ISSN:0975-9646

Blocking Technique of Dataflow in Networks

B.Suneel Kumar, S.V.V.D Venu Gopal, M.Satish Kumar

ASR Engineering College,
Tanuku, W.G Dist, Andhra Pradesh.

***Abstract*— A Customized system to detect, monitor and block the data packets according to the definitions submitted to the mechanism. The mechanism is robust easy to implement, maintain, update and enhance. The mechanism takes input as sample data packets which are to be blocked and checks those definitions with the data packets according to the protocols and algorithms which are parts of the mechanism.**

***Keywords*— firewall, packet, sniffers, application layer, data stream, intrusion, detection system, network.**

I. INTRODUCTION

A network is a series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain sub networks the most common topology general configurations of networks include the bus, star, token ring, and mesh topologies. Networks can also be characterized in terms of spatial distance as Local Area Networks (LANs), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs) interrupt the communication path at the application layer and force the data [1] packets to identify themselves. Alternatively, the nodes can try to extract the information by analysing the application layer part of the communication data. Both methods have drawbacks.

The active or passive gathering of user information is not always possible.

The passive information retrieval is costly and may result in a reduction of performance. Additionally it involves a considerable implementation effort.

II. NEED FOR SYSTEM

There exists a need of a middle part between the passive and active approaches where in the applications and data packets [2] can be successfully monitored while overcoming the glitches and disadvantages prevalent in the accessible techniques and methodologies.[3] the proposed mechanism acts as bridge between the to realms there by paving way for simpler and more effective data stream blocking on network.

III. TECHNIQUES USED CURRENTLY

A. Putting Blanket Ban on Data Transfer Which is Commonly Called as Limited Connectivity

This is another of the rudimentary techniques where in the administrators stop on networks transmission to block the data streams intended to be blocked and there by hampering other transmissions as well.

B. Network Switches Closing Down Manually

This is the crudest form of prohibition of particular application or data streams from being circulated over the network several educational institutions still practice this wing to lack of awareness and initiative.

C. Employing Firewall[4]

Firewall is a system or combination of systems that enforces a boundary between networks, which is an electronic gate that limits access between networks in accordance with local security policy. There are three broad categories of firewalls.

D. Employing Network Sniffer

It is computer software or hardware that can interest and log traffic passing over a digital network or part of a network.[5] as data streams flow across the networks, the sniffer captures each packet and eventually decodes and analyses its content according to the appropriate specifications.

1) *Packet Filtering:* In packet filtering only the protocol and the address information of each packet is examined. Its contents and context are ignored. The firewall pays no attention to applications on the host or local network and it "knows" nothing about the sources of incoming data. Filtering consists of examining incoming or outgoing packets and allowing or disallowing their transmission or acceptance on the basis of a set of configurable rules, called policies.

2) *Application Level Gateway:* Application layer firewalls work on the application level of the TCP/IP stack, and may intercept all packets travelling to or from an application. They block other packets usually dropping them without acknowledgement to the sender. In principle, they can prevent all unwanted outside traffic from reaching protected machines. It does not route traffic on the network layer. All traffic stops at the firewall which may initiate its own connections if the traffic satisfies the rules.

3) *Circuit Relay:* It is a firewall approach that validates connections before allowing data to be exchanged. It doesn't simply allow or disallow packets but also determines whether the connection between both ends is valid according to configurable rules, then opens a session and permits traffic only from the allowed source and possibly only for a limited period of time. Whether a connection is valid is dependent on some/all of the following factors-destination IP address and/or port, source

IP address and/or port, time of day, protocol, user, and password.

4) *Intrusion Detection System:* It functions as a network packet sniffer which, based on comparisons of packet contents with known virus signatures or application signatures encapsulated as rules, can initiate action and record events and information related to them in a log file and/or database.

Comparison of Techniques Disadvantages

1) Network Sniffers: Leaves data susceptible to exposure. Hackers can use packet-sniffer to access information, such as a user address from the data stream and network security can be compromised.

Offers little flexibility. Creating complex access rules with packet filters can be difficult.

Offers no user-based authentication. Packet filters are restricted to denying are granting access based on source or destination addresses are ports. There is no way for a packet filter to authenticate information coming from a specific user.

Maintains no state related to communication. Packet filters make decisions based on individual packets and not on the "Context" of the traffic.

2) Packet Filtering: With packet filtering, users can connect directly from network to network. Address information in packet can potentially be falsified or "spoofed" by the sender.

The data are requests contain in allowed packets may ultimately cause unwanted things to happen. The policies (configurable rules) are through to create, maintain and update.

3) Circuit Relay: It operates at the transport layer and may require substantial modification of the programming that normally provides transport functions (e.g.: Winsock).

It is focused on sender, receiver, protocol rather than the contents of data packets being transmitted.

The connections validated as secure by it or not checked for the contents and applications originating from them.

4) Application level Gateway: Extremely slow because several processes are required to be started in order have a request serviced.

Separate programs are required to be written in order to black a certain class of data or applications.

Clients behind the firewall must be proxitized(that is, must now how to use the proxy, and be configured to do so) in order to use the services.

5) *Intrusion Detection System:* Slow because each and every data packed is checked against the rules.

Not viable in scenarios concerning real time data packet transmission.

IV. SUGGESTED MECHANISM

A. Goal

To detect, monitor and block network based applications like LAN Games, broadcasting software etc.

B. Plan

We have our target applications identified. Their sample data packets are taken to create the definition bank, which then shall be checked with the data packets to identify their status.

1) Header Check: The data packets to be checked will be inspected in two stages. The first stage will be header inspection and in the second stage the detailed contents of the packet will be matched with sample packets. Only those data packets whose header contents are doubtful get their data inspected thoroughly. Thus a two tier checking mechanism is deployed for transmission permission.

2) Freeway: If suppose there is a secured connection between two nodes and a threshold number of data packets being transmitted on that connection continuously pass the test then the subsequent packets will be exempted from checking.

3) Aging: The feature to avoid being exploited shall be modelled on the lines of process synchronization. Each data transmissions will be like a process waiting in queue. Each process wants its data packets to be checked so that the process can move forward. A process after achieving threshold number of continuous successful tests gets freeway (moved to allowed queue) but its priority here immunity decreases as the time increases and it has to come back in queue to get immunity again. Hence the principle of aging implemented with an improvised perspective.

V. ADVANTAGES OF OUR SOLUTION

A. Advantages of Features

Freeway the transmissions cleared by mechanism continue and a fair pace. Their flow is not ob structured in name of checking.

Aging this shall prevent a connection from transmitting infinitely if it clears the test once.

Header checks this generates considerable insight even by the inspection of contents of header. Thus higher throughput and speed are achieved.

B. Advantage Criterion

Accuracy our target applications have no escape route with this mechanism, as they will be matched against samples from amongst them.

Security the various strategies like masking and spoofing will fail as well against the architecture of the proposed mechanism.

Maintenance since only the sample data packets need to be fed to the mechanism for updating the definition database, it can be managed with comparative ease as compared to coded rules, regulations and protocols.

Speed in the trade off between customized mechanism with higher speed and dynamic mechanism with slower speed we have chosen the former complying with our goal.

VI. FUTURE SUGGESTIONS

The mechanism can be made customizable to provide for making the trade-off between the security level and speed dynamic in nature. In other words more security features like generating of data packets definition to be checked dynamically from the given packets, in depth searching of each packet be introduced and user having the ability to decide which of these he wishes to deploy because all of them will have their cost in terms of speed.

REFERENCES

[1] *Associating Network Flows with user and Application Information,* Ralf Ackerman, Utz Roedig, Michael Zink,Carsten Griwodz, Ralf Steinmetz, *ACM Multimedia Workshop, 2000, Marina Del Rey CA USA.*

[2] *The New Lexicon Websters Encyclopedic Dictionary of the English language. New York: Lexicon.*

[3] *Detecting Intruders on a Campus Network: Might the Threat be coming from within?* Rich Henders, Bill Opdyke, *SIGUCCS '05, November 6-9, 2005, Monterey, California, USA.*

[4] *A History and Survey of Network Firewalls,* Kenneth Ingham, Stephanie Forrest, *The University of New Mexico Computer Science Department Technical Report 2002-37. Consortium for computing sciences in colleges.*

[5] *Taxanomy of free Network sniffers for Teaching and Research,* Victor A Clincy and Nael Abu-Alaweh, *JCSC 21,1(October 2005), Midwestern Conference.*

[6] *Internet Firewalls: Frequently Asked Questions, Compiled by* Matt Curtin, Marcus Ranum and Paul Robertson.

[7] *The Evolution of Intrusion Detection Systems,* Paul Innella, *Tetrad Digital Integrity, LLC, November 16, 2001.*

[8] *While paper, Firewall software and Internet Security,2002 vicomsoft Ltd.*

[9] *Evaluation of the Firewall Industry, Cisco Documentation, Network Security.*

[10] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.*

[11] *TCP/IP Protocol suite,* Behrouz A. Forozhaun.

B. Suneel Kumar, studying M.Tech(CSE) Akula Sreeramulu Engineering College, Tanuku, West Godavari District, Andhra Pradesh.

S.V.V.D Venu Gopal (M.Tech) working as an Assistant Professor in Akula Sreeramulu Engineering College, Tanuku, West Godavari District, Andhra Pradesh.

M.Satish Kumar(M.Tech) Associate Professor working as Head of the Department in Akula Sreeramulu Engineering College, Tanuku, West Godavari District, Andhra Pradesh.