ANCOM
National Authority for Management and Regulation in Communications of Romania

Bucharest Talks

VIITORUL COMUNICAȚIILOR. 5G ÎNTRE BENEFICII ȘI PROVOCĂRILE DE SECURITATE CYBER

04 Iunie 2019, Bucuresti

Virgilius Stanciulescu
ANCOM
Consilier IT&C

- Abordarea zilelor și mai exact obișnuințele zilnice se vor schimba substanțial odată cu dezvoltarea tehnologiei, care va conecta tot ceea ce ne înconjoară.
- **Cu ajutorul rețelelor 5G**
  - conexiunile vor fi mai rapide
  - lucrurile care joacă un rol în confortul de zi cu zi vor fi conectate
  - beneficii încă puțin înțelese sau cunoscute de către fiecare dintre noi.

- Pentru operatorii de rețele de telecomunicații:
  - rețeaua de fibră optică
  - integrarea fix – mobil
  - conlucrează pentru a deschide calea către 5G și mai departe respectiv pentru a ține pasul cu:
    - vitezele necesare pentru transportul
    - unor cantități uriașe de date
    - cu întârziere minimală (de ordinul milisecundelor)
    - cu un număr masiv de elemente conectate.

Despre tehnologia 5G: etape

- **Strategia** pentru implementarea tehnologiei 5G: realizată de un grup interministerial, care cuprinde şi reprezentanţi din industria de comunicaţii.
- **ANCOM a dezbătut** şi adoptat, împreună cu industria, în cadrul unei şedinţe a Consiliului Consultativ, planul de măsuri şi calendarul naţional privind alocarea benzii de frecvenţe 470-790 MHz, precum şi opţiunile de reglementare asociate, sub forma unei foi de parcurs naţionale privind alocarea şi utilizarea viitoare a benzii de frecvenţe 470-790 MHz
- **Un prim pas** esential: eliberarea, în timp util, a spectrului radio adecvat pentru dezvoltarea viitoare a sistemelor de comunicaţii mobile de bandă largă.
- Pentru ca banda de 700 MHz să fie disponibilă, ANCOM a propus modificarea **TNABF** (Tabelul naţional de atribuire a benzilor de frecvenţe radio) şi atribuirea benzii de 790 MHz serviciului mobil terestru, în acest moment banda fiind atribuită serviciilor de televiziune digitală terestră.

Despre tehnologia 5G: etape

- Elaborarea și adoptarea poziției naționale privind acordarea drepturilor de utilizare a spectrului radio disponibil în benzile de frecvențe de 700 MHz, 800 MHz, 1500 MHz, 2600 MHz, 3400-3600 MHz și 26 GHz pentru sisteme de comunicații electronice pe suport radio de bandă largă.
- O altă acțiune cu impact asupra implementării tehnologiilor 5G este încheierea de **acorduri bilaterale** de coordonare cu țările vecine.
- ANCOM: monitorizarea spectrului radio în benzile de frecvențe care fac obiectul licitației

- **Documentaţia** pentru licitaţia privind frecvenţele destinate tehnologiei 5G: va fi finalizată până în iulie 2019
- **Licitaţia** de spectru va fi încheiată cel târziu în decembrie 2019

Despre tehnologia 5G: etape

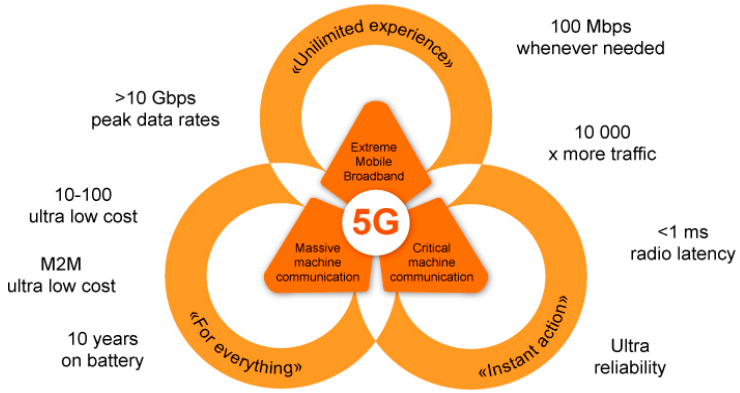
- La nivel european, au fost identificate următoarele benzi de frecvențe prioritare pentru introducerea timpurie a sistemelor de comunicații mobile de generația a 5-a în Uniune:
  - banda de 700 MHz (694-790 MHz),
  - banda 3400-3800 MHz
  - banda de 26 GHz (24,25-27,5 GHz).

Despre tehnologia 5G: etape

- Banda de frecvențe de 700 MHz (694-790 MHz):
  - este foarte importantă pentru furnizarea unei acoperiri extinse,
  - în special în zonele care pun probleme de rentabilitate economică,
  - zonele rurale, montane sau alte zone îndepărtate.
  - adecvată pentru asigurarea unei acoperiri eficiente pe arii extinse, precum și a unei acoperiri îmbunătățite în interiorul clădirilor
- Banda de 3400-3800 MHz:
  - bandă primară adecvată pentru introducerea serviciilor 5G înainte de 2020,
  - oferă lărgimi de bandă relativ mari
  - bun compromis între acoperire și capacitate,
  - creștere semnificativă a capacității și susținerea comunicațiilor de bandă largă îmbunătățite, precum și a aplicațiilor care au nevoie de latență mică și înaltă fiabilitate, cum sunt aplicațiile pentru misiuni critice (automatizări industriale și robotică).
- Banda de 26 GHz:
  - este considerată bandă pionier pentru armonizarea timpurie pentru 5G în Europa
  - oferă peste 3 GHz de spectru continuu
  - permite furnizarea de rețele dense de mare capacitate pe distanțe scurte,
  - aplicații și servicii 5G revoluționare, ce presupun viteze de transfer de date foarte mari, capacitate crescută și latență foarte mică.

5G: caracteristici tehnice

- Volumul de date transmis: de 1.000 de ori mai mare, decât în prezent
- Numărul de dispozitive ce vor putea fi conectate: de sute de ori mai multe.
- Viteza de procesare a datelor: 10Gbps, iar specialiștii estimează că se vor atinge viteze și mai mari.
- Latenţa redusă: timpul comanda – răspuns
  - în rețelele 4G este de aproximativ 50 de milisecunde,
  - în rețelele 5G de o milisecundă
- Consum redus de curent



5G: aplicații

- Accesul la internet mobil de mare viteză chiar și în zone aglomerate: concerte, festivaluri, evenimente sportive

- Download filme rezoluție 4K
  - o chestiune de secunde

- Transmisiuni TV în direct și evenimentele sportive vor deveni adevărate **experiențe vizuale imersive**, **virtuale**, chiar și pentru cei care nu vor participa personal, în viața reală.

De ex privitorul ar putea vedea imaginea unui joc de fotbal asa cum o vede un anumit jucator☺

5G: aplicații

- posibilitatea participării virtuale, senzoriale, la evenimente reale. Sună bine, nu?
- Experimentele și demonstrațiile efectuate au demonstrat ca este posibil, iar pătrunderea acestor experiențe în viața de zi cu zi va depinde și de capacitatea de absorbție și consum a utilizatorilor finali.

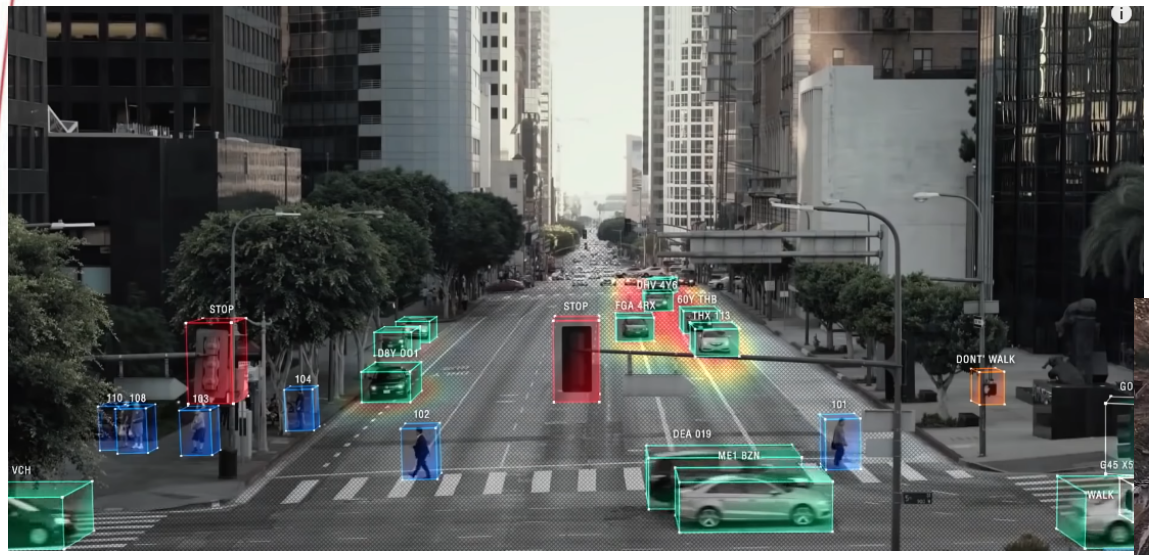
În perioada de testare
un operator din România
a facut un experiment
cu un concert rock
cu o hologramă!

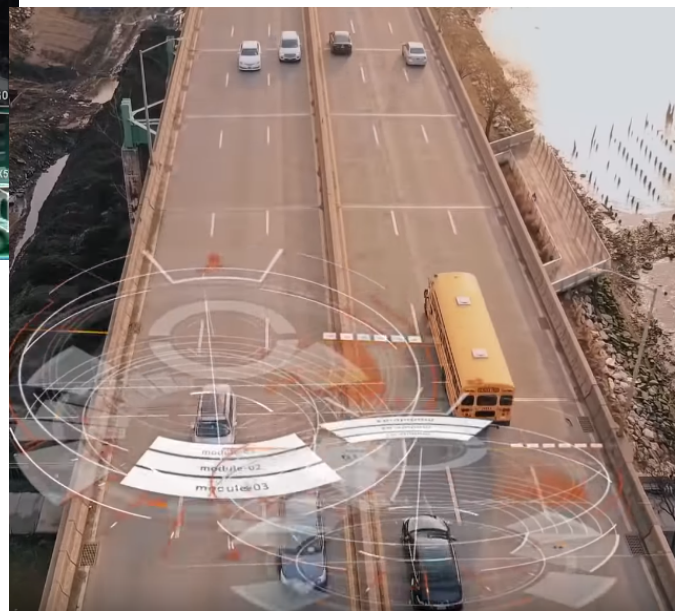
5G: Internet of Eyes

- Monitorizare dinamică a traficului: detectie obiecte și determinare poziție în timp real,
- aplicabilități multiple pentru soluțiile de tip
  - smart city,
  - managementul traficului
  - siguranța publică.
- coloana vertebrală pentru IoT
  - conectând obiectele din jurul nostrum
  - în modalități pe care nu le-am fi crezut posibile.

- Autovehicule independente, care interacționează cu semafoarele
- Comunicațiile vehicul cu vehicul
- Vehicul cu infrastructură
- Senzorii integrați în șosele, căi ferate și piste de zbor vor comunica între ei și cu vehiculele inteligente, pentru îmbunătățirea controlului infastructurii și serviciilor critice.

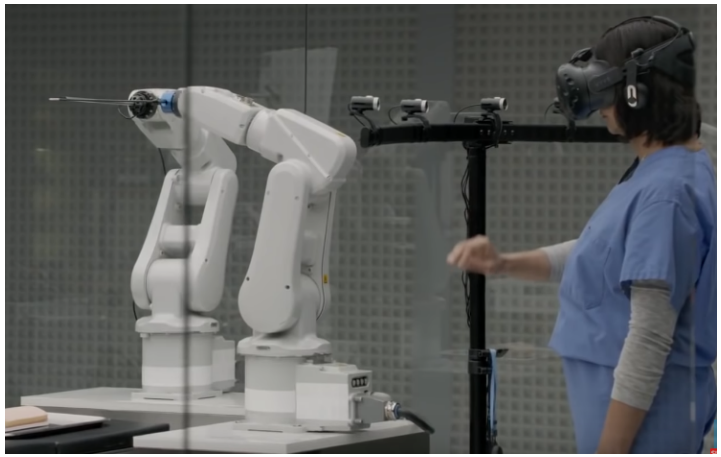
5G: Internet of Eyes





Internet of Skills

- potențialul roboticii în cloud:
  robot controlat la distanță,
- Operație medicală,
  - în combinație cu realitatea virtuală,
  - pentru a realiza internetul tactil,
  - respectiv transmiterea la distanță
  - în timp real a senzației de atingere.
- Medici opereaza pacienti la distanţă. \
  - căşti de realitate virtuală şi mănuşi special



- Agricultura:
  senzori umiditate,
  ingrasaminte, predictii

- Drone: control device

Immersive Gaming

- realitate augmentată pentru filme și jocuri care vor permite o imersiune vizuală virtuală totală, la 360 de grade

5G: expansiune

- Până în 2023, 20% din populaţia lumii va avea acoperire 5G.

- Potrivit estimărilor, tehnologia 5G va genera afaceri de peste 1.200 de miliarde de dolari până în 2026

5G: vulnerabilități

Vorbind despre vulnerabilități și riscuri associate, identific cel puțin două origini ale acestora:

- una legată de nivelul aplicație, adică vulnerabilități asociate noilor tipuri de servicii și aplicații
- una legată de aspectele tehnice legate de tehnologii în sine, de module de management sau protocoale.

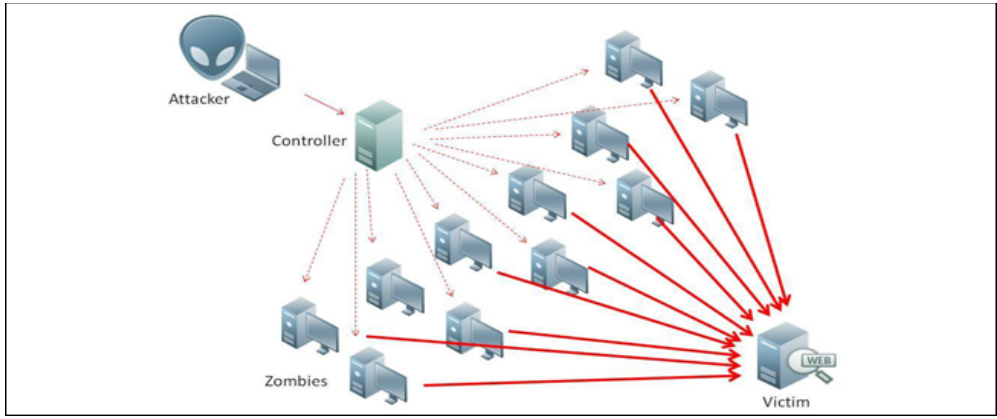
5G: vulnerabilități

- Extrapolarea actualelor atacuri de tip DDoS:
- Creste numărul de dispozitive interconectate
- crește masa critică a dispozitivelor potențial a fi preluate în Botnet
- inițiere atacuri mult mai puternice către:
- un număr și mai mare decât în prezent de ținte, și, atenție:
- la viteze incomparabil mai mari!

Din punct de vedere tehnologic, echipamentele de respingere a atacurilor vor trebui să țină pasul:

- fie ele fizice,
- fie bazate software (AI)

capacitate de
raspuns adaptată.

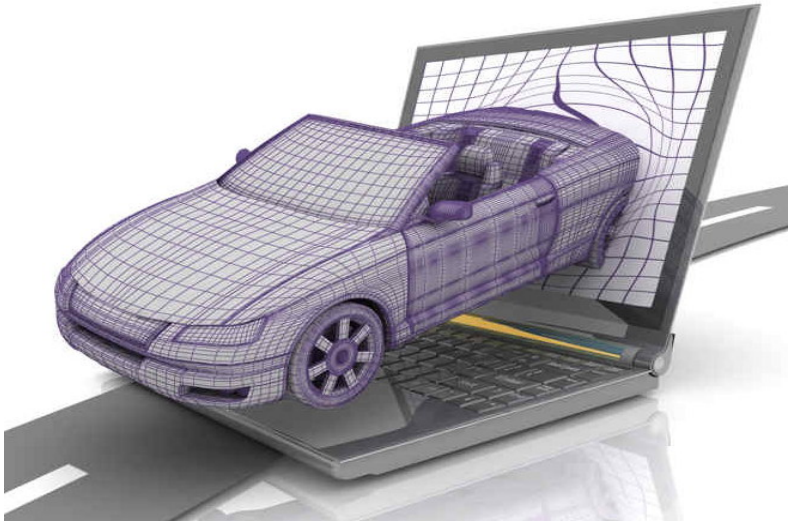


5G: vulnerabilități

Furtul de informații va putea atinge nivele uriașe:

- acum vorbim de exfitrari de informații și furt de date personale, interceptări ale traficului în vederea decriptării de parole sau informații confidențiale,
- în cazul revoluției industriale 4.0 ce aduce cu sine prototipizare virtuală și trimiterea modelului online direct pe linia de fabricație:
  - un atac de tip man-in-the-middle ar putea însemna:
  - furtul modelului (proprietate intelectuală, spionaj industrial) sau
  - denaturarea sau înlocuirea acestuia, schimbarea de caracterisitici înainte de începerea execuției fizice.

Rezultatele și efectele negative incomensurabile.



5G: vulnerabilități

- Deturnarea dronelor sau vehiculelor autonome
- Falsificarea sau furtul datelor personale
- Compromiterea operatiilor cu roboti la distanta
- Interceptarea datelor de la senzori

5G: vulnerabilități

- defectele de securitate ale rețelelor de internet 2G, 3G și 4G ar putea fi repetate și în cazul 5G.
- ENISA: studiu "Signalling Security in Telecom SS7/Diameter/5G"
- Protocoalele SS7 si Diameter: probleme de securitate
- atacurile SS7 pot fi complexe:
  - deoarece atacatorii câștigă tot mai multe cunoștințe și dezvolta scenarii de atac eficiente.
  - O protecție de bază va acoperi probabil majoritatea atacurilor, dar va lăsa loc pentru atacurile complexe sau orientate care pot provoca daune la nivel social, economic sau politic (de exemplu, spionaj etc.).
  - SS7: ENISA: majoritatea furnizorilor adoptă măsuri de securitate minime. Măsurile de securitate de bază oferă doar un nivel de bază de securitate. De asemenea, infrastructura SS7 este destul de veche în unele cazuri și nu toate echipamentele susțin adoptarea de măsuri de securitate, nici măcar cele de bază.
- Diameter: protocol de autentificare, autorizare
- Design: concepte împrumutate din SS7, împreună cu vulnerabilitățile sale.
- Protocol pur bazat pe IP: există un risc crescut de acces prin hacking.
- Acest lucru îl face teoretic, mai simplu de exploatat decât SS7

5G: vulnerabilități

- defectele de securitate ale rețelelor de internet 2G, 3G și 4G ar putea fi repetate și în cazul 5G.
- ENISA: studiu "Signalling Security in Telecom SS7/Diameter/5G"
- "The future use of this protocol or similar approached should be avoided"!
- "Carriers will need a new signalling architecture that can address the impact of introducing billions of roaming and static devices, the subscriber behaviour and bandwidth requirements, and new applications."
- "Nevertheless there is a certain risk of repeating history. Given the improvements that 5G will bring, having the same security risks can be extremely dangerous."

ENISA

5G: probleme

- SDN centralizeaza platforma de control al retelei si permite programabilitate si usurinta in administrare
- Conform studiilor: creeaza oportunitati pentru hacking-ul retelei, favorizand DDos, si expunerea API-urilor catre exterior.
- Controlerul SDN permite modificare software de rute si fluxuri, exista posibilitatea expunerii vizibile a acestuia, ce poate duce la Ddos sau la bottleneck.

- VNF (Virtual Network Functions): platformele curente au probleme cunoscute: nu ofera izolare si securitate serviciilor de comunicatii virtualizate
- Se impun masuri de securitate sporita si data privacy pentru furnizorii de cloud, cresterea relatiei de incredere, abordari de securitate frontend, back-end si network based.

5G: probleme

- SDN centralizeaza platforma de control al retelei si permite programabilitate si usurinta in administrare
- Conform studiilor: creeaza oportunitati pentru hacking-ul retelei, favorizand DDos, si expunerea API-urilor catre exterior.
- Controlerul SDN permite modificare software de rute si fluxuri, exista posibilitatea expunerii vizibile a acestuia, ce poate duce la Ddos sau la bottleneck.

Masuri:

- Arhitectura SDN permite monitorizare a securității reactiva si proactive
- Analiza de traffic si modificarea politicilor de securitate și introducerea serviciilor de securitate.
- Politicili de securitate consistente ale rețelei: pot fi implementate datorită vizibilității globale a rețelei,

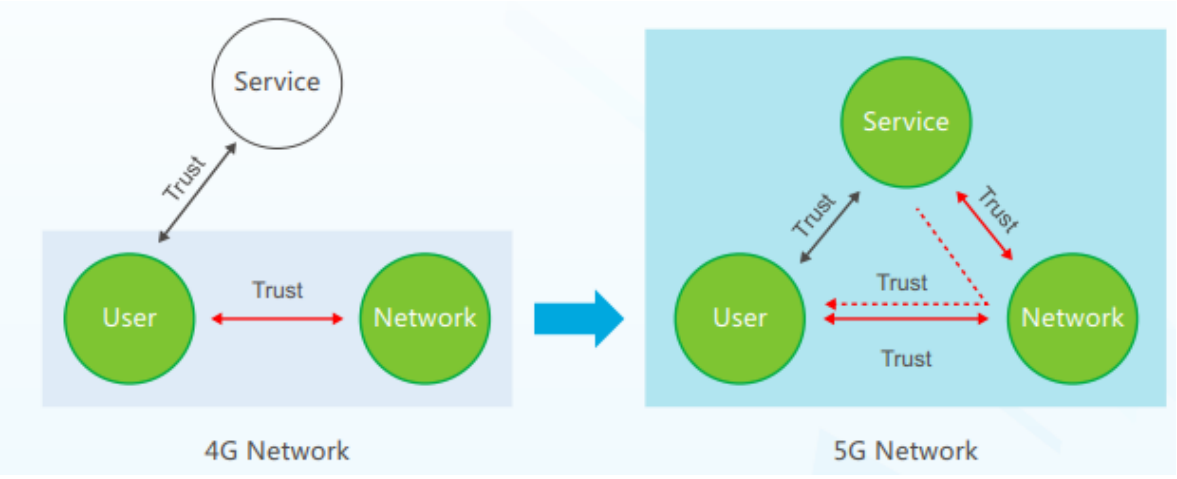
5G: probleme

- VNF (Virtual Network Functions): platformele curente au probleme cunoscute: nu ofera izolare si securitate serviciilor de comunicatii virtualizate

- Masuri:
- Securitate printr-un orchestrator de securitate în corespondență cu arhitectura care asigură securitatea nu numai a funcțiilor virtuale într-un mediu multi-tenant, ci și a entităților fizice ale unei rețele de telecomunicații.

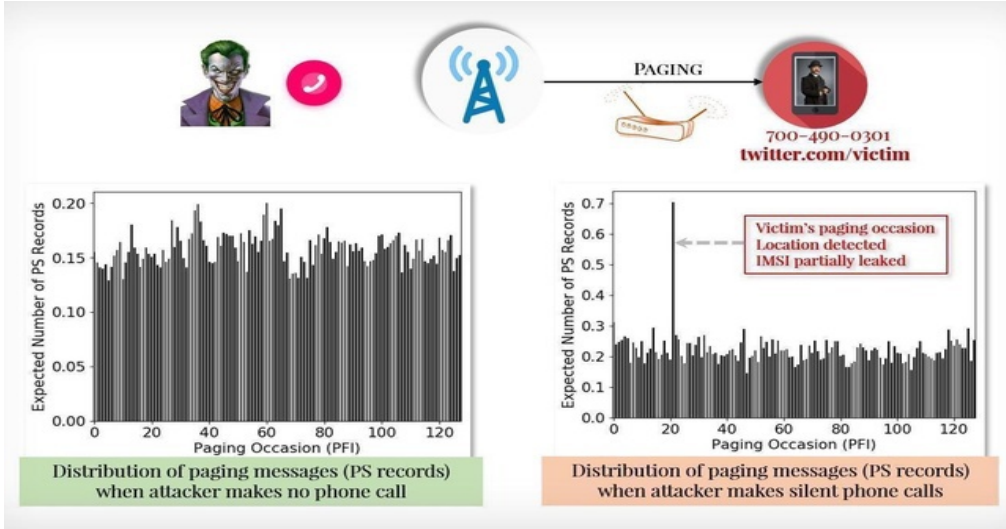
5G: probleme

- Trimiterea cheilor de criptare pt interfetele radio prin canale nesecurizate
- Se impun:
- Masuri de securitate sporita si data privacy pentru furnizorii de cloud
- cresterea relatiei de incredere,
- abordari de securitate frontend, back-end si network based.
- Izolarea si segmentarea retelelor in functie de serviciile oferite pentru a oferi protectie suplimentara
- Noi modele de trust si identity management care sa includa si furnizorul de servicii
- Securitate End 2 End



5G: noi vulnerabilitati
Atacurile Torpedo, Piercer, IMSI-Cracker

- 26 februarie 2019: Cercetatori ai Universitatilor Purdue si Iowa au dat publicitatii o lucrare in cadrul "Network and Distributed System Security" in care demonstreaza noi vulnerabilitati in retele 4G si 5G
- Atacul numit „Torpedo": apelează şi anulează apelul către ţintă de mai multe ori consecutiv, ducând astfel către o vulnerabilitate în sistemul de paginare al reţelei.
- Practic, iniţiatorul atacului poate trimite un mesaj către dispozitivul ţintei, fără ca acesta să înregistreze un apel. De aici, poate fi cu uşurinţă urmărit apelul şi pot fi trimise mesaje noi false, sau blocate alte mesaje care ar putea să vină.



5G: noi vulnerabilitati
Atacurile Torpedo, Piercer, IMSI-Cracker

- Atacul Torpedo deschide calea către alte două tipuri de atacuri.
- Piercer: poate fi folosit pentru a detecta identitatea dispozitivului prin dezvăluirea codului unic IMSI, atac valabil doar pe reţele 4G
- IMSI-Cracking, care poate să afle codul IMSI prin „brute force" atât pe reţele 4G, cât şi pe cele 5G, în ciuda faptului că acesta este criptat pe ambele tipuri de reţele.
- Reţelele 5G ar trebui să fie mult mai bine securizate decât cele 4G, dar acestea sunt în continuare vulnerabile la atacuri care funcţionau şi pe generaţia veche de antene telecom.
- Dispozitivele Stingray ar putea fi cu uşurinţă adaptate pentru atacuri pe reţele 5G, si se poate afla geolocaţia utilizatorilor de telefoane sau alte echipamente 5G. Dar ce ne facem cand nu sunt folosite doar de fortele de ordine? Un astfel de dispozitiv poate fi produs cu 200$

5G: noi vulnerabilitati
Atacurile Torpedo, Piercer, IMSI-Cracker

- GSMA, alianţa mondială care reprezintă operatorii de telefonie mobile a fost informata
- GSMA a recunoscut aceste probleme, însă nu este clar dacă vor fi sau nu rezolvate.
- Întrucât reţelele 5G încă nu sunt pornite, există şansa ca acestea să poată fi modificate înainte de lansarea oficială.
- Vulnerabilitatile au fost demonstrate si publicate, însă nu şi codul folosit pentru a demonstra vulnerabilităţile, Torpedo, Piercer şi IMSI-Cracking fiind mult prea periculoase în mâinile utilizatorilor.
- În timp ce IMSI-Cracking şi Torpedo pot fi rezolvate exclusiv de GSMA, vulnerabilitatea care duce la atacul Piercer poate fi „reparată” exclusiv de către operatori.

Va multumesc!