Assessing and Controlling Risks associated with Denial of Service (DoS) attacks on organizational networks

Abhinav Gajja, Deepam Vipinchandra Shah, Dheeraj Asnani, Edgar Daniel Perez Riveros, Johannes Leo Zutt L'Hotellier, Narendrakumar Chandrakumar, Tejas Kale

ABSTRACT

Assessment and control of information security risks have emerged as a primary mean by which organizations secure information infrastructure. Key assets are identified and protected as a part of risk management strategy. In this process, commonly Denial of Service (or DoS) attacks are overlooked. DoS service is traditionally not considered as information security risk, hence the treatment of that remains low priority. But in the recent past, several such attacks had made high profile business's web servers unavailable or un-accessible for considerable period of time, which consequently caused monitory and reputational losses. Hence now there is a substantial need to consider DoS attacks as a potential risk for information security and its assessment and treatment should be included in organization's risk management process. This paper examines the major forms of DoS attacks that are lodged on critical network infrastructure of an organization, targeting the availability and access of its critical business and IT Services and further how the risk of such attacks can be reduced or mitigated through risk management process.

Keywords: Denial of Service, Risk Management, Risk Assessment, Risk Control, Risk

Introduction

In this day and age, millions of computers across the world are connected on multiple hardware and software platforms through the internet (Hussain et.al n.d). There has been a significant increase in web based services and businesses in last two decades. Every small or big organization, ranging from small scale industries to large multinational banks, are dependent on their networks to connect to internet and provide multiple internet based services to serve various personal and professional needs for people and corporations. However, this exponential increase in the interconnectivity of computers over networks has also enabled malicious users to misuse resources and mount denial of service attacks.

Denial of service attacks have the potential to affect various areas in an organization, primarily attacking the network infrastructure and the services relying on the network. Denial of service attacks have an aggressive and menacing intrusive behavior towards the network infrastructure and its components like hosts, routers, gateways, switches or an entire network (Jamdagni et al. 2014).

Organizations have adopted various approaches to manage significant information security risks affecting their key risk assets however until recently, DoS attacks were not considered as part of this. This has been the case now as there has been an increasing shift to e-business capabilities, relying on intercommunication between computers, and 24x7 availability of services. Any loss of network or unavailability of network can cause a financial, reputational and information loss.

The information security risk management process establishes the organization's context, identifies information assets, threat and vulnerabilities, then assesses the impact and probability of threats occurring

and puts control strategies in place (Visintine, 2003; Roper, 1999). Since DoS is not considered as a direct attack on key information assets, organizations have dealt such a risk as low for a long period of time.

The major contribution of this paper is to provide a risk management perspective to DoS attacks which historically has not been considered as standard risk for information security. This paper first discusses and supports the inclusion of DoS as a threat or risk for business and its assets, attacking the seamless web based operations of the organization. Further, this literature, gives a risk management point of view to identify, analyze, evaluate and treat the threats associated with DoS attacks.

This literature review based paper is structured in the following way. The first section the paper talks about DoS attacks, the evolution of such attacks and importance of managing risks associated with DoS. The second section describes the risk management process overview and the phases form the crux of managing risks associated with DoS. The third section associates different phases like context establishment, risk assessment, risk identification, risk analysis, risk evaluation and risk treatment, with respect to denial of service attacks. Finally, we conclude the study of the paper.

Denial of Service (DoS) Attacks

Denial of Service (DoS) attack is an attempt to make machine resources or network resources unavailable for its end users for an indefinite amount of time (Krishnan & Saravanan 2010; Sarita & Saini 2013; Loukas & Öke 2010; Ogechi et al. 2013). Examples could be overwhelming the network with useless traffic, disrupting connection between specific machines, etc. When an attack is attempted by more than one individual or multiple machines or bots the attempt is called as Distributed Denial of Service (DoS) attack (Krishnan & Saravanan 2010). From an organizational perspective attacks originating from one source called DoS or those originating from multiple computers are known as DoS attack.

The concept of DoS /DoS attack was initially a fun activity for computer whiz kids when Internet was designed for openness but, such attempts gradually evolved as a powerful tool for intentional crime (Sarita & Saini 2013). Although, DoS attacks were prevalent since early 1980s (Loukas & Öke), the first occurrence of an organized crime was seen in 1990s when the flood command was used to ping a network and, the first high profile organized attack that nearly ran an organization out of business was detected in 1996 (Loukas & Öke). The traces of the attack are a few decades old but, have emerged devastatingly with intentions becoming more profitable.

DoS attacks are broadly categorized in two ways, based on their nature of operation (Ogechi et al. 2013). Firstly, the ones which use illegal data packets to hamper the services. Attackers send an unusual payload that opposes the network standards and its presence causes the operating systems to hang up the operations due to unexpected flow data loads. One of the similar and well known attack is called as Ping of Death in which, a data packet larger than standard is sent to the target systems to overflow its buffer capacity leading the systems to crash. Secondly, there are the ones which overwhelm the network with the useless data packets to utilize the complete available bandwidth of the network. These attacks are usually called as Bandwidth Attack that paralyses the communication network as seen in year 2000 with some high profile web services of Yahoo and CNN, causing a huge financial loss (Sarita and Saini 2013).

Availability of network resources and security are few major concerns with organizational network, emerging in an era of technological advancement (Ogechi et al. 2013). Every advancing step towards security wouldn't only mean the networks are safer but, would actually mean the chances of being attacked are slightly reduced. There have been more techniques discovered than ever to create lasting impact on organizations that not only affects the organization itself but, also hampers the economic development as a whole. It becomes very important for any organization to effectively manage the risks arising from DoS /DoS attacks.

Risk Management Process

'Risk' refers to the threat of loss of information or an asset that incorporates a value to an organization or an individual, and the range of threats measured in terms of impact and probability (Shedden et al. 2010).

Risk Management is the overall process of identifying and controlling risks that an organization faces (Spears and Barki 2010). It lays out basic outline of identifying, assessing and controlling the risks involved

with the existence of their information systems. Modern computing services share similar network environment features and a DoS attack aims at making these services unavailable to the end users for indefinite amount of time by attacking the infrastructure. In order for businesses to maintain confidentiality and integrity of their systems must identify all such possible risks and list them (Shedden 2010).

This paper analyses the DoS/DDoS attacks from a risk management perspective and discusses the different phases in order to develop an understanding about the risks and its control measures. Different organizations approach Risk Management differently, however the underlying concept remains the same (Shedden 2010). The basic concept, as part of the Risk Management process, includes the following phases:

- Context Establishment

Context Establishment is where an organization seeks to understand the technology infrastructure that is needed to secure its key information assets. This is achieved by examining the information assets which are vital and vulnerable to the organization thereby setting evaluative criteria for risk evaluation (Shedden et al. 2010).

- Risk Assessment

Risk Assessment process is a series of activities that aim to identify, analyze and evaluate the risks involved with DoS attacks.

  - Risk Identification: Diagnose the interfaces or points which are vulnerable to threats and identify the tools and techniques used by the attackers to exploit these vulnerabilities (Shedden et al. 2010).
  - Risk Analysis: Examine the existing controls within the organization and the subsequent consequences and likelihood of the risks occurring using either qualitative or quantitative techniques. This paper sees the impacts as Tangible and Intangible.
  - Risk Evaluation: organization compares the result of the risk analysis (i.e. the risks found that may impact the organization's information security) with the risk evaluation criteria from the context establishment phase to outline the priority of treatment.

- Risk Treatment

Further, understanding the DoS attacks and how they disrupt the communication, the last phase is to determine the countermeasures necessary to be in place to avoid attacks from hampering the infrastructure capability to serve the purpose in securing the valuable information assets.

Denial of Service (DoS): A Risk Management Perspective

Context Establishment

Context establishment is the first concrete phase that determines the strategic and organizational context, considering the organization's industry type and environment, in order to determine the scope of the risk assessment and identify the key risk assets within the scope (Shedden et. al, 2010). The focus of this paper is on DoS/DDoS attacks on organization's networks, therefore the context has a heavy focus on identifying the key components that make up the infrastructure (mostly networks), which are critical to the operation of key business and IT services.

The context establishment phase also outlines a risk evaluation criteria. The criteria includes making decisions about the particular threats that can be dealt with, and which threats can be ignored (Shedden et. al, 2010). With respect to DoS/DDoS attacks, criteria needs to be set about the threats that have the potential to affect the critical network components by which the organizations suffer the most.

Context establishment also identifies the key risk assets (Shedden et. al, 2010). Although, identification of risk asses is organization and industry specific, though from of DoS/DDoS attacks perspective risk assets would be the network infrastructure of an organization and organization and its users or customers are largely affected by unavailability of the services or access to those services if any such attack happens.

Risk Assessment

The Risk Assessment phase deals with Risk Identification, Risk Analysis, and Risk Evaluation in order to provide an overall assessment of risks and priority of risks to be treated as part of the Risk Treatment phase. The next sections talk about these from a DoS /DoS point of view.

Risk Identification

Risk Identification primarily deals with identifying critical assets, threats, and vulnerabilities using a systematic, comprehensive study of the entire organization (Shedden et. al, 2010). Once the critical assets are identified, the organization then needs to identify the threats to those assets and its vulnerabilities that can be exploited by an attacker (Shedden et. al, 2010). Although, it is organization specific, denial of service attacks mainly occur at the following levels (Sarita & Saini 2013):

- Network: Attacks (known as flood attacks) that aim to exhaust the hardware resources of network devices (e.g. router, switches).
- Operating System (OS): Attacks that aim to freeze, crash or reboot the operating system because of buffer overflow.
- Application: Attacks that bring down the services or the entire system
- Data Flooding: Attacks that transmit massive data to affect the system or device performance.
- Protocol: Attacks that initiate a number of sessions, keeping them half-open making the host run out of memory.

Due to the complexity of the organizations, whether small or large, key business and IT services depend on organization's network for its end-to-end operation (Ogechi et al., 2013). Organizational networks, proving to be the first entry point to electronic entry into the organization's infrastructure to access the services /or applications for any users or customers, play an important role in ensuring the availability of those critical assets (Ogechi et al., 2013). Security of these networks, therefore ensures the identification of key threats that exploit the physical vulnerabilities that exist in the networks (Ogechi et al., 2013). The outcome of Risk Identification phase provides a list of threats that requires to be analyzed (Shedden et al., 2010). Threats that take the form of DoS attacks, combining the above described levels, mainly fall under two main categories - Flood Attacks and malformed packet attacks.

Flood attacks intend to crash the network devices or flood systems with more traffic than they are designed to handle (Ogechi et al. 2013). Tools that are capable of causing flood attacks include the smurf flood attack, where ICMP echo packets (ping of death) are sent to broadcast addresses of the hosts. This causes significant impact to bandwidth and processing power (Ogechi et al. 2013). TCP SYN Attack and UDP flood attacks are further extensions that can result in reduction of throughput of the network and may eventually cause the shutdown of the system. (Ogechi et al. 2013; Gengen and Siaterlis 2013)

Malformed packet attacks take advantage of the bad design of the application or system's code that processes the packets. Attacks aim to send ill-formed packets and exploit the vulnerability of such application and systems. Ping of Death is one such attack in which, a data packet way more than the standard size is sent to the target system to overflow its buffer capacity leading the systems to crash (Sarita 2013 ; Ogechi et al. 2013). A 'Chargen' attack targets the UDP port 19 in order to exhaust its bandwidth. A teardrop attack is another example where some systems fail to cope correctly with packet fragmentation thereby rebooting or halting the system (Ogechi et al. 2013). The Land attack is another similar attack whose aim is to reboot or crash the system as the packet is formed with same address as the origin and destination. (Ogechi et al. 2013). The Win Nuke attack specifically targets windows operating systems by sending out-ofband data on ports thereby forcing system reboot (Ogechi et al. 2013).

There are various other threats that form a DoS attack however the main concept remains the same and asset vulnerabilities of mostly all organizations are exploited by either one or more of the threats explained above.

Risk Analysis

A Denial of Service attack has a capability to severely impact an organization's business operations and profits. The impact can significantly vary depending upon several factors such as the organization sector, the company dependency to information services and the expertise level of the attack. As discussed in previous sections, the analysis of this typology of attacks is to focus on organizations that are heavily dependent on information systems (IS) for their business operations. Disruptions even for a short period of time varying from few seconds to several minutes or hours, lead to financial or economic losses (Rao et al. 2011).

There are mainly following two types of impacts identified:

- Tangible: An impact that causes an organization a measurable loss i.e. an actual physical damage. These losses could be loss of infrastructure or capital and which could be weighed financially. But, these losses do not account for the full impact and may accompany with intangible losses.
- Intangible: These losses on the other hand are the ones which are dependent on other losses and cannot be actually measured. Loss of reputation and economic imbalance are some intangible losses.

With a security breach into businesses' information network, an organization may face loss of capital due to corrupt or missing data and also may fall in goodwill and reputation. From an impact perspective, such breaches may vary in following ways:

- Business can have its end users deterred from connection establishment. This will impact day to day business operations.
- For a stock trading institute, the firm can suffer stock price or volume variations. Prices or volumes can be in favor of an attacker dealing in particular stock or against the economy.
- Information of military operations could be accessed and leaked to use against a country.

Some similar events was experienced in the year 2000 by NASDAQ with their daily traded, volumes and stock prices, and also experienced by Yahoo, eBay and Amazon (Rao et al. 2011).With the evolution of advanced technology, attackers can perpetuate a criminal impact to any system from virtually or physically anywhere which makes it hard to trace them. In addition, a collateral damage is associated with DoS attacks since now a days, a huge amounts of data is transferred between enterprises. Hence, those companies that in some way are part of a flow of information with the company that receive the attack is highly likely to be affected (Rao et al. 2011).

Risk Evaluation

The outcome of this phase is to define the risk treatment strategies to manage the DoS risk attacks in order to allow the organization to achieve their goals and support the business strategy.

In order to execute the risk evaluation of DoS attacks, it is necessary to assess the outcomes (impact and likelihood) from the risk analysis phase according with the organizations appetite of risk. One option to develop this task is to use an economic model of risk evaluation that relate the Value-At-Risk (VAR) for each security protocol that is used by the organization. In other words VAR is a metric that represents how many components of the IS infrastructure accept to compromise by a DoS attack with a defined level of confidence (Cao 2010). However it is important to clarify that VAR is a tool to measure the risk and it could vary from one organization to another depending on the risk management context and risk appetite.

The goal of Risk Evaluation is to evaluate the risks, based on its analysis and as per the criteria from context establishment phase, thereby providing an input to Risk Treatment phase in order to determine which risk is treated first and as per what strategy (Shedden 2010). This is further explained in the next section.

Risk Treatment

One of the most important steps in the risk management process is to implement measures that can be used to control the risks that have been identified as being unacceptable (Berg 2010), as per its evaluated priority.

The treatment of risks associated with DoS attacks requires protection measures to be put in place which minimize the effects and costs of the attack.

The risks which have been identified from the Risk Analysis and Evaluation phases can be broken up into four different control strategies: Avoidance, Transference, Mitigation and Acceptance (Mirela and Maria 2008). Some strategies are more effective than others although they are not mutually exclusive and the chosen control strategy will depend on the specific scenario. The paper now discusses these scenarios in relations to DoS attacks (Amancei 2011; Berg 2010; Devine 2011; Mirela and Maria 2008;Wang et al. 2005).

Avoidance refers to not undertaking the activity which is likely to trigger the risk. To avoid DoS attacks from an infrastructure perspective network segregation and security policies such as DMZ, Firewalls and blocking unnecessary traffic can be put in place. From an application perspective implementing antivirus systems and performing patching of applications can be done to avoid potential DoS attacks. Due to the lack of understanding around DoS attacks training of staff in risk awareness and information sharing can also assist with avoiding potential DoS attacks. The disadvantage of this treatment is that it can be quite expensive and lead to loss of benefits such as innovation.

Transference refers to transferring or sharing the risk with another organization. Companies such as 'Prolexic' exist to offer mitigation services for DDoS attacks (Devine 2011). Another transference method is to obtain insurance to ensure financial certainty and combat the variable cost risk of DoS attacks. Although organizations need to keep in mind that the party transferring the risk to may not adequately manage the risk.

Mitigation refers to reducing the impact of the risk. The literature reviewed presents many different approaches and are not limited to the ones highlighted by this paper (Amancei 2011; Berg 2010; Devine 2011; Mirela and Maria 2008;Wang et al. 2005).

Applications or Infrastructure can be designed to allow for scalability which will assist in mitigating a DoS attack. Depending on the network infrastructure, proxy networks can be implemented to tolerate/mitigate DoS attacks. Proxy networks are able to improve the end users performance by increasing the delivered bandwidth and reducing latency. They can also be used to provide scalable DoS resilience to meet the size of the attack and enable the application performance to be protected (Wang et al. 2005). Scalability can also be reviewed after the Applications and Infrastructure is implemented by performing baseline testing and deciding on how much additional capacity to build in to allow for DoS attacks. However there needs to be a cost benefit analyses done to determine the allowable size. Implementing a security management framework can be done to develop an awareness of DoS attacks across the organization and allow for other processes such as Business Continuity Management (BCM) and Service Level Agreements to be updated to include clauses for DoS attacks.

Acceptance refers to understanding and accepting/retaining the risks. As risk treatment is used to reduce levels of unacceptable risk. If the cost to implement risk treatment is greater than the likelihood and impact of the risk occurring an organization would choose to accept/retain the risk unless required to for compliance reasons. Therefore some organization may choose to leave DoS vulnerabilities in their systems simply due to the costs to mitigate them. An important item to remember is that risks should continually be monitored as their likelihood and impact may change over time, therefore something which is currently acceptable may need to be mitigated in the future.

(Amancei 2011; Berg 2010; Devine 2011; Mirela and Maria 2008 ;Wang et al. 2005)

Conclusion

The basic idea behind the Internet was to have openness in communication with speed and reliability. The fast paced development of technology and its standards have attracted organizations in relying their businesses on the web services. Existence of tools and techniques to bypass the security standards governing the web networks, have evolved as a devastating way to impact an organization or an economy as a whole. We analyzed the Denial of Service attacks on the organization's networks, impacting their business profits as well as their reputation in the market. We have analyzed such attacks interrupting the end user services from the risk management perspective which focused on Identification of such threats, their analysis and evaluation and finally treatment. Denial of Service attacks or similar malicious activities can be as severe as

completely running out of business. The treatments represent as a countermeasure to avoid, transfer and mitigate risks involved in such attacks.

Overall, this paper helps in understanding the risks involved with DoS and DDoS attacks and the care that needs to be taken to protect an organization's integrity from such attacks.

References

Amancei, C 2011, 'Practical Methods for Information Security Risk Management', vol. 15, pp 151-159.

Berg, HP 2010, 'RISK MANAGEMENT: PROCEDURES, METHODS AND EXPERIENCES', vol. 1, pp. 79-94.

Bojanc, R, & Jerman-Blažič, B 2013, 'A Quantitative Model for Information-Security Risk Management', Engineering Management Journal, 25, 2, pp. 25-37

Cao, Z., Guan, Z., Chen, Z., Hu, J. & Tang, L. 2010, "Towards Risk Evaluation of Denial-of-Service Vulnerabilities in Security Protocols", Journal of Computer Science and Technology, vol. 25, no. 2, pp. 375-38

Chin Wen, C, Zaidi, I, Khor Chia, Y, & Ng Sew, L 2014, 'The Value-at-Risk Evaluation of Brent's Crude Oil Market', AIP Conference Proceedings, 1602, pp. 1118-1125

Devine, SM 2011, 'DDoS: threats and mitigation', pp. 5-12

Hussain, A, Heidemann, J, & Papadopoulos, C n.d., 'A framework for classifying denial of service attacks', Acm Sigcomm Computer Communication Review, 33, 4, pp. 99-110

Jamdagni, A, Tan, Z, He, X, Nanda, P, & Liu, R 2014, 'A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis', IEEE Transactions On Parallel & Distributed Systems, 25, 2, pp. 447-456

Krishnan, S, & Saravanan, V 2010, 'Defending Denial of Service: State Overload Attacks', International Journal Of Advanced Networking & Applications, 2, 3, pp. 719-722

Loukas, G, & Öke, G 2010, 'Protection Against Denial of Service Attacks: A Survey', Computer Journal, 53, 7, pp. 1020-1037

Mirela, G, & Maria, B 2008, 'INFORMATION SECURITY MANAGEMENT SYSTEM', Annals Of The University Of Oradea, Economic Science Series, 17, 4, pp. 1358-1363

Neumann, PG 2000, 'Denial-of-Service Attacks', Communications of the ACM, 43, 4, p. 136

Namkyun B and Namhi. K,Experimental Study of DDoS Defense System for Web Service 2013, International Journal of Security and Its Applications Vol.7, No.5, pp.147-156

OGECHI, I, INYIAMA, H, & CHUKWUGOZIEM, I 2013, 'AN ANALYSIS OF CURRENT COMPUTER NETWORK ATTACK PROCEDURES, THEIR MITIGATION MEASURES AND THE DEVELOPMENT OF AN IMPROVED DENIAL OF SERVICE (DoS) ATTACK MODEL', International Journal Of Engineering & Technology (0975-4024), 5, 2, p. 1781

Rao, A, Warsame, M, & Williams, J 2011, 'INTRADAY STUDY OF THE MARKET REACTION TO DISTRIBUTED DENIAL OF SERVICE (DOS) ATTACKS ON INTERNET FIRMS', Academy Of Accounting & Financial Studies Journal, 15, 2, pp. 59-72

Sarita, & Saini, K 2013, 'Denial of Service Attacks in Wireless Networks', International Journal Of Computer Science & Management Studies, 13, 4, p. 7

Shedden, P., Ruighaver, A.B., Ahmad, A., 2010. Risk Management Standards – The Perception of Ease of Use. Journal of Information Systems Security. 6(3)

Spears, J, & Barki, H 2010, 'USER PARTICIPATION IN INFORMATION SYSTEMS SECURITY RISK MANAGEMENT', MIS Quarterly, 34, 3, pp. 503-A5

Wang, J, Liu, X & Chien, A 2005, 'Empirical Study of Tolerating Denial-of-Service Attacks with a Proxy Network', vol. 14, pp. 51-62.

Author/s:
Gajja, Abhinav;Shah, Deepam Vipinchandra;Asnani, Dheeraj;Riveros, Edgar;L'Hotellier, Johannes;Chandrakumar, Narendrakumar;Kale, Tejas

Title:
Assessing and controlling risks associated with Denial of Service (DoS) attacks on organizational networks

Date:
2014-08

Publication Status:
Unpublished

Persistent Link:
http://hdl.handle.net/11343/42193