Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 1-6 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

THE ANALYSIS OF THE DIFFERENCE OF 4G AND 5G SECURITIES.

4G და 5G უსაფრთხოების განსხვავებების ანალიზი

მ. იავიჩი. კავკასიის უნივერსიტეტი
M. Iavich. Caucasus University of Georgia
გ. იაშვილი. კავკასიის უნივერსიტეტი
G. Iashvili. Caucasus University of Georgia
ა. გაგნიძე. სამეცნიერო კიბერუსაფრთხოების ასოციაცია
A.gagnidze Scientific Cyber Security Association
ლ.ნაჭყებია. სამეცნიერო კიბერუსაფრთხოების ასოციაცია
L.Nachkebia Scientific Cyber Security Association
შ. ხუხაშვილი. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი
S. Khukhashvili. Ivane Javakhishvili Tbilisi State University

ABSTRACT: The paper analyzes the difference between 4G and 5G architectures. The difference between 4g and 5G security is also analyzed. We analyzed the new security features of 5G, the advantages and disadvantages are identified. Are analyzed the existing attacks on 5G, such as MNmap, MiTM and Battery drain attacks. The recommendation for securing 5g are provided.

აბსტრაქტი: აღნიშნული სტატია აანალიზებს განსხვავებებს 4G და 5G ქსელების არქიტექტურებს შორის. ასევე განხილულია 4G და 5G ქსელების უსაფრთხოება. აქ გავაანალიზეთ სიახლეები 5G-ს უსაფრთხოების სისტემაში, მათი დადებითი და უარყოფითი მხარეები. ასევე განხილულია არსებული შეტევები 5G-ზე: MNmap, MiTM და Battery drain(ბატარეის გამოფიტვის შეტევა). აგრეთვე მოყვანილია რეკომენდაციები სისტემისთვის უკეთესად დასაცავად.

საკვანძო სიტყვები: *4G და 5G, უსაფრთხოება, ფიჭური ქსელი*

Keywords: *4G vs 5G, security, cellular network*

შესავალი

5G არის მე-5 თაობის მობილური ქსელი, წინამორბედი 4G LTE ქსელის თვალსაჩინო გაუმჯობესება. 5G შექმნილია, რათა შეძლოს დიდ მონაცემებთან გამკლავება და შეესაბამებოდეს თანამედროვე საზოგადოების მოთხოვნებს, უზრუნველყოს მილიონობით IoT მოწყობილობის ჩართულობა და სამომავალი ინოვაციები. თავდაპირველად, 5G იმუშავებს არსებულ 4G ქსელთან ერთად, მომდევნო ეტაპზე კი - როგორც დამოუკიდებელი ქსელი.

5G-ს აქვს შემდეგი უპირატესობები: უფრო სწრაფი კავშირი და გაზრდილი მოცულობა, შეყოვნების პატარა დრო (სწრაფი უკუკავშირი).

ტექნოლოგია	შეყოვნება(მილიწამი)
3G	100მწ
4G	30მწ
5G	1მწ(თეორიულად)

1. გამოყენების შემთხვევები

- მასიური მანქანათაშორისი კომუნიკაცია, ანუ ინტერნეტით დაკავშირებული მოწყობილობები (IoT), რაც გულისხმობს მილიონობით ურთიერთდაკავშირებულ მოწყობილობას ადამიანური რესურსის ჩარევის გარეშე, ისეთ მასშტაბებზე რაც აქამდე ჯერ არ ყოფილა.
- დაბალი შეყოვნების მქონე კომუნიკაცია - უზრუნველყოფს მოწყობილობების მონიტორინგს რეალურ დროში, ინდუსტირულ რობოტებს და სატრანსპორტო საშუალებებს შორის კომუნიკაციას, ავტომობილების აუტონომიურ მართვას და უფრო უსაფრთხო სატრანსპორტო ქსელს. დაბალი შეყოვნების მქონე კომუნიკაცია გვაძლევს შესაძლებლობას ვისარგებლოთ დისტანციური სერვისებით, მაგალითად,ჯანდაცვის სფეროში.

- გაუმჯობესებული მობილური კავშირი - უზრუნველყოფს მნიშვნელოვნად გაზრდილ სიჩქარეს და გაზრდილ გამტარუნარიანობას, რათა მსოფლიო იყოს მუდმივ კავშირში.

ბიზნესისა და მრეწველობისათვის, 5G და IoT უზრუნველყოფს დიდი რაოდენობით მონაცემებს და მათი ანალიზის შედეგად ისეთ დასკვნებს, რაც აქამდე არ ყოფილა. ბიზნესი მიიღებს გადაწყვეტილებებეს, რომელიც უშუალოდ იქნება დაყრდნობილი მანამდე არსებულ მონაცემებზე, რაც ხელს შეუწყობს მაგ.: აგრარული სფეროს გაციფრულებას, მომხმარებელთან ურთიერთობის ხარისხის ამაღებას. ახალი ტექნოლოგიების დანერგვას, როგორებიცაა: ვირტუალური და აუგმენტირებული რეალობა რაც ყველასათვის იქნება ხელმისაწვდომი. რა თქმა უნდა, ეს გააჩენს აქამდე ჯერ არ არსებულ შესაძლებლობებს. 5G და ვირტუალური რეალობის ერთობლიობა შესაძლებლობას მოგვცემს ვირტუალურად ვიმოგზაუროთ სასურველ ქალაქში, ვუყუროთ ფეხვურთის მატჩს და განვიცადოთ იგივე შეგრძნებები რაც სტადიონზე ყოფნისას და მრავალი სხვა.

5G იქნება ძირეული კომპონენტი სამომავლოდ ,,ჭკვიანი ქალაქების“, ‘‘ჭკვიანი სახლების“, ,,ჭკვიანი სკოლების“ შესაქმნელად. რეალურს გახდის ისეთ შესაძლებლობებს, რისი წარმოდგენაც კი ძნელი შეიძლებოდა ყოფილიყო აქამდე.

2. **5G-ს მუშაობა 4G-თან ერთად**

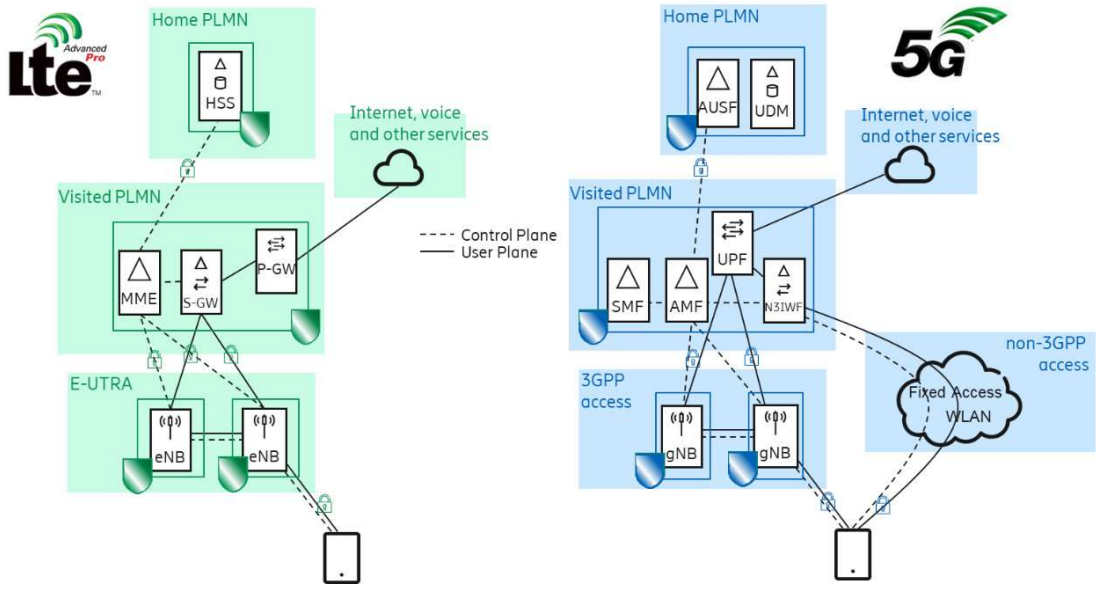
როდესაც 5G-სთან მიერთდება მოწყობილობა, ის მიუერთდება ასევე 4G ქსელსაც. ანუ პირველ ეტაპზე, სანამ 5G დამოუკიდებელ სისტემად ჩამოყალიბდება, არსებული 4G ქსელი 5G-სთან დაკავშირებისას მისი გამაძლიერებლის ფუნქციას შეასრულებს.

3. **4G vs 5G security**

5G და 4G ქსელების უსაფრთხოების არქიტექტურა მსგავსია. ორივე სისტემაში უსაფრთხოების მექანიზმები შეიძლება დაიყოს ორ ჯგუფად:

- პირველი ჯგუფი მოიცავს ქსელთან წვდომის დასამყარებლად საჭირო უსაფრთხოების მექანიზმებს. აქ არის უსაფრთხოების ისეთი კომპონენტები, რომლებიც უზრუნველყოფს მომხარებლის უსაფრთხოებას და იცავს შეტევებისაგან რომლებიც ხორციელდება მოწყობილობასა და მიმღებ ანტენას შორის

- მეორე ჯგუფი კი მოიცავს ქსელის დომეინის უსაფრთხოების მექანიზმებს. ეს მექანიზმები უწყობს ხელს ანტენებს შორის ინფორმაციის უსაფრთხოდ მიმოცვლას. მაგალითად მიმღებ რადიო ანტენასა და ძირითად ქსელს შორის.



უსაფრთხოების ძირითადი პროცედურა 3GPP ქსელებში არის აუტენთიფიკაცია, ცნობილი როგორც პირველადი აუტენთიფიკაცია 3GPP 5G უსაფრთხოების სტანდარტში. ეს პროცედურა სრულდება ყოველთვის როდესაც, მაგალითად, პირველად ირთვება მობილური ტელეფონი.

წარმატებული აუტენთიფიკაციის შემდეგ, იქმნება გასაღებები სესიისათვის. გასაღებები გამოიყენება მოწყობილობასა და ქსელს შორის კომუნიკაციის დასაცავად [1, 2]. აუტენთიფიკაციის პროცედურა 3GPP 5G უსაფრთხოების სისტემაში ისეა შემუშავებული, რომ

ჰქონდეს გაფართოებული აუტენთიფკაციის პროტოკოლის (EAP) მხარდაჭერა. აღნიშნული პროტოკოლი არის კარგად დამუშავებული და ფართოდ გამოიყენება IT გარემოში.

EAP იძლევა საშუალებას გამოვიყენოთ განსხვავებული ტიპის სენსიტიური მონაცემები, რომლებიც ინახება SIM ბარათზე: სერთიფიკატები, გასაღებები, მომხმარებლის სახელები/პაროლები. ამ აუტენთიფიკაციის მეთოდის მოქნილობის მთავარი მიზეზი არის ის, რომ ხელს უწყობს 5G-ს დანერგვას როგორც სატელეკომუნიკაციო ინდუსტრიაში, ასევე სხვა ინდუსტრიებში.

თავდაპირველი აუტენთიფიკაციისა და გასაღებების განაწილების პროცედურები ხელიმსაწვდომს ხდის აუტენთიფიკაციას მომხმარებელსა და ქსელს შორის და ასევე ქმნის არსებით კავშირებს მომხმარებელსა და ქსელს შორის უსაფრთხოების მომავალი პროედურებისათვის. ძირითადი პროდუქტი რაც ამ პროცედურების შემდეგ იქმნება არის „მთავარი გასაღები“ KSEAF, რომელსაც გადასცემს შიდა ქსელის AUSF ფუნქცია მომსახურე ქსელის SEAF ფუნქციას.

„მთავარი გასაღების“ კონცეფცია გვაძლევს საშუალებას ვაწარმოოთ გასაღებები უსაფრთხოების მრავალი განსვავებული მიზნისათვის ისე, რომ აუტენთიფიკაციის ხელახალი გავლა არ იქნება საჭირო. მაგალითად 3GPP ქსელში ავტორიზაციისას შექმნილი გასაღები, ასევე გამოიყენება მომხმარებელსა და Non-3GPP Interworking Function (N3IWF) შორის.

4. 5G უსაფრთხოების უპირატესობები

5G იყენებს ქსელის შრეებად დაყოფის კონცეფციას. ჩვენი კვლევის თანახმად ეს არის 5G-ს მთავარი უპირატესობა 4G LTE-სთან მიმართებაში. განსაზღვრების თანახმად, ქსელის ცალკეული შრე არის დამოუკიდებელი, ლოგიკური ქსელი, რომელიც მუშაობს გაზიარებულ ფიზიკურ ინფრასტრუქტურაზე, რომელსაც შეუძლია უზრუნველყოს სერვისის შესაბამისი ხარისხი. ეს კი ნიშნავს, რომ ჩვენ შეგვიძლია მთლიანი 5G დავყოთ თანაუკვეთ კომპონენტებად(ნაწილებად). ეს კონცეფცია ანალოგიურია VLAN-ის, რაც მოგვცემს საშუალებას, რომ დავყოთ და უსაფრთხოდ ვმართოთ სერვისები როგორიცაა:

- მობილური კავშირგაბმულობა: საკომუნიკაციო სისტემები, გართობა, ინტერნეტი
- მასიური IoT შრე: სამეწარმეო საქმიანობა, გადაზიდვები
- კრიტიკული IoT შრე: აუტონომიური სამედიცინო ინფრასტრუქტურა

აღნიშნული კონცეფცია სასარგებლოა უსაფრთხოების პერსპექტივიდანაც, რადგან სისტემა იქნება მეტად დაცული, სტრუქტურირებული და ადვილად სამართავი.

5. შეტევები 5G-ს უსაფრთხოებაზე

5G არქიტექტურაზე აღინიშნება წარმატებული შეტევები. ბოლო წლებში, მკვლევარებმა აღმოაჩინეს ხარვეზები 5G-ს უსაფრთხოების სისტემაში, რაც ხელს აძლევს ჰაკერებს სისტემაში ჩააშენონ მავნე კოდი და მიიღონ სასურველი შედეგები. აქ განვიხილავთ რამდენიმე მიზანმიმართულ შეტევას:

- **Mnmap**
  მკვლევართა გუნდმა მოიპოვა ინფორმაცია, რომელიც ქსელში გაგზავნილი იყო ღია ტექსტის სახით და ამის მეშვეობით მათ შექმნეს მოწყობილობების რუკა, რომლებიც დაკავშირებული იყო ამ ქსელთან. ასევე მათ შექმნეს ცრუ საბაზო სადგური და იმახსოვრებდნენ მიერთებული მოწყობილობების მონაცემებს. ამის შედეგად მათ შეეძლოთ დაედგინათ მოწყობილობის: მწარმოებელი, მოდელი, ოპერაციული სისტემა, მოწყობილობის ტიპი და ვერსია. ასევე შეეძლოთ დაედგინათ იყო თუ არა ეს მოწყობილობა ავტომობილი, როუტერი, USB თუ სხვა.

- **MiTM**
  ახლანდელი 5G შემტევს აძლვს საშუალებას განახორციელოს MiTM შეტევა. MiTM-ის იმპლემენტაციით შესაძლებელია ბატარეის გამოფიტვის შეტევის განხორციელება. შემტევს შეუძლია MIMO-დან (5G სიხშირეების მიმღები და გამცემი მოწყობილობა) ამოიღოს ფიზიკური ნაწილი, რომელიც უშულოდ პასუხისმგებელია მაღალ სიჩქარეზე. ამის შედეგად, სისტემა ექვივალენტური გახდება 2G/3G/4G ქსელების და შეეძლება იმ სისუსტეების გამოყენება რაც აღნიშნულ ქსელებს აქვთ.

- **Battery drain attack.**

  ეს შეტევა მიმართულია NB-IoT მოწყობილობებზე. ისინი გარკვეული დროის შუალედებით აგზავნიან ინფორმაციის მცირე პაკეტებს. ამ პაკეტებს შეუძლიათ გამოფიტონ ბატარეის ისეთი ზომის ენერგია, რაც 10 წელი ეყოფოდა ენერგიის შენახვის მდგომარეობაში(power saving mode). შემტევს შეუძლია ისეთი მოდიფიკაცია გაუკეთოს ამ მდგომარეობაში მყოფ მოწყობილობას, რომ მას ქონდეს უწყვეტი აქტივობა და მუდმივად ეძებდეს ქსელს დასაკავშირებლად. ამ შემთხვევაში, შემტევს შეუძლია დააკავშიროს მოწყობილობა სასურველ ქსელთან, შემდეგ კი განახორციელოს სასურველი ქმედებები, როგორც ქსელთან ასევე მოწყობილობასთან მიმართებაში.

6. დასკვნა

ჩვენს კვლევაზე დაყრდნობით შეგვიძლია ვთქვათ, რომ 5G-ს აქვს ახალი ფუნქციები, რომლებიც აუმჯობესებს უსაფრთხოებას. აღსანიშნავია, რომ 5G უახლესი ტექნოლოგიაა და მისი უსაფრთხოება სათანადოდ არაა გამოკვლეული ამ ეტაპისათვის. ამ სტატიაში მოვიყვანეთ არსებული შეტევები 5G-ზე, რაც თვალნათლივ გვანახებს 5G უსაფრთხოების

სისუსტეებს. აქედან ჩანს, რომ დიდი სამუშაოა გასაწევი და შესამუშავებელია უფრო მძლავრი უსაფრთხოების სისტემა 5G-ს ეფექტურად მუშაობისათვის.

შენიშვნა:

აღნიშნული სამუშაო შესრულებულია CARYS-19, PHDF-19-519 და კავკასიის უნივერსიტეტის მიერ დაფინანსებული გრანტის ფარგლებში.

The work was conducted as a part of PHDF-19-519, the grant financed by Caucasus University and CARYS 2019 [CARYS-19-121]

ლიტერატურა:

1. Gagnidze, A., Iavich, M, Iashvili, G. : Novel version of merkle cryptosystem. Bull. Georgian Natl. Acad. Sci. 11(4), 28–33 (2017)

2. Avtandil Gagnidze & Maksim Iavich & Giorgi Iashvili, 2017. "Some Aspects Of Post-Quantum Cryptosystems, " Eurasian Journal of Business and Management, Eurasian Publications, vol. 5(1), pages 16-20.

3. S. Zhang, "An Overview of Network Slicing for 5G, " in IEEE Wireless Communications, vol. 26, no. 3, pp. 111-117, June 2019, doi: 10. 1109/MWC. 2019. 1800234.

4. P. Popovski, K. F. Trillingsgaard, O. Simeone and G. Durisi, "5G Wireless Network Slicing for eMBB, URLLC, and mMTC: A Communication-Theoretic View, " in IEEE Access, vol. 6, pp. 55765-55779, 2018, doi: 10. 1109/ACCESS. 2018. 2872781.

5. V. Sciancalepore, K. Samdanis, X. Costa-Perez, D. Bega, M. Gramaglia and A. Banchs, "Mobile traffic forecasting for maximizing 5G network slicing resource utilization, " IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, Atlanta, GA, 2017, pp. 1-9, doi: 10.1109/INFOCOM.2017.8057230.