ApTI– Asociația pentru Tehnologie și Internet
info@apti.ro
www.apti.ro

27 mai 2013

Punctul de vedere al ApTI referitor la Proiectul de Decizie privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și raportarea incidentelor cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice

Cu privire la Proiectul de Decizie privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și raportarea incidentelor cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice, supus consultării publice de către ANCOM, vă rugăm să primiți propunerile și comentariile de mai jos ale Asociației pentru Tehnologie și Internet (ApTI), ca reprezentant al societății civile interesat de dezvoltarea unei lumi digitale sigure și deschise.

Având în vedere concluziile desprinse de către ANCOM din cele două studii efectuate în anul 2012 cu privire la securitatea și integritatea serviciilor și rețelelor de comunicații electronice, conform cărora *„doar o parte dintre furnizori au proceduri clare și documentate pentru asigurarea continuității rețelelor și serviciilor, în majoritatea cazurilor stabilirea unor măsuri de securitate efectuându-se reactiv, în momentul apariției unui incident*”, ApTI consideră că adoptarea unei decizii care să abordeze problema măsurilor minime de securitate ce trebuie luate de către furnizori este o măsură necesară și bine-venită. Astfel, ApTI susține inițiativa ANCOM, și, în urma analizării proiectului de decizie, precum și a cadrului legislativ de bază (în speță, ordonanța de urgență a Guvernului nr.111/2011 privind comunicațiile electronice), propune următoarele:

1. Evaluarea securității rețelelor și serviciilor de comunicații electronice și auditul de securitate

Proiectul de decizie este construit pe baza art.46 și art.47 din OUG nr.111/2011 privind comunicațiile electronice și detaliază obligațiile furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului în ceea ce privește luarea tuturor măsurilor de securitate adecvate pentru administrarea riscurilor care pot afecta securitatea rețelelor și serviciilor și notificarea ANCOM cu privire la existența unor incidente cu impact semnificativ asupra securității rețelelor și serviciilor de comunicații electronice.

Analizând prevederile Capitolului IV - Securitatea și integritatea rețelelor și serviciilor de comunicații electronice din OUG nr.111/2011, considerăm că este necesar ca proiectul de decizie să detalieze și prevederile art.49:

Art. 49. - (1) În vederea aplicării prevederilor prezentului capitol, ANCOM poate solicita furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului:

a) să furnizeze toate informațiile necesare evaluării securității și integrității rețelelor și serviciilor, inclusiv politicile interne de securitate aplicabile;

b) să se supună, pe cheltuiala proprie, unui audit de securitate realizat de un organism independent sau de o altă autoritate competentă și să transmită ANCOM rezultatele auditului.

(2) ANCOM poate verifica și evalua măsurile stabilite de furnizori pentru a garanta securitatea și integritatea rețelelor și serviciilor, precum și respectarea acestora în cazurile de încălcare a securității rețelelor și serviciilor sau pierdere a integrității rețelelor, putând impune măsuri în acest sens.

Astfel, suntem de părere că obligația ca furnizorii să stabilească și să implementeze măsuri de securitate în domeniile prevăzute în proiectul de decizie nu poate fi suficientă pentru a „garanta integritatea rețelelor și pentru a asigura continuitatea furnizării serviciilor" (art.46 alin.(3) din OUG nr.111/2011), în lipsa unor proceduri care să permită **verificarea acestor măsuri și evaluarea securității rețelelor și serviciilor, de către ANCOM.**

Astfel, având în vedere prevederile art.49 din OUG nr.111/2011, considerăm că este necesară completarea proiectului de decizie cu o serie de prevederi referitoare la următoarele aspecte:

a) evaluarea măsurilor de securitate (art.49 alin.(2))

- introducerea obligației ca furnizorii să informeze, periodic, ANCOM în legătură cu măsurile de securitate stabilite și implementate în baza art.3 din proiectul de decizie;
- ANCOM să verifice și să evalueze aceste măsuri, urmând să stabilească dacă acestea sunt adecvate pentru a garanta securitatea și integritatea rețelelor și serviciilor;
- în cazul producerii unor incidente de securitate, ANCOM să evalueze dacă furnizorii au respectat măsurile de securitate adoptate;

b) auditul de securitate (art.49 alin.(1) lit.b))

- introducerea obligației ca furnizorii să prezinte ANCOM, anual, rezultatele a două audituri de securitate: un audit realizat intern, de către resurse proprii furnizorilor, și un audit realizat de către un auditor extern independent. În domeniul securității informației, auditul extern este singurul instrument care poate demonstra terților (inclusiv consumatorilor și clienților) că nivelul de securitate implementat este unul adecvat. Eventual, periodicitatea auditului poate să fie diferită în funcție de mărimea operatorului. Este foarte probabil ca marii operatori deja să facă aceste audituri, astfel încât costurile de implementare să fie mici sau 0.

c) măsuri pentru rezolvarea problemelor identificate

- dacă, în urma evaluării măsurilor de securitate implementate de către furnizori, precum și a rapoartelor de audit, ANCOM identifică o serie de probleme de securitate la nivelul furnizorilor, să poată să impună (sau cel puțin să recomande, iar, dacă nu se respectă, să facă public acest lucru) acestora adoptarea anumitor măsuri care să contribuie la rezolvarea problemelor identificate.

2. Recomandări ANCOM privind soluționarea problemelor de securitate identificate de experți independenți

În momentul de față există cercetători/experți în securitate informatică, români și străini, care, în urma activităților de cercetare desfășurate, identifică riscuri și vulnerabilități la adresa securității rețelelor și serviciilor de comunicații electronice. Mai multe exemple de astfel de vulnerabilități actuale și nerezolvate de operatori români sunt prezentate în anexă și se referă la securitatea rețelelor de telefonie mobilă.

Pentru a încuraja astfel de activități de cercetare și pentru a crea o punte de legătură între acești cercetători, pe de o parte, și furnizori și autoritatea de reglementare, pe de altă parte, considerăm că ar fi util ca ANCOM să organizeze, anual, o întâlnire cu furnizorii de rețele și servicii de comunicații electronice și cu cercetători/experți independenți, în cadrul căreia să poată fi semnalate și discutate vulnerabilitățile identificate la nivelul rețelelor și serviciilor de comunicații electronice.

Ulterior acestor discuții, ANCOM ar putea să emită o serie de recomandări (sau chiar obligații, în contextul punctului 2) către furnizori cu privire la soluționarea problemelor de securitate semnalate și să urmărească punerea în aplicare a acestor recomandări sau obligații.

3. Sancțiuni pentru nerespectarea obligațiilor referitoare la măsurile de securitate și la notificarea încălcării securității

OUG nr.111/2011 prevede, la art.142 și art.143, că nerespectarea obligațiilor furnizorilor de a lua toate măsurile adecvate pentru administrarea riscurilor care pot afecta securitatea rețelelor și serviciilor și de a notifica încălcarea securității reprezintă contravenții și se sancționează cu amenzi.

Considerăm că este necesar ca proiectul de decizie ANCOM să facă referire la aceste sancțiuni, astfel încât furnizorii să fie pe deplin informații în legătură cu riscurile la care se expun în cazul nerespectării tuturor prevederilor deciziei.

4. Notificarea incidentelor de securitate

Întrucât furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a notifica ANCOM în legătură cu incidentele care au „un impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice”, considerăm că ar fi util ca raportul anual de activitate al ANCOM să conțină o serie de informații generale referitoare la aceste notificări: numărul incidentelor notificate, o descriere sumară a acestor incidente (informații care pot fi publicate fără a genera riscuri), durata de timp în care respectivele incidente au fost soluționate, câte dintre aceste incidente au fost notificate publicului și/sau clienților afectați.

Printr-o astfel de măsură se va asigura o mai bună informare a utilizatorilor de rețele și servicii de comunicații electronice, mai ales având în vedere faptul că furnizorii nu au obligația de a îi notifica în legătură cu toate incidentele de securitate survenite la nivelul rețelelor și serviciilor de comunicații electronice.

5. Sintagma „securitatea și integritatea rețelelor și serviciilor de comunicații electronice”

În proiectul de decizie se folosește sintagma „securitatea și integritatea rețelelor și serviciilor de comunicații electronice”, care este definită drept „capacitatea unei rețele sau a unui serviciu de comunicații electronice de a rezista evenimentelor, accidentale sau rău intenționate, care pot compromite sau afecta continuitatea furnizării rețelelor și serviciilor la un nivel de performanță echivalent cu cel anterior producerii evenimentului”.

Întrucât, în practică, integritatea reprezintă, de fapt, o componentă a securității, alături de confidențialitate și disponibilitate, propunem utilizarea sintagmei „securitatea rețelelor și serviciilor de comunicații electronice” în locul celei de „securitate și integritate a rețelelor și serviciilor de comunicații electronice” în tot cuprinsul proiectului de decizie și definirea acesteia prin referire la cele trei noțiuni de confidențialitate, integritate și disponibilitate:

„securitatea rețelelor și serviciilor de comunicații electronice - capacitatea unei rețele sau a unui serviciu de comunicații electronice de a rezista evenimentelor, accidentale sau rău intenționate, care pot compromite sau afecta **confidențialitatea, integritatea și disponibilitatea informațiilor, precum și** continuitatea furnizării rețelelor și serviciilor la un nivel de performanță echivalent cu cel anterior producerii evenimentului”.

În susținerea acestei propuneri, menționăm că în Strategia de securitate cibernetică a României, adoptată prin hotărârea Guvernului nr.271/2013, sintagma „securitate cibernetică” este definită prin raportare la confidențialitatea, integritatea și disponibilitatea informațiilor, astfel:

*„securitate cibernetică - starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea**, integritatea, disponibilitatea, autenticitatea şi non-repudierea informațiilor** în format electronic, a resurselor şi serviciilor publice sau private, din spațiul cibernetic.”*

Cu stimă,

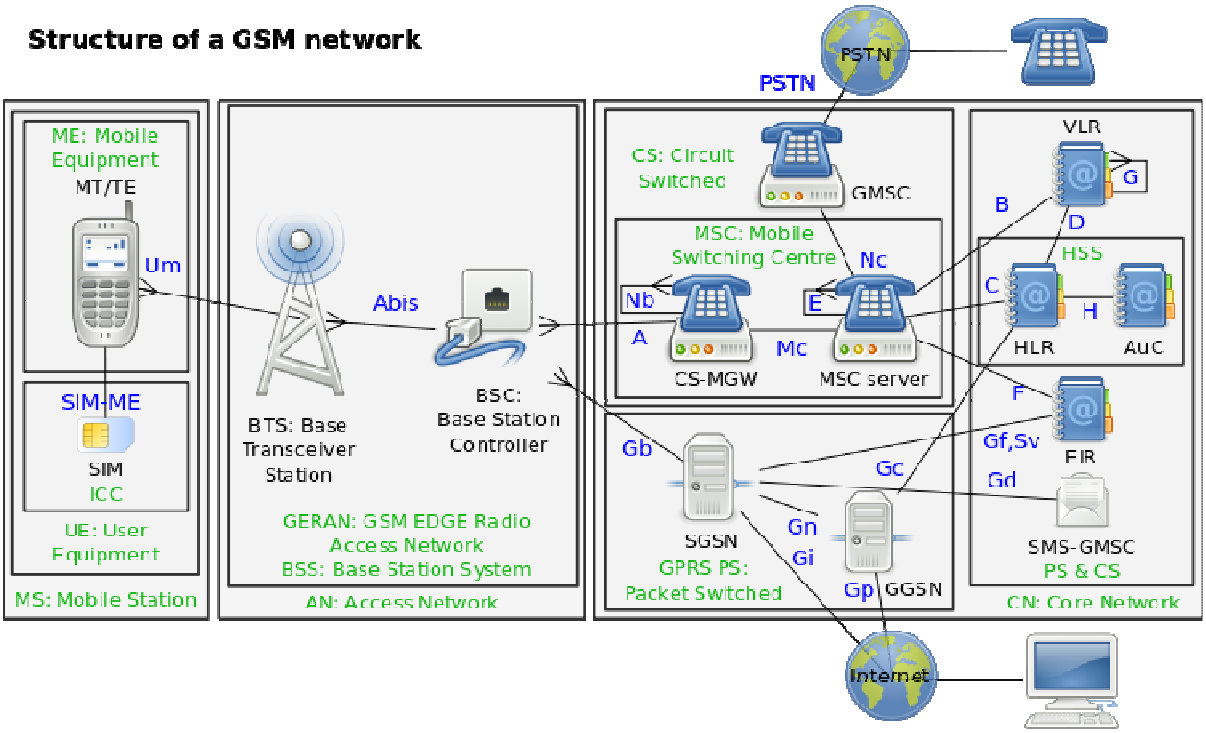
Bogdan Manolea
Director Executiv
ApTI - Asociația pentru Tehnologie și Internet

Anexă

Despre securitatea rețelei de telefonie mobile

GSM (Global System for Mobile Communications) este unul dintre cele mai vechi protocoale de comunicație digital fără fir, fiind și cel mai răspândit.

O structură simplificată a protocolului arată astfel:



Sursa: Wikipedia

Un mare avantaj al acestui protocol este acela că permite criptarea comunicației între telefon și BTS (stația transceiver de bază). Fiind însă un sistem destul de vechi, acesta are și câteva probleme ce țin de securitatea comunicațiilor.

1. Autentificarea și criptarea

Atunci când un telefon cere acces în rețea, aceasta îi va cere telefonului să se autentifice. În timpul acestei autentificări are loc un schimb de chei și răspunsuri pentru a valida accesul. Odată autentificat, BTS-ul îi va cere telefonului să efectueze criptarea comunicației folosind unul din următoarele algoritme de criptare: A5/0 (comunicație necriptată), A5/1 (cea mai folosită metodă), A5/2 (asemănătoare cu A5/1 însă cu o criptare mai slabă), A5/3 (cea mai nouă și puternică metodă de criptare).

Din punct de vedere al securității privind algoritmul de criptare folosit, lucrurile stau astfel:

- A5/0: nu se folosește deloc criptarea comunicațiilor și astfel orice persoană care deține instrumentele necesare poate captura și vedea în text clar schimbul de informații dintre celelalte telefoane și BTS;
- A5/2: criptare foarte slabă, poate fi decriptat în timp real, astfel încât, începând cu anul 2007, 3GPP a interzis folosirea acestui algoritm în noile telefoane (http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_37/Docs/SP-070671.zip);

- A5/1: algoritmul folosit cel mai intens în prezent, inclusiv de către operatorii de telefonie mobilă din România. În cadrul conferinței de securitate BlackHat din 2009 a fost anunțat faptul că acest algoritm a fost spart și astfel se poate decripta traficul interceptat (https://srlabs.de/decrypting_gsm/);
- A5/3: cel mai puternic algoritm, încă nu a fost decriptat.

Pe baza celor prezentate anterior, există câteva probleme de securitate ce afectează în prezent operatorii de telefonie din România:

a) Autentificarea într-un singur sens: telefonul mobil se autentifică la BTS, însă nu există o autentificare a BTS-ului în sine. Efecte: telefonul se conectează la cel mai puternic semnal, astfel încât cineva care își creează propriul BTS și emite cu o putere mai mare va determina ca telefonul să se conecteze la acest BTS fals. Mai mult, stația transceiver alege modalitatea de criptare, ceea ce înseamnă că poate impune telefonului să nu folosească niciun fel de criptare. În acest mod, interceptarea întregii comunicații (voce, SMS, date) va fi ușor de făcut. Un exemplu care poate fi mai bine înțeles este în cazul comunicării, prin tehnologia wireless (fără fir), a unui computer cu un router. Computerul se conectează la rețeaua wireless care deține cel mai puternic semnal, presupunând că există două astfel de rețele ce au același nume. Dacă o persoană rău-voitoare deține controlul stației cu cel mai puternic semnal, atunci orice schimb de informații poate fi văzut, citit, ascultat. Pe piață există o serie de astfel de echipamente, denumite ***IMSI catcher***, ce capturează traficul dintre telefon și BTS prin crearea unui BTS fals. (http://www.alibaba.com/industry-promotion/imsi-catcher-industry-promotion.html)

Din păcate, pentru această problemă nu există o soluție pe care operatorii o pot implementa. Totuși, publicul ar trebui să fie înștiințat și conștient de existența acestei probleme.

b) **Algoritmi de criptare cu securitate slabă:** așa cum menționam anterior, rețelele de telefonie GSM din România utilizează criptarea A5/1, algoritm care s-a dovedit a nu fi unul tocmai puternic. Fiecare pachet schimbat între telefon și stație are o lungime de 23 bytes, astfel încât, dacă informația în sine are o lungime mai mică, se va umple până când atinge 23 bytes. În majoritatea cazurilor valoarea acestui octet este 2B.

SDCCH trace	
238530	03 20 0d 06 35 11 **2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b**

Captură pachet SDCCH ce conține octeți pentru completarea lungimii

Această problemă poate fi rezolvată parțial dacă acești octeți sunt toți diferiți. Rezolvarea parțială vine din faptul că timpul necesar pentru decriptare crește exponențial de 2 ori pentru fiecare byte diferit. Organizația globală 3GPP (The 3rd Generation Partnership Project), care se ocupă de standardul GSM, a recomandat încă din anul 2008 ca acești bytes de umplere să fie aleatorii.

When sent by the network, either the octets containing fill bits shall take the binary value "00101011", ***or each fill bit shall be set to a random value****. When sent by the mobile station, either the octets containing fill bits shall take the value "00101011" or "11111111",* ***or each fill bit shall be set to a random value.*** 3GPP TS44.006, Section 5.2, pagina 12

Operatorii de telefonie mobilă din România folosesc în continuare aceiași octeți de completare, fiecare cu valoarea standard 2B.

Metoda anterior expusă este cea mai rapidă și simplă de implementat pentru a împiedica decriptarea mesajelor GSM. O altă metodă mai greu de implementat, dar care ar aduce un plus de securitate, o reprezintă schimbarea ordinii în care mesajele de tipul *System Information* au loc.

2. Subscriber Identity Module (SIM)

Cartela SIM este practic un circuit integrat pe care sunt stocate informații precum IMSI (International Mobile Subscriber Identity), chei de autentificare în rețeaua de telefonie mobilă, dar și aplicații ce poartă denumirea de SIM Application Toolkit (SAT). Aceste aplicații permit cartelei să inițieze singure diverse acțiuni (apelare vocală, trimiterea de mesaje scurte etc.).

Tocmai din această capabilitate a SIM-ului de a prelua controlul a fost identificată o problemă în standardul 3GPP. În mod obișnuit, operatorii pot controla de la distanță aplicațiile scrise pe cartelă, întrucât aceștia dețin cheile de criptare necesare. Astfel, operatorii trimit un mesaj text de tip comandă, ce va fi adresat direct SAT. Totuși, oricine poate trimite astfel de mesaje urmărind specificațiile 3GPP, chiar dacă nu are cheile corecte. În comanda transmisă, care, practic, reprezintă un SMS, modulul SIM este instruit să răspundă cu statusul execuției acestei comenzi: dacă a fost executat cu succes sau nu. Întrucât răspunsul pleacă către numărul care a trimis comanda, asta înseamnă că orice telefon poate fi controlat de la distanță pentru a trimite singur mesaje către orice număr, inclusiv numerele cu suprataxă. Pentru detalii https://vimeo.com/37593949

Operatorii pot împiedica exploatarea acestei vulnerabilități prin filtrarea mesajelor scurte (SMS), astfel încât cele ce sunt trimise de către clienți să nu fie de tip SIM Toolkit. În România, toate rețelele GSM / 3G /4G ale operatorilor sunt afectate, cu excepția operatorului S.C. COSMOTE Romanian Mobile Telecommunications S.A., care nu are o aplicație SIM Toolkit pe cartelele proprii.

3. Identitatea apelantului

Sistemele operatorilor de telefonie mobilă se bazează pe identitatea apelantului pentru autentificarea la servicii precum mesageria vocală, sisteme IVR (Interactive Voice Response) etc.

Astfel, au fost identificate câteva probleme:

a) majoritatea sistemelor IVR cer utilizatorului să introducă numărul de telefon înainte de a-i fi prezentate celelalte opțiuni, în cazul în care se apelează prin folosirea numărului lung (format E.164). În acest caz, chiar dacă se introduce un alt număr decât cel alocat respectivului abonat, sistemul permite accesul și astfel se pot iniția o serie de acțiuni precum activarea/dezactivarea unor servicii, modificarea planului tarifar, schimbarea setărilor etc.

Pentru a rezolva această problemă, operatorii pot bloca accesul la modificări privind opțiunile active, lăsând liber doar accesul către interacțiunea cu un operator al serviciului de relații clienți.

b) prin existența unor servicii ce permit modificarea apelantului (a numărului de apel), deoarece autentificarea este făcută strict pe baza acestui număr, se poate avea acces la sisteme precum mesageria vocală, relații clienți, etc. Astfel, datele private ale clienților sunt expuse oricui.

Soluția este de a implementa toate serviciile după principiul „security by default”. Pentru sistemele IVR: să se permită accesul doar la a intra în legătură cu un operator (în cazul apelului făcut către numerele în format lung). Pentru mesageria vocală: fiecare nou client (fie post sau prepay) să aibă dezactivată mesageria vocală, iar la primul acces utilizatorul să își definească o parolă ce va fi întotdeauna cerută; pentru clienții existenți, să fie cerută întotdeauna parola deja definită, indiferent de modalitatea de acces.