Journal scientific and applied research, vol. 17, 2019
International Journal

Original Contribution ISSN 1314-6289

IMPLEMENTATION OF TCP SYN FLOOD CYBER ATTACK IN THE COMPUTER NETWORK AND SYSTEMS

Petar Kr. Boyanov

DEPARTMENT OF MANAGEMENT OF SECURITY SYSTEMS, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712,115, UNIVERSITETSKA STR,

E-MAIL: peshoaikido@abv.bg

ABSTRACT: *In this paper implementation of SYN Flood cyber attack in the computer network and systems is performed.*

KEY WORDS: *DDOS, Education, Exploit, Flood, Information resources, LAN, Scanner, Security, SYN, Vulnerability, Windows 7, Windows 8.*

1. Introduction

This cyber attack is characterized in that it is an attack directed entirely at a computer machine or a computer network for the purpose of reducing the performance or completely blocking the operation of the computer machine. In this way, these cyber attacks prevent authorized and legitimate users from gaining access to a computer or computer network. The symptoms of SYN Flood cyber attacks are associated with the inability to access a particular website or all certain websites, an increase in the amount of false emails received and too slow network performance [1], [3], [4], [6], [9], [11], [13].

Most cybercriminals use Distributed Denial of Service (DDoS) cyber attack, which uses a large number of compromised hosts (zombies) who are ordered to attack the victim's remote computer machine. Thus Denial of Service cyber attacks are divided into [12], [14], [15], [16]:

- Cyber attacks aimed at bandwidth.
- Flood cyber attacks with requests for system services.
- Cyber-attacks with sending packets with "SYN" (SYN FLOOD) flag activated.
- ICMP flood cyber attacks;
- Cyber attacks on clients with equal access, etc.

Once a cybercriminals execute this attack, the consequences for the organization can be [2], [5], [7], [8], [9], [10], [12]:

- Causing large financial losses.
- Completely shutting down or blocking the organization's Internet connection.
- Completely isolate the organization from the Internet.

This paper is structured as follows. First, in section 2, detailed parameter’s configuration for SYN Flood attack is performed. The achieved results are presented in section 3. The final conclusions and recommendations in section 4 are made.

2. Experiment

The science experiment in a specialized university computer lab in the Faculty of Technical Sciences at Konstantin Preslavsky was made. All of the hosts in this lab were connected each other in Local Area Network (LAN). The investigated computer network was consisted of 10 hosts and each of them was using an additional 150 Mbps High Gain Wireless USB Adapter TL-WN721N. In the computer lab a Cisco RV315W Wireless-N VPN Router has been used and configured. The Dynamic Host Configuration Protocol (DHCP) in the router’s configuration has been configured on purpose each host in this computer lab to obtain a valid IPv4 addresses, network mask, DNS server addresses and default gateway. The network ID of this LAN is 192.168.1.0/24. The research host was configured with the following IPv4 address 192.168.1.118/24.

The operating system installed on the attacking computer is Kali Linux 4.12.0-kali-amd64#1 SMP Debian x86-64 GNU/Linux. The purpose of the science experiment is to execute the SYN flood cyber attack against target host in local area network. The utility ping for this purpose will be used.

3. Results

Flooding by sending countless many ICMP requests with activated only SYN bit is one of the most serious type of Denial of Service cyber attacks. In practice this cyber attack is known as the SYN Flood.

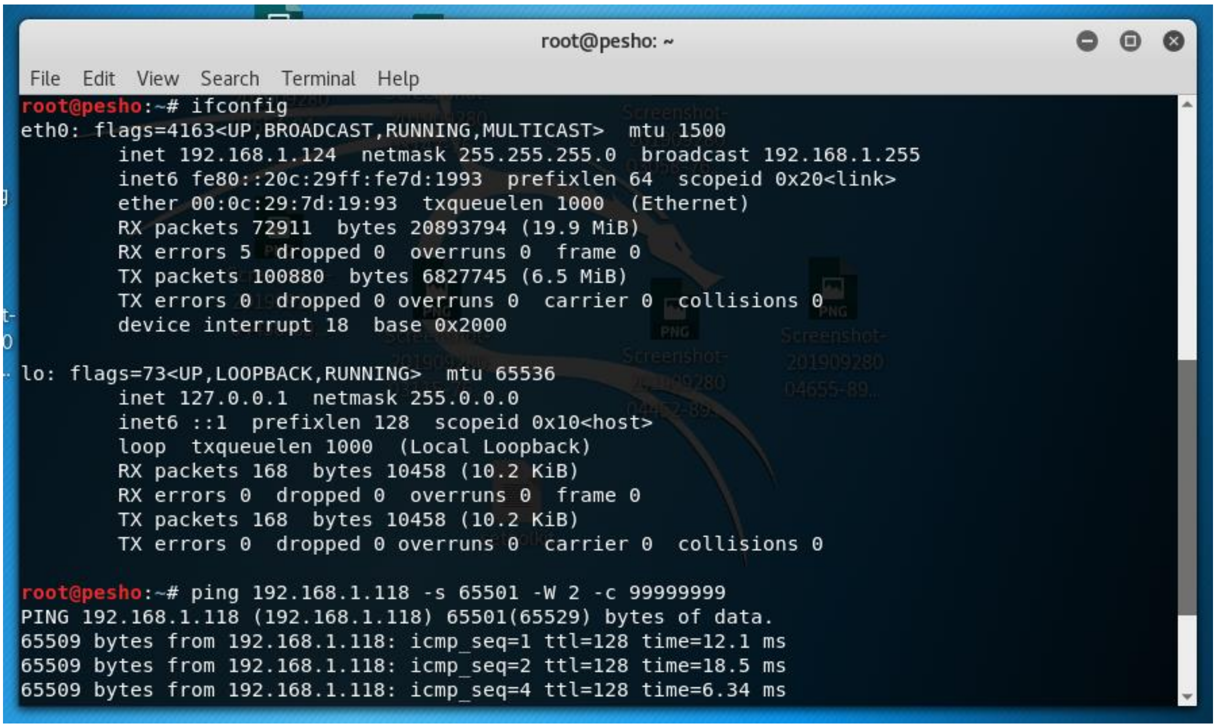
The cyber attack’s parameters are configured as follows:

- IPv4 address of the computer victim - 192.168.1.118.
- IPv4 address of the attacking host - 192.168.1.124.
- Size of each packet - 65501 bytes.
- Request timeout - up to 2 millisecond.
- Total number of requests to be sent - 99999999. The attack under a Linux based operating system (Kali Linux) was started. This is shown on fig.1.

The consequences that can result in the victim's computer machine are blocking the network card and necessary restarting the entire computer machine.

If this attack is done very often, it may cause the network card to be completely blocked and damaged.

The SYN Flood cyber attacks aims to overflow the network buffer with only SYN-enabled network packets. This means that the three-way handshake process over TCP is not completed and the cybercriminals continue to send packets with only activated SYN flag to the victim machine. The malicious users doesn’t send ACK flag back to the victim machine and therefore these connections are half-opened and consuming hardware (machine) resources. As a result, a legitimate user can no longer establish a network connection with the victim's host because of started SYN Flood cyber attack. If this attack is combined with sending countless requests under the ICMP protocol, then the victim machine can be blocked even faster.



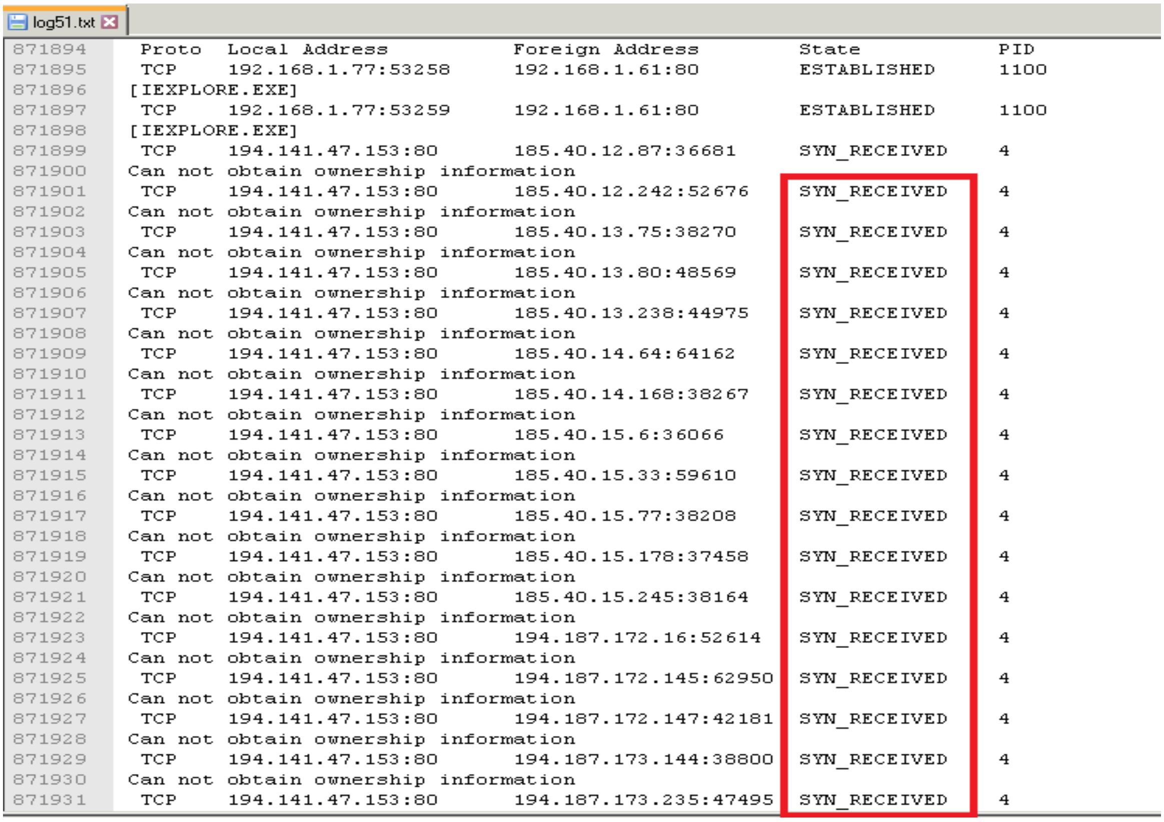
```
root@pesho:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.124  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe7d:1993  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7d:19:93  txqueuelen 1000  (Ethernet)
        RX packets 72911  bytes 20893794 (19.9 MiB)
        RX errors 5  dropped 0  overruns 0  frame 0
        TX packets 100880  bytes 6827745 (6.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 18  base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 168  bytes 10458 (10.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 168  bytes 10458 (10.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@pesho:~# ping 192.168.1.118 -s 65501 -W 2 -c 99999999
PING 192.168.1.118 (192.168.1.118) 65501(65529) bytes of data.
65509 bytes from 192.168.1.118: icmp_seq=1 ttl=128 time=12.1 ms
65509 bytes from 192.168.1.118: icmp_seq=2 ttl=128 time=18.5 ms
65509 bytes from 192.168.1.118: icmp_seq=4 ttl=128 time=6.34 ms
```

Fig. 1. Started SYN Flood cyber attack

In the computer space, some of the most malicious software programs used to perform denial-of-service cyber-attacks are:

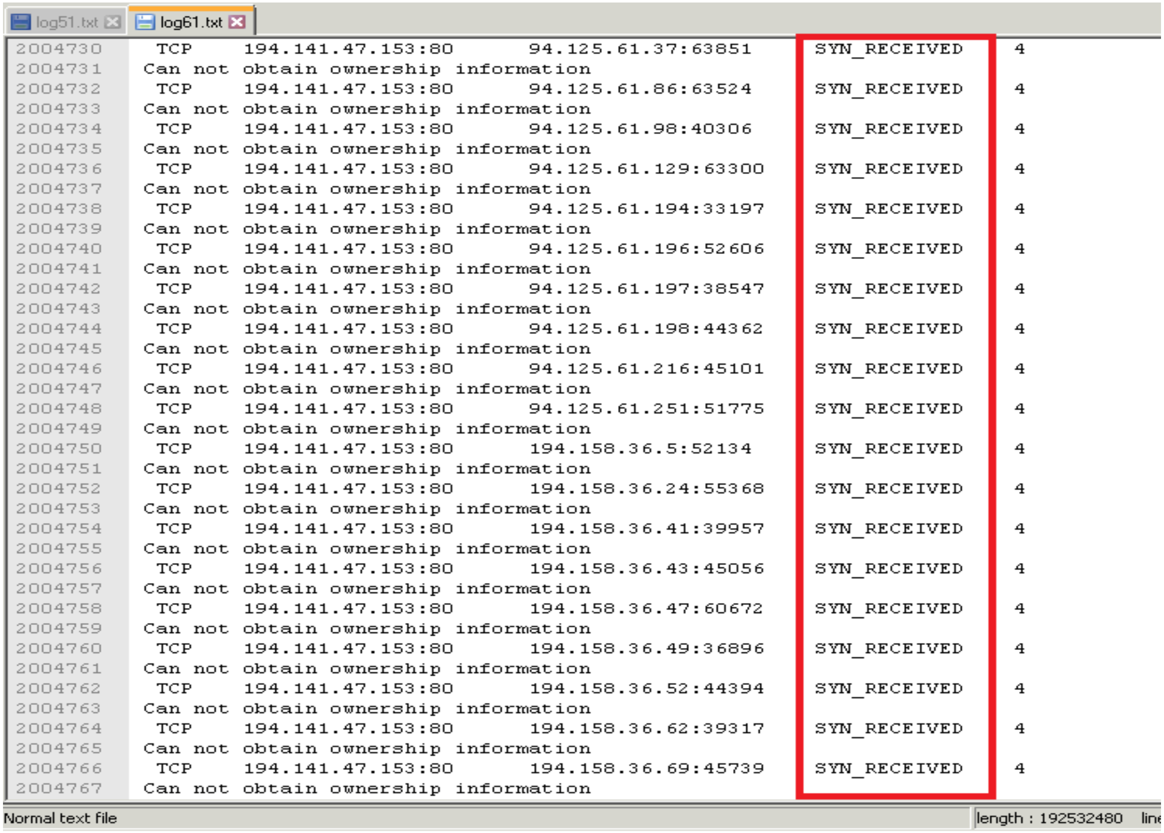
- Sprut.
- DoS HTTP.
- PHP DoS.
- Janidos.
- Supernove.
- BanglaDoS and etc.

This scientific article also shows an additional real cyber attack directed against TCP port 80 on host with IPv4 address 194.141.47.153. Four websites are hosted on this server operating system and at the same time they are exposed to real cyber-attack of type SYN Flood. In this case the cyber attack is created using a botnet in order to mask the IP addresses of the infected devices. These devices are working as zombies and the cybercriminals redirect all their network connections to this server machine.



```
 Proto  Local Address          Foreign Address        State           PID
 TCP    192.168.1.77:53258     192.168.1.61:80        ESTABLISHED     1100
[IEXPLORE.EXE]
 TCP    192.168.1.77:53259     192.168.1.61:80        ESTABLISHED     1100
[IEXPLORE.EXE]
 TCP    194.141.47.153:80      185.40.12.87:36681     SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      185.40.12.242:52676    SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      185.40.13.75:38270     SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      185.40.13.80:48569     SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      185.40.13.238:44975    SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      185.40.14.64:64162     SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      185.40.14.168:38267    SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      185.40.15.6:36066      SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      185.40.15.33:59610     SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      185.40.15.77:38208     SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      185.40.15.178:37458    SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      185.40.15.245:38164    SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      194.187.172.16:52614   SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      194.187.172.145:62950  SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      194.187.172.147:42181  SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      194.187.173.144:38800  SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80      194.187.173.235:47495  SYN_RECEIVED    4
```

Fig. 2. SYN Flood cyber attack against real server machine



```
 TCP    194.141.47.153:80       94.125.61.37:63851        SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       94.125.61.86:63524        SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       94.125.61.98:40306        SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       94.125.61.129:63300       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       94.125.61.194:33197       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       94.125.61.196:52606       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       94.125.61.197:38547       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       94.125.61.198:44362       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       94.125.61.216:45101       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       94.125.61.251:51775       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       194.158.36.5:52134        SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       194.158.36.24:55368       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       194.158.36.41:39957       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       194.158.36.43:45056       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       194.158.36.47:60672       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       194.158.36.49:36896       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       194.158.36.52:44394       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       194.158.36.62:39317       SYN_RECEIVED    4
Can not obtain ownership information
 TCP    194.141.47.153:80       194.158.36.69:45739       SYN_RECEIVED    4
Can not obtain ownership information
```

Fig. 3. SYN Flood cyber attack against real server machine

NOTE: All of the scientific experiments and studies in this paper were conducted in a specialized computer lab at the Faculty of Technical Sciences at the Konstantin Preslavsky University of Shumen, consisting of several hosts. Everything illustrated and explained in this paper is for research purposes and the authors are not responsible for any misuse.

4. Conclusion

The Certified Ethical Hackers, Networks Security Officers and System Administrators have to take the following security actions and mechanisms, such as:

- Exclusion of all unnecessary system services from the operating system.
- Uninstall all unused software programs.
- Scan files received from external organizations and organizations.
- Configuring multiple firewalls in the organization's demilitarized zone (server farm) and configure multiple systems to detect intrusion after the demilitarized zone.
- Use of special software analysts to detect vulnerabilities and weaknesses in the configuration and settings of the employee's operating system. The network operating system of the routers in the organization must also be scanned. The most useful analyzers that can be used are: Advanced Mail

Bomber, Apache JMeter, GFI LanGuard, Mail Bomber, Nessus, Nmap and Webserver Stress Tool.

References:

[1] Bhattacharyya, D., Alisherov, F. Penetration testing for hire. International Journal of Advanced Science and Technology, 2009, vol. 8, pp. 1-8.

[2] Fox, E., Bush, J., Ashley, S., Webb, I. Common Hacking Tools for Linux and Windows, 2002, CS 581 Semester Project, pp. 1-17.

[3] Marquez, J. An Analysis of the IDS Penetration Tool: Metasploit. The InfoSec Writers Text Library, 2010, pp. 1-6.

[4] Moore, H. D. Metasploitation. In CanSecWest Security Conference, 2006, pp. 1-28.

[5] Shrestha, N. Security Assessment via Penetration Testing: Network and System Administrator's Approach: Security, Network and System Administrator, Penetration Testing, Master's thesis, 2012, pp. 1-98.

[6] Hristov, H., Scanning for vulnerabilities in the security mechanisms of the hosts in the academic institutions and government agencies, Mathematical and Software Engineering, ISSN 2367-7449, Vol. 4, No. 1, 2018, pp. 1-6.

[7] Linko Nikolov, Krasimir Slavyanov, „On the contemporary cybersecurity threats“, I st CONFSEC 2017, 11-14.12.2017, Borovets, ISSN Print: 2603-2945, ISSN Online: 2603-2953, стр. 142-144; url: http://confsec.eu/sbornik/2-2017.pdf.

[8] Nikolov G. L., Fetfov M. O., Borisova R. A., Security concerns in javascript coding, MATTEX 2018, Volume 2, part 2, Conference proceeding, v. 2, pp. 27 – 31, Section Communication and Computer Technologies, ISSN: 1314-3921.

[9] Nikolov G. L., Wireless network vulnerabilities estimation, International Scientific Journal “Security & Future”, Vol. 2 (2018), Issue 2, pg(s) 80-82; WEB ISSN 2535-082X; Print ISSN 2535-0668.

[10] Nikolov, L., Slavyanov, V., Network infrastructure for cybersecurity analysis. International scientific conference 2018, “Vasil Levski” National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2018, ISSN 2367-7902.

[11] Nikolov, L., Slavyanov, Kr., On the contemporary cybersecurity threats, Security & Future,Vol. 1 (2017), Issue 3, ISSN 2535-0668, pp.111-113.

[12] Tsankov, Ts., Denev D. R., Use in Internet of Protocols Transport Layer Security and its now-deprecated predecessor Secure Sockets Layer. Annual of Konstantin Preslavski University of Shumen, Vol. VIII E, 2018.

[13] Parashkevanova, G., Tsankov, Ts., Cybercrime as the main contemporary threat to large organizations, Conference proceedings Mattex 2016, ISSN 1314-3921.

[14] Savov, I., Edin pogled varhu sashtnostta na kiberprestapleniyata, spisanie „Politika i sigurnost”,VUSI, 2017, ISSN 2535-0358, s. 36-47.

[15] Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.

[16] Tasheva N. Zh., Bogdanov A. R., Anonymous communication system in cyberspace using tor protocol, Proceedings of Scientific Conference 2014 - Defense Technologies,Faculty of Artillery, Air Defense and Communication and Information Systems, 2014, ISBN 978-954-9681-49-9, pp. 259-265.