IDENTIFICAREA VULNERABILITĂTILOR SS7

Autor: Daria STUPINA, student SI-141

Universitatea Tehnică a Moldovei, catedra Automatică și Tehnologii Informaționale

ABSTRACT: *SS7 este folosită de mai mulți operatori din lume, atât pentru rețeaua celulară, cât și pentru rețele cu fir. Acest set de protocoale a devenit foarte popular din cauza trecerii la IP și a conectării ușoare a tehnologiilor noi la rețele SS7 existente, folosind porți de semnalizare. Este și una din tehnologiile de baza ale rețelelor 2G și 3G. Deci este foarte important de analizat problema securității și de identificat vulnerabilitățile pentru protejarea eficientă a confidențialității, integrității și disponibilității sistemelor, pe care le folosim în fiecare zi.*

CUVINTE CHEIE*: SS7, vulnerabilitatea, SIGTRAN, SMS, IMSI, interceptarea.*

Introducere

Procesul de setare a apelurilor voce în telefoanele mobile actuale este bazat pe tehnologia SS7, proiectată în anii 70 secolul trecut. Securitatea protocoalelor era bazată pe protecția fizică a nodurilor și canalelor de comunicație, obținerea accesului nesancționat în rețeaua SS7 era imposibilă. La începutul anilor 2000 a fost dezvoltată specificația SIGTRAN, care a permis transmiterea mesajelor SS7 prin rețele IP. Astfel, au fost moștenite toate slăbiciunile de securitate a protocoalelor SS7. În rezultat, răufăcătorii au posibilitatea de a trimite, intercepta și schimba fără control mesajele protocoalelor SS7, executând diferite atacuri la rețele mobile și abonații lor.

1. Pregătirea pentru un atac

Pentru un atac răufăcătorul are nevoie de un calculator pe baza Linux SO, pe care instalează un soft, care lucrează ca echipamentul operatorului. Acest soft poate fi găsit pe Internet cu acces liber. Doar că mai este nevoie de conectare ca operator, ceea ce este cel mai dificil într-un atac. În unele țări, răufăcătorii au mai multe posibilități de a cumpăra licența de operator pe piața neagră. Oricum, un răufăcător poate să găsească licența și la unele Onion website-uri**.**

2. Determinarea locației abonatului

Pentru determinarea locației abonatului *la primul pas* trebuie de repetat acțiunile ce duc la obținerea IMSI abonatului și adresa comutatorului care îl deservește. Aceasta se face prin mesaj SRIFSM. Răufăcătorul emulează lucrul centrului-SMS.

La această etapă este posibil de trimis o solicitare la baza de date a comutatorului, dar în acest caz există o posibilitate de a primi o informație inexactă, deoarece nu este cunoscut, dacă telefonul abonatului a făcut careva acțiuni active în celula, în care el este prezent. Pentru a afla locația lui, trebuie de forțat telefonul abonatului să facă așa tip de acțiuni, dar fără că abonatul să observe.

Standardul pentru mesajele SMS implică posibilitatea de a genera un mesaj astfel, ca aceasta să fie invizibil pentru abonat. Este numit Silent SMS. Telefonul primește mesaj, dar nu dă nici-un semnal și nu afișează pe el în lista mesajelor primite.

La pasul al doilea, răufăcătorul continuă emularea lucrării centrului-SMS. El trimite Silent SMS abonatului, cu operația MT-ForwardSM. Mesajul merge la comutator, adresa cărora era primită la primul pas, dar adresarea abonatului este efectuată prin IMSI. După trecerea acestui mesaj, informația despre locația abonatului în baza comutatorului se actualizează, conținând datele despre LAC și CID actuale.

La pasul trei, rămâne de trimis solicitare la comutator pentru primirea datelor despre celula care deservește abonatul. Acest lucru este făcut cu mesajul ProvideSubscriberInfo, care trece la comutator, abonatul este adresat prin IMSI, pe care deja le cunoaștem. În rețele de comunicare mobilă acest mesaj este folosit pentru transmiterea informației despre locația abonatului, care este apelat pentru tarifare online. Dacă abonatul este în roaming, se conectează schema de tarifare potrivită.

Mesajul ProvideSubscriberInfo returnează un set de identificatori ai celulei care le servește – MCC (Mobile Country Code), MNC(Mobile Network Code), LAC, CID. În Internet este posibil de găsit multe servicii, care dau posibilitatea de a determina coordonatele geografice a stației de bază și zona de acoperire a unei celule.

4. Blocarea apelurile de sosire

Pentru a bloca apelurile de sosire pentru abonat trebuie doar de trimis în rețeaua de casă un mesaj UpdateLocation de la numele MSC.

Atacul poate fi descris după pașii următori:

A. Un mesaj trece la HLR. Abonatul adresează după identificatorul IMSI și UpdateLocation – adresa unui nou comutator.

B. HLR în baza sa dezleagă comutatorul real.

C. HLR trimite profilul abonatului la echipamentul răufăcătorului.

Deci, abonatul trebuie să fie în afara zonei de acoperire a rețelei pentru apelurile de sosire până când nu se întâmplă una din acțiuni: abonatul trece în zona de acoperire a altor comutatoare, abonatul își repornește telefonul mobil, abonatul face un apel sau trimite mesaj-SMS.

Oricare din aceste acțiuni activează procedura UpdateLocation, care actualizează adresa comutatorului la o adresă reală în baza de date HLR.

5. Interceptarea SMS

Interceptarea SMS este rezultatul unui DoS atac, când răufăcătorul arată adresa echipamentului lui la MSC fals. Se presupune, că răufăcătorul a primit toți identificatorii abonatului ME 1, de care el are nevoie și a făcut un atac DoS reușit, specificând ca un MSC fals adresa nodului lui.

Atacul poate fi descris după pașii următori:

A. Abonatul cu ME 1 trimite mesajul abonatului cu ME 2, acest mesaj ajunge la comutatorul care deservește expeditorul.

B. Comutatorul redirecționează mesajul la centrul-SMS. Aceasta se întâmplă în mesajul MO-ForwardSM al protocolului MAP.

C. Centrul-SMS nu știe unde este acum abonatul cu ME 2, deci el direcționează apelul la HLR în mesajul SRIFSM.

D. Fiindcă abonatul cu echipament ME 2 este victima atacului DoS, în baza de date HLR se conține o informație falsă despre locația lui. Pe această informație falsă HLR trimite la centrul-SMS în mesaj de răspuns SRIFSM.

E. Centrul-SMS direcționează mesajul SMS la adresa obținută prin mesajul MT-ForwardSM protocolului MAP.

6. Manipularea USSD-cererilor

Atacul de manipulare a USSD-cererilor este analogică unui mesaj legitim cu USSD-cerere, trimis de la VLR la HLR. Datele necesare sunt: numărul de telefon al abonatului, adresa HLR și un șir de USSD-cereri. Numărul de telefon este cunoscut de la început, iar adresa HLR se poate obține printr-un atac decris în punctul 3, iar descrierea USSD-cererilor se poate găsi din pagina oficială a operatorului. În rezultat, răufăcătorul are posibilitatea de a transfera fonduri între conturile utilizatorilor. Acest tip de atac poate rămâne neobservat mult timp, dacă răufăcătorul folosește și un atac de interceptare a mesajelor SMS, pentru interceptarea mesajelor de amenințare despre manipulanții de cont.

7. Substituire profilului abonatului în VLR

În procesul de înregistrare a abonatului pe comutator profilul lui copiază din baza de date HLR în baza de date VLR. Un profil constă din informația despre serviciile activate și dezactivate ale abonatului, parametrii de readresare, adresa platformei de tarifare online și alte detalii. Un atacator poate face trimiterea în VLR fals al profilului abonatului.

În acest caz, atacatorul are nevoie de numărul de telefon, IMSI al abonatului, adresa VLR și detalii despre profilul abonatului. IMSI și adresa VLR atacatorul le obține printr-un atac de determinare a identificatorului IMSI, iar detaliile despre profil se obțin printr-un atac DoS.

Un profil fals forțează MSC/VLR de a servi abonatul în conformitate cu parametrii oferiți de răufăcător. De exemplu, abonatul poate face apeluri fără tarifare.

Atacul de profil fals poate fi folosit la fel și pentru interceptarea convorbirilor telefonice.

8. Interceptarea apelurilor de sosire

Interceptarea apelurilor de sosire este continuarea atacului de substituire a profilului. În profilul abonatului-victimă, răufăcătorul schimbă adresa platformei de tarifare, specificând adresa echipamentului pe care îl controlează. După aceste acțiuni, în momentul unui apel de ieșire al abonatului, cererea de tarifare trece la echipamentul răufăcătorului. Această cerere conține numărul abonatului, la care trece apelul. Răufăcătorul are

posibilitatea de a readresa apelul de voce la echipamentul lui și face un apel-conferință pentru trei părți: abonatul care face apelul, abonat la care trece apelul și abonatul care interceptează.

În rezultat, traficul de voce decodificat trece prin echipamentul răufăcătorului și se returnează la abonat. Conversație va avea loc, dar partea a treia va participa nesancționat.

9. Readresarea apelurilor de sosire

Atacul de readresare a apelurilor de sosire este bazat pe scenariul apelului de sosire și este continuarea atacului DoS. La apelul de sosire MSC (GMSC) se transmite cerere la HLR în scopul determinării zonei MSC/VLR a abonatului. Avem nevoie de această informație pentru rutarea apelului la comutatorul potrivit.

După atacul DoS, HLR readresează cererea, pe care el a primit-o, pe un MSC/VLR fals, care trimite numărul pentru readresarea apelului (MSRN). HLR transmite acest număr la GMSC, care realizează readresarea apelului la MSRN furnizat.

În rezultat, atacatorul influențează mecanismul de rutare a apelurilor de voce. Astfel, se readresează apelul de sosire adresat abonatului-victima la orice număr.

10. Refuzul în deservire MSC pentru apelurile de sosire

Pe baza atacului de refuz în deservire MSC pentru apelurile de sosire, este procedura de selectare a numărului de roaming (MSRN) la setarea apelului de sosire. În timpul apelului, mai întîi se determină MSC/VLR actual pentru abonat și apoi crearea unui canal de voce pentru acest comutator. Pentru aceasta se folosește un număr roaming temporar. În situația normală timpul de viață a unui număr roaming este mai mic decât o secundă. Dar valorile timer-ilor pentru retenția numărului de roaming, date în echipament sunt de 30 – 45 de secunde. Prin transmiterea cererilor la comutator în mod masiv, răufăcătorul poate întrerupe posibilitate de a efectua apeluri telefonice de sosire, deoarece numerele de roaming pot fi cheltuite.

În acest atac, răufăcătorul are nevoie numai de IMSI unui abonat și adresa comutatorului și să fie indisponibili toți abonații, care sunt în zona de deservire a acestui comutator.

Concluzii

Vulnerabilitatea rețelelor de comunicație celulară pe baza tehnologiei SS7 dă posibilitate unui răufăcător de a realiza atacuri serioase, rezultatul cărora poate fi pierderea banilor abonaților, spargerea datelor confidențiale sau încălcarea disponibilității abonaților și elementelor de rețea în privința intereselor părților terțe.

Cert este că acum oamenii mai mult comunică prin aplicații, care sunt numite messenger-i. Dar dacă luăm ca exemplu Telegram, care la intrarare are nevoie de o SMS confirmare înțelegem că situația este deja mai dificilă. Sau, de exemplu, dacă un răufăcătorul, specializat în spargerea conturilor bancare, este interesat de a obține parola unică de la bancă a victimelor pentru efectuarea plății.

Interceptarea SMS poate fi folosită și în cazurile când victimele recuperează parolele pentru diferite servicii din Internet, ca poșta electronică, rețele sociale, portaluri de servicii diferite etc.. Toate aceste servicii pot conține informație confidențială, valoarea ei fiind destul de mare.

Mulți operatori mobili solicită parola de acces în biroul personal prin SMS. Accesând datele de acces un răufăcător poate să controleze servicii, să transfere fonduri între conturi, să primească istoria mesajelor SMS etc.. Determinarea locației abonatului, de asemenea, este o posibilitate pentru răufăcători, să amenințe confidențialitatea.

La nivel global putem să vorbim și despre manipularea prin comunicațiile mobile în zonele de conflict, ce poate aduce la consecințe globale. Prin Internet mobil, comunicarea celulară devine unul din mijloacele de penetrare a altor infrastructuri importante.

Bibliografie

1. *Trust in Cyberspace*, Fred B. Schneider, Editor , Committee on Information Systems Trustworthiness (Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council) National Academy Press, Washington, D.C. 1998

http://cryptome.org/tic.htm [23.04.16]

2. *Report of the Defense Science Board Task Force on Defensive Information Operations* (2000 Summer Study, Volume II), March 2001

http://www.au.af.mil/au/awc/awcgate/dod/dsb_protecting2.pdf [23.04.16]

3. Here's Why Anyone Could Hack Your Phone, Shane Harris, April 23, 2016

http://www.thedailybeast.com/articles/2016/04/23/here-s-why-anyone-could-hack-your-phone.html [24.06.16]

4. *Signalling Transport* (sigtran). – The Internet Security, 1999-2007

https://datatracker.ietf.org/wg/sigtran/documents/ [04.07.16]
5. *HOW EASY IS IT TO HACK A CELLULAR NETWORK*, 2015
https://blog.kaspersky.com/hacking-cellular-networks/10633/ [05.07.16]
6. *The corresponding Relations of SS7 with OSI seven layer architecture*, 2014
http://facekhmer21.blogspot.md/2014/02/ss7-basic-protocol-introduction.html [11.07.16]
7. *Raport pentru conferința PHDays*, 2014
http://www.ptsecurity.ru/ [08.07.16]
8. *AdaptiveMobile launches SS7 Protection to secure operator core networks against privacy and fraud attacks*, 2015
https://www.adaptivemobile.com/press-centre/press-releases/adaptivemobile-launches-ss7-protection [08.07.16]