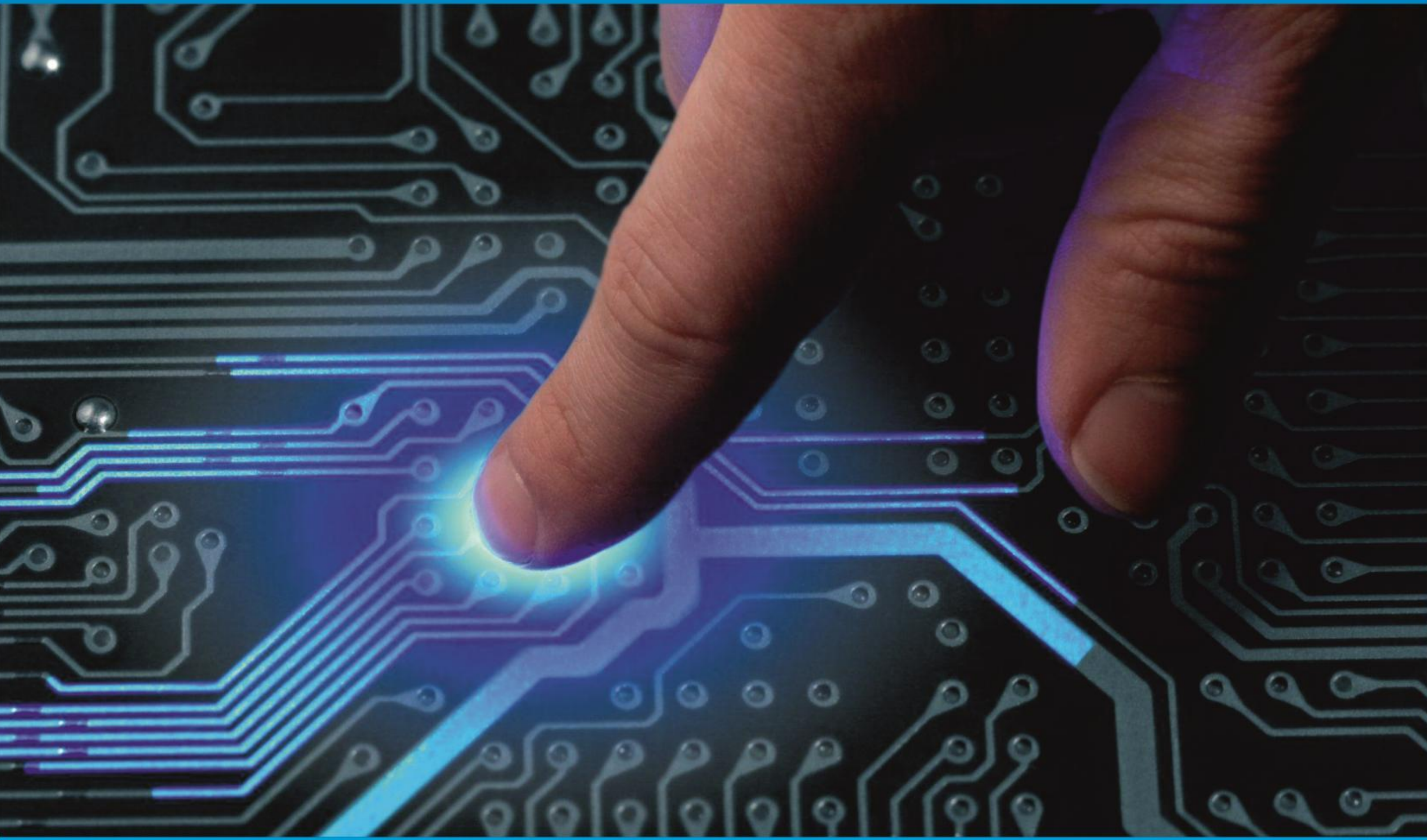
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 11, November 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

A Study on Network Security

Toshinee Bhasin[1], Prof.Mrs.Rama S.Bansode[2]

P.G. Student, Department of Computer Application, P.E.S. Modern College of Engineering, Pune, Maharashtra, India[1]

Research Scholar, TMV Pune & Asst. Professor, P.E.S. Modern College of Engineering, Pune, Maharashtra, India[2]

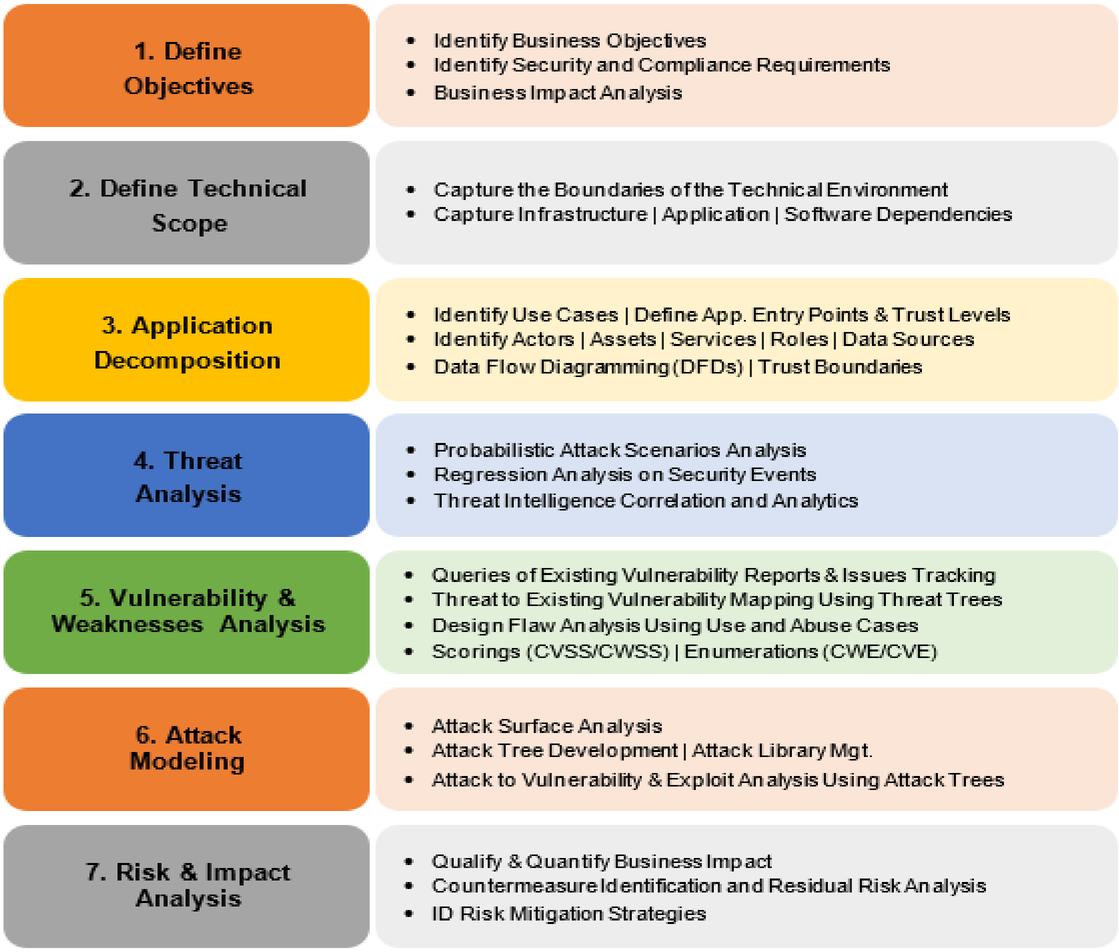
ABSTRACT: Network security has become more salient to non-public computer users, organizations, and also the military. With the looks of the web, security became a significant concern and also the emergence of security technology. the web structure itself allows for several security threats to occur. Many businesses secure themselves from the net using firewalls and encryption mechanisms. The business has created an "intranet" to stay connected to the web and secure from possible threats. Secure Network has now become a desire of all organizations. Safety risks are rising on a regular basis, resulting in high-speed, vulnerable and insecure wired/wireless networks and Internet services. Now a day's security measures work more importantly towards fulfilling the forefront demands of today's growing industries. Wi-Fi networks are quite common in providing wireless network access to different resources and connecting various devices wirelessly. There's a requirement for various requirements to handle Wi-Fi threats and network hacking attempts. This paper explores precautions associated with different network scenarios so a protected network environment could even be exhibit in an exceeding corporation. During this paper, we'll study different sorts of attacks together with styles of security mechanisms that may be applied to stay with the necessity and architecture of the network.

KEYWORDS: Cryptography, Security Attacks, Security Measures, Security Tools, WAN, Security Factors, Firewalls, Gateways, Intrusion Detection, Network Security, attacks, hackers, Cloud-environment security, zero-trust model (ZTM), Trend Micro internet security.

I. INTRODUCTION

The world is becoming more interconnected because of the net and new networking technology. There's an oversized amount of personal, commercial, military, and government information on networking infrastructures worldwide. There are two sorts of fundamentally different networks: data networks and synchronous network comprised of switches. The online is taken into consideration as a knowledge network. Since this data network consists of computer-based routers, the data are visiting be obtained by special programs, like "Trojan horses," planted within the routers. E-business applications like e-commerce, supply-chain management, and remote access allow companies to streamline processes, lower operating costs, and increase customer satisfaction. Such applications require mission-critical networks that accommodate voice, video, and data traffic, and also these networks must be scalable to support increasing numbers of users and also the necessity for greater capacity and performance. However, as networks enable more and more applications and are available to more and more users, they become ever more in danger of a wider range of security threats. To combat those threats and make sure that e-business transactions don't seem to be compromised, security technology must play a limitless role in today's networks. The synchronous network that consists of switches doesn't buffer data so isn't threatened by attackers. That's why security is emphasized in data networks, rather a touch just like them online, and other networks that link to the web. The general subject of network security is explored by the following research:

1. Internet architecture and vulnerable security aspects of the web.
2. styles of internet attacks and security methods.
3. Security for networks with internet access.



1. Define Objectives
- Identify Business Objectives
- Identify Security and Compliance Requirements
- Business Impact Analysis

2. Define Technical Scope
- Capture the Boundaries of the Technical Environment
- Capture Infrastructure | Application | Software Dependencies

3. Application Decomposition
- Identify Use Cases | Define App. Entry Points & Trust Levels
- Identify Actors | Assets | Services | Roles | Data Sources
- Data Flow Diagramming (DFDs) | Trust Boundaries

4. Threat Analysis
- Probabilistic Attack Scenarios Analysis
- Regression Analysis on Security Events
- Threat Intelligence Correlation and Analytics

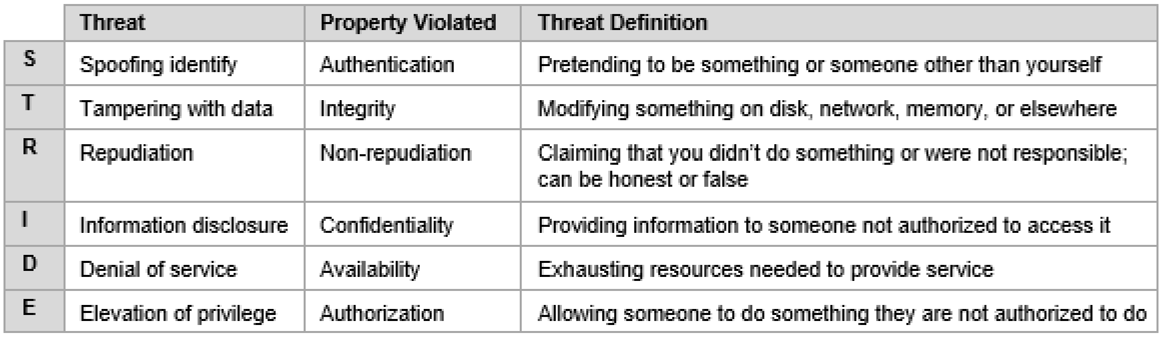
5. Vulnerability & Weaknesses Analysis
- Queries of Existing Vulnerability Reports & Issues Tracking
- Threat to Existing Vulnerability Mapping Using Threat Trees
- Design Flaw Analysis Using Use and Abuse Cases
- Scorings (CVSS/CWSS) | Enumerations (CWE/CVE)

6. Attack Modeling
- Attack Surface Analysis
- Attack Tree Development | Attack Library Mgt.
- Attack to Vulnerability & Exploit Analysis Using Attack Trees

7. Risk & Impact Analysis
- Qualify & Quantify Business Impact
- Countermeasure Identification and Residual Risk Analysis
- ID Risk Mitigation Strategies

II. NETWORK SECURITY THREAT MODELS

Network security refers to activities designed to guard a network. These activities make sure the usability, reliability, and safety of a business network infrastructure and data. Effectual network security focuses on a spread of threats and hinders them from penetrating or spreading into the network. a number of the everyday cyber-attack models. the foremost common threats include:



	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

A. FLOODING:

In1998, the Upper American crust, "The Digital Disturbance Theater," came up with the Flood Net, an application to stop the Mexican President's website. Flood net may well be a java applet that automates the "refresh" button to click repeatedly. Sufficient users online would run the applying and hence cause the site's server to continuously refresh until saturation and thus halt and disable the webpage. An attacker has used similar applications to want into hostage commercial websites in exchange for ransom. An emergency organization should have a competent security specialist (White-hat hacker) to see that web technology is complex, with ever-changing patterns in web scripting languages and browser configurations.

B. TROJANS:

An skilled programmer is capable of creating a Trojan, a secret application that runs in the background. A Trojan enables a hacker to become a ghost user on your PC/Workstation. Hackers can always come and upload a malicious code via the Trojan. Such a code is also the one that kills your antivirus program after which, it takes your snap via webcam or taps into your office conversations from your laptop microphone. Trojans come tucked away neatly on pirated software and also the so-called cracks we all prefer to use because the adage goes, it's difficult to cheat an honest person. The converse is true for people who would escape this pitfall. allow them to invest in genuine software.

C. BLUETOOTH:

Bluetooth is emerging as a versatile networking technology connecting workstations to printers, smartphones, etc. I see the potential for mischief; where data could be wirelessly intercepted for malicious use. Such technology is currently non-existent, to the best of my knowledge, but a practical possibility.

D. PHISHING:

This is when emails appearing to return from well-known organizations pop on your browser, sending you links and requesting private information like MasterCard numbers, account passwords, or congratulating you for winning. be careful with that nice email from a web site you are doing not even have an account with. Look-alike websites are not uncommon. they'll have your login and 'refill' your details; after which they'll make online purchases under your name or if they're diabolical enough, they're going to lock you out of your account. (I lost my yahoo account that way). Numerous cybersecurity forums and workshops exist where one can always learn ways to possess a footing over scammers and keep your business team informed.

E. RADIO JAMMING:

This can be a rare DOS (Denial of Service) technique to disrupt information flow in an exceedingly wireless router network, accomplished by the employment of noise-generating radio devices. However, special Equipment exists, that may be accustomed track anonymous radio-noise sources, should interference be detected.

F. SERVER SECURITY HOLES:

Server Security can be compromised via security holes in a web application like add ons / plugins such as Joomla / WordPress. It is advisable to use only secure connections whenever possible. This includes the use of SSL connections for email and SFTP (Secure File Transfer Protocol) instead of the more common but insecure FTP protocol.

G. ZERO DAY/HOUR ATTACK:

The 'sticky keys' feature (sethc.exe) on your XP or Windows7 OS. It is a good accessibility feature that allows one to press special keys only once at a time. This application runs on the login window when you press the shift key five times even before you've entered your password. One only needs to rename the command prompt shell (cmd.exe) to sethc.exe on a logged-in computer. By this, they will have gained full control of your laptop or workspace computer anytime later without passing through any known account. How? By simply pressing the shit key five times and voila, the command prompt! Try this for yourself (Hope they got that patched on Windows 8). Zero hours/day attacks take advantage of software vulnerabilities that are yet to catch the eye of a software manufacturer. Should you discover such a bug, report to the software company for a patch to make up for the bug in later releases. Otherwise, a hacker may discover the same loophole later, and use it maliciously.

III. TYPES OF ATTACKS

Networks are subject to attacks from malicious sources. And with the looks and increasing use of internet attach is most typically growing on increasing. the foremost categories of Attacks could also be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" within which an intruder initiates commands to disrupt the network's normal operation. A system must be able to limit damage and recover rapidly when attacks occur. There are some more styles of attack that are essential to be considered:

A. **Passive Attack:** A passive attack monitors unencrypted traffic and appears for clear-text passwords and sensitive information which can be used in other sorts of attacks. The monitoring and listening of the communication by unauthorized attackers are named as a passive attack. It includes traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information like passwords. Passive interception of network operations enables adversaries to work out upcoming actions. Passive attacks end within the disclosure of knowledge or data files to an attacker without the consent or knowledge of the user.

B. **Active Attack**: during a vigorous attack, the attacker tries to bypass or forced the lock secured systems within the happening communication. this might be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to bypass or break protection features, to introduce malicious code, and to steal or modify information. The unauthorized attacker's monitors hear and modify the information stream within the communication are cited as active attacks.

C. **Distributed Attack:** A distributed attack requires that the adversary introduce code, sort of a worm or back-door program, to a ―trusted component or software that will later be distributed to many other companies and users Distribution attacks target the malicious modification of hardware or software at the factory or during distribution.

D. **Insider Attack:** According to a Cyber Security Watch survey insiders were found to be the cause in 21 percent of security breaches, and a further 21 percent may have been due to the actions of insiders. More than half of respondents to another recent survey said it's more difficult today to detect and prevent insider attacks than it was in 2011, and 53 percent were increasing their security budgets in response to insider threats.

E. **Close-in Attack:** A close-in attack involves someone attempting to get physically close to network components, data, and systems to learn more about a network. Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities to modify, gather, or denying access to information. One popular form of close-in attack is social engineering. In a **social engineering attack**, the attacker compromises the network or system through social interaction with a person, through an e-mail message, or phone. Various tricks can be used by the individual in revealing information about the security of the company. The information that the victim reveals to the hacker would most likely be used in a subsequent attack to gain unauthorized access to a system or network.

F. **Spyware attack**: A serious computer security threat, spyware is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information. And this capture information is maliciously used as the legitimate user for that particular kind of work.

G. **Phishing Attack:** In a phishing attack the hacker creates a fake website that looks exactly like a popular site such as the SBI bank or PayPal. The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

H. **Password attack**: An attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a **dictionary attack**, **a brute-force attack**, and a **hybrid attack**. A dictionary attack uses a word list file, which is a list of potential passwords. A brute-force attack is when the attacker tries every possible combination of characters.

IV. TECHNOLOGIES FOR PROVIDING SECURITY TO THE NETWORK

Internet threats will continue to be a major issue in the global world as long as the information is accessible and transferred across the Internet. Different defense and detection mechanisms were developed to deal with attacks mentioned earlier. Some of these mechanisms along with advanced concepts are mention in this section.

A. **Cryptographic systems**: Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

B. **Firewall:** A firewall is a front line defense mechanism against intruders to enter in the system. It is a system designed to prevent unauthorized access to or from a private network. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. Firewalls can be implemented in both hardware and software, or a combination of both. The most widely sold solution to the problems of Internet security is the firewall. This is a machine that stands between a local network and the Internet and filters out traffic that might be harmful. The idea of a ―solution in a box has great appeal to many organizations and is now so widely accepted that it's seen as an essential part of corporate due diligence. Firewalls come in basically three flavors, depending on whether they filter at the IP packet level, at the TCP session-level, or the application level.

C. **Driving Security**: to the Hardware Level To further optimize performance and increase security, Intel develops platforms that also include several complementary security technologies built into multiple platform components, including the processor, chipset, and network interface controllers (NICs). These technologies provide low-level building blocks upon which a secure and high performing network infrastructure can be sustained. These technologies include Virtualization Technology, Trusted Execution Technology, and Quick Assist Technology.

D. **Intrusion Detection Systems**: An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connections in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack. The typical antivirus software product is an example of an intrusion detection system.

E. **Anti-Malware:** Software and scanners Viruses, worms, and Trojan horses are all examples of malicious software or Malware for short. Special so-called anti-Malware tools are used to detect them and cure an infected system.

F. **Secure Socket Layer (SSL)**: The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server so that any information exchanged is protected within the secured tunnel. SSL provides authentication of clients to the server through the use of certificates. Clients present a certificate to the server to prove their identity.

G. Dynamic Endpoint: Modeling Observable's security solution, represents a profoundly new way to look at IT security. It models each device on your network, so you can understand normal behavior and quickly take action when a device starts acting abnormally. There's no need to install agents on the devices or attempt to use deep-packet inspection, giving you a powerful solution to overcome these new security challenges.

H. Mobile Biometrics: Biometrics on mobile devices will play a bigger role in authenticating users to network services, one security executive predicted. Biometrics emerging on mobile endpoints, either as applications that gather users' behaviors or as dedicated features on mobile endpoints that scan personal features. For example, the iPhone 5s finger scan will emerge in 2014, if these features are open and extensible, it could lead to real innovation in ensuring the identities of remote users.

VI. SOME ADVANCED NETWORK SECURITY POLICIES

A. Making Security in Clouds Environment

Analysts project that IT spending will increase slightly from 2013. This increase in investment is attributed to cloud computing [10]. Over half of IT organizations decide to increase their spending on cloud computing to spice up the flexible and efficient use of their IT resources. Intel Trusted Execution Technology (Intel TXT) is specifically designed to harden platforms against hypervisor, firmware, BIOS, and system-level attacks in virtual and cloud environments. It does so by providing a mechanism that enforces integrity checks on these pieces of software at launch time. This ensures the software has not been altered from its known state. This TXT also provides the platform level trust information that higher-level security applications require to enforce role-based security policies. Intel TXT enforces control through measurement, memory locking, and sealing secrets.

B. Zero-Trust Segmentation Adoption

This model was initially developed by John Kindervag of Forrester Research and popularized as a necessary evolution of traditional overlay security models. One alternative that's a powerful candidate to enhance the protection situation is that the zero-trust model (ZTM). This aggressive approach to network security monitors each piece of knowledge possible, under the idea that each file could be a potential threat. It requires that every one resource be accessed securely, that access control air a need-to-know basis and strictly enforced. The systems verify and never trust; that each one traffic be inspected, logged, and reviewed which system be designed from the within out rather than the surface in. It simplifies how information security is conceptualized by assuming there aren't any longer ―trusted‖ interfaces, applications, traffic, networks, or users. It takes the old model ―trust but verify and inverts it because recent breaches have proved that when a company trusts, it doesn't verify.

C. Trend Micro Threat Management Services

Because conventional security solutions do not adequately protect against the evolving set of multilayered threats, users need a replacement approach. Trend Micro delivers that approach with the Trend Micro Smart Protection Network. The Smart Protection Network infrastructure provides innovative, real-time protection from the cloud, blocking threats before they reach a user's PC or a company's network. Leveraged across Trend Micro's solutions and services, the Smart Protection Network combines unique Internet-based, or ―in-the-cloud, technologies with lighter-weight clients. By checking URLs, emails, and files against continuously updated and correlated threat databases within the cloud, customers always have immediate access to the newest protection wherever they connect—from home, within the corporate network, or on the go. Threat Management Services offers an approach to network security that assesses risk and provides insight on potential gaps within this security environment. The Smart Protection Network consists of a worldwide network of threat intelligence technologies and sensors that deliver comprehensive protection against all kinds of threats— malicious files, spam, phishing, web threats, denial of service attacks, web vulnerabilities, and even data loss. By incorporating in-the-cloud reputation and patent-pending correlation technologies, the Smart Protection Network reduces reliance on conventional pattern file downloads and eliminates the delays commonly related to desktop updates. Businesses take pleasure in increased network bandwidth, reduced processing power, and associated cost savings.

VII. CONCLUSION

Security may be a very difficult and vital topic. Everyone includes a different idea regarding security' policies, and what levels of risk are acceptable. The key to assembling a secure network is to define what security means to your need of the time and use. Once that has been defined, everything that goes on with the network is evaluated concerning that policy. it is important to make systems and networks in such how that the user isn't constantly reminded of the safety system around him but Users who find security policies and systems too restrictive will find ways around them. At the identical time, breakthroughs in technology will provide even greater network security, therefore, greater peace of mind to work in innovative business environments. There are different sorts of attacks on security policies and also growing with the advancement and therefore the growing use of the net. during this paper, we are attempting to check these different sorts of attacks that penetrate our system. because the threats are increasing, so for secure use of our systems and internet there are various security policies also are developing. it was a surprise to work out most of the events going down within the same technologies being currently used. The combined use of IPv6 and security tools like firewalls, intrusion detection, and authentication mechanisms will prove effective in guarding property for the near future. The network security field may evolve faster to cater to the threats further within the future. during this paper, we've mentioned a number of the protection policies that may be used mostly by several users and a few new advanced qualities that fit today's more penetrating environments like Trend micro security mechanism, use of huge data qualities in providing security, etc. Security is everybody's business, and only with everyone's cooperation, an intelligent policy, and consistent practices, will or not it's achievable.

REFERENCES

1) R. Bace, R., and P. Mell, “Intrusion Detection Systems”, NIST Special Publication SP 800- 31, November 2000.
2) Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24-28, Sep 1998
3) “Security Overview,” www.redhat.com/docs/manuals/enterprise/RHEL-4- Manual/security-guide/ch-sgs-ov.html.
4) Molva, R., Institut Eurecom,“Internet Security Architecture,” in Computer Networks & ISDN Systems Journal, vol. 31, pp. 787-804, April 1999
5) Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008
6) Stallings, W. (2006): Cryptography and Network Security, Fourth Edition, Prentice Hall.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ✆ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details