**Integrated Next Generation Network Security**

**Model**

Harnidh Kaur1, Kirti Sharma2, Simran Kaur3, Smriti Sharma4

Student, Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India1,2,3,4

**ABSTRACT**

**In today’s scenario, cyber threats are becoming labyrinth and difficult to manage. The traditional security management systems are not capable to handle upcoming novel threats resulting in performance deterioration. In this paper various next generation technologies have been integrated together that provide an efficient, manageable, robust and flexible system that not only effectively tackles all the existing attacks but can mutate itself to fight against zero-day attacks. The proposed system includes intelligent techniques that are required for the future cyber world like Next Generation Intrusion Prevention System(NGIPS), Network Breach Exposure System(NBES), Cloud based Antivirus, Anti-spam, Personalized censor-ware, Sparta(access control service), Monican(control and management technique). It will result in a reliable, efficient and quick responsive system to obtain remarkable results in the network security.**

***Keywords- Cavernous Packet Examination∙ NBES∙ APG∙ PHGE∙ Bayesian Filter ∙General Management***

**INTRODUCTION**

Network security as a specialized field in computer networking that involves securing a computer network infrastructure. With the increase in dependence on the computer systems, network security is one of the major concerns. Losses of private information, access by unwarranted sources are problems that scrape the surface only. Despite of the existing technologies, there is no panacea to the network security problem as it is fast transmuting into rampant hazard. Presented integrated security system, is another effort to deal with this peril situation.

This system is an amalgamation of mechanisms that are not only flexible and robust but also adept enough to tackle any next generation upcoming threats. This system is highly optimum and is determined to provide best services in securing the network. Its major components are Next Generation Intrusion Prevention System(NGIPS), Network Breach Exposure System(NBES), Cloud based Antivirus, Anti-spam, Personalized censor-ware, Sparta(access control service), Monican(control and management technique).

The continuously evolving and increasing intrusion by worms or viruses is leading to a major loss of data. In the present scenario, where major emphasis is being laid on data warehousing and Big Data even a slight discrepancy or loss of data can lead to inefficient working. The proposed system is not just a conventional UTM (unified threat management) that simply combines the security system but is responsible for thwarting any attacks by sensing the network itself.

The network CPE based integrated security system which can effectively cope with the various security threats by indentifying and authenticating seven layers of internet traffic can be applied without overloading the network traffic. It can also be regarded as the optimum solution to cope with unknown network based threats in the future.

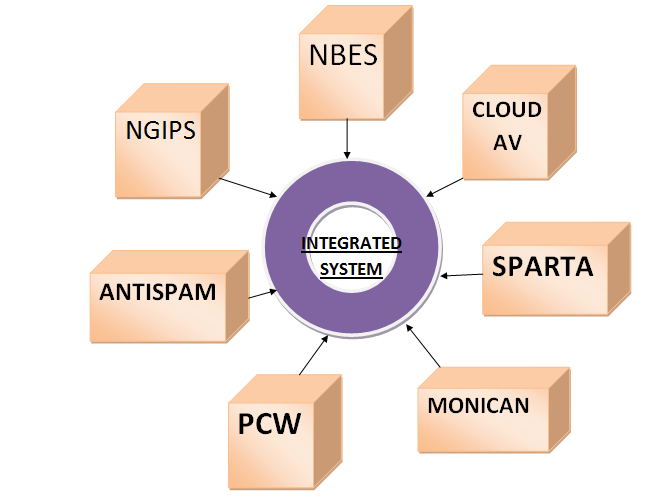


Fig. A.Components of integrated security system

1. **NEXT GENERATION INTRUSION PREVENTION SYSTEM**

Intrusion prevention system is a network security technology that inspects the stream of traffic to detect and prevent any malicious activity. It maintains a log about all such activities and attempts to block/prevent it. IPS can take such measures as sending an alarm, dropping the malicious packets and it can even block the offending IP addresses.

Next-Generation Intrusion Prevention System is an unconventional and innovative system that secures the network from emerging threats and risks. NGIPS is built on top of traditional IPS and has additional capabilities like user awareness and application awareness. These features assist NGIPS to provide fast, reliable and accurate solutions in an economical manner.

* 1. **NEED FOR NGIPS**

IPS deals with traditional threats. As new attacks are developed for breaching the safety of the network, it becomes necessary to evolve our security systems in order to cope with and survive such attacks. To enhance the accuracy of responses, we need additional knowledge like network behavior, user identity, and the devices connected on the network. This data is easily made available through this improved system.

Another reason for employing NGIPS is that the core idea of conventional IPS system was to safeguard the server and server based applications. But new threats are targeting the client side via applications. So modifications need to be done to secure both client and server side applications.

* 1. **CHARACTERISTICS OF NGIPS**

Inspection of encrypted traffic:-In industries where security and integrity are crucial, such as finance, it’s been observed that as much as 70% of all network traffic is encrypted .In order to save both time and resources most of the intrusion prevention systems pass these encrypted packets considering them to be risk free. As a result, now encryption is used as a means of bypassing the security controls. For example-certain file sharing and social messaging applications frequently exploit encryption to hide, leading to liability and compliance issues. The typical IPS fails to provide a solution to these security challenges. This system solves these problems by employing a dedicated appliance for decryption (and re-encryption) of network traffic.

Application Knowledge and full stack reflectivity:-The NGIPS should have knowledge of all the applications running on the network. It should have full stack visibility which includes not only applications, but also operating systems, versions, devices, networks and even files. In addition to enforcing acceptable use policies and preserving bandwidth, application control actually reduces the attack surface by blocking unknown or forbidden applications and nullifies application trickery such as port hopping and traffic tunneling. Moreover by restraining certain features of operating system, it can improve the productivity thereby decreasing the extent of network area exposed to risk.

Content Awareness:-The main objective of any IPS system is the ability to identify and counteract various threats. The threats cannot be only of conventional type but ,with emerging technologies, can also be embedded in content such as Adobe PDFs and Microsoft Office files. The NGIPS system is capable of carving files for analysis out of many protocols, encodings and several compression methods. With the file carved, the system produces unique indicators for each file type to make a determination of ‘disposition’ of that file. If the disposition is determined to be less than good then the transfer of that file is blocked.

Contextual understanding:-Context refers to the group of conditions that exist where and when an attack takes place. This context is a significant measure to determine the priority of response. The NGIPS system is capable of integrating information from sources outside the system in order to take effective decisions. This information can be based upon several factors like

1. **Network awareness** – The NGIPS system should be fully aware of network including various hosts connected to the network, network and host configuration changes, and compliance with IT policies. If certain devices or applications are currently disconnected on a particular network then security for such devices can be turned off so as to increase productivity, decrease load and to avoid unneeded checks. When a new machine emerges on the network, its protections are automatically turned on. Similarly certain attacks can be marked as of ‘low priority’ based on their context.
2. **Behavior awareness** – This type of awareness includes understanding of what type and amount of network traffic should be considered ‘normal’. Thereafter it is the job of NGIPS to monitor and report any abnormal or unfamiliar traffic. Anomalous network traffic may indicate a threat trying to attack the server so identifying it prevents system breaches and data loss. In addition to this behavior awareness also monitors bandwidth consumption to help diagnose performance degradation.
3. **Identity awareness** – The NGIPS system must be aware of the identity of various users connected on the network either individually or as members of groups. This data is available from both Microsoft Active Directory systems and a variety of open standards-based LDAP directory servers. This can be used to identify the victims as well as the attacker thereby speeding the response.

Inline, Bump-in-the-Wire Configuration:-If the NGIPS device, configured for inline operation fails or crashes (perhaps because of hardware failure, software malfunction, or power loss) then it is configured to “fail open” as not to cause disruption in network connectivity. In this case, ingress and egress interfaces of an interface set are mechanically bridged, thus continuing to pass traffic (without further inspection). Thus network operation is unaffected by the failure.

Agile engine:-Agility is defined as ability to adapt to the changing needs in order to maintain significance against varying security demands. A key component to make NGIPS system agile is Snort. The NGIPS is ‘agile’ in the following ways:

1. **Default Detection**- In order to save time and effort required to configure the system, following three options are provided:
2. *Protection over connectivity*- it is the highest level of security with maximum number of checks enabled. It is used when network security is preferable relative to user’s convenience.
3. *Connectivity over protection*- it is the least restrictive security level and is used when access to network resources is at highest priority.
4. *Balanced protection and security*- it provides optimal solution to organizations with typical security needs.
5. **Custom Configurations**- In addition to the above mentioned basic policies, NGIPS provides users with the option to customize the detection rules and set various other policies to accommodate their requirements.
6. **NETWORK BREACH EXPOSURE SYSTEM**

Network breachexposure system (NBES) monitors the traffic crossing the network and detect the intrusion which after being compared with the previously known set of malicious activities. Network security aims to protect the machine from unauthorized and potentially unsafe activities. Intrusion detection senses the unusual activity and alerts the administrator. It is very clear that firewalls are not enough to secure a network completely because the attacks committed from outsideof the network are stopped whereas inside attacks are not. This is the situation where breach detection systems are in charge. BES is used in order to stop attacks, recover from them with the minimum loss or analyze the security problemsso that they are not repeated. Cavernous packet examination (CPE) is a very common method of network breach exposure.Implementation of Signature based Network breach exposure system (NBES) requires to match a predefined string or predefined pattern that is already identified as harmful to the network. The system used to implement NBES should have the feature of dynamic reprogramming, fault tolerant, susceptible to attacks, easy to install and should be general to detect different types of attacks.There are two types of intrusion detection system:-

1. **Exploitation Detection** - Exploitation basedBreach exposure system (BES)aims to distinguish events that violate system policy. It can only detect known attacks.
2. **Glitch Detection** - Glitchbased BESs try to analyze abnormal activities and flag these activities as attacks. It can also detect new attacks.

Exploitation detection have very low false positive rate. Since they depend on comparing the incoming traffic with known strings, they are unable to identify novel attacks. Hence a high false negative (Failure to detect an actual attack) rate is observed.

To detect intrusions, there are two techniques namely Hybrid NBES and Honeypots. Snort is the chosensystem as Exploitation-based BES while Packet header glitch exposure (PHGE) and Network traffic glitch exposure (NETGE) are chosen as Glitch-based BES. Glitch detection based breach exposure systems are divided into many sub-categories that are statistical methodologies, data mining, genetic algorithms and immune systems, etc. Among these sub-categories, statistical methods are the most commonly used ones in order to detect breaches by analyzing strange activities occurring in the network. PHGEand NETGE statistical methods are chosen as the glitch-based breach exposure systems in this paper. We have implemented a hybrid BES by mounting glitch based BESs PHGE and NETGEto Snort as a preprocessor. PHGE models protocols rather than client behaviors. Also, it uses a time-based model depending on the dynamic reprogramming of network. PHGE flags only the first anomaly it detected as an alert even if there is a series of the same glitch recurring. This feature of PHGE helps reducing the number of fakealerts. NETGE, models single packets like PHGE, uses dynamic-conditioned rules,and models values that are known.

Fig. 2.1Hierarchy of BES

Signature-based systems can only detect attacks that are known before whereas glitch-based systems are able to detect unknown attacks. Glitch-based BESs makes it possible to detect attacks whose signatures are not included in statute files. According to this approach, behaviors deviating from behaviors assumed as ‘‘normal” are thought to be attacks and glitch detectors compute the deviation in order to detect these attacks. Glitch detectors construct profiles of users, servers and network connections using their normal behaviors. Using the data, that is accepted as normal produced these profiles. After the profile construction, detectors monitor new event data, compare the new data with obtained profile and try to detect deviations. These deviations from normal behaviors are flagged as attacks.

Snort is an open source and rule based network breach exposure system. Using Snort, it is possible to combine new functionalities during compilation. Snort is the most commonly used signature-based breach exposure system. Snort is a network breach exposure system that runs over IP networks analyzing real-time traffic for detection of misuses. Snort depends on a template-matching scheme.

1. **Approach**
2. *Using PHGE and NETGE-*

In PHGE model normal values are the values seen at the time of training. Deviations from these values are detected at the test phase. PHGE calculates glitch scores for every packet and makes no distinction between incoming and outgoing traffic.

Network traffic glitch exposure (NETGE) is the second glitch-based approach added to Snort as a preprocessor in this paper. NETGE also models packets as PHGE does and it operates in two stages: the first stage is the filtering of incoming client sessions to distinguish beginning of sessions. The second stage is the modeling stage. Filtering stage eliminates the traffic up to 98–99%. This elimination simplifies the traffic for the modeling stage. Only the traffic data, which provide evidence of attacks are included in, is passed to the modeling stage. PHGE and NETGE are added one by one to signature-based BES namely Snort as a preprocessor in this paper.After surveying many papers and techniques we have concluded that final system is called the hybrid BES (Snort + PHGE + NETGE) and it is tested ona dataset containing 201 attacks. It is observed that number of attacks detected increases much more with the hybrid BES. Snort, on its own, is able to detect 27 attacks. After PHGE is added as a preprocessor, this number increases to 51 and finally after NETGE is added as a preprocessor the number of attacks detected increases up to 146.As a result it can be mentioned that combining PHGE and NETGE as a preprocessor which are glitch-based systems with the signature-based BES Snort, contributes to breach exposure positively. The hybrid BES is said to be more powerful than the signature-based on its own because it uses the advantages of glitch-based approach for detecting unknown attacks.

1. *Using Honeypots*

C:\Program Files\Microsoft Office\MEDIA\CAGCAT10\j0205582.wmfAnother technique to detect intrusions is called Honeypots. Honeypots are incorporated in network with firewall and Breach exposure systems to provide concrete secure platform to an organization. The disadvantage of above discussed system is that it detects those malicious activities that are blocked by Firewall and may also generate large number of false positives. Honeypots then introduced in the network to utilize the network’s unused IPs and the attacker’s behavior is analyzed on these Honeypots. Honeypots improve BES too by decreasing the numbers of false positives and accurate. Honeypots is an individual security resource that provides features such as early warning system, and capturing novel exploits to gathering intelligence on rising threats. There are two types of Honeypots. First is research Honeypots and other one is production Honeypots. Research Honeypots are basically used to achieve information about the new ways of attacks, viruses, worms which are not detected by BES. These Honeypots are used for research purposes. Its primary function is to trace the path of attacker and gain knowledge about the new ways of attacks performed threats. Production Honeypots are easy to organize and are primarily used by companies or corporations. These Honeypots are assembled with server inside the network of the organization to improve overall security. It provides instant security to production resources. Honeypots assumes that the traffic sent is unauthorized that means there is no false positives and no false negatives. One more advantage of using Honeypots is that, it can work in any IP environment including IPv6. IPv6 is the new version of IPv4.

C:\Program Files\Microsoft Office\MEDIA\CAGCAT10\j0205582.wmf

C:\Program Files\Microsoft Office\MEDIA\CAGCAT10\j0205582.wmf

DATABASE

BACK END SERVER

NBES

NBES

Internet

Firewall

Firewall

Fig. 2.2NBES in internal mode deployment

Nowadays, the demand for a secure network is on upstarting .Network security can be maintained by making use of various authentication techniques. User has to use authentication technique depending on requirement. One crucial challenge with computer and network security is the determination of the difference between normal and potentially unsafe activity. The core component of popular BESs, like Snort, is a Cavernous packet examination (CPE) that checks incoming packets against a database of known signatures (also called rules). Exploitation of traffic classification and load statistics may bring significant savings in the design of Network breach exposure system (NBES). The ultimate design goal for a breach exposure system is the development of automated and adaptive design tool for network security. Honeypots is an exhilarating new technology with huge potential for security communities.

1. **CLOUD ANTIVIRUS**

Antivirus software is one of the most widely used tools for detecting and protecting from the malicious and unwanted files. It is deployed on most desktops and workstations in enterprises across the world. However, the traditional host-based antivirus is ineffective against zero-day attacks or next-generation malware. Therefore, the malware detection capabilities are shifted to the cloud by implementing the antivirus as an in-cloud network service, extolling the speed of cloud computing to deliver real-time protection. Since most of the analyzing capabilities have been shifted to the cloud computing, it imposes less strain on the system’s performance and resources compared to the host-based antivirus.

A) **Host-based antivirus software**

Traditional antivirus software relies upon signatures to identify malwares. When a malware arrives, it is scrutinized by the dynamic analysis system. Proper signatures of the malware are extracted from the file and added in the signatures database of the antivirus [4].When a particular file has to be scanned, it is matched with the signatures stored in the database, and if it matches the signature then the antivirus knows which malware it is and takes the appropriate procedure against it.

However, this approach is not effective against new malwares, which are not yet analyzed, due to two reasons. First, many of the malwares remain undetected by the antivirus. There is a significant chance of vulnerability between when a threat is first seen and when malware researchers generate the signature and modify the software to detect it. Second, the malwares exploit the vulnerabilities of the ever-increasing complexity of the antivirus software.

1. **Antivirus as an in-cloud network service**

Cloud antivirus is a technology that uses lightweight software on end-hosts, while offloading the majority of data analysis on the provider’s cloud infrastructure [5]. One of the benefits of offloading analysis to the cloud is that the decision engine’s logic is not directly accessible by the attackers. Oberheide [6] proposed in his thesis “N-Version Antivirus in the Network Cloud” a new model for detection functionality currently performed by antivirus. The key changes are:

1. **Malware analysis by cloud engine**-Instead of performing the complex analysis on every end-host, the lightweight software captures the relevant details about the new files and provides them to the cloud engine for analysis. Then it permit/deny access to the file based on the report returned by the cloud service.
2. **Multiple scanning engines**-The analysis should be performed by deploying multiple, heterogeneous detection engines in parallel for detecting malicious and unwanted files.

NETWORK SERVICE

FILE

ANALYSIS ENGINE

HOST AGENT

THREAT REPORT

Fig. 3.1Flow of process for cloud AV

1. **Approach**

In this, we use cloud as Software as a service (Saas), where users are provided access to application software and databases, referred to as on-demand software. We combine the traditional signature-based detection technique with dynamic detection method based on heuristics and behavior.

1. **Optimized Signature-based matching**

This method depends on the signature database and string matching algorithm (for similar DNA sequences) to find variants of virus efficiently. Based on the self-replicating characteristic of the virus, many replicas of the virus co-exist in the system. Viruses scan the targeted files and insert the malicious code in the normal files. When any virus is detected, its signature is stored temporarily in the cache so that the replicas need not be matched with large amount of signatures in database. So, signature matching time is greatly reduced.

1. **Dynamic analysis using heuristic and behavioral methods**

This method analyses the suspicious file’s characteristics and behavior to declare it affected. Heuristic analyzer looks for suspicious commands indicative of a class or family of viruses. If a file contains matching code patterns, then it is declared as infected.For depth analysis, behavioral analyzers can also be used. Behavioral analyzers execute the suspicious file or program in a virtual environment logging what actions it performs. Depending on the actions, analyzer declares the file infected.

Cloud

File For Scan

No

Static Analysis

No Virus

Yes

Dynamic Analysis

No

Normal

Yes

Viruses

NOTIFICATION: - Threat Report to User

Fig. 3.2Flowchart for malware detection

The report is then submitted to the user for him to take necessary actions if the file is infected. We combined the optimized signature-based matching and heuristic technique to detect known as well as unknown viruses. This approach provides 35% better detection coverage against recent threats compared to a single antivirus engine and a 98% detection rate across the cloud environment.

1. **ANTI SPAM**

‘Spam’ is defined as flooding the internet with multiple copies of a single message in order to impose the message on people who would not otherwise choose to receive it. They are mainly used for commercial advertising, often for dubious products. Sometimes clicking on links in spam email may send users to phishing websites or sites that are hosting malware.

There are two main types of spams- Usenet spam and Email spam. Cancellable Usenet spam is a single message sent to 20 or more newsgroups. These types of spam generally deprive the users from useful content by overwhelming them with a stream of advertising posts. Email spam targets individual users with direct mail messages

Spam detection techniques can be broadly classified into 1) Based on machine learning 2) Not based on machine learning. Machine learning is a technique that discovers and studies the algorithms that can learn from and make predictions on data.

SPAM Detection Techniques

Not Based on Machine Learning

Based on Machine learning

Rule Based, Signatures, Black listing, Hash-based, Traffic analysis

Independent

Dependent

Bayesian, Neural networks, Memory Based, Markov random fields, artificial immune system

Adaptive, Trust Network

Fig. 4.1 Types of spam detection techniques

Dependent solutions mainly constitute a part of a bigger spam detection solution (which can be either based on machine learning or not). They act as a secondary system. Independent solutions mainly construct their own database according to which they differentiate the mails and messages.

Some of the commonly used spam detection techniques are-

1. **Rule Based analysis** - It is a quick and simple technique that uses certain predefined rules to find expressions that are similar across spams. But relative to new detection techniques, this method has certain drawbacks. The rule set is fixed. So if a new threat arrives then the system must be updated to recognize that mail as a spam. If the spam arrives before this updating, then the system fails to achieve its objective.
2. **Signatures** - For each identified spam they generate a distinctive symbol or a value called signature. When a mail arrives the system compares its signature with the values stored in its database. If an equivalent value is found the mail is categorized as spam. It generates quite a low level of false positives. But the major limitation is that if a spam is received before its signature has been disseminated then this method fails to detect it. Moreover, for efficient maintenance of the database the older signatures are removed thereby providing the attackers an opportunity to attack.
3. **An efficient approach**-

Bayesian ﬁltering is an effective and a widely used technology for spam detection. It is a popular statistical technique of email filtering. It overcomes most of the limitations of previously known techniques. Naïve Bayes classifiers work by correlating the use of tokens, with spam and non-spam emails and the using Bayesian inference to calculate a probability that an email is or is not a spam.

Depending upon the types of mails received and user’s choice, a rule set is constructed. The sender is unfamiliar to this rule set. The rule set is modifiable and is adaptive to the user’s choices.

Two tables are maintained in Bayesian filters- one of spam tokens and one of ‘ham’ (legitimate) mail tokens. Each spam has an associated probability using which the system categorizes a mail as a spam. Similarly probabilities are maintained for each ham. Probability values are initially established by training the ﬁlter to recognize spam and legitimate email, and are then continually updated based on email that the ﬁlter successfully classiﬁes. Incoming email is tokenized on arrival, and each token is matched with its probability value from the user’s records. The probability associated with each token is then combined, using Bayes’ Rule, to produce a probability that the email is spam.

This method categorizes a legitimate and a spurious mail based on user’s feedback which enhances its accuracy and allows detection of new spam types.

The performance of this filter is more effective at the user level as compared to the mail server level. As each user will differently consider some mails as spam therefore a database constructed from user’s data will provide more accurate results.

To calculate the overall probability of an email being spam (P):

P = (1)

Where xi is the probability of a word that was included in previous mails that were classified as spam.

1. **PERSONALIZED CONTENT FILTERING**

Censor-ware is used by corporations as part of internet firewall computers to restrict or control the content which a user is authorized to view on the Internet via the Web, e-mail or other means. Censor-ware blocks the unwanted content of the Webpage or e-mail. As the diverse information on the internet is available to all the users, the need for content filtering is impeccable. Content filtering ensures security, prevents legal trouble and improves user productivity.

The simple and easy method is to block webpage based on URL filtering and IP addresses. However, it is not efficient for unknown websites and it is difficult to obtain the complete block list. Given that the internet consist of tens of billions of web-pages with millions added per day, this approach is ineffective at providing protection from objectionable content [8]. Also, the traditional content filtering tools block the entire webpage found objectionable. Instead of completely blocking a page, it is efficient to block only those segments which contain objectionable content since different portions of the web page holds different contents. This method provides fine-grained blocking and automatic identification of the segments of the web page to be blocked.

The objective of the content filtering is to propose a model for web page segmentation and incorporating personalization to enhance the capabilities of the content filtering process. The model incorporates two methods:

1. **The web page content filtering-**There exist many approaches for web page content filtering such as rating systems [9], text classification based approach [10], [11]. The approach used in our model is keyword based blocking method.
2. **The web page segmentation-** Web page segmentation is the process of dividing the web page into segments based on certain criteria. DOM based web page segmentation approach is used, in which HTML tag tree’s Document Object Model will be used for segmenting.

The model has three main components:

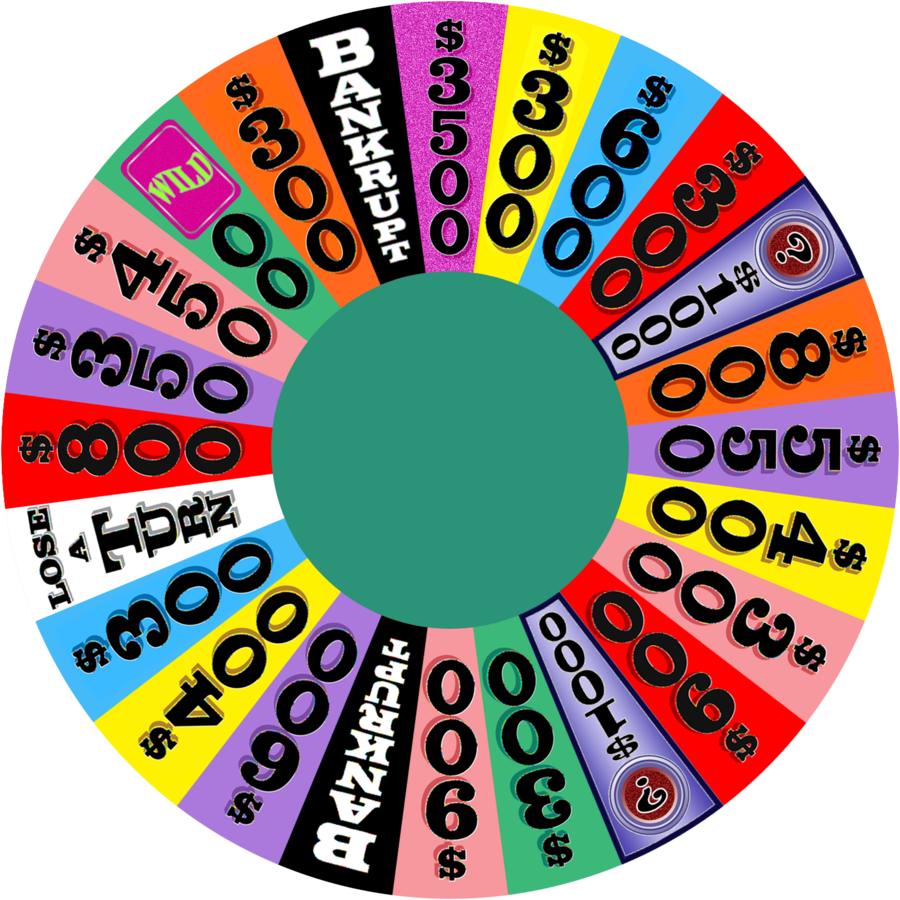
1. **Segmentor**- This component is responsible for segmenting the web pages into logically smaller segments.
2. **Personalizer**- This component is used for incorporating personalization while filtering content. It consults a list of permitted and denied keywords.
3. **Filter**- This component filters the segments which contain objectionable content.

Source page

Segmentor

Personalizer

Filter



Filtered Page

Fig. 5.1Model of personalized censor ware

In this approach, each page which the user requests is segmented into smaller units for the filtration. This is achieved by the segmentor component. The source page is mapped as a DOM tree. After performing the segmentation, each segment is processed individually by the filter component. Each segment contains three components:

1. *Text*
2. *Link*
3. *Image*

Each segment is individually scrutinized for the three components whether they contain objectionable content which needs to be blocked. The model incorporates the personalization aspect. The user can configure according to his requirements. For personalization, the model consults a bag comprising allowed and denied list of keywords. The keywords in the allowed list give a positive value while keywords in denied list give negative value. If the cumulative value of the individual segment exceeds a threshold value, that segment is displayed, else blocked. If the segment is blocked, message “segment blocked” will be displayed.

This model has 88% accuracy in filtering out the segments containing objectionable content [12].

1. **SPARTA**

The new research in the field of network security and internet has not only lead to the development of some path breaking technologies, but also has created some difficult to handle and predict attacks and viruses. These new threats lead to sensitive information being coerced or its loss. In such a case mechanisms to both protect and prevent any such attacks is essential. In order to achieve prevention we use Network Access Control.

Network access control (NAC) can be defined as the scheme of bolstering the security of the network by limiting the access to the network resources, conforming to some protocols. A traditional network NAC restricts the data that each particular user can access, as well as implementing anti-threat applications such as firewalls, antivirus software and spyware-detection programs. The available NAC devices are not equipped enough to handle the avant-garde attacks and are not flexible enough of incorporate the changes brought about by the perpetual research, making them a transient.

The proposed system “SPRATA” is a step towards integrating the various security products that were earlier deemed as incompatible and provide an end to end protection to the host. Its assessment is not limited to the users but extends to the nodal hosts, while ensuring the veracity of those nodes. Sparta has an open architecture giving it that much needed edge over the present technologies. Several access control models, such as Role based access control (RBAC) model and Task based authorization control model (TBAC), have been proposed. Sparta’s architecture is composed of two entities: Entrée Retriever (ER) and Access Protocol Governor (APG). However, 3 entities - Protocol Point (PP), Perilogos Reclamation Point (PRP), and Synaptic Managers and Controllers are supplements that can be augmented according to network needs. It needs to be noted that this technology is only being suggested to aggrandize the access control mechanisms in the threat management technology already present in the host, and acts a veneer to the capabilities of the used technology.

SPARTA

Fig. 6.1Components of SPARTA(Access control mechanism)

1. **Major Components**

To give a better idea about the components of SPARTA their functions have been summarized below-

1. *ER* is responsible for sagacity of the network node, where it tabulates information such as firewall used, OS and other vital information.
2. The ER sends the information about state of health and user identity to *APG*.
3. APG authenticates user’s identity and evaluates health status of ER with protocols, and then makes decision about enabling access to the network to ER.
4. Further, APG informs about the decision to *PP* which is responsible for execution of the decision taken.
5. PP enforces policies and controls access to the protected network.

Sparta uses stores all the pre requisite information gathered by the ER in tabular form. Its main design has three tables each storing some information. The description of the information is given below-

1. **Node-Attestation Table**- the Node-Attestation Table contains four fields: source IP address, position, testament number, and timeout value. It is accountable for all the packets from the source IP address, which is sent by a user who has positions. The testament number is given by the base threat management technology being used in the host. Only the APG can add entries to the Node-Attestation Table. Entries will be removed when timeout due to inactivity or by the APG. The APG might remove an entry belonging to a host when it does not qualify for network access, or it has left the network.
2. **Testament-Resource table**-The Testament-Resource Table contains two fields: testament number and resources. It describes the association between testaments and resources authorized. Testament-Resource Table and Node-Attestation Table have a common field testament. Considering them together, UTM knows which source IP address could access what resources, and then generates dynamic firewall policies. UTM-Testament-Resource table is firstly generated and stored in APG by network policies. When a connection between UTM and APG is just set up, the APG pushes the table to UTM. And only APG can update the table.
3. **Protection-Action table**- It is a table responsible for mapping between testament number and salvation protocol. Testament-Resource table, Protection-Action table is also transferred to host by APG when a connection between host and APG is set up.

Fig: 6.2Hierarchy of ER table

*Access Protocol Governor (APG)*

APG can easily be described as “intelligence” of the network. This is where network administrator deploys its policies. According to the specifications of our model, out of all the technologies available XACML can be used for its implementation. Major tasks of APG are:

1. Resolution of the network policies, and their dissection to determine the available resources and the roles which have permission to access, what salvation protocols the testament number indicates.
2. Authenticate user identity, and assign position to the host.
3. Assessment of host health status, retrieve host protection capabilities and assign testament number to the host.
4. It is also responsible for mapping IP address, user, MAC address, position, salvation protocols, and switch information together.
5. Send decisions to the switches and host threat management technology. Also APG records testament-resource and user position in the tables in the questions.
6. **SPARTA Attack Prevention Technique**

Spoofing is one of the major attacks that have been a cause of concern for currently used techniques. In this attack using various IP addressing masking techniques the attacker may adopt an IP address which can gain access to the host easily. Due to the masked IP, many of the presently used network security mechanisms are not able to forestall them. However the technology being develop can detect such attacks by appraising the change in IP address. Here APG is the main player

Another possible attack is that attackers can still intrude the hosts with high protection ability because of some wrong operations made by users or wrong policies made by network administrator. Therefore, in our design, Sparta would be required to filter these flows randomly and periodically instead of “all pass”; the timeout value of Node-Attestation Table is used to check the availability lifetime of host protection ability in order to avoid some un-predictable change of host health status.

1. **MONICAN**

The proposed system is an integration of many different technologies hence for proper control and management is essential. The sacrosanct requirement of a monitoring system can be felt.

For this purpose a technology “MONICAN” a new age control and management technology will be ideal.

The main features of this monitoring device include-

* *General Management*
* *Network Routing and Services*
* *Network Device Management*
* *Threat protection*
* *Authentication*

Other than the aforementioned capabilities MONICAN juxtaposes the user driven protocols with the network monitoring protocols. It gives user the opportunity to define access and the role of the host requesting access.MONICAN acts as the ideal system for not only the proposed integrated system for any other network security related device in question. The main features of the MONICAN have been elaborated below-

* 1. **General Management**

Other than providing a user friendly interface, MONICAN is capable of role based administration. It has the capability of providing centralized management for multiple security devices which are virtually incompatible. This system is a self-service portal with a capability to provide one click VPN setup. This system is the archetype of a flexible and mutable model that can be perceived by handler. Other than its general features, a very useful GUI enhances the sniffing capabilities of the user many folds. Overall, MONICAN is the epitome of any control system.

* 1. **Network Routing and Services**

Multiple routing capabilities such as static, multicast, dynamic, snooping are effectively available in the proposed system. This has the capability of providing auto health check and availability of clustering. This device can balance upto 10 appliances with high availability for active/passive clustering. Its interface link aggregation capability is one of the most desirable features in any monitoring device. The contingency attacks that our integrated system is capable of handling are shown with the network information in MONICAN.

* 1. **Network Device Management**

One of the major gateways for attacks on system can be monitoring devices as they are not well equipped with capability of intrusion protection. The proposed system, can be used for intrusion detection as it performs deep packet inspection. It has the capability of recognizing more than 18,000 patterns which are more than any other monitoring device of its range. It uses pattern matching algorithm and aging for a more optimizing results. We are shown the operations being performed by each device separately in the form of screens providing the user opportunity to analyze the functions of each device separately. The networks in the system are shown with a country wise demarcation, giving us data to analyze the type of data being sent and received by the majority. With separate inbound/outbound settings and exception a complete protection package is provided to us. To take its protection capabilities to the next level an identity based authentication rules and configuration are provided.

* 1. **Threat Protection**

MONICAN’s threat protection capabilities are the better than any device in its range. It can detect and clock network traffic attempting to control the servers using any application layer facility and firewall. This is accomplished by identifying the infected hosts on the network and containing their network activity. Another technique that helps it in thwarting the attacks is by selective sandboxing of suspicious code to determine malicious intent. MONICAN is equipped with the capability of managing every device in the network and showing their status at the same time to the user.

* 1. **Authentication**

Taking the network protection to the next level, the proposed system adds another layer to the protection capabilities of the integrated system by adding the feature of server settings check, this is done by combining authentication cache flush for user groups and graphical browsers. Scheduled backend synchronization help the system working fine at all times. The most striking feature of MONICAN is its policy testing capability tool for URLs that is operating at all times.

With all the features MONICAN is not only an ideal device for control and management of integrated system but also any other devices that are involved.

**CONCLUSION**

The integrated system works effectively to provide a secure network. The various components complement each other’s job and provide a solution to almost every possible attack. The next generation IPS prevents malicious attacks using additional features like user awareness, application awareness etc. Network breach exposure system (NBES) provides next-level intrusion detection techniques using various methods like Cavernous packet examination (CPE), NETGE, PHGE etc. It produces very few numbers of false positives. Antivirus software is a necessity in today’s society where new malwares are continuously developed. Cloud based antivirus technique is an optimal technique that incorporates both static and dynamic analysis. Anti-spam techniques are implemented in various ways (software, hardware, service) and at various levels(user, server). Bayesian filtering is widely used technique that greatly improves filter accuracy. Personalized content filtering blocks only particular portion of websites instead of blocking the complete URL. Sparta provides an ideal solution for access control. Monican is a monitoring solution that senses the network and notifies any degradation in performance.

**REFERENCES**

1. Wikipedia. http://en.wikipedia.org/wiki/Honeypot.
2. Przemyslaw Kazienko & Piotr Dorosz. Intrusion Detection Systems (IDS) Part I - (network intrusions; attack symptoms; IDS tasks; and IDS architecture). www.windowsecurity.com › Articles & Tutorials
3. Sutapa Sarkar& Brindha.M. High Performance Network Security Using NIDS Approach. *I.J. Information Technology and Computer Science,* 2014, 07.
4. Ask Karin, Automatic Malware Signature Detection, <http://www.gecode.org/~schulte/teaching/theses/ICT-ECS-2006-122.pdf>, 2006, 10.
5. What is cloud antivirus and how does it work?, https://zeltser.com/what-is-cloud-anti-virus/ .
6. Oberheide J.,Cooke E. and Jahanian F., “Cloud N-VersionAntivirus in the Network Cloud”,Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI 48109 (2007).
7. Hatem S.S., Wafy M.H., El-Khouly M.M., “Malware Detection in Cloud Computing”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 4, 2014
8. Meeting the Challenges of Web Content Filtering http://dansguardian.org/downloads/content\_filtering\_challenges.pdf.
9. Paul Resnick and Jim Miller. PICS: Internet access controls without censorship. Communications ofthe AGM, 39(10):87-93, 1996.
10. Du, R.; Safavi-Naini, R.; Susilo, W.; Web filtering using text classification, The 11th IEEEInternational Conference on Networks, 2003. ICON2003.pages:325 – 330.
11. Weiming Hu, Ou Wu, Zhouyao Chen, Zhouyu Fu, Maybank, S., "Recognition of PornographicWeb Pages by Classifying Texts and Images", Pattern Analysis and Machine Intelligence, IEEE Transactions on, On page(s): 1019 - 1034, Volume: 29 Issue: 6, June 2007.
12. Kuppusamy K.S., Aghila G., “A Personalized Web Page Content Filtering Model based on Segmentation”, IJIST Vol.2, No.1, January2012.
13. Fachao Deng, Anan Luo, Yaokun Zhang, Zhen Chen1, Xuehai Peng,Xin Jiang, Dongsheng Peng.,”TNC-UTM: A Holistic Solution to Secure Enterprise Networks”,the 9th International Conference for Young Computer Scientists.
14. D.E.Taylor. Survey & Taxonomy of Packet Classification Techniques. ACM Computing Surveys,Volume 37, Issue 3, 238-275. Sep 2005.
15. <http://tnc.inform.fh-hannover.de/wiki/index.php>
16. <http://www.webopedia.com/TERM/N/network_security.html>
17. Sophos security made simple UTM feature list