Research Paper Engineering

Denial-of-Service (DoS) Attack Detection in Cloud Computing

* T. Poornachandar ** D. Jaya Prakash

* Assistant Professor / Computer Science and Engineering, Annapoorana Engineering College, Salem

** Assistant Professor / Computer Science and Engineering, Dhirajlal Gandhi College of Technology, Salem.

ABSTRACT

Cloud computing is a sophisticated computing system. In cloud computing environment, cloud servers affords requested cloud services, occasionally may crash after in receipt of enormous quantity of requests. The denial of service (DoS) attack thwart the authentic cloud clients from in receipt of service. Denial of Service attack is produces by Internet Packet (IP) Spoofing, packet flooding attacks. It makes the cloud clients request seem to be unusual. Cloud clients can adapt efficiently to an attack by growing their request rate based on time-out windows to calculate attack rates. The cloud server is to process client requests rates with high prospectus to sniffing the attack flows by selective random variety packet flows. In this paper, we present a concept for packet monitoring techniques adaptive Selective verification (ASV). This will identify the flooding attack request within the cloud computing technologies and improve the most favorable performance.

Keywords : Cloud Computing, Denial-of-Service attack, IP Spoofing, Adaptive Selective Verification.

Introduction

Cloud computing is a next generation computing technology. It is one of today's the largest part stimulating technologies, because it will decrease the cost and complication of applications, and it is flexible and scalable. So these most of the benefits distorted to cloud computing. In cloud computing environment, cloud servers affords requested cloud services, occasionally may crash after in receipt of enormous quantity of requests. The denial of service (DoS) attack thwart the authentic cloud clients from in receipt of service. Denial of Service attack is produces by Internet Packet (IP) Spoofing, packet flooding attacks. It makes the cloud clients request seem to be unusual. Cloud clients can adapt efficiently to an attack by growing their request rate based on time-out windows to calculate attack rates. The cloud server is to process client requests rates with high prospectus to sniffing the attack flows by selective random variety packet flows. In this paper, we present a concept for packet monitoring techniques adaptive Selective verification (ASV). This will identify the flooding attack request within the cloud computing technologies and improve the most favorable performance.

In this paper we establish Adaptive Selective Verification (ASV) which is a distributed adaptive method for attackers' efforts to refuse service to legitimate cloud clients based on selective verification. Our schemes apply on bandwidth of the cloud computing network flows but the intensity of security employed by the clients dynamically regulates to the current intensity of attack. At a high level, the cloud clients exponentially ramp-up the amount of requests they send in successive time-windows, up to a threshold. The server implements a reservoir-based random sampling to effectively sample from a sequence of incoming packets using bounded space. This enables adaptive bandwidth payments with server state whose size remains small and constant regardless of the actions of the attacker.

Our analysis, experiments, and simulations demonstrate that the proposed DoS based adaptive Selective Verification mechanism is effective and efficient compared with the existing methods. In particular, it possesses the some advantages: The implementation of the proposed method gets no modifications on current routing software. The DoS adaptive Selective Verification need to update on the existing routing software, which is tremendously tough to achieve on the cloud computing. On the other HAND, our proposed method can work independently as an additional module on routers for supervising and inspecting the data flow by using random sampling.

The proposed strategy is basically different from the existing Dos detection techniques. adaptive counter-measures that are deployed dynamically and proportionally to blunt attacks at minimal cost. Auction-based bandwidth payments accomplish this by an accounting system in which clients build credit by sending dummy bytes in congestion-controlled streams, and the cloud server occasionally takes requests from clients that have assemble the most credit. This may require significant server state and is vulnerable to adversaries who are able to create network blocking that causes legitimate clients to back off while attackers ignore back-offs. Selective verification requires no server state or congestion assumptions; however, the existing state-of-the-art does not provide any accurately analysed strategy for adaptation.

Related Work

Shui Yu et al [3]., has stated their work on Denial-of-service (DoS) attacks are considered within the state of a shared channel model in which attack rates may be large but are bounded and client request rates vary within fixed bounds. It is exposed that clients can adapt effectively to an attack by raising their request rate based on timeout windows to approximate attack rates. The server will be able to process client requests with high probability while pruning out most of the attack by selective random sampling. The protocol Adaptive Selective Verification (ASV) is shown to use bandwidth efficiently and does not require any server state or assumptions about network congestion. The main results of the paper

are a formulation of most favorable performance and a proof that Adaptive Selective Verification is most favorable. Introduce Adaptive Selective Verification (ASV) which is a distributed adaptive mechanism for thwarting attackers' efforts to deny service to authorized clients based on selective verification. That system uses bandwidth as currency but the level of security employed by the clients dynamically adjusts to the recent level of attack. At a high level, the clients exponentially ramp-up the number of requirements they send in consecutive time-windows, up to a threshold. The server implements a reservoir-based random sampling to successfully sample from a sequence of incoming packets using bounded space. This enables adaptive bandwidth payments with server state whose size remains small and constant regardless of the actions of the attacker.

Sanjeev Khanna et al [4]., has stated their work on Adaptive Selective Verification attacks are a growing concern as they continue to cause an important threat to the reliability of the Internet. Such attacks can happen at all levels in the protocol stack and threaten both routers and hosts. Many attacks aim to reduce insufficient resources (e.g., CPU, memory, disk) by generating illegal requests from one or many, probably negotiated, attacker-controlled hosts.

Zou et al. [26] provide ideas that are effective for filter schemes, although it is unclear how they can be applied to bandwidth payments. Srivastsa et al. [20] show how to use information available in the application layer to identify and differentiate between low and high utility clients to provide better service to more valuable customers. Their solution requires more feedback from the application than selective verification and is more applicable to scenarios where the clients have a history of interactions with the server. Wang et al. [22] show how to provide adaptation for client puzzles. Because of the nature of the client puzzle schemes, where the cost factor of the defense on the server is minimal, their proposal mainly focuses on cost minimization for the clients.

Maneesha Sharma, provides Cloud computing has generated a lot of interest and competition in the industry and it is recognize as one of the top 10 technologies of 2010[1]. It is an internet based service delivery model which provides internet based services, computing and storage for users in all market including financial, health care & government. In this paper we did systematic review on different types of clouds and the security challenges that should be solved. Cloud security is becoming a key differentiator and competitive edge between cloud providers. This paper discusses the security issues arising in different type of clouds.

Distributed Cloud Intrusion Detection Model NIDS and HIDS are not suitable for security environment of cloud. Cloud as middleware layer, which having an audit system that design to cover an attacks that HIDS and NIDS can't cover. Irfan Gul,et al.[2] have suggested So by means of using this model we able to bring the IDS as middle ware and any information from cloud user to CSP will reached through by means of it. This middleware is said to be as third party and it was fully maintained by service provider.

Perhaps the most counter-intuitive DoS countermeasure strategy is the use of bandwidth as payment. In such a scheme, clients use additional bandwidth to get access. The idea is that attackers are using all of the bandwidth available to them (or the maximum bandwidth they can afford to use without being detected by other mechanisms) to execute an attack, whereas legitimate clients are using only the resources they require to accomplish their less-demanding objectives. Hence legitimate clients have bandwidth to spare and can use this fact to differentiate themselves from attackers. This strategy was introduced in [8] in the context of authenticated broadcast using selective verification and extended to general Internet protocols in [21] using bandwidth auctions. Selective verification allows clients to send extra requests and the server samples from these requests probabilistically. This technique is very effective in diminishing the effects of a DoS attack if a sufficient level of client redundancy is employed

Vikas Chouhan provides Cloud computing can be defined as a new style of computing in which dynamically scalable and often virtualized resources are provided as a services over the Internet. Advantages of the cloud computing technology include cost savings, high availability, and easy scalability. DoS attacks do not wish to modify data or gain illegal access, but instead they target to crash the servers and whole networks, disrupting legitimate users' communication. DoS attacks can be launched from either a single source or multiple sources. Multiplesource DoS attacks are called distributed denial-ofservice (DDoS) attacks. When the operating system notices the high workload on the flooded service, it will start to provide more computational power to cope with the additional workload.

PROPOSED WORK

3.1. SYSTEM ARCHITECTURE

3.1.1 Cloud Computing Dos attack Detection

The attacker first establishes a network of computers that will be used to generate the huge volume of traffic needed to deny services to legitimate users of the victim. To create this attack network, attackers discover vulnerable cloud hosts on the cloud computing system. DoS attack; the master computer orders the zombies to run the attack tools to send huge volume of packets to the victim.

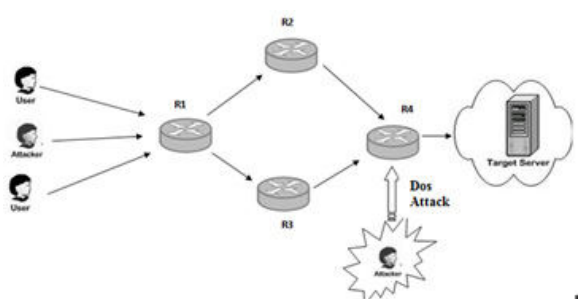

Fig .Cloud Computing Dos attack Detection

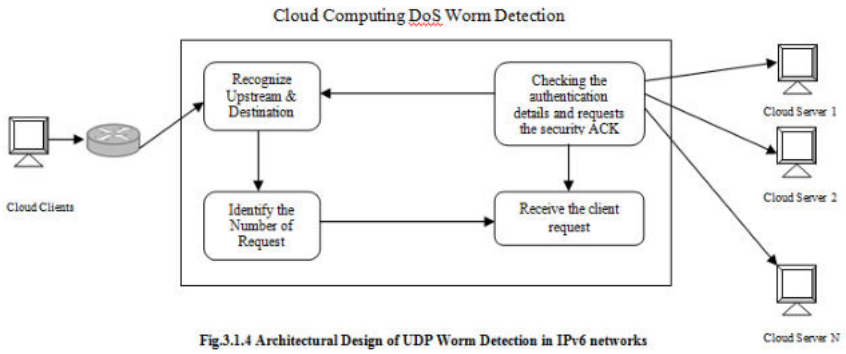

Fig.3.1.4 Architectural Design of UDP Worm Detection in IPv6 networks

Conclusion

In conclusion, ASV advances the state-of-the art in bandwidth based DoS defense mechanisms by introducing a cloud computing technology by using distributed adaptive solution based on selective verification. In ASV, the cloud clients exponentially ramp-up the number of requests they send in consecutive time windows, up to a threshold. The server implements a reservoir based random sampling to effectively sample from a sequence of incoming packets using bounded space. The novel theoretical analysis of the protocol proves that the performance of ASV the performance of ASV adjusts extremely quickly to prevailing attack parameters. In addition, it is shown that the effect of ASV on Internet cross traffic is minimal, and comparable to that of its naïve non-adaptive counterpart, which represents no-defense attack-only scenarios.

REFERENCES

[1] Tripathi, A.; Mishra, A.; IT Div., Gorakhpur Centre, Gorakhpur, India "Cloud Computing Security Considerations", Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference. | [2] M. Abadi, M. Burrows, M. Manasse, and T. Wobber. Moderately hard, memory-bound functions. ACM Trans. Inter. Tech., 5(2):299–327, 2005. | [3] M. AlTurki, J. Meseguer, and C. A. Gunter. Probabilstic modeling and analysis of dos protection for the asv protocol. Electronic Notes on Theoretical Computer Science, 234:3–18, 2009. | [4] I. R. C. T. Fan, M. E. Muller. Development of sampling plans by using sequential (item by item) selection techniques and digital computers. J. Amer. Statist. Assoc., 57:387–402, 1962. | [5] C. Dwork, A. Goldberg, and M. Naor. On memory-bound functions for fighting spam. In CRYPTO, 2003. | [6] D. Eastlake. RFC: 2535, Domain Name System Security Extensions. | [7] C. A. Gunter, S. Khanna, K. Tan, and S. S. Venkatesh. Dos protection for reliably authenticated broadcast. In NDSS'04: | [8] Network and Distributed System Security Symposium. The Internet | [9] Society, 2004. |