Comparison of Pattern Matching Techniques for Host Based Intrusion Detection System

CH. Vidyasagar[*], R. Swapna [**], B. Raju [***]

[*] Computer Science & Engineering, Kakatiya Institute of Technology and Science, Warangal, India
[**] Asst. Professor, Computer Science & Engineering, Kakatiya Institute of Technology and Science, Warangal, India
[***] Asst. Professor, Computer Science & Engineering, Kakatiya Institute of Technology and Science, Warangal, India

Abstract- This project analyzes the security status of computer network, generating of network attack graph is a hot topic in this domain. After analyzing network security attributes including the host, user privilege, connection relation, etc., the model of computer network security status space is built.

Index Terms- Network Security, Intrusion Detection

I. INTRODUCTION

The rapid growth of the network influences the economy, politics, culture and many aspects of the society. The deeper and wider the network applications is, the more obvious and more complex the computer and network's security problems are. Hackers and virus can find more ways to launch attack with the development of the network technology. The security problem of computer network is more complex. In this project we use attack graph to provide a view of network security status. This article presents a method to generate attack graph for network security analysis based on security status space. In actual implementation environment of the host computer, the system visitors can be classified according to the capability to access the system resource. A lot of researchers have described on this direction. Synthesizing the attacker's starting point and object, host information and network topology information, the graph-based description represents the threat to security of information system, and it is called an attack graph. According the definition of SSP, the SSP may be used to describe the attack graph. When the node transfers, the SS of attacker is changed. To analyze the network security, based on the analysis of network security incidents and attacker's actions, we make several assumptions. In this project we use a forward-search, breadth-first and depth-limited attack steps limited attack route producing algorithm to find the attack routes, then utilize the tools to generate attack graph. The attack route producing algorithm is described as following: From the initial network state, it finds all network states the attacker could get directly, and adds these network states into State queue, It chooses a state from State queue as Cur state, and finds all network states which could be got directly from Cur state as New states. If a state is new, then it would be added into State queue. If the State queue is empty, the algorithm finishes. When each attack depends on the previous attack on attack route, the attack route is called minimal attack route. Contrast to the method that has been previous used, our method can directly find all minimal attack routes. At the same time, in attacker's point of view, breadth-search guarantees to find all of the attack routes.

II. PREVIOUS WORK

As an important aspect of network security, evaluating the computer security through the analysis to the computer network is very important and could protect us form being hacked. Vulnerability scanning is a traditional way to conduct network security analysis. This method can check whether or not there are any known vulnerabilities. This technique is just suitable to check system security qualitatively partially but cannot check a whole system. The ways to find the complex attack paths or list which can lead to changes of the system status are presented by analyzing the security model. For example, the earliest concept of attack graph a method named Privilege Graph is developed. The other model provides for modeling chains of network exploits. Some researchers analyzed these Unix-based systems security using model-checking technique.

III. PROPOSED SYSTEM

A. Initialize Network

In actual implementation environment of the host computer, the system visitors can be classified according to the capability to access the system resource. The system Assign Privileges, Assign Roles, Assign Visitors, Compute Connection Relation, Save Connection Relation

B. Process Logs

To the attacker who attempts to exploit the target it is a process, which needs to be performed step by step. The attack can be represented by a two-tuples Attack_rule=(Preconditions, Postconditions), in which Preconditions is the preconditions set, Postconditions is corresponded results set. The preconditions set includes four elements which is represented as Preconditions={Src_privilege, Dst_privilege, Vuls, Protocols}. Src_privilege represents the lowest privilege class which attacker should have on the host where the attacks are launched. Dst_privilege represents the highest privilege class which attacker should have on the object host. Vuls represents the vulnerability which the attack rule depend on. Protocols describe the needed connection relation between the attack host and the object host. In general we Create Attack Tuple, Assign

Preconditions, Assign Post Conditions, Generate Attack Rules Create Security Status Space.

C. Generate Attacks

Synthesizing the attacker's starting point and object, host information and network topology information, the graph-based description represents the threat to security of information system, and it is called an attack graph and it can be described in the attack graph. In this module, we use nodes of attack graphs Determine Source, Determine Destination, Compute Security Space, Check for Node transfer and change in relations, Create attack Graph.

D. Analyse Attacks

In this module we use a forward-search, breadth-first and depth-limited (attack steps limited) attack route producing algorithm to find the attack routes to generate attack graph. From the initial network state, it finds all network states the attacker could get directly, and add these network states into State queue. It chooses a state from State queue as Cur state, and finds all network states which could be got directly from Cur state as New states. If a stateis new, then it would be added into State queue. When each attack depends on the previous attack on attack route, the attack route is called minimal attack route. In general we Apply forward Search, Apply Breadth First Search, Apply Depth limited Search, Find all network states, Retrieve and display Routes.

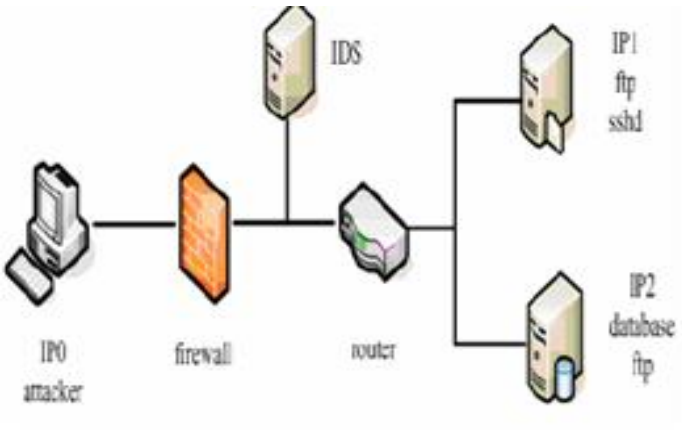

Figure 1: System Architecture

IV. RESULTS

The concept of the paper is implemented and different results are shown below

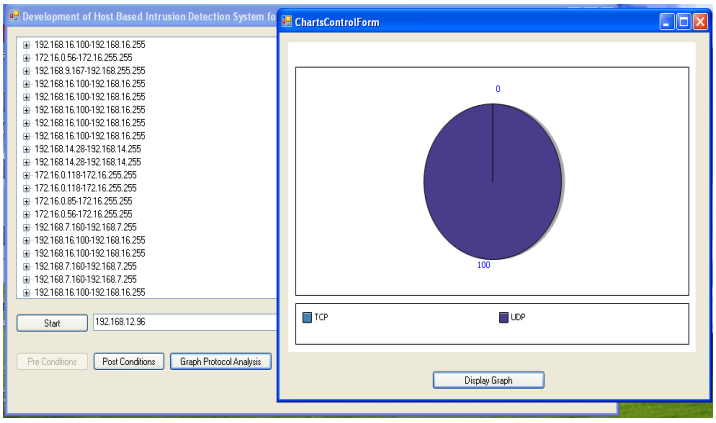

Figure 2: Protocol Analysis of captured packets

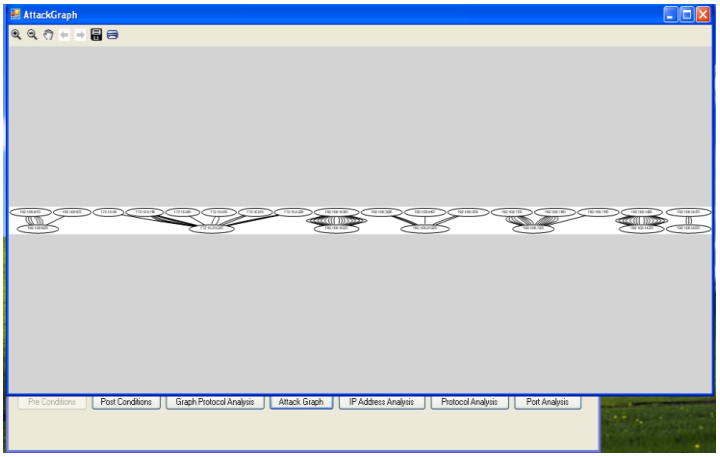

Figure 3: Detection of Intrusion System.

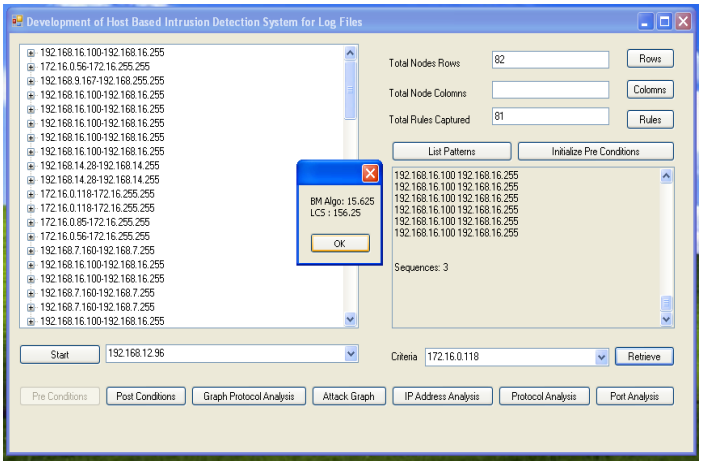

Figure 4: Comparison of Delay Time.

The Fig 6, and Fig 7 shows the real time results compared.

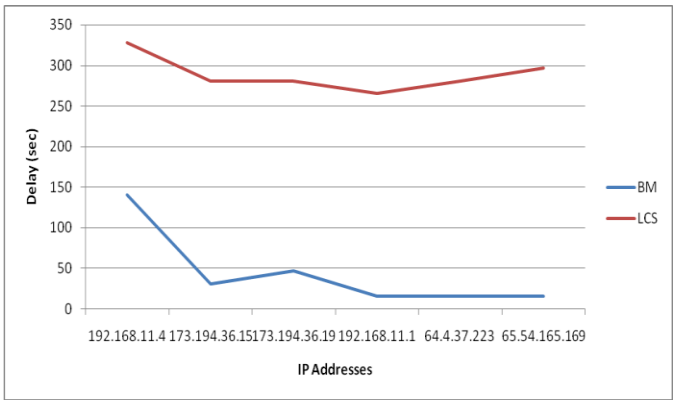

Figure 5: Proposed System Comparison

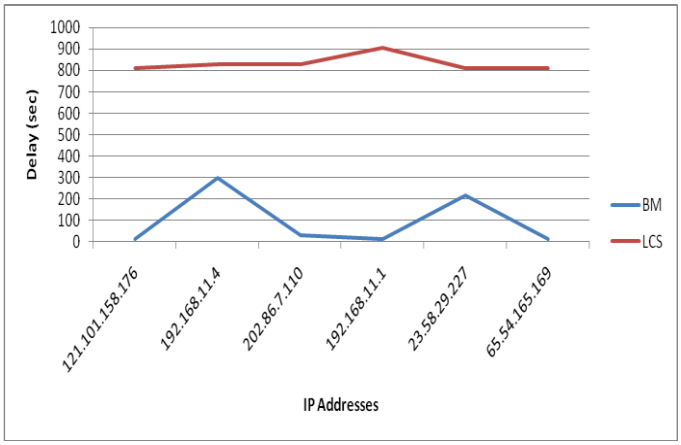

Figure 6: Proposed System Comparison

Performance Analysis

The paper has been implemented in .Net technology on a Pentium-IV PC with 20 GB hard-disk and 256 MB RAM. The proposed paper's concepts show efficient results and has been efficiently tested on different systems.

V. CONCLUSION

The tools to generate attack graph based on security status space for network security analysis are designed and implemented, and the experiment indicates the method is usable and effective. Many related research should be done in the future, the results from network scan tools should be used in the tools. The generating algorithm should be optimized and the method to analyze attack graph should be further studied.

.

REFERENCES

[1] R.Ritchey and P.Ammann, "Using model checking to analyze network vulnerabilities", In Proceedings of the IEEE Symposium on Security and Privacy, MAY 2001, pp 156-165.

[2] P.Ammann, D. Wijesekera and S. Kaushik, "Scalable, Graph-Based Network Vulnerability Analysis", In Proceedings of CCS 2002: 9th ACM Conference on Computer and Communications Security, Washington, DC, November 2002.

[3] L.Swiler, C.Philips, D.Ellis, and S.Chakerian, "Compter-Attack Graph Generation Tool", In Proceeding of the DARPA Information Survivability Conference & Exposition II, Anaheim, California, June 2001.

[4] Rodolphe Ortalo, Yves Deswarte and Affiliate, "Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security", IEEE Transactions on Software Engineering, Vol.25, Sept./Oct. 1999, pp.633-650.

[5] S. Templeton and K. Levitt, "A requires/provides model for computer attacks", In Proceedings of the New Security Paradigms Workshop, Cork, Ireland, September 2000.

AUTHORS

First Author – CH.Vidyasagar, M.Tech, Dept. of Computer Science & Engineering, Kakatiya Institute of Technology and Science, Warangal.
vidya.chikkula@gmail.com

Second Author – R.SWAPNA, M.Tech, Asst. Professor, Dept. of Computer Science & Engineering, Kakatiya Institute of Technology and Science, Warangal.
swapnarud6@yahoo.co.in

Third Author – B.RAJU, M.Tech, Asst. Professor, Dept. of Computer Science & Engineering, Kakatiya Institute of Technology and Science, Warangal.
raju.nestham@gmail.com

Correspondence Author
CH.Vidyasagar, vidya.chikkula@gmail.com, 9701683319.