**ROMÂNIA**

**MINISTERUL APĂRĂRII NAȚIONALE**

**ACADEMIA TEHNICA MILITARĂ**

**„FERDINAND I”**

**FACULTATEA DE SISTEME INFORMATICE ȘI SECURITATE CIBERNETICĂ**

**Specializarea: Calculatoare și sisteme informatice pentru apărare**

**și securitate națională**



***Aplicație destinată telefoanelor mobile în vederea detecției conectării acestora la stații de***

***bază false care se interpun între terminalul mobil și stațiile de bază ale furnizorilor oficiali***

***de servicii GSM (IMSI CATCHER DETECTOR)***

CONDUCĂTOR ȘTIINȚIFIC:

**Col. conf. univ. dr. ing. BĂDOI ION**

ABSOLVENT:

**Ștefan OLTEANU**

Conţine \_\_\_\_\_\_\_\_\_\_\_ file

Inventariat sub nr\_\_\_\_\_\_\_

Poziţia din indicator: \_\_\_\_

Termen de păstrare: \_\_\_\_\_

**BUCUREȘTI**

**2020**

**ABSTRACT**

**REZUMAT**

**CUPRINS**

[1 INTRODUCERE 10](#_Toc38390063)

[1.1. Importanța temei alese 10](#_Toc38390064)

[1.2. Scopul și obiectivele lucrării 10](#_Toc38390065)

[1.3. Prezentarea metodologiei de cercetare 11](#_Toc38390066)

[1.4. Rezumatul lucrării pe capitole 11](#_Toc38390067)

[2 Clasificarea stațiilor de bază în funcție de legalitate 12](#_Toc38390068)

[2.1. Reglementări cu privire la *Imsi Catcher* 12](#_Toc38390069)

[2.1.1. Utilizarea IMSI Catcher în afara legii 13](#_Toc38390072)

[2.2. Modalități prin care IMSI Catcher exploatează rețeaua 14](#_Toc38390073)

[2.2.1. Rețele de comunicații GSM 14](#_Toc38390074)

[2.2.2. Securitatea în GSM 15](#_Toc38390075)

[6 BIBLIOGRAFIE 15](#_Toc38390076)

**LISTĂ DE FIGURI**

# INTRODUCERE

## Importanța temei alese

Dispozitivele de tip *Imsi Catcher* există încă din anul 1993(1)însă erau mari, greoaie și mai ales scumpe. Datorită acestui lucru și a faptului că existau puțini producători, aceste dispozitive nu au fost folosite decât de unele agenții guvernamentale. În zilele noastre, apariția SDR-urilor[[1]](#footnote-2) a permis crearea unor proiecte de acasă și astfel înmulțirea atacurilor asupra rețelelor GSM. Mai mult, dacă inițial aceste atacuri au fost dezvoltate pentru a putea captura codurile IMSI[[2]](#footnote-3) de la telefoanele din apropiere – de unde vine și numele atacului -, versiunile actuale oferă posibilitatea de a intercepta atât apeluri telefonice cât și mesaje.

Prin urmare, această temă este cu atât mai importantă, cu cât nu există modalități de detectare a acestor atacuri, disponibile publicului larg. De asemenea, intrucât numarul acestora a fost în continuă creștere, este necesară informarea persoanelor cu privire la riscurile la care se expun în momentul în care telefonul se conectează la o stație de bază ce nu aparține unui furnizor de servicii local. Un articol realizat de cei de la Washington Post arată că numărul dispozitivelor de interceptare ilegale, găsite în oraș pe parcursul a mai puțin de două zile, este de aproximativ 18 (2). Așadar, nevoia unei aplicații care să ajute la detectarea acestor atacturi ce pun în pericol drepturile societății, este mai mult decât evidentă.

## Scopul și obiectivele lucrării

Scopul acestei lucrări de licență este acela de a expune problematica atacurilor de tip *Imsi Catcher*, de a evidenția modalități de detecție și nu în ultimul rând de a crea o aplicație Android funcțională care să pună în practică modalitățile precizate mai sus.

Printre obiectivele care trebuiesc atinse pe parcursul rezolvării acestei teme se numără un număr de informații cu ajutorul cărora cititorul iși poate face o idee complexă despre modul de funcționare atât a dispozitivului cu care se realizează atacul cât și a dispozitivului de interceptare. De exemplu:

* informații despre modul în care o rețea GSM functionează și ce puncte slabe are;
* prezentarea pe larg a modalităților prin care un dispozitiv *Imsi Catcher* exploatează rețeaua și reușește să capteze atât locația utilizatorului cât și mesaje sau apeluri telefonice;
* descrierea metodelor folosite în cadrul aplicației pentru a detecta atacul;
* s.a.m.d.

Obiectivul principal este ca la finalul lucrării să se poată demonstra cum se realizează atacul și detecția prin simularea unei stații de bază GSM care să preia semnalul telefonului mobil. Acesta din urmă va trebui să detecteze că celula[[3]](#footnote-4) la care este conectat nu aparține furnizorului de telefonie mobilă la care utilizatorul este abonat.

## Prezentarea metodologiei de cercetare

## Rezumatul lucrării pe capitole

# Clasificarea stațiilor de bază în funcție de legalitate

## Reglementări cu privire la *Imsi Catcher*

Aceste dispozitive folosite în mare parte de agențiile de securitate statală au ridicat probleme în legătură cu libertatea și intimitatea civilă. De aceea folosirea acestora se realizează numai conform regulilor scrise în *Codurile de Procedură Penală* (3)*.*

Orice utilizare a unui dispozitiv de tip *Imsi Catcher* se realizează sub jurisdicția *Convenției Europene a Drepturilor Omului,* care stabilește un nivel minim de protecție atât pentru viața privată a individului cât și pentru corespondența acestuia (4). Toate aceste legi ar trebui să analizeze foarte bine comportamentul dispozitivelor, întrucât acestea nu sunt folosite numai pentru monitorizarea prezenței telefoanelor mobile într-o anume zonă, având ca scop identificarea locației pe hartă a acestora, ci și pentru a aduna informații despre utilizatori sau despre dispozitivele pe care aceștia le folosesc.

Pe lânga drepturile descrise mai sus, pe care un astfel de atac ar putea să le încalce, se mai adaugă și încălcarea dreptului la libertatea întrunilor pașnice. Există numeroase modalități prin care acest lucru este posibil, cum ar fi (5):

* persoanele ce cunosc modul de operarare ale acestor tipuri de dispozitive, nu vor mai participa la întalniri, proteste sau orice altă manifestare pașnică deoarece vor ști că prin captarea comunicațiilor mobile, aceștia pot fi urmăriți;
* prin captarea, editarea și rutarea comunicațiilor, abilitatea persoanelor de a comunica între ele va fi alterată;
* în unele cazuri, este chiar posibil ca unele guverne să trimită mesaje tuturor telefoanelor mobile aflate în zona în care se desfășoară o întalnire pentru a intimida, manipula sau pentru a împrăștia utilizatorii.

Deși există o lege europeană care face referire la protejarea individului, nu există legi specifice pentru utilizarea acestor dispozitive. Guverne din Statele Unite ale Americii și Germania au stabilit legi și politici care limitează modalitățile în care agențiile statatale pot utiliza în mod legal dispozitive de tip *Imsi Catcher.* Mai mult, Judecătorii din SUA au impus restricții suplimentare. Câteva exemple referitoare la legile adoptate de Ministerul de Justiție din SUA cu privire la utilizarea *Imsi Catcher* vor fi expuse mai jos: (6)

* limitarea folorii acestor dispozitive numai pentru identificare;
* cererea supervizării interne pentru utilizarea acestora;
* nevoia unui mandat pentru utilizarea acestora în situații care nu sunt urgente sau excepționale.

În cazul Germaniei, *Imsi Catcher-urile* au fost supuse legilor federale încă din anul 2002, atunci când utilizarea acestora a fost autorizată ca urmare a atacurilor de pe 9/11 din Statele Unite ale Americii. Curtea de Justiție Germană are dreptul de a autoriza folosirea unui astfel de dispozitiv numai în cazul în care există dovezi clare că o crimă serioasă are loc. Mai mult, persoanele care sunt vizate de aceste dispozitive trebuie anunțate că au fost subiecții unui *Imsi Catcher*, fără a pune în pericol anumite aspecte ale investigației (6).



### Utilizarea IMSI Catcher în afara legii

Deși atât în Europa cât și în Statele Unite ale Americii există reglementări în legătură cu utilizarea acestui tip de dispozitive, guvernele, agențiile de securitate și anumite persoane rău intenționate le utilizează fără un mandat. Spre exemplu, în 2014, poliția din Florida a recunoscut că a folosit *Imsi Catcher-uri* de cel puțin 200 de ori fără a recunoaște acest lucru în fața judecătorilor sau a avea un mandat care să le permită folosirea acestui dispozitiv (7).

Ideea care ridică probleme în acest sens, este aceea că poliția nu folosește acest tip de dispozive numai pentru prindere criminalilor dar și pentru spionarea populației. Chiar dacă în SUA exista numeroase state care dețin astfel de dispozitive, utilizarea lor nu este una transparentă, fapt care a ridicat multe semne de întrebare, deoarece nu se știe dacă acestea au fost folosite cu un mandat sau nu (8).

Pe lângă poliție sau guverne, dispozitivele de tip *IMSI Catcher* sunt adesea folosite si de spioni statali pentru a intra în posesia unor date despre ofițerii de inteligență. Acest lucru este posibil prin identificarea codurilor IMSI ale telefoanelor acestor ofițeri, care sunt localizate 8 ore pe zi în același loc. (9)

## Modalități prin care IMSI Catcher exploatează rețeaua

Ținta unui *IMSI Catcher* este rețeaua GSM. Acest dispozitiv se infiltrează in rețeaua GSM printr-un atac de tip *man-in-the-middle[[4]](#footnote-5).* Practic, acesta reprezintă o antena falsă, ce este plasată între telefonul țintă si antena adevărată, a furnizorului de servicii. Chiar dacă standardele GSM oferă protecție împotriva riscurilor, datorită autentificării mutuale între dispozitiv și rețea, protocolul nu este sută la sută sigur, deoarece atacatorii pot declasa servicii cum ar fi 3G sau LTE în servicii de rețea non-LTE care nu au nevoie de această autentificare mutuală specificată mai sus.

În capitolele ce urmează vor fi prezentate detalii despre rețelele GSM, modul acestora de funcționare, securitatea lor cât și despre câteva tipuri de atacuri cunoscute.

### Rețele de comunicații GSM

GSM sau *Global System for Mobile Communications,* standard folosit pentru a descrie protcoalele din a doua generație( 2G) de rețele celulare digitale, a fost pentru prima oara folosit în anul 1991 în Finlanda. În jurul anului 2010, acesta a devenit un standard global pentru comunicațiile mobile, operând în peste 193 de țări și teritorii. Pentru o bună funcționare a tuturor echipamentelor compatibile cu această rețea dar și interconectarea acestora într-un mod corespunzător, standardul pune la dispoziție 161 de recomandări. Toate aceste reguli privind sistemele și serviciile GSM sunt guvernate de ETSI( *European Telecommunications Standards Insitute)* (10)*.*

În Europa, standardul GSM folosește benzi de frecvență între 900 MHz și 1800 MHz pe când în Statele Unite ale Americii este folosită banda de 1900 MHz. Din această cauză, telefoanele mobile care pot opera pe ambele continente sunt numite *tri-band,* în timp ce acelea care operează doar în Europa sunt cunoscute sub denumirea de *dual band*. Deoarece standardul acceptă un maxim de 9,6 kbps se pot transmite doar voce sau un volum mic de date, cum ar fi mesaje text sau mesaje multimedia (11).

### Securitatea în GSM

Deși standardul GSM este considerat a fi cel mai sigur sistem de telecomunicații celulare din ziua de azi deoarece folosește autentificarea folosind o cheie pre-partajată și autentificare de tip întrebare-răspuns, acesta este vulnerabil la diferite tipuri de atacuri, fiecare din ele țintind o altă parte a rețelei.

Operatorii de telefonie mobilă sunt astfel obligați să asigure atât securitatea propriilor servicii dar și a clienților întrucât acestora le trebuie oferită garanția că nimeni nu le poate intercepta conversațiile sau să le detecteze locația. Cu toate acestea, o rețea sigură nu înseamnă o rețea care să îngreuneze apelurile telefonice sau transmisia de date. Astfel, principalele mecanisme de securitate folosite în standardul GSM sunt împărțite în 4 mari categorii (12):

**Autentificarea utilizatorului** se realizează printr-un mecanism de securitate de tipul întrebare-răspuns. Un număr random de 128 de biți este trimis către stația mobilă care la rândul ei calculează un răspuns pe 32 de biți bazat pe numărul primit dar și pe cheia de autentificare individuală. Criptarea acestui răspuns este realizată cu ajutorul algoritmului A3.

**Criptarea datelor și semnalului** se asigură că datele utilizatorilor, cum ar fi mesaje text dar și voce, sunt protejate împotriva interceptării. Procesul de criptare este îndeplinit cu ajutorul algoritmului A5. Tot procesul de comunicare începe, însă, printr-o cerere la rețeaua GSM pentru a specifica modul de criptare. Astfel, operatorul de rețea este cel care decide modul în care se va desfășura întregul proces de comunicare. Mai mult, cheia de criptare este schimbată la intervale regulate de timp pentru a face rețeaua chiar mai rezistentă la interceptări. Calculul acestei chei are loc în interiorul SIM-ului și astfel această informație nu va fi niciodată divulgată de SIM.

**Confidențialitatea identității utilizatorului** asigură securitatea IMSI[[5]](#footnote-6) prin faptul că într-o comunicație GSM, codul IMSI este comunicat rar. Este mult mai sigur să se folosească un cod TMSI[[6]](#footnote-7) pentru a evita descoperirea identității unui utilizator al rețelei. Acest lucru presupune că un atacator ce interceptează comunicația nu va putea afla dacă un anume telefon mobil se află în aria căutată.

**Cartela SIM** asigură securitatea prin simplul fapt că în cazul pierderii, aceasta va cere un cod PIN pentru a putea fi folosită. Metoda este utilă doar în cazul în care codul PIN este activat și cel implicit a fost schimbat de către deținătorul cartelei.



**Fig. 2.2.2.a**

### Tipuri de atacuri populare

# BIBLIOGRAFIE

1. *IMSI-Catch Me If You Can: IMSI-Catcher-Catchers.* **Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, Edgar Weippl.** 2014, ACSAC '14: Proceedings of the 30th Annual Computer Security Applications Conference, p. 10.

2. **Ashkan Soltani, Craig Timberg.** Tech firm tries to pull back curtain on surveillance efforts in Washington. *The Washington Post.* [Online] The Washington Post, 09 17, 2014. [Cited: 04 09, 2020.] https://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f\_story.html.

3. **Wikipedia.** Imsi-catcher. *Wikipedia.* [Online] 03 11, 2020. [Cited: 04 09, 2020.] https://en.wikipedia.org/wiki/IMSI-catcher.

4. **Naarttijärvi, Markus.** *Swedish police implementation of IMSI-catchers in a European law perspective.* Umeå : Computer Law & Security Review, 2016.

5. **International, Privacy.** *Privacy International’s contribution to the half-day general discussion on Article 21 of.* s.l. : Privacy International, 2019.

6. **Tamir Israel, Christopher Parsons.** *Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada.* Toronto : Telecom Transparency, 2016.

7. **Wikipedia.** Stingray phone tracker. *Wikipedia.* [Online] Wikipedia, 04 10, 202. [Cited: 04 13, 2020.] Stingray phone tracker.

8. **Lee, Timothy B.** The police are secretly using fake cellphone towers to spy on people. *Vox.* [Online] Vox, 04 22, 2015. [Cited: 04 13, 2020.] https://www.vox.com/2015/4/22/8463239/stingray-fbi-secret.

9. **Catherine Cullen, Brigitte Bureau.** Someone is spying on cellphones in the nation's capital. *CBC News.* [Online] CBC, 04 03, 2018. [Cited: 04 21, 2020.] https://www.cbc.ca/news/politics/imsi-cellphones-spying-ottawa-1.4050049.

10. **Wikipedia.** GSM. *Wikipedia.* [Interactiv] 13 09 2019. [Citat: 09 04 2020.] https://ro.wikipedia.org/wiki/GSM.

11. **xlxmarketing.** The Cell Phone Mysteries, What Are Dual Band, Tri Band And Quad Band Cell Phones And Where Will They Work? *Chinavasion.* [Online] Chinaviasion, 11 21, 2008. [Cited: 04 21, 2020.] https://blog.chinavasion.com/1099/the-cell-phone-mysteries-what-are-dual-band-tri-band-and-quad-band-cell-phones-and-where-will-they-work-part-2/.

12. **Korkusuz, Ammar Yasir.** *Security in the GSM Network.* Bogazici University, Electrical-Electronics Engineering Department : s.n., 2012.

1. Software Defined Radio – sistem de comunicare radio. Componente care în mod normal ar fi implementate hardware, precum amplificatoare, modulatoare sunt implementate pe partea de software. [↑](#footnote-ref-2)
2. International Mobile Subscriber Identity – cod alocat utilizatorului de către operatorii de telefonie, ce le permite să identifice abonatul in funcție de numărul de telefon. [↑](#footnote-ref-3)
3. Celulă – releu GSM ce deservește o mică suprafață, mai mult sau mai puțin rotundă si cu diametrul de aproximativ 8-10 kilometri. (10) [↑](#footnote-ref-4)
4. Atac man-in-the-middle – tip de atac în care o persoană rău intenționată se infilitrează între furnizorul de date și

   țintă. Acesta poate fi atât pasiv, doar pentru monitorizare, cât și activ prin alterarea datelor. [↑](#footnote-ref-5)
5. International Mobile Subscriber Identity – identifică în mod unic fiecare utilizator dintr-o rețea GSM [↑](#footnote-ref-6)
6. Temporary Mobile Subscriber Identity [↑](#footnote-ref-7)