Chemical Technology, Control and Management

Volume 2018
Issue 3 *SPECIAL ISSUE 4-5*

Article 8

10-19-2018

Analysis challenge protection of information from attacks and construction of a formal model for protecting network traffic.

M.M Karimov
Director of the State Testing Center under the Cabinet of Ministers of the Republic of Uzbekistan, Address: Bogi Shamol street, 12, 100202, Tashkent city, Republic of Uzbekistan, dr.mmkarimov@rambler.ru

Sh.R Gulomov
PhD of Providing Information Security Department Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Address: Amir Temur street, 108, 100200, Tashkent city, Republic of Uzbekistan, sherhisor30@gmail.com

Analysis challenge protection of information from attacks and construction of a formal model for protecting network traffic.

Cover Page Footnote

Tashkent State Technical University, SSC «UZSTROYMATERIALY», SSC «UZKIMYOSANOAT», JV «SOVPLASTITAL», Agency on Intellectual Property of the Republic of Uzbekistan

ISSN 1815-4840
CHEMICAL TECHNOLOGY. CONTROL AND MANAGEMENT
2018, Special issue №4-5 (82-83) pp.33-37. https://doi.org/10.34920/2018.4-5.33-37
International scientific and technical journal
journal homepage: https://uzjournals.edu.uz/ijctcm
Since 2005

ANALYSIS CHALLENGE PROTECTION OF INFORMATION FROM ATTACKS AND CONSTRUCTION OF A FORMAL MODEL FOR PROTECTING NETWORK TRAFFIC

M.M.Karimov[1], Sh.R.Gulomov[2]

[1]Director of the State Testing Center under the Cabinet of Ministers of the Republic of Uzbekistan,
Address: Bogi Shamol street, 12, 100202, Tashkent city, Republic of Uzbekistan
E-mail: [1]dr.mmkarimov@rambler.ru
[2]PhD of Providing Information Security Department Tashkent University of Information Technologies named after Muhammad al-Khwarizmi,
Address: Amir Temur street, 108, 100200, Tashkent city, Republic of Uzbekistan
E-mail: [2]sherhisor30@gmail.com

Abstract: *In this paper a formal model for protecting information from DDoS attacks, allows to improve the efficiency of computer networks, taking into account the interaction of detection modules and the use of formal set-theoretic constructions are proposed.*

Keywords: *DDoS attacks, SYN Flood, HTTP Flood, MAC-flood, VoIP flood, DNS amplification, Smurf-attack.*

Introduction

Currently, the basic concepts of cyber security are accessibility, integrity and confidentiality. Distributed Denial of Service (DDoS) attacks affects the availability of information resources. DDoS is considered successful if it has led to inaccessibility of the information resource. The success of the attack and the impact on the target resources are different in that the impact damages the victim.

There are several methods for increasing the power of DDoS attacks, but the basic idea is almost the same. The attacker performs IP spoofing and sends fake requests to the vulnerable UDP-server. Not knowing that the requests are fakes, the server is preparing a response. The problem occurs when the server sends thousands of replies to the attacked host, thereby causing its denial of service. Attacks using the enhancement methods are very effective, since the size of the response packets exceeds the size of the request packets. As a result, an attacker, even with insignificant resources, can implement a powerful DDoS attack. Researchers regularly record such attacks, but new previously unknown methods, cybercriminals use extremely rarely. This includes, in particular, the Memcached attack, which involves augmenting the attack using memcached UDP. In recent days, the number of attacks Memcached began to grow rapidly.

1. The problems protection of information from networks attacks

Currently, the following trends in the development and use of modern information technology (IT) are observed:

– the complexity of the computer system software;

– collection and storage of large information databases on electronic media;

– direct access to the resources of the computer system of a large number of users of different categories and with different access rights in the system;

– aggregation in the general information array of various access methods;

– increase in the cost of resources of computer systems;

– the use by most public and private organizations of special anti-virus programs as a means of security;

– wide use of the Internet, etc.

On the Internet for a long time, not only using e-mail, but also doing business there, doing trade on the exchange, making purchases, making private negotiations, exchanging confidential information with colleagues. On hard drives lies everything "that is acquired by excessive work": ideas, diaries, workings, collections of valuable materials, confidential information. This is tens, if not hundreds of gigabytes of valuable information, which is often much more expensive than the computer itself, and even completely invaluable. But the situation today is such that every minute computer information can be compromised. Here are some reasons for the loss of information (from practice):

- theft of information;
- "work" of scammers;
- disks in the hard disk;
- hardware or software failures;
- damage to information storage devices;
- virus attacks and so on.

The most surprising thing is that most of those who faced such troubles were far from green beginners, only yesterday they sat at the computer and therefore poorly familiar with its basics [1]. Businessmen, traders, students and even web designers, they are all in the so-called "risk zone", because they have really valuable information for them, but most of them - through their fingers look at computer security issues.

Attacks at the operating system level. Adherence to an adequate security policy is a much more difficult task for this level. the internal structure of modern operating systems is extremely complex. The success of the hacker attack algorithm depends on the architecture and configuration of the specific operating system that is the object of this attack. The task of the hacker is to find a weak point in a particular system of protection, and not to organize an effective attack on operating systems only with the help of sophisticated tools based on the latest achievements of science and technology. The simpler the attack algorithm, the more likely it is to be completed without errors and failures. Attacks to which almost any operating system can be subjected:

– password theft;

– spying on the user when he enters the password;

– obtaining a password from the file in which this password was saved by the user;

– search for a password that users, not to forget, write on calendars, in notebooks or on the back of computer keyboards;

– theft of the external medium of the password information;

– full search of all possible password options;

– selection of the password for the frequency of occurrence of symbols and bigrams, using the dictionaries of the most frequently used passwords, involving knowledge of a specific user;

– scanning of computer hard disks;

– garbage collection;

– abuse of authority;

– run the program on behalf of the user who has the necessary credentials, or as a system program;

– replacing a dynamically loadable library used by system programs, or changing environment variables that describe the path to such libraries;

– modification of the code or data of the operating system's subsystem;

– denial of service;

– capture of resources.

It is important to note that it is impossible to completely eliminate the threat of hacking a computer system at the OS level, regardless of the measures taken.

Therefore, the security policy should be carried out so that, even overcoming the protection created by the operating system, the hacker could not cause serious damage.

*Attacks at the level of database management systems***.** To protect the operating system is much more difficult than the database management

system (DBMS), but to gain access to the DBMS files, most hackers do this with the help of OS facilities, and it is necessary to crack the computer system protection at the OS level. However, if you use a DBMS that does not have enough reliable security mechanisms, or a poorly tested version of the DBMS containing errors, or if errors were made by the DBMS administrator when determining the security policy, it becomes quite possible to overcome the security implemented at the DBMS level by the hacker. There are two specific scenarios for attacks on DBMS, to protect against which it is required to apply a special.

In the first case, the results of arithmetic operations on numeric fields of the DBMS are rounded down, and the difference is summed up in some other DBMS record.

In the second case, the hacker gets access to the DBMS records fields, for which only statistical information is available. The idea of a hacker attack on a DBMS is to tricky formulate a query so that the set of records for which statistics are collected consisted of only one record.

Attacks at the level of network software. Network software (NS) is the most vulnerable, because the communication channel through which messages are transmitted is most often not protected, and anyone who can access this channel, respectively, can intercept messages and send their own.

At the level of free software, the following hacker attacks are possible:

- LAN segment;
- interception of messages on the router;
- creating a false router;
- Imposing messages;
- denial of service.

2. A formal model for protecting network traffic from DDoS attacks

This is a simplified classification by protocols and by the mechanism of action used to transmit data in computer networks [2-3], the vulnerabilities of which are used by hackers, organizing attacks. In Table III is given the classification of DDoS attacks in the computer networks.

Table 1

Classification of DDoS attacks in the computer networks

By protocols	**On the mechanism of action**		
	The first group is attacks aimed at overflowing the communication channel, in other words, various types of flooding.	The second group which has fewer types of denial-of-service attacks, are attacks that exploit the network protocol stack vulnerability	The third group is DDoS attacks on the application layer
TCP HTTP UDP ICMP	1. DNS amplification 2. Fragmented UDP flood 3. ICMP flood 4. NTP amplification 5. NTP flood 6. Fragmented ACK flood 7. Ping flood 8. UDP flood 9. UDP-flood using a botnet 10. VoIP flood 11. Flood with media data 12. Attack with ICMP ECHO broadcast packets 13. Attack with broadcast UDP packets 14. Fragmented ICMP flood 15. DNS flood 16. Other attacks with amplification (amplification)	1. SYN Flood 2. IP null attack 3. Attack of fake TCP sessions 4. TCP null attack 5. Attacks with modification of the TOS field 6. ACK / PUSH ACK flood 7. RST / FIN flood 8. SYN-ACK flood 9. TCP null / IP null attack 10. Attack of fake TCP sessions with multiple SYN-ACKs 11. Attack with the substitution of the address of the sender with the address of the recipient 12. Attack with redirection	1. HTTP flood 2. Application failure attack 3. HTTP flood with single requests 4. Attack with fragmented HTTP packets 5. HTTP flooding with single sessions 6. Session attack. Attack with slow sessions

		of traffic of high-loaded services 14. Attack of fake TCP sessions with multiple ACKs	

In Table 2 is presented DDoS-attacks are possible on each of the seven levels.

Table 2

Comparative analysis of possible attacks on the OSI model

OSI model		Examples of DDoS technologies	Consequences of DDoS attack
7	Application layer	PDF GET requests, HTTP GET, HTTP POST, HTTP flood, Slowloris Attack (web site forms: login, photo / video upload, feedback confirmation)	Lack of resources. Excessive consumption of system resources by services on the attacked server.
6	Presentation layer	Underlying SSL requests: checking encrypted SSL packages is very resource intensive, attackers use SSL for HTTP attacks on the victim server	Attacked systems may stop accepting SSL connections or automatically rebooting
5	Session layer	The attack on the Telnet protocol uses the weak points of the Telnet server software on the switch, making the server inaccessible	It makes it impossible for the administrator to control the switch
4	Transport layer	SYN-flood, Smurf-attack (attack ICMP-requests with changed addresses)	Reaching the limits of the width of the channel or the number of permissible connections, disruption of the network equipment
3	Network layer	ICICMP flood - DDoS attacks on the third layer of the OSI model, which use ICMP messages to overload the bandwidth of the target network	Reducing the throughput of the attacked network and the possible congestion of the firewall
2	Data link layer	MAC-flood - overflow with data packets of network switches	Data flows from the sender to the recipient block all ports
1	Physical layer	Physical destruction, physical disruption to work or management of physical network assets	Network equipment is unusable and needs repair to resume work

The formal model of information of protection from DDoS attacks is described using formal set-theoretic constructions [4-5].

Let's imagine a model of information protection from DDoS attacks in the form of a tuple:

$$M =< IP, OP, HN, HC, IA, U > \quad (1)$$

where IP – Incoming packets; OP – Outgoing packets; HN – a set of nodes (hosts) of the computer network; HC – set of connections between nodes of the computer network; IA – scenario of the implementation of the attack; U – a parameter characterizing the user's actions.

Figure 1 shows a formal model of information of protection from DDoS attacks.

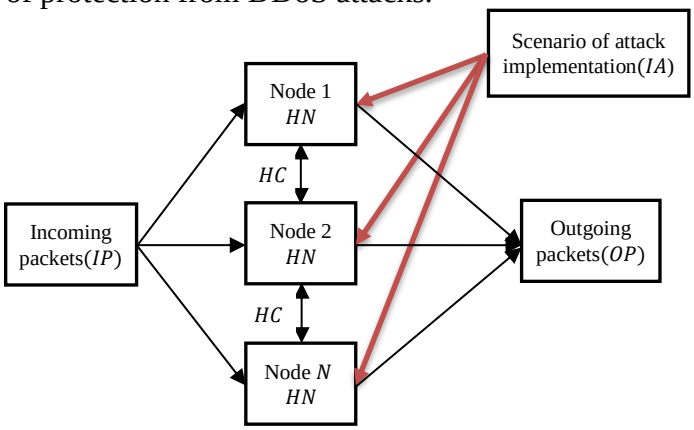

Figure 1. ***Formal model of information protection from DDoS attacks***

The set of HN nodes is given in the form of a tuple of elements:

$HN =< \text{Equipment}, \text{Role}, \text{Software}, \text{Hardware}, \text{Function} >$

where Equipment – multiple types of equipment corresponding to the node of the computer network; Role – set of functional roles of the node; Software –a variety of software components used by the nodes; Hardware – a set of hardware components used by the nodes; $\text{Function: Role} \rightarrow \text{Software}$ – function that implements mapping of the set of functional roles of a node to a set of software components.

The software and / or hardware component of the software is a protocol that implements a set of rules and allows for the connection and exchange of data between two or more devices included in the network.

The set of HC links between the nodes of the computer network in the context of various protocols is described as follows: it is assumed that the nodes $1,2, \ldots N$ of the network are connected by some protocol if there is at least one non-empty finite sequence with the initial node 1 and the end node 2 through which will be a message.

The scenario for implementing the attack contains:

$$IA =< FA_{\text{fuction attack}}, AA_{\text{against attack}}, LA_{\text{legitimate activities}}, WAA_{\text{warning about attack}}, RTA_{\text{response to attack}} > \quad (2)$$

where $FA_{\text{fuction attack}}$ – the functioning of the DDoS attack; $AA_{\text{against attack}}$ – Deterrence of DDoS attacks and counteracting attacks; $LA_{\text{legitimate activities}}$ – legitimate activity of the computer network; $WAA_{\text{lwarning about attack}}$ – Warning about DDoS attacks; $RTA_{\text{response to attack}}$ – response to DDoS attacks.

In this case, each intermediate scenario becomes the object of subsequent decomposition.

Scenarios $FA_{\text{fuction attack}}$ contain sub-scenarios for the spread of the DDoS attack, its management and the implementation of attacks.

Scenarios $AA_{\text{against attack}}$ contain sub-scenarios to counteract the spread of DDoS attacks, counteracting its management and countering the implementation of attacks.

Scenarios $LA_{\text{legitimate activities}}$ are designed to generate legitimate traffic patterns.

Scenarios $WAA_{\text{lwarning about attack}}$ are designed to mitigate the consequences of an attack on a victim.

Scenarios $RTA_{\text{response to attack}}$ are designed to detect and respond to DDoS attacks.

Conclusion

With the classification of DDoS attacks in the computer networks and comparative analysis of possible attacks on the OSI model, a formal model for protecting network traffic from DDoS attacks is proposed, which allows more efficient protection of networks from unauthorized traffic.

REFERENCES

1. Kotenko and E. Doynikova, “Security assessment of computer networks based on attack graphs and securi ty events”, Bali, Indonesia, LNCS, vol. 8047. Springer Verlag, pp. 462-471, April 2014,
2. A.Behrouz Forouzan, “Data Communications and Networking”, 5th Edition McGrawHill Forouzan series, NewYork USA, 2007, p. 1134.
3. William Stallings, “Data and Computer Communications” (10th Edition), International Edition, 2013, p. 912.
4. D. van Dalen: Logic and Structure (4th extended ed. Revised). (Springer Verlag, Berlin, 2008).
5. M. Rathjen: Metamathematical Properties of Intuitionistic Set Theories with Choice Principles. In: S.B. Cooper, B.Lowe, A. Sorbi (eds.): New Computational Paradigms: Changing Conceptions of What is Computable (Springer, New York, 2008) P.287312.