Techniques to Detect DoS and DDoS Attacks and an Introduction of a Mobile Agent System to Enhance it in Cloud Computing

Abdelali Saidi[1], Elmehdi Bendriss[2], Ali Kartit[3], Mohamed El Marraki[1]

[1]LRIT associated unit to CNRST (URAC 29), Faculty of Sciences, Mohammed V University, PB 1014, Rabat, Morocco
[2]UFR SI3M, ENSIAS PB. 6624 - Al Irfane, Rabat 10112, Morocco
[3]LTI, departement TRI, ENSAJ Chouaib Doukkali University, El Jadida, Morocco

***Abstract* — Security in cloud computing is the ultimate question that every potential user studies before adopting it. Among the important points that the provider must ensure is that the Cloud will be available anytime the consumer tries to access it. Generally, the Cloud is accessible via the Internet, what makes it subject to a large variety of attacks. Today, the most striking cyber-attacks are the flooding DoS and its variant DDoS. This type of attacks aims to break down the availability of a service to its legitimate clients. In this paper, we underline the most used techniques to stand up against DoS flooading attacks in the Cloud.**

***Keywords* — Cloud computing; DoS DDoS; Mobile agent.**

I. Introduction

Cloud computing is, without any doubt, the future of IT systems. It brings along some advantages that can attract any type of companies. For example, Cloud gives high computing capabilities as a service (without buying the hardware) at a cheap cost, etc.

A. Cloud features

To be more attractive, the Cloud has to ensure the following features [1]:

- On-demand self-service: give the consumer the possibility to provision power of computing as needed without any human interaction;
- Broad network access: make the Cloud available from any type of network using any client platform;
- Resource pooling: the Cloud uses a multi-tenant model to serve multiple consumers. The resources have to be pooled to maximize the number of consumers;
- Rapid elasticity: make the consumers think that the resources are unlimited and available anytime they want more;
- Measured service: Cloud systems must monitor resources usage appropriate to the type of service. This can be done by using a metering capability.

B. Service models

To select a Cloud solution, the consumer must begin by deciding the appropriate service model. Following, the most popular services that Cloud offers:

- Software as a service (SaaS): the users can rent a set of applications running on the Cloud by the provider;
- Platform as a service (PaaS): the users have the service of implementing their applications on the Cloud and run it;
- Infrastructure as a service (IaaS): the users can rent a specific infrastructure from the Cloud and run any kind of applications even the operating system.

C. Deployment model

After the service model, the future consumer must think about how he would benefit from the Cloud. Here we have four models of the Cloud deployment:

- Private Cloud: The Cloud infrastructure will be used by a single consumer. The infrastructure can be maintained in the client's local or by a third party;
- Community Cloud: the Cloud will be used by a set of consonants clients that share a common interest. Also, the infrastructure can be deployed in the clients' locals like it can be managed by a third party;
- Public Cloud: the Cloud infrastructure is deployed by a Cloud provider for any client who wants to consume;
- Hybrid Cloud: is the composition of two or more deployment model.

II. Security issues in Cloud Computing

Basically, Cloud computing is a good IT infrastructure well maintained. Its main objective is to discharge clients from the infrastructure management. This will help the clients to focus only on their activities. However, besides security issues of IT systems, the Cloud brings some more specific issues.

A. Data security

In a traditional IT infrastructure, data is kept locally. And the owner does whatever it takes to ensure its confidentiality. Using the Cloud to store its data can seem doubtful since the client doesn't have any idea of how the data will be processed and where. Normally, the Cloud provider must ensure that even its own administrator won't have any way to reach the data or even log onto the clients' accounts.

B. Network security

When an organization trusts a Cloud provider, it must be aware of that the Internet will be used to transfer data from and to the Cloud. Internet is the most unpredictable network in the world; cyber-attacks are launched around the clock in it. Among the risks that threat every network communication we have:

- Packet Sniffing: it permits to intruders to analyze the traffic;
- Man in the Middle: it exploits a vulnerability in TCP/IP stack to deflect the traffic;
- IP Spoofing: it sends packets with a forged source IP address;
- Port scanning: it helps to detect network services running on a

DOI: 10.9781/ijimai.2017.4312

distant host;
- Network penetration: it permits to log on unauthorized session.

C. Data location

The first thing a potential Cloud client must do is to ask for a certification about the location where services will be stored. This can create a very annoying problem for the data confidentiality if the data is stored in a country where the regulation gives the right to some organizations to look onto the private data without the owner permission. For example, in the USA, USA PATRIOT ACT gives the government services access to data stored in any server.

Additionally, the Cloud is a multi-tenant system. It means that the computational resources will be used by many clients. The Cloud provider must ensure a perfect data isolation. Every client must be at ease regarding its data accessibility.

D. Web applications security

Accessing its Cloud requires a connection from the Internet and a terminal provided with a web client. It means that the applications deployed on the Cloud are mostly based on web platforms. This brings to the Cloud some issues related to the web shape. The open web application security project (OWASP) released a document about the ten most critical web application security risks [2]:

- Injection;
- Broken authentication and session management;
- Cross-site scripting;
- Insecure direct object references;
- Security misconfiguration;
- Sensitive data exposure;
- Missing function level access control;
- Cross-site request forgery;
- Using components with known vulnerabilities;
- Unvalidated redirects and forwards;

E. Virtualization issues

Since the virtualization is mostly used in the Cloud environments, it adds also some issues. The SANS institute have summarized some mistakes to avoid when using the virtualization [3]:

- Misconfiguring virtual hosting platforms, guests and networks;
- Failure to properly separate duties and deploy least privilege controls;
- Failure to integrate into change/lifecycle management;
- Failure to educate other groups, particularly risk management and compliance staff;
- Lack of availability or integration with existing tools and policies;
- Lack VM visibility across the enterprise;
- Failure to work with an open ecosystem;
- Failure to coordinate policy between VMs and network connections;
- Failure to consider hidden costs;
- Failure to consider user-installed VMs.

III. DoS and DDoS detection techniques

Several techniques have been proposed to mitigate DoS and DDoS attacks. These techniques can be classified into three types:

- Filtering techniques;
- Trace back techniques;
- Intrusion detection.

A. Hop-count filtering (HCF)

HCF is a filter dedicated to classify traffic based on the number of hops [4]. Initially, this filter has been used to handle IP spoofing attacks, but since most DoS attacks techniques send traffic with spoofed IP addresses, the filter can be useful also to detect DoS and DDoS attacks.

To calculate the number of hops that a packet has done before we receive it, we look into the TTL field. The value that we retrieve is simply the number of hops that the packet had the right to do before reaching its destination. To calculate the number of hops, we need to have an idea about its initial TTL value. According to [5] the initial value can be 30, 32, 60, 64, 128 or 255, and it depends on the operating system. And since the diameter on the Internet between two distant terminals rarely exceeds 30 hops [6] we can say that the initial TTL value is the smallest initial value that is superior to the received TTL.

Mukaddam et al [7] have enhanced this technique by adding a new parameter: RTT (Round Trip Time) to the considerations of the filter. This parameter give to the filter the possibility to make the difference between some packets that have done the same number of hops but different times of the round trip. Another enhancement of this method was given by Wang et al [8] proposing to implement the filter on the gateways. Maheshwari et al [9][10] underline the problem of computing time because of the large amount of packets that the filter can receive. To adjust this problem, they propose a technique called DPHCF-RTT that will create collaboration between the gateways and taking the different initial TTL values that may have been used into consideration.

B. Confidence based filtering (CBF)

CBF is a technique that helps to detect every deviation of the traffic from its normal shape [11]. It is also an enhancement of the HCF technique which considers different fields in the packet. CBF is based on some correlation between these fields that can be noticed after a period. This correlation builds a normal profile and the CBF filter tries to detect every deviation from it.

Fig. 1 illustrates how the CBF filter works.

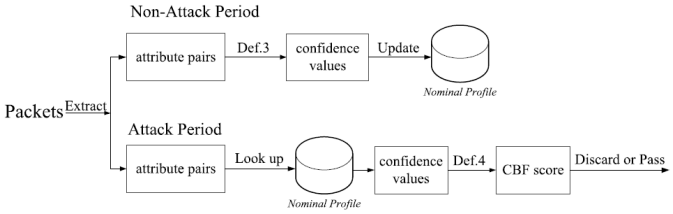

Fig. 1. CBF filter working

Priyanka et al [12] propose an enhancement of this filter by adding a new field in the packet header. This field will be called "confidence value" and it will be filled by every gateway it passes by. This will eventually give a modification into the IHL field. Mamtesh et al [13] propose an enhancement where the CBF will work neighboring a HCF filter.

C. Random port hopping (RPH)

RPH is a technique that permits to a server to change the port number when communicating with a legitimate client. Firstly, this technique was used to sidetrack spies. Lee et al [14] used this technique to mitigate DoS and DDoS attacks.

To guess the port number on which the server will wait for a packet, the client and the server must pre-share a key and divide time to slots. In the beginning of every slot, the client has to calculate the port number using an algorithm and the pre-shared key.

Zhang et al [15] propose a solution to make the server able to communicate with different clients in the same time. Lu et al [16] supported this technique by studying the rate of success when detecting attacks.

D. IP traceback

IP traceback is a technique that permits to track down spoofed packets to determine their true origin. There are different ways to track back a packet:

- Link testing: this method begins from the default gateway of the attack target and tries to detect the previous hop one by one recursively. This method consider that the attack remains active until we find the originator;
- Logging: this method tries to log every packet that has passed through a key gateway from the Internet. With this technique, the attack may be detected even if the attacker had finished. But, we have to consider the resources that will be consumed on the routers just to log the packets;
- ICMP traceback: Every router will randomly take a packet from 20 000 one and send an ICMP message to the owner of the destination IP address. This will help the destination to have an idea about the route that a packet has taken before being received.

E. Mobile agent techniques

A mobile agent is a program which can move from a computer to another autonomously and continue its execution. It brings some advantages that make mobile agents suitable for building intrusion detection systems like:

- Computation bundles:
- Parallel processing:
- Dynamic adaptation:
- Tolerant to network faults:
- Flexible maintenance:

Several works adopt mobile agents to face DoS and DDoS attacks. Akyazi and Uyar proposed four methods; three of them use mobile agents [17]. Each method use Snort like a sensor. The contribution of the mobile agent platform is reducing bandwidth usage by moving data analysis near to the source of the intrusion data. Zamani and al [18] propose a mobile agent platform inspired from danger theory to build an intrusion detection system resilient to DDoS attacks. This system represents a model of immunization of distributed intrusion detection system. Armoogum and mohamudally [19] underlined the issues of most IP traceback solutions such as high false positives, enormous storage requirements at routers and huge additional data in network traffic. To mitigate these problems, a mobile agent platform was proposed for real-time traceback of distributed attacks. Demir and al [20] proposed an enhancement of this type of solutions by demonstrating how a careful placement of agents can improve an earlier DDoS detection.

IV. A mobile agent system to enhance DoS and DDoS detection in Cloud Computing

Our mobile agent system begins by classifying virtual machines into several sets. Each set of VMs will be monitored by a mobile agent. Eventually, the number of VMs in a set affects the quality of the mobile agent service. The mobile agent has to move from a virtual machine to another following a priority metering capability. This capability helps to define the order of VMs but can be broken if one of them is in a critical situation. Thus, we placed sensors in every VM to keep eye on the hardware usage. If a sensor detects an overtaking it sends an event to the mobile agent. This latter will have to move to this VM and the order will be reset [21].

A. VMs order

When the mobile agent of a set of VMs moves, it will choses the next VM following the order of priority. Assuming a set having five VMs (A, B, C, D and E) with priorities respecting that order. If the mobile agent is currently working on B and receives an event from D the mobile agent will move to B and the order will be like:

D -> B -> C -> E -> A

Thus, the mobile agent choses the next VM based on the time of last visit.

B. Components of the mobile agent

The mobile agent must analysis a VM, decide if something wrong in it, respond a proper reaction and be aware of some states of the other VMs. To handle all of this, the mobile agent must contain the following components:

- Listening module: this part of the mobile agent will receive the sensors traps;
- Analyze module: this one studies information in the environment logs to find suspicious data;
- Decision module: this one compares the suspicious data the attacks' scenarios we have in our database to decide if it is an attack;
- Response module: this latter chose the best reaction to execute automatically in order to limit damages.

C. Scenarios

Different scenarios that our mobile agent can handle:

- Multiple VMs fall in critical condition simultaneously: when the mobile agent is proceeding in VM which is in a critical condition and receives another trap from another one, the mobile agent will create another instance of it and send it to this latter VM. Every agent clone must send the result of its work to the parent agent.
- A distributed attack that targets multiple VMs in deferent sets: if there is a malicious data that can be part of coordinated attack reaching VMs in different sets, the agent who suspects this must send a trap to every mobile agent. These latters have to take this in consideration.

V. Conclusion

In this paper, we presented valuable works on the detection of DoS and DDoS. We noted the "HCF filter" and its generalization "the CBF filter" that both try eliminate packets with spoofed IP addresses, the RPH that try to divert the attacker, the IP traceback that tries to detect the source of the attack and the mobile agent systems that try to give another way to detect DoS and DDoS attacks in the Cloud. Then, we introduced our mobile agent system and depicted its way to handle things for different VMs. We are still working on the implementation of our solution and studying other scenarios that the mobile agent can run into.

References

[1] National Institute of Standards and Technology. « The nist definition of cloud computing ». 2011.

[2] OWASP. « The ten most critical web application security risks ». 2013. http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf

[3] SANS Institute. « Top Virtualization Security Mistakes (and How to Avoid

Them) ». 2009. https://www.sans.org/reading-room/whitepapers/analyst/top-virtualization-security-mistakes-and-avoid-them-34800

[4] Cheng Jin, Haining Wang, and Kang G. Shin. Hop-count filtering: "An effective defense against spoofed ddos traffic". In Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS '03, pages 30–41, New York, NY, USA, 2003. ACM

[5] The Swiss Education and Research Network. "Default ttl values in tcp/ip". 2002.

[6] Bill Cheswick, Hal Burch, and Steve Branigan. Mapping and visualizing the internet. In Proceedings of the 2000 USENIX Annual Technical Conference, pages 1–12, 2000.

[7] A. Mukaddam and I.H. Elhajj. Round trip time to improve hop count filtering. In Broadband Networks and Fast Internet (RELABIRA), 2012 Symposium on, pages 66–72, May 2012.

[8] Xia Wang, Ming Li, and Muhai Li. A scheme of distributed hop-count filtering of traffic. In Wireless Mobile and Computing (CCWMC 2009), IET International Communication Conference on, pages 516–521, Dec 2009.

[9] R. Maheshwari, C.R. Krishna, and M.S. Brahma. « Defending network system against ip spoofing based distributed dos attacks using dphcf-rtt packet filtering technique ». In Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on, pages 206–209, Feb 2014.

[10] C.R. Krishna R. Maheshwari. « Mitigation of ddos attacks using probability based distributed hop count filtering and round trip time ». International Journal of Engineering Research and Technology (IJERT), 2(7), 2013.

[11] Wanchun Dou, Qi Chen, and Jinjun Chen. A confidence-based filtering method for ddos attack defense in cloud environment. Future Gener. Comput. Syst., 29(7):1838–1850, September 2013.

[12] Priyanka Negi, Anupama Mishra, and B. B. Gupta. « Enhanced CBF packet filtering method to detect ddos attack in cloud computing environment ». CoRR, abs/1304.7073, 2013.

[13] Mamtesh and Rajender Nath. "An improved defense mechanism based on packet filtering to mitigate ddos attack in cloud computing environment". IJCA, 5, 2015.

[14] H.C.J. Lee and V.L.L. Thing. « Port hopping for resilient networks ». In Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th, volume 5, pages 3291–3295 Vol. 5, Sept 2004.

[15] Zhang Fu, M. Papatriantafilou, and P. Tsigas. « Mitigating distributed denial of service attacks in multiparty applications in the presence of clock drifts ». Dependable and Secure Computing, IEEE Transactions on, 9(3):401–413, May 2012.

[16] Yue-Bin Luo, Bao-Sheng Wang, and Gui-Lin Cai. Effectiveness of port hopping as a moving target defense. In Security Technology (SecTech), 2014 7th International Conference on, pages 7–10, Dec 2014.

[17] U. Akyazi and A.S.E. Uyar. « Distributed intrusion detection using mobile agents against ddos attacks ». In Computer and Information Sciences, 2008. ISCIS '08. 23rd International Symposium on, pages 1–6, Oct 2008.

[18] M. Zamani, M. Movahedi, M. Ebadzadeh, and H. Pedram. « A ddos-aware ids model based on danger theory and mobile agents ». In Computational Intelligence and Security, 2009. CIS '09.International Conference on, volume 1, pages 516–520, Dec 2009.

[19] M. Duraipandian and C. Palanisamy. « An intelligent agent based defense architecture for ddos attacks ». In Electronics and Communication Systems (ICECS), 2014 International Conference on, pages 1–7, Feb 2014.

[20] O. Demir, B. Khan, G. Ben Brahim, and A. Al-Fuqaha. « Optimizing agent placement for flow reconstruction of ddos attacks ». In Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International, pages 83–89, 1July 2013.

[21] Abdelali Saidi, El Mehdi Bendriss, Ali Kartit and Mohamed El Marraki. "A Mobile Agent System to Enhance DoS and DDoS Detection in Cloud Computing". European Journal of Scientific Research. Volume 131 No 2. April, 2015.

Abdelali Saidi is a PhD Student in Networks Security at Mohammed V University in Morocco since 2011. He has a Master degree in Systems and Computer Networks from Ibn Tofail University. He teaches in the area of computer science (Linux, IP Networks, and Information Security) since 2012. His main interest is Cloud Computing Security researches. abdelali.saidi@gmail.com

Elmehdi Bendriss received his PhD degree in Networks Security from ENSIAS, Mohamed V University in 2014. He also holds MSC in IT from the same University and an engineering diploma from INPT since 2002. He's now working on systems and networks Security and especially in Cloud computing. He's been teaching in the area of Computer Science (Systems and Networks administration, Information Security, Virtualization) since 2003. bendriss@gmail.com

Ali Kartit received the PhD degree in Computer Science (November 2011) Specialty Security of Computer Networks. He graduated from the University Mohamed V Faculty of Rabat. Now, He works as an assistant professor at the University Chouaib Doukkali of El Jadida. The author has developed a rich and diverse experience of over 14 years in the computer world, including 10 years in technical and vocational education as a computer network trainer and manager module "computer network security notions" and 4 years in the corporate world as Administrator of computer networks and Head of the park. The author is a certified Cisco and Microsoft Exchange Server 2003. His research area covers security policies of firewalls, the Intrusion detection systems (IDS) and cloud security. alikartit@gmail.com

Mohamed El Marraki received the Doctorate and the Doctorate of the State degrees in algebra and number theory, respectively, from the Bordeaux University, France in 1991, and the Mohammed V-Agdal University, Rabat, Morocco, in 1996; he also received the Doctorate in "dessin d'enfant theory" from the Bordeaux University, France in 2001. He joined Mohammed V University, Rabat, Morocco, in 1996, first as an associate professor and full Professor since 2000, where he is teaching. Over 19 years, he developed teaching and research activities covering various topics of Mathematics, cryptography and graph theory which allow him to advise 5 PhD theses and publish over 60 journal papers and conference communications. Mohamed El Marraki is member of the several "Scientific Program Committee" of the International conference. He is a member of several mathematical and computer science journals. marraki@fsr.ac.ma