CHAPTER 3
Hierarchical Classification of Security

3.1 Introduction

Security threats are attributable to human or natural disasters. The threats due to human can be malicious or non-malicious [LINK16]. Most of the security breaches such as session hijacking, spoofing, Cross Site Scripting (XSS) etc. are caused by the malicious users. To secure software systems, we need to protect against all such types of threats. With the exponential growth of security breaches, identification of the various security measures can be applied to secure software systems is challenging.

Security has been classified on the basis of data/ information sensitivity such as top secret, secret, confidential, restricted, and unclassified [LINK17]. On the principle of threats and crime prevention methods, security is classified for data at store, network and access rights, etc. [LINK18]. Security has also been classified for coding errors into seven kingdoms that relate to input validation and representation, API abuse, security features, time and state, errors, code quality and environment [TCM05]. Taxonomy of security flaws categorized on the basis of genesis, time of introduction, and location helps in focusing the attention of the developers towards the origin of flaws [L+94]. It has been observed that the existing classifications provide single level of categorization/ subtypes or are based on the flaws that are generated after the software is released for the operational use. Moreover, classifications are specialized in some particular domain and may not able to provide a broad view of security as the classifications do not cover all the security domains in detail. Due to ad-hoc knowledge regarding various security domains, it makes the security considerations difficult since the planning of the project.
Thus, there is a need to classify security so as to gain understanding of the various security measures required to secure a software system. In this regard, we present hierarchal classification of security that presents various security domains such as hardware security, system and application software security, network security etc. It supports the identification of security domains that are considered for securing the software systems. Further, various types of software systems such as web-based, client/ server based, desktop based softwares etc. are analyzed to identify the security domains to be considered to address the security issues of the softwares. A brief background regarding classification of security is presented in Section 3.2. We then discuss the hierarchical classification of security followed by all its subclasses in 6 levels in Section 3.3. Further, the security issues of different types of software systems are covered in Section 3.4. Subsequently, it also analyses security domains to be considered for securing the software systems considered under study. The results that help in identification of the dominance of the security domains and its usefulness to system stakeholders followed by conclusion are covered in Section 3.5. Lastly, we conclude with the summary on the coverage of the chapter in Section 3.6.

3.2 Background

Security of a software system is adversely affected by increasing connectivity, extensibility and size complexity [MCG06]. Security risks have become a common knowledge for the organizations therefore different ways to ensure security are opted such as software security, communication security, network security, etc. Security can also be improved by limiting physical access to the computer system through hardware mechanisms such as biometric identification that impose restrictions on the use of computer systems and programs, operating system mechanisms that enforce rules to avoid un-trusted programs and through programming strategies. It is not always possible to design the systems with foolproof security as security is a problem of comprehensive control. Hence, various methods are required to ensure security of software,
information, and data. It has been observed that security is required in all the steps of Information Processing, such as during read/ write/ modify/ delete operations, transport of information, and storing of information [LINK18, BHW06].

The software systems are challenged by the intruders easily due to presence of vulnerabilities. The flaws may be introduced in a software by developers (knowingly or unknowingly) during design and development, deployer (if system not configured properly), or even during maintenance if the changed system is not tested for security. The vulnerabilities may be discovered even during the operation of the software system. Hence, RedHat classifies security on the basis of impact on a 4-point scale ranging from low to critical for judging the severity of security updates [COX05]. Thus, to understand which part of software development lifecycle introduces more flaws, the security flaws are organized into taxonomy. Security flaws taxonomy on the basis of genesis organizes flaws as intentional and inadvertent. The intentional flaws can be malicious and non-malicious. The flaws can be categorized on the basis of time of introduction during development, maintenance and operations phases; while flaws can also be categorized on the basis of location such as software and hardware. The software flaws can owe to operating system, support and application software [L+94]. Another classification method categorizes security flaws in association with software lifecycle phases as the flaws are the root cause of security vulnerabilities [AZ11].

The kind of security required depends on the project risks, size, communication complexity and development methodology used [LINK19]. To achieve security, the first step is to build security in the product itself [ZD07, FS08]. The next stage involves securing the computer, data, networks and the software from the outsiders and also from the in-house destructive users. Depending on the type of application such as website, ERP, kiosk etc., and type of data such as open, secret, and top secret, appropriate security measures can be implemented. This can be achieved by access control principles, both at hardware level as well as at software level. Hence, classification of security is important which helps a person to understand what all
security measures are required at hardware level as well as at software level for an individual system or for a system connected in a network.

Security has also been classified upon the degree of protection required as top-secret, secret and confidential. The top secret data and systems are of national importance and its unauthorized use can lead to national damage like national defense plans. Unauthorized users of the secret data and systems may also lead to damages that may damage national security and plans e.g. scientific plans [LINK17]. The Common Body of Knowledge (CBK) has classified security issues into application and system development/ operations, access control systems/ security, architecture/ operations, telecom and network/ operations, operation security/ application and system, telecom and network/ hardening/ operations and legal. Based on this classification, Security Reference Guide has classified security into application security, operating system security, network security, hardening the system, wireless security, and legal and ethical issues of security domains [PF04]. Security has also been classified as computing security, data security, application security, information security and network security [LINK20]. Taxonomy of security considerations define various classes of risk that owe to application layer, network layer and platform layer. Some of the threats include data exposure/ manipulation; functional manipulation; application, network and system denial of service; unauthorized system administration etc. [WW03]. Thus, literature review reveals that security has been classified in different domains and has been explained in a particular aspect. However, there is a need to classify security as a whole in the IT environment covering different domains.

The literature also deals with the security issues of specific type of application. Security issues involved in healthcare domain needs to focus on secure communication by message encryption, authentication and authorization [XLG08]. E-commerce threats are mainly privacy issues, viruses and Trojan horses; where virus acts as Denial-of-Service (DoS) attack tool [MT02]. Networks and host security cannot overcome the root cause of security threats; hence OWASP presents security of an enterprise web application from the
viewpoint of application security [LEB]. It can be observed that the causes of security threats have been argued and solutions are provided but are not able to present all the security aspects required to secure a software system. Thus, there is a need to identify the security domains that must be considered to deal with the security threats of various categories of software system. It reveals that security is a multi-faceted problem and requires multiple solutions. The managers and developers cannot rely on only few security domains.

3.3 Proposed Hierarchical Classification

To understand the various dimensions of security, we classify security hierarchically at six levels ranging from Level 1 to Level 6. Level 1 defines the major types of security required by the organization for implementing secured software systems. It categorizes security into further three classes viz. Hardware security, Logical security and Security management as shown in Fig. 3.1. Level 2 to Level 6 define the subtypes for achieving parent level security. In following section, we discuss the proposed hierarchical classification of security in IT environment:

3.3.1 Hardware Security

It is concerned with secured access of the computer hardware, networks etc. or in general physical devices so that unauthorized users are not permitted to use the system [MIC09]. This can be done through non-electronic or electronic devices or by the combination of the two to prevent access to hardware. Examples may include lock and keys, security guard, guard dogs, alarm system etc. [LINK21, LINK22]. The systems are also required to be protected from heat, dust and pests. A surge protector and UPS can guard the computer physically against the fluctuations and power outage. Further, system can be secured by separating network and work place into functional areas and by separation of duties. Separation of duties ensures that an individual can not complete a critical task by himself [LINK23]. Another mechanism to safeguard the systems
Fig 3.1: Proposed Hierarchical Classification of Security
physically is through the use of Microsoft’s Active Directory software application. Active directory is hierarchical framework of objects such as users, printer, computer or a group. It defines permissions to logical assets defined by schedules, groups and times [PIN12]. Hardware security can be achieved via electronic and non-electronic means.

**Non-electronic Security**

Non-electronic hardware security can be achieved by mechanized keys and smart card that allows physical access to authorized users of the system. Security to the physical location of the computer system can be provided by double door system, fences, badge systems, site selection, computer system friendly fire extinguishers, guard dogs, security guard who is supposed to check that no body takes in and out any objectionable material such as CD, pen-drive, etc. Most of the organizations provide systems without floppy drives, CD drives or pen drives to have better control over the system [GR95].

**Electronic Security**

Electronic security prevents access to physical devices through access control devices/ software. The access control mechanisms used can be biometric identification through badge readers, fingerprints, handprints, voice patterns, signature samples, retinal scans etc. These mechanisms provide high level security having low traffic at entrance. The other means to protect computer system and data include backup power, sensors and alarms to detect intrusion and power loss, smoke and fire, and closed circuit TV with video motion detection system. The electronic locks such as fingerprint lock (biometric locks) or keypad locks can also be used to protect the servers or the working place. The access to the system can also be restricted by smart cards which contain the details of the users including biometric identification. Cryptoprocessor, a microprocessor designed for execution of cryptographic algorithms, can be used for various security applications such as storage devices, embedded systems, network routers, etc. It can also be used to manage digital keys providing strong authentication [POL98, KCK].
3.3.2 Logical Security

It is the security mainly by non-physical means such as authentication and authorization methods. Some of these methods include login/ passwords, biometrics, public and private keys, access rights etc. One of the uses of authentication is access control wherein the user can be authenticated using one time passwords, time based passwords, captcha, confirmation emails, Kerberos for network authentication etc. Two general important logical controls are separation of duties and Principle of Least Privilege (PoLP). PoLP requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. Separation of duties refers to dividing the roles and responsibilities so that no single person or process is responsible for a task [LAN03]. Logical controls when applied can reduce the damage caused by unauthorized use of the system resources [GR95]. Logical security can be implemented at different levels viz. development level, system level and at information level. Hence, it can be categorized into three subclasses viz. software security, system security and information security.

3.3.2.1 Software Security

Software security deals in preventing threats from arising in the system itself by reducing the vulnerabilities. It has been mentioned that catching security vulnerabilities in the design phase has been more cost effective than in implementation, which is more cost effective than in testing [HSJ01]. Hence, software must be secured by itself. Moreover, building security during development also increases reliability. The key security design principles are threat modeling and code reviews [ZHA06]. Poor security relates to missing or improper features, defects, errors, poor code quality etc. Some of the missing or improper features may relate to authentication, access control, confidentiality, cryptography, privilege management etc., while defects may relate to unexpected interactions between threads, processes, time, and information rush. Errors may be due to improper error handling code. The common errors that appear during coding can be due to lack of input validation and representation, API abuse,
security features, time and date, hard coded passwords, code quality, encapsulation, and environment. Some of the errors include buffer overflow, cross site scripting, insecure temporary file, empty catch block, null reference, comparing class by name, J2EE mis-configuration, missing error handling page such as error 404 to catch Java exceptions, etc. [TCM05]. The software security can be achieved by system software and application software security.

### 3.3.2.1.1 System Software Security

It is the security through system software such as operating system. Secure operating systems are based on operating system kernels that enforce security policies such as Bell-La Padula model, Biba model, Clark Wilson model etc. [LAN81, LINK24]. Security policies can be based on access matrix or roles. Role based security policy is defined on the roles the user has in the organization. It is more central to the security needs of non-military organizations [FK92]. A single-user OS provides security through boot level password whereas a multi-user OS provides boot level password for the administrator along with access privileges and authentication for the other users. For example, Unix, Windows XP and others use Access Control List (ACL) to implement access matrix. The Alternate Data Stream (ADS) gives a way to hackers to hide their files and later on retrieve them to create security breaches. Similarly, LINUX have security problems because of its complexity, open source updates etc. [PF04]. Proper installations and educating users about security can reduce the problems to a great extent.

### 3.3.2.1.2 Application Software Security

To secure the application software, security must be implemented in the product itself [TIR08]. Security implementation requires us to understand the type of vulnerabilities in the software. CWE lists 25 most common security vulnerabilities found in software such as SQL injection, OS command injection, buffer overflow, XSS etc. [SANS11]. OWASP lists most common web application security such as SQL injection, XSS, broken authentication and session management, cross site request forgery, security mis-configuration,
insecure cryptographic storage, failure to restrict URL access, insufficient transport layer protection, and un-validated redirects and forwards [OWASP10]. OWASP releases the list every three years. Such lists acts as a guide for the system developers to get knowledge about the prevalent vulnerabilities so that preventive actions can be taken. Moreover, secure SDLC can be used from major players such as CLASP form OWASP, SDL from Microsoft and Cigital’s TouchPoint or can be developed in-house. Most of the security issues occur due to non-availability of the security requirements from the users. The other reasons include inefficient design and coding that are not able to incorporate security aspects [AG05]. Appropriate development platform for development of a system adds to security enhancement of the product. Java can be used to develop complex web-enabled applications, while Perl is suited to develop system administration and web-CGI based applications [LA02]. Since no language or development platform can make the software secure, the correct use of features of development platform plays very important role in developing secured software. For example, the problem of buffer overflow mainly occurs with C/ C++ code that can be handled by careful coding [HLV05]. The developers incorporate the security issues as per their own knowledge and understanding. Appropriate software, hardware, and procedural methods can be applied to protect the software from external threats. The application software should be tested for security using penetration testing, and firewalls must be deployed to inspect all traffic.

3.3.2.2 System Security

System security (also known as computer security) refers to the process of preventing and protecting the system against unauthorized access by users of computer system. It also deals with planning to safeguards the system against threats and/ or attacks. The threats are mainly from the hackers that can be insiders as well as outsiders and can be intentional or unintentional [WHI03, SQS00]. The most common method for incorporating security is through access controls that can be achieved by authentication, authorization and audit mechanisms. Authentication determines the users of the system; authorization determines what the users can access on the system whereas
audit identifies what user did when he accessed the system. Some of the authentication mechanisms include passwords, smart card and smart USB tokens. The other methods to protect computer include antivirus software, passwords, encryption, smart cards, library control systems etc. The security mechanisms depend on the type of software system. Thus, system security can be categorized for single user system (not networked) and networked system security since the security requirements for these types of systems are different.

3.3.2.2.1 Single user System (Non-Networked)

This is the safest system but such type of system needs to be protected from unauthorized users if left alone. A single user PC can be protected by password for BIOS or BIOS like programs and screen locking facility. The BIOS password will prevent changes in BIOS setting as well as system booting. Laptops and other mobile devices can be protected by power-on passwords, locking automatically after some inactive time, turning off wireless connections unless required, use encryption for locking sensitive data, etc.

3.3.2.2.2 Networked System

A networked system can be protected by a password, firewall and also by changing the IP address so that no one can share the data without permission. Password provides authentication mechanism for the network users. Once authenticated, the access rights of read, write and execute can be controlled from the server. Audit management software can also be installed on server to check the activities of the users while firewalls can check the incoming traffic for security. Depending on the type of networked system, security can be categorized as peer-to-peer and server based system security.

3.3.2.2.1 Peer-to-Peer System Security

Peer-to-peer networks are concerned with approximately 10-12 users who can share files without the use of a centralized server (true P2P network). Since each node acts both as client and server, implementing and maintaining security features is difficult. Basic security can be achieved by authentication,
authorization and encryption [SUN02]. The downside of P2P is that every system in the network must have same username and password to make the network usable. To make the work easy, users may remove the password after sometime, or network share may allow anyone to access the network leading to security implications. Some P2P protocols (such as Freenet) attempt to hide the identity of network users by passing all traffic through intermediate nodes thereby achieving anonymity [LINK25].

### 3.3.2.2.2 Server based System Security

Server based systems usually are networked with more than 15 computers. It is easier to maintain security in a server-based system as compared to peer-to-peer network. This is because data and other resources reside with server; therefore security mechanisms must be implemented on server. Servers are prone to unauthorized access and DoS attacks. Thus, managing security of the server is as important as managing application or website [LINK26]. In a server-based environment, access rights are assigned to different users through server and the integrity of the users must be verified before allowing access. The management of such types of rights is easy in centralized networks. The server can also be secured by only having required softwares and uninstall which are not required. The server software should be upgraded on regular basis and must install recent security patches. Server must be configured as per the security needs and must not rely on default settings. If numbers of users are large, then different servers must be dedicated to each task or have virtual server for each task so that implementing security is easy. Depending on the type and size of network, major security issues can be implemented through platform and network security.

#### Platform Security

The platform security (or server software security) architecture provides a number of different capabilities, such as access to the network connections or to the complete file system. To access a system resource, a client program must hold the appropriate capability such as an access token that corresponds to access permission of sensitive system resources. The operating system must provide only
essential services and disable the network services that are not required such as Telnet, FTP etc. Strong password policy must be enforced and the password should be changed at regular intervals. While developing server side of the software, appropriate scripting language must be chosen to reduce security flaws as scripting language gives path to hackers to exploit web server. The developers must also be aware of security implications e.g. improper coding in scripting languages may lead to SQL injection, XSS attacks etc. Such flaws are result of trusting the input [TCM05]. The passwords must be encrypted by deploying proper encrypting mechanisms to achieve confidentiality.

**Communication security**

Communication security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized users along with the effectiveness (or lack) of these measures combined together [LINK28]. Thus, networks can be secured by assigning appropriate access rights [SQS00]. Securing network infrastructure is like securing possible entry points of attacks by deploying appropriate defense. The networks can be secured by use of firewall and proxy, antivirus software, password, encryption and protocols. For higher security, computer network authentication protocol, Kerberos, can be installed so that the communicating nodes have to prove their identity on a non-secure network in a secure manner. Kerberos assumes that the network connections are the weakest link in network security [LINK29]. Kerberos uses symmetric key cryptography and optionally public key cryptography. In general, systems are to be protected both at platform level and at network level.

### 3.3.2.3 Information Security

Information security deals with the confidentiality, integrity and availability of information. Information security also deals with access to Information System (IS), secure communication, security management, and development of secured IS [SO07]. Information security can be achieved by proper information security policies, staff training and education, risk assessment
and risk treatment plan etc. The security plan must identify the assets, the risks associated along with the risk acceptance capacity and the procedures to keep the risk at acceptable levels. Information security is mainly an issue of web security and data security; therefore, it is bifurcated into two sub classes.

3.3.2.3.1 Web security

The security problem mainly arises due to sharing of the data through Internet. Almost daily, new security risks are being identified. The confidentiality, integrity, and availability of information on the Internet are three basic security issues [DEK97]. The main categories of the threats for the information security include Intrusion or Hacking, Viruses and Worms, Trojan Horse, Spoofing, Sniffing, DoS etc. [JES06]. Internet security can be achieved by access control services and communications security [OPP97]. The web-based system can use Kerberos technology, intrusion detection system along with the firewall etc. The web security can be achieved via server security and communication security.

Server Security

The computer that hosts web server is vulnerable since it is on the "public" Internet. Since a web server can be accessed from outside the organization, hence it is more prone to attacks such as DoS attacks, pishing attacks and unauthorized access. It should be isolated from internal network by placing it in a DMZ or perimeter network. The main risk occurs when users connect to databases of web servers to access information [SHI05]. The security problems are mainly due to flaws in design of hosted application, flaws in server operating system, weak passwords, and lack of operational control [CERT-In04]. Internet servers should not mount general files required by users and should avoid general user logins. The virus scanning software should not be disabled at any time. Thus, defense should be applied in depth such as perimeter defense, host defense, application defense and data/ resources defense to secure server.
Communications Security

The communications can be easily established using HTML but it may not provide security. Measures to secure communication include cryptosecurity, transmission security, emission security and traffic analysis [NASA]. These measures are designed to protect transmission from interception. Cryptosecurity deals with sound cryptosystems and their use. Cryptosystems results in confidentiality and authenticity of the transmitted data. The transmission security is concerned with measures designed to protect transmissions from interception and exploitation by frequency hopping, spread spectrum etc. For business sites, the security can be implemented with the help of Secure Socket Layer (SSL) and Secure Electronic Transaction (SET) protocols [TRP03]. SSL ensures integrity of data between web server and the browser by establishing an encrypted link to secure online transactions and customer data while SET protocol is for secure electronic card transaction [LINK30]. The data when transmitted should be encrypted and private and public encryption key infrastructure should be used. Firewalls, proxy servers, Virtual Private Network (VPN), Kerberos are some of the methods to stop unnecessary information, sites and traffic.

3.3.2.3.2 Data Security

In an organization, data is the most critical asset. Data can be intellectual or financial property, or personal identification detail that needs to be protected. For an organization, data loses cost huge amount of money as well as loss of reputation and goodwill in the market. Data security includes safeguarding the data against the unauthorized and authorized users; intentionally or unintentionally to achieve data integrity and data confidentiality. Securing the perimeter is not sufficient; therefore the data security needs to be achieved by logical and physical security.

Logical Security

Logical security of data is achieved by authentication, authorization, and encryption. A database user can be authenticated by use of password. Authorization can be implemented through access controls in a database software
so that only authorized users can read/ write/ modify the data. Implementing PoLP makes sure minimum rights for the user to accomplish the work. It helps in meeting integrity objectives and minimizes the damage caused by accident or error. PoLP also ensure minimum rights for access to stored objects in files, flow of information from one stored object to another, inference of confidential values stored in statistical databases, and encryption of confidential data stored in files or transmitted on communication lines [DD79].

**Physical Security**

The data can be secured physically by taking backup at regular intervals and keeping it at secured place as well as through anti-virus software. The sensitive data must be encrypted during backup, if available, whether kept on PC or other removable device. It also includes the security of the database server.

**3.3.3 Security Management**

Security management focuses on introducing methodologies that are practical and feasible to achieve security. Licensed version of software requires money to procure but pirated copies are easy to get and are very cheap. This causes financial loss to the company. Legal compliance help to solve this problem to some extend by the help of copyright act. The managers and developers should also be aware of the security policies, the formal models and the legal compliances such as HIPPA, SOX etc. The appropriate security policies/ formal models/ legal compliances should be applied depending on the type of application. For example, HIPPA is concerned with security and privacy of individually identifiable health information in U.S. providing three types of security safeguards administrative, physical, and technical [LINK31]. Security can be successfully achieved through policies of management, organization and government. The organizations should also follow the standards such as Common Criteria (CC), SSE-CMM, ISO/ IEC17799 etc.
3.3.3.1 Organizational Policies

The organization’s security policy can be defined by access control, information flow and confidentiality policies [SCH00]. Security can be achieved by developing good basic working practices and establishing procedures to maintain it. The security policy is also important to create a security-conscious atmosphere and establish a disciplined approach. The staff should be reliable (The HR manager should test a person before recruiting). Sensitive information should be split into sections that only authorized staff should handle it; no member of staff should have access to all the information [LINK18]. The organizational policies may also include Team Software Process (TSP) and Personal Software Process (PSP) for process improvement. TSP develops mature and discipline software engineering practices that help to develop reliable software product in considerable less time and cost [HUM00].

3.3.3.2 Management Responsibilities

The management must do risk analysis, should formulate security policies, develop security plan and architecture. The management control may include deciding on security policies and procedures. The policies can be formulated on disaster recovery, contingency and emergency planning as well as background investigations to analyze potential risks of future performance. The other policies may include security awareness and technical training to the staff members, separation of duties to help deter fraud, user registration for computer access, performance evaluation to encourage quality performance and also providing vacations as tensed employees may make more errors [KT]. The management must also formulate plans for access control policies to help deter malicious users through role-based access control [FK92].

3.3.3.3 Governmental Policies

*IT Act 2000* provides rules and regulation for the security of computer hardware, software and procedures; and copyright so as to reduce piracy. It also gives provision for digital signatures so as to authorize the document. The *IT Act 2000* have laws for various offences such as tapering with computer source
documents, hacking, breach of confidentiality and privacy, cyber regulations etc. [ITACT00].

3.3.3.4 Standards

A number of international standards are available that provides guidelines for information security. TCSEC provides guidelines for user documentation that describes protection mechanism, the procedures for examining and maintaining the audit files etc. Similarly ISO/IEC 17799 offers comprehensive set of controls for initiating, implementing, maintaining and improving information security. It provides guidelines which comprises of two parts, first part is code of practice and other part gives specification for information security management like security policy, asset management, physical and environmental security etc. [ISO05]. ISO/ IEC 18028-3 provide telecommunications and information technology industries cost-effective comprehensive security solutions [LINK33].

3.4 Software Systems and Security Issues

The software systems are developed based on organizational scope and the technology used for implementation. Depending on organizational scope, projects can be based on Internet, Intranet, and Extranet. Based on the underlying architecture, software system can use client/server, web technology and cloud based technology. The websites can be static or dynamic depending on the contents of the website. In the same context, we have selected 10 types of software systems namely; static website (P1), dynamic website (P2), web-based enterprise application (P3), Intranet based systems (P4), Extranet based systems (P5), client/server based systems (P6), e-commerce based systems (P7), Kiosk based systems (P8), cloud based systems (P9) and desktop based systems (P10). The security required for the various types of software systems are discussed below.
P1. Static Website

Static websites are based on one-tier architecture. It is normally an informative website containing organizational profile and information about its products and services. Site may also provide mechanism to contact the organization through e-mail. Static website is normally developed using HTML, CSS, Java Script and other such related technologies. It provides same information to all its users hence it presents lowest risk as it does not contain any sensitive information. Since it does not contain any script that needs to be executed at server hence does not require specific security planning. Poorly designed site may leave sensitive information visible and may suffer script injection. For example, files placed in the site’s hierarchy can be retrieved by Internet user by adding path name to the site’s URL. Such security flaws can be avoided by careful planning and implementation in appropriate scripting language and exploiting its security features. While deployment, static website can be self certified for security clearance.

P2. Dynamic website

Dynamic website is based on two-tier architecture. It allows user to view data and query the system. Dynamic websites such as yahoo.com, msn.com etc. can be developed in DotNet, PHP, Java, Ruby-on-Rails, etc. with backend as MySQL, SQL Server, Oracle etc. The scripts executing at the server pose majority of security risks. Appropriate platform such as Java can be used to implement security features provided by it. For example, applet in Java has minimum authority on the client machine while Active X control in VB gives complete access to all the resources of the client machine [FO01]. The data sent in the form of plain text leads to the web communications insecurity. For example, the personal data gathered using form must be encrypted when sending over communication channel to ensure security of data from eavesdropping. The authorization rights of server platform must permit the modification/ deletion of web contents by the authorized user. The web applications are vulnerable to attacks such as XSS, buffer overflows, SQL injection etc. XSS is a result of
accepting web request or data from un-trusted sources. The data is then sent to web server without validating malicious contents [LINK34]. Some other common attacks include buffer overflow and SQL injection. Most of these vulnerabilities are result of insure coding. The databases must be logically secured by authorization rights for accessing/ addition/ modification/ deletion of the data, while physically securing data through regular backups.

**P3. Web-based Enterprise Application**

The web enterprise applications such as ERP and B2B sites are based on 3-tier architecture and can be developed using DotNet, PHP, Java, Ruby-on-Rails etc. with database as MySQL, SQL Server, Oracle etc. Core security services of web applications i.e. confidentiality, integrity and availability are exploited by the known vulnerabilities. The classes of vulnerabilities are mentioned in CWE, *OWASP Top 10* etc. that includes XSS, buffer overflow, authentication and session management, insecure configuration management, etc. The vulnerabilities focus on applications’ insecurity that can be addressed during the development process. Secure intranet infrastructure is attributable to access control services and communication security services [J+01]. Access control ensures confidentiality and integrity by protecting data against its unauthorized use during rest as well as during communication. The access control can be decided by the management with the help of security models such as discretionary access control (DAC), mandatory access control (MAC) models, role-based access control (RBAC) or task based access control (TBAC) models. The incorrect usage of protocols may lead unauthorized users to modify/ delete/ corrupt data during transmission. The data during communication over the net can be secured using PKI facilities in the form of *SSL/ TLS, IPsec*, and *SSH* protocols. The platform such as .NET framework provides key management through WebPermission class that controls the accessing rights of HTTP Internet resources. In enterprise applications, the web and database contents can be altered only by authorized users. The security features provided by databases helps secure the data at rest by granting access rights. The network servers of the enterprise application can be further secured by firewalls to restrict illegitimate traffic. At hardware level,
firewall can be configured to restrict IP addresses and the communication ports [FO01].

**P4. Intranet based Systems**

Intranet is based on Internet technology and uses connectionless protocol TCP/IP to share and use information by the utilizing web pages within an organization. Such systems (e.g. web-based HRM) can be developed on the same technologies as Web-based applications. Since Intranet provides many facilities to the employees such as email, message boards, company news etc.; hence faces security challenges especially from insiders. The insiders may break databases to gain advantage from confidential information. Hence, data must be protected by encrypting confidential data such as password and enforcing access rights based on roles [TC97]. The access rights can also be set for accessing the web pages based on organizational policies. It can be depicted through Access Control Lists (ACL) where subject represents user and object represents a web page [L+11]. Physically, the data can be secured through regular backups. The Intranet must also be protected from the outsiders as the insiders use the same browser for accessing Intranet as well as Internet. We present a case study on system security of Texas Health Resources, a geographically dispersed organization using Intranet. The internal access to health care portal of Texas Health Resources is managed by SSL VPN solution. VPN ensures privacy of data of doctors, patients, and other sensitive information. It also allows authentication, authorization and auditing of all transactions. Texas Health care is being developed in compliance with HIPAA [LINK35]. Exploiting the abilities of development platform can also enhance the security of the developed software. For example, .NET has ability to create web service applications (supported by Microsoft’s IIS) [CEL03]. Passwords are the most common mechanism to protect resources of the system. Usually, passwords are easy to guess and can be interpreted. Software systems must account for strong password including characters, numbers, and special characters. Further, the servers need to be physically protected by controlled access through login and passwords, biometric identification, identity card, etc.
P5. Extranet based Systems

Extranet is extended Intranet that allows sharing of organizational resources with the partners often using public Internet. Hence, extranets such as Supply Chain Management systems suffer security threats not only from partners and hackers but also from employees. The security breaches are normally due to unauthorized outsiders, and authorized insiders that may break into the databases for confidential data such as salary. The hackers may breach the system networks through the use of sniffing device, and eavesdropping. A case study of Greenpartners, a company that grow and package vegetables and fruits as per customers’ need, is discussed to identify the security issues of extranet based systems. It uses extranet for linking with the producers to look at market prices and register their supplies. To achieve organizational goal of user friendly access to extranet and ensure confidentiality and authentication, Greenpartners use VASCO’s DIGIPASS technology to allow users to login without installing any specific software. It allows generating dynamic one time password for login to extranet. To protect the LAN, DIGIPASS authentication for Windows logon is installed at the user’s workstation. Thus, it uses same authentication server (IDENTIKEY) for LAN and extranet [LINK36]. Other security concerns regarding extranet can be encryption of data traversing the network, use of certificates, and restricting the services offered to the partners [MEL99]. The extranets can also be protected by use of firewall, VPNs, and secure web servers. The web servers can be secured by proper configuration [DIK01]. The physical security, application software security, system software security, server based communication security, logical and physical data security issues are same as that for Intranet based software.

P6. Client/ Server based Systems

The security threats of client/ server system are mainly due to client, server and the network [WLC99]. The clients are least secured as these are easily accessible. The client machine can be secured through the use of disk drive locks, biometric identification, passwords, and security mechanisms offered by the
system software. Some of the security threats to client/server system include spoofing, browsing, penetration and eaves dropping. Disabling controls not required by the client may also prevent information security threats such as browsing and spoofing [BAY96]. This is due to the fact more the services are provided, more ports are left open for the intruders. Threats due to eavesdropping can be controlled by encryption and token based authentication. The security risks due to networks include XSS, session hijacking, disclosure of private data etc. and are generally due to insecure configuration. XSS and SQL injection are mainly the concerns of server side coding while DOM based XSS mainly owe to client side raising need for application software security. Server can guarantee authentication and authorization through access control mechanisms and encryption of confidential data such as passwords are implemented through operating system. Default operating system settings such as remote registry services, print server services etc. must be granted to users based on access rights and privileges and should be disabled if not required. The access rights and privileges to the various services must be updated from time to time based on organizational policies [M+23]. Further, application based access mechanisms can be implemented through operating system and DBMS. Unauthorized network and system usage can be checked by use of log files. Also, remote access can be restricted by configuring firewall. The data can be secured physically by regular backups and anti-virus software.

**P7. e-Commerce based Systems**

Since the e-commerce based systems rely on Internet, most of the security issues are same as that of web-based enterprise systems. Threats to client systems are mainly due to active content forms, and malicious code such as virus and spoofing. Server threats are due to web-server and commerce server, database, common gateway interface, and password hacking threats [SMB05]. The e-commerce threats can result from attacks as well as technological failure. Such threats may be the result of poorly developed software system and poor server configuration [LINK37]. To understand the security concerns of e-commerce site, we present a case study based on Amazon.com. Amazon.com
provides online catalog to navigate among the range of products offered by the site and allows making purchases. It uses databases to store product specifications, product availability, shipping information, stock levels, and other related information. It also manages customer and supplier details, shopping cart details along with the previous purchase records to know about customer preferences. The site allows payment through credit card. It suffers security vulnerabilities such as XSS and single wrapping attack. Security can be implemented through the use of public-key cryptography, digital signature and digital certificate for ensuring confidentiality, authenticity and integrity. SSL and SET protocols are used to ensure communication and transaction [LINK30, LINK38]. The implementation related security flaws are due to platform and application software related security flaws. Physically data must be secured through backups.

**P8. Kiosk based Systems**

Kiosks are single stand-alone systems providing services such as airline check-in, tourist information, ATMs etc. The Kiosk systems require physical, network, application software, operations security and software solutions for security. Some of the risks of Kiosk system are related to thefts, network jacks, media devices etc. The Kiosks systems can be protected physically by custom keyboards, cabinet locks, diskless CPUs, BIOS setting and passwords, alarm, etc. The networks can be protected by firewalls, spyware, secure wireless deployment, and DMZ setups for kiosks [UHL06]. Kiosks also need to be PCI compliance if it accepts credit card information and perform online transactions. Kiosk software provides minimum functionality to its users as it is based on PoLP. The Kiosks systems disable standard input dialogs provided by the operating system such as “open with” or “save as” dialogs in Windows operating system. The Internet based kiosk also blocks ActiveX and Java Applets, downloading of files, browsing menus that allow too much configuration control to the user and prevent accessing URLs not applicable to function tasks. It also disables certain short cut keys combinations [CRA08, LINK39]. Thus, most of the security control relate to configuration settings of operating system, browser, networks and physical
security. The application software and the database software must also provide appropriate access rights for various types of users. The application software should implement remote monitoring function that allows the deployer to override changes made locally. The software should eliminate the keyboard completely and allow only touch screen and virtual keyboards to make it nearly impossible to activate certain event or shut down. It eliminates the use of shortcut keys to obtain access to the applications and stored files [SLA11].

**P9. Cloud based System**

Cloud based systems uses many technologies such as networks, databases, operating systems, etc. Hence, the security flaws related to these technologies contribute to the insecurity of cloud based systems [H+10b]. The security domains affecting security of cloud include application security architecture, software development lifecycle, economics, metrics, tools and services, and vulnerabilities [CSA10]. Some of the threats to cloud based systems include DoS attacks, side channel attacks, authentication attacks and Man-in-the-middle cryptographic attacks [GRE]. Further, the new threats are added to cloud’s run-time environment due to the three layers of cloud computing services i.e. Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The security services provided by IaaS provider are Web Application Security Scanning, Source Code Analysis for Web Application Firewalls and Host based Intrusion Detection/ Prevention System (IDS/ IPS). Such security services facilitate security at application layer and support the customer in fulfilling application specific compliance requirements [CSA10]. In a case study based on biggest cloud storage provider Dropbox, its weaknesses have been reviewed that affect the software system using cloud. The weaknesses have been the result of not verifying the hash result of the files and the host ID authentication [M+11]. Thus, in a cloud based system, main security issues lies with the cloud itself while the other risks are due to the application software.
P10. Desktop based Systems

The desktop based software systems are safest as compared to all the types of systems. Such systems can be secured by password for user authentication at operating system and application level, and by means of biometric identification to prevent malicious users from taking charge of the system.

3.5 Results and Conclusion

In this chapter, we explored the different types of software systems discussed in Section 3.4 to examine the research objectives. Based on the data collected through research articles, company websites, and case studies, we analyzed using qualitative data analysis techniques. Coding method is applied to identify security trends [SEA09]. The coding method promotes the identification of the security issues of the software product and categorizes them into various security domains as discussed in Section 3.3. The nodes of the hierarchical classification represent the security domains. The security domains considered are hardware security (S1), application software security (S2), system software security (S3), single user system security (S4), peer-to-peer network security (S5), server-based system security (S6), server-based platform security (S7), server-based communication security (S8), web-server security (S9), web communications security (S10), logical data security (S11), physical data security (S12) and security management (S13). Table 3.1 facilitates in identifying the security trends and provides generalized view of security considerations for the various types of projects.

In our study, we have analyzed the type of security required for the various software systems. As seen from Table 3.1, application software security may be considered for all software systems but the main security concerns for application software security are mentioned as passwords and secure coding. It has been mentioned that 75% of breaches are mainly due to vulnerabilities in the applications although most of the security efforts lie with the networks [LIM09]. It has also been argued that considering security throughout the development
### Table 3.1 (a): Categorization of Security Issues

<table>
<thead>
<tr>
<th></th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
<th>P4</th>
<th>P5</th>
<th>P6</th>
<th>P7</th>
<th>P8</th>
<th>P9</th>
<th>P10</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>Firewall, CCTV cameras, locks, biometric identification etc.</td>
<td>Firewall, CCTV cameras, locks, biometric identification etc.</td>
<td>Firewall, CCTV cameras, locks, biometric identification etc.</td>
<td>Firewall, CCTV cameras, locks, biometric identification etc.</td>
<td>Firewall, CCTV cameras, locks, biometric identification etc.</td>
<td>Firewall, spyware, locks, custom keyboards, diskless CPUs, BIOS password, alarms, CCTV cameras, etc.</td>
<td>Firewalls, spyware, locks, custom keyboards, diskless CPUs, BIOS password, alarms, CCTV cameras, etc.</td>
<td>Firewalls, spyware, locks, custom keyboards, diskless CPUs, BIOS password, alarms, CCTV cameras, etc.</td>
<td>Firewalls, spyware, locks, custom keyboards, diskless CPUs, BIOS password, alarms, CCTV cameras, etc.</td>
<td>Firewalls, spyware, locks, custom keyboards, diskless CPUs, BIOS password, alarms, CCTV cameras, etc.</td>
</tr>
<tr>
<td>S3</td>
<td>Secure OS configuration</td>
<td>Secure OS configuration</td>
<td>Secure OS configuration</td>
<td>Secure OS configuration</td>
<td>Secure OS configuration</td>
<td>Secure OS configuration</td>
<td>BIOS password</td>
<td>Passwords</td>
<td>Passwords</td>
<td>Passwords</td>
</tr>
</tbody>
</table>

Contd …
Table 3.1 (b): Categorization of Security Issues

<table>
<thead>
<tr>
<th></th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
<th>P4</th>
<th>P5</th>
<th>P6</th>
<th>P7</th>
<th>P8</th>
<th>P9</th>
<th>P10</th>
</tr>
</thead>
<tbody>
<tr>
<td>S4</td>
<td></td>
<td></td>
<td></td>
<td>Passwords, biometric identification</td>
<td>Disable save as, open with etc., block download, browsing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Log files, network usage etc.</td>
<td></td>
<td></td>
<td></td>
<td>By use of cloud services</td>
</tr>
<tr>
<td>S8</td>
<td></td>
<td></td>
<td>Encryption</td>
<td>Encryption</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S9</td>
<td>User authentication (Optional)</td>
<td>Data and user authentication</td>
<td>User authentication</td>
<td>User authentication</td>
<td>User authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Contd…
Table 3.1 (c): Categorization of Security Issues

<table>
<thead>
<tr>
<th>S10</th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
<th>P4</th>
<th>P5</th>
<th>P6</th>
<th>P7</th>
<th>P8</th>
<th>P9</th>
<th>P10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sending data in plain text</td>
<td>PKI, SSL/ TLS, IPsec, SSH</td>
<td>Firewall, proxy server, VPN</td>
<td>Firewall, proxy server (if external connectivity)</td>
<td>Firewall, proxy server (if external connectivity)</td>
<td>Firewall, proxy server (if external connectivity)</td>
<td>PKI, cryptography, digital signature, and certificate, SSL/ SET</td>
<td>Firewall, switches, router, IDS/ IPS</td>
<td>Firewall, switches, router, IDS/ IPS</td>
<td>Firewall, switches, router, IDS/ IPS</td>
</tr>
<tr>
<td>S12</td>
<td>backup</td>
<td>Backup, antivirus</td>
<td>Backup, antivirus</td>
<td>Backup, antivirus</td>
<td>Backup, antivirus</td>
<td>Backup, antivirus</td>
<td>Backups, antivirus</td>
<td>Backups, antivirus</td>
<td>Backups, antivirus</td>
<td>Backups, antivirus</td>
</tr>
<tr>
<td>S13</td>
<td>Self certification for security clearance</td>
<td>Security cert, Access control using RBAC, MAC, DAC</td>
<td>Access control using ACL, RBAC, digital cert, industry standard</td>
<td>Access control using ACL, RBAC, digital cert</td>
<td>Access control using ACL, RBAC, digital cert</td>
<td>Access control using ACL, RBAC, digital cert</td>
<td>Digital certification, digital signature, PCI compliance</td>
<td>PCI compliance, PoLP</td>
<td>Organizational policies,</td>
<td>Organizational policies,</td>
</tr>
</tbody>
</table>


process of the software can substantially improve the security of the software [D+04, DAU10]. Security management is considered to be next important aspect for securing the software systems. Except for desktop systems, security management is required for all the types of software systems. Most of the software systems are considering organizational policies to secure the systems. Physical data security is important to protect the data against the loss due to data corruption. Logical data security is required in web-based enterprise application, intranet, extranet, client/server, e-commerce, dynamic website, and cloud based system. According to Symantic, majority of IP theft is committed by the technical insiders who are authorized to access the data. Hence, the management needs to focus on access control matrix and role based access control mechanisms [LINK32]. Web communication security is important for dynamic website, web-based enterprise applications, Internet, Intranet, Extranet and cloud based systems.

The hierarchical classification of security and its importance in various types of software can be beneficial to management, developers as well as system and network administrators in addressing the various security issues regarding the type of application being developed. The usefulness of the classification to the various stakeholders is discussed below:

**Management**

The security management personnel may be able to focus on the key security aspects required for the implementation and maintenance of the system. Classification shall also help to focus on the perimeter defense as well as appropriate security policies, procedures, compliances and risk management. The management may also promote the training of the system personnel to manage security of the system.

**Development Team**

The classification guides the system developers regarding the areas to focus while implementing security. The developers mainly have to focus on the software development process, taking into considerations the security features of
platform, hardware, operating system, networking, and communication. It shall guide the team in testing the various aspects of system during development and after implementation.

**Administrators**

The system administrators can focus on securing the data logically and physically. Based on the current security breaches, the administrators can secure the systems by updating the system software configurations, server configurations, and communications security protocols. The systems can also be secured by access control mechanisms for application software, data, and networks. Further, the systems can be secured by means of hardware control that must be updated as required.

Security is a multifaceted problem in the networked environment and therefore requires multiple solutions. Moreover, no matter how good the security devices are, they all are composed of imperfect software. Security is the problem of the applications as well the software and hardware required for securing the system. Mostly, problems arise not only from unexpected interactions between security software and application software, but also due to human operational errors which may be deliberate or unintentional. Thus, security of a system must take into consideration the security features from the various security domains such as hardware security, application software security, communications security, organizational policies, etc. The classification will help the various stakeholders in systematic consideration of security for different kinds of software systems.

**3.6 Summary**

In this chapter, we presented hierarchical classification of security in an attempt to understand the different security dimensions while implementing software system. At Level 1, Security has been classified as physical security, logical security and security management based on major types of security
required by the organization for implementing secured software systems. Security is further classified at 5 more levels ranging from Level 2 to Level 6. Based on the classification, various security domains are identified required for secure implementation of software systems. Further, we discussed various software projects such as web-based applications, dynamic website, client/server based, kiosk based software systems etc. Based on the analysis, it has been recognized that the application software security is the key for secured software systems although security has to be treated as an integral part of the overall system design. The classification indicates the need for considering various security domains during the development of secure software systems. The hierarchical classification may help the managers, development team and administrators to understand and consider security during development of software in a better way.