ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Novel Prevention Technique for SCADA System against Distributed Denial of Service (DDoS) Attack

Animesh Srivastava[1]

Assistant Professor, Dept. of IT, Sikkim Manipal University-DE, Gangtok, Sikkim, India

ABSTRACT: Some Important services such as emergency response, water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, wind farms, civil defense siren systems, and large communication systems are increasing coming under threat. we propose, an architecture that hides the service IP address making it hard for an attacker to find, attack and disable the service. Provides access to the service through numerous lightweight proxies, which present a very wide target for the attacker. However, unlike these solutions uses a novel approach to hide the service from both clients and proxies, thus eliminating the need to trust proxies or apply a filtering perimeter around the service destination.

I. INTRODUCTION

We develop a novel Distributed DoS (DDoS) defense architecture. Making it virtually impossible to attack the service directly. This is in contrast to approaches that while hiding the service location from the general public, still exposes the service address to a small set of trusted proxies. Such proxies could become a primary target for the attacker, or worse, if compromised would expose the service address.

Proxies send traffic over ephemeral hidden paths, which are created on the underlying network using a technique akin to multicast routing. The paths are under complete control of the service and can be easily removed if a proxy misbehaves.

Proxies can still be discovered and attacked; Architecture uses any cast to limit proxy access. Since any cast packets are directed to the local proxy by the underlying routing system, an attacker is forced to have bots in the same any cast region as the clients to attack their proxy. However, since proxies are lightweight many can be quickly deployed and the any cast regions can be made smaller in an effort to isolate attackers. This dilution can not only help legitimate clients circumvent attackers, but can make it easier to expose bots whose activity becomes more
visible. Even so, the attack is localized to a private proxy, which can be easily and quickly disconnected by the service, and will only affect clients currently using that proxy.

It has hiding the service destination address and providing access to the service through a large front-end of proxies that themselves do not know the destination address, and that form distinct regions in network, and that are issued differently to distinct clients based on trust can effectively defend against large scale Distributed Denial of Service attacks. Specifically, we make the service resilient to inside attacks from compromised proxies by hiding the destination address from them and providing them with a temporary path that can be removed at any time to prevent them from causing harm. We isolate and localize attackers to smaller network regions so that they are dispersed, become easier to defend against or can be discovered and removed. The destination to issue different proxies to different clients such that an attacker cannot easily harm the data exchange between the destination and a legitimate client. Finally, we make proxy discovery robust by making the clients learn about a small number of proxy addresses that remain valid for a long duration, but are associated with a large group of ever changing proxies.

DOI: 10.15680/IJIRCCE.2016. 0409175

II. BRIEF REVIEW OF THE PREVIOUS WORK

A DoS attack is an explicit attempt to disable the available service of a victim site or node from a legitimate client(s) by an automatic or manual single attack source. The nature of a DoS attack is to deplete the victim's resources. These resources can be network bandwidth, processing power, or operating system data structures. DoS attack technology has continued to evolve and has remained a serious threat with significant impact on Internet infrastructures, organizations and individual hosts [2]. However, it is also possible that compromised hosts coordinate to flood a victim with overwhelming attack packets. The attack takes place simultaneously from multiple-attack sources called a Distributed DoS (DDoS) attack. A DDoS network can be established by compromising many computers infected by the malware that acts simultaneously and is coordinated under the control of an attacker(s) in order to break into th e system of the victim, exhaust resources, and force a denial of service.

DDoS attack which uses millions of zombies machines mostly with artificial source addresses creates a surge of traffic without packet content signature. The available link bandwidth varies in accordance with the statistics of the input traffic [5]. These statistics of arriving traffic are not stationary as internet parameters like network traffic load, mix of traffic; mix of congestion control actions and on/off flow keeps on changing. The bottleneck link in the victim network is consumed by the huge volume of unwanted traffic created by various tools used to attack server. The defense technique proposed here, aims to provide enormous bandwidth to legitimate users at the time of attack. The satisfactory efficiently to detect and filter out attack traffic is not being fully achieved by most of the current defense approaches.

To mitigate the risks of DoS and DDoS attacks procedures, software and hardware can be put in place that will protect systems prior to attack. It can detect malicious activity as it occurs. Then support the organization in reacting appropriately as required. As a result of the nature of DoS attacks, it is often the case that strong reactive mechanisms are the best form of defense. These aspects motivate use to give an approach based on no rate limiting control attack and IP hiding architecture. A computer industry report by the DoS attack prevention company Prolexic noted that there was a 27.5 percent increase in attacks from Q3 2012 to Q4 2012, with a 67% increase in attack duration and a 20% increase of average attack bandwidth [2]. This same report noted that over 55% of the sources of these attacks came from China and the next highest country of origin was from Germany with just over 9% of the source DoS traffic [2].

Problem

In DDoS attacks, attackers can set up different types of attack sources and then implement various packet-transmission strategies and various packet forms to disrupt the available services of their victims. Consequently, DDoSdefense systems need to deploy variety of DDoS detection methods in order to mitigate the damage from the attacks. This can be slow depending on computational processes and they may be unable to serve improvement purpose in real-time. The DoS management framework presented provides coverage of security before an incident, during an incident and after an incident. This is achieved by detailing a governing strategy and specific recommendations at both operational and technical levels for:

- Protecting against DoS attacks.
- Detecting attacks when they occur.
- Responding appropriately to defend current and future attacks.

III. DDOS ATTACK AND FLASH CROWD

We are motivated by the fact that the feature of traffic volume in flash crowds is different
from DDoS attacks. Therefore, the flow similarity among flash crowds is much stronger than that among DDoS attack. DDoS attacks and flash crowds share similar behavior, and we need to differentiate these effectively to avoid raising false alarms. In fact, it is a big challenge for defenders to discriminate between DDoS flooding attacks and flash events. There are serious consequences if we cannot do this. On one hand, attackers can mimic the traffic features of flash crowds to disable our detectors. On the other hand, our detectors may treat legitimate flash crowds as DDoS attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Table 1: Flash Crowd Vs DDoS

Category	Flash crowd	DDoS
Network status	Congested	Congested
Server status	Overloaded	Overloaded
Traffic Type	Genuine	Malicious
Response to Traffic Control	Responsive	Unresponsive
Traffic Source	Mostly Web	Any
Flow size	Large Number of Flows	Any
Predictability	Mostly Predictable	Unpredictable

IV. NETWORK MODELS

Table 2: Classification of DoS Attacks [7]

Attack	Affected Area	Example	Description
Network Level Device	Routers, IP Switches, Firewalls	Ascend Kill II, “Christmas Tree Packets”	Attack attempts to exhaust hardware resources using multiple duplicate packets or a software bug.
OS Level	Equipment Vendor OS, End-User Equipment.	Ping of Death, ICMP Echo Attacks, Teardrop	Attack takes advantage of the way operating systems implement protocols.
Application Level Attacks	Finger Bomb	Finger Bomb, Windows NT RealServer G2 6.0	Attack a service or machine by using an application attack to exhaust resources.
Data Flood (Amplification, Oscillation, Simple Flooding)	Host computer or network	Smurf Attack (amplifier attack) UDP Echo (oscillation attack)	Attack in which massive quantities of data are sent to a target with the intention of using up bandwidth/processing resources.
Protocol Feature Attacks	Servers, Client PC, DNS Servers	SYN (connection depletion)	Attack in which “bugs” in protocol are utilized to take down network resources. Methods of attack include: IP address spoofing, and corrupting DNS server cache.

Table 3. DDoS prevention Techniques [1-6]

Name of Technique	Approach Used	Advantage	Disadvantage
Ingress Filtering	Ingress Router set to drop traffic with IP address not matching to domain prefix.	Reduces DoS attack due to IP spoofing , locates source of attack if ISP’s have ingress filtering instead of customer links	It just reduces, does not prevent use of forged source address of another host within permitted prefix filter range.
Route Based Distribu	Uses routing information. It works on basis that for every	Synergistic filtering effect is possible, spoofed IP flows are	Difficult to update route-based filters in real time. Acquiring global knowledge of whole n/w topology has scalability issues

DOI: 10.15680/IJIRCCE.2016. 0409175

ted Packet Filtering	link in internet, there is limited number of source IP addresses from which traffic comes.	prevented from reaching other Autonomous Systems.	
History Based IP-Filtering	A pre-built IP address database is used and an edge router acknowledges the incoming packets accordingly.	It is robust, there is no need of studying the whole network topology	If the invader knows that the IP packet filter is based on prior connections, they might deceive the server to be included in the IP address database
Secure Overlay Services (SOS)	Hash based routing is used, the user traffic is authenticated via SOAP then traffic is routed though small number of nodes called as servlets to victim.	Distributed system that offers exceptional protection to the specified target at the cost of modifying client systems.	Not recommended for public servers.

Table 4. DDoS Mitigation and Tolerance Techniques [4-9]

Name of Technique	**Approach Used**	**Advantage**	**Disadvantage**
Integrated Intserv	Uses the Resource Reservation Protocol (RSVP) to manage the resources allocation along the path that a particular traffic passes.	The bandwidth and buffer space for a particular link is assured for specific traffic flow	Due to pre allocation of resources their consumption increases.
Differentiated Services	Based on Type of Service byte in IP header	Allocates resources based on TOS of incoming packet	Requires cooperation of multiple administrative domains.
Class Based Queuing	Queues for different type of packets and different packets for different type of service is set, bandwidth is assigned to queues	Maintains QoS during DDoS attack	It is difficult to maintain queues.
Resource Pricing	propose a distributed gateway architecture and a payment protocol that imposes dynamically hanging	They identify allotting a priority mechanism to desirable clients as being key, and punish clients that cause load on the server.	Malicious user can populate the system with fake requests at low price, thus driving up the price for legitimate users.

	prices on both network, server, and information resources		
PushBack	First, a local Aggregate Congestion Control (ACC) detects the congestion at the router level and devises an attack signature. The signature defines a traffic aggregate as a group of traffic flows with a common property Then, a local ACC determines an appropriate rate limit for this aggregate.	PushBack can effectively mitigate DDoS attacks when the attacker's machines are gathered in few places.	When attackers are widely distributed over the Internet, the legitimate traffic also is rate-limited and PushBack will not be successful.

Table 5: Countermeasures for DoS Attacks [7]

Attack	Countermeasure Options	Example	Description
Network Level Device	Software patches, packet filtering	Ingress and Egress Filtering	Software upgrades can fix known bugs and packet filtering can prevent attacking traffic from entering a network.
OS Level	SYN Cookies, drop backlog connections, shorten timeout time	SYN Cookies	Shortening the backlog time and dropping backlog connections will free up resources. SYN cookies proactively prevent attacks.
Application Level Attacks	Intrusion Detection System	GuardDog, other vendors.	Software used to detect illicit activity.
Data Flood (Amplification, Oscillation, Simple Flooding)	Replication and Load Balancing	Akami/Digital Island provide content distribution.	Extend the volume of content under attack makes it more complicated and harder for attackers to identify services to attack and accomplish complete attacks.
Protocol Feature Attacks	Extend protocols to support security.	ITEF standard for itrace, DNSSEC	Trace source/destination packets by a means other than the IP address (blocks against IP address spoofing). DNSSEC would provide authorization and authentication on DNS information.

V. CONTRIBUTIONS

we develop a strong location hiding architecture where not only is the destination hidden from the sources but even the proxies do not know its address. We show that this architecture is a viable DDoSdefense solution running on real routers. The specific contributions of our work are as follows:

1. Architecture achieves strong location hiding property in which neither the proxies nor the sources know about the destination address. Architecture does not place trust on the proxies or requires trusted components to operate. In order for a proxy to reach the destination, we develop a novel hidden paths mechanism. Hidden paths share many similarities with multicast routing, and can be implemented on routers without sacrificing efficiency when forwarding traffic. Also, most of the multicast functionality available on routers could be reused to implement hidden paths. They also do not require hardware or architectural changes to routers.

2. Although IP any cast has been used to protect DNS servers from DDoS attacks, to our knowledge no other location hiding architecture has applied IP any cast to render attackers powerless. Using IP any cast in Architecture has two benefits; first the any cast Setup Proxy's (SPs) separate the attackers and dilute them (i.e., attackers can no longer muster strength with numbers) and second, any cast SPs have a very small address footprint so proxy discovery becomes simpler and can be made robust. In addition, any cast SPs localize attackers to smaller regions, which could lead to the discovery of the bots, or they can be handled using techniques such as client puzzles [4].

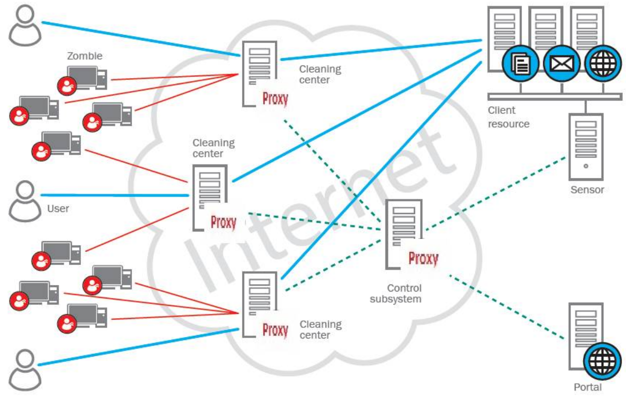
3. We provide a model in which the service can assign different data proxies to client depending on how a client is trusted. This model is different from making all proxies public and letting the client chose a proxy. We believe that making the proxies public will allow the attacker to strategize and disable portions of the proxies at a time to disrupt some legitimate clients. If an important legitimate client happens to be on a targeted proxy, its communication will be disrupted. Our approach, on the other hand, has the potential to prevents these situations.
The attacker does not know all data proxies and hence is limited to targeting setup proxies.

4. We construct a small scale Architecture using routers and prove that;

1) It is possible to completely hide the destination network by disabling route announcements for the destination network into the global Internet.

2) Hidden paths can be constructed out of multicast routing functions available on current routers. Specifically, Single Source Multicast (SSM) can be used for this purpose.

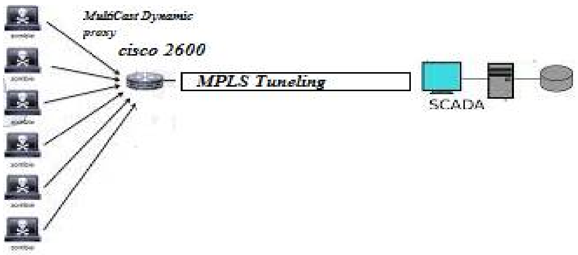
3) Hidden paths can be quickly added and deleted in the order of milliseconds to seconds respectively. Thus, new proxies could be easily added and compromised proxies can be removed quickly once they are identified.



Fig(1) : New Defending Architecture

Routers

For instance, an intermediate router inside a network could use an MPLS(Multiprotocol Label Switching) tunnel to forward the packets to a border router that has an Architectural forwarding entry a SCADA (supervisory control and data acquisition) system. As for the software changes on routers to implement the new protocol for Architecture hidden paths, our implementation on routers shows that single source multicast could be used as an alternative until the full Architecture protocol is implemented on routers. Moreover, since many functions in Architecture are similar to multicast routing (such as the multicast forwarding table), the implementation could borrow these existing functions to implement Architecture hidden paths.



Fig(2) : MPLS Tunneling For data transfer

Challenges in Location Hiding

Location hiding architectures need to ensure that the destination remains hidden despite compromised or malicious proxies. Minimizing the number of trusted components, carefully controlling what information is released to the proxies, and controlling how the proxies reach the destination are important factors to consider when hiding the service location. Otherwise, once the destination's address is out, the attacker will circumvent the proxy layer and directly target the destination. To avoid such potential threats, and putting a defensive filtering perimeter around the destination, so that even if the destination address is revealed to the attacker, the damaging traffic can be limited at this perimeter. However, filtering presents yet another set of challenges; for instance, the filtering perimeter must be large enough to cover bottlenecks near the destination network.

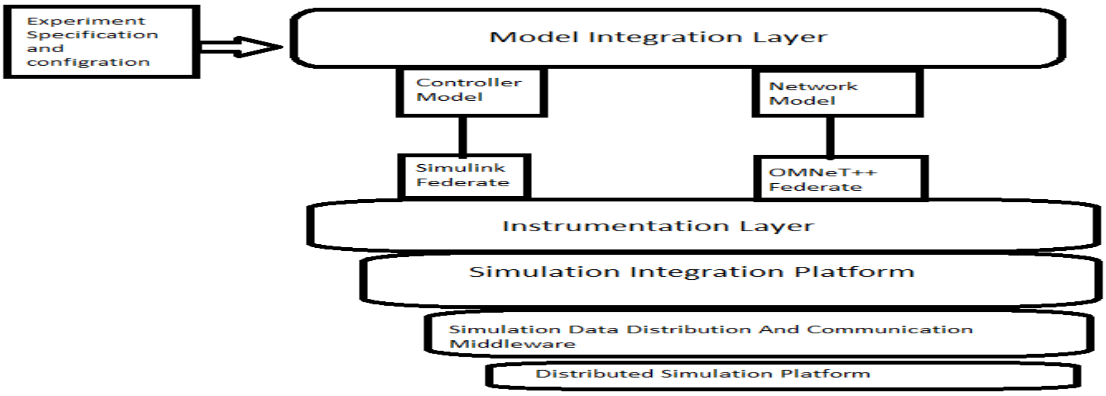
Location hiding architectures need to make the service resilient in the face of attacks on the proxies. Since the destination is no longer a direct target, the attacker will target the proxies instead. One approach to dealing with attacks on the proxies is to use a large number of proxies, and change them periodically to evade the attacker. However, in order to quickly recruit and deploy large numbers, the proxies must be lightweight, i.e., they need not require special hardware, software or store sensitive user information. Recruiting proxies from end-hosts such as peer-to-peer networks is one way to get them in large numbers, but they are generally not trustworthy.

Location hiding architectures need to assign and manage proxies in such a way that collateral damage to legitimate clients is limited. Although increasing the number of proxies may present a very wide target for the attacker, a legitimate client using a proxy to reach the destination may still be affected if that proxy is attacked. In fact, the attacker may selectively target specific proxies to disable or disrupt portions of the proxy network. The destination needs to assign and manage proxies in such a way that collateral damage to legitimate clients is minimized in
the presence of large scale DDoS attackers.

Lastly, location hiding architectures need to have a scalable and robust discovery mechanism for the clients to learn about the proxies. To reach the service, clients need to learn about the proxies using the discovery mechanism. However, this discovery service must be able to cope with frequent changes in the proxy set, and moreover, it must be robust against attacks; otherwise the discovery service will become a single point of failure for the entire system.

Simulation of SCADA system

In a SCADA system it is essential to model and simulate communication network in order to study mission critical simulation such as network failure or attack. Even a simple SCADA system is composed of several unit in various domains system , network and physical environment .System could include simulating controller and plant dynamics in Simulink or MatLab , Network architecture and behaviors in a network simulator like OMNeT++ ,etc.


Experiment Specification and configration
Model Integration Layer
Controller Model
Network Model
Simulink Federate
OMNeT++ Federate
Instrumentation Layer
Simulation Integration Platform
Simulation Data Distribution And Communication Middleware
Distributed Simulation Platform

VII. CONCLUSION

This paper proposes a novel location hiding architecture to protect critical services from DDoS attacks. Our architecture achieves strong location hiding property, neither the sources nor the proxies know the destination address. Moreover, the destination network itself is not announced into global routing, and therefore nobody can send packets to the hosts inside that network without going through the Architectural communication model. Since the attacker does not know the destination address, directed attacks on the service are no longer possible.

REFERENCES

1. Hussam M. N. Al Hamadi, Chan YeobYeun, Mohamed Jamal Zemerly .A Novel Security Scheme for the Smart Grid and SCADA Networks Wireless Personal Communications December 2013, Volume 73, Issue 4, pp 1547-1559.
2. Chin-Ling Chen, Chih-Yu Chang," A Two-Tier Coordinated Defense Scheme against DDoS Attacks", IEEE, 2011
3.G. Preetha, B.S. Kiruthika Devi, and S. Mercy Shalinie. Combat model based ddos detection and defence using experimental testbed: a quantitative approach. International Journal of Intelligent Engineering Informatics, pages 261-279, 2011.
4.T. Thapngam, S. Yu, W. Zhou, and G. Beliakov, "Discriminating DDoS Attack Traffic from Flash Crowd through Packet Arrival Patterns," in *Proceedings of the 30th Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2011)*, Shanghai, China, 2011, pp. 969 - 974.
5.Danny McPherson and Dave Oran. Architectural considerations of IP anycast. Draft-iab-anycast-arch-implications, February 2010.
6. http://thehackernews.com/2013/03/world-biggestddosattackthat-lmost.html
7.Behrouz A. Forouzan. Cryptography and network security, Fifth Edition ,Tata McGraw Hill Publication, 2010.
8. Arbor-Networks, "Worldwide Infrastructure Security Report: 2010 Report," Arbor Networks, 2011.
9. Shubha KherJinran Chen and ArunSomani. Mitigating denial of service attack using proof of work and token bucket algorithm. Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks, pages 65{72, 2011}

BIOGRAPHY

Animesh Srivastava is a Assistant Professor in the Information Technology Department, Sikkim Manipal University – DE ,Gangtok. Her research interests are Software Engineering, Network etc.