SVEUČILIŠTE U ZAGREBU
Fakultet elektrotehnike i računarstva

Diplomski studij

Sigurnost komunikacija

Sigurnost signalizacije u telekomunikacijskim mrežama

Ak. godina 2022/2023

Creative Commons

- **slobodno smijete:**
  - **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
  - **remiksirati** — prerađivati djelo
- **pod sljedećim uvjetima:**
  - **imenovanje**. Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
  - **nekomercijalno**. Ovo djelo ne smijete koristiti u komercijalne svrhe.
  - **dijeli pod istim uvjetima**. Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu. Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Tekst licencije preuzet je s http://creativecommons.org/.

Neke ključne riječi u mobilnim mrežama

- IMSI
  - *International Mobile Subscriber Identity*
  - Određuje zemlju, operatora i jedinstveni identifikator
- MSISDN
  - *Mobile Subscriber International Integrated Services Digital Network Number*
  - Telefonski broj (npr. 385991234567)
- IMEI
  - *International Mobile Equipment Identity*
  - Jedinstveni identifikator sklopovlja / mobitela
  - Analogija s MAC adresom
- P-TMSI
  - *Packet Temporary Mobile Subscriber Identity*
  - Anonimizirani i privremeni IMSI – kako se „pravi” IMSI ne bi slao preko signalizacijskog kanala

Kriptografija u mobilnim mrežama

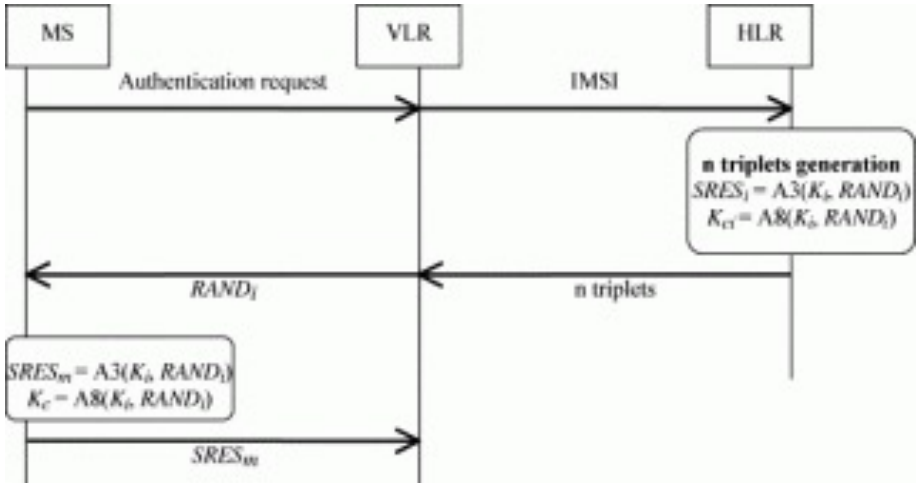
- Obitelj algoritama "A”
  - Karakterizira ih ”*security by obscurity*"
  - Svaka novija generacija mreže koristi bolje algoritme
  - Stari algoritmi su probijeni!
- Jedan od načina prisluškivanja…
  - Većina operatera treba podržavati starije generacije
  - Npr. 2G ili "EDGE" u područjima slabe naseljenosti, smanjenje na 2G u uvjetima visokog prometa itd.
  - Kada dođe do nadogradnje koriste se stari algoritmi
  - Ometanje novijih mreža (npr. 5G) radi prisilnog smanjivanja razine?

Kriptografija u mobilnim mrežama- algoritmi

- A3
  - Autentifikacijski algoritam
    - Koristi se pri spajanju na mobilnu mrežu / baznu stanicu / "toranj”
- A8
  - Algoritam za generiranje ključeva za šifriranje
  - Koristi se za generiranje sjedničkih ključeva za algoritam A5
- A5
  - Šifriranje tokova podataka (*stream*) između uređaja i baznih stanica
    - A5/0 : nema šifriranja
    - A5/1 : LFSR šifriranje tokova, 64 bitni ključ
    - A5/2 : LFSR šifriranje tokova, 64 bitni ključ
    - A5/3 : KASUMI, 128 bitni ključ
    - A5/4 : 128 bitni ključ, kao A5/3

Autentifikacija u mobilnim mrežama - GSM

- Simetrično šifriranje
  - Simetrični ključ pohranjen u sigurnosnom elementu na SIM kartici (SE, HSM)
  - Operater također ima isti ključ (naravno)
  - Zašto se ne koristi asimetrična kriptografija?



https://blog.cryptographyengineering.com/2013/05/14/a-few-thoughts-on-cellular-encryption/

Autentifikacija u mobilnim mrežama

- Problemi s GSM-om?
  - Nema autentifikacije baznih stanica / „tornjeva”
    - „IMSI *catchers*” i napadi MITM
  - Loši i probijeni algoritmi
- Dobre stvari u 3G/LTE/UMTS
  - Bolji algoritmi (KASUMI)
  - Duži ključevi
  - *Authentication and Key Agreement*
    - Autentifikacija bazne stanice putem MAC-a
  - Ipak, ne zaboravimo: moguće ometanje kako bi se koristila starija tehnologija…

https://blog.cryptographyengineering.com/2013/05/14/a-few-thoughts-on-cellular-encryption/

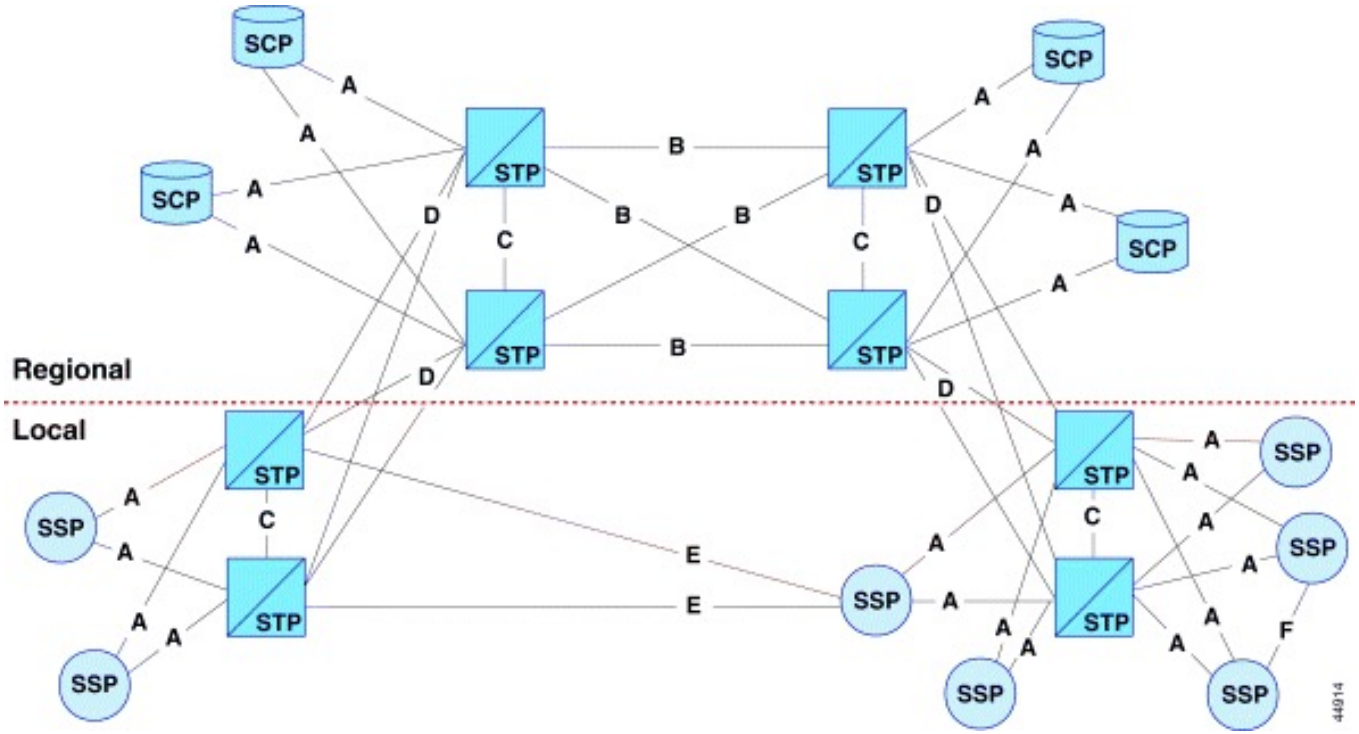
Signalizacija u telekomunikacijskim mrežama

- Specifičnost: odvojeni kanali za signalizaciju i promet
- Danas najkorišteniji protokol - *Common Channel Signaling System no. 7* - (CC)SSno7 ili **SS7**
  - Osmišljen tijekom 70ih, standard tijekom 80ih
  - Zadužen za kontrolu poziva – uspostavljanje i prekidanje
  - Odvojeni kanal za signalizaciju
  - SMS se prenosi preko signalizacije!
- Danas se SS7 koristi u svim telekomunikacijskim mrežama
  - I za povezivanje različitih mreža (npr. više operatora mobilne mreže)
- Temelji se na povjerenju između mreža / davatelja usluge
  - Autentifikacija?

Signalizacija u telekomunikacijskim mrežama

- Sjetimo se:
  - evolucija mreža je velikim dijelom okarakterizirana uvođenjem IP složaja u jezgrenu mrežu
- „SS7 u IP mrežama” = SIGTRAN (*signaling transport*)
  - Omogućuje korištenje SS7 u mrežama temeljenim na IP-u
  - SIGTRAN koristi *Stream Control Transmission Protocol* (SCTP) za slanje signalizacije u IP mrežama
- *Stream Control Transmission Protocol*
    - Protokol transportnog sloja
    - UDP paketi

Arhitektura SS7

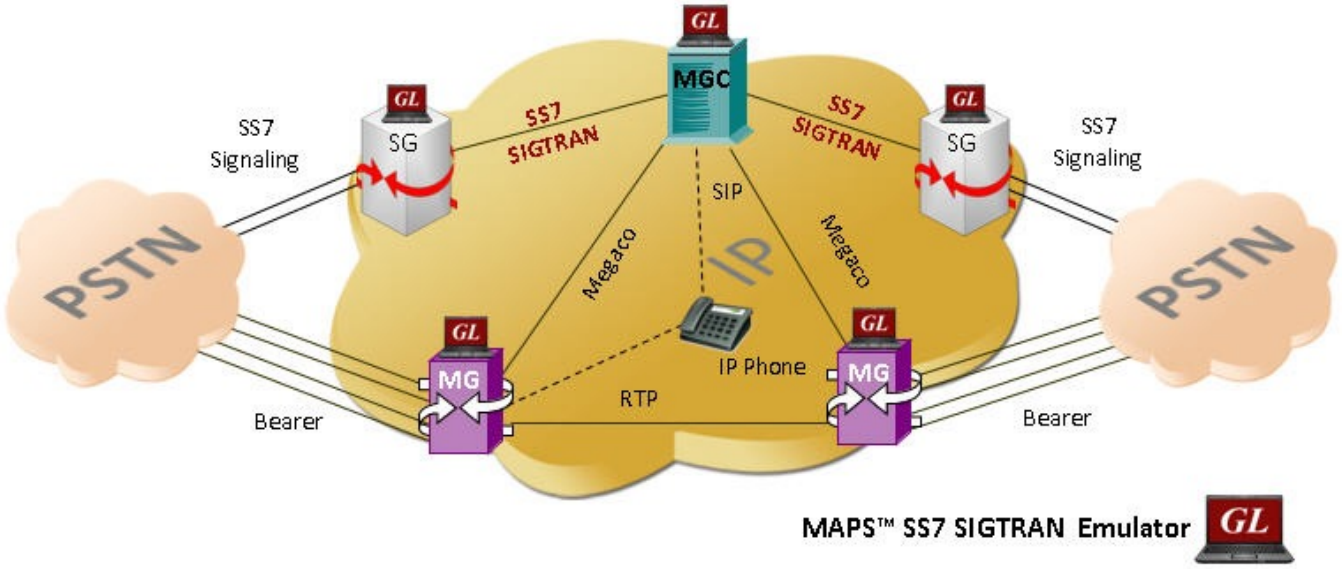


https://docstore.mik.ua/univercd/cc/td/doc/product/tel_pswt/vco_prod/ss7_fund/ss7fun02.htm

SSP – Signal Switching Point

STP – Signal Transfer Point

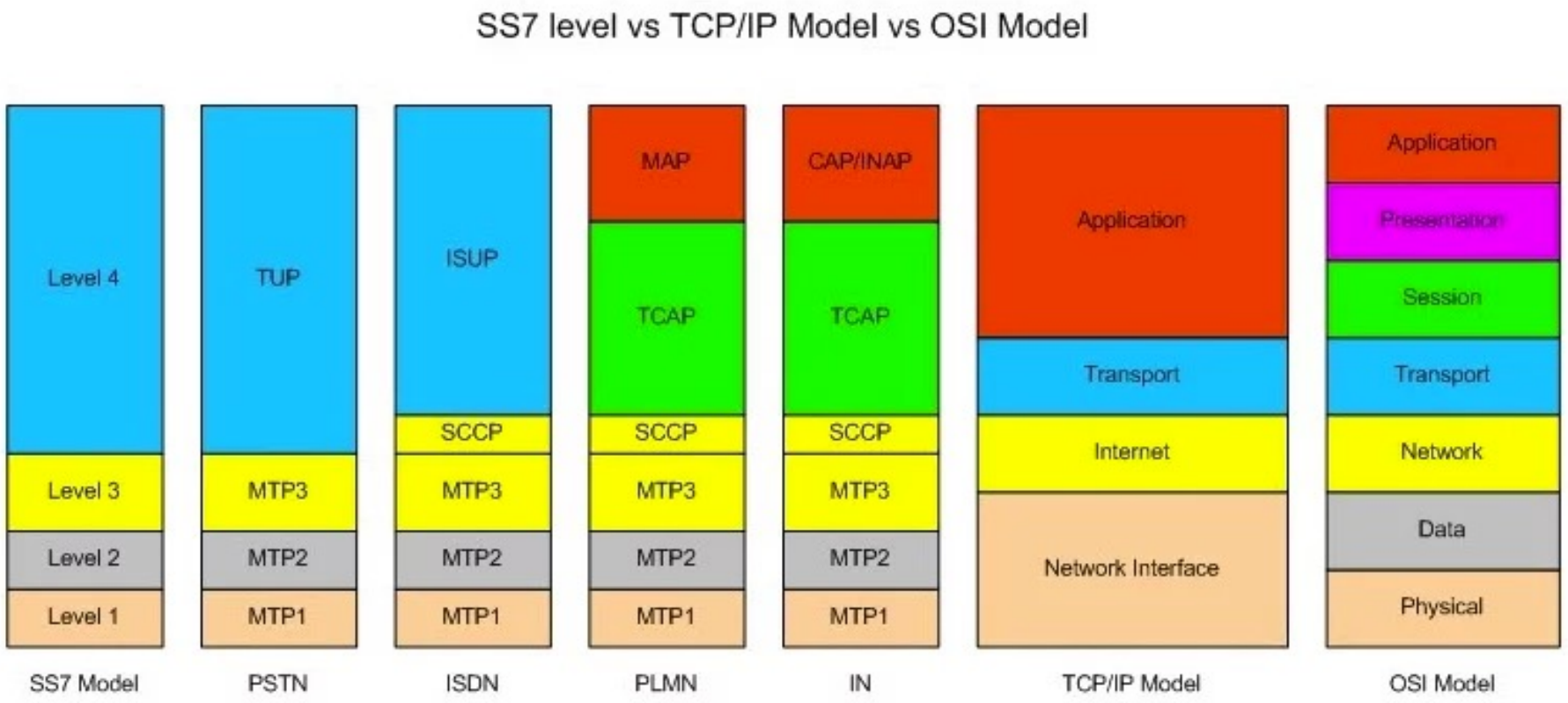
Arhitektura SS7 u IP mrežama



https://www.gl.com/maps-sigtran.html

- Potencijalni problem
  - Spoj različitih mreža
    - tehnološki istih, a pogotovo različitih
- Tipično - lokalno VoIP preko protokola SIP, u jezgri SS7

SS7 i mapiranje na različite modele

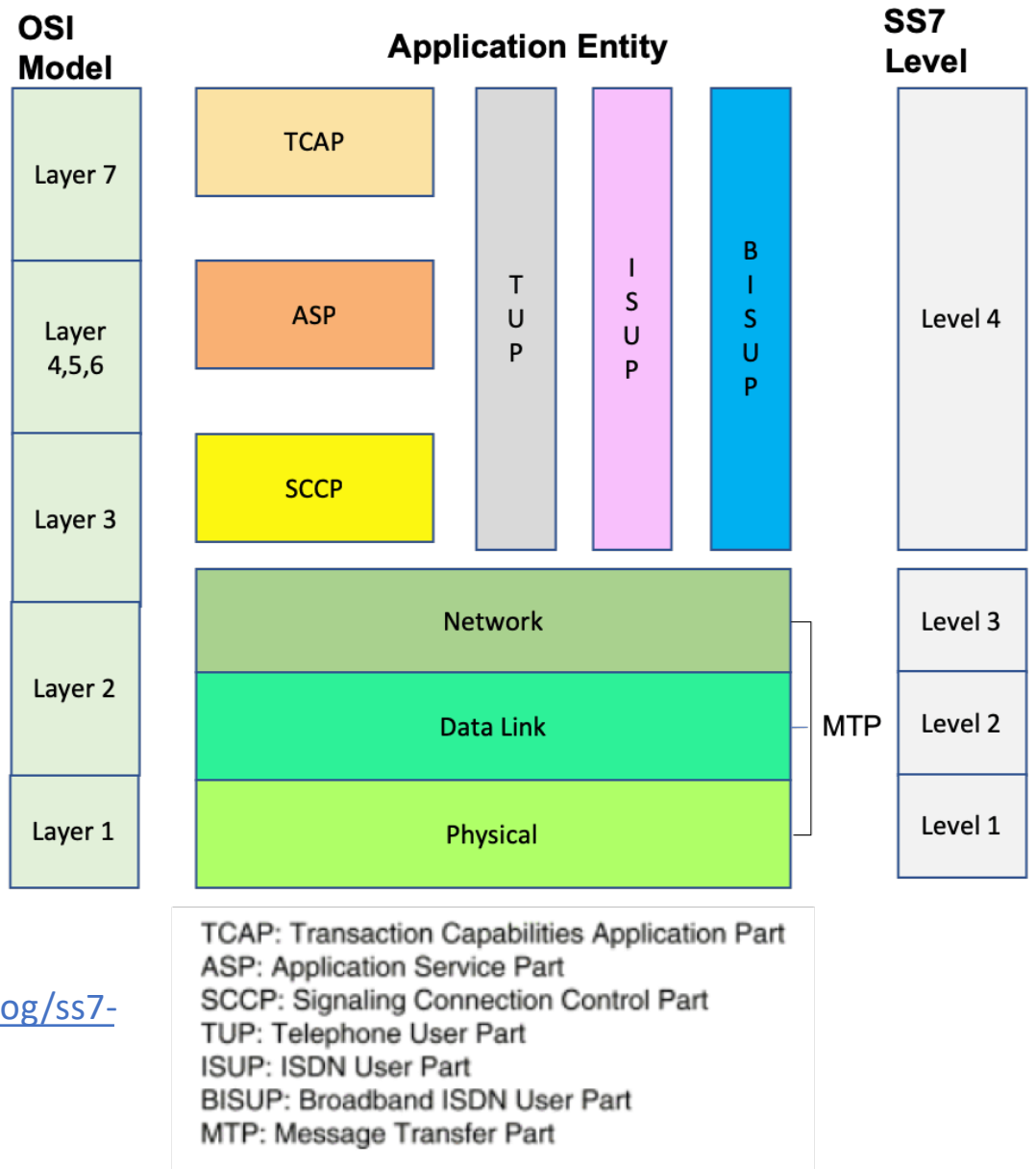


MTP - Message Transfer Part (1 - physical, 2 - data link layer, 3 - network)
SCCP – Signalling Connection Control Part
TCAP – Transaction Capabilities Application Part
MAP – Mobile Application Part

TUP – Telephone User Part
ISUP – ISDN user Part
BISUP – Broadband ISDN User Part

https://www.poplabtelecom.com/free-introduction-to-ss7-protocol-stack-in-2021/

SS7 vs OSI



https://www.firstpoint-mg.com/blog/ss7-attack-guide/

Napadi u SS7 – krađa IMSI

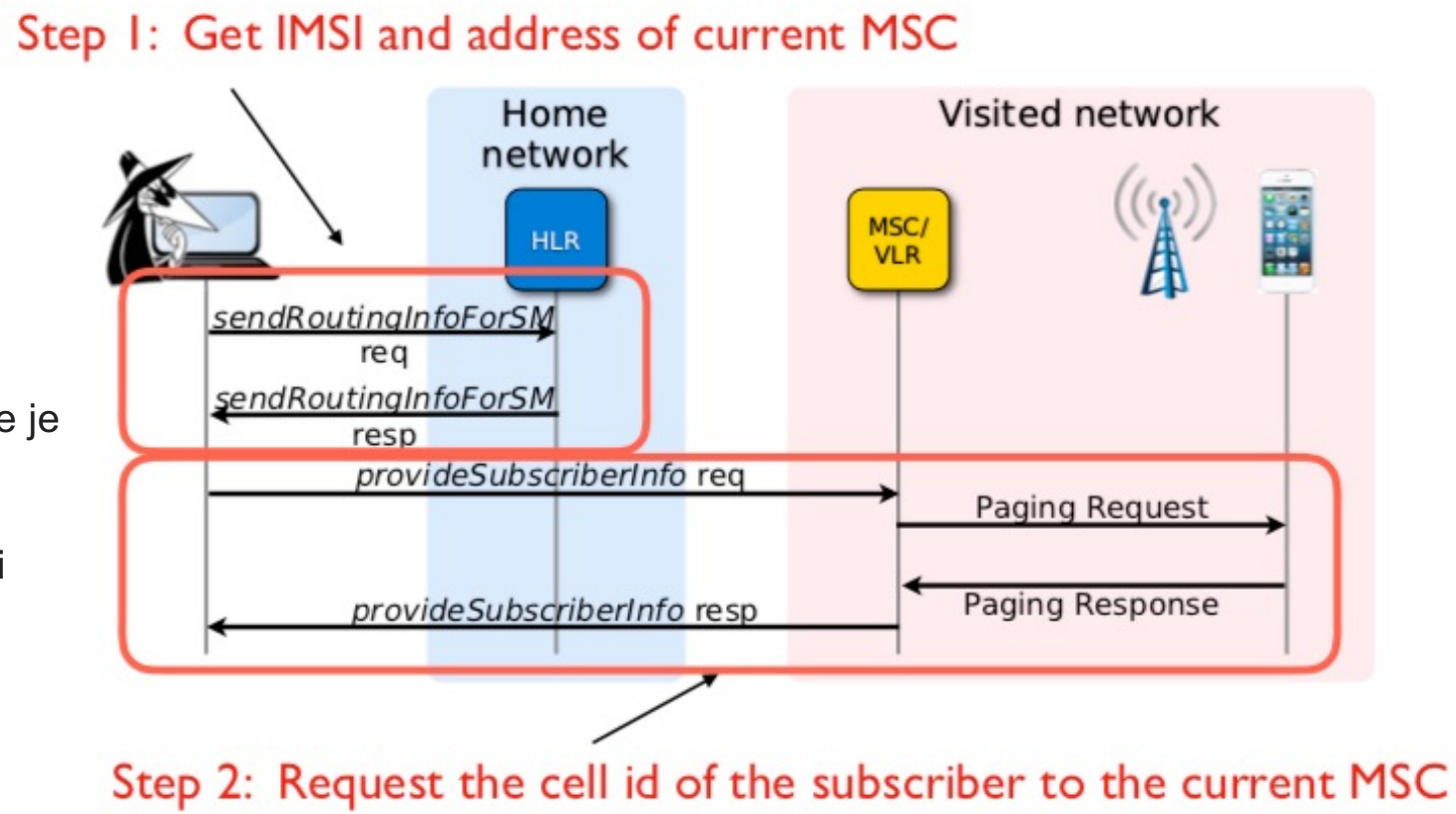
- IMSI (*International Mobile Subscriber Identity*)
  - Broj mobitela (+385…)
- Ipak – na zračnom sučelju vidi se TMSI (*Temporary* IMSI)
  - Napadač očita TMSI
- Ako napadač ima pristup SS7 može tražiti IMSI koji odgovara TMSI-ju
- Može se koristiti za povredu anonimnosti, praćenje…

Napadi u SS7 – otkrivanje lokacije korisnika

- Napadač se predstavlja kao „strani” HLR (VLR?) i kontaktira HLR (*Home Location Register*)
  - HLR – baza podataka o korisnicima „domaće” mreže, (VLR – *Visitor LR)*
- Šalje MAP poruke s upitom o korisniku
  - *Mobile Application Part* (MAP)
    - Protokol aplikacijskog sloja za razmjenu informacija između čvorova mobilne mreže
  - Kao odgovor dobija:
    - *Cell ID* (CID) – ćelija mobilne mreže, npr. 46033
    - *Mobile Country Code* (MCC) – kod države, npr. 219 za HR
    - *Mobile Network Code* (MNC) – kod mobilne mreže, npr. 02 je Telemach u HR
    - *Location Area Code* (LAC) – kod lokacijskog područja, npr. 1
  - http://www.cell2gps.com/, https://www.radiocells.org/

Napadi u SS7 – praćenje lokacije korisnika

- *Send-Routing-Info-for-SM-Request* (SRR)
  - Dolazi poziv/SMS – gdje je korisnik?
- *Paging*
  - Mreža mora uvijek znati gdje je korisnik
  - Paging poruke ga "pozivaju" i traže



https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/education/SOWN_AS19/cellular-security.pdf

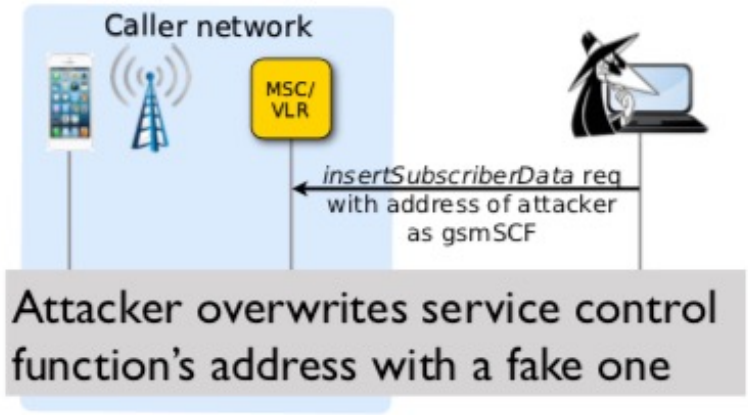
Napadi u SS7 – prisluškivanje

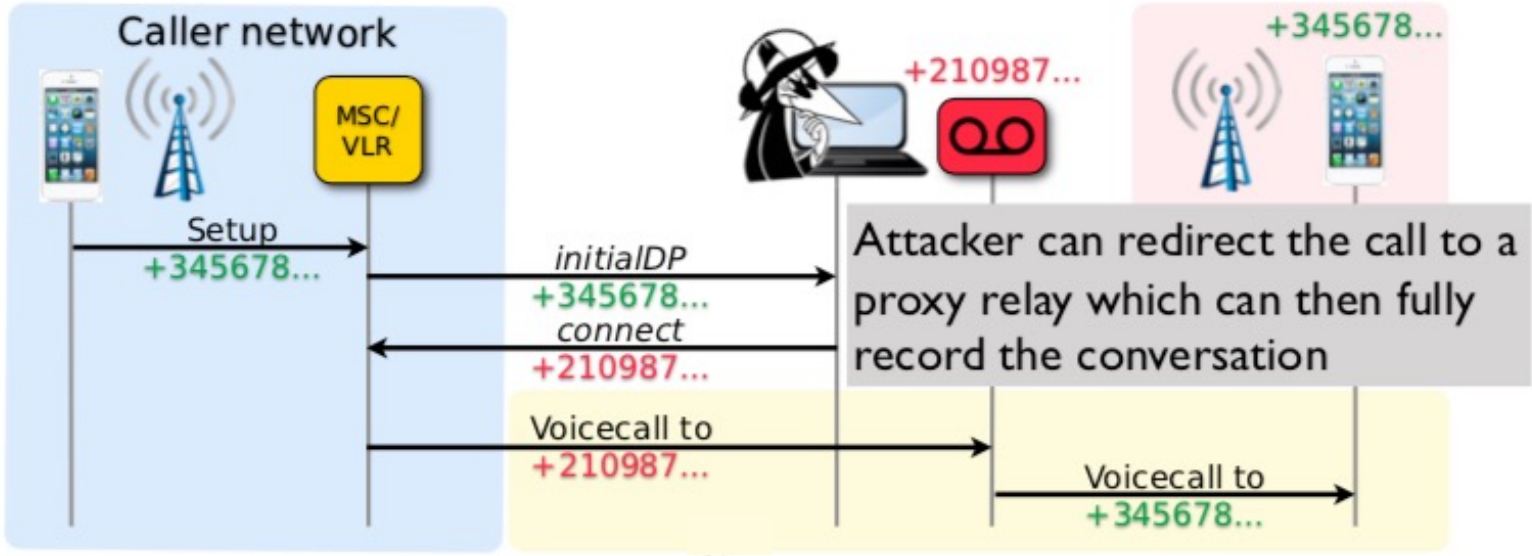
- Moguće prisluškivanje dolaznih i odlaznih poziva bez obzira na napadačevu lokaciju u mreži u odnosu na žrtvu (domaća, roaming)
  - https://www.cellusys.com/2015/10/20/8-ss7-vulnerabilities-you-need-to-know-about/
- Odlazni poziv
  - Koriste se dodatne funkcionalnosti IN (*Intelligent Network*) koje su osmišljene za razvoj usluga s dodanom vrijednosti u fiksnim mrežama (PSTN)
  - *Customized Applications for Mobile network Enhanced Logic* (CAMEL)
    - Usluge s dodanom vrijednosti koje proširuju GSM
    - Korisno za napadače – usluga nadzire pozive korisnika iz domaće mreže kada je u roaming
    - CAMEL usluge su "smještene" u gsmSCF – *GSM Service Control Functions*
  - Napadač koristi CAMEL kako bi odlazne pozive preumsjerio k sebi, a zatim ih prosljeđuje na pravo odredište - MITM

Napadi u SS7 – prisluškivanje

- Moguće prisluškivanje dolaznih i odlaznih poziva bez obzira na napadačevu lokaciju u mreži u odnosu na žrtvu (domaća, roaming)
  - https://www.cellusys.com/2015/10/20/8-ss7-vulnerabilities-you-need-to-know-about/
- Dolazni poziv
  - Sličan princip kao kod odlaznog poziva
  - No, jednostavniji jer se koriste uobičajene funkcije za prosljeđivanje poziva
  - Napadač putem MAP poruka proslijedi poziv k sebi a zatim uspostavlja novi poziv prema žrtvi
  - Ponovno MITM!

Prisluškivanje





https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/education/SOWN_AS19/cellular-security.pdf

Napadi u SS7 – presretanje poruka SMS

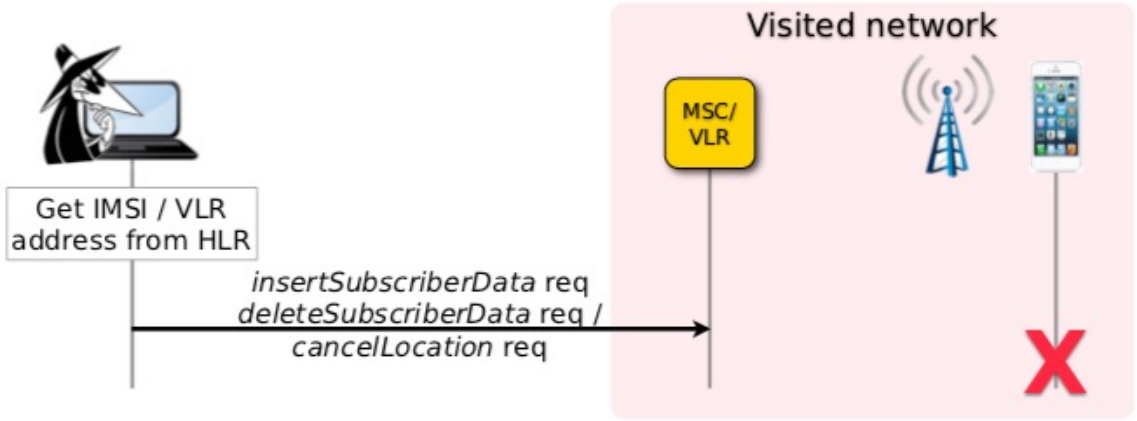
- Napadač se lažno predstavlja kao MSC ili VLR (*Mobile Switching Center* ili *Visitor Location Center*) i traži promjenu lokacije u ime žrtve
- Šalje MAP poruku *Update Location* na žrtvin HLR
  - Smisao: promijeno sam lokaciju, nova lokacija žrtve je napadač, tj. njegov lažni MSC / VLR
- Nakon toga, mreža misli da je žrtva na novoj lokaciji (ili u drugoj mreži ako je lažni VLR) i tamo šalje SMS poruke namijenjene žrtvi
- Problem: MFA, kodovi za usluge, bankarstvo…

Napadi u SS7 – lažiranje USSD zahtjeva

- *Unstructured Supplementary Service Data* (USSD)
  - Koristi se npr. za slanje zahtjeva za nadoplatu prepaid računa
  - Ali i ozbiljnije stvari, npr. mobilna bankarstva
- Koncept je da se napadač lažno predstavlja kao žrvta i traži nadoplatu, kod ili neku transakciju
- Nakon pokretanja transakcije, presereće SMS namijenjen žrtvi tako da žrtva nije uopće svjesna da se nešto događa

Napadi u SS7 – uskraćivanje usluge

- Očigledno se može manipulirati signalizacijom (prethodni slideovi)
  - Prema tome, uskraćivanje usluge se može izvesti na više načina!



https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/education/SOWN_AS19/cellular-security.pdf

Još neki problemi

- Sve navedeno podrazumijeva da napadač ima pristup signalizacijskoj mreži i SS7
  - Očekivali bismo da je to teško izvedivo
- Ipak, SCTP čvorovi dostupni su na mreži!
  - *Well-known ports* definirani
  - SCTP – *4-way handshake*
- *SCTP ranjivosti*
  - *https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=SCTP&search_type=all&isCpeNameSearch=false*
- SCTPscan - Finding entry points to SS7 Networks & Telecommunication Backbones
  - https://www.p1sec.com/corp/research/tools/sctpscan/
  - https://www.blackhat.com/presentations/bh-europe-07/Langlois/Presentation/bh-eu-07-langlois-ppt-apr19.pdf

Privatnost?

- CDR - Call data records
- Anonimizacija i deanonimizacija
- Analiza i predviđanje kretanja, tko priča s kim…

Caller SIM	Callee SIM	Outgoing BTS	Incoming BTS	Timestamp	Call duration (sec)
0458685984	0488595496	12	365	2018-01-18 15:22:12	456
0458685984	0458685984	12	25	2018-01-18 22:24:12	35
0469875254	0498563201	879	567	2018-01-19 08:47:10	125
(...)	(...)	(...)	(...)	(...)	(...)

https://www.researchgate.net/figure/Sample-of-typical-call-data-records_tbl1_325681249

Literatura

- Tobias Engel: SS7: Locate. Track. Manipulate.
  - https://www.youtube.com/watch?v=-wu_pO5Z7Pk
- 8 SS7 vulnerabilities you need to know about
  - https://www.cellusys.com/2015/10/20/8-ss7-vulnerabilities-you-need-to-know-about/
- Signalling Security in Telecom SS7/Diameter/5G - ENISA
  - https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g
- SCTPscan - Finding entry points to SS7 Networks & Telecommunication Backbones
  - https://www.blackhat.com/presentations/bh-europe-07/Langlois/Presentation/bh-eu-07-langlois-ppt-apr19.pdf