Perspective Zero-Day Attack Path Investigation With Semantics Aware Execution Scheme

M.Rajakumaran[1], S.Deepika[2], S.Priadharshini[3], C.Sajee[4]
[1]Assistant Prof, Dept of Computer Science and engineering
[2, 3, 4]Dept of Computer Science and engineering
[1, 2, 3, 4] E.G.S. Pillay Engineering College (Autonomous), Nagapattinam.

Abstract- *Nowadays, many companies and/or governments require a secure system and/or an accurate intrusion detection system (IDS) to defend their system services and the user's private information. DDoS attacks jam the network service of the target using multiple bots hijacked by crackers and send frequent packets to the target server. Servers of many companies and/or governments have been victims of the attacks. In such an attack, detecting the crackers is tremendously difficult, since they only send a command by multiple bots from another network and then leave the bots quickly after command execute. The proposed strategy is to develop an intelligent detection system for DDoS attacks by detecting patterns of DDoS attack using system packet analysis and exploiting machine learning techniques to study the patterns of DDoS attacks. In this study, we analysed large numbers of network packets provided by the Center for Applied Internet Data Analysis and applied the detection system using an Ad-hoc On-demand Distance Vector (AODV) and Adaptive Information Dissemination (AID) protocols. The discovery system is accurate in detecting DDoS attacks. Distributed Denial-of-Service (DDoS) attacks are usually launched through the botnet. Unfortunately, the recent emergence of attacks performed at the application layer has multiplied the number of possibilities. Finally botnet detection procedure has been applied which is based on stability of bots.*

I. INTRODUCTION

Network Security

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.[citation needed] Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

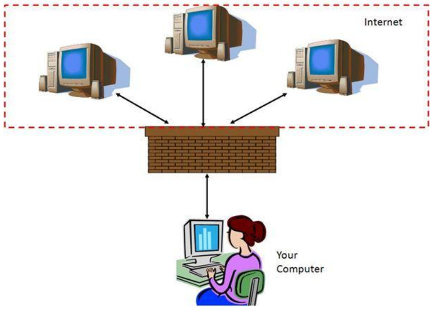

Figure 1.1 Example of Network Security diagram

A key problem when addressing DDoS attacks is attack detection. Several DDoS detection systems have been proposed. Most of them can be classified as either signature based or abnormal behavior based mechanism. As DDoS attacks have no common attack signatures and a sophisticated or experienced attacker may change the attack pattern frequently, detecting attacks by performing pattern matching against a database of known attack signatures is not feasible. However, DDoS traffic generated by today's tools often has characteristics that make it possible to distinguish it from normal traffic using statistical measurement [2, 12, 22]. This abnormal behavior can be used to define methods to improve the detection accuracy at each individual node.

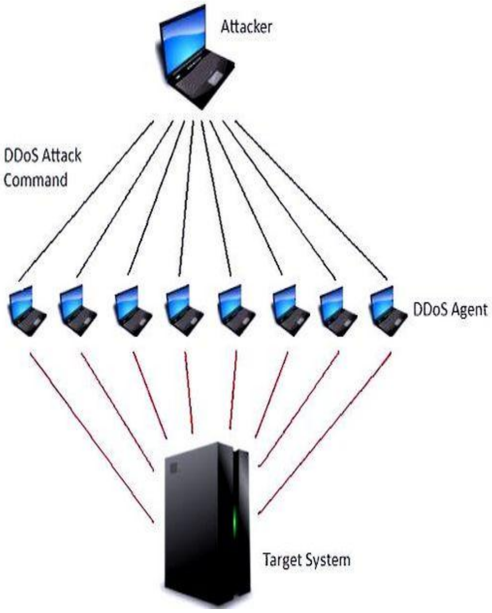

Figure 1.4 DDoS Attacker Scenario

II. EXISTING PROCESS

- Compared with other DDoS detection methods, detecting by entropy is proved to have many advantages, such as more simple, higher sensitivity, lower rate of false positives
- Many attackers in different locations continuously send a great deal of packets at the same time, which is out of the target device's processing ability, making the legitimate user out of service.
- This enables attackers can launch DDoS attacks towards SDN network from multiple layers.
- It works well when the attack traffic is very huge.

III. PROPOSED METHODOLOGY

- Wireless communication technologies have made great progress the experience of mobile users.
- SDN can greatly facilitate big data acquisition, transmission, storage, and processing and big data will impact the design and operation of SDN.
- Distributed Denial of Service (DDoS) flooding attacks is the main method to destroy the availability of the server or the network.

IV. DETECTION TECHNIQUE:

Detecting Distributed Denial of Service Attacks by Sharing Distributed Beliefs

We propose a distributed approach to detect distributed denial of service attacks by monitoring the increase of new IP addresses. Unlike previous proposals for bandwidth attack detection schemes which are based on monitoring the traffic volume, our scheme is very effective for highly distributed denial of service attacks. Our scheme exploits an inherent feature of DDoS attacks, which makes it hard for the attacker to counter this detection scheme by changing their attack signature. Our scheme uses a sequential nonparametric change point detection method to improve the detection accuracy without requiring a detailed model of normal and attack traffic. In a multi-agent scenario, we show that by sharing the distributed beliefs, we can improve the detection efficiency.

V. ARCHITECTURE

DDoS is short for Distributed Denial of Service. DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

VI. IMPLEMENTATION RESULTS

TESTING AND IMPLEMENTATION

Verification and Validation Testing:

Verification is a Quality control process that is used to evaluate whether or not a product, service, or system complies with regulations, specifications, or conditions imposed at the start of a development phase. Verification can be in development, scale-up, or production. This is often an internal process.

Validation is Quality assurance process of establishing evidence that provides a high degree of assurance that a product, service, or system accomplishes its intended requirements. This often involves acceptance of fitness for purpose with end users and other product stakeholders.

Unit testing: Unit testing is a software verification and validation method in which a programmer tests if individual units of source code are fit for use. A unit is the smallest testable part of an application. In procedural programming a unit may be an individual function or procedure.

Unit testing allows the programmer to refractor code at a later date, and make sure the module still works correctly.

The procedure is to write test cases for all functions and methods so that whenever a change causes a fault, it can be quickly identified and fixed.

Readily-available unit tests make it easy for the programmer to check whether a piece of code is still working properly.

System Testing

System testing of software or hardware is testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. System testing falls within the scope of black box testing, and as such, should require no knowledge of the inner design of the code or logic

This test is done to the project overall system can perform all of its functions in a realistic operating environment.

The system is capable of handling all transactions during periods of peak load without failure or unreasonable delays. Peak Load occurs during busy seasons such as lunch breaks. The system should be able to recover from failures caused due to power failures, hardware problems etc,

It involves two kinds of activity

1. Integrated Testing
2. Acceptance Testing

1. Integrated Testing

Integration testing is a logical extension of unit testing. In its simplest form, two units that have already been tested are combined into a component and the interface between them is tested. A component, in this sense, refers to an integrated aggregate of more than one unit. In a realistic scenario, many units are combined into components, which are in turn aggregated into even larger parts of the program. The idea is to test combinations of pieces and eventually expand the process to test your modules with those of other groups.

2. Acceptance Testing

Acceptance testing is black-box testing performed on a system (for example: a piece of software, lots of manufactured mechanical parts, or batches of chemical products) prior to its deliver. It is also known as functional testing, black-box testing, QA testing, application testing, confidence testing, final testing, validation testing, or factory acceptance testing.

VALIDATION TESTING

Software validation is achieved through a serious of tests that demonstrate conformity with requirements. Thus the proposed system under consideration has been tested by validation & found to be working satisfactory.

OUTPUT TESTING

Asking the user about the format required by them tests the output generated by the system under consideration. It can be done in two ways, one on screen and other is printer format. The output format on the screen is found to be correct as the format designed in system test.

VII. CONCLUSION

A DDoS detection method based on fuzzy synthetic evaluation decision-making model. Also make a comparable experiment to show its advantage to other DDoS detection algorithm based on single factor. DDoS attacks, divide the attack into three levels and use these three levels of attack data to initialize the parameters of the DDoS detection method. Host-based DDoS detection framework called BRAIN is proposed that adds another dimension to detect DDoS attacks in real-time. The results illustrate that the inclusion of hardware behavior into detection increases accuracy significantly. BRAIN is a low cost, adaptive and highly accurate DDoS detection framework with 99.8% accuracy. Anomaly detection in BRAIN is doctrine around behavior derived from hardware events. It may be even possible to model and detect other network attacks using behavior derived from these hardware events.

VIII. FUTURE ENHANCEMENT

The PDoS is a pure hardware targeted attack which can be much faster and requires fewer resources than using a botnet or a root/vserver in a DDoS attack. Because of these features, and the potential and high probability of security exploits on Network Enabled Embedded Devices (NEEDs), this technique has come to the attention of numerous hacking communities. Using entropy as a summarization tool, it is able to show that the analysis of feature distributions leads to significant advances on two fronts: (1) it enables highly sensitive detection of a wide range of anomalies, augmenting detections by volume-based methods, and (2) it enables automatic classification of anomalies via unsupervised learning. It is demonstrated the utility of treating anomalies as events that alter traffic feature distributions shown that treating anomalies in this manner yields considerable diagnostic power, in detecting new anomalies, in understanding the structure of anomalies, and in classifying anomalies. The work proposed that entropy is an effective metric to capture unusual changes induced by anomalies in traffic feature distributions. The work in has demonstrated the utility of treating anomalies as events that alter traffic feature distributions. It shows that treating anomalies in this manner yields considerable diagnostic power, in detecting new anomalies, in understanding the structure of anomalies, and in classifying anomalies. It also shows that entropy is an effective metric to capture unusual changes induced by anomalies in traffic feature distributions.

REFERENCES

[1] Imperva, "Q2 2015 Global DDoS Threat Landscape: Assaults ResembleAdvanced Persistent Threats," https://www.incapsula.com/blog/ddos-globalthreat-landscape-report-q2-2015.html.

[2] V. Jyothi, S. K. Addepalli, and R. Karri, "Deep Packet Field ExtractionEngine DPFEE A Pre-processor for Network Intrusion Detection andDenial-of-Service Detection Systems," IEEE ICCD, pp. 287–293, 2015.

[3] X. Wang and R. Karri, "Numchecker: Detecting kernel control-flow modifyingrootkits by using hardware performance counters," IEEE DAC, pp.1–7, 2013.

[4] K. Kato and V. Klyuev, "An Intelligent DDoS Attack Detection SystemUsing Packet Analysis and Support Vector Machine," IJICR, pp. 478–485,2014.

[5] K. Devi, G. Preetha, G. Selvaram, and S. M. Shalinie, "An impact analysis:Real time DDoS attack detection and mitigation using machine learning,"ICRTIT, pp. 1–7, 2014.

[6] A. Ramamoorthi, T. Subbulakshmi, and S. M. Shalinie, "Real time detectionand classification of ddos attacks using enhanced svm with string kernels,"ICRTIT, pp. 91–96, 2011.

[7] Z. Li, C. Wilson, Z. Jiang, Y. Liu, B. Y. Zhao, C. Jin, Z.-L. Zhang, and Y. Dai, "Efficient batched synchronization in drop box-like cloud storage services," in Proc.ACM/IFIP/USENIX 14th Int. Middleware Conf., 2013, pp. 307–327.

[8] A. Li, X. Yang, S. Kandula, and M. Zhang, "CloudCmp: Comparing public cloud providers," in Proc. ACM SIGCOMM Internet Meas. Conf., 2010, pp. 1–14.

[9] A. Bessani, M. Correia, B. Quaresma, F. Andr_e, and P. Sousa, "DepSky: Dependable and secure storage in a cloud-of-clouds," in Proc. 6th Conf. Comput. Syst., 2013, pp. 31–46.

[10] P.Wendell, J. W. Jiang, M. J. Freedman, and J. Rexford, "Donar: Decentralized server selection for cloud services," in Proc. ACM SIGCOMM Conf., 2010, pp. 231–242.

[11] M.Sathiamoorthy, M.Asteries, D.Papailiopoulos, A.G.Dimakis, R.Vadali, S. Chen, and D. Borthakur, "XORing elephants: novel erasure codes for big data," VLDB Endowment, vol. 6, no. 5, pp. 325–336, 2013.