International Journal of Information, Engineering & Technology

Volume 10, Issues 2, PP 1-26, ISSN: 2360-9194, April, 2018
Double Blind Peer Reviewed International Research Journal
http://arcnjournals.org
Journal Series: Global Academic Research Consortium (garc)

A Critical Analysis of Web Security Mechanisms

[1]Ukwosah Ernest Chukwuka and [2]Akinyemi Adesina A.
Department of Computer Science, Federal University Wukari, Taraba State, Nigeria
[1]eukwosah@gmail.com, ukwosah@fuwukari.edu.ng

Abstract: *This study critical analysis of web security mechanisms focus on elaboration of various web security vulnerable attacks that exist nowadays. The recent security measures are analyzed in details on how to tackle against vulnerable or malicious attacks emanated from malevolent users, distort the genuine operation of web services performance. The issue of securing our network protocols is vital, to ascertain confidentiality, reliability and integrity among versatile users around the globe. Malevolent users tends to abuse the use of web services for their selfish interest of making profit or causing distortion for smooth and reliable usage of web applications. Software experts, developers and designers have develop many web security software that serves as security mechanisms against abusive and crook usage of web services. This paper intention is to review different security attacks in web applications and services, analysis existing and recent security mechanisms developed to tackle several known web security attacks.*

Key words: *Security mechanism, security attacks, intrusion detection and defense mechanisms.*

Published by
Africa Research Corps Network (ARCN)

in Collaboration with
International Academic Journal for Global Research (iajgr) Publishing (USA)

Strictly as per the compliance and regulations of:

1.0 INTRODUCTION

Web applications have widely grown in the global economy. It has become very important in the fields of commerce, entertainment, social interactions, government and non-governmental bodies. They play vital roles in national infrastructures such as health-care, national security, and power grid, and others. It has become one of the most important communication channels, between several Service Providers and Clients on the Internet. The crucial problems arise as hackers and attackers invent means to distort the genuine operations in the web. These vulnerable attackers' raises strong issue of web security menace.

The web needs security measures, and several security techniques and tools have been developed for the purpose of web security regulations, intrusion detection and defense mechanisms. Despite the security measures developed by Software developers and security providers, the vicious attackers continue to develop new methods of tactical vulnerable attacks to web services operations. Some attackers gang ask for ransom to deactivate dangerous propelled code they injected into web applications, browsers, servers and databases of targeted organizations. Developing web security mechanisms are crucial area that requires serious concerns for researchers to dive into for adequate solutions to web security issues. Many Web security researchers, security specialists, software developers, business owners and corporate practitioners have been tremendously providing solutions as patches to known security attacks on the web. The Open Web Application Security Project (OWASP) have been identifying serious web application vulnerabilities and providing remedies to many of them. The security of web applications have raises concerns and receiving more attention from governments, corporations, and research communities.

2.0 REVIEW OF RELATED WORKS

The authors in [1] propose an Attack Injector Tool (AJECT) to support the discovery of vulnerable attacks in network servers, particularly IMAP Severs. It used predefined test classes of attacks to launch to a target system and apply some sort of fuzzing and mutation testing to automate penetration testing of web applications.

Researchers develop Vulnerability and Attack Injection Tool (VAIT) to provide performance evaluation of web security mechanism. The Intrusion Detection System (IDS) was evaluated by injecting vulnerability and attacking them automatically, the VAIT find weaknesses in the IDS. The VAIT experiments two commercial web applications to check the ability to detect SQL injection vulnerabilities in web application. These scanners were unable to detect most of the vulnerabilities injected, despite that they were easily probed and confirmed by the scanners [2].

According to [4] many security problems are related to how bad different programming languages are in terms of tendency for mistake. String Analysis and vulnerability is very essential in security issue analysis widely researched. Data sanitization technique using reverse proxy is used to prevent SQLi and XSS attacks. This technique is used to sanitize the users input that may be transform into database attack. A filter program is used which

redirects the user input to the proxy server. In a proxy server, data cleaning algorithm is triggered using sanitizing application.

Vega – is GUI – based, cross-platform tool written in Java, which can extended using its Java script API. W3af is a free open-source web application scanner design and implemented for finding and exploiting SQL injection and web application vulnerabilities. Some of the existing web application scanner are based on predefined rules and known defects recorded in vulnerability database [5].

A methodology that use vulnerability databases, such as OSVDB (Open Source Vulnerability Database, to scan for probable existence of directories and files that malevolent users usually try to find out treats as an entry point. Some known scanners like AppScan and Zap Proxy provides rule based SQL injection detection capabilities, through which they can construct a number of attacking exploits. These tools detect points in web application responses to the generated attacks [6].

An author develops a Black-box testing tool for detecting SQL injection vulnerabilities. The black-box approach is based on simulation of SQL injection attacks against web applications. The scope of analysis is limited to HTTP responses and HTML pages received from the application server [5].

The Researchers in [7] mentioned that Pallavi and Trivedi in 2011 gave solution to prevent serious attack that is a wormhole attack by use of digital signatures. It ensures that a sender who wants to send packet to destination node will create a secure path with the help of digital signature verification.

In [8] gave layer approach for processing of data in intrusion detection system. To remove unwanted and redundant data from packets, the layer approach of TCP/IP model is used for the faster preprocessing of data in intrusion detection system.

Authors handle the issue of complexity and throughput that are the problems in intrusion detection system (IDS). They compared several IDS system and provide a scheme that uses the combination of artificial neural network algorithms. The combined algorithm yield better performance [9].

The authors in [10] proposed the algorithm to detect black hole and gray hole attacks in ad-hoc networks. The researchers demonstrated the adaptive approach using cross layer design and prove their theory by using path-based method to overhear the next node. So, it saves system resources by not sending out extra control messages. A collision rate reporting is established to reduce the false positive rate under high network load.

The authors in [11] present Evaluation of Web Security Mechanisms using Vulnerability and Attack Injection**.** They propose a methodology and a prototype tool to evaluate web application security mechanisms. The methodology is based on the idea that injecting realistic vulnerabilities in a web application and attacking them automatically can be used to support the assessment of existing security mechanisms and tools. To provide results, the proposed vulnerability and attack injection methodology study large number of vulnerabilities in web applications. Also, the paper presents the implementation of the

Vulnerability & Attack Injector Tool (VAIT) that allows the automation of the whole process.

A paper titled Fault Injection for Formal Testing of Fault Tolerance used methodology to extend a debugging tool aimed at testing fault tolerance protocols developed by BULL France. It has been applied successfully to the injection of faults in the inter-replica protocol that supports the application-level fault tolerance features of the architecture of the ESPRIT-funded Delta4project. The results of these experiments are analyzed in detail [12].

Fault Injection and Dependability Evaluation of Fault-Tolerant Systems describes a dependability evaluation method based on fault injection that establishes the link between the experimental evaluation of the fault tolerance process and the fault occurrence process. The main characteristics of a fault injection test sequence aimed at evaluating the coverage of the fault tolerance process. [13].

2.1 Security attacks

The security attacks are divided into Passive Attacks and Active attacks. Active attacks are subdivided into external attacks and internal attacks. The summary of all attacks are as follows [3] [14]:

2.1.1 **Passive Attacks** - The attacker listen to channel and packets that contain secret information like IP addresses, location of nodes etc., but it allows the operation of the network. These attacks are difficult to identify. Passive attacks are further subdivided as eavesdropping, traffic analysis, and traffic monitoring.

2.1.1.1 Eavesdropping - The confidential information that is kept secret during transmission are obtained by malicious node e.g. location, private key, public key or even password.

2.1.1.2 Traffic Analysis - Attacker monitors packet transmission to gather vital information such as the source, destination, and source-destination pair.

2.1.1.3 Jellyfish attack - Attacker guilty for unwanted delay of data packets for a random period of time. The attacker introduces the delay in sending packets that was receives. So an attacker succeed to break the performance of the network

2.1.2 ACTIVE ATTACKS - An active attack either obstruct the normal operation of a particular node or target to breakdown the operation of the entire network. An active attack tries to alter or destroy the information that is being exchanged [24]. The active attack can be categorized into two classes: external attacks and internal attacks. External attacks are attacks launch from outside the network. Such attacks can be prevented by using powerful encryption techniques for source authentication and firewalls. Example of external attacks is the wormhole attacks. Internal attacks are launched by the internal Compromised nodes within the network. A single node or multiple nodes could launch an attack individually without collusion and co-ordinate collaboration. It is difficult to identify the internal attacks [19], [20].

2.1.2.1 Denial of service attack (DoS) - Denial of service attack prevents the normal use or management of communication facilities. Example is the disruption of an entire network either by disabling the network or by overloading it with messages so as to degrade performance. In this, attacker does not corrupt data [3].

2.1.2.2 Black hole - In this attack black hole node absorbs all the traffic towards itself and doesn't forward to other nodes [17].

2.1.2.3 Wormhole Attack - An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole [21].

2.1.2.4 Rushing attack - Rushing attacker forward routing packets as quick as possible to gain access to multicast forwarding group before the legal node. By this way rushing attack can slow down the performance of network [16].

2.1.2.5 Jamming attack - A malicious node start monitoring transmission in the network and check at which frequency the communication takes place between the nodes. After that, attacker transmits the signals with the same frequency of the signal to generate weaker signals, disrupting communications, interference or noise [18]. Two types of jammer, High power pulsed full band jammers and Low power partial-band jammers, can be used [3].

2.1.2.6 Sybil attack - A malicious node creates different accounts from different IP addresses in the network. Sybil attacker uses a number of nodes identities simultaneously. In this case the destination node may not be able to detect the misbehavior because the attacker may get access to all pieces of fragmented information or may alter all the packets towards the same destination [3].

2.1.2.7 Location disclosure attack - In the location disclosure attack, the attacker discloses the authentic information regarding the location or structure of the network [16].

2.1.2.8 Byzantine attack - In this attack, a compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services. SMT (secure message transmission) is the secured data communication protocol against Byzantine attack [3].

2.1.2.9 Spoofing Attack - Spoofing attack is also called impersonation attack in which Fake messages are injected into network. Spoofing attack is occurred when a malicious node misrepresents the IP and MAC address of the authentic node through which they uniquely identifies and then hide in the network [8].

2.1.2.10 Sinkhole attack - A sinkhole node tries to attract the data toward itself from all nearby nodes. A malicious node generates fake routing information and presents itself as legal nodes for the route. Sinkhole node attempts to draw all network traffic according to

itself, modifies the data packets, decrease the network life time, create complicated network and finally destroy the network [3].

2.1.2.11 Gray-hole attack - The gray-hole attack is called routing misbehavior attack. In this attack a malicious node behave as a genuine node during rout discovery process. After creation of route, this malicious node silently drops packets which are sent to it. But some time node drops packets partially not only due to its malicious nature but also due to overload, congestion or Selfish nature [3].

2.1.2.12 Fabrication Attack - It is an active attack which breaks authenticity by exposed itself to become the source entity. After become a part of the network it sends error message to other legal nodes to say the route is not available any more. Then other node will then update their table with this false information. By this way, it drops the routing packets, forwarding packets and discloses the authentic information such as IP or MAC address of the valid nodes. There are three kinds of fabrication attacks are to generate route error messages, to corrupt routing information and to flood routing table [3].

2.1.3.13 Replay attack - This attack usually targets the freshness of routes. In this attack an attacker firstly record the message and then resend the old message to the other nodes to make update their routing table to stale routes. To add time stamp and reject the old message as suspicious and use asymmetric key to message are used for preventing replay attack [3].

2.1.3.14 Resource consumption attack - In this attack, malicious node forwards unnecessary packets to the victim node and always request for route discovery to consume the battery life, network bandwidth [3].

2.1.3.15 Flooding attack - In flooding attack, a malicious node may also inject false packets to consume the available resources into the network, so that valid user can not able to use the network resources for valid communication [19]. The flooding attack is possible in all most all the on demand routing protocols such as SRP, SAODV, and ARAN (Authenticated Routing for Ad-Hoc Networks) etc. flooding attack can be categorized in two categories, RREQ flooding and DATA flooding [21].

3.0 The Architecture of the System

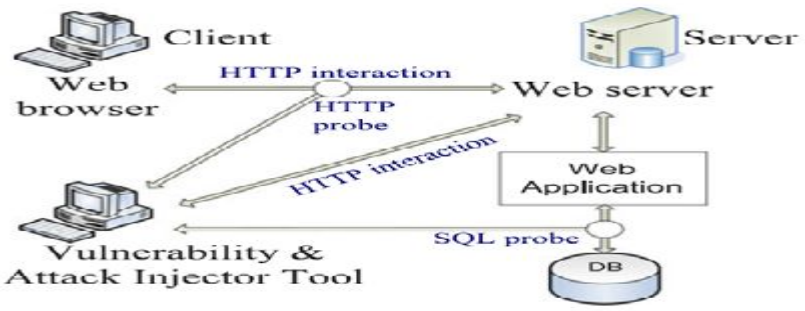

Figure 1: VAIT in typical setup [3]

In figure 1, the attack injection uses two external probes, one for the HTTP communication (HTTP PROBE) and other for the database communication (SQL PROBE). These probes monitor the HTTP and SQL data exchanged, and send a copy to be analyzed by the attack injection mechanism. This is a key aspect of the methodology to obtain the user interaction and the results produced by such interaction for analysis, so they can be used to prepare the attack [3].

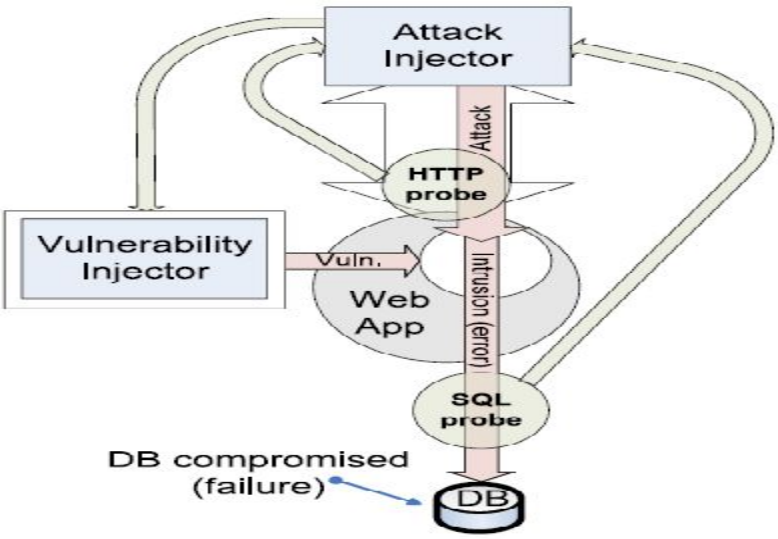

Figure 2: VAIT internal components [3]

In figure 2, this tool HTTP probe and SQL probe are two main components; these two components are used to monitor the communication between web browser and web server, web application and database respectively. These two probes are used to gather information related to various vulnerabilities like SQLi and/or XSS. In VAIT Vulnerability injector is used to inject vulnerabilities in to the web application ,after injecting the vulnerabilities the web applications security mechanisms performance is monitored and check for the errors occurred due to the injected vulnerabilities, if there is any error it will be reported to the vulnerability and attack injector tool through HTTP and SQL probes. Similarly the attack injector is used to inject the attacks in to the web application and its performance is observed and reported to the vulnerability and attack injection tool through various probes used in system (e.g. HTTP probe and SQL probe) [3].

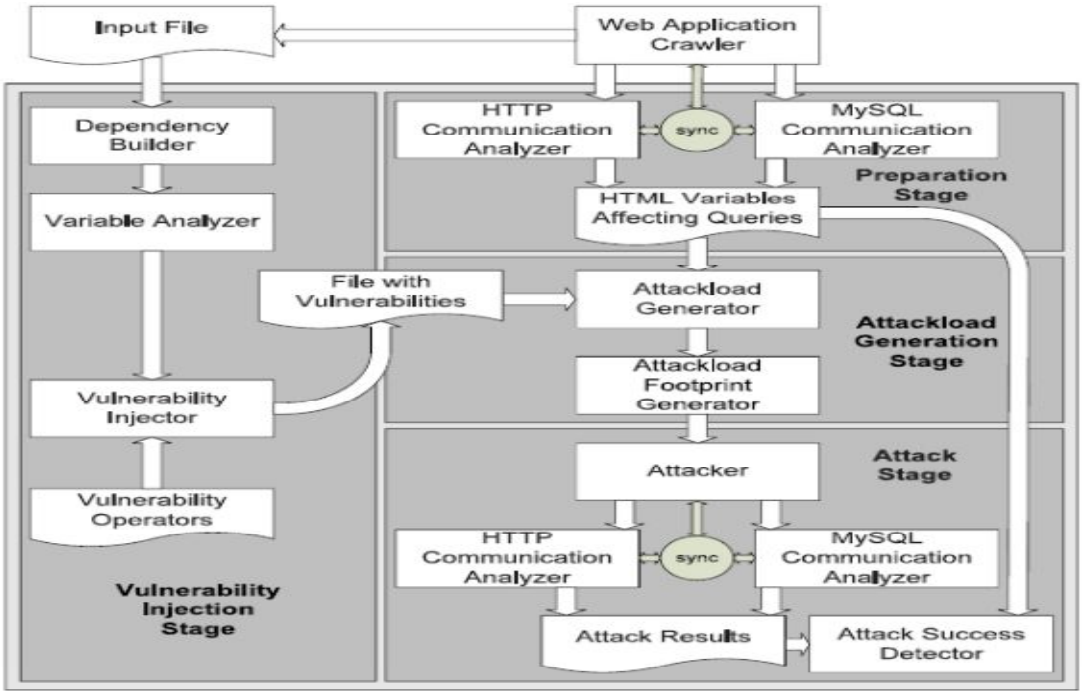

Figure 3: System Architecture of VAIT [3]

There are mainly four stages in Vulnerability and Attack Injector Tool. These stages are Preparation Stage, Vulnerability Injection Stage, AttackLoad Generation Stage and Attack stage

4.0 Analysis and Design Methodology

4.1 Security Mechanisms

4.1.1 Cryptography - Cryptography is used to protect data from interception. It is the study of methods to send data in unrecognizable form so that only the intended user can recognize and read the message. There are two basic cryptographic terms, Plain Text, the text or data which we want to encrypt, and Cipher Text, the encrypted form of plain text.

Cryptography concerns with two things, which are, when Data is coming from the apparent or trusted source and contents of data are not altered. The goals which we want to achieve from cryptography are Confidentiality (to secure the data between authorized users), Data Integrity (the ability to detect manipulation of data by unauthorized users), Authentication (identification of sender and receiver) and Non-repudiation: (when one entity denies previous commitments, there must be a solution, usually a third party to resolve this situation) [26].

We can classify cryptography into these three independent dimensions:

1. Types of operation used to change the plain text into cipher text. Major focus is on “no information loss”. Two general rules used in all types of encryption algorithms;

Substitution, in which all units of plain text are replaced by some other units and Transposition, in which all units are rearranged.

2. Communication depends on the number of keys used. If single key is shared between sender and receiver, this type of encryption is called symmetric encryption or conventional encryption and the shared key is called secret key. If two different keys are used between sender and receiver, this termed as asymmetric encryption or public-key encryption or two-key encryption.

3. The procedure in which the plain text is processed. The way in which input blocks of elements produce an output block against each input block is called block cipher while the way in which input elements process continuously and produce out put of one element at a time is called stream cipher [27].

4.1.2 Conventional or Symmetric Encryption - It was the only encryption scheme available before the public-key encryption. One secret key is shared among the sender and the receiver. The entire procedure of conventional encryption consists of five stages [3]:

1. Plain Text: The original message or data which we want to be encrypted.

2. Encryption Algorithm: Encryption algorithm performs different transformations on the data.

3. Secret Key: Secret key is the input to the encryption algorithm. Different transformations performed by the encryption algorithms depend on the secret key.

4. Cipher Text: This is the out put of scrambled message.

5. Decryption Algorithm: Reverse of the encryption algorithm, it produces the plain text with the help of same secret key and the cipher text.

The encryption process consists of an encryption algorithm and a secret key. The value of key does not depend on the plain text. If we change the value of key the algorithm will produce a different output or cipher text. When cipher text is produced we can fetch the plain text back by using the decryption algorithm with the help of same secret key.

One important thing is that the security of the conventional encryption depends on the secret key not on the algorithms. Even if we know the cipher text and algorithms, it is practically impossible that a message can be decrypted with the help of cipher text and encryption/decryption algorithm. Symmetric and public key symmetric, are the two types of algorithms. In most symmetric algorithms, two communication parties use the same key for encryption and decryption so it is called secret-key, single-key or one-key algorithm. For safe communication key must remain secret. Symmetric algorithms are divided in two categories on the basis of their operations on plain text. Stream Ciphers which operate plain text as single bit or byte, while Block Cipher operates on plain text as a group of bits, these groups of bits are called blocks [3].

There are different symmetric algorithms which are Data Encryption Standard (DES), Triple Data Encryption Algorithm (TDEA) and International Data Encryption Algorithm (IDEA).

DES is the popularly used encryption scheme. Its algorithm referred to as Data Encryption Algorithm (DEA) and is a block cipher. The block of the plain text is 64-bit long. The secret key is of 56-bit long [28].

Another example of symmetric algorithm is TDEA also known as 3DES. This algorithm are more secure uses three executions of DES algorithms encryption-decryption-encryption.

4.1.3 Public-Key or Asymmetric Encryption

Instead of using one key which is used in conventional encryption, asymmetric uses two separate keys. The use of two keys makes the communication more secure and authenticated. Asymmetric scheme has six ingredients [3]:

- Plain Text: The original message or data.
- Encryption Algorithms: Encryption algorithm performs different transformations on the data.
- Public and Private Key. The transformation by the encryption algorithm totally depends on these keys. These keys are selected in such a way that if one is use for encryption, the other is used for decryption.
- Cipher Text: This is the out put scrambled message.
- Decryption Algorithm: Reverse of the encryption algorithm.

The Public and private keys are used in public-key encryption, the public key is used publicly while private key is only used by its owner [3].

The following steps are followed in public-key encryption

- Each and every user in a network generate a pair of keys, one is used for encrypting the message while other is for decrypting the message.
- From those two keys each user places one key in a public register, so that every other user can access that key. In this way each user has a collection of public keys of all the users in network.
- If user A wants to send a message to user B, A encrypts a message with B's public key.
- When user B receives the message he/she decrypts it by using his/her private key. No one else can decrypt this message.

So in this approach private keys are generated locally only for user itself and could not be shared, while every participant has a collection of public keys. For examples, if user A wants to send a message to user B, Instead of data confidentiality user B only want to assure that the data is coming from user A. In this case A uses his own private key to encrypt the data, when B receives the cipher text; he/she can decrypt the data with A's public key which proves that message has been encrypted by A.

Encrypting the message Using recipient's public key provides confidentiality while encrypting the message using sender's private key provides authenticity, the term used for this phenomenon is called Digital Signature. In digital signatures sender signed the message with its private key which can be verified by any user who has the sender's public key.

Asymmetric cryptography depends on the cryptographic algorithms based on two keys. The some conditions which every algorithm accomplish are: it must be easy for any party to generate public and private key. It is easy for sender A to encrypt the message by using public key to produce the cipher text. It is easy for recipient B to decrypt that message with private key to recover the original text. Determining the private key is not possible for any party even if they know the public keys. It should not possible for any opponent to recover the original message by using the public key and cipher text. Any one can use any key for encryption whiles other for decryption [29].

RSA and Diffie-Hellman are the two most widely used algorithms for public-key cryptography. RSA is a block cipher and used for encryption as well as signature. Encryption is similar to signature in RSA except that the private key is used for singing while public key is used for verification. Some other algorithms are Digital Signature Standards (DSS) and Elliptic-Curve cryptography (ECC) [3].

The major weakness in public-key encryption is that public key is public. intruder could pretend to be user A and can send its public key to any other participant or even can broadcast his public key. The solution is to use public-key certificate; issued by a third party which is called Certificate Authority (CA) [3].

4.2 Security Mechanisms Solutions

In this phase we will discuss the different web security mechanisms and applications which are recently used nowadays.

4.2.1 Application Level Solutions

Security solutions at application level further divided for different applications, discussed one by one.

4.2.1.1 Authentication Level

The verification of any identity called authentication which also verify the integrity of data. If an individual request generated for an operation, without knowledge of that individual it is often difficult to decide that either this operation is allowed or not. Traditional authentication methods are not suitable for computer networks having sensitive data. We will discuss little bit about most important authentication specifications which are currently in use.

4.2.1.2 Kerberos

In traditional networks a user types a password to verify its identity during login phase, this process is called authentication. Password based authentication is not a good solution

because passwords sent across the network and any intruder can intercept these password. A strong authentication based cryptography required so that intruder could not gain information that will helpful to impersonate him. The most common example of this type of authentication is Kerberos, which is based on conventional encryption. It is a distributed authentication service in which server verifies a user without sending information on network. Developed in mid 80's, currently having two versions V4 and V5. V4 is still running at many sites but V5 is considered as standard. One drawback of Kerberos is that they are not good against the Trojan horse programs and password guessing attack [30].

4.2.1.3 X.509

It is an authentication protocol based on public-key certificate. The authentication protocols defined in X.509 are commonly used, for example in S/MIME, IP Security and in SET. That an intruder can generate false public keys in public-key infrastructure, to tackle this threat we have to trust on a third party which will generate certificates. The Certificate consists of public key of the user, signed by the private key of that trusted party and that party is called Certificate Authority (CA) [3].

4.2.2 Email Level

The most widely used and growing network application across all platforms is electronic mail. We will look at two schemes that used most for authentication and confidentiality of email [3].

4.2.2.1 Pretty Good Privacy

PGP is the remarkable effort of Philip R. Zimmermann which Provides confidentiality and authentication service for email and file storage applications. PGP combines the best features of both cryptographic schemes. When a user encrypts a message with PGP it first compresses the message then creates a one time secret key for data encryption, this key is called session-key. Firstly the data is encrypted with this one time session key then session key also encrypt by the recipient's public key. This encrypted session key and cipher text then transmit to the recipient. On recipient's side PGP recovers that session key with the help of private key and this recovered session key then use to decrypt the cipher text [3]. The operation of PGP consists of five steps:

1. Authentication: when sender creates a message a 160-bit hash code of the message is generated with the help of Secure Hash Algorithm -1 (SHA-1) which is a cryptographic hash function. By using sender's private key this hash code is encrypted with RSA. The receiver then recovers the hash code by decrypting it with the sender's public key. At the end receiver generates a new hash code for the message to compare it with the recovered hash code if both hash codes are same then the message is said to be authentic message.

2. Confidentiality: PGP provides the confidentiality by encrypting the message. CAST-128, IDEA and 3DES algorithms are used for encryption. Initially sender generates a message with a 128-bit session key; which is randomly generated only for one time. After this the message is encrypted with IDEA, 3DES or CAST-128 algorithms. Session key is encrypted

with RSA using recipient's public key. At the end user recover the session key with its private key and use it to decrypt the message.

3. Compression: PGP by default compresses the message after applying the signature but before encryption. The reason for compress the message before encryption is that it is more difficult to get the information from a compressed message. For compression ZIP algorithms is used.

4. E-mail Compatibility: When PGP used the partial or all resulting block consists of 8-bit octets while many email systems only allow ASCII text. To avoid this PGP uses radix-64 conversion, which expand the message by 33% .

5. Segmentation and Reassembly: Emails with maximum message length are restricted. To avoid this restriction PGP break the message that is too large and at the receiver end reassemble the block again [31].

The reasons of PGP popularity are; availablity of free variety of platforms, based on well known cryptographic algorithms and developed by a single person that's why not governed by any standard organization [3].

4.2.2.2 Secure/Multipurpose Internet Mail Extension (S/MIME)

MIME accommodate the non-ASCII data. MIME is not a mail transfer protocol it is only an extension of SMTP and a supplementary protocol that allows non-ASCII data to be sent through SMTP. Any email message consists of two parts, header and the body. Header has the information that helps in message transmission while body format is normally unstructured. MIME permits emails to attach sound, picture and enhanced text hence MIME defines that how the body part of message can be structured. MIME itself has no security services. S/MIME provides security for MIME data by sign the data and by use of public-key encryption. It provides authentication of data by using digital signature and integrity of data by encryption. Both PGP and S/MIME are on IETF standard but S/MIME emerges as an industrial standard [3].

4.2.3 IP Level

Applying security on IP level can ensure the secure communication for the applications that has security mechanism [3].

4.2.3.1 Internet Protocol Security (IPSec)

IPSec is not a single protocol. It is a general framework by using a set of algorithms it allows different entities to communicate securely with each other. It provides encryption and authentication to all traffic at IP level with the help of strong cryptography. Authentication and encapsulation are two basics of IPSec. Two protocols that provide authentication and encapsulation are Authentication Header (AH) and Encapsulation Security Payload (ESP). These two protocols used in combination or alone to provide a desired set of security services for the IP layer.

- ESP: It covers the packet format and issues related with the use of ESP for packet encryption and optionally authentication.
- AH: It covers the packet format and issues that how the AH use for packet authentication.
- Encryption Algorithm: It covers that how the set of encryption algorithms used for ESP.
- Authentication Algorithm: It covers that how the set of authentication algorithms used for AH and optionally for ESP authentication.
- Domain of Interpretation (DOI): The values which are required for the other documents to relate with each other are covered by DOI.
- Key Management: It describes the key management schemes. Oaklay and ISAKMP is an example of two schemes.

Another fundamental part of IPSec is Security Association (SA). It is a one way relationship between sender and receiver that is responsible for security services and to the data carried on it. It make by the use of either ESP or AH. If we want to apply both AH and ESP protection on a traffic stream then we need two SAs. Transport mode and Tunnel mode are two types of SAs which provides different types of protection to data. In transport mode protection provides to only upper-level protocols like TCP, UDP or ICMP while entire IP packet is protected in tunnel mode. IPSec is to provide security of all distributed applications like data transfer, remote login, web access and email [3].

4.2.4 Web Level

Web is acessible to all, most of the users are not aware of the risks. Browser side risks, wrong configuration in web servers are some types of risk that helps intruders to unauthorized remote access and interception of data which sent form client/server to browser and browser to client/server [3].

Transport Mode SA Tunnel Mode SA AH Authentication provide to IP Payload and selected portion of IP header and IPv6 Extension header Authenticate the entire inner IP Packet plus selected portion of outer IP header ESP Encrypt IP Payload and any IPv6 extension header Encrypt inner IP packet. ESP with authentication Encrypt IP Payload and any IPv6 extension header. Authenticate IP payload but no IP header. Encrypt and authenticate inner IP packet client/server. We will discuss two standardized schemes Secure Socket Layer (SSL)/Transport Layer Security (TLS) and Secure Electronic Transaction (SET) that are used for web security [3].

4.2.4.1 SSL/TLS

Various approaches are used for web security and they have different scope of applicability with corresponding location in TCP/IP protocol suite. One way is to provide web security at IP layer level which we already discussed earlier. One advantage of using IPSec is that it is transparent to end users and we can filter the traffic. Another solution is that to provide security just above TCP. SSL is one of the most commonly used security mechanism available on Internet. Like other security protocols SSL is also based on cryptography. After SSLv3, Internet Engineering Task Force (IETF) renamed it as TLS which now considered as

standard. TLS is almost same like SSLv3. SSL/TLS encrypt the data at transport layer. Instead of HTTP normal port 80, SSL comes up with a special URL identity "HTTPS" which uses port 443 to establish a secure SSL session. SSL supported browsers are used mostly for sensitive data like credit card information. TLS provides end to end authentication and then secure communication using cryptography. SSL protocol runs above TCP/IP and follow these steps [3]:

- With the help of public-key cryptography, clients check the server certificate that it is issued by a trusted Certificate Authority (CA).
- Same technique repeated for server it check the client's certificate and public ID that it is issued by a trusted Certificate Authority.
- Using public-key cryptographic technique an SSL encrypted connection established between server and client.

SSL protocol further consists of two sub protocols. SSL Record Protocol and SSL Handshake Protocol. SSL record protocol describes the format used to transmit data. The most complex part of SSL is handshake protocol that allows server and client to authenticate each other and by using SSL record protocol transfer the data between SSL enabled server and client. TLS/SSL authenticates to both communication parties (servers and clients) and provide data integrity, that's why can helpful against replay attack, man-in-the middle attack and masquerade attacks [3].

4.2.4.2 Secure Electronic Transaction

Secure Electronic Transaction (SET) is a security protocol designed for protecting credit cards transactions over internet. Developed by VISA and MasterCard and some other big companies involve are IBM, Microsoft etc. The goal of SET is to authenticate buyer and merchant identity and then confidential transaction [3].

SET uses different technologies for authentication and encryption. For confidentiality of information and integrity of data DES and RSA used with SHA-1 hash codes, X.509v3 certificate used for authentication of card holder account and merchant account. Privacy achieve through dual signatures. The reason of using dual signature is that in SET transaction there are two recipients involve one is merchant and other is bank. Customer sends order information to merchant and payment information to the bank for these two signatures are used, one signature is for merchant and one is for bank. The key features of SET are [3]:

- Using DES algorithm it provides confidentiality of data even prevent merchant to learn the cardholder's detail.
- RSA digital signatures with the use of SHA-1 hash codes provides integrity of data which secure the payment information, personal data and order information that send from cardholder to merchant.
- Using X.509 certificates it authenticates cardholder account and merchant account.

4.4 System Level Solutions

On the basis of the web security mechanisms, different security solutions were. These security solutions are further dived into two main categories, application level security solutions and system level security solutions. Due to differentiation of user base and software base trespasses, system level security solutions are further divided into IDS, IPS, antivirus applications and firewalls [3].

4.4.1 Intrusion Detection System (IDS)

The IDS is the system which detects any unauthorized access or intrusion in a system or network. It is a security solution which has a passive position in a system or network against these intrusions. In a network deployment the function of the IDS is to monitor the traffic or network activity without impacting the traffic [32]. IDS in a network only detects or identifies any changes in network but does not perform a resistive action against such changes.

The IDS system uses two approaches for notification of intrusion in a network [33].

4.4.1.1 Statistical detection

It depends on the statistical behavior of the network; the statistical detection approach has further division into two sub categories.

- Threshold detection - In threshold detection, the IDS can monitor the number of established connections in a specific time or the number of new user requests for a specific application that runs on a network.
- Profile based detection - In profile based detection, the IDS system monitors the behavior of a user at different time slots. It monitors the user login/logoff session times on the network also counts the number of password failure attempts by user in short time intervals.

4.4.1.2 Rule based detection

Rule based intrusion detection system performs the activity, if any change is found in the rules of proper network flow. It is also important because it works on customized settings of the network assigned by the network/system administrators [3].

The IDS security solutions are further classified into three main categories which are Network based intrusion detection system (NIDS), Host based intrusion detection system (HIDS) and Distributed intrusion detection system (DIDS) [34].

- Network based intrusion detection system (NIDS) - Network based intrusion detection system works in a network. It monitors all the network traffic especially at hardware layer based traffic. The NIC is that first it generates an ICMP request for acquiring a physical address (IP address). This request is broadcast on network. Some time NIC gets bulk of ICMP requests which can create a chance of network congestion situation. NIDS monitors all the same types of intrusions with appropriate NICs and creates a log file. Similarly NIDS has a feature to monitor all

the network switches communication, if it observes any network intrusion through these switches then it makes a report [34].

- Host Based Intrusion detection system (HIDS) - Host-based intrusion detection system is deployed only on a local machine or system. It is responsible to monitor local system based activities or intrusions i.e. CPU performance, file sharing resources and functionality of system applications like web-server application and mail-service [3].
- Distributed intrusion detection system (DIDS) - In DIDS there is one central control machine that performs a role of administrator or manager and all remaining IDS systems behave like clients. These IDS client machines normally called IDS-sensors. All these IDS sensors can detect the intrusions in the network or system and send a report to the main IDS manager. These IDS-sensors are in the form of NIDS, HIDS or both. So we can say that the DIDS is a combination of both NIDS and HIDS systems. The one main feature of DIDS system is that all IDS sensors send their reports of network and local system based intrusions to the IDS manager and an IDS manager is responsible to update its IDS sensor patches or signature database against new bugs and intrusions that occurs in the network [34].

4.4.2 Intrusion Prevention System (IPS)

The intrusion Prevention System performs a role of protection against intrusions that occurs in a network or local system. It works on the basis of output of IDS system log files. So IPS system is an extension of the IDS system. But there are some differences between IDS and IPS. IDS system works in a passive mode, i.e. it only has the ability to detect any intrusion in the network, whereas an IPS works in an active mode. An IPS performs action when it founds any packet dropping or unauthorized connection. [35][36]

Functions of an IPS system are same as of an IDS system. It may work as a standalone machine or system known as Network Based Intrusion Protection System (NIPS) that have the ability to block or deny any unauthorized interruption that occurs in the network. Or it may perform a role with an existing system or operating system known as Host Based Intrusion Protection System (HIPS). HIPS protect and deny local unauthorized activities, like high utilization of CPU from any type of service and movement of local system files within the system or to another system. As per functionality of an IPS system, we can say that a router access control list or firewall rules might be consider a basic IPS system [46] and similarly the combination of blocking capability of a firewall and deep packet inspection through an IDS system is known as an intrusion prevention system. [37].

4.4.4 Antivirus Techniques

Antivirus techniques are already explained in chapter 5, there are number of malicious applications/softwares which perform harmful activities within a local system or on network. These applications can be in the form of different “viruses” which may infect or modify the system files or applications, or can be in the form of “worms” that may create their own replicas in a system and utilize the vacant space in system. Some of these applications perform their role only on local system or some of them travel from one machine to other machine through network resources or other medium like USB or

wireless transfer among machines. For protection from these types of malicious applications we use antivirus techniques on our network or system known as antivirus applications. An antivirus technique follows these sequence of operations stated below[33].

- Detection - The first step of an antivirus application is that it has the ability to detect the occurrence of a virus or other malicious program in system application or in data file.
- Identification - After detection function the second step of an antivirus is that it has the ability to identify the type of virus with its malicious aims.
- Removal - The virus removal is the last step of an antivirus application.

There are many functional techniques used by antivirus applications for detection, identification and the removal of viruses from a system or a network. Some of these techniques are: [33] [37].

4.4.4.1 Generic Decryption (GD)

The generic decryption is an antivirus technique designed for the polymorphic type of viruses. Polymorphic virus contains total encryption architecture. It contains an encrypted virus signature as well as an encrypted key in its internal body; whereas it has an outer body cover which is also encrypted. The outer cover decrypt by its internal key. So it is very complicated to detect the virus signature through a simple antivirus. The generic decryption antivirus technique has the ability to detect and clean the type of viruses which have polymorphic architecture. It followed some steps described below [33]

- Generic decryption technique first generates a virtual machine into a real machine. This virtual machine has complete hardware and applications same like in actual machine.
- In the process of scanning or diagnosing, system and data files are placed in virtual machine one by one.
- If the polymorphic virus exists in any placed file, then polymorphic virus performs act to this file first it decrypt is outer cover body by its own internal key.
- As it decrypt its own outer body. It has opened its internal structure, specially its virus signature, in front of any generic decryption antivirus, And then generic decryption antivirus can easily removed this virus from this file. This process occurs only in virtual machine that is created by generic decryption antivirus; this virtual machine is also totally isolated to actual machine and its applications. In this way polymorphic virus does not have an effect on the actual machine at the time of its operation.

4.4.4.2 Digital Immune System

A digital immune system or digital immune antivirus is a technique that provides a protection against those types of viruses which have the characteristics to spreading from one computer to other computer through a network. Normally “worm” is considered such type of virus. Digital immune system has its own scanner elements on every client machine in a network; these scanner elements first detect such type of viruses on local client machine, then the scanner client machine sends this information to the main administrator

machine, which is also a part of the same network. Administrator machine collect the information and send it to virus analysis machine. The virus analysis machine may exist on same network or may be on wide area network. The virus analysis machine has some working blocks in its architecture [3].

- 1st block; this block is isolated with other blocks. It is used to detect the virus and read out its structure, i.e. virus type.
- 2nd block; it detects virus signature.
- 3rd block; this is the last block of virus analysis machine, it removes the viruses form the infected files.

After removing viruses from that file, virus analysis machine sends this information to the whole network clients. All network clients update this virus signature information in their databases. A digital immune system is very efficient to detect and remove such type of viruses which spread over the network [33].

4.4.4.3 Behavior Blocking Software

The behavior blocking antivirus software integrates with the operating system of a host computer and monitors program's behavior in real time [38]. This application runs on both, server and clients but the main protection is done by the server side. The behavior blocking system can monitor the system files with operating system's behavior. So if any changes occur in system files it detects and send a report to the administrator and wait for an action from the administrator. Updating the main server is the responsibility of administrator [33].

4.2.4 Firewalls

A firewall is a barrier which performs isolation between two different networks or systems. It decides that which kind of traffic can pass through a network and in which direction. Firewalls functionalities are as follows:

- Administrator sets acceptable software behavior policies and uploads them to a server
- Malicious software manage to make it through the firewall Sandbox
- Behavior blocking software at server flags suspicious code, sandbox software prevent it from proceeding
- Server alerts administrator that suspicious code has been identified and sandbox, awaiting administrator's decision on whether the code should be removed or allowed to run Server running behavior blocking software Administrator provides an additional level of defense system providing the capabilities to add much tighter and more complex rules of communication between different network segments or zones [32].

A firewall may contain only one system or it may consist of more than one system. The role of firewall is to provide protection of one network from other network. The connection architecture of a firewall in a network is that it creates a barrier between two networks. For this it must have at least two network interfaces one for the network which is intended

to protect and other for the network that is exposed to [39]. Simply a firewall protects the internal network from external network.

Considering the connection architecture of a firewall there are some important points to understand.

- Physically firewall is connected with two or more than two networks through its interfaces, so that all incoming and outgoing traffic has a single point for communication. Therefore all traffic must pass through firewall for communication purpose from one direction to another direction.
- The second point is that only authorized traffic is passed through firewall, either traffic is coming in to the network or going out from the network. All incoming or outgoing traffic must fulfill the security measures that define in a firewall as rules.

A firewall follows below parameters [33].

- Service control - A firewall controls those services that want to pass through the firewall. It also controls the communication services which have some additional functional parameters, like source/destination IP addresses with their specific ports and type of protocols.
- Direction control - A firewall controls those services, which has rights of communication. Means firewall can restrict incoming traffic to come inside the network and can restrict the outgoing traffic to go outside the network or may be allowed to both type of traffic.
- User control - It can assign that which user can access to which services. These users can be either from the local network or from the outer world.
- Behavior control - With the help of a firewall administrators can control the working behavior of a service and a user. They can assign that a user either have full access rights on a service or on a system, or partial access rights to that particular service or system. At the same time firewall can decide that the same user is not allowed to access other parts of that particular service or system.

The type of firewall is right for a given control architecture [33]. Firewalls can be divided into four categories: Packet filter firewall, Application gateway, Circuit level gateway and Stateful filter firewall [33][40].

Packet Filter Firewall - A packet filter firewall monitors all incoming and outgoing network based packets. It allows or denies packet to pass through one network to another network. It checks the packet parameters and compares them with its own tables that contains packet parameters after that a packet filter firewall decides to allow or deny the packet. The packet parameter field normally contains, source/destination IP address, source/destination services ports, types of packets (either TCP or UDP) and information flags that notify the purpose of packet. Due to its packet filtering functionality, it may allow specific packets form specific interfaces for communication. This rule can be implemented for both inside and outside traffic. Packet filter firewall is easy to implement and does not require a high level of configuration in a standard network. It is also known as first generation level firewall [40].

A packet filter can remove the bug which exists in TCP (three way handshake) communication, which a hacker can as a SNY flood attack. For detection and protection against a SYN flood attack we can use a packet filter firewall in a TCP interception mode [41]. In TCP interception mode a packet filter firewall catches the TCP request "SYN" flag packet from outside the network, which is coming toward a targeted server for establishing a TCP (three way handshakes) connection from an unidentified user. Firewalls do not allow this packet before identification of user. So firewall sends a "SYN-ACK" flag packet to the user. If there is a valid user then it sends an "ACK" flag packet to the firewall. This confirms the validity of user so now packet filter firewall sends request to server to establish a TCP connection otherwise discards the first "SYN" flag packet request [3].

Application Level Gateway - An application level firewall provides more shelter and reliability than a typical packet filter firewall. Application level firewall works on application level and they can better analyze the traffic at application layer. It provides a client-server network environment. All hosts that want to communicate with outside the world use the firewall as a gateway, hosts are considered as client while the application level firewall performs as a server. So we can say that an application level firewall is also an application level gateway. Since all traffic must pass through the firewall so it has full command on authentication and authorization of data traffic. It filters the traffic at very high level that's why it provides a high level of security [3].

Stateful Inspection Firewall - A stateful inspection firewall is a combination of multiple firewalls, especially with packet filter firewall and application level gateway. It scans the packets at network level and read packet content at application level. It provides more security and is called 3rd generation level firewall [40].

4.4.4 Virtual Private Network

VPN as a private network across a public network such as a internet . A VPN is created by establishing a virtual point-to-point connection by virtual tunnelling protocol. Virtual private network done by secure way during the connection it provide a secure path and information exchange through these path and it can't be easily hack because tunnelling is so secure that the own network can't track the IP address [25].

4.5 RSA Key Generation Algorithm [42]

- Two large prime numbers are considered. Let them be p,q.
- Calculate n = pq and (Ø) phi = (p-1)(q-1).
- Select e, such that 1 < e < phi and gcd(e, phi) = 1.
- Calculate d, the private key, such that de =1 mod phi.
- One key is (n, e) and the other key is (n, d). The values of p, q, and phi should also be kept secret.
- N is known as the modulus.
- E is known as the public key.
- D is known as the secret key.

Encryption

Sender A does the following:

- Get the recipient B's public key (n, e).
- Identify the plaintext message as a positive integer m.
- Calculate the ciphertext c = m^e mod n.
- Transmits the ciphertext c to receiver B.

Decryption

Recipient B does the following:

- Consider his own private key (n, d) to compute the plain text m = c^d mod n.
- Convert the integer to plain text form.

5.0 Observation/Findings

In respect to this study it was observed that:

1. Many security mechanisms evaluation methods suffer from false positive and false negative detection systems. So evaluation methods should core consist of multisource fusion decision, threat spread analysis and attack intention guess algorithm [43].
2. The usage of multi-biometrics is advantageous over uni-biometrics as it is resilience to spoofing and has low False Acceptance Rate (FAR) [44].
3. Using Captcha and Graphical (CaRP) password system to handle security problem like guessing attack, relay attack and shoulder surfing attack [45].
4. Applying Liquid State Machine (LSM) to enhance the overall performance of network. Then it will remove drawback of SVM (Support Vector Machine) and ESN (Echo State Network) [46].
5. Using Genetic Algorithm (GA) to make the total cryptography process much faster, robust and highly secure network [47].

6.0 Conclusion

The web platform is built as genuine infrastructure without more initial awareness that security challenges will emanate to be a tough problem or such a beautiful platform. The malicious users inventing series of means to obstruct the transmission process on the web. Then, software security developers have to provide patches to existing web security mechanisms to curb several kinds of vulnerabilities attacker from malicious users. Despite the good number of security mechanisms developed, the vulnerable attackers still produce new attacking strategies and launch to the web to destroy it intended operations or slow down its performance. The task of providing more dynamic and robust security measure is a great task and challenge to software developers and other people of liked interest.

References

[1] Fonseca J, Seixas N., Viera M., Madeira, H. "Analysis of Field Data on Web Security vulnerabilities'' IEEE transaction on Dependable and secure Computing 2014.

[2] M.S. Patole1, Sagar D. Kothimbire "A Review on Web Security Mechanism Performance Evaluation Using Vulnerability and Attack Injection" International Journal of Science and Research (IJSR) 2014.

[3] Nadeem Ahmad, M. Kashif Habib, "Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution", Master Thesis, Electrical Engineering, School of Engineering Blekinge Institute of Technology (BTH), SE - 371 79 Karlskrona, Sweden Thesis No: MEE10:76 Sept. 2010.

[4] Kirti Randhe, "Security Engine for prevention of SQL Injection and CSS Attacks using Data Sanitization Technique", IJIRCCE, 2015.

[5] Zoron Djuric, "Black Box Testing Tool for Detecting SQL Injection Vulnerabilities", IEEE, 2013.

[6] Rani V. Bhor, Harmeet K. Khanuja, "A Survey on Vulnerability and Attack Injection for Evaluation of Web Security Mechanism", International Journal of Science and Research (IJSR), Volume 3 Issue 12, December 2015.

[7] R. Divya Paramesvaran, Dr. D. Maheswari, "Study of Various Security Attacks in Network Layer and the Mitigation Techniques for MANET", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 2, February 2016.

[8] Kamini Nalavade, Dr. B. B. Meshram, "Layered Approach for Preprocessing of Data in Intrusion Prevention Systems", International Journal of Computer Applications Technology and Research (IJCATR) Volume 3 Issue 6 June 2014.

[9] S. Saravanakumar, Umamaheshwari, D. Jayalakshmi, R. Sugumar, "Development and implementation of artificial neural networks for intrusion detection in computer network", International Journal of Computer Science and Network Security2010. Vol. 10, No. 7, pp. 271-275.

[10] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU, "An Adaptive Approach to Detecting Black and GrayHole Attacks in Ad Hoc Network", 2010 24th IEEE International Conference on Advanced Information Networking and Applications (AINA),Perth, Australia, April 20-23, 2010, pp.775-780.

[11] Jose Fonseca, Marco Vieira, and Henrique Madeira, "Evaluation of Web Security Mechanisms Using Vulnerability & Attack Injection", IEEE Transactions on Dependable and Secure Computing, Vol. 11, No. 5, September/October, 2014.

[12] D. Avresky, J. Arlat, J.C. Laprie, and Y. Crouzet, "Fault Injection for Formal Testing of Fault Tolerance," IEEE Trans. Reliability, Vol. 45, Vo. 3, pp. 443-455, Sept. 2011.

[13] J. Arlat, A. Costes, Y. Crouzet, J.C. Laprie, and D. Powell, "Fault Injection and Dependability Evaluation of Fault-Tolerant Systems," IEEE Trans. Computers, Vol. 42, No. 8, pp. 913-923, Aug. 2011.

[14] Gurmukh Singh, "Security Attacks and Defense Mechanisms in Wireless Sensor Network: A Survey", International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 4, April 2016.

[15] William Stallings, Network Security Essentials Applications and Standards, 2nd ed., New Jersey: Pearson Education, 2003, pp. 6.

[16]http://www.queencitynews.com/modules.php?op=modload&name=News&file=article&sid=1666

[17] Network Model, http://www.tcpipguide.com/free/t_TheBenefitsofNetworkingModels.htm

[18] The TCP/IP Protocol Suite, http://www.fujitsu.com/downloads/TEL/fnc/pdfservices/TCPIPTutorial.pdf

[19] TCP dump, http://www.usenix.org/publications/login/1998-8/tcpdump.html

[20] The Java Tutorial, http://java.sun.com/docs/books/tutorial/networking/sockets/definition.html

[21] Application Layer in TCP/IP suite, http://en.wikipedia.org/wiki/Application_Layer

[22] "Glossary of Internet Security Terms", http://www.auditmypc.com/glossary-of-internet-security-terms.asp

[23] "Introduction to Computers/System Software-Wikiversity" http://en.wikiversity.org/wiki/Introduction_to_Computers/System_software

[24] Yeu-Pong Lai and Po-Lun Hsia, "Using the vulnerability information of computer systems to improve the network security", Journal of Computer Communications, vol. 30, Issue. 9, pp. 2032-2047, 30 June 2007.

[25] Babul K. Ladhe, Akshay R. Jaisingpure, Pratik S. Godbole, Dipti S. KhodeInternational, "Review on Rising Risks and Threats in Network Security", Journal of Research In Science & Engineering, Volume: 1 Special Issue: 1 www.ijrise.org|editor@ijrise.org [135-139].

[26] E-Thesis http://ethesis.nitrkl.ac.in/77/1/Yellapu.pdf

[27] Dr. K.Duraiswamy and Mrs. R.Uma Rani "Security Through Obscurity", http://www.rootsecure.net/content/downloads/pdf/security_through_obscurity.pdf

[28] William Stallings, Network Security Essentials Applications and Standards, 2nd ed., New Jersey: Pearson Education, 2003, pp. 34-42

[29] William Stallings, Network Security Essentials Applications and Standards, 2nd ed., New Jersey: Pearson Education, 2003, pp. 68-72

[30] B Clifford Neuman and Theodore Ts'o " Kerberos: An Authentication Service for Computer
Networks", Journal of IEEE Communications Magazine, vol. 32, Issue. 9, pp. 33-38, Sep 1994.

[31] William Stallings, Network Security Essentials Applications and Standards, 2nd ed., New Jersey: Pearson Education, 2003, pp. 123-128

[32] Idaho National Laboratory; "Control System Cyber Security; Defence in Depeth Strategies", external report # INL/EXT-06-11478, May 2006

[33] William Stallings, "Network Security Essential; Applications and Standards", ISBN-13: 978-0-13-706792-3

[34] Jay Beale, Andrew R. Baker, Joel Esler, Toby Kohlenberg & Stephen Northcutt, "Snort: IDS and IPS toolkit" ISBN-13: 978-1-59749-009-3

[35] Ted Holland, "Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth", GSEC Practical v1.4b, Option 1, February 23, 2004

[36] Intrusion Protection System; URL:http://en.wikipedia.org/wiki/Intrusion_prevention_system

[37] Desai, Neil. "Intrusion Prevention Systems: the Next Step in the evolution of IDS." Security
Focus. 27 February 2003. URL: http://www.securityfocus.com/infocus/1670 visions and perspectives"

[38] Behavior Blocking Antivirus Protection; http://www.symantec.com/connect/articles/behavior-blocking-next-step-anti-virus protection

[39] Firewall; http://www.vicomsoft.com/knowledge/reference/firewalls1.html

[40] Type of Firewalls; shttp://en.wikipedia.org/wiki/Firewall_%28computing%29

[41] Chris Bryant, CCIE #12933, "CCNA Security and CCNP ISCW Tutorial: "SYN Flooding Attacks" and TCP Intercept" URL: http://www.thebryantadvantage.com/CCNASecurityCCNPISCWTCPIntercept.htm

[42] Pinki Singh & Ruchir Bhatnagar, "Encryption Algorithms with Emphasis on Probabilistic
Encryption & Time Stamp in Network Security", International Journal of Research in Engineering & Technology (IJRET), Vol. 3, Issue 5, May 2015, pp. 39-46.

[43] Xiangdong Cai, "Network Security Threat Situation Evaluation Based on Fusion Decision and Spread Analysis", International Journal of Security and Its Applications, Vol. 9, No. 3 (2015), pp. 383-388, http://dx.doi.org/10.14257/ijsia.2015.9.3.30

[44] R.Divya, V.Vijayalakshmi, "Analysis of Multimodal Biometric Fusion Based Authentication Techniques for Network Security", International Journal of Security and Its Applications, Vol. 9, No. 4 (2015), pp. 239-246, http://dx.doi.org/10.14257/ijsia.2015.9.4.22

[45] Priyanka Y. Patil, Manju R. Patil, Nilima R. Barhate, Prashant C. Harne, Ashvini P. Patil, "Solving Hard AI Problem using CaRP as Online Network Security", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue: 3, pp. 1042 – 1044, March 2015.

[46] Ms. Rucha P. Joshi, Mrs. Shanthi K. Guru, "Enhancing the Security of a Network System using Liquid State Machine- A Novel Approach", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue: 5, pp. 2622 – 2625, May 2015.

[47] SomalinaChowdhury, Sisir Kumar Das, Annapurna Das, "Application of Genetic Algorithm in Communication Network Security", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 1, January 2015.