ინფორმატიკა

IP-ფრაგმენტაციაზე დაფუძნებული საფრთხეების ანალიზი და დაცვის მექანიზმები განაწილებულ ქსელურ სისტემებში

მიხეილ დონაძე
ელ-ფოსტა: mikheil.donadze@bsu.edu.ge
ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტი

ბესიკ ბერიძე
ელ-ფოსტა: b.beridze@bsu.edu.ge
ბათუმის შოთა რუსთაველის სახელმწიფო უნივერსიტეტი

აბსტრაქტი: კორპორაციული საინფორმაციო ქსელებისა და საერთაშორისო სატელეკომუნიკაციო ტექნოლოგიების სწრაფი განვითარების პირობებში, განაწილებული გამოთვლითი სისტემების უსაფრთხოების უზრუნველყოფა სახელმწიფო, სახელისუფლებლო და ძალოვანი უწყებებისთვის კრიტიკულ გამოწვევად იქცა. თანამედროვე შეტევების აღმოჩენის სისტემებისა (IDS) და პაკეტების ფილტრაციის ტექნოლოგიების უმეტესობა ვერ ახორციელებს ფრაგმენტირებული დატაგრამების სრულფასოვან ანალიზს. აღნიშნული ხარვეზი მნიშვნელოვნად ზღუდავს კომპიუტერული შეტევების დროულ იდენტიფიცირებასა და მავნე ტრაფიკის ბლოკირებას, რაც ქმნის ნოყიერ ნიადაგს რამდენიმე ფრაგმენტზე განაწილებული „მომსახურებაზე უარის“ (DoS/DDoS) ტიპის შეტევების რეალიზაციისთვის.

სტატიაში გაანალიზებულია ისეთი სპეციფიკური საფრთხეები, როგორიცაა Tiny Fragment Attack და გადაფარვითი ფრაგმენტების (Overlapping Fragments) გამოყენების სცენარები. კვლევის მიზანს წარმოადგენს IP-ფრაგმენტაციის თავისებურებების სიღრმისეული ანალიზი და მასშტაბირებადი საინფორმაციო-გამოთვლითი სისტემების დაცვის ეფექტური, დინამიური მექანიზმების შემუშავება.

საკვანძო სიტყვები: კომპიუტერული ქსელები, IP ფრაგმენტაცია, TCP, ქსელური უსაფრთხოება, DoS შეტევები

1. შესავალი.

დღეს თანამედროვე მსოფლიოში თანამედროვე საინფორმაციო საზოგადოებაში ქსელური და გამოთვლითი სისტემები კრიტიკულ ინფრასტრუქტურას წარმოადგენს. ინფორმაციული სისტემების გლობალიზაცია და ჰეტეროგენული გარემო, ფუნქციონალური შესაძლებლობების ზრდასთან ერთად, მნიშვნელოვნად ზრდის ქსელური შეტევებისა და საფრთხეების დონეს. ინფორმაციული უსაფრთხოების უზრუნველყოფა დღეს სახელმწიფო და კორპორაციული სტრუქტურების ერთ-ერთ მთავარ გამოწვევად იქცა.

თანამედროვე ქსელების ერთ-ერთი ძირითადი მოთხოვნაა მასშტაბირება - სისტემის უნარი, შეინარჩუნოს წარმადობა და უსაფრთხოება ქსელის სირთულის ზრდის მიუხედავად. ქსელების მრავალფეროვნების გამო, შუალედურ არხებს ხშირად აქვთ განსხვავებული MTU (Maximum Transmission Unit), რაც IP-ფრაგმენტაციის მექანიზმის გამოყენებას აუცილებელს ხდის. ეს პროცესი გულისხმობს დიდი პაკეტების დანაწევრებას და მათ შემდგომ აწყობას დანიშნულების წერტილში.

მიუხედავად პრაქტიკული აუცილებლობისა, IP-ფრაგმენტაცია ქმნის სერიოზულ უსაფრთხოების რისკებს. ხშირად, ფილტრაციის სისტემები და მარშრუტიზატორები სრულყოფილად ამოწმებენ მხოლოდ პირველ ფრაგმენტს, რაც თავდამსხმელებს საშუალებას აძლევს, გვერდი აუარონ დამცავ მექანიზმებს და განახორციელონ მომსახურებაზე უარის (DoS/DDoS) ტიპის

შეტევები. არსებული „დამცავი გარსები“ (Gateway) ყოველთვის ეფექტური არ არის, რადგან განაწილებული ქსელის ელემენტები ადვილად აღმოსაჩენია საინფორმაციო ნაკადების ანალიზით. გამოვლენილმა ხარვეზებმა და დინამიური მასშტაბირების პირობებში არსებულმა საფრთხეებმა განაპირობა წინამდებარე კვლევის აქტუალობა. სტატიის მიზანია IP-ფრაგმენტაციის თავისებურებების ანალიზის საფუძველზე, ჩამოყალიბდეს მასშტაბირებადი საინფორმაციო-გამოთვლითი სისტემების დაცვის ეფექტური მექანიზმები [1,2,3].

2. ძირითადი ტექსტი.

IP ფილტრაციის დროს, იმ შემთხვევაში, როდესაც მარშრუტიზატორის შესასვლელზე შემოდის ფრაგმენტირებული დატაგრამა, მარშრუტიზატორი ამოწმებს მხოლოდ დატაგრამის პირველ ფრაგმენტს (პირველი ფრაგმენტი განისაზღვრება IP-სათაურის დაძვრის ველის მნიშვნელობით Fragment Offset=0). თუ პირველი ფრაგმენტი არ აკმაყოფილებს გატარების პირობებს, ის განადგურდება. დანარჩენი ფრაგმენტების უსაფრთხოდ გატარება შეიძლება, არ დაიხარჯება ფილტრის გამოთვლითი რესურსები, რადგან პირველი ფრაგმენტის გარეშე დატაგრამა მაინც ვერ აიწყობა დანიშნულების კვანძზე [5,6].

ფილტრის კონფიგურირებისას ქსელურ ადმინისტრატორს ხშირად აქვს ამოცანა: დაუშვას კავშირები ინტერნეტის TCP-სერვისებთან, ინიცირებული შიდა ქსელის კომპიუტერების მიერ, მაგრამ აკრძალოს შიდა კომპიუტერების კავშირების დამყარება გარე კომპიუტერებთან ამ უკანასკნელების ინიციატივით. დასმული ამოცანის გადასაწყვეტად ფილტრი კონფიგურირდება გარე ქსელიდან შემომავალი TCP-სეგმენტების გატარების აკრძალვაზე, რომლებსაც აქვთ დაყენებული SYN ბიტი ACK ბიტის არარსებობისას; სეგმენტები ამ ბიტის გარეშე დაუბრკოლებლად გატარდება დაცულ ქსელში, რადგან ისინი შეიძლება ეკუთვნოდეს კავშირს, რომელიც უკვე დამყარდა შიდა კომპიუტერის ინიციატივით.

ფილტრაციის კონფიგურირებისას ხშირად გამოიყენება მიდგომა, რომლის მიხედვითაც გარე ქსელიდან შემომავალი TCP-სეგმენტები SYN ალმით და ACK ალმის გარეშე იბლოკება. თუმცა, ფრაგმენტაციის გამოყენებით შესაძლებელია აღნიშნული შეზღუდვის გვერდის ავლა.

Tiny Fragment Attack (RFC 1858) ეფუძნება TCP-სეგმენტის ხელოვნურ ფრაგმენტაციას ისე, რომ TCP-სათაურის მხოლოდ პირველი 8 ოქტეტი მოხვდეს პირველ ფრაგმენტში.

ბოროტგანმზრახველი ქმნის ხელოვნურად ფრაგმენტირებულ დატაგრამას TCP-სეგმენტით, ამასთან პირველ ფრაგმენტს აქვს მონაცემთა ველის მინიმალური ზომა - 8 ოქტეტი (შეგახსენებთ, რომ ფრაგმენტების ზომები მითითებულია 8-ოქტეტიან ბლოკებში). დატაგრამის მონაცემთა ველში იმყოფება TCP-სეგმენტი, რომელიც იწყება TCP-სათაურით. პირველ 8 ოქტეტში TCP-სათაურში არის გამგზავნისა და მიმღების პორტების ნომრები და Sequence Number ველი, მაგრამ ალმების მნიშვნელობები არ მოხვდება პირველ ფრაგმენტში. შესაბამისად, ფილტრი გაატარებს დატაგრამის პირველ ფრაგმენტს, ხოლო დანარჩენ ფრაგმენტებს ის არ შეამოწმებს.

ამგვარად, SYN-სეგმენტის შემცველი დატაგრამა წარმატებით მიეწოდება დანიშნულების კვანძს და აწყობის შემდეგ გადაეცემა TCP მოდულს [5,6].

ნახ. 1-ზე ნაჩვენებია 2 ფრაგმენტისგან შემდგარი დატაგრამის მაგალითი (IP-სათაურები გამოყოფილია ნაცრისფრად). ამ ფრაგმენტში მოთავსებულია მხოლოდ პორტების ნომრები და Sequence Number ველი, ხოლო ალმები (მათ შორის SYN) გადადის მეორე ფრაგმენტში. შედეგად,

ფილტრი ატარებს პირველ ფრაგმენტს, ხოლო დანიშნულების კვანძზე TCP-სეგმენტი წარმატებით აიწყობა და მუშავდება.

IP Header MF = 1, Fragment Offset = 0	
Source Port	Destination Port
Sequence Number (SN)	

IP Header MF = 0, Fragment Offset = 1								
Acknowledgment Number (ACK SN) = 0								
Data Offset	Reserved	-	-	-	-	S Y N	-	Window
Checksum								Urgent Pointer = 0
Options								Padding

ნახ. 1. TCP-სეგმენტის ფრაგმენტაციის მაგალითი, სადაც TCP-სათაურის პირველი 8 ოქტეტი მოთავსებულია პირველ ფრაგმენტში, ხოლო SYN ალამი - მეორე ფრაგმენტში

აღწერილი მეთოდი ცნობილია როგორც *Tiny Fragment Attack* (RFC 1858) და ეფუძნება TCP-სათაურის ველების განზრახ გადატანას არაპირველ ფრაგმენტებში. მეთოდი, ეფექტურია მხოლოდ გარკვეულ შემთხვევებში და არ წარმოადგენს უნივერსალურ საშუალებას ფილტრაციის სხვა პირობების გასავლელად. ამის მიზეზია ის, რომ TCP-ის სათაურში (ისევე როგორც სხვა სატრანსპორტო პროტოკოლების შემთხვევაში) ყველა „საინტერესო ველი“ მოთავსებულია სათაურის პირველ 8 ოქტეტში და, შესაბამისად, ვერ გადაინაცვლებს მეორე ფრაგმენტში.

ამ ტიპის შეტევისგან დაცვის მიზნით, ფილტრაციის მარშრუტიზატორმა, ბუნებრივია, არ უნდა შეამოწმოს დატაგრამების არაპირველი ფრაგმენტების შინაარსი. ასეთი მიდგომა პრაქტიკულად გაუტოლდება დატაგრამების აწყობას შუალედურ კვანძზე, რაც მნიშვნელოვნად გაზრდის გამოთვლით დატვირთვას და შესაძლოა სწრაფად ამოწუროს მარშრუტიზატორის რესურსები [4].

სრული დაცვის უზრუნველსაყოფად საკმარისია გამოყენებულ იქნეს ერთ-ერთი შემდეგი მიდგომა:

- **არ გაიაროს ის დატაგრამები**, რომელთათვისაც *Fragment Offset = 0* და *Protocol = 6 (TCP)*, ხოლო მონაცემთა ველის ზომა ნაკლებია გარკვეულ ზღვრულ მნიშვნელობაზე (მაგალითად, 20 ოქტეტი), რაც აუცილებელია ყველა „საინტერესო ველის“ სრულად გადასაცემად;
- **არ გაიაროს ის დატაგრამები**, რომელთათვისაც *Fragment Offset = 1* და *Protocol = 6 (TCP)*. ასეთი დატაგრამის არსებობა მიუთითებს, რომ TCP სეგმენტი სპეციალურად არის ფრაგმენტირებული სათაურის გარკვეული ველების დასამალავად და რომ ქსელში არსებობს პირველი ფრაგმენტი, რომელიც შეიცავს მხოლოდ 8 ოქტეტ მონაცემს. ამ შემთხვევაში, მიუხედავად იმისა, რომ პირველი ფრაგმენტი ფილტრს გაივლის, დანიშნულების კვანძი ვერ შეძლებს სრული დატაგრამის აწყობას, ვინაიდან მეორე ფრაგმენტი ფილტრის მიერ განადგურდება.

აღსანიშნავია, რომ რადგან რეალურ ცხოვრებაში არასდროს მოგვიწევს დატაგრამის ფრაგმენტაცია მინიმალურ ზომამდე, რისკი ზემოთ შემოთავაზებული ფილტრაციის მეთოდების გამოყენებით ლეგიტიმური დატაგრამების დაკარგვის ნულის ტოლია.

ფრაგმენტაციის მეორე ასპექტი, რომელიც საინტერესოა უსაფრთხოების თვალსაზრისით, არის გადაფარვითი (overlapping) ფრაგმენტები. შემთხვევა, როდესაც მეორე ფრაგმენტის მონაცემები ნაწილობრივ ფარავს პირველი ფრაგმენტის მონაცემებს. ასეთ დროს საბოლოო შედეგი დამოკიდებულია IP სტეკის რეალიზაციაზე კონკრეტულ ოპერაციულ სისტემაში.

ხშირად გამოყენებული რეალიზაციების შემთხვევაში, გადაფარვითი ფრაგმენტის მონაცემები გადაწერს წინა ფრაგმენტის შესაბამის ნაწილს, რის შედეგადაც შესაძლებელია TCP-სათაურის კრიტიკული ველების შეცვლა და SYN-სეგმენტის მიღება ფილტრაციის გვერდის ავლით.

განვიხილოთ TCP-სეგმენტის შემცველი დატაგრამის მაგალითი, რომელიც შედგება ორი ფრაგმენტისგან (ნახ.2, IP-სათაური გამოყოფილია ნაცრისფრად).

<table>
<tr><td colspan="10">IP Header
MF = 1, Fragment Offset = 0</td></tr>
<tr><td colspan="5">Source Port</td><td colspan="5">Destination Port</td></tr>
<tr><td colspan="10">Sequence Number (SN)</td></tr>
<tr><td colspan="10">Acknowledgment Sequence Number (ACK SN)</td></tr>
<tr><td>Data Offset</td><td colspan="2">Reserved</td><td>-</td><td>ACK</td><td>-</td><td>-</td><td>-</td><td>-</td><td>Window</td></tr>
<tr><td colspan="7">Checksum</td><td colspan="3">Urgent Pointer = 0</td></tr>
<tr><td colspan="10">0</td></tr>
</table>

<table>
<tr><td colspan="10">IP Header
MF = 0, Fragment Offset = 1</td></tr>
<tr><td colspan="10">Acknowledgment Number (ACK SN) = 0</td></tr>
<tr><td>Data Offset</td><td colspan="2">Reserved</td><td>-</td><td>-</td><td>-</td><td>-</td><td>SYN</td><td>-</td><td>Window</td></tr>
<tr><td colspan="7">Checksum</td><td colspan="3">Urgent Pointer = 0</td></tr>
<tr><td colspan="8">Options</td><td colspan="2">Padding</td></tr>
</table>

ნახ. 2. გადაფარვითი ფრაგმენტები

პირველი ფრაგმენტის მონაცემთა ველში არის სრული TCP-სათაური, ოფციების გარეშე, შევსებული ნულებით ზომამდე, რომელიც რვა ოქტეტის ჯერადია. მეორე ფრაგმენტის მონაცემთა ველში - სხვა TCP-სათაურის ნაწილი, დაწყებული რიგით მეცხრე ოქტეტიდან, რომელშიც დაყენებულია SYN ალამი.

ჩანს, რომ მეორე ფრაგმენტი ედება პირველს (პირველი ფრაგმენტი შეიცავს ოქტეტებს 0-23 საწყისი დატაგრამის მონაცემებიდან, ხოლო მეორე ფრაგმენტი იწყება ოქტეტიდან 8, რადგან მისი Fragment Offset=1). დანიშნულების კვანძის ქცევა, რომელმაც მიიღო ასეთი დატაგრამა,

დამოკიდებულია IP მოდულის რეალიზაციაზე. ხშირად დატაგრამის აწყობისას მეორე, გადაფარვითი ფრაგმენტის მონაცემები იწერება წინა ფრაგმენტის ზემოთ. ამგვარად, მაგალითში მოყვანილი დატაგრამის აწყობისას TCP-სათაურში გადაიწერება ველები დაწყებული ACK SN-დან მეორე ფრაგმენტიდან მნიშვნელობების შესაბამისად, და საბოლოოდ მიიღება SYN-სეგმენტი [5,6].

თუ Tiny Fragment Attack-ისგან დასაცავად გამოიყენება ზემოთ აღწერილი პირველი მიდგომა (დატაგრამის პირველი ფრაგმენტის შემოწმება), მაშინ გადაფარვითი ფრაგმენტების მეშვეობით ბოროტგანმზრახველს შეუძლია გვერდი აუაროს ამ დაცვას.

მარშრუტიზატორი, რომელიც იყენებს მეორე მიდგომას, წარმატებით გაუძლებს Tiny Fragment Attack-ს გადაფარვითი ფრაგმენტებით.

რადგან ფილტრაცია გულისხმობს ერთი პაკეტების ქსელში გატარებას და სხვების ბლოკირებას, ფრაგმენტაციის დროს ქსელში შეღწევას შეძლებენ მხოლოდ ის ფრაგმენტები, რომლებიც არ შეიცავენ ბლოკირებული პაკეტების სათაურებს (tcp, udp ან icmp), რადგან ქსელის დამცავი ფილტრაციის მოწყობილობა ვერ ახერხებს სათაურის ველის მდგომარეობის ანალიზს. სიტუაცია პირდაპირ აჩვენებს, რომ უნდა დაიბლოკოს ყველა ფრაგმენტი, რომელთა იდენტიფიკატორები ემთხვევა დაბლოკილი ფრაგმენტის იდენტიფიკატორს. თუმცა, ზოგიერთი ქსელური მოწყობილობა არ ინახავს ამ ინფორმაციას, რადგან ისინი აანალიზებენ დაბლოკილი ფრაგმენტის შემდეგ პაკეტებს, როგორც ცალკეულს, დამოუკიდებელს და არ ატარებენ ანალოგიას წინა ან მომდევნო პაკეტებთან. ზოგიერთი ქსელური მოწყობილობის მუშაობის ასეთი პრინციპი დაკავშირებულია იმასთან, რომ საჭიროა თითოეული პაკეტის ანალიზი, რისთვისაც საჭიროა შესაბამისი რესურსები, როგორც დროითი, ისე აპარატულ-პროგრამული, რაც ყოველთვის მისაღები არ არის ამ კლასის მოწყობილობებისთვის. გაცილებით უფრო მარტივია უფრო გამარტივებული არქიტექტურის შექმნა, რომელიც იმუშავებს ბევრად უფრო სწრაფად.

იქმნება სიტუაცია, როდესაც ქსელში გადის პაკეტები, რომლებიც არ აკმაყოფილებენ ბლოკირების კრიტერიუმებს, რადგან არ არის სათაური, რომელიც იდენტიფიცირებას უკეთებს პაკეტის კუთვნილებას ტრაფიკის ამა თუ იმ ტიპისადმი (tcp, udp, icmp).

თუ დაყენებული ალამის მქონე დატაგრამა კვეთს ქსელს, სადაც საჭიროა ფრაგმენტაცია, მარშრუტიზატორი ადგენს მას და უბრუნებს გამგზავნ ჰოსტს, როგორც ICMP შეცდომის შეტყობინებას. ეს შეტყობინება აჩვენებს ქსელის MTU-ს, რომელიც მოითხოვს ფრაგმენტაციას (ეს შეცდომის შეტყობინება შეიძლება გამოიყენოს თავდამსხმელმა ქსელის გარკვეული სეგმენტის MTU-ს დასადგენად, სადაც მდებარეობს მისთვის საინტერესო სამიზნე და შემდგომში შეიძლება გამოიყენოს ეს მნიშვნელობა თავისი მიზნებისთვის, მაგალითად, თავისი პაკეტების გენერირებისთვის ამ MTU-თი ბრანდმაუერის გასავლელად). ზოგიერთი ჰოსტი, გამოყენებული ოპერაციული სისტემის მიხედვით (შესაბამისი tcp/ip სტეკი), განზრახ გზავნის ქსელში საწყის დატაგრამას დაყენებული ფრაგმენტაციის ალმით, ადგენს MTU-ს დანიშნულების ჰოსტთან მიმავალ გზაზე. თუ ICMP შეცდომის შეტყობინება ბრუნდება უფრო მცირე MTU-თი, ჰოსტი ახდენს დანიშნულების ჰოსტისთვის განკუთვნილი დატაგრამების დაპაკეტებას ჯგუფებად, რომლებიც იმდენად მცირეა, რომ თავიდან აიცილოს ფრაგმენტაცია. ამასთან დაკავშირებით, ფრაგმენტაცია ამცირებს ქსელის მუშაობის ეფექტურობას მთლიანობაში, რადგან ერთი ფრაგმენტის დაკარგვის შემთხვევაში საჭიროა ყველას ხელახლა გაგზავნა (ამ თავისებურებაზე იგება "დატბორვის" ტიპის შეტევები ფრაგმენტირებული პაკეტებით) [5,6].

3. დაცვის მექანიზმები (რეკომენდაციები).

ფრაგმენტაციაზე დაფუძნებული შეტევებისგან დაცვის მიზნით რეკომენდებულია შემდეგი მიდგომები:

- TCP ტრეფიკისთვის პირველი ფრაგმენტის მონაცემთა ველის მინიმალური ზომის კონტროლი (არანაკლებ TCP-სათაურის სრული სიგრძისა);
- Fragment Offset ≠ 0 მქონე TCP ფრაგმენტების ბლოკირება;
- გადაფარვითი ფრაგმენტების იდენტიფიკაცია და განადგურება;
- ფრაგმენტირებული პაკეტების მკაცრი პოლიტიკის გამოყენება პერიმეტრულ მოწყობილობებზე.

აღნიშნული მიდგომები პრაქტიკულად არ იწვევს ლეგიტიმური ტრაფიკის დაკარგვას, ვინაიდან რეალურ ქსელებში მინიმალური ზომის ფრაგმენტაცია იშვიათად გამოიყენება.

5. დასკვნა.

IP-ფრაგმენტაცია წარმოადგენს აუცილებელ ქსელურ მექანიზმს, თუმცა მისი არასწორი ან ბოროტად გამოყენება ქმნის სერიოზულ საფრთხეებს საინფორმაციო უსაფრთხოებისთვის. სტატიის ფარგლებში ნაჩვენებია, რომ Tiny Fragment Attack და გადაფარვითი ფრაგმენტები ეფექტურად გამოიყენება ფილტრაციის გვერდის ავლისთვის. შესაბამისად, მასშტაბირებადი და უსაფრთხო ქსელური ინფრასტრუქტურის უზრუნველსაყოფად აუცილებელია ფრაგმენტაციის თავისებურებების გათვალისწინება და შესაბამისი დაცვის მექანიზმების ინტეგრაცია.

COMPUTER SCIENCES

IP FRAGMENTATION–BASED ATTACKS AND PROTECTION MECHANISMS IN DISTRIBUTED AND HETEROGENEOUS NETWORK SYSTEMS

MIKHEIL DONADZE
***E-mail**: mikheil.donadze@bsu.edu.ge*
Batumi Shota Rustaveli State University

BESIK BERIDZE
***E-mail:** b.beridze@bsu.edu.ge*
Batumi Shota Rustaveli State University

ABSTRACT: In the context of the rapid advancement of corporate information networks and international telecommunication technologies, ensuring the security of distributed computing systems has become a critical challenge for government, administrative, and law enforcement agencies. Most modern Intrusion Detection Systems (IDS) and packet filtering technologies are unable to perform a comprehensive analysis of fragmented datagrams. This technical limitation significantly hinders the timely identification of cyberattacks and the blocking of malicious traffic, thereby creating a fertile ground for the execution of Denial of Service (DoS/DDoS) attacks distributed across multiple fragments.

This paper examines the tension between the demand for increased intrusion detection efficiency and the necessity of aggregating heterogeneous information-computing systems. This problem is further exacerbated by the technical possibility of concealing destructive actions within individual fragments.

The study analyzes specific threats, such as Tiny Fragment Attacks and Overlapping Fragment scenarios. The primary objective of the research is to conduct an in-depth analysis of IP fragmentation characteristics and to develop effective, dynamic protection mechanisms for scalable information-computing systems.

KEYWORDS: computer networks, IP fragmentation, TCP, network security, DoS attacks

გამოყენებული ლიტერატურა:

1. L. Aubard, J. Mazel, G. Guette, and P. Chifflier, „Overlapping IPv4, IPv6, and TCP data: exploring errors, test case context and multiple overlaps inside network stacks and NIDSes with PYROLYSE“, Aug. 2025
2. C. Hopps, „Aggregation and Fragmentation Mode for Encapsulating Security Payload (ESP) and Its Use for IP Traffic Flow Security (IP-TFS)“, RFC 9347, Jan. 2023
3. K. Fujiwara and P. Vixie, „IP Fragmentation Avoidance in DNS“, IETF Internet-Draft, Dec. 2023
4. A. Haggag, „Implementation and Evaluation of IPv6 with Compression and Fragmentation for Throughput Improvement of Internet of Things Networks over IEEE 802.15.4“, Wireless Pers. Commun., vol. 130, pp. 1449–1477, Mar. 2023
5. Y. Han, L. Zhang, Y. Wang, X. Deng, Z. Gu, and X. Zhang, „Research on the Security of IPv6 Communication Based on Petri Net under IoT“ Sensors, vol. 23, no. 11, Art. no. 5192, 2023
6. Tze Uei Chai1, Hock Guan Goh, Soung-Yue Liew,Vasaki Ponnusamy, „Protection Schemes for DDoS, ARP Spoofing, and IP Fragmentation Attacks in Smart Factory“, Systems, vol. 11, no. 4, Art. 211, Apr. 2023