ISSN:2320-0790

An International Journal of Advanced Computer Technology

Analysis of an Integrated Security System using Real time Network Packets Scrutiny

K. Umamageswari[1], L. Thiyagarajan[2], K.P. Suresh Kumar[3]

[1] Student, Research Department of Computer Science,
[2]Head of the Department, Research Department of Computer Science,
[3]Head of the Department, Department of Computer Applications.
[1,2,3]Indo – American College, Thiruvalluvar University, Vellore -632115, Tamilnadu, India

Abstract: With the tremendous growth of internet services, websites are becoming indispensable and common source through which they are made accessible to all. Intrusion by worms or viruses through the network is continuously increasing and evolving. Firewall and intrusion detection and prevention subsystem, and its functionality is becoming more advanced for the security system against external attacks that use various security vulnerabilities. As such, enterprises are investing in various measures for an integrated security system to identify the threats of network security-based security vulnerabilities and cope with theme effectively. In sum, the network visibility plane should facilitate the following changes in network monitoring for the purposes of promoting disaggregation of analytics tool functions for long term monitoring sustainability and flexibility. In this work, the network packet in-depth test-based, integrated security system that analyzes the threat factors through an overall study of network packets dispersed in real-time and applies various protection functions to manage with integrated security threats in the future.

Keywords: Real – time Network Packet, Deep Packet Inspection (DPI), Advanced Persistent Threats (APT), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Open System Interconnection (OSI) model

I. INTRODUCTION

With the recent advancement in information communication technology, the need for secure networks using integrated security system methods because intrusion by worms or viruses through the network is continuously increasing and evolving has increased rapidly. Moreover, incidents such as leak of high volume of personal information and large-scale system faults caused by external hacking often occur. Although firewalls block attempts at unauthorized intrusion, they only inspect the headers of the packets; thus, they are still vulnerable to attacks through the authenticated IP and open ports.

Intrusion detection on the network layer involves monitoring various network services and finding abnormal service or behaviors by monitoring the IP packets of the service or sessions as the connections between the terminals. In the former, the system can monitor and analyze a packet to determine which malicious contents it has and which known attack patterns it contains, since communication is established through packet exchanges between an origin and a destination. Such monitoring of packets is widely applied in traditional security systems and network analysis system such as IDS (Intrusion Detection System) and IPS (Intrusion Prevention System). Since it must inspect all packets in the network, however, it generates high overhead in the analysis system and has difficulties in detecting unknown attack patterns. To address such problem, the system applies deep packet inspection (DPI) technology to inspect the packet in depth in terms of contents. The task that takes the most time in a network-based security system such as firewall or IPS is pattern matching inspection, which compares the packets with a set of pattern rules. The method of comparing the port, IP address, and type of pattern used only in the existing security system to evaluate harmfulness is not suitable under the large-capacity, intelligent, and advanced persistent threat (APT) environment. Therefore, this paper seeks to discuss the concept and functions of an integrated security system based on real-time network packet deep inspection to cope with possible hacking and security threats in cyber space.

II. PROPOSED WORK

The objective of this thesis is to determine the feasibility of implementing integrated security systems that can simultaneously address process control, safety and security complicate things more. These complex integrated systems simplify plant operations and reduce on-going system maintenance costs. The security system against external attacks that use various security vulnerabilities consists of firewall and intrusion detection and prevention subsystem, and its functionality is becoming more advanced. As such, enterprises are investing in various measures for an integrated security system to identify the threats of network security-based security vulnerabilities and cope with theme

effectively. IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) must inspect all packets in the network; however, it generates high overhead in the analysis system and has difficulties in detecting unknown attack patterns. Identify the threats and risks with a generic integrated security system with respect to cyber security. It should analyze the applicable security standards and guidelines on the market to find out how well they match the need of integrated security systems. Construct a generic hardening architecture to increase the cyber security of integrated security systems. The architecture should comply with the analyzed standards as close as possible.

III. INTEGRATED SECURITY SYSTEM

An analysis of threats and potential vulnerabilities that might affect an integrated security system will be performed. The analysis will be performed at each tier in the security design, that is: threats against the system perimeter, attacks from the internal network and attacks against towards the applications and their hosts. Each single, specific, detailed threat will not be covered, but instead the focus is to include all major different forms of it-security threats against an integrated security system from a top down view.

An integrated security system can be attacked with a lot of different approaches. The complexity increases as more users connect to the system. There is the alarm central, office computers, VPN to remote offices computers, edge devices, modem connections and internal threats. Before starting to analyze the threats and risks that are specific to integrated security systems, then one must understand the very nature in which they exists. Physical security systems, especially modern, ip-based, integrated security systems, reside in many domains.

A. *Intelligent Security*

Intelligent security refers to the next-generation security information analysis technology that improves security intelligence by analyzing the correlation between the data and security events generated by the network, system, and application system of the main IT systems to cope with unknown fatal attacks such as APT.

Existing security methods have shown limitations against the subtler, more precise cyber-attacks under the rapidly changing IT environment; hence the importance of detecting subtle attacks by understanding the correlations instead of simply blocking a threat factor. Intelligent security as defined by the Gartner Group is the concept and methodology enabling the interaction of various security technologies. It pertains to the context-based analysis technology that integrates data from various sources and has interrelationship. From the short-term perspective, it is expressed in the form of context-aware security and is considered the leading security technology for the next decade.

Therefore, it is expected to overcome the limitations of the pattern-based attack control technique utilized by existing security systems and evolve into a technology that detects new unknown attacks by analyzing the correlation of various elements (system process, activity level, network transaction, *etc.*,). Studies are actively being conducted on the integrated security system technology utilizing security event information management technology integrating the network and system security products group to defend against targeted attacks and big data processing technology.

B. *Network Packet Structure and Type of test*

Network packets and IP (Internet Protocol) network, which is the smallest unit, are transferred or routed. Computer communications links that do not support packets, such as traditional point-to-point telecommunications links, simply transmit data as a bit stream. When data is formatted into packets, the bandwidth of the communication medium can be better shared among users than if the network were circuit switched.

A network packet is mainly divided into header and payload. The control information provides data the network needs to deliver the user data, for example: source and destination network addresses, error detection codes, and sequencing information. Data are partitioned, encrypted, compressed, and packed before they are transmitted and subsequently unpacked, decrypted, and reassembled following their transmission. Such process is deployed by a reference model generally called OSI (Open System Interconnection) layer. In the OSI layer and packet architecture, headers occupy 1 ~ 4 layers, but the payload occupies layer 5 or higher. The network equipment generally includes the switch hub, firewall, router, and server. The functions of each network device are performed in OSI layers 1 ~7. As shown in Figure 1, a switch hub processes the MAC header, whereas the firewall decomposes and processes 4 layers including the IP header.

The network packet inspection type is generally categorized by how many network layers are inspected. **3-level packet** inspection is divided into shallow packet inspection (or stateful packet inspection, SPI), medium packet inspection (MPI), and deep packet inspection (DPI).

Figure 1. OSI 7 Layers and Packet Inspection Level

SPI inspects the header data and drops the packet if the data are included in the blacklist. In other words, SPI cannot read the session, presentation, and application layers; consequently, it cannot inspect the payload part of the packet. Since it evaluates the packet using only the header data, SPI cannot thoroughly analyze (especially inference of the application) the traffic but can process high-volume traffic very fast compared to DPI.

MPI means the application proxies because it does not retrieve the data directly from the PC but passes it through a temporary storage unit called proxy. When a packet is inputted into a proxy system, the proxy system checks the packet header in accordance with the parse list. An application proxy is aligned with the network routing devices so that network administrators can apply the predefined rule across-the-board by having all traffic pass through the proxy system. To decide whether a packet will be transmitted, the blacklist of SPI only considers the IP address, whereas the parse list of MPI decides based on the data format type and Internet address.

A **DPI** system stores hundreds of thousands of packets in the memory until there is sufficient information to match the already identified packet type. When a new packet is matched to the identified packet list, the system recognizes which application created the packet and applies the rule to decide whether the packet will be transmitted. It can be used in a large-scale network environment since it is designed to process hundreds of thousands of packets and determine which program generates which packets in a second. If the DPI system cannot identify the application even after inspecting the packet header and payload parts, it checks the pattern to find out how the packet is exchanged between the computers. To address the limitations of Packet-Filtering, Application Proxy, and Stateful Inspection, a technology known as Deep Packet Inspection (DPI) was developed. DPI operates at L3-7 of the OSI model. DPI engines parse the entire IP packet, and make forwarding decisions by means of a rule-based logic that is based upon signature or regular expression matching. That is, they compare the data within a packet payload to a database of predefined attack signatures (a string of bytes).

Deep packet inspection (DPI) is an advanced method of packet filtering that functions at the Application layer of the OSI (Open Systems Interconnection) reference model. The use of DPI makes it possible to find, identify, classify, reroute or block packets with specific data or code payloads that conventional packet filtering, which examines only packet headers, cannot detect. Analysis of packet headers can be done economically since the locations of packet header fields are restricted by protocol standards. However, the payload contents are, for the most part, unconstrained. Therefore, searching through the payload for multiple string patterns within the DataStream is a computationally expensive task.

DPI technology can be effective against buffer overflow attacks, denial of service (DoS) attacks, sophisticated intrusions, and a small percentage of worms that fit within a single packet. Promising approaches to these problems include a software-based approach (Snort implementing the Boyer-Moore algorithm), and a hardware-based approach (FPGA's running a Bloom filter algorithm). First, the DPI technology has evolved to analyze Internet traffic in real-time and process them differentially. Second, many different functions can be supported by a system. As such, it can be used for various purposes such as security, traffic management, blocking of malicious contents, and customized advertising. Real-time DPI -- wherein security devices such as router and switch read and analyze in real-time not only the packet header but also the payload part containing the data contents of the OSI 7 layer-based packet as shown in Figure 1 indicates two attributes. Therefore, real-time total inspection of network packets must use DPI to inspect even the payload part in the 7-layer architecture. DPI-based network traffic analysis enables checking of vulnerabilities, risk factors, and possibility of intrusion such as hacking by collecting network traffic pattern data and performing total inspection and analysis of the packets.

IV. CONCEPT OF INTEGRATED SECURITY SYSTEM

In today's business environment, security integrated systems services play a key role in enabling enterprise organizations to achieve targeted benchmarks and growth initiatives. An integrated security system is an information system that integrates the functions of individual security systems to enable real-time network packet inspection, analysis, vulnerability prevention, service optimization, network control, and network log recording. The network core is the trusted domain of a single organization. It includes network devices that typically only have internal (trusted) interfaces that are wholly within and controlled by a single group or administrative domain. Generally, the only packets destined to these devices should be internal control plane and management plane traffic generated by other network elements or management stations also within the same administrative domain.

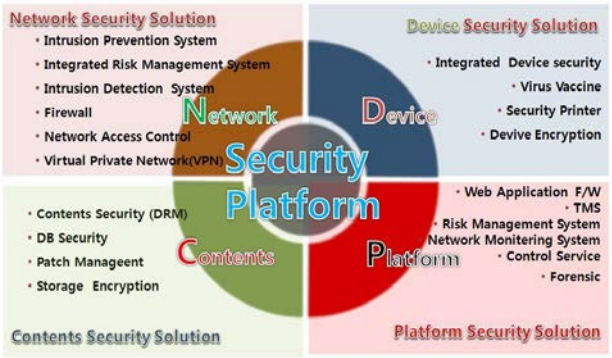

Figure 2. Features of Integrated Security System

As shown in Figure 2, a commercial security system consists of the network, device, contents, and platform to perform various functions. Network security solutions include IPS, IDSS, firewall, network access control system,

integrated risk management system, and VPN. An integrated security system is a security system integrating the security systems performing the above functions.

V. INTEGRATED SECURITY SYSTEM UTILIZATION

Integrated systems that can simultaneously address process control, safety and security complicate things more. These complex integrated systems simplify plant operations and reduce on-going system maintenance costs. Integrated security is typically achieved through a combination of unique software modules and communications media. Software makes the managed technologies of CCTV, EAC, intrusion detection systems (IDS) and communications interface within the chosen operating system. Finally, any integrated security system must be both flexible and scalable in order to accommodate existing investments in cabling and equipment.

A. *Architecture of an Integrated Security System*

The core purpose of this project is to provide a hardening architecture for integrated physical security systems from a cyber-security perspective. The architecture should attempt to provide sufficient security for usage in facilities with a high security profile. A set of standards and guidelines for cyber security in information system and digital control systems should be used as a foundation for the architecture. An analysis of the standards should be provided with respect to the various threats and risks that concern an integrated security system.

An integrated security system consists of packet signature definition, categorization, control, and authentication steps. It supports the service of each of the assorted application programs as well as the user/group, bandwidth guarantee, and authentication in real-time using the packet inspection policy, visualizes the policy, and monitors it.

Table 1. Main Functions of the Integrated Security System

Requirement	Scope
Storage/Integrated Analysis	APP-ID, User ID, etc.
App Detection	Signature-based detection
Integrated Authentication	Transmitted/Received packets and contents
Access Control	Network and contents control
Log Management	Event and log collection and utilization
Policy Control	User/Access policy
Monitoring	Real-time event

The primary role of security in the core is to protect the core, not to apply policy to mitigate transit attacks within the data plane. Such attacks should be filtered at the network edge to mitigate the risk of transit attack traffic from adversely affecting transit authorized traffic. Further, anti-spoofing protection mechanisms need to be deployed at the edge; otherwise, it is not possible to accurately verify IP source addresses, which increases the risk of IP spoofing attacks.

Nevertheless, control and management plane security policies are applied in support of the defense in depth and breadth strategy to protect the core in the event that edge policies are bypassed. Just as with the network edge, different types of IP core networks exist. The architecture should attempt to provide sufficient security for usage in facilities with a high security profile. Ultimately, network security architecture takes advantage of internal and external security intelligence to help organizations automate their network security defenses.

B. *Key Requirements of Integrated Security System*

The real-time, network packet deep inspection-based, integrated security system must inspect all network packets and their payloads without delay and in real-time and analyze and subsequently process the signature-based services quickly. It must also manage the traffic of all application program sessions passing through the system and save the traffic logs. Conservative security systems are operated mostly to prevent the intrusion of malicious codes and virus using the firewall, IDS, and IPS subsystems, however, it can neither block the attacks unless they are known malware nor quarantine the network and prevent the proliferation of damage since the network cannot be operated normally once inundated.

Moreover, since most applications communicate through dynamic ports/IP addresses, the existing security system that performs control using the port and IP address cannot handle hacking and APT attacks. As such, the real-time, network packet deep inspection-based, integrated security system requires more precise, real-time management of traffic and control of all applications and users beyond simple control using the port and IP address of the network packet. The main functions of an integrated system are listed in Table 1.The security requirements of network communication services are tailored to the special requirements of the applications and the capabilities of a network. In general, security requirements depend on the vulnerability of the communicated data. The implementation of those security requirements must match the available network services.

VI. APPLICATIONS OF INTEGRATED SECURITY SYSTEMS

The real-time, network packet deep inspection-based, integrated security system can be applied in various areas in addition to security system function, personal information protection, and security control. One of the primary benefits of the traditional firewall/IDS deployment is that the failure of one component does not leave the network completely unprotected. Deploying devices with separate functionality also prevents being locked in to a single vendor. Additionally, IDS appliances can be deployed throughout the LAN and can monitor internal traffic as opposed to boundary areas between networks.

Figure 3 Various Areas Where the Integrated Security System can be utilized

It can manage network traffic, and it can be utilized in system tracking tasks such as packet-based billing solution and network load measurement and management by analyzing the log with the following points:

- *Help Ensure Performance for Mission-Critical Applications*
- *Provide Rapid Protection against Malicious Attacks*
- *Improve Web Response*
- *Improve Multi service Performance*
- *Reduce WAN Expenses*

Automated remediation activities like these can lead to continuous improvement in network security controls and help systematize security investigations for more rapid response with the points observed here:

- *Identify the threats and risks with a generic integrated security system with respect to cyber security.*
- *Analyze applicable security standards and guidelines on the market to find out how well they match the need of integrated security systems.*
- *Construct a generic hardening architecture to increase the cyber security of integrated security systems.*
- *The architecture should comply with the analyzed standards as close as possible.*

VII. OPERATIONAL CASES AND PERFORMANCE EVALUATION

In this chapter, we are going to discuss about the certain operations and performance evaluations of the integrated security for network packets with deep inspection. To evaluate objectively the performance of the integrated security system, the instrument conforming to the network performance test standard RFC2544 (Methodology for Network Interconnect Devices) and Smart Flow software were used. For our security analysis we rely on techniques from data and control flow analysis.

Using DPI, communications service providers can allocate available resources to streamline traffic flow. For example, a message tagged as high priority can be routed to its destination ahead of less important or low-priority messages or packets involved in casual Internet browsing. DPI can also be used for throttled data transfer to prevent P2P (peer-to-peer) abuse, improving network performance for most subscribers. The security implications of DPI are widespread because the technology makes it possible to identify the originator or recipient of content containing specific packets, a capability that has sparked concern among advocates of online privacy.

Table 2. Result of Integrated Security System Evaluation

Tested Item	Test Result
RFC 2544Test	128 Byte: 99.7% 256 Byte: 99.4% 512 Byte: 99.3% 1024 Byte: 99.4% 1280 Byte: 99.2% 1518 Byte: 99.1%
Service Recognition Test	Service recognition rate of actual traffic: Around 87%
No. of Flows Processed simultaneously	30 million flows
New Flows per Second	1.5 million flows/sec.
Latency	FPGA processing: 3 Host processing: 160 ~ 180

DPI has at least three significant limitations. First, it can create new vulnerabilities as well as protect against existing ones. While effective against buffer overflow attacks, denial of service attacks and certain types of malware, DPI can also be exploited to facilitate attacks in those same categories. Second, DPI adds to the complexity and unwieldy nature of existing firewalls and other security-related software. DPI requires its own periodic updates and revisions to remain optimally effective. Third, DPI can reduce computer speed

because it increases the burden on the processor. DPI appliances can introduce their own native vulnerabilities as a consequence of their mechanisms of action. To resolve this, new programmable ASICS coupled with efficient algorithms can realistically parse the entire contents of each packet at gigabit speeds. Also, combining Firewall and IDS within a single device should simplify device configuration and management.

The performance evaluation indicates that the system can process at least 99% without delay using the existing network equipment. Neither were there performance degradation or delay, new flows/sec., *etc.*, in the high-volume network environment. These are analysis techniques that automatically compute information about the entire behavior of a software system including its behavior when the systems are under attack. In more detail, the analysis techniques work by finding conservative over approximations to system behavior. With regards to security, this means that the analysis can guarantee the absence of attacks because they provide information about the entire behavior of a system.

VIII. CONCLUSION

The aim of this paper to study and confirm that the network packet deep inspection-based, integrated security system, which can effectively handle with a variety of security threats by identifying and authenticating 7 layers of Internet traffic, can be applied without congestion the network traffic. The possibility of sharing information through networking has been growing in geometrical progression. As indicated by the recent security issues and intrusion cases, APT attacks and worm and hacking must be dealt with continuously with more advanced techniques.

An IDS identifies potential attacks within the network traffic by monitoring and identifying malicious traffic and generating alarms for each threat. The IDS watches the traffic within the network, looking for protocol and traffic anomalies, known signatures and other identifiers of malicious traffic. Intrusion prevention systems operate within the data stream and can act on security threats to thwart attacks by stopping malicious traffic that may be present. The real-time, network packet deep inspection-based, integrated security system proposed in this paper can be used as an effective security measure based on the policy of the enterprise operating the information system and understanding of the administrator. . But there are concerns as well as to include even more advanced application classification techniques such as Surgical Pattern Matching, Conversation Semantics, Deep Protocol Dissection, Behavioral and Statistical Analysis, Future Flow, Awareness and Flow Association.

For future studies, intelligent security analysis using big data techniques are used and this progress in capture, mediation, and delivery of packets hints at how monitoring can further leverage macro trends in the larger IT space and modernize network management.

IX. REFERENCES

[1] Mohit Shrivastava and Chaitra, Dr. Rajashree Shettar, Proceedings of the International Conference , “Computational Systems for Health & Sustainability” A Novel Packet Classification technique for VoIP candidature in Deep Packet Inspection, April, 2015 - by R.V.College of Engineering, Bangalore, Karnataka, India.

[2] Kiril Stoichev, “The need for establishment of professor for designer of Integrated Security Management System”, Institute of Metal Science, Equipment and Technologies with Hydro aerodynamics Centre, Bulgarian Academy of Sciences, Sofia, Bulgaria International Journal of Economics, Commerce and Management United Kingdom, May 2015 .

[3] Jackson, William. "Force multiplier: PSIM leverages video surveillance networks in Baltimore". *GCN*. 1105 Public Sector Media Group. Retrieved 24 April 2014.

[4] "Physical Security Information Management (PSIM) Market in the APAC Region 2014-2018". *Technavio*. Infinti Research Limited. Retrieved 21 May 2014.

[5] "Atlanta Operation Shield". *Atlanta Police Foundation*. Atlanta Police Foundation. Retrieved 24 April 2014.

[6] Craighead, Geoffrey. "Special Report: Government Security - Sharing Video with Police". *SecurityInfoWatch.com*. Cygnus Business Media. Retrieved 24 April 2014.

[7] "Frost & Sullivan: Compliance to Standard Operating Procedures will Fuel Uptake of PSIM Software". *Frost & Sullivan*. Frost & Sullivan. Retrieved 24 April 2014.

[8] Bremner, Paul. "PSIM software continues to see strong growth despite increased competition". *IHS Technology*. IHS Technology. Retrieved 21 May 2014.

[9] "Global Physical Security Market is Expected to Reach USD 125.03 Billion in 2019: Transparency Market Research". *Transparency Market Research*. Transparency Market Research (TMR). Retrieved 24 April 2014.

[10] M. Nicolett and K. M. Kavanagh, “Magic Quadrant for Security Information and Event Management,” Gartner Group, (2012) May.

[11] Allot Communications (2007). “Digging Deeper Into Deep Packet Inspection(DPI).” H. Asghari, M. van Eeten and M. Mueller, “Unraveling the Economic and Political Drivers of Deep Packet Inspection”, GigaNet 7th Annual Symposium, (2012) Novmber 5.

[12] BEREC, “BEREC response to EC questionnaire on specific aspects of transparency, traffic management and switching in an Open Internet”, (2012).

[13] Jeong Beom Kim Professor, “A Study on the Development of Next Generation Intelligent Integrated Security Management Model using Big Data Technology” on International Journal of Security and Its Applications, Industry-Academic Cooperation Foundation, Namseoul University), Vol. 9, No. 6 (2015), pp. 217-226.