Comparing Two Models of Distributed Denial of Service (DDoS) Defences

Siriwat Karndacharuk
Computer Science Department
The University of Auckland
Email: skar018@ec.auckland.ac.nz

Abstract

A Controller-Agent model proposed by Tupakula & Varadharajan (2003) is being compared and contrasted against a Capabilities-Based model Anderson, Roscoe, & Wetherall (2003b) in this paper. The investigation is based on the classification of DDoS attacks and defences proposed by Mirkovic and Reiher (2004). Both models offered interesting approaches, however with the limitations and the assumptions they based on make them impractical for real life implementation. Anyway, their contribution to the DDoS research is valuable for other researchers.

1. Introduction

Distributed Denial-of-Service (DDoS) attacks are the major threats to the hosts or the organization that provide services on the Internet. WWW, DNS, and file sharing services are the examples of the popular attacked services since attacking on these services can lead to a considerable impact on the Internet community (Householder, Manion, Pesante, Weaver, & Thomas, 2001). Pervasive proposals have been proposed as the defence mechanisms in order to counteract these attacks. However, there are no appropriate benchmarks that facilitate the evaluation between alternative approaches (Mirkovic & Reiher, 2004).

The aim of this paper is to provide the intensive comparison between two dissimilar DDoS defence methods with a number of different kinds of attacks supplied by (Mirkovic & Reiher, 2004). Also this paper focuses only on the *use* phase of a DDoS attack. One approach is a Controller-Agent model offered by (Tupakula & Varadharajan, 2003). The other is a Capabilities-Based system suggested by (Anderson et al., 2003b).

2. DDoS Overview

A "denial-of-service" (DoS) attack can be achieved technologically by an attacker in order to prevent the legitimate users from being served by a particular service (Householder et al., 2001). While a large number of attacking units are set up to accomplish the same objective as a denial of service in a "distributed denial-of-service" attack (Mirkovic & Reiher, 2004). In other words, the DDoS attack is a subset of DoS attack.

2.1 How does DDoS attack work?

According to (Mirkovic & Reiher, 2004), they describe the DDoS general attack mechanism as follows. Firstly, an attacker needs to gather a number of machines to generate a volume of traffic to the victim service. This phase is called *recruiting* phase by the authors. It is usually done by scanning the remote machines and looking for security defects. The attacker then *exploits* the vulnerability to break into the recruited machines and *infects* them with a DDoS program. The whole methodology is referred by the authors as a *recruit/exploit/infect* strategy. Once sufficient machines are accumulated, then those machines are remotely controlled to launch the attack by the attacker. The later is called *use* phase.

The recruit/exploit/infect strategy is usually automated (Householder et al., 2001; Mirkovic & Reiher, 2004). Furthermore, once a machine is infected with DDoS program, it can be used to recruit more agents (Mirkovic & Reiher, 2004).

In order to reduce the possibilities of being discovered, IP spoofing technique is used to hide the source addresses of the subverted machines (Mirkovic & Reiher, 2004).

3. Are they talking about the same topic?

The title of both comparing papers refers to the denial-of-service. Are they going to talk about DoS or DDoS? The different between these terms is described in section 2. In (Tupakula & Varadharajan, 2003), DDoS terminology is mentioned many times so that a reader can be sure that it is talking about DDoS issue. However, in (Anderson et al., 2003b), DDoS is never mentioned in the article. It is not clear if the authors will talk about the general DoS or specific DDoS attacks. However, the phrases "… millions of machines …" are mentioned several places, this can be evident that the authors are talking about DDoS. The ultimate source that perfectly clarify this issue is from the presentation slides from (Anderson, Roscoe, & Wetherall, 2003a). These slides ensure that the authors definitely talk about DDoS.

4. Approaches

The underlining mechanism of Capabilities-Based model is to expand the existing Internet infrastructure with a Request-To-Send (RTS) server together with Verification Points (VPs) on the data path. A source needs to request for a permission to send a packet to a destination before actually do the sending process. This approach requires a synergy between the source and destination organisations. In contrast, the Controller-Agent model can be done within a single organisation.

However, both approaches utilise the idea of embedded information in the IP packets to identify the validity of the packets.

Another issue is that under Controller-Agent model, the DDoS defence mechanism only be activated during the time of attack, thus there is no overhead under the normal circumstance. Conversely, there will always be the overhead for Capabilities-Based model.

5. Classification as suggested by (Mirkovic & Reiher, 2004)

As stated by Mirkovic & Reiher (2004), a real attack or defence might compose of several suggested categories. Also several proposed categories may not occur before in the real life. This means that a single proposed category might not relevant to one kind of real life attack unless combining with one or more proposed categories. In that case, the notification message will be displayed under a particular category.

Note that the explanation of each type of attack comes from (Mirkovic & Reiher, 2004) and will not further be cited in this section as it will make this paper unnecessary longer.

5.1 Degree of Automation

This section considers how an attacker communicate with the agent (infected) machines which beyond the scope of this paper so it will not be mentioned here.

5.2 Exploited Weakness

There are two sub-categories under this section, *Semantic* and *Brute-Force.* Since the line between them is not exactly clarify by the authors. So they will be considered as one big group.

Generally, it is the attacks that exploit a particular feature or a program bug on a victim's machine such as TCP SYN attack, and CGI request attack. For the program bugs, it is the administrator's responsibility to get an up-to-date patch, and then again out of the scope of this paper.

Under the Controller-Agent defence mechanism, this kind of attack can be handled properly given a victim notify a controller in time. In fact, it is not feasible for the victim to recognise (for instance, the multiple CGI requests) as an attack signature, because it can not distinguish between the legitimate and malicious requests.

The similar situation applied to the Capabilities-Based model, since an RTS server can not differentiate among a number of legitimate requests (probably almost all of them with malicious intention) asking for the permission.

5.3 Spoofed Source Address

If the source addresses are spoofed, the Controller-Agent system will be able to drop the spoofed packets at the edge routers where the attacking comes from. Nonetheless, a victim needs times to recognise the attack signature while the mechanism of Capabilities-Based model does not allow any malicious machines sending the spoofed packets.

5.4 Attack Rate Dynamics

This paper will not go in details for this section and will consider only two types of attack rate which are *Constant rate* and *Variable rate*.

A constant rate attack is an ordinary DDoS attack which aims to disrupt the victim's machine while a variable rate intends to degrade the victim's service over time. The different between them are the amount of packets and the time of an attack. The constant rate attack may crash a victim's machine at once by sending a large amount of packets while the variable rate attack keeps sending a portion of packets just to keep the server busy for a long time.

Under the constant rate attack, the Controller-Agent model may be able to detect and drop the packets provided the victim notify the controller in time. However, this mechanism may not be able to detect the variable rate attack since it looks like the non-harmful operation.

"Note that unlike the current Internet, a distributed attack flooding the RTS channel has no effect on already established connections with valid tokens." (Anderson et al., 2003b, p.4) The previous sentence only makes sure that the Capabilities-Based model will allocate the bandwidth for the established connections. What about the future connections?

The authors of Capabilities-Based model also mentioned that the critical mission can always keep the connection alive. Still, in the real world there might not be a critical mission. Take an example of a web server that desire to serve a customer, every one has the same priority. In this case, if a million machines (form by an attacker) would like to connect to the web server at the same time, a million tokens of permission will have to be generated somehow. Either the RTS server has a queue overflow or the destination machine unable to handle tons of the requests would happen.

Similarly, the Capabilities-Based model may not be able to detect the variable rate attack since it can not distinguish between the authentic and malicious ones.

5.5 Possibility of Characterisation

The characterised attacks can be identified by a mixture of IP header and protocol header values or maybe packet contents. For instance, the TCP SYN attack (a packet with SYN bit set in the TCP header may be fraction of an attack), etc.

The characterisable attacks are very helpful in terms of defining the attack signatures for the Controller-Agent based model which in turn leads to the immediate respond from a victim to the controller during the time of attack.

They also may be useful for the Capabilities-Based model in order to define the permission policy. For example, if a machine keeps asking for a particular type of service for an unusual period of time, the system may reduce the number of packets this machine can send for the same period of time.

5.6 Persistence of Agent Set

Variable *agent set* means the active agent machines may be different at any one time as opposed to *Constant agent set*.

The Controller-Agent model may be able to cope with both attacks efficiently (again with the assumption of not-too-late notification) since it focuses on a victim machine. Regardless of the source addresses, if a destination address of a packet matches the victim address and an attack signature matches the signature in the database, then the packet is dropped.

The Capabilities-Based model may be able to deal with the constant agent set correctly but may be not the variable agent set because the system may think that the operations from different set of agents are legitimate.

5.7 Victim Type

Application, Host, and *Resource attacks* occur on the machines, so both approaches may be able to handle them appropriately.

However, *Network* and *Infrastructure attacks* may not be prevented suitably by both mechanisms as stated by the authors that "Infrastructure attacks can only be countered through the coordinated action of multiple Internet participants." (Mirkovic & Reiher, 2004, p.46)

5.8 Impact on the Victim

This section is beyond the scope of this paper.

6. Incremental Deployment

The Controller-Agent model can be implemented as a stand alone system within an organisation. It can be set up with a small section at the beginning and extended it over time.

The Capabilities-Based model is interesting; however it is a dependent model. It requires cooperation from other organisations to make it work properly. In addition, to make it fully functional; every single organisation has to employ the same system. This is not feasible since some organisations may not want to spend extra expense in the facilities that are not necessary yet. The probability that the small organisations may be under attack is lower than the large organisations why should they bear the cost.

It is also not feasible to change something which is already working. The Internet infrastructure may not be perfect, but it is working.

7. Limitation

"… in case of severe DDoS the victim may not be in a position to send a request to its controller. In this case the victim has to contact the controller out of band and the process starts manually." (Tupakula & Varadharajan, 2003, p.279) Notice that the Controller-Agent based model may not work correctly when there is a brutal attack. This limitation makes this approach questioning since most of the DDoS attacks are severe attacks.

8. DDoS Defence Challenge

Several barriers that prevent the development of DDoS defence systems as described by (Mirkovic & Reiher, 2004) are presented below.

- A problem is hard to be handled alone.
- Under the cooperation scheme, the organisation that is not suffered from the attack will have to share the cost.
- Insufficient of DDoS attack information.
- No suitable benchmarks available.
- Large-scale testing is hard.

9. Conclusion

The limitation and assumptions they based on make the two approaches impractical to implement in the real life. Furthermore, as stated in section 8, without a good benchmark there is difficult to justify if a system is ready to be employed or not.

However, their contribution to the DDoS defence research area is valuable and this will surely help other researchers in developing the research in this area.

References

Anderson, T., Roscoe, T., & Wetherall, D. (2003a). *Perventing Internet Denial-of-Service with Capabilities*. University of Washington and Intel Research. Retrieved 23 October 2004, from the World Wide Web: http://www.cs.washington.edu/homes/djw/talks/ddos-hotnets.pdf

Anderson, T., Roscoe, T., & Wetherall, D. (2003b, November 2003). *Preventing Internet Denial-of-Service with Capabilities.* Paper presented at the Proceedings of Hotnets-II, Cambridge, MA.

Householder, A., Manion, A., Pesante, L., Weaver, G. M., & Thomas, R. (2001, October 2001). *Managing the Threat of Denial-of-Service Attacks*. CERT Coordination Center. Retrieved 23 October 2004, from the World Wide Web: http://www.cert.org/archive/pdf/Managing_DoS.pdf

Mirkovic, J., & Reiher, P. (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communications Review, 34*(2), 39-53.

Tupakula, U. K., & Varadharajan, V. (2003). A Practical Method to Counteract Denial of Service Attacks. *The Twenty-Fifth Australasian Computer Science Conference (ACSC2003), 16*, 275-284.