International Journal of Engineering Research and Development
ISSN: 2278-067X, Volume 1, Issue 3 (June 2012), PP.45-54
www.ijerd.com

Dominance of Security in an Umbrella of Networks

Smriti Jain[1], Maya Ingle[2]
[1]*MCA Department, SRGPGPI*
[2]*Maya Ingle, SCSIT, DAVV, Indore, M.P., India*

Abstract**—**Attacks against networked system are common and increasing, therefore, IT practitioners need to secure the system. Hence, security is recognized as a key feature for sharing data among enterprises and the semantic web. Sharing increases the risk like viruses, fraud, and misuse of data. Data can be secured internally by a secured product and secure settings, as well as externally by using encryption, firewalls, antivirus etc. This paper classifies the networks and their security issues. The paper also judges the dominance of security during development of software meant for different types of networks. The dominance is further verified by the IT professionals from industry.

Keywords**—**Networks, Client Server, Internet, Intranet, TCP/ IP

I. INTRODUCTION

Networks play a major role in the business software and are entry point for a system. Networks are supposed to allow free flow and share the information. The sharing leads to increase in the susceptibility of viruses, fraud, misuse of resources etc. This leads to one of the important aspects of any network i.e. security management. Data security can be maintained by ensuring confidentiality, availability and integrity. Availability can be maintained by fighting against denial of service, integrity ensures trust of data and data source whereas confidentiality refers to the guarantee against eavesdropping [1].

Networks can be classified according to wide variety of characteristics like data transport medium, communications protocol used, scale, topology, and organizational scope. According to the medium, networks can be wired or wireless. Another classification of networks is based on use of communication protocols like Ethernet, Internet Protocol Suite (TCP/ IP) etc. The networks defined on the basis of scale are Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN), Enterprise Private Network (EPN), Virtual Private Network (VPN) etc. Organizational scope defines networks to be Internet, Intranet and Extranet [2]. Networks are also categorized according to different criteria viz. geographic spread (LAN, MAN and WAN), access restrictions (public, private and value added networks), communications model (point-to-point and broadcast model), and switching model (circuit switching and packet switching) [3][4][5]. Network architectures are also defined as peer-to-peer networks and client/ server networks. The layered network architecture makes the introduction of new protocol, technologies and standards difficult. To resolve such problems, non-layered network architectures called Service Unit based Network Architecture (SUNA), Role-Based network Architecture (RBA) and Object-Oriented Network Architecture were introduced [6]. Reference model for Object-Oriented Network Architecture is Modular Communication Systems (MCS) that eases the design of composable, extendable, and reusable network communication systems[7][8]. SUNA has a modularized architecture where a "service unit" (SU) is used as the basic module, and is efficient and easy to expand. The SU is the smallest entity that provides services and hides its internal details. The SU provides services for the application layer and the whole network and doesn't receive any services. The literature reveals that the types of networks have been classified in various ways but not have been categorized under one umbrella. Further, security issues of the various types of networks having layered architecture are covered in the literature, but have no indication of security issues of non-layered architecture as they are still in nascent stage. Literature also indicates that the networks are classified according to different perspectives; still there is a scope to classify the networks in different domains more rigorously. The networks being classified do not discuss security issues according to the development of software.

To understand the umbrella of networks, the paper presents classification of networks and their security issues. It also discusses the dominance of security in various life cycle stages of software development. The rest of the paper is described as follows. Section II presents the network classification according to different domains and the security issues and threats. Section III discusses the dominance of security considerations on the various Software Development Lifecycle (SDL) stages to be implemented on the certain type of network. Section IV presents case study to analyse the dominance of software development life cycle phases on various networks. Finally, Section V concludes with results and conclusion.

II. CLASSIFICATION OF NETWORKS

The following subsections classify networks, as shown in Figure 1, in detail and understand the various security issues associated with them. All the types of networks are protected by firewalls to some extent. The use of networks is also restricted through logons and passwords. The other security measures are discussed along with the classification

A. Networks Based on Size

The networks can be classified according to the geographical area or size (Figure 1-a). It is mainly classified as LAN, MAN, and WAN where LAN can be wired or wireless. LAN can be based on Ethernet or ARCNET (Attached Resources Computing NETwork) supporting bus and star network.

1) Local Area Network: LAN mainly suffers from insider threats that include risk to distributed file system, remote services access, inadequately protected message services etc. It also suffers from outside threats like viruses if connected to Internet. LANs can be secured by adequate access policies, training, and protection mechanisms in the workstation environment as well as during transmission. The security mechanisms for LAN include authentication and authorization, access control, data and message confidentiality, data and message integrity, non-repudiation, and logging and monitoring [9]. Depending on the media used to connect devices, LAN can be wired or wireless.

1.1) Wired LAN: Security can be achieved in wired LAN by access permissions for LAN and as well as computer. Perimeter defense for any wired LAN connected to Internet is implemented by installing firewall software product as wired Ethernet hubs and switches do not support firewalls [11]. Many devices like Virtual Private Network (VPN) concentrators, VPN routers, Dial-in-Servers, etc. that act as gateway to LANs offering remote access must be secured. Remote access authentication, authorization and accounting can be done using remote access server that can act as central control to monitor network access. The most popular wired LAN is Ethernet. Ethernet has the advantage that all systems can monitor the transmission of all other network and this is also the biggest reason for security breaches. The system can be configured to read all details by network administrator and keep track of system usage.

1.2) Wireless LAN: Some of the threats associated with WLANs include rouge access points, denial-of-service attacks, passive capturing etc. 802.11 describe spread spectrum code publicly, and most access points broadcasts SSID multiple times per second; hence provide weak form of security. By default, data transmissions on WLANs are insecure. WLANs can use Wired Equivalent Privacy (WEP) protocol to encrypt data sent over network. It uses 64 bit or 128 bit key entered by user to encrypt the data. The vulnerability with this protocol is that the key is sent prior to the data to be encrypted over the network and the same key is used to encrypt every data packet. Another method used in wireless networks is Wi-Fi Protected Access (WPA) protocol developed by Wi-Fi addressed some weaknesses of WEP. Here individual packets are encrypted separately, but all the devices in the network must use WPA. Another way to add security is by enabling Media Access Control (MAC) address which is printed on Network Interface Card by the manufacturer. Enabling the MAC address filtering will allow to accept connections of the devices with MAC addresses being permitted [11]. Other ways to protect devices is by setting password.

2) Metropolitan Area Network: Security can be attained through VPN which segments private data from other traffic. VPN also encrypts the data between all physical sites. To protect the data during transmission, encryption technology like SSL can be used. A firewall can be installed to restrict unauthorized sites and data. The network managers must carefully manage the VPN user access policies which gets difficult if VPN is provided by ISP [12]. Various VPN solutions are available and are discussed and analyzed in [13].

3) Wide Area Network: WAN connects computers along large distances at various sites. Security can be attained by following the compliance available like HIPPA for healthcare services, Sarbanes-Oxley (SOX) for integrity and privacy in financial world, Family Educational Rights and Privacy Act (FERPA), which controls privacy of student records, grades and related information. Depending on the equipment used in a given wireless system, encryption may be implemented on the transmitter/ receiver, at the point of any firewalls, or by using an additional encryption or VPN device. Security can be implemented by dedicated encryption devices, routers to filter unnecessary traffic, physical controls, authentication policy for the external devices, signatures, monitoring network traffic etc. [1][14].

B. Networks Based on Design

Based on the network design, the networks can be classified as stand-alone systems, peer-to-peer networks, client/ server networks, and application/ server networks. The client/ server systems can be further classified as 2-tier, 3-tier, 4 tier and web-based architectures (Figure 1-b).

1) Stand alone systems (no server-single user): A unique id and password shall identify the user. The password can be set via BIOS settings, operating system settings, and the software settings.

2) Peer-to-peer networks: P2P network do not have a server to control and monitor the network. Hence, such a network cannot be secured instead each workstation is responsible for securing itself by authenticating the users through logon and passwords. P2P systems face DoS service attack, sybil attack where the intruder acquires multiple identifiers to undermine some function of the system. The documents can be secured by signature verification key rather than key based on specific words as these are vulnerable to dictionary attack [15]. If the network is also connected to Internet, then it needs to be secured by installing anti virus software and by restricting the unwanted sites.

3) Client/ Server networks**:** The client server system consists of three components viz. client, server and network. The clients (PCs) are the least secured and are not having same considerations as the mainframes. The clients are easy to use and are easily accessible. Once the client is logged on, even by malicious user, all the services of the client are then available to the logged user. Hence, the client machines can mostly be protected physically, say, disk drive locks, biometric identification, logons and passwords, and other security mechanisms offered by the client platform or installed. Security holes like session hijacking, disclosing of private data, cross-site scripting (XSS) attacks are opened to attackers when configuring Web.config (ASP.NET) incorrectly. A server must guarantee authentication, authorization and data security. XSS and SQL injection attacks are mainly the concerns for server side coding while DOM based XSS in a major concern at client-side. Default operating system settings like remote registry services, print server service etc. are mostly not secure, hence such services should be disabled if not required. More the services provided, more ports are left open for the intruders. Remote access should be restricted to specific IPs. The development and testing should not be done on real life databases as this will open the doors for intruders during testing of the system. The permissions and privileges should be updated from time to time by the administrator. To check unauthorized usage, various log files like for OS, web server, network usage, etc should be used. Moreover, security tools provided with the servers should be used. The detailed description on server security is also provided in [16]. The client server networks can be further classified on architectures, file servers, and classes of applications.

3.1) Networks based on client/ server architecture: Client/ server model is targeted to support user access to data bases and hence has three levels - user-interface level, processing level, and data level. The user interface level contains interface to the user and permits display management, processing level contains the applications, and data level contains the actual data. Based on the placement of the programs for the three levels on client and server machine, the client server defines two-tier and three-tier architecture (multi-tier architecture). The other architectures defined are four-tier and web-based.

3.1.1) Two-tier Architecture: It has high performance with less number of users as it is easy to use and maintain but has less flexibility and scalability. The two tiers of a client/ server architecture can be divided among client and server in five different ways as discussed in [17].In a 2-tierd structure, the web server communicates directly with database server and other network resources, which makes the system more vulnerable. Attacking a web server will make all the network resources available to the intruders. 2-tier can have fat client (the client has application logic layer and presentation layer) or thin client (the client has only presentation layer). Thin clients can be preferred to fat clients as it does not have the ability to become zombie hosts. It is also easier to control application installations downloaded from web and restrict access to websites as compared to fat client [18].

3.1.2) Three-tier Architecture: It provides higher security as there is less software on the client. The middle tier between user interface and database server can either be Message server, Application server or Transaction processing monitors. The security issues include where to implement security i.e at the database level or at the shared business components. But managing overall security is comparatively easier as the application layer (middle-tier) is centralized.

3.1.3) Four-tier Architecture: Four-tier CS architecture may consists of presentation, application, domain and database layers. Four tiers in a web application can be thin client, web servers, application servers, and database servers.

3.1.4) Web based Architecture: A Web based architecture is client server architecture based on WWW technologies, that can be 3-tier architecture having web browser for client, web server for server and database server; or a 4-tier architecture in which presentation tier is split into web services tier and web browser [19].

3.2) Client/ server with file servers: The client server architecture with file servers is divided into three categories viz. centralized computing and distributed processing.

3.2.1) Centralized computing: Centralized computing is considered to be more secure from the standpoint that there are less access points. Thus the authentication, authorization etc. can be controlled via server.

3.2.2) Distributed processing: JAVA offers security through security APIs and also allows development of security manager. CORBA can also help implement identification and authentication, authorization and access control, security auditing, non-repudiation, and administration [20].

3.3) Client/ Server with classes of Applications: Such systems are mainly classified as host based system, client based system, cooperative processing system, and server based processing systems.

3.3.1) Host Based System: Also called Terminal Server based system, is not a true client/ server based system but is like a traditional mainframe environment where the clients acts as dumb terminals and all the processing power lies with server. The only job the terminals have is to provide input and show the display on the monitor [21]. Such types of systems are quite secure as the entire system is controlled via central unit but it suffers from server bottlenecks.

3.3.2) Client Based System: In the client based processing system, all application processing is done at the client whereas all data validation and other data logic functions are implemented at server.

3.3.3) Cooperative Processing system: Application processing is done at both client and server to achieve optimization. Such processing is complex to set up and hence the security concerns.

3.3.4) Server Based Processing: In server based systems, all processing is done at server and the client provides the graphical user interface. Hence, all the major security concerns lie with the server.

C. Network Architectures Based on Layering

The networks can be based on no layer, layered architecture or non-layered architecture as shown in Figure 1-c. The layered architectures classified are TCP/ IP and SNA whereas non-layered architecture is categorized as object oriented network architectures, Role-Based Network Architecture (RBA) and Service Unit based Network Architecture (SUNA).

1) No layer: Such type of system is a standalone system and requires security applicable for any single user system like user id, password, biometric identification, firewall etc.

2) Layered Architecture: Most of the network structures have the foundation on layered architectures. Some of the layered architectures include TCP/ IP and SNA and are discussed below.

2.1) TCP/ IP: TCP/IP protocol suite is required for establishing any communication on the network. TCP uses sequence numbers to ensure that the data is given in correct order and are established during the initial three-way handshake. It gives maximum of 75 seconds to establish connection considering longer delays. The malicious host keeps sending SYN request and fills the listen queue which leads to Denial of Service (DoS) attack or can be used as a tool for IP spoofing. The administrator has to apply some security levels else the flaw could allow remote attackers to cause vulnerable systems to repeatedly restart when processing specific SNMP requests leading to DoS conditions. To accomplish the benefits of TCP/IP, the users and connections must be authenticated and the data traveled must be secured [22][23].

2.2) SNA: System Network Architecture is not so safe anymore hence IBM recommends that number of policy based security like firewall must be applied. SNA threats can even go undetected by intrusion detectors. One of the main reasons for threats is improper configuring the parameters. This is mainly because the SNA mainframe applications were developed when there were not many security threats. Some of the common attacks are spoofing, man-in-the-middle attack, pishing, session forwarding, DoS attack etc.[24].

3) Non-layered Architectures: – The layered architecture makes the introduction of new technologies difficult, hence non-layered architectures are introduced [6]. The three architectures are Object-Oriented Network Architecture, RBA and SUNA are discussed below.

3.1) Object Oriented Network Architectures: It eases the design of composable, extendable, and reusable systems in modular network communication systems and the collaboration with systems dealing with other networking aspects such as network management and open distributed processing.

3.2) RBA: In the layered architecture, a number of unexpected interactions are introduced like firewall, proxies etc. which were not considered during the initial development of Internet. To overcome communication through layered architecture, RBA organized communication using modular protocol unit called roles. The roles are not organized hierarchically and hence provide better communication.

3.3) SUNA: SUNA overcomes the limitation of layered architecture like functional duplication, error detection in multi-layers and the repetition of addresses etc. It uses “service unit” which is the smallest unit that provides services to whole network and doesn’t receive any services.

D. Networks Based on Organizational Scope

The networks can also be classified according to organizational scope as public and private (Figure 1-d). Internet is a public network whereas Intranet and Extranet are private to an organization. The security issues of the networks are discussed below.

1) Public Network: The networks that are owned by any organization and are accessible for all are public networks. Internet is categorised under public network.

1.1) Internet: TCP/IP can be made secure with the help of cryptographic methods and protocols that have been developed for securing communications on the Internet. These protocols include Secure Socket Layer (SSL) and Transport Layer Security (TLS) for web traffic, Pretty Good Service (PGP) for email, and IPsec for the network layer security [25]. IPSec provides security and authentication by cryptography. IPSec protocols, Authentication header (AH) and Encapsulating Security Payload (ESP) provide data integrity, data origin authentication, and anti-replay service. PGP provides confidentiality by encrypting messages to be transmitted or data files to be stored using an encryption algorithm such 3DES or CAST-128 if required by the communicating organizations. Other mechanisms include using firewalls that can be implemented using firewall gateway and filters, malware, and antivirus software. [26]

2) Private Network: Private networks are owned by an organization and are accessible by their employees, vendors, dealers, customers etc. Intranet and Extranet are the privately owned networks based on Internet technology.

2.1) Intranet: Intranet is based on standard Internet technology using a connectionless protocol TCP/ IP, and is hence easy to deploy as compared to WAN. Firewalls and passwords are common mechanisms used for protecting the data, but it does not ensure the security of data "in the wires" unless proper mechanisms are considered. Firewall is a perimeter defence and hence cannot secure the system from insiders. Most of the passwords are easy to guess and hence cannot provide complete security especially from insiders' attacks. The data passing through wires can be "sniffed" and hence can be intercepted. The security goals of Intranet include authentication, privacy, content integrity, non-repudiation, and ease of use. The ease of use is important in the sense that if security system is too cumbersome for users, they may try to circumvent it. These security objectives can be attained through use of Public Key Infrastructure (PKI) using digital certificate technology. PKI is suited for organizations using open networks like TCP/ IP [27]. Data encryption can be used for added security of data. Virtual Private Network (VPN) can be further used to secure the Intranet from the other networks.

2.2) Extranet: Extranet also covers almost the same security issues as that of Intranet. Extranet is more viable to the security breaches and hence each user must be uniquely identified using authentication techniques. A real-time monitoring, altering and auditing facilities must be employed to detect fraud and abuse. A VPN can be used for securing the private network from other networks [28][29].

E. Networks Based on Computing Models

Networks classified on the basis of computing model are distributed computing model, centralized computing model and collaborative computing model (Figure 1-e). The computing models discussed below share almost the same security issues as client server model.

***1) Distributed computing systems models:* –** Processes run on processors. There are various models that show how the processors can be organized and are mainly minicomputer model, workstation model, workstation server model, processor-pool model, and hybrid model and are discussed below [30].

1.1) Minicomputer model: It is an extension of centralized time-sharing systems. In this model, each minicomputer has several users logged on to it where each user is logged on to a specific minicomputer, with remote access to other minicomputers. Early ARPAnet is an example of minicomputer model.

1.2) Workstation model: In this model, several workstations are interconnected by a communication network. For example, university department may have several workstations scattered throughout a building or campus, each workstation equipped with its own disk and serving as a single-user computer. Since lot of CPU time is wasted during idle time like night, these workstations are connected by a high speed LAN so that idle workstations may process jobs of other users logged onto other workstations that are busy. Thus, it is a network of personal workstations. The network can have diskful workstation i.e. each workstation with its own disk and local file system, or diskless workstation i.e. workstation without local disk.

1.3) Workstation-server model: It consists of few minicomputers and several workstations that can be either diskless or diskful. Minicomputers are used for implementing file systems for diskless workstations. Thus each minicomputer is used as server machine that provides one or more services. Servers run server process for managing and providing access to shared resources. Processor is allocated to each user. For example, V-System.

1.4) Processor-Pool model: Processors are pooled together to be shared by all the users as needed. Pool of processors consists of large number of microcomputers and minicomputers attached to a network. Each processor has its own memory to load and run a system program or application program of distributed computing system. Here the user does not log to a particular machine but to the system as a whole. Some of the examples include Amoeba, Plan 9, and the Cambridge Distributed Computing System.

1.5) Hybrid Model: It takes advantages of both workstation-server model and processor pool model. In the distributed models, the resources on computer must be protected against destruction and unauthorized access. The network can be attacked passively or actively. Some of the passive attacks are browsing, leaking, inferencing, and masquerading. The active attacks include viruses, worms, logic bombs, integrity, authenticity, denial, delay, and reply attack. Enforcing security is difficult as there is no single point of control and data travels through insecure communication networks. Encryption is the only means to secure data travelling across the net [30].

2) Centralized Processing Model: This model is also known as thin client computing model and is more secure compared to distributed computing model. This model is again in use with web technology as thin clients are used that work as almost diskless workstation with technology as AJAX.

3) Collaborative Computing Network Model: In this model, nodes also share processing capabilities apart from sharing data, resources, and other services thereby increasing the processing speeds.

F. Networks Based on Topologies

Networks are also classified on the basis of the topologies used (Figure 1-f). Topologies can be ring, star, bus, mesh etc.

1) Bus: In bus topology, the packet is send to all the nodes on the network. If the packet is not for the particular system, it is discarded. This leads to security implications as the hacker may use packet sniffer and receive a packet not intended for its use.

2) Star: In star topology all nodes are connected to single point which means single point of attack. Such systems may be attacked by DoS attack and the entire system may crash by single device.

3) Ring: Data travels many numbers of points before reaching the final destination. But it is harder to tap without altering the network administrator. It is more secure than bus as it has no terminators

III. SECURITY DOMINANCE

The various types of networked systems and the dominance of security in software life cycle stages are shown in Table I. It illustrates that most of the client server based software must consider security especially during design, coding and deployment stages of software development. Most of the multi-user systems are based on client/ server technology. The client and server side software security has to be incorporated during coding stage of system development and further, client and server can be secured during deployment stage.

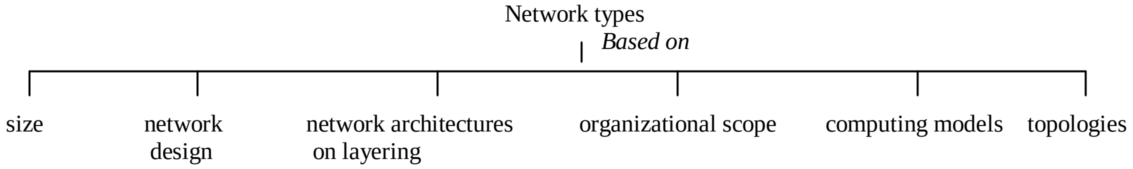

Fig 1: Network classification

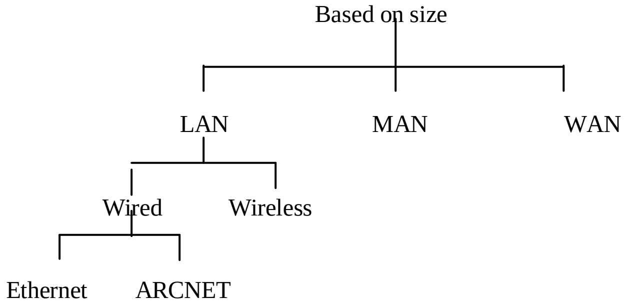

Fig 1 (a): Networks Classification based on Size

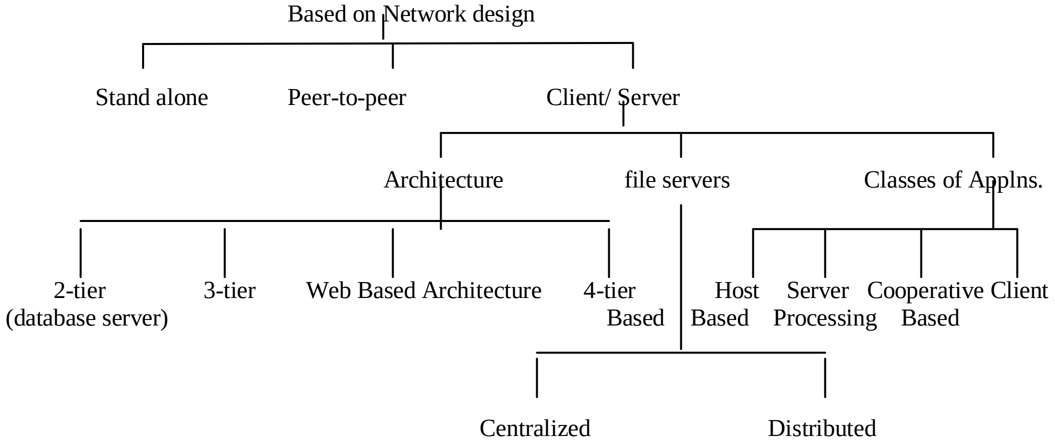

Fig 1 (b): Classification of Networks based on Network Design

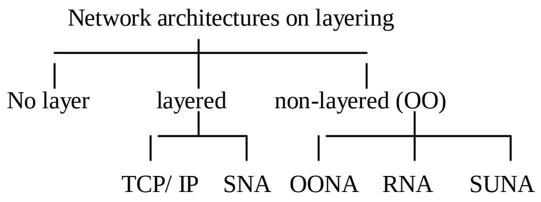

Fig 1 (c): Networks Classification based on Layering

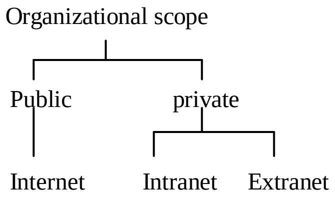

Fig 1(d): Networks Classification based on Organizational Scope

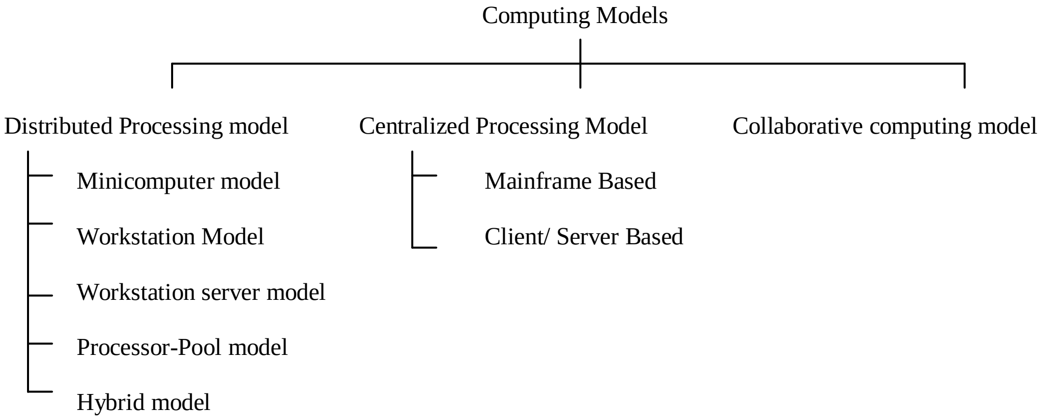

Fig 1(e): Classification of Networks based on Computing Models

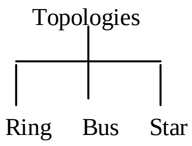

Fig 1(f): Classification of Networks on the basis of Topologies

The security at deployment stage has to be considered from planning itself. Other ways include encryption that provides secure transaction and, firewalls secure the perimeter. Client/ server (C/ S) with centralized server use SSL for server and client authentication. The server must be configured properly to avoid a number of security attacks like XSS, DoS, session hijacking etc. C/ S systems can be designed having thin or thick client. The thin client provides more security as the clients can be diskless or even stateless. The decision regarding type of client has to be incorporated during the design of the system. The responsibilities of client and server will help decide the security measures to be considered for developing the system. During deployment, mapping of drives to users can be enforced to enhance security. Further, Kerberos can be used for network key authentication. During the testing of C/ S based systems, live data should not be used to test the system as this leave doors open for the intruders for that time period.

The most obvious requirement to safeguard a system is through access control. This can be implemented through proper design and implementing it during deployment. In LAN, WLAN, MAN and peer-to-peer networks based applications, authentication and authorization can be attained through logons and passwords whereas confidentiality and privacy through encryption. During deployment, VPNs, PKI etc. can be used for securing the system. Internet, Intranet and Extranet based applications use PKI for authentication, authorization, confidentiality, non-repudiation, and data integrity for users and data while in transmission. Security aspect is weak in P2P systems. Hence, firewalls are used to safeguard network data that can be implemented during deployment.

IV. CASE STUDY

The following section presents case to study the dominance of security on the umbrella of networks during software development process.

A. Data Collection

The data has been collected using a self designed questionnaire to examine the research questions. The questionnaire consists of questions regarding the dominance of security on SDL phases related to different types of networks. The sample consists of 35 software professionals with moderate and high experience with designations as directors, project managers, project leads, senior software engineer etc. Based on the data, percentage analysis was conducted to validate the data.

B. Data Analysis

Percentage analysis was conducted to check the dominance of security on SDL stages during development of software for different types of networks. As seen from the Table II, the dominance of deployment stage was accepted by the respondents when a software is meant to be deployed on any kind of network like LAN, MAN, WAN, P2P, Internet, Intranet, Extranet and Client/ Server. The requirements gathering phase was not given dominance by the respondents as security is more of an implementation issue rather than customer concern. Security is more of design issue of network Administrator than the software issue for LAN, WAN, MAN, P2P, Intranet, Intranet, and Extranet, hence it is also not considered for implementation and testing phase. Most of the respondents accepted that security must be implemented during the deployment phase for any kind of network. The OS considered for client side include Windows NT, Windows XP, Linux etc. can be configured for security during deployment. Network monitoring and management tools like Nagios, MRTG, Kismet, JFFNMS etc. can also be installed. When asked for security dominance on other phases of SDL, more than 85% of the IT professionals agreed that for the software based on client/ server architecture, security plays a major aspect to be considered during phases like design, coding, testing and deployment. Less than 60% response for networks except client/ server systems for design, implementation, and testing phases of SDL shows that major security consideration is login and passwords and hence not given sufficient dominance as it is the basic security requirement. Backups can secure data during maintenance phase. The corrective actions should be taken to prevent further access violations and isolating the violated systems. The amount of violation can be detected by obtaining sniffer traces, copy of log files etc. Hence maintenance was not ranked high as such remedies are obvious security mechanisms adopted by the security administrator.

Table I: Network's security dominance on SDL phases

	Types of networks	Req. Gathering and Analysis	Design	Impl/ Coding	Testing	Deployment	Maintenance
1	Ethernet LAN					X	
2	Wireless LAN					X	
3	MAN					X	
4	WAN					X	
5	P2P					X	
6	2- tier Client/ Server		X	X	X	X	
7	3 - tier Client/ Server		X	X	X	X	
8	4 - tier Client/ Server		X	X	X	X	
9	Web Based C/ S		X	X	X	X	
10	C/ S with centralized server		X	X	X	X	
11	C/ S with distributed server		X	X	X	X	
12	Host Based C/ S		X	X	X	X	
13	Server Based C/ S		X	X	X	X	
14	Client Based C/ S		X	X	X	X	
15	Internet					X	
16	Intranet					X	
17	Extranet					X	

Table II: Impact of Network Type on SDL Phases

	Types of networks	Req. Gathering and Analysis	Design	Impl/ Coding	Testing	Deployment	Maintenance
1	Ethernet LAN	14%	28%	14%	14%	91%	14%
2	Wireless LAN	14%	40%	31%	57%	97%	28%
3	MAN	40%	40%	57%	57%	100%	31%
4	WAN	40%	57%	57%	57%	100%	40%
5	P2P	14%	14%	28%	28%	85.7%	14%
6	2- tier Client/ Server	40%	85.7%	88.5%	94%	100%	48.5%
7	3 - tier Client/ Server	48.5%	85.7%	88.5%	94%	100%	48.5%
8	4 - tier Client/ Server	40%	85.7%	85.7%	91%	97%	48.5%
9	Web Based C/ S	40%	91%	85.7%	94%	100%	48.5%
10	C/ S with centralized server	57%	80%	88.5%	97%	100%	40%
11	C/ S with distributed server	57%	91%	94%	94%	100%	40%
12	Host Based C/ S	40%	91%	91%	94%	97%	48.5%
13	Server Based C/ S	40%	94%	97%	97%	100%	48.5%
14	Client Based C/ S	40%	94%	97%	97%	100%	48.5%
15	Internet	37%	28.5%	31%	48.5%	100%	57%
16	Intranet	37%	57%	48.5%	57%	100%	57%
17	Extranet	37%	57%	48.5%	57%	100%	57%

V. RESULTS AND CONCLUSION

There are a number of views of the IT professionals regarding the dominance of security on networks during software development process as illustrated in Table II. The requirements gathering and maintenance phases are not given acceptance by the respondents as network security is more of deployment issue rather project inception issue for all kinds of projects. During the development of the projects based on client/ server architecture, security needs to be considered during design, implementation, testing and deployment stages. Security implementation during deployment of the project is considered for all kinds of networks.

Communication and data access via networks is key requirement to any business; hence most of the software systems deal with the challenges faced by the security issues. Although network administrators can deal with most of the risks associated with the system being deployed, but major security lies in building the software right. Hence the software system developers must also consider security aspect during SDL for any networked system and incorporate the security within the system. In this paper, we have classified the various types of networks and discussed their security issues to assist system designers and developers assess security considerations in networks. The paper also elaborates on security considerations while developing software intended for a particular type of network. From the software development point of view, the paper will help consider security types in the various sorts of networks.

REFERENCES

[1] (2012) “Ethernet WAN Security How to Protect Business-Critical Data over High-Speed Ethernet Networks,” White paper by SafeNet. [Online] Available: http://www.infosec.co.uk/ExhibitorLibrary/88/High_Speed_Ethernet_Security_White_Paper_by_SafeNet_v4_0_20.pdf

[2] (2012) Computer Networks. [Online] Available: http://en.wikipedia.org/wiki/Computer_network

[3] Sharam Hekmat, *Communication Networks*, PragSoft Corporation,. [Online] Available: www.pragsoft.com/books/CommNetwork.pdf.

[4] R.S.Rajesh, K.S.Easwarakumar and R.Balasubramanian. *Computer Networks – Fundamentals and Applications*, Vikas Publishing House Pvt. Ltd., 2002.

[5] Uyless D. Black. *Data Communication and Distributed Networks.* PHI, 2002.

[6] Y. Wang, M. Xia, F. Yi and J. Zeng. “Research on New Types of Network Architecture,” *In the Proc. of the Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT’05)*, IEEE, 2005.

[7] Stefan Boecking. “Object oriented network protocol”, *Beijing, Machinery Industrial Press* (ISBN 7-111-08076-9/TP), 2000.

[8] Stefan Boecking, et al. “A Run-Time System for Multimedia Protocols”, *Fourth International Conference on Computer Communications and Networks (ICCCN'1995)*, pp.178-185, Sep 1995.

[9] *Specifications for Guideline for The Analysis Local Area Network Security*, Federal Information Processing Standards Publication 191, Nov, 1994.

[10] (2012) Wired and Wireless Networks [Online] Available: http://compnetworking.about.com/cs/homenetworking/a/homewiredless.htm

[11] (2012) Slides on “New Perspectives on Internet,” The Internet, 7th Ed. [Online] Available: http://www.slideshare.net/dpd/tutorial-7-wireless-networking-and-security-presentation

[12] Sixto Ortiz Jr . *Virtual Private Networks: Leveraging the Internet, Computer,* Nov. 1997, pp. 18-20.

[13] Ahmed A. Jaha, Fathi Ben Shatwan, and Majdi Ashibani. “Proper Virtual Private Network (VPN) Solution,” *In the Proc. of the Second International Conference on Next Generation Mobile Applications, Services, and Technologies*, IEEE Computer Society, 2008, pp. 309-314.

[14] Dan McDonald. *Wireless LAN Security*, 2010. [Online] Available: http://www.smslp.com/knowledge/wireless-wan-security/

[15] Allan Friedman and L Jean Camp. “Peer-to-Peer Security”, *Telecommunications Policy Research Conference,* Sep. 2003. [Online] Available: citeseerx.ist.psu.edu/viewdoc/

[16] Karen Scarfone, Wayne Jansen, Miles *Tracy. Guide to General Server Security, NIST, Special Publication 800-123,* July 2008.

[17] A.S. Tanenbaum. *Distributed Systems – Principles and Paradigms*, Pearson Education, 2007.

[18] Paul A. Strassman. 5 Secure reasons for Thin Clients, Baseline, [Online] Available: http://www.baselinemag.com/c/a/Projects-Security/5-Secure-Reasons-for-Thin-Clients-%5B2%5D/

[19] Gagnesh Arora, Deepika Arora. “Web Based Client Server Technology – A Three Tier Architecture” [Online] Available: gagnesharora.com/ieee2.pdf.

[20] April L. Moreno. “Distributed Systems Security: Java, CORBA, and COM+,” *SANS Reading Room*, SANS Institute, 2002.

[21] (2012) Basic Network types. [Online] Available: http://www.pcc-services.com/network_types.html

[22] Jay Nanavati. “Security Issues of 802.11i & TCP/IP”, [Online] Available: http://tifac.velammal.org/CoMPC/articles/38.pdf

[23] Chris Chambers, Justin Dolske, and Jayaraman Iyar. TCP/IP Security, [Online] Available: http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html

[24] Anura Guruge. *SNA Mainframe Security, Software Diversified Services*, June, 2009. [Online] Available: http://www.sdsusa.com/netqdocs/SNA.Security.090721.pdf

[25] (2012) Internet Security,. [Online] Available: http://en.wikipedia.org/wiki/Internet_security.

[26] Acunetix – Web Application Security. [Online] Available] http://www.acunetix.com/websitesecurity/webserver-security.htm

[27] (2012) Guide to Securing Intranet and Extranet. [Online] Available: http://www.windowsecurity.com/whitepapers/guide_to_securing_intranet_and_extranet_servers.html#goals

[28] Karen A. Korow Diks. *Security Considerations of Extranet*. SANS Institute, 2001. [Online] Available: http://www.sans.org/reading_room/whitepapers/basics/security-considerations-extranets_527

[29] Jennifer Jordan. *Extranet Security - A technical overview from a Business Perspectives*, 1997. [Online] Available: http://csrc.nist.gov/nissc/1997/proceedings/053.pdf

[30] Pradeep K.Sinha. *Distributed Operating Systems: Design and Concepts*, IEEE Computer Society Press, Prentice Hall of India Private Ltd., New Delhi, 2004.