ISSN No. 0976-5697

Volume 2, No. 2, Mar-Apr 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Ideological Network Security System through Firewall

Mr. Vijay K. Kale*
Department of Comp –Sc & IT, MGM'S Dr. G.Y.P
Aurangabad, India
Vijaykale1685@gmail.com

Dr. V. P. Pawar
Director Siddhant Institute Of Computer Applications,
Pune, India
drvrushsen_pawar@rediffmail.com

Prof. Dinesh Chandra Jain
Department of Computer Science & Engineering,
SVITS- Indore, India
dineshwebsys@gmail.com

Abstract: The expansion of the Internet and the number of sensitive applications that require strong security shadow a growth in demand for security management capabilities. As electronic commerce, secure messaging and firewall applications proliferate, management applications will be needed to limit administrative burdens while also allowing greater flexibility and control of security operations. Before an effective security system capability can be developed and demonstrated, there are a few prerequisites.

Keyword: *HTTP, SNMP, VPN, firewall*

I. INTRODUCTION

General security solutions try to establish perimeters or layers of protection to filter what data passes in or out. Multiple layers and access points make robust network security systems a natural example of distributed operations in both implementation and management aspects. The level of threat to the resources and data within a system makes active management of security capabilities an Important distributed operations mission. Computer security has been of interest since the first multi-user systems[1]. Only recently, since vital data and critical business functions moved onto networked systems, have network security mechanisms proliferated.

User expectations of system quality, privacy, performance, and reliability are growing. The complexity and interdependent nature of network security demands an up to-date system view and the capability to gather and correlate underlying event details.

A security program depends on the correctness, completeness, and reliability of three related components – security policy, implementation mechanisms, and assurance measures. Our goal is to promote a better Understanding of the issues and approaches to integrated, consistent security management [2]. Develops the foundation for a security concept using common security attributes, extension of the network infrastructure to encompass security management, and core challenges to a more robust security management environment as shown in following fig.1.

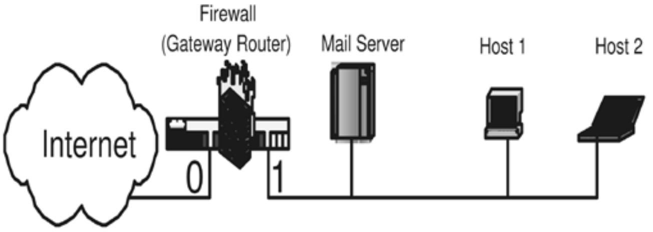

Figure 1.Firewall connection

Serving as the first line of defense against malicious attacks and unauthorized traffic, firewalls are crucial elements in securing the private networks of most businesses, institutions, and even home networks. A firewall is placed at the point of entry between a private network and the outside internet so that all incoming and outgoing packets have to pass through it. A packet can be viewed as a tuple with a finite number of fields; examples of these fields are source/destination IP address, source/destination port number, and protocol type. A firewall maps each incoming and outgoing packet to a decision according to its policy (i.e., configuration).

The policy of a firewall is the most important component in achieving the security and functionality of the firewall However, most firewalls on the Internet are poorly configured, as witnessed by the success of worms2 and viruses like Blaster and Sapphire which could be easily blocked by a well-configured firewall. It has been observed that most firewall security breaches are caused by configuration errors an error in a firewall policy means that some.

II. PROBLEM OF STATEMENT

The objective of the research is to develop secure infrastructure needs improvement to handle complex city, variety and quantity of new security applications.

III. SIGNIFICANCE OF STUDY

The Network system use in computer networking the available products related to management of security application is quite sparse. Despite vendor hype, tools for secure applications are limited in capabilities and generality [3]. Although a few firewall vendors have used SNMP identify security alarms to a network management station, most security research has focused on techniques and data analysis. Intrusion detection, multicast Conferencing and web (HTTP) security have received some attention, but no security MIBs neither exist nor are integrated security functions in wide use.

Firewalls are crucial elements in network security, and have been widely deployed in most businesses and institutions for securing private networks. The function of a firewall is to examine each incoming and outgoing packet and decide whether to accept or to discard the packet based on its policy. Due to the lack of tools for analyzing firewall policies, most firewalls on the Internet have been plagued with policy errors. A firewall policy error either creates security holes that will allow malicious traffic to sneak into a private network or blocks legitimate traffic and disrupts normal business processes, which in turn could lead to irreparable, if not tragic, consequences. Because a firewall may have a large number of rules and the rules often conflict, understanding and analyzing the function of a firewall has been known to be notoriously difficult. An effective way to assist firewall administrators to understand and analyze the function of their firewalls is by issuing queries. An example of a firewall query is “Which computers in the private network can receive packets from a known malicious host in the outside Internet?” Two problems need to be solved in order to make firewall queries practically useful: how to describe a firewall query and how to process a firewall query. In this paper, we first introduce a simple and effective SQL-like query language, called the Structured Firewall Query Language (SFQL), for describing firewall queries. Second, we give a theorem, called the Firewall Query Theorem, as the foundation for developing firewall Query processing algorithms. Third, we present an efficient firewall query processing algorithm, which uses decision diagrams as its core data structure. Fourth, we propose methods for optimizing firewall query results. Finally, we present methods for performing the union, intersect, and minus operations on firewall query results. Our experimental results show that our firewall query processing algorithm is very efficient: it takes less than 10 milliseconds to process a query over a firewall that has up to 10,000 rules. The Researcher a number of contributions in this paper. First, went reduce a simple and effective SQL-like query language. This is called the Structured Firewall Query Language, for describing firewall queries. Second, we present a theorem, the Firewall Query Theorem, as the foundation for developing firewall query processing algorithms. Third, we present an efficient query processing algorithm that uses firewall decision diagrams as its core data structure. Our experimental results show that this query processing algorithm is very efficient. Fourth, we present methods for optimizing firewall query results. At last, we present methods for performing the union, intersect, and minus operations on firewall query results. Firewalls are the mainstay of enterprise security and the most widely adopted technology for protecting private net-works. As the quality of protection provided by firewall directly depends on the quality of its policy (i.e., configuration), ensuring the correctness of firewall policies is important and yet difficult. a firewall policy, we propose a systematic structural testing approach for firewall policies. We define structural cover-age (based on coverage criteria of rules, predicates, and clauses) on the policy under test. To achieve high structural coverage effectively, we have developed three automated packet generation techniques: the random packet generation, the one based on local constraint solving (considering individual rules locally in a policy), and the most sophisticated one based on global constraint solving (considering multiple rules globally in a policy).We have conducted an experiment on a set of real policies and a set of faulty policies to detect faults with generated packet sets. Generally, our experimental results show that a packet set with higher structural coverage has higher fault-detection capability (i.e., detecting more in-jested faults our experimental results show that a reduced packet set (maintaining the same level of structural coverage with the corresponding original packet set) maintains similar fault-detection capability with the original set. Researcher has developed a systematic structural testing approach for firewall policies. We defined three types of structural coverage for firewall policies: rule, predicate, and clause coverage criteria. Among the three proposed packet generation techniques, the global constraint solving technique often generated packet sets to achieve the highest structural coverage. Generally, our experimental results. Showed that a packet set with higher structural coverage has higher fault detection capability (i.e., detecting more injected faults). Our experimental results showed that a reduced packet set maintains similar fault-detection capability with the original set.

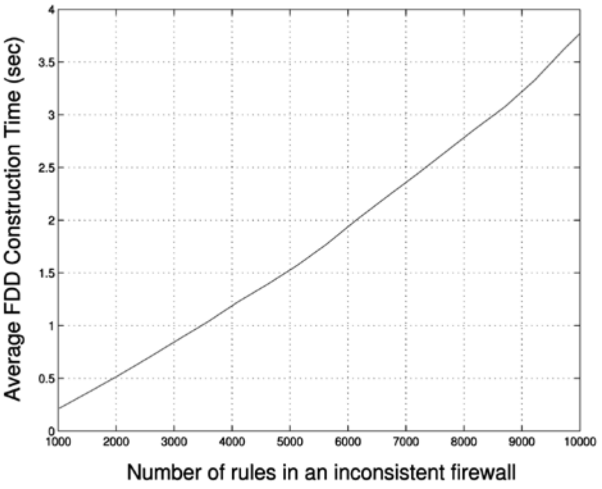

Figure: 2

The widely deployed Virtual Private Network (VPN) technology allows roaming users to build an encrypted tunnel to a VPN server, which henceforth allows roaming users to access some resources as if that computer is residing on their home organization’s network. Although the VPN technology is very useful, it imposes security threats to the remote network because their firewall does not know what traffic is flowing inside the VPN tunnel. To address this issue, we propose Guard, a framework that allows a policy owner and a request owner to collaboratively determine whether the request satisfies the policy without the policy owner knowing the request and the request owner knowing the policy. Research first present an efficient protocol, called Xhash, for oblivious comparison, which allows two parties, where each party has a number, to compare whether they have the same number, without disclosing their numbers to each other. Then, we present the V Guard framework that uses Xhash as the basic building block. The basic idea of V Guard is to first convert a firewall policy to non-overlapping numerical rules and then use Xhash to check whether a request matches a rule. Comparing with the Cross-Domain Cooperative Firewall (CDCF) framework, which represents the state-of-the art, V Guard is not only more secure but also orders of magnitude more efficient. On real-life firewall policies, for processing packets, our experimental results show that V Guard is 552 times faster than CDCF on one party and 5035 times faster than CDCF on the other party. We propose V Guard, a privacy preserving framework for collaborative enforcement of firewall policies. In terms of security, comparing with the state-of-the-art CDCF scheme, V Guard is more secure because of two major reasons. First, V Guard converts a firewall policy of an ordered list of overlapping rules to an equivalent no ordered set of non-overlapping rules, which enables rule shuffling and consequently MSU cannot identify which original rule matches the given packet. Second, V Guard obfuscates rule decisions, which prevents MSU from knowing the decision for the given packet. In terms of efficiency, comparing with the state-of-the-art CDCF scheme, V Guard is hundreds of times faster than CDCF in processing packets because of two reasons. First, V Guard uses a new oblivious compare son scheme proposed in this paper, which are three orders of magnitude faster than the commutative encryption scheme used in CDCF. Second, V Guard uses firewall decision diagrams for processing packets, which is much faster than the linear search used in CDCF. We want to emphasize that the V Guard framework can be applied to other types of security policies as well. It is also worth noting that the Xhash scheme can be used for other applications that require oblivious comparison According to recent studies, security is the biggest challenge faced by small and medium sized businesses .ever changing security thread can wreak havoc on business operation, affecting profitability and customer satisfaction .Securing it’s network is prime concern for any network administrator and security personal. Security thread may be from the insider i.e. from the trusted network users itself or may be from outsiders i.e. from ex-employees associates, and hackers.

Firewall using iptables is a powerful tool for network traffic analysis and implementation of subsequent customized security features in a Red hat LINUX operating system environment iptables as a integrated part of Linux can be configured as a formidable network security tool and one system administrator can ensure the data/ information security in his network environment. Here we have shown different flexible feature of iptables and how it can be implemented considering the site requirement. We have also shown how the whole system may be configured to implement it in the system level for automatic evocation of different firewall rules at start up time itself.

Networking is to secure the confidential data of the user from the other users .lot many thread challenging the network security system at every moment .for this region ,to increase the security for the system .this security utility failures are reported most frequently give to wrongly motive human activity or powerful threat in to system., which are more powerful than security utility. Every hacker normally hack the information of the user when the people near to them or the people knowing by them etc., but when the user sum time may enter in to harm full coding web site or install harm full software the hacker can easily identify their IP address and the user sensitive data than the hacker want to hack the sensitive information of the person.

The security of the internet interdomain routing system hinges on whether autonomous system (ASes) can trust the information them receive from each other via the border gateway protocol (BGP). Frequently ,this trust has been misguided ,resulting in wide-spread outages and significant concur about feature attacks .despite the seriousness of these problem , proposal for the more secure version of BGP have been stymied by serous impediments to practical deployment. The proposed architecture is inclemently deployable, protects against shilling attacks and deters malicious operator behavior.

As this paper hypothesizes about our reputation system potential benefited for BGP security, work will focus on implementation specifics and validation .we plan on devising efficient method to dynamically recalculate and manage large number of received votes.

IV. OBJECTIVE OF RESEARCH PAPER

The objective of the present research work is to develop real-time monitoring and control of active applications that implement one or more security services.

V. METHODOLOGY, TOOLS & TECHNIQUE TO BE USE

We define security management as the” real-time monitoring and control of active Security applications that implement one or more security services.” The purpose of security management is to ensure that the security measures are operational, in balance with current conditions with the security policy [4]. Not only must the services function correctly and in a timely fashion, they must counteract existing threats to generate justifiable confidence in the system trustworthiness. One of the largest security pitfalls is to focus on certain security products or technologies without defining a balanced security policy and thereby gaining a false sense of security. Protection is only as strong as the weakest link. Assurance is the conventional term for methods that are applied to assess and ensure a security system enforces and complies with intended security policies. One may use assurance tools before, during, or after security Mechanism operations. Post-processing of security events typically includes audit trail Analysis and related off-line intrusion detection and trend analysis methods. Many Intrusion Detection System (IDS) applications began as post-processing functions due to limited processing and software capabilities, but most are migrating toward interactive, Real-time operations Pre-operational analysis of security may involve extensive testing and the use of rigorous logical analysis referred to as formal methods[5][6]. This approach is widely applied in critical aviation, nuclear power and medical systems, as well as security kernels; to enhance reliability the need for highly reliable security systems cannot be satisfied only through design and testing, especially since protection from malicious parties is a fundamental need1. Developers for critical

A. Critical system depends somewhat on the low like hood of random conditions to cause error states, but Systems have found that reliable systems must address:
B. Fault prevention during design and development,
C. Fault detection during operations and
D. Fault recovery during abnormal or error states.

Network security management applications concentrate on the latter two areas as they relate to networks. Like security kernels, security mechanisms must properly implement security, but the assurance role typically occurs in a separate application Rather than internally. Security management tools are active assurance methods that function to monitor operational security services, allowing observation and reaction to key fault, configuration, and performance status [7]. While security kernels and security mechanisms are like automobile drivers who are ultimately responsible for safe operations, security management is like the traffic cop who reinforces the rules and assists in trouble spots. Security management has two roles–monitoring and control. The first involves data collection that provides insight for system stakeholders2 on whether security operations achieve the security policies intended by the system design [8]. Status presentation may be in the form of real-time graphical displays or periodic printed reports of data trends or exceptions. The frequency and granularity of data gathering are necessarily tradeoffs with the network traffic volume and processing load of monitoring Components. The second role of security management is to provide a means to adjust the level of security monitoring and operational safeguards if the current Level computer hackers purposely search for the weak points that exist in any complex system. 2 Stakeholders is a term meant to imply all responsible persons, beyond just the system operators and users. It may include data or business application owners or equivalent security a creditors in government organizations. Rent level does not match security policy or the desired level of risk. Traditionally, security management has been viewed as a special case of network Management. Security and management are interdependent by their nature, so each needs.

The services of the other. A security of system is a prerequisite of much high reliability and secure applications, particularly management of security. This is the so-called of security requirement. To date, much more work has been done to define security mechanisms than to extend management capabilities to security applications [9][10].

[a] The basic System Mechanisms:

a. Confidentiality and integrity
b. Data transport
c. Common data encoding
d. liveness

[b] Software:

a. Mat lab.
b. Secure mail suites.
c. Internet defense and detection
d. Internet acceleration and management server.
e. Secure Mail suite.

[c] Technique:

a. Firewall Query Theorem.
b. Firewall Detection algorithm.
c. Complexity of rule-Based Firewall Query Processing algorithm.
d. Firewall Query Algebra.

[d] Database:

a. Oracle
b. DB2
c. Ms SQL
d. Sybase
e. Informix
f. Ms-access
g. Linux Database
h. Iptable
i. Ipchain

[e] Tools:

a. Pass crackers
b. Sniffers
c. Vuln Scanners
d. Wireless
e. Exploitation
f. Packet crafters

VI. PROPOSED WORK

Through the proposed research work we are interested in security management as a test bed for exercising computational techniques in the field of Networking. With the help of Firewall. Thus the goal of this research paper is to provide the advanced network management system.

A. The Scope of the Proposed Research Work [11]:

[a] Banking Sector
[b] Mobile Technology
[c] Internet café
[d] E-Commerce
[e] Government office
[f] Military
[g] Railway station
[h] Airport

VII. CONCLUSION

A number of contributions in this paper First, we introduce a simple and effective SQL-like query language, which is called the structured Firewall Query Language, for describing firewall queries. Second, we present a theorem, the Firewall Query Theorem, as the foundation for developing firewall query processing algorithms. Third, we present an efficient query processing algorithm that uses firewall decision diagrams as its core data structure. Our experimental results show that this query processing algorithm is very efficient. Fourth, we present methods for optimizing firewall query results. At last, we present methods for performing the union, intersect, and minus operations on firewall query results.

The expansion of the Internet and the number of sensitive applications that require strong security for shadow a growth in demand for security management capabilities. As electronic commerce, secure messaging and firewall applications proliferate, management applications will be needed to limit administrative burdens while also allowing greater flexibility and control of security operations. Before an effective security system capability can be developed and demonstrated, there are a few prerequisites. First, a secure management infrastructure must be in place. SNMPv3 is poised as the secure successor to SNMPv1. Next, a security MIB must be defined to allow SET/GET operations on essential values for the security application to be managed.

This is a contentious and difficult step because of the need to map terms and status parameters from many different vendor applications and features to a small set of commonly defined values. In this paper, we have suggested a core security MIB with some general parameters applicable to all security applications. The core MIB can be extended to define configuration and status parameters for

security applications and vendor features in the same manner as other MIBs. The foundational work of defining a common core of security management infrastructure attributes and MIB definitions will allow progression to the next phase of capability development, that is, better correlation of management events with security problems. The modification of agent modules and security management applications to effectively access a common set of security values will open new management features. Innovative use of security management views and synergy with other management and security information across the network can unleash new power for security system. security applications and vendor features in the same manner as other MIBs. The foundational work of defining a common core of security management infrastructure attributes and MIB definitions will allow progression to the next phase of capability development, that is, better correlation of management events with security problems. The modification of agent modules and security management applications to effectively access a common set of security values will open new management features. Innovative use of security management views and synergy with other management and security information across the network can unleash new power for security system.

VIII. REFERENCES

[1] Firewall Policy Queries “Alex X. Liu, Member, IEEE, and Mohamed G. Gouda, Member, IEEE 2009”. IEEE transactions on parallel and distributed system, Vol. 20.

[2] S. Bahkss and M. Zaria. Dynamic Multi-path Routing and how it compares with other Dynamic Routing Algorithms for High Speed Wide Area Networks. ACM Computer Communications Review, vol. 22, no.468, 2007.

[3] Lanier Watkins, Cherita Corbett, and Raheem Beyah. “Using Link RTT to Passively Detect Unauthorized Wireless Nodes.” To appear in the International Journal of Security and, Vol. 4. Nos. 1/2, 2009.

[4] C. Gui and P. Mohapatra, "A Framework for Self-Healing and Optimizing Routing Techniques for Mobile Ad Hoc Networks,” ACM/Springer Wireless Networks (WINET),pp. 29-46, Vol. 14, Feb. 2008.

[5] “A Game-theoretic Model for Capacity-constrained Fair Bandwidth Allocation”,Intl Journal of Network Management (IJNM), Vol 18, No. 6, 2008.With Yonghe Yan, Ehab Al-Shaer

[6] “On Dynamic Optimization of Packet Matching in High Speed Firewalls”,IEEE Journal on Selected Areas in Communications (JSAC) special issue on High-SpeedNetworkSecurity:Architecture,AlgorithmsandImplementations, Vol. 24, No. 10, pp1817-1830, October 2008.Hazem Hamed, Ehab Al-Shaer,

[7] Haiping Xu, Mihir Ayachit, and Abhinay Reddyreddy, "Formal Modeling and Analysis of XML Firewall for Service-Oriented Systems," International Journal of Security and Networks, Vol. 3, No. 3, 2008, pp. 147-160.

[8] Somanath Tripathy and Sukumar Nandi, `LCASE: Lightweight Cellular Automat abased Symmetric-key Encryption`, (available online) Intl. Journal of Network Security**,** vol.8 (3), pp.243-252, 2009**.**

[9] Somanath Tripathy and Sukumar Nandi, `Secure User-identification and Key Distribution Scheme Preserving Anonymity`, Intl. Journal of security network (inderscience), vol. 3(3), pp.201-205, 2008**.**

[10] A. Wool, “The Use and Usability of Direction-Based Filtering in Firewalls,” Computers & Security, vol. 23, no. 6, pp.459-468, 2007.

[11] J. Xu and M. Singhal, “Design and Evaluation of a High-Performance ATM Firewall Switch and Its Applications,” IEEE J. Selected Areas in Comm., vol. 17, no. 6, pp.1190-1200, 2007.

Mr. Vijay Kale Recienved M.Sc.Computer Science Digree from Dept.Computer Scince & IT,Dr.Babasaheb Ambedkar Marathwada University Aurangabad (MS) India.also Presently working as Lecturer at. MGM’s Dr.G.Y.P. College of Computer science and IT, Aurangabad.

Dr.Vrushsen Pawar received MS, Ph.D.(Computer) Degree from Dept .CS & IT, Dr.B.A.M. University & PDF from ES, University of Cambridge, UK. Also Received MCA (SMU), MBA (VMU) degrees respectively. He has received prestigious fellowship from DST, UGRF (UGC), Sakaal foundation, ES London, ABC (USA) etc. He has published 90 and more research papers in reputed national international Journals & conferences.

He has recognize Ph.D Guide from University of Pune, SRTM University & Sighaniya University (India). He is senior IEEE member and other reputed society member. Currently working as a Professor & Director in SICA institute is affiliated to University of Pune, MS, India.

Prof. Dinesh Chandra Jain has completed B.E (Comp-Sc) and M.Tech (IT) degree and his Research paper published in various reputated International Journals and He is presently working as a Assistant Professor in the Department of Comp. Science & Engg. at SVITS, Indore. He is pursuing **PhD in Computer-Science**.