Research Journal of Applied Sciences, Engineering and Technology 7(13): 2711-2713, 2014
DOI:10.19026/rjaset.7.590
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: September 09, 2013 Accepted: October 19, 2013 Published: April 05, 2014

Research Article

Evaluating Energy based DDOS Attacks using Cosmic FFP and Energy Points

[1]P.C. Senthil Mahesh and [2]Paul Rodrigues
[1]Department of CSE, Dhaanish Ahmed College of Engineering, Anna University, Chennai,
[2]Department of CSE, Velammal Engineering College, Chennai, Tamil Nadu, India

Abstract: The aim of the study is to improve security and identify DDOS attacks. Security should be considered affront during software development as millions of dollars are lost due to security breaches in software. There are many kinds of security breaches and of these DDOS attacks plays a leading role and as such it is vital that new techniques be identified to combat this rising menace. In this study a new sizing techniques called energy Points are used to identify the energy based DDOS attacks.

Keywords: DDOS attacks, energy points, FFP

INTRODUCTION

DDOS stand for "Distributed Denial of Service." A DDOS attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet. Unlike Denial of Service (DOS) attacks, Denial of Service Attacks (1999) and Palmieri *et al*. (2011) in which one computer and one internet connection is used to flood the targeted resource with packets, a DDOS attack uses many computers and many Internet connections. A security report says 65% of Banks in 2012 in USA were affected by DDOS attack (www.smart-payments.info).
Stephen and Ruby (2003) classifies, DDOS attacks as:

- Volume based attacks
- Protocol attacks
- Application layer
- Energy based attacks

We are analyzing energy based attacks in the recent past, Green computing, environmental friendly computing paradigms has gained a lot of attention in the academic and industrial arena. Koomey (2007) and BONE Project (2009) estimates that ICT worldwide energy consumption amounts to more than 8% of the global electricity production and the energy requirements of data centers, storage and network equipment are foreseen to grow by 12% per year. Such a huge electricity demand will result in environmental and engineering issues and bottlenecks. Bickford *et al*. (2011) states that Energy dissipated by electronic components especially computing devices is harmful to nature. There are billions of computing devices from low end desktops to high end servers; these machines dissipate millions of watts of energy (McDowell, 2004; Moore *et al*., 2006). The energy is released in the form of Co_2 and is very harmful to the environment. Energy based Dos attacks exploit the energy consumption of applications to affect the computing devices and nature. Ricciardi *et al*. (2011), Carl *et al*. (2006) and Barroso (2007) states that researchers have made an attempt to evaluate network based DDOS attacks under power consumption perspective. Regarding energy consumptions CPU contribution to the server power consumption goes from 25 to 55% depending on the server, followed by memory and network interfaces, disks, motherboard and fans consume less energy. The energy consumption components are mainly CPU, disks, Network Interface Card (NIC). The high energy consuming component is CPU/Memory. The goal of such energy-oriented attacks is to maximize the power consumption by keeping the CPU and memory on the target systems as busy as possible, they try to add additional load on the servers by introducing a large number of service requests which deny most of the resources to the legitimate ones and keep the CPUs working at their maximum operating frequency.

Another effective way of draining more and more system energy is overloading the device's hard disks with millions of read or writes operations by forcing them to constantly operate at their maximum sustained transfer rate or to continuously spin up and down the hard disks spindle engines. This kind of attack is very common in the offending strategies of several computer viruses and Trojans that are typically able to directly run malicious codes on the target nodes. In the worst cases, the malicious agents can alter the operating system kernel or some application binary code so that

Corresponding Author: P.C. Senthil Mahesh, Department of CSE, Dhaanish Ahmed College of Engineering, Anna University, Chennai, Tamil Nadu, India, Tel.: +91 98402 12341

more energy is needed for their execution. However, the binaries altered in such a way may or not continue to behave correctly from the users' point of view. Finally, the last device/component that can be solicited is the network interface, when its energy consumption depends on the actual connection rate.

DDOS based energy attacks causes the following problems:

- **Energy costs:** This DDOS attack has direct and immediate energy expenses.
- **Neutralizing energy saving systems:** This attack is aimed at disconnecting energy saving systems from the main source.
- **Incrementing the operating temperature:** Aimed at incrementing the cooling power consumption.
- **Exhausting the power budget:** Editions of new components in the data centers may exhaust budget base lined for power consumption.
- **Incrementing dirty emissions:** It will raise both the energy consumption and the costs associated with the increased (GHG) Green House Gas emissions.

In this study a new sizing techniques called Energy Points are used to analyze the energy based attacks.

FFP

In late 1998, some members of WG12 met informally in London and decided to develop a new FSM Method, starting from basic established software engineering principles. This method is Read operations consume more energy than writes (approximately R = 13.3 μ_W/kbyte) against W = 6.67 μ_W/k byte. Entry and exit operations consume almost zero. There E and X = 0:

One Read Energy Point E_R = 13.3 μ_W/k byte
One Write Energy Point E_w = 6.67 μ_W/k byte
Total energy points EP = Total RE + Total WE in kw

A case study to demonstrate this process known as Cosmic Function Point.

Fundamental idea behind cosmic FFP is to divide the complete monolithic application into layers and components. Sizing is done by identifying the data movements in each component. These data movements are identified as Read Write Entry and Exit. The total summation of this complete size of the application. Figure 1 illustrates the overall relationship between the four types of data movement, the functional process to which they belong and the boundary of the measured software.

FFP's and energy consumptions related as FFP depends on data movements in the component boundary. The following section deals in detail on counting energy points.

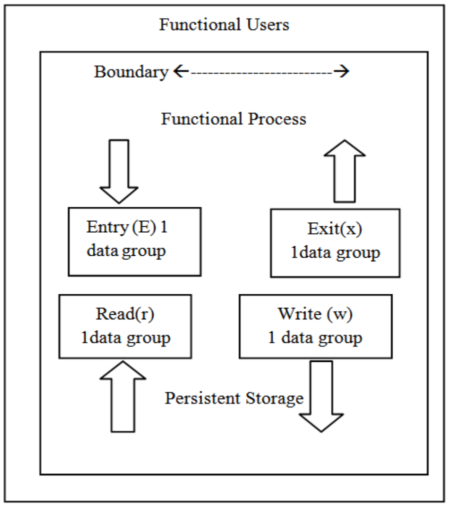

Fig. 1: Details the four types of data movement and their relationship with the functional process and data groups

CASE STUDY

Application of energy points, For more details Reference (CRS_RUP case study). The Use case system explains course registration system with a state-of the-art on-line system that allows students and professors access through the Internet. The requirements as supplied have been reorganized in the following sequence:

- Login (by all users)
- Maintain professor information (by the registrar)
- Select courses to teach (by professors)
- Maintain student information (by the registrar)
- Register for courses (by students)
- Monitor for course (by the application)
- Close registration (by the registrar)
- Submit grades (by professors)
- View report card (by students)

Let us see an example for Login Information.

Login:
Brief description: This use case describes how a user logs into the Course Registration System. The actors starting this use case are Student, Professor and Registrar.

Flow of events: The use case begins when the actor types his/her name and password on the login form.

Basic flow-login: The system validates the actor's password and logs him/her into the system. The system displays the Main Form and the use case ends.

Alternative flows:
Invalid name/password: If in the basic flow the system cannot find the name or the password is invalid,

Table 1: The functional user requirement

ID of req.	Process descriptions	Triggering event	Sub-process desc
1.2	Logon	Login by user id and password	Enter name and password
		Read name and password	User data
		Display error messages	Messages

Table 2: The data movement

Data group	Data movement type	Cfsu	∑Cfsu	FFP	Attribute	EP
System	E	1			0	
User data	R	1			2	2x kb/E_R
Messages	X	1			0	
		3				

an error message is displayed. The actor can type in a new name or password or choose to cancel the operation, at which point the use case ends.

Table 1 and 2 shows the size of User ID and password may vary depending upon the machine configuration. For our Illustration, let us assume the User ID and password of size 10 bytes each. Let us further assume around 100 records of user id and password. Therefore the total read energy points is 1cfsu = (10×100+10×100).

E_R = Attribute * Total Kb/E_R = (10×100 + 10×100) /1000 = 2 E_R as per the definition 1 Read operation is 13.3 μ_W/k byte. Therefore 2×13.3 = 26.6 μ_W/k byte. The same way we can calculate for Write Energy points.

Ep should be monitored continuously to check for any deviation in the energy consumption. If any deviation is observed, energy attack can be suspected and remedial measures can be taken.

CONCLUSION

Energy point is a useful technique to monitor, Change in Energy level for specific application. By using the Energy points concept we can Prevent DDOS Based Energy Level attacks and reduce the Co_2 Emission, which is the goal of Green computing.

REFERENCES

Barroso, U.H., 2007. The case for energy-proportional computing. IEEE Comput., 40: 33-37.

Bickford, J., H.A. Lagar-Cavilla, A. Varshavsky, V. Ganapathy and L. Iftode, 2011. Security versus Energy Trade-offs in Host-based Mobile Malware Detection. MobySis 11, Bethesda, Maryland, USA.

BONE Project, 2009. WP 21 topical project green optical networks: Report on year 1 and updated plan for activities. NoE, FP7-ICT-2007 216863, BONE Project.

Carl, G., G. Kesidis, R.R. Brooks and S. Rai, 2006. Denial-of-Service attack-detection techniques. IEEE Internet Comput., 10(1): 82-89.

Denial of Service Attacks, 1999. Retrieved from: http://www.cert.org/tech_tips/denialofservice.html, (Accessed on: 2010.11.10).

Koomey, J.G., 2007. Estimating total power consumption by servers in the U.S and the world. Final Report, Lawrence Berkeley National Laboratory, Stanford University.

McDowell, M., 2004. Understanding Denial-of-service Attacks. National Cyber Alert System, Cyber Security Tip ST04 -015.

Moore, D., G.M. Voelker and S. Savage, 2006. Inferring internet denial of service activity. ACM T. Comput. Syst., 24(2): 115-139.

Palmieri, F., S. Ricciardi and U. Fiore, 2011. Evaluating network based Dos attacks under the energy consumption perspective. Proceeding of the International Conference on Broadband and Wireless Computing, Communication and Applications, pp: 374-379.

Ricciardi, S., D. Careglio, U. Fiore, F. Palmieri, G. Santos-Boada and J. Solé-Pareta, 2011. Analyzing local strategies for energy-efficient networking. Proceeding of the IFIP TC 6th International Conference on Networking (NETWORKING, 2011). Valencia, Spain, LNCS 6827, pp: 291-300.

Stephen, S. and L. Ruby, 2003. Taxonomies of Distributed Denial of Service Networks, Attacks, Tools and Countermeasures. Retrieved from: http:// www.ee.princeton.edu/~rblee/DDoS%20Survey%20Paper_v7final.doc.