DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5231

ISSN No. 0976-5697

Volume 9, No. 1, January-February 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

MULTI LAYER ADAPTIVE NETWORK SECURITY APPROACH

Mohammad Tanveer Khan,
Dept. of Computer Applications, ICSC,
University of Kashmir, Srinagar, India

Imtiyaz Ahmad Najar
Computer Programmer,
SKUAST-K Srinagar, India

***Abstract*:**. Network security refers to all the characteristics, features, measures, operational procedures, protocols , policies and practices required to monitor an unauthorized access to data and to provide an acceptable level of protection for transmission of data across the networks and at the same time preserve the, integrity , availability and confidentiality of information. Inspite of all the security products available today (mostly non-adaptive), on-going efforts and current solutions, it is known fact that security across networks and applications is not adequate. Runtime security adaptation has great potential in providing timely and fine grained security control. A multi-layer adaptive security model is an unified approach to address both the reliability of a fragile network infrastructure as well as defend against malicious attacks. This paper aims at designing a secure runtime adaptive network solution which shall provide a comprehensive set of security policies and mechanisms for creating a dynamic adaptive security solution for transmission of data across network applications and environments. The type of security addressed in this paper is specifically data privacy and 'self adaptive' implies the ability to change the security policies, procedures and mechanisms automatically at runtime through an intelligent trade off policy.

Keywords: -Adaptive security, Intrusion detection systems, Network Monitors, Packet Analyzer, Risk Assessment

I. INTRODUCTION

Traditionally, security issues are addressed by cryptographic encryption and decryption techniques implemented in upper layers of the network protocol stacks, which have inherent difficulties and vulnerabilities in secret key distribution and high computational complexity [18, 19]. A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware components. All these components work together to increase the overall security of the computer network. The study of adaptive security in computer networks is rapidly growing area of interest [10, 17]. Network security requires certain security services to be provided which include authentication, access control, data confidentiality, data integrity and non-repudiation. Adaptive network security refers to the self-managing characteristics of network resources, adapting to unpredictable changes while hiding intrinsic complexity to operators and users. Dynamic Adaptive security can watch a network for malicious traffic and behavioral anomalies, identify real-time changes to systems, automatically enforce end point protections and access rules, block malicious traffic, follow a compliance dashboard while providing audit data, and more[3].

Adaptive Security includes adaptive intrusion detection systems which allow individual trust management to conserve processor resources [17], adaptive agents where the system itself moves between different domains and has to detect and adapt to various malicious scenarios [5], adaptive security in resource constrained networks where appropriate security protocols are selected at runtime based on the current network conditions [6,7] and threats[12], adaptive security infrastructures (ASI) where the ASI consists of many security systems which cooperate to ensure minimal policy conflicts [8, 9] and many more.

There are three major types of security threats on the network: physical attacks, dialog attacks, penetration attacks. Physical attacks occur when an attacker has physical access to hardware such as computer or network infrastructure. Dialog attacks are attacks on data in transit, such as traffic analysis, message interception etc. Penetration attacks involve system breaches in order to steal information or damage the victim's system. Penetration attacks include port scanning, malware etc.

This paper addresses the concerns of system security and system performance, in particular separating these concerns at design time and addressing the contention between them with a intelligent adaptive security solution at runtime. The type of security addressed in this paper is specifically data privacy and 'adaptive' implies the ability to change the security policies and mechanisms at runtime through an intelligent trade off policy. The Adaptive Security solution presented in this paper is a dynamic tunable solution as it enables adaptation of crosscutting concerns in response to current environmental conditions. More precisely, it enables runtime security adaptation based on current server load. This is achieved through a policy based mechanism which provides better security when resources are available whilst still respecting client quality of service constraints.

II. LITERATURE REVIEW

Adaptive systems typically require additional information, not traditionally accepted as a justified concern of the system, to make adaptation decisions. Such a general view of adaptive systems leads to a research area which is vast, multidisciplinary and involves a wide range of systems [11]. A paper by Brenda Timmerman [13] which considers the issue of dynamically masking network traffic to protect against traffic analysis attacks. It allows the cross-cutting concern of security (i.e. the amount of masking) to be altered in response to changing security policies, which in turn is partly based on current system load. Higher network load might result in a policy change to reduce network masking and so free resources to deal with the increased network traffic, and vice versa. Lawrence

Teo et al. [14] describes a dynamic risk-aware access control architecture which provides additional runtime support to firewalls by monitoring the environment. It monitors client requests at runtime and makes intuitive risk based assessments on each request before allowing traffic through. Similarly R.M Venkatesan et al. [2] considers a firewall which adapts to threats by changing security policies for each user at runtime based on Intrusion Detection System (IDS) input. Kang et al. [15] also considers using IDS input in the context of real-time embedded systems to allow the system systems to allow the system to perform optimally until a real security threat occurs. Finally M.E El-Hennawy et al. [16] also tries to alleviate security processing costs through segmenting data and applying a different level of encryption to each segment by varying the algorithm key size. Lee et al. [4] proposed a system using combined misuse and anomaly detection approaches to generate rules for IDS. For improving efficiency, multiple model cost based approaches are applied. These analyze and detect models with high accuracy but low cost. A distributed architecture is proposed for evaluating models in real time. To improve usability adaptive learning algorithms are used for incremental updates. To reduce reliance on the labeled data unsupervised learning is studied.

III. PROPOSED ADAPTIVE SECURITY MODEL DESIGN

In order to design a dynamic adaptive security model the system should have the functions of real-time invasion monitoring, vulnerability scanning, protection, system security mechanism, self learning and security policy updating. Monitoring and detection mechanisms are classified in two main categories.

a) *Signature based detection*: Models built from well known attack types, i.e., from already known attack patterns.

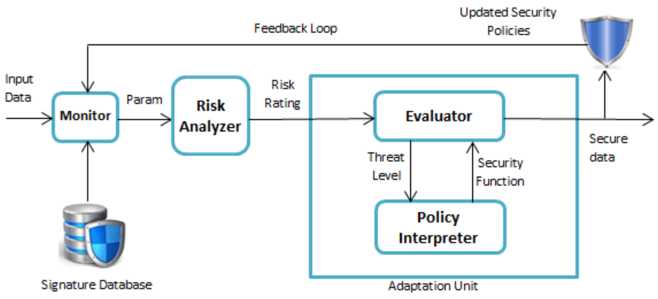
b) *Anomaly based detection*: This detection is based on heuristics or rules and any deviation from the traffic profile created during training phase is considered anomalous.

The proposed adaptive security model uses both the methods for providing maximum security across the network. The key aspect in building an adaptive security model is to decide the states and symbols that are to be used to build the model. Choosing right set of attributes for a model is very important as this step would ensure effective usage of available data. For our experiments, we use TCP header information present in packets as features.

The proposed model consists of the following components. Monitor (M), Analyzer (A) and Reflector (E) as shown in Figure 1.

3.1 Monitor

In order to detect the network intrusion the monitor will first check the signature database for the possible threat and in case of a match will raise a flag otherwise the monitor will proceed for the anomaly based detection method.



In order to detect the attack traffic, the system must be taught to recognize normal system activity.The two phases of a majority of anomaly detection systems consist of the training phase (where a profile of normal behaviors is built) and testing phase (where current traffic is compared with the profile created in the training phase)[1]. Any behavior that fall outside the predefined or accepted model of behavior generates an event. The monitor flags any traffic that deviates from clean traffic profile as suspicious. The rationale behind this method is that clean traffic and malicious traffic are not generated from the same distribution. Thus the role of monitor is to study the network environment and measures the changes in behavior of network to detect the possible intrusion. Monitor reports the changes along with threat parameters to the next component of the system, the Analyzer.

3.2 Risk Analyzer

Once the monitor detects a threat or infrequent pattern it raises a flag and passes the threat parameters and network information to the risk analyzer. Risk analyzer being the significant component of the proposed security model, it takes into consideration all network parameters and analyses the risk involved and makes a risk assessment.

Risk confirmation is mainly about identifying possible risks in network and classifying them. Risk forecast is to foresee direct losses and indirect losses when risks occur. During the process of risk assessment, value of assets, impacts of damage, seriousness of threats, possibilities of threats, and vulnerabilities of assets play key roles.

Calculation of Risk Rating

Risk rating is a quantitative measure of the network’s threat level before the adaptive security model reflects the changes in security policies and mechanisms. The proposed model calculates a risk rating number using the following factors:

Signature rating (SR): The value indicates the degree of attack certainty.

Damage rating (DR): The value indicates the amount of damage an attack can cause.

Target rating (TR): This value indicates the target criticality.

Vulnerability rating(VR) : This value indicates how much vulnerable the target is.

Prior rating (PR): This factor indicates the value if the attacker is already in the watch list maintained by the security model.

By taking all the above mentioned factors into consideration the risk rating is calculated using the formula:

$$\text{Risk Rating} = \frac{(SR*DR*TR)}{1000} + VR + PR$$

3.3 Evaluator

The main job of the evaluator is to calculate the threat rating which is a quantitative measure of the network's threat level after the adaptive security model reflects the changes in security policies and mechanisms. The proposed model calculates threat rating using the following factors:

Threat Level Calculation

Threat Level = Risk Level - Alert Level

The alert level for some threats can be specified as:

- 10: deny-intruder
- 9: deny-intruder-victim-pair
- 8: deny-intruder-service-pair
- 7: deny-connection
- 6: deny-packet
- 5: modify-packet
- 4: request-block-host
- 3: request-block-connection
- 2: reset-connection
- 1: request-data rate-limit

For example, if an alert had a risk level of 50 and the adaptive security model mitigates the event with a deny-packet action, the threat rating would be calculated as:

Threat Rating = Risk Rating - Alert Rating, or 50 - 6 = 44.

Thus threat rating is a better measure than risk rating and taking the adaptive security model mitigation action into account, threat rating helps to focus on the most important intrusion issues that have not been mitigated.

3.4 Policy Interpreter:

The main objective of calculating the risk rating and threat level is to provide recommendations that maximize confidentiality, integrity and availability while still providing functionality and usability. Based on the decision taken by the evaluator after assessment of threat level, the job of reflector is to specify the appropriate security policies and change the network configuration to dynamically adapt the new network policies and mechanisms in order to ensure fail safe state. The policy interpreter determines the safety valve of network by adopting the need based security policies which in turn prevent the intrusion and ensure the privacy and security of data transmission. It is pertinent to mention that the evaluator can apply the new security policies either on risk rating or threat rating, but threat rating focuses on the most important threats that have not been mitigated and hence is a preferred measure. The feedback loop reports back to monitor and assures the security of data transmission. When security policies are adapted through the evaluator component the monitor component's measurements are affected in the next feedback loop because of the adaptation. Thus the executor maps the given policy rules to the source data indicating to the Security unit which security function to apply to which sets of data.

IV. WORKPLAN REALIZATION

The proposed enhanced adaptive network security model modifies the security policies and mechanisms at runtime and maximizes the privacy and protection of network data from the threats of numerous invasions. In comparison to other existing security models, the proposed adaptive network security model places more emphasis on network security using dynamic adaptation. The adaptive model starts working from packet filtering and ends in updating security policies. Comprehensive packet analysis (TCP packet Header) is the first step in monitoring network security. The packet is analyzed for the threat level and security measures and policies which satisfy the appropriate needs are drawn up, followed by network quality of service assessment. Then the network monitoring module will reinforce security and basic precautionary measures will be deployed, and system security mechanisms and policies will be established according to the results of packet analysis. Once a security threat is detected by the network monitoring module, detection and fore-warning measures are introduced into the model to monitor the work of security system, and detect whether the work of the present system is in accordance with security strategies. The proposed adaptive network security (ANSM) model can be expressed using the following relations:

S (ANSM) = M(Monitoring) +R(Risk Analysis) +D(Detection & Alert) + A(Analyzing) +P(Policy)+ P(Reinforce Security Policy) + K(Knowledge Base)

Briefly described as follows:

State variables:
Mn = Monitoring
Ra= Risk Analysis
Pa= Packet Analyzing
Da = Detection &Alert
Po = Policy
Re = Reinforce security Policy
Kn=Knowledge
S = (Mn, Ra,Pa,Po, Re, Dw,Kn)
C = (Pa, Da,Re)
P = (Da, Re,K)

```
Rules: create_object (S);
If (!C) then
{
    create (C);
}
Else
{
    P = P + K;
    Create (P);
}
```

V. CONCLUSION

Network security is a continuous process and demands regular network analysis, testing and maintenance. In current scenario there are number of ways, which guarantee for the safety and security of the network but it cannot be said that they will be everlasting. In this paper we propose a dynamic and flexible security framework which makes real-time adjustment and control on the policy state using the self adaptive mechanism based on incident triggered and policy-driven model. When network changes or new security technology or attack measures emerge, the network security model has the ability to respond and adapt to new situations. Thus it provides a viable method for network security validation in dynamic environment but further research is needed to develop new tactics , integrate new mechanisms and make the security model self learning.

REFERENCES

[1] Khalkhali, I; Azmi, R; Azimpour-Kivi, M; Khansari, M. "Host-based web anomaly intrusion detection system, an artificial immune system approach". ProQuest.

[2] R. Venkatesan and S. Bhattacharya, "Threat-adaptive security policy," Performance, Computing, and Communications Conference, 1997. IPCCC 1997., IEEE International, pp. 525–531, Feb 1997.

[3] Special Webcast: Real-Time Adaptive Security: Proactively Mitigating Risks". Retrieved 6 January 2009.

[4] Wenke Lee and Salvatore J. Stolfo and Philip K. Chan and Eleazar Eskin and Wei Fan and Matthew Miller and Shlomo Hershkop and Junxin Zhang, Real Time Data Mining-based Intrusion Detection, IEEE, 2001.

[5] S. Alampalayam and A. Kumar, "An adaptive security model for mobile agents in wireless networks," Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE, vol. 3, pp. 1516–1521 vol.3, Dec. 2003.

[6] C. Chigan, L. Li, and Y. Ye, "Resource-aware self-adaptive security provisioning in mobile adhoc networks," Wireless Communications and Networking Conference, 2005 IEEE, vol. 4, pp. 2118–2124 Vol. 4, March 2005.

[7] P. Schneck and K. Schwan, "Dynamic authentication for high-performance networked applications,"Quality of Service, 1998. (IWQoS 98) 1998 Sixth International Workshop on, pp. 127–136, May 1998.

[8] L. Marcus, "Local and global requirements in an adaptive security infrastructure," International Workshop on Requirements for High Assurance Systems (RHAS 2003), Sept 2003.

[9] A. Shnitko, "Practical and theoretical issues on adaptive security," Proceedings of FCS'04 Workshop on Foundations of Computer Security, Workshop on Logical Foundations of an Adaptive Security Infrastructure, June 2004.

[10] IEEE Journal on Selected Areas in communications, Special issue on Secure Communications, vol. SAC-7,May 1989.

[11] B. H. C. Cheng, H. Giese, P. Inverardi, J. Magee, and R. de Lemos, "08031 – software engineering for self-adaptive systems: A research road map," in Software Engineering for Self-Adaptive Systems, ser. Dagstuhl Seminar Proceedings, B. H. C. Cheng, R. de Lemos, H. Giese, P. Inverardi, and J. Magee, Eds., vol. 08031. Internationales Begegnungs- und Forschungszentrum fuer Informatik (IBFI), Schloss Dagstuhl, Germany, 2008.

[12] P. McKinley, S. Sadjadi, E. Kasten, and B. Cheng, "Composing adaptive software," Computer,vol. 37, no. 7, pp. 56–64, July 2004.

[13] B. Timmerman, "A security model for dynamic adaptive traffic masking," in NSPW '97:Proceedings of the 1997 workshop on new security paradigms. New York, NY, USA: ACM, 1997, pp. 107–116.

[14] L. Teo, G.-J. Ahn, and Y. Zheng, "Dynamic and risk-aware network access management," in SACMAT '03: Proceedings of the eighth ACM symposium on access control models and technologies. New York, NY, USA: ACM, 2003, pp. 217–230.

[15] K.-D. Kang and S. H. Son, "Towards security and QoS optimization in real-time embedded systems," SIGBED Rev., vol. 3, no. 1, pp. 29–34, 2006.

[16] M. El-Hennawy, Y. Dakroury, M. Kouta, andM. El-Gendy, "An adaptive security/performance encryption system," Electrical, Electronic and Computer Engineering, 2004. ICEEC '04. 2004 International Conference on Computer Engineering and Systems, pp. 245–248, September 2004.

[17] IEEE Network Magazine, Special issue on Network Security, vol. 1, April 1987

[18] B. Schneier, ``Cryptographic design vulnerabilities," Computer, vol. 31,no. 9, pp. 29_33, Sep. 1998.

[19] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, ``Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," Proc. IEEE, vol. 100, no. 11, pp. 3056_3076, Nov. 2012.