Hardware Based Total Secured Networks The Network Filter Chip

Ashish Srivastava

***Abstract*—This paper proposes a new technique for Network security. Network security has been a serious matter of concern network since the day computer network came into existence. The solution which is available in the market for network security is software level approach to secure networks but this is not a permanent solution against virus and hacking. This paper purposes a permanent solution for network security. This paper purposes a hardware level approach to prevent virus and hacking problems by focusing on the behavior of bit. As we know data travels in form of bit/byte/kilo byte/mega byte by this we can say that smallest unit of data transfer is bit so our solution for preventing the virus and hacking is that we will stop that particular bit which may cause infection to computer system, on hardware level. In such a way the computer networks can be made secured.**

***Index Terms*—Network security, NFCL, AAN, BNNC, logical port, physical port, AAR, TLH ,ULH ,NID ,NLH ,ILH, LTL.**

I. Introduction

Networks security became serious matter of concern since it came into existence. Cyber crimes caused huge loss of several organization and individuals. The biggest issue which is associated with software program is that software program needed to update at regular time period. A virusand hacking prevention technique which is being used for preventing virus is only a software approach. Each and every day a new virus and hacking technique comes into light and antivirus companies again try to find out new solution but this is not a permanent solution for hacking and virus. In this paper we have established relation between the data flow stream with the hardware level antivirus. OSI and TCP/IP models are being used in transmission. OSI and TCP/IP models both have different layers to perform task. Basically Physical layer is responsible for transmitting and receiving of all data packet. Data packet contains data but a virus may be hidden in data packets. There is no any other medium by which virus can come in computer system or networks so if virus is coming in data packet through physical layer so to prevent virus, restriction can be applied after physical layer to prevent virus. Hacking is also big problem now a day for hacking if we are able to extract the data packet on the physical layer means according to the bits stream extraction we can block the physical or logical port and we know by port actual transmission take place. In such manner the computer networks can be made secured.

Manuscript received April 18, 2012; revised June 5, 2012.

Ashish Srivastava is with the SRM University NCR Campus, Ghaziabad, India (e-mail: ashish.srivastava03@hotmail.com).

II. Problem Description

A. Computer System Security as Challenge

Computer system and computer Networks Security has been a serious matter of concern from the day computer network came into the existence .Cyber crime from all over the world caused huge loss of several organization and the individuals .Computer Network penetration occurs where any person tries to misuse of services provided by the any network .These services can't be terminated because these are those essential service without which use of network is worth so ensuring security of a network without terminating any service is a challenge .As the technology is growing new hacking technique and virus are coming into the existence.

B. Computer Network Security as Challenge

In most cases a network administrator knows that hacking their own network is the best way to ensure security of their network but he is not aware of latest exploits used by hackers or crackers, in other cases he doesn't even know how to practice hacking their own network. In such cases only three options left:

- To leave the network un-analyzed and hope that there are no security flaws in the network.
- To call an ethical hacker to analyze the network.
- Take surveillance on the network and warn against the read to the administrator as most of antivirus does.

III. Related Implementation

A. Antivirus Software

Antivirus software is most common and widely uses solution against the computer virus. Antivirus is the software level approach to prevent computer system from the virus. An antivirus program basically uses a database signature for preventing the virus. The major problem with antivirus program is that we need to update the database of the antivirus database at the regular interval to prevent the computer system from latest virus. [1]

B. Firewall

Firewall is also one of the software approaches to prevent computer system from unwanted attacks. Firewall is virtual wall between the computer system and internet. Firewall filters each data packets which are coming to the computer system and stop the suspicious data packet on the wall and let enter remaining data packet in computer system.

DOI: 10.7763/IJFCC.2012.V1.93

C. Network Security Linux Distributions

These Linux distributions contain an extensive set of Open Source network security tools and customized kernels that can be used for monitoring and discovering network flaws. This virtually can turn any PC into a network security pen-testing device without having to install any software. Even ethical hackers as a most part use these distributions as their platform for the penetration.

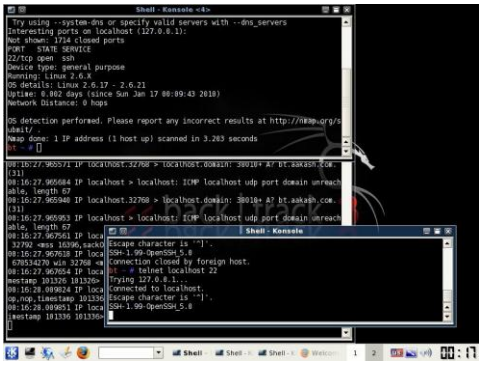

Fig. 1. Penetration testing using backtrack linux distribution.

These all require enough knowledge about the usage of various security tools provided with these distribution so they do not provide a powerful user interface and hence it can only be used by professional ethical hackers and most of them doesn't have any update procedure to define protection from exploits discovered after distribution release. [2]

D. Offline Network Security Analyzers

Offline Network Security Analyzers are tools that audit a network either from the server or from a client machine. The tool analyzes the network configurations, running services, server banners etc. These programs are efficient only when they are utilized from server machines. As another drawback, audit from these tools does not include advanced security flaws detection like MY-SQL injection, Brute force attacks etc.

IV. Proposed Solution

A. Network Filter Chip Layer (NFCL)

We have introduced a new layer "NFCL" in both models OSI and TCP/IP, as we know that TCP/IP is modified model of OSI model so both model have some same layers but architecture and working of the both model is different. We have modified the both model and made a new model NFCL models for networking.

In NFCL model, a new layer has been introduced between the data link layer and physical layer and three layer of OSI model also has been modified. Three sub layers are newly introduced in OSI model which are: NID in data link layer, NLH in network layer, AAR in transport layer. In TCP/IP model a new layer also has been introduced between the internet layer and network access layer or host to network layer and also two layer of TCP/IP model has been modified which are ILH in internet layer and AAR in transport layer. The NFCL layer has been introduced in OSI model and TCP/IP model. NFCL have also two sub layers TLH and ULH.

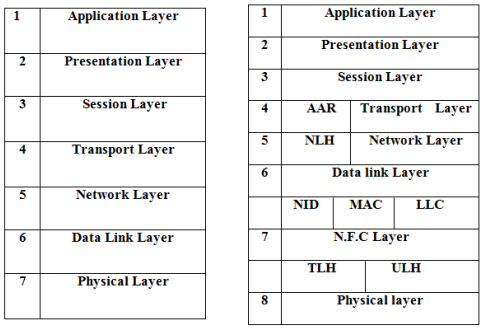

Fig. 2. Comparison of OSI model and NFCL model.

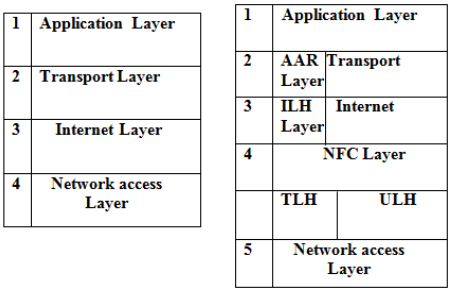

Fig. 3. Comparison of TCP/IP model and NFCL model.

B. Why Network Filter Chip Layer Has Been Introduced Between Data Link Layer and Physical Layer in OSI and in TCP/IP Between Internet Layer and Network Access Layer.

The basic reason for introducing the new layer just after the physical layer is for security reason because when any data transmission or receiving take place than data transfers or receive in form of bit/byte/kilo byte /mega byte per second so if we see the smallest form of data transmission or receiving so it is bit. Here we can conclude one thing that bit is further transforming in byte, byte in kilo byte, kilo byte in mega byte and so on. So if any virus comes into computer system than that also comes in form of bit on physical level and will further transforms in virus file in upper layer so however if we are able stop that particular bit which is may cause virus on upper level then we can prevent virus .In such a way we can prevent virus on physical level from computer system. One more reason to introduced new layer just after physical layer is that we are focusing on the bit to prevent the virus and hacking from computer system. On data link layer, if once bit converts into frame than it is almost impossible to prevent virus from on hardware level of computer system level because it is very difficult task to find out that particular bit which can form the virus in the frames.

C. Why Three Layer of OSI Model Has Been Modified and Also Why Two Layer of TCP/IP Has Been Modified.

We have introduced three more sub layer in both models. First sub layer is NID which has been added with data link layer to pass generated request by NFC layer to network layer. Second sub layer is NLH which has been added with networks layer to pass the request to the transport layer by data link layer and third and last layer is AAR which has been added with the transport layer to block the port to prevent hacking according to generated request. As we know that transport layer is the actually a software based layer so AAR embedded layer .This have full authority to block physical or logical port of computer system at any time when it senses that any particular bit which may affect our computer system.

To prevent the hacking we need to separate the data packet and requests which has been generated by TLH sub layer because on the further level the data packet and request bits may be mixed and AAR sub layer will be confused between data packet and requests bits therefore we have introduced three sub layer in OSI model to separate the request bits on each layer. In TCP/IP model due to same problem we have modified two sub layers: ILH in internet layer and AAR in transport layer.

D. Block Diagram of Network Filter Chip Layer

NFCL is a hardware level approach to prevent the virus and hacking from the computer system. The NFCL follows a certain procedure and algorithms, pattern matching for preventing the virus and hacking from the computer systems.

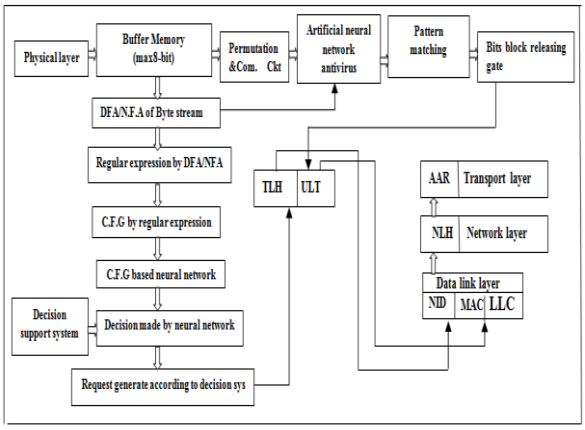

Fig. 4. Block diagram NFCL.

We have developed the NFCL in such a manner that it prevents the virus and hacking from computer system totally and makes the networks secured. NFCL has been divided in the two sub layer TLH and ULH. Both layer are being used for different works but they are interrelated for prevent the hacking and virus from systems and servers.

E. Artificial Neural Network Antivirus

Artificial neural networks antivirus is hardware level approach for preventing virus and hacking so it is designed in such a way that it do not need any database for detecting virus and if there is no database so we do not need to update or upgrade anything in hardware level neural network. This artificial neural network antivirus is only triggering the virus infection strategies to prevent the virus. [8], [9], [10] We are not making any virus signature for detecting virus only virus infection strategies are being concerned here because all viruses have been classified and each and every virus has its own infection strategies so here we are only triggering the infection strategies by artificial neural networks antivirus.

F. Pattern Matching Algorithm

Pattern matching is also important part of the NFCL because on this level by pattern matching we decide that bit may cause infection or not so we call it bit matching algorithm. The basic plan of pattern matching is to form neural networks. We know that artificial neural network has been made by the all possible combination which can be made by 8 bits. All possible combination will be search to extract the pattern by the bits which can cause virus on further stages .For avoiding confusion we will denote the digital 0 by alphabet a, and 1 by the alphabet b. Here we are taking the example of 6 bits**.** [7]

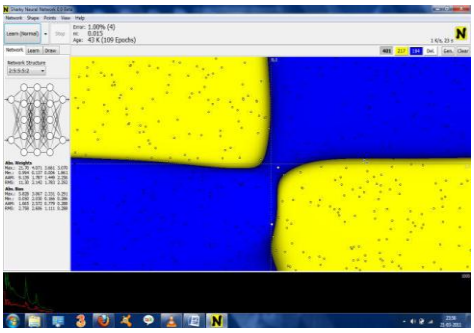

Fig. 5. A sample neural network of eight bit variables.

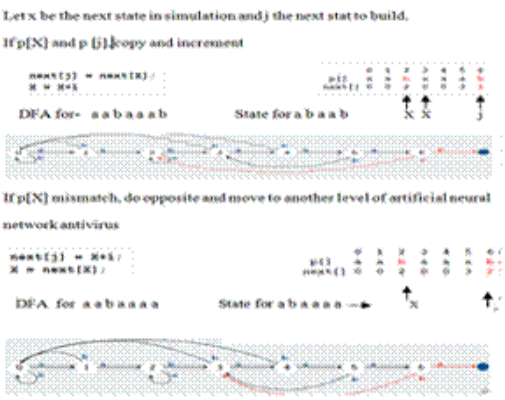

Fig. 6. Illustrating pattern matching.

- A separate state has been made for each and every bit which is participating in the process.
- Match the input bit and move to i+1 state or next level of artificial neural networks antivirus.
- If mismatching occurs than move to previous state and
  after that start finding the in other level of neural networks.
- Here we want to discuss an important point is that we are making the pattern matching on based of DFA or NFA but neural network antivirus play a very important role here because all the pattern matching done by help of neural network so each and every time pattern matching is taking place as liner but in the neural network each and every bit is matching many times on different level of neural network antivirus.
- Algorithm:

```
int j = 0;
for (int i = 0; i < N; i++)
{
   if (t.charAt(i) == p.charAt(j)) j++;   // match
   else j = next[j];                      // mismatch
   if (j == M) return i - M + 1;          // found
}
return -1;                                // not found
```

Fig. 7. A bit matching algorithm.

G. Protocols for Network Filter Chip Layer (NFCL)

Protocol (special set of rules) is used for transmitting and receiving the data from one end to another end. We have made protocols which will be used in NFCL by which TLH sub layer and ULH sub layer. So first we will discuss the protocol of ULH sub layer. NFCL work is taking place by two sub layers.

1	2	3	4	5	6	7	8
PTN	LTL v.1	LTL v.2	LTL v.3	LTL v.4	LTL v.5	LTL v.6	NTD

Fig. 8. Names of protocol by work flow of ULH.

Second sub layer is TLH sub layer which is being used for Prevent hacking.TLH have certain protocol by which process are taking place in NFC layer.

1	2	3	4	5	6	7	8	9	10	11
LTL V.2.1	LTL V.2.2	LTL V.2.3	LTL V.2.4	LTL V.2.5	LTL V.2.6	LTL V.2.7	LTL V.2.8	NTN V.2.9	NTA V.2.10	ATL V.2.11

Fig. 9. Names of protocol by work flow of TLH.

As we have mentioned that NFC layer have two sub layer.TLH sub layer and ULH sub layer.TLH sub layer to prevent hacking and ULH sub layer to prevent virus from computer system. We have also modified three layers of the OSI layer and one layer of TCP/IP model for which we have developed the special protocols which are NTN v.2.9 for NID sub layer of data link layer, NTA v.2.10 for NLH sub layer of network layer and for AAR sub layer of transport layer we have developed the ATL v.2.11 protocol.

H. How to Control the Physical or Logical Port of Computer System to Prevent Hacking.

Our solution to prevent hacking is that we will make block the port by extracting the bit stream of the data for that we have made a large procedure for converting the bits into the grammar and this grammar will be read by the neural network which will able to make decision about the physical or logical port of the computer system. For generating the request for each and every port per second is very difficult task for which are exponential function logic gate systems will be used.

As we know currently more than 65000 ports are in use for communication. So for managing the port we will use the function. As we know that 65000 port are being used for communication so If we put the value of x =11.09 than we can manage 65512 port per second by the exponential circuit.

Fig. 10. Exponential function graph.

$y = e^x$
Where y= Generated Requests
e^x=Max number of ports for which request has been generated

Fig. 11. Exponential circuit creation.

V. Usage Examples

The bits stream is coming from the physical layer to data link layer by PTN protocol.

1) The bit stream is received by buffer memory which have max limit till 8 bits by LTL v.1 protocol. On this level upcoming bits store temporary. Here the bits go for two different processes. First process is to remove the virus bit and second process is for when any suspicious kind of request detected by NFC layer than for blocking the logical or physical port of computer system so first we will discuss how we will stop that particular infected bit.
2) Once the bits are stored in the buffer memory than we make a possible permutation and combination by permutation and combination circuit. It takes place by protocol LTL v.2.
3) The possible combination of 8 bits can be arrange in 256 ways and neural network use 256 possible ways to find out that any particular block may cause virus or not in upper layers .It uses protocol LTL v.3 for find out virus by neural network or it see the behavior of the particular bit or group of bit. There may be 40320 permutation can be made by the 8 bit which are going to come into the buffer memory of NCF layer of 1 byte so large neural network is required.
4) The possible 256 arrangement of 1 byte traversing by the artificial neural network antivirus after traversing pattern matching take place by LTL v.4 protocol. The pattern matching is used for checking the 256 arrangement that which block of bit may form the virus it further stages.
5) After pattern matching the bits block releasing gate stop the particular block or groups of block which may form virus in upper layer by protocol LTL v.5 and let pass remaining block which cannot form virus on further layer.
6) The bits block releasing gate release the stream of bits For the ULH sub layer of NFC sub layer by the help of protocol LTL v.6.
7) ULH sub layer of NFCL sub layer store and pass the bit stream to the MAC sub layer of data link layer by the help of protocol NTD. Data link layer gets a virus free bits block from NFC layer and after that normal process take place of transmission or receiving.
8) 8) NFA or DFA by bit stream block represent that when buffer memory stores the 8 bit or 1 byte of the coming bit on the basis that stored bit we make a NFA or DFA. NFA or DFA will be made according to the requirement of bit stream. Where NFA is required there NFA will be used and where DFA is required DFA will be used. This process will take place by the help of LTLv.2.1.
9) Now we will discuss the how TLH work is being take palce.TLH call the protocol at each and every stages and we will see how TLH work is taking place by protocol. LTL v.2.1 is designed in such a manner that it can make the DFA and NFA for all possible combination which may be used in the neural networks for pattern matching and to form the neural networks, Fig. 12 and Fig. 13.
10) Regular expression by DFA or NFA block representthat by using this we are making the regular expression by help of protocol LTL v.2.2. This is most important level to prevent hacking because we extracting the bit stream here and now we are able to recognize by bit stream that which data packet may cause hacking or can say that which kind of request it is containing.
11) CFG by regular expression block represent we will make the grammar on the basis of the regular expression. This context free grammar is being used for to give relationsh- ip between the regular expressions and this process is taking place by protocol LTL v.2.3.LTL v.2.4 provide such feature that we are able to CFG based neural network. This block represents that we are

making the neural network of CFG but basically the neural network is being made of the bits.

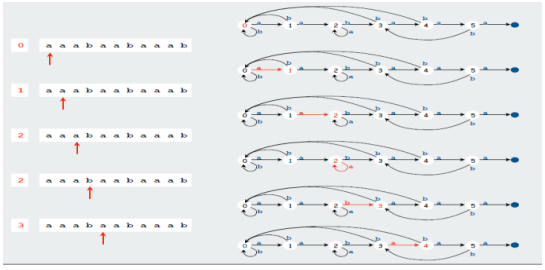

Fig. 12. Construction of DFA or NFA part [1].

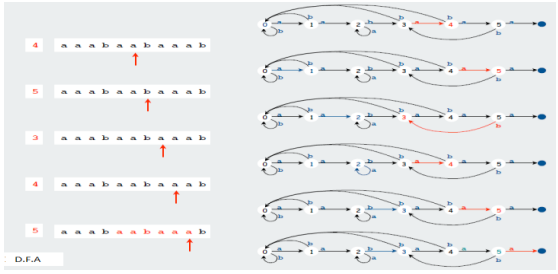

Fig. 13. Construction of DFA or NFA part [2].

12) Regular expression CFG is just helping to find out the relationships among them.
13) Decision support system and decision by neural network block works together to recognizing the data packet behavior means that how the data packet will behave on the further level and according to port blocking request will be generated for transport layer and these process is taking place by the help of protocol LTL v.2.5.
14) By the protocol LTL v.2.6 we are able to generate Request. This block represents that here request is being generated which will be accepted by transport layer to block physical or logical port.
15) TLH block will store that request and will send to the NID sub layer of data link layer by the help of LTLv.2.7 and after that all the process will take place as normal routine.
16) NID block represent that NID sub layer of data link layer will receive that request by the help of LTL v.2.8 and all process are taking place a normal routine but only difference is that which request is generated by the TLH block that will be processed separately on each and every level of data transmission or receiving.
17) NLH sub layer of network layer will receiving that request which is send by the NID sub layer of data link layer. It stores that and sends to further level this process will take place by help of NTN v.2.9 protocol.
18) AAR sub layer of transport layer is most important to prevent hacking because here is the stage where port blocking will be done on the basis of the generated request. In the initial stages all block will be block but as request will be generated according to request that port will be open or close both procedure will take place by the protocol NTA v.2.11 and ATL v.2.11 respectively.

VI. Utilities of Using Proposed Solution

This solution is hardware based solution for preventing virus and hacking so it do not need any kind of regular software update against the newly coming virus or hacking technique.

This solution will prevent the virus on the hardware level so it prevents system from any kind of software corruptions or failures. The Organization and individual do not need to concern about newly coming virus and hacking technique and to find the solution for new virus and hacking.

This hardware solution can be saved a huge amount of money which is being spent by the individuals and large organization for security purpose.

The tool doesn't require any maintenance routines as the software need to regularly update the database to trap the new virus.

NFCL can very helpful for the large servers because large servers need huge maintenance and for that big amount of money is needed .NFCL model can reduce a large amount of maintenance and money.

VII. Future Scope

Many features can be implemented based on this solution like hardware level authentication, privacy, encryption decryption, real time security scanner which scans network flaws on networks automatically within defined intervals and send the reports to network administrators.

The potential of this solution can be further enhanced by adding some more neural networks which can guide the computer system against many other attacks which take place and harmful for organization and individuals ,which will include a set of defined steps to perform an attack scenario.

The efficiency of NFCL can be enhanced by using more than module because in the paper we have demonstrated process by 1 byte buffer memory.

VIII. Conclusion

Network Security has been a serious concern from years. Unfortunately today's methods are unable to ensure complete network security. A huge data loss can be prevented by our solution which is cause by virus and hacking. Our solution provides total security to organizations and individuals from virus and hacking. We have tried our best to make understand this research paper and included many things which will help to make understand this research paper. We have given all important

Acknowledgment

There are too many people to thank. Many people have contributed in the development of this paper. I owe my deep regards and honor to express our gratitude to my parents for providing me invaluable support, guidance all through this paper.

References

[1] Antivirus programs: [Online]. Available: http://en.wikipedia.org
[2] Backtrack Linux Homepage: [Online]. Available: http://www.backtracklinux.
[3] D. Comer, *Computer Networks and Internets with Internet Applications. 3rd Edn.* Prentice Hall, Inc. 7. 2001.
[4] C. Hare and K. *Siyan, Internet Firewalls and Network Security. 2nd ed.* New Readers. Network Security. 2nd ed. New Readers.

[5] C. Scott, P. Wolfe, and M. Erwin, Virtual Private Networks. O'Reilly10
[6] E. Dorothy and Denning, *Information Warfare and Security Addisonwesley*, 1999.
[7] KMP Pattren matching alorithm [Online]. Available: http://en.wikipedia.org
[8] S. C. Lee and D. V. Heinbuch, Training a neural network-based intrusion detector to recognize novel, 2001.

Ashish Srivastava, Currently I am pursuing my B.Tech degreeindepartment of computer science and Engineering from the SRM University,NCR Campus, India. My research area is network security, Embedded system, Cryptography,Machine Learing.
Email I.D : ashish.srivastava03@hotmail.com