© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 04 | October - December 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in
Peer Reviewed and Refereed Journal

REVIEW ON SECURITY OF MULTIMEDIA DATA OVER DISTRIBUTED NETWORK OVER IDS

Seema Sangwan
Assistant professor computer science
Pt N.R.S Govt college Rohtak.
Email id: cma.sangwan124001@gmail. com

ABSTRACT:- Organizational strategy and infrastructure for protecting data transmissions and physical assets across computer networks. Security in a network takes the form of both hardware and software measures. When asked to define network security, most people focus only on the tools used to monitor and punish breaches. Multimedia includes visuals, sound, moving pictures, and text. The majority of multimedia files tend to be somewhat large. This research includes thorough information about kinds of IDS, life cycle, diverse domains, forms of assaults & tools. Intrusion detection systems are becoming more important for the day-to-day safety of businesses and their network users. IPS specifies about preventive measures for security. In lifetime phases evolved & stages are represented. There are, however, additional hurdles to jump.

Keyword:- Network Security , Intrusion Detection System, intrusion detection

[1] INTRODUCTION

Organizational strategy and infrastructure for protecting data transmissions and physical assets across computer networks. Security in a network takes the form of both hardware and software measures. When asked to define network security, most people focus only on the tools used to monitor and punish breaches. Protecting the privacy, security, and reliability of all data and systems on the network should be a top priority for any enforcement effort. The CIA trio is comprised on the following three tenets: Confidentiality entails guarding resources from prying eyes. Having the assets' integrity maintained by making sure any changes made to them are done so in a predetermined and approved way When assets are available, they are readily accessible by authorised users at all times. It is the goal of strict enforcement to ensure the integrity and confidentiality of any data sent across a network. Classifying traffic flows according to application, user, and content is the first step. Any content delivery application, independent of its transport mechanism (port, protocol, evasion technique, or SSL) must be verified as such by a firewall.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 04 | October - December 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in
Peer Reviewed and Refereed Journal

When an app is properly identified, the data it transports may be seen in its entirety. Identification of apps and mapping of their usage to a user identity, together with constant content inspection for CIA preservation, might streamline policy administration.

Prevention from external attacks

When used in conjunction with a firewall, an intrusion prevention system (IPS) may offer an additional layer of protection by performing a "negative selection" on potentially harmful data. Unlike the passive Intrusion Detection System (IDS), which scans traffic and reports back on threats, the Inline Predictive Security (IPS) system is placed inline (in direct communication path between source and destination), actively analysing and taking automated actions on all traffic flows that enter the network. These deeds include, more specifically:

First, an alert will be sent to the administrator (as would be seen in an IDS)

Second, ignoring potentially harmful data packets

Third, restricting access by IP address

The fourth step is to reset the connection.

Due to its position as an inline security component, IPS must function without negatively impacting network throughput. Furthermore, it has to be quick to respond since vulnerabilities might be exploited in very real time.

[2] LITERATURE REVIEW

After the development of the internet inside surveillance and monitoring systems, the notion of intrusion detection was developed in the early 1980s.

There was an overnight boost in visibility and adoption throughout the industry's security infrastructure. Several developments in IDS technology have contributed to the present state of the art in intrusion detection. James Anderson, in a document he wrote for a government agency, proposed a method based on the idea that audit trails included useful information that may be useful in tracing abuse and analysing user behaviour [16]. The advent of detection and the growing significance of audit data ultimately led to massive enhancements across all OS subsystems [16].

Both Intrusion Detection Systems and Host-Based Intrusion Detection Systems (HIDS) were first defined. With the help of Dorothy Denning and SRI International, the most recent attempt to create an intrusion detection system got underway in 1983 [17]. In the early 21st century, the intrusion detection market begins to produce income and grow. ISS created Real secure, an intrusion detection network. After evaluating the market for a year, Cisco decided that network intrusion detection was a top priority and bought Wheel Group to acquire security solutions [17]. Federal Intrusion Detection Networks, created in response to Presidential Decision Directive 63, are only one example of the government's involvement that is fueling IDS development [17].

A Java Based Network Intrusion Detection System was the topic of study by Allam Appa Rao, P.Srinivas, B. Chakravarthy, K.Marx, and P. Kiran (IDS) As more technologies become available, the frequency with which they are exploited by hackers and intruders continues to rise at a disturbing rate. Unfortunately, in today's always-online society, there's nowhere to go unseen. You may be located using a variety of means, including but not limited to domain name system (DNS) lookup, network service lookup (NSlookup), newsgroups, web site crawling, email property lookup, etc. For this study, the researchers developed and deployed an IDS that uses predefined algorithms to detect network intrusions. Since Java is used for development, JPCap is required so that users may access winpcap. Network packets are collected "live," or as they arrive at the network's interface. In order to protect computers in networks that are linked to the Internet in some way, IDS is built to give basic detection methods.

Research on "INTRUSION DETECTION SYSTEM - A STUDY" was conducted by Dr. S.Vijayarani1 and Ms. Maria Sylviaa.S.To detect intrusions into a network or computer system, an Intrusion Detection System (IDS) may keep tabs on system or network activity. The exponential expansion and widespread use of the internet has prompted new questions regarding the security of digital data transmissions. These days, hackers use a wide variety of techniques to get sensitive data. In order to identify these intrusions, several different methodologies, algorithms, and procedures exist. The primary goal of this article is to present an in-depth analysis of intrusion detection, including its definition, history, life cycle, various intrusion detection methods, attacks, toolkits, problems, and applications.

[3] TYPES OF INTRUSION DETECTION SYSTEM

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 04 | October - December 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in
Peer Reviewed and Refereed Journal

"There are many types of IDS technologies based on the type of events that they monitor and the ways in which they are deployed. Here in this document we discuss the following four types

1. Network Based IDS
2. Wireless IDS
3. Network Behavior Anomaly Detection
4. Host Based IDS

1 NETWORK BASED IDS

Network based IDS (NIDS) monitors' network traffic for a particular network segment and analyses the network and application protocol activity to identify suspicious activity. It is most commonly deployed at a boundary between networks such as in routers, firewalls, virtual private networks etc.

2 WIRELESS IDS

A wireless local area network (WLAN) IDS is similar to NIDS in that it can analyse network traffic. However, it will also analyse wireless-specific traffic, including scanning for external users trying to connect to access points (AP), rogue APs, users outside the physical area of the company, and WLAN IDSs built into APs. As networks increasingly support wireless technologies at various points of a topology, WLAN IDS will play larger roles in security..

3 NETWORK BEHAVIOR ANOMALY DETECTION

Network behavior anomaly detection (NBAD) views traffic on network segments to determine if anomalies exist in the amount or type of traffic. Segments that usually see very little traffic or segments that see only a particular type of traffic may transform the amount or type of traffic if an unwanted event occurs. NBAD requires several sensors to create a good snapshot of a network and requires benchmarking and base lining to determine the nominal amount of a segment's traffic

4 HOST BASED IDS

In Host-based IDS (HIDS) technology, software agents are installed on each of the computer hosts of the network to monitor the events occurring within that host only. HIDS analyze network traffic and system-specific settings such as software calls, local security policy, local log audits, and more. It performs log analysis, file

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 04 | October - December 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in
Peer Reviewed and Refereed Journal

integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. HIDS are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

[4] IDS WORKING

1) Establishment of Network

Local area network. Each node is connected neighboring node. This is independently deployed in network area. & also deploy each port no is authorized in a node.

2) Packet Creation

Sender module would select multimedia file. & selected data would be converted into fixed size of packets. Then packet would be send from source to detector.

3) Find authorized & un authorized port

The intrusion detection is defined as a mechanism for a WSN to detect existence of inappropriate, incorrect, or anomalous moving attackers. Checking would be done whether path is authorized or unauthorized. If route is authorized data packet of multimedia file is send to valid destination. Otherwise packet would be deleted".

[5] SCOPE OF RESEARCH

Finding reliable data sources and labelling their output as reliable, Allowing only trustworthy data to create semantically important sections of queries, including SQL keywords and operators, via the use of dynamic tainting during runtime. This strategy is based on positive tainting, which explicitly identifies trustworthy data in a programme, as opposed to prior techniques based on dynamic tainting. There are real-world benefits to using this method rather using other approaches, many of which need for very specialised and complicated runtime settings. It has a minimal execution overhead and is specified at the application level without modifying the runtime system.

REFERENCE

[1] Corinne Lawrence- "IPS – Future of Intrusion Detection"- University of Auckland - 26th October 2004.

[2] Karthikeyan .K.R & A. Indra- "Intrusion Detection Tools & Techniques a Survey"

[3] Anita K. Jones & Robert S. Sielken –"Computer System Intrusion Detection A Survey "International Journal of Computer Theory & Engineering, Vol.2, No.6, December, 2010

[4] Vera Marinova-Boncheva-"A Short Survey of Intrusion Detection Systems"-. Bulgarian academy of sciences.

[5] Carl Endorf, Eugene Schultz, Jim Mellander "Intrusion detection & prevention" by Written-published by McGraw-Hill.

[6] "Top 125 Network Security Tools"- SecTools.Org- http://sectools.org/tag/ids/sec

[7] PeymanKabiri & Ali A.Ghorbani-"Research on Intrusion Detection & Response Survey"-International Journal of Network Security, Vol.1, No.2, PP.84–102, Sep. 2005

[8] Christopher Low –"Understanding Wireless attacks &detection "-GIAC Security Essentials Certification (GSEC) Practical Assignment 13 April 2005 -SANS Institute InfoSec Reading Room.

[9] Bace, Rebecca-"An Introduction to Intrusion Detection &Assessment"- Infidel, Inc. for ICSA, Inc.