a particular order and which are responsible for payment, record keeping, and other business aspects of transaction. The part for credit card processing system is operated by financial processors that accept transactions from merchants and forward them to the merchant's bank. Transaction security is a paramount for a financial processor and includes the privacy and accuracy of records, and the authenticity and integrity of requests;
4) **Payment gateway** – the computer system or systems that routes payments instruments into existing financial networks such as for credit card authorization and settlement.

The heart of every e-commerce application is its database containing generally the catalog, the buying transactions and the related payments transactions. That heart is the most attractive prize for crackers because generally it stores all your customers' information, possibly even their payment information. The simplest way to assure the protection is to permit access to that database only to authorized users granted to realize specific operations. The access realized

on the basis of a username and password, generally from server-side scripts, by using connections strings containing, among other parameters, the following argument types: server name, user name, and password. To protect this vital information follows that rules:

- create a general user to access the database (not from administrators group) having insert, update, and select privileges and use these to define the connection string required to access and manipulate the database records;
- store the connection string in a separate script that will be included as a file when needed;
- encrypt all stored passwords.

For assuring secure electronic transactions Visa and MasterCard joined together (in 1995) to develop the Secure Electronic Transaction (SET) protocol, a technical standard for safeguarding payment card purchases made over open networks. SET is designed to mimic the traditional card transaction flow and in addition it includes the use of public key certificates to authenticate the parties to each other. Figure 3.8 illustrates the changes in the main architecture for e-commerce with SET and table 3.2 shows SET goals and requirements for different category of participants.

Table 3.2 SET goals and requirements

Category	Goals	Requirements
CardHolder	Provide confidentiality of information Authenticate merchant to cardholder Improve perception of safety of electronic commerce	Obtain and install cardholder software (wallet) Obtain SET client certificate
Banks	Reduce merchant fraud Build electronic commerce volume	Implement certificate hierarchy Implement certificate systems for cardholders
Merchants	Easy integration Build electronic commerce volume Reduce transaction costs	Implement SET merchant software

By his nature the HTTP protocol do not ensure any protection for the text information sended or received. There's nothing to stop anybody out there from listening and recording your details. Fortunately, we have other methods that can ensure transactions are secure and that the credit card details and other confidential information are not compromised [HKSU]:

- **Encryption:** the message must be *encoded* before sent to the web server and received back from the web server. The web server has a public key, and users will have a private key that enables them to decode the information. Only having the public key and the private key together will allow you to encrypt the message. The web server will have a public key and its own private key at the other end. To encrypt messages, you use a secure communications protocol. Either Secure Sockets Layer (SSL) or Secure HTTP (HTTPS) would provide this functionality. In Windows environmeent you can specify encryption methods and whether to use SSL on a connection in the Web.config file.
- **Certificates:** To guarantee that the site you are dealing with at the other end is reputable, it can be certified by a Certificate Authority. Verisign (www.verisign.com) is perhaps the

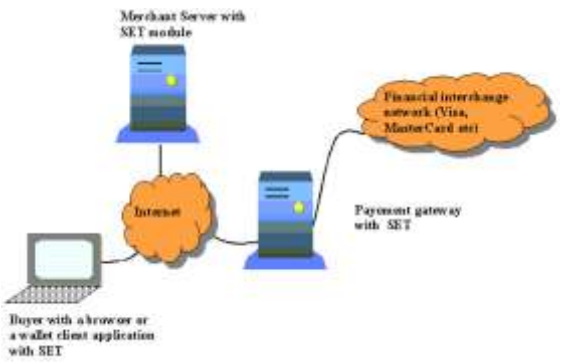

Figure 3.2 The functional architecture for e-commerce with SET

most common Certificate Authority. The authority is paid a yearly fee by the e-commerce vendor and in return, the authority performs checks on the business to prove that it is legitimate. These checks are then recorded in the form of a certificate. You can browse particular sites' certificates during the checkout process. To make your site trustworthy, you should go about obtaining a certificate from a Certificate Authority.

The functional architecture with SET changes as depicted in figure 3.13.

References

[ITech-09] Vasile AVRAM, Dragos VESPAN, Diana AVRAM, Alina ION, Internet Technologies for Business, Editura ASE, 2009

[AvDg-03-07] Vasile AVRAM, Gheorghe DODESCU, *Informatics: Computer Hardware and Programming in Visual Basic*, Editura Economică, Bucureşti, 2003 (reeditat 2007), ISBN:973-590-920-0 (pg 421-426)

[CSI-10] CSI Computer Crime Institute, 15th Annual 2010/2011 Computer Crime and Security Survey, www.GoCSI.com

[CW-08] Alan Calder, Steve Watkins, IT Governanace: A Manager's Guide to Data Security and ISO27001/ISO 27002, 4th Edition, Kogan Page, 2008

[IntStat-13-17] Sara Radicati, Justin Levenstein, Email Statistics Report, 2013-2017, THE RADICATI GROUP, INC., http://www.radicati.com

[HPL-08] John Recker, Tyler Close, Angela Maduko, Craig Sayers, A Semantic Wiki for Continual Collaborative Information Management, HP Laboratories, HPL-2008-90

[HS-10] Shon Harris, CISSP All-in-One Exam Guide, Fifth Edition, McGraw-Hill/Osborne, 2010

[IS-11] Sommerville, Ian. Software engineering, 9th Edition, Pearson, 2011, ISBN 10: 0-13-703515-2, ISBN 13: 978-0-13-703515-1

[HTMK-07] Harold F. Tipton, Micki Krause Information Security Management Handbook, Sixth Edition, Volume 1, Auerbach Publications, 2007

[CISSP-12] James M. Stewart, Mike Chapple and Darril Gibson, CISSP: Certified Information Systems Security Professional Study Guide, Sixth Edition, Sybex, 2012

[Web 2.0-09] James Governor, Dion Hinchcliffe, and Duane Nickull, Web 2.0 Architectures, O'Reilly - *Adobe Developer Library*, 2009, ISBN: 978-0-596-51443-3 Beijing • Cambridge • Farnham • Köln • Sebastopol • Taipei • Tokyo (pg 21-22)

[RK-10] Rupert Kendrick, Cyber Risks for Business Professionals, A Management Guide, IT Governance Publishing, ISBN 978-1-84928-093-8, 2010