SCENARII DE ATAC CIBERNETIC A INFRASTRUCTURII DE SEMNALIZARE A REȚELELOR 4G

Nicolae BOTNAREVSCHI

Universitatea Tehnică a Moldovei, Facultatea Electronică și Telecomunicații,
Departamentul Telecomunicații și Sisteme Electronice, IMTC-161/fr, Chișinău, Republica Moldova

Rezumat. *În prezentul articol urmează a fi analizate principalele scenarii de atac a infrastructurii de semnalizare a operatorilor de telefonie mobilă 4G. Vor fi analizate modul de acțiune al răufăcătorilor, posibilele pierderi pricinuite operatorului de telefonie mobilă precum și a abonaților săi în urma atacului. De asemenea, vor fi analizate modalitățile de protecție și prevenire al atacului atât din partea operatorului cât și al abonatului.*

Cuvinte cheie*: Protocolul DIAMETER, Protocolul SS7, Securitate informațională, Escrocherie mobilă, Atac cibernetic, Vulnerabilitate de securitate informațională.*

Introducere

Rețelele de telefonie mobilă în baza tehnologiilor 4G, pe an ce trece devin din ce în ce mai populare. La etapa actuală majoritatea operatorilor mari de telefonie mobilă deja propun abonaților utilizarea beneficiilor rețelei 4G cum ar fi viteză ridicată de acces la internet până la 300Mbps, calitatea sporită a serviciilor, organizarea de videoconferințe, accesarea instantanee a paginilor web cu conținut și grafică complexă. Se subînțelege că pe lângă toate beneficiile enumerate mai sus abonații solicită și un nivel sporit a calității serviciilor și nu în ultimul rând un nivel sporit de securizare.

Practic toți abonații de servicii 4G într-o măsură mai mare sau mai mică sunt și abonații rețelelor de tehnologii mai vechi cum ar fi rețele 3G. Practic toți operatorii de telefonie mobilă la moment asigură doar transferul de date prin tehnologia 4G, însă expedierea SMS-urilor și transmiterea datelor vocale se efectuează prin rețele 3G, folosindu-se tehnologia Circuit-Switched FallBack, care permite modificarea periodică a tehnologiei utilizate. Licurul acesta poate fi observat la majoritatea smartfoanelor, unde lângă indicatorul de rețea “4G” în timpul apelurilor vocale se modifică pe “3G”, “H”, “E” sau chiar “G”. În acest moment de timp abonatul devine vulnerabil față de riscurile de securitate din rețele de generație trecută.

Mulți pot afirma că în rețelele de telefonie mobilă 4G protocolul drept protocol de semnalizare a fost modificat de pe SS7 caracteristic rețelelor 2G, 3G pe protocolul DIAMETER caracteristic rețelelor 4G și respectiv 5G. Însă, din păcate, protocolul DIAMETER folosit într-o măsură mai mare sau mai mică este supus exact la aceleași vulnerabilități ca și protocolul SS7.

Componentele și protocoalele de bază a EPC (Evolved Packet Core)

Comparativ cu rețelele de generație anterioară, rețeaua 4G este construită după principiul All IP Network, ceea ce a permis transmiterea sub formă de pachete atât a datelor cât și a traficului vocal. Din aceleași considerente structura EPC a devenit mai simplă, ceea ce a dus la sporirea randamentului rețelei și la sporirea vitezei de transmisie atât a datelor de la abonat cât și a informațiilor de serviciu. De fapt, rețeaua 4G este construită din câteva blocuri critice cum ar fi HSS, MME, P-GW(PCEF), S-GW, OCS/OFCS, PCRF, și respectiv stația de bază denumită eNodeB și echipamentul abonatului.

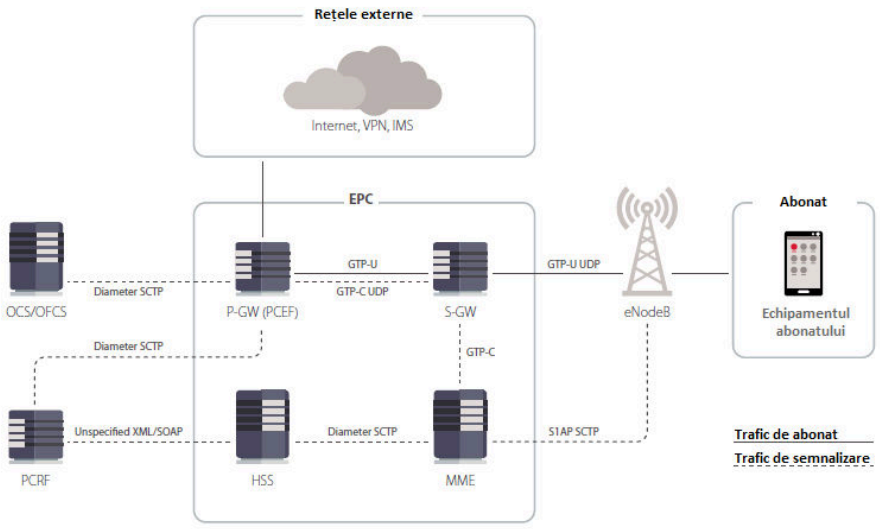

Figura 1. Structura generalizată a EPC

HSS sau Home Subscriber Server, reprezintă prin sine o bază de date imensă ce reunește câteva componente a rețelelor anterioare cum ar fi VLR, HLR, AUC, EIR, și este destinată pentru păstrarea informațiilor despre abonați.

S-GW sau Service Gateway asigură transmisia și prelucrarea informațiilor de la abonat dintre echipamentele abonaților și stațiile de bază eNodeB.

PCRF sau Policy and Charging Rules Function - este un element din rețeaua celulară LTE, responsabilă pentru tarificarea și gestionarea facturilor pentru serviciile folosite. Permanent interacționează cu seriviciul de Biling al operatorului.

MME sau Mobility Management Entity reprezintă un nod de control a mobilității rețelelor LTE. Este folosit pentru prelucrarea informației de semnalizare, legată de gestiunea mobilității abonaților în cadrul rețelei.

Tipuri de atac

Un interes sporit pentru răufăcători îl reprezintă interfețele specializate, prin care are loc schimbul de date dintre elementele EPC (Elowed Packet Core). Printre aceste interfețe are loc atât transportul informațiilor de serviciu dintre elementele rețelei, cât și transportul informațiilor de la de abonat, așa numitul trafic de semnalizare. Luând în considerare că interfețele nu dispun de un mecanism intern de criptare a datelor transmise, răufăcătorul poate înfăptui următoarele atacuri:

- Interceptarea identificatorilor personali ai abonatului cum ar fi MSISDN, IMSI
- Determinarea locației abonatului
- Atac de tipul "persoană la mijloc", ceea ce permite interceptarea credențialelor către poșta electronică, credențialelor de acces la careva servicii web, etc.
- Interceptarea SMS-urilor
- Ascultarea apelurilor VoLTE prin metoda interceptării pachetelor
- Crearea sesiunilor false din numele abonatului în scopuri de fraudă
- Atacuri de tip DoS sau DDoS, asupra abonatului care vor cauza pierderi în transmiterea datelor, iar în timpul apelurilor VoLTE vor provoca întreruperea apelului
- Atacrui de tip DoS, DDoS asupra echipamentului sau a infrastructurii în întregime a operatorului.

Scenariile majorității covârșitoare a atacurilor, sunt bazate pe exploatarea vulnerabilităților din cadrul furnizării serviciilor de roaming și a deficiențelor interacțiunii inter-operatorii prin rețeaua GRX (GPRS Roaming Exchange, sau schimbului de date în roaming în mediul GPRS). Traficul de semnal și de utilizator depășește limitele rețelei unui singur operator și este transmis

atât prin rețeaua de tranzit GRX, cât și prin rețeaua operatorului oaspete. Pentru a asigura autentificarea și aplicarea regulilor tarifare pentru utilizatori, participanții la schimbul inter-operator interacționează între ei prin interfețe deschise. Și respectiv un atăcător poate profita de disponibilitatea acestor interfețe pentru a efectua atacuri asupra abonaților sau asupra echipamentelor unui operator de telecomunicații.

Scenariu de atac de tip DoS asupra abonatului

În nucleul EPC, este posibilă efectuarea a câtorva scenarii de atac cibernetic, ce vor conduce la un atac de tip DoS, ce va conduce la blocarea conexiunii la rețeaua operatorului a echipamentului de abonat. În cazul în care conexiunea este întreruptă o singură dată, atunci după restartarea echipamentului abonatul se va reconecta la rețea. Dar în cazul în care atacatorul va transmite continuu mesaje false către MME atunci conexiunea la rețea a abonatului va fi întreruptă pe întreaga durată a atacului. Astfel de acțiuni vor afecta negativ calitatea serviciilor prestate, încrederea și loialitatea abonaților față de operator.

Un asemeni tip de atac devine posibil de realizat în cazul în care lipsește, sau nu este configurat corect procesul de verificare a identității expeditorului, când din numele a S-GW, răufăcătorul, expediază o solicitare GTP-C “Delete Bearer Request” către MME, cu indicarea a TEID a abonatului țintă și adresa IP a S-GW.

De asemenea, este posibilă blocarea periodică a accesului la rețea, când răufăcătorul va afla TEID a sesiunii curente a abonatului și va îndrepta un request de tip “Delete Session Request” către gătre P-GW. Scenariul atacului va fi indicat în Figura 2.

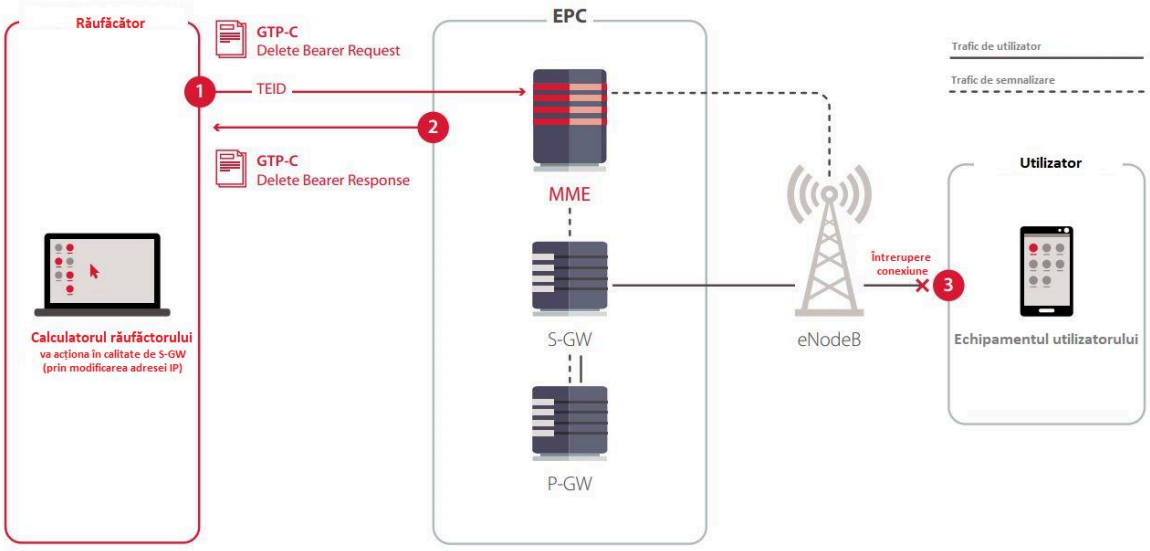

Figura 2. Reprezentarea grafică a unui atac de tip DoS asupra echipamentului de abonat

În cazul în care atacul a avut loc cu succes conexiunea la rețea a abonatului va fi întreruptă imediat și reconectarea va fi posibilă după restartarea echipamentului.

Concluzie

Furtul banilor, determinarea locației abonatului, interceptarea SMS-urilor și a apelurilor vocale sunt doar cele mai evidente oportunități pe care le poate câștiga un răufăcător în urma unui atac cibernetic asupra infrastructurii de semnalizare asupra unui operator sau al altuia. Din câte arată experiența Ucrainei, Irak, Siria, sau al altor zone de conflict, manipulările cu rețele de telefonie mobilă prin dezinformarea abonaților pot conduce la escaladarea revoltelor în masă.

De asemenea, luând în considerare aria sporită de acoperire, costuri scăzute la echipamentele de utilizatori, vitezele sporite de transmisie a datelor, rețelele LTE se utilizează în masă pentru dirijarea la distanță cu procesele tehnologice a diferitor întreprinderi, a altor procese vitale în funcționarea unor întreprinderi și a statelor în întregime.

Dacă operatorii de telefonie mobilă nu vor începe activ implementarea unor sisteme adecvate de securizare a infrastructurii de semnalizare atât pe baza protocolului DIAMETER cât și SS7 atunci jertfele unor atacuri cibernetice pot deveni nu doar abonați sau întreprinderi, ci, chiar țări în întregime.

Conform rapoartelor analitice publicate de Positive Technologies și a recomandărilor ENISA pentru asigurare unui grad admisibil de securitate e suficientă:

- Monitorizarea traficului DIAMETER și SS7 în cazul în care în rețea se utilizează procedurile de Circuit-Switched FallBack
- Inventarizarea nodurilor din rețeaua de semnalizare atât SS7 cât și DIAMETER
- Verificarea funcții de filtrare a request-urilor de semnalizare
- Analiza posibilităților de realizare a atacurilor și a fraudelor tehnologice
- Depistarea și înlăturarea vulnerabilităților de securitate a protocoalelor și a erorilor de configurare a echipamentelor etc.

Conducător: Andrei CHIHAI

Referințe

Cărți:

1. ТИХВИНСКИЙ В.О., ТЕРЕНТЬЕВ С.В., ЮРЧУК А.Б. *Сети мобильной связи LTE. Технологии и архитектура*. Москва: Эко-Трендз, 2010.

Referinţe Web:

2. CICHONSKI J., FRANKLIN J.M., BARTOCK M., *Guide to LTE security* [online]. 2017, [accesat 08.02.2020]. Disponibil: https://doi.org/10.6028/NIST.SP.800-187

Reglementări legale și legi, organizații:

3. RFC6733, *Internet Engineering Task Force* (IETF) [online]. 2012, [accesat 08.02.2020]. Disponibil: https://tools.ietf.org/html/rfc6733