Telco Security 101

Raúl Sandoval a.k.a. z3nhx

¿Quien soy?

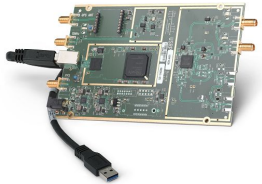
- Ingeniero en sistemas computacionales.
- Experiencia en temas de ciberseguridad
  - Pruebas de penetración.
  - Forense digital
- Cofundador de Rogue Security.
- Los últimos 3 años de mi carrera lo he dedicado a temas de seguridad en protocolos de telecomunicaciones.

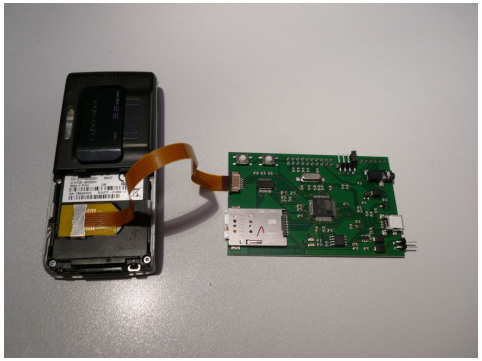
DISCLAIMER

No soy experto en el tema, aún me falta mucho por recorrer y aprender, esta plática está pensada para transmitir mi experiencia en el tema, por si alguien está interesado en esta área.

¿Cómo empezar?

- SDR
  - BladeRF de Nuand
  - USRP de Ettus
- Open5GS
  - https://open5gs.org/
- SimTrace
  - https://osmocom.org/projects/simtrace/wiki/SIMtrace
- SIM Cards
  - https://sysmocom.de/products/sim/
- Teléfonos rooteados Android
- Pinephone





Normativas y estándares de seguridad

- **3GPP** (5G Security - TS 33.xxx series).
- **ETSI** (NFV Security, MEC Security).
- **GSMA** (Security Guidelines - SEPP, Interconnect Security).
- **NIST**, **ISO/IEC 27001**, **PCI DSS** (para protección de datos).
- Regulaciones locales (ej. GDPR, Ley de Telecomunicaciones en México, etc.).

Principales amenazas en telecomunicaciones.

- **Intercepción de comunicaciones**
  - (Ataques MITM, IMSI Catchers, SS7/SIGTRAN Hacking).
- **Ataques en la red móvil**
  - (ATA, DoS en Core 5G, DDoS en MEC).
- **Vulnerabilidades en la infraestructura**
  - (Routers, IMS, VoLTE, Core, RAN).
- **Fraude en telecomunicaciones**
  - (SIM Swapping, Bypass de interconexión).
- **Amenazas en IoT y MEC**
  - (Ataques a redes LPWAN, seguridad en dispositivos IoT).
- **Explotación de APIs y Exposición de Datos**
  - (REST APIs en 5G, problemas en Open API).
- **Renta de GT’s**

Aspectos de seguridad

- **Autenticación y cifrado** en LTE (IMSI / TMSI) y 5G (SUCI /SUPI, 5G SEPP).
- **Seguridad en la señalizacion:** SS7 (3G) / Diameter (4G) / SIP , HTTP2 (5G).
- Protección dentro del core:
  - 3G -> HLR , VLR , SMSC, etc..
  - 4G -> MME, HSS, etc …
  - 5G -> AMF, UPF, SMF , SBA
- **Arquitecturas Zero Trust** en implementaciones 5G.

GTPDOOR Malware Threatens Mobile Networks

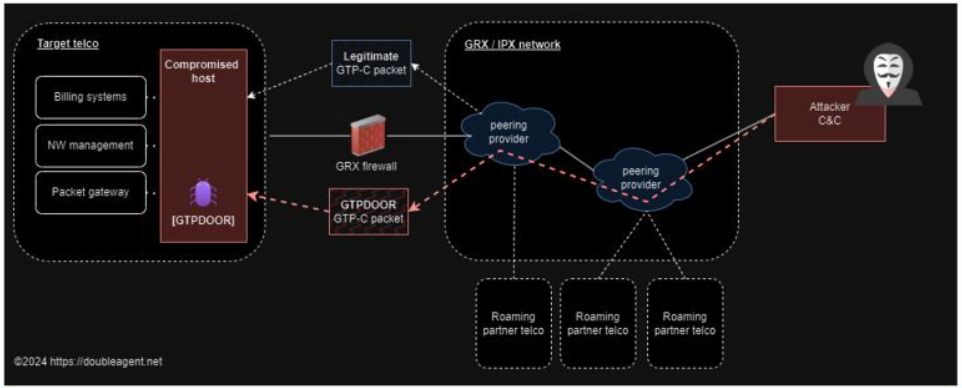


Image created with DALLE-3

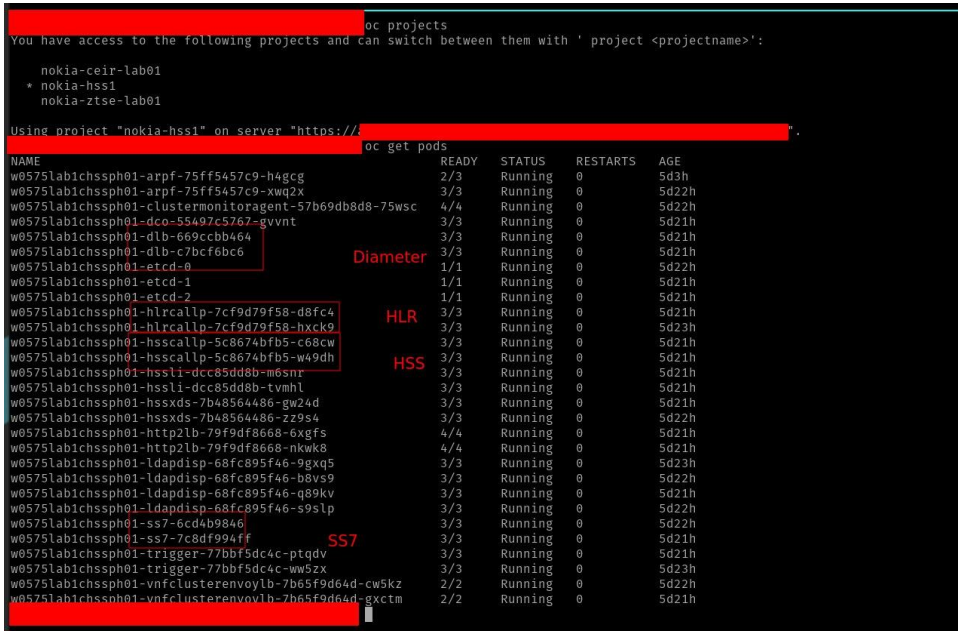
We discover **119 vulnerabilities** in LTE/5G core infrastructure, each of which can result in **persistent denial of cell service to an entire metropolitan area or city** and some of which can be used to **remotely compromise and access the cellular core**. Our research covers seven LTE implementations (Open5GS, Magma, OpenAirInterface, Athonet, SD-Core, NextEPC, srsRAN) and three 5G implementations (Open5GS, Magma, OpenAirInterface); we find **vulnerabilities in every single LTE/5G implementation tested**.

Our research finds these vulnerabilities are present in both well-maintained open-source LTE/5G cores and in proprietary software, both of which have active deployments in commercial settings. To learn more about how we were able to discover these vulnerabilities, take a look at our paper.

Seguridad en infraestructura de red y virtualización.

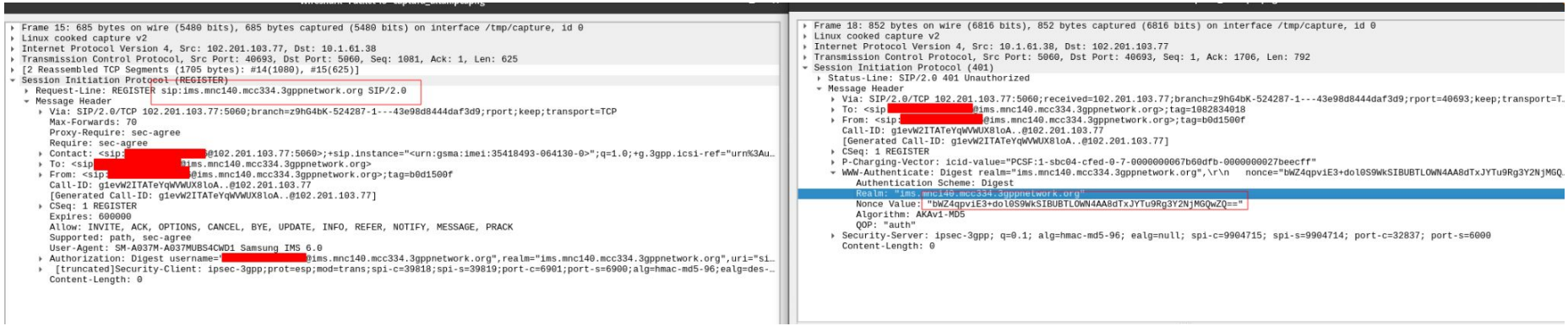
- Seguridad en redes SDN / NFV
- Protección de contenedores en Openshift / Kubernetes.
- Hardening en OpenStack, VMWare, AWS Telco Cloud.
- Hardening y protección de IMS y VoLTE / VoWiFi.

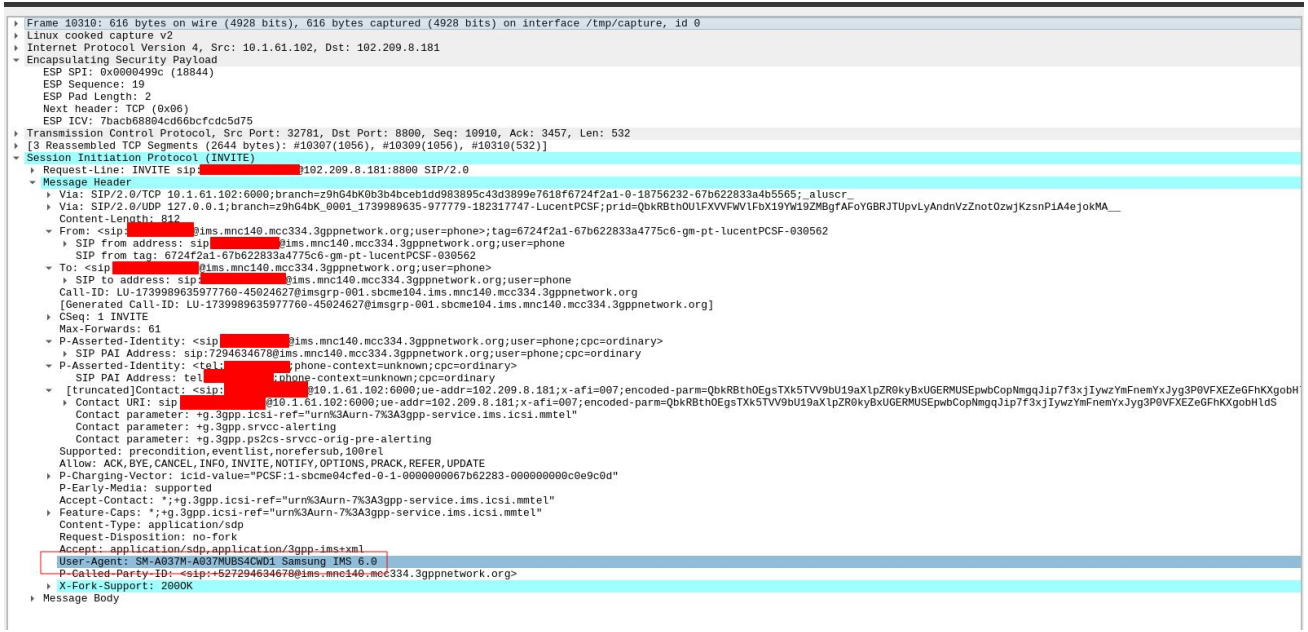
Cluster OpenShift productivo



Seguridad en VoLTE y VoIP

- Intercepción de llamadas VoLTE / VoWiFi
- Fraude en protocolos SIP y ataques de IMS.
- Seguridad en SIP, RTP , RSTP
- Autenticación en VoLTE (AKAv1-MD5, MILENAGE).
- Fuga de información en headers del protocolo SIP.


Frame 15: 685 bytes on wire (5480 bits), 685 bytes captured (5480 bits) on interface /tmp/capture, id 0
Linux cooked capture v2
Internet Protocol Version 4, Src: 102.201.103.77, Dst: 10.1.61.38
Transmission Control Protocol, Src Port: 40693, Dst Port: 5060, Seq: 1081, Ack: 1, Len: 625
[2 Reassembled TCP Segments (1705 bytes): #14(1080), #15(625)]
Session Initiation Protocol (REGISTER)
Request-Line: REGISTER sip:ims.mnc140.mcc334.3gppnetwork.org SIP/2.0
Message Header
Via: SIP/2.0/TCP 102.201.103.77:5060;branch=z9hG4bK-524287-1---43e98d8444daf3d9;rport;keep;transport=TCP
Max-Forwards: 70
Proxy-Require: sec-agree
Require: sec-agree
Contact: <sip:[redacted]@102.201.103.77:5060>;+sip.instance="<urn:gsma:imei:35418493-064130-0>";q=1.0;+g.3gpp.icsi-ref="urn%3Au…
To: <sip[redacted]@ims.mnc140.mcc334.3gppnetwork.org>
From: <sip:[redacted]@ims.mnc140.mcc334.3gppnetwork.org>;tag=b0d1500f
Call-ID: g1evW2ITATeYqWVWUX8loA..@102.201.103.77
[Generated Call-ID: g1evW2ITATeYqWVWUX8loA..@102.201.103.77]
CSeq: 1 REGISTER
Expires: 600000
Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, UPDATE, INFO, REFER, NOTIFY, MESSAGE, PRACK
Supported: path, sec-agree
User-Agent: SM-A037M-A037MUBS4CWD1 Samsung IMS 6.0
Authorization: Digest username="[redacted]@ims.mnc140.mcc334.3gppnetwork.org",realm="ims.mnc140.mcc334.3gppnetwork.org",uri="si…
[truncated]Security-Client: ipsec-3gpp;prot=esp;mod=trans;spi-c=39818;spi-s=39819;port-c=6901;port-s=6900;alg=hmac-md5-96;ealg=des-…
Content-Length: 0
Frame 18: 852 bytes on wire (6816 bits), 852 bytes captured (6816 bits) on interface /tmp/capture, id 0
Linux cooked capture v2
Internet Protocol Version 4, Src: 10.1.61.38, Dst: 102.201.103.77
Transmission Control Protocol, Src Port: 5060, Dst Port: 40693, Seq: 1, Ack: 1706, Len: 792
Session Initiation Protocol (401)
Status-Line: SIP/2.0 401 Unauthorized
Message Header
Via: SIP/2.0/TCP 102.201.103.77:5060;received=102.201.103.77;branch=z9hG4bK-524287-1---43e98d8444daf3d9;rport=40693;keep;transport=T…
To: <sip[redacted]@ims.mnc140.mcc334.3gppnetwork.org>;tag=1082834018
From: <sip:[redacted]@ims.mnc140.mcc334.3gppnetwork.org>;tag=b0d1500f
Call-ID: g1evW2ITATeYqWVWUX8loA..@102.201.103.77
[Generated Call-ID: g1evW2ITATeYqWVWUX8loA..@102.201.103.77]
CSeq: 1 REGISTER
P-Charging-Vector: icid-value="PCSF:1-sbc04-cfed-0-7-0000000067b60dfb-0000000027beecff"
WWW-Authenticate: Digest realm="ims.mnc140.mcc334.3gppnetwork.org",\r\n nonce="bWZ4qpv1E3+dol0S9WkSIBUBTLOWN4AA8dTxJYTu9Rg3Y2NjMGQ…
Authentication Scheme: Digest
Realm: "ims.mnc140.mcc334.3gppnetwork.org"
Nonce Value: "bWZ4qpv1E3+dol0S9WkSIBUBTLOWN4AA8dTxJYTu9Rg3Y2NjMGQwZQ=="
Algorithm: AKAv1-MD5
QOP: "auth"
Security-Server: ipsec-3gpp; q=0.1; alg=hmac-md5-96; ealg=null; spi-c=9904715; spi-s=9904714; port-c=32837; port-s=6000
Content-Length: 0


Frame 10310: 616 bytes on wire (4928 bits), 616 bytes captured (4928 bits) on interface /tmp/capture, id 0
Linux cooked capture v2
Internet Protocol Version 4, Src: 10.1.61.102, Dst: 102.209.8.181
Encapsulating Security Payload
ESP SPI: 0x0000499c (18844)
ESP Sequence: 19
ESP Pad Length: 2
Next header: TCP (0x06)
ESP ICV: 7bacb68804cd66bcfcdc5d75
Transmission Control Protocol, Src Port: 32781, Dst Port: 8800, Seq: 10910, Ack: 3457, Len: 532
[3 Reassembled TCP Segments (2644 bytes): #10307(1056), #10309(1056), #10310(532)]
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:[redacted]@102.209.8.181:8800 SIP/2.0
Message Header
Via: SIP/2.0/TCP 10.1.61.102:6000;branch=z9hG4bK0b3b4bceb1dd983895c43d3899e7618f6724f2a1-0-18756232-67b622833a4b5565;_aluscr_
Via: SIP/2.0/UDP 127.0.0.1;branch=z9hG4bK_0001_1739989635-977779-182317747-LucentPCSF;prid=QbkRBthOUlFXVVFWVlFbX19YW19ZMBgfAFoYGBRJTUpvLyAndnVzZnotOzwjKzsnPiA4ejokMA__
Content-Length: 812
From: <sip:[redacted]@ims.mnc140.mcc334.3gppnetwork.org;user=phone>;tag=6724f2a1-67b622833a4775c6-gm-pt-lucentPCSF-030562
SIP from address: sip:[redacted]@ims.mnc140.mcc334.3gppnetwork.org;user=phone
SIP from tag: 6724f2a1-67b622833a4775c6-gm-pt-lucentPCSF-030562
To: <sip:[redacted]@ims.mnc140.mcc334.3gppnetwork.org;user=phone>
SIP to address: sip:[redacted]@ims.mnc140.mcc334.3gppnetwork.org;user=phone
Call-ID: LU-1739989635977760-45024627@imsgrp-001.sbcme104.ims.mnc140.mcc334.3gppnetwork.org
[Generated Call-ID: LU-1739989635977760-45024627@imsgrp-001.sbcme104.ims.mnc140.mcc334.3gppnetwork.org]
CSeq: 1 INVITE
Max-Forwards: 61
P-Asserted-Identity: <sip:[redacted]@ims.mnc140.mcc334.3gppnetwork.org;user=phone;cpc=ordinary>
SIP PAI Address: sip:7294634678@ims.mnc140.mcc334.3gppnetwork.org;user=phone;cpc=ordinary
P-Asserted-Identity: <tel:[redacted];phone-context=unknown;cpc=ordinary>
SIP PAI Address: tel:[redacted];phone-context=unknown;cpc=ordinary
[truncated]Contact: <sip:[redacted]@10.1.61.102:6000;ue-addr=102.209.8.181;x-afi=007;encoded-parm=QbkRBthOEgsTXk5TVV9bU19aXlpZR0kyBxUGERMUSEpwbCopNmgqJip7f3xjIywzYmFnemYxJyg3P0VFXEZeGFhKXgobH
Contact URI: sip:[redacted]@10.1.61.102:6000;ue-addr=102.209.8.181;x-afi=007;encoded-parm=QbkRBthOEgsTXk5TVV9bU19aXlpZR0kyBxUGERMUSEpwbCopNmgqJip7f3xjIywzYmFnemYxJyg3P0VFXEZeGFhKXgobHldS
Contact parameter: +g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
Contact parameter: +g.3gpp.srvcc-alerting
Contact parameter: +g.3gpp.ps2cs-srvcc-orig-pre-alerting
Supported: precondition,eventlist,norefersub,100rel
Allow: ACK,BYE,CANCEL,INFO,INVITE,NOTIFY,OPTIONS,PRACK,REFER,UPDATE
P-Charging-Vector: icid-value="PCSF:1-sbcme04cfed-0-1-0000000067b62283-000000000c0e9c0d"
P-Early-Media: supported
Accept-Contact: *;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
Feature-Caps: *;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
Content-Type: application/sdp
Request-Disposition: no-fork
Accept: application/sdp,application/3gpp-ims+xml
User-Agent: SM-A037M-A037MUBS4CWD1 Samsung IMS 6.0
P-Called-Party-ID: <sip:+527294634678@ims.mnc140.mcc334.3gppnetwork.org>
X-Fork-Support: 200OK
Message Body

Seguridad en las SIM Cards y eSIMS

Ataques Relacionados

- **Clonación de SIM:** Si un atacante obtiene **Ki**, puede duplicar el SIM.
- **Intercepción de IMSI:** Redes **2G sin cifrado** pueden filtrar IMSI.
- **Ataques de replay:** Si no se protege la autenticación, se pueden repetir valores RAND.
- Ki (Authentication Key)
- OP y OPC (Operator Key y OP Computed).

Pruebas de penetración en redes de telecom.

- **Herramientas utilizadas** (sipp, s6a-simulator, ss7maper, sigploit, Open5GS, srsRAN).
- **Metodologías para pentesting de redes móviles** (ATA, SIGTRAN, GTP fuzzing).
- **Evaluación de APIs y explotación de fallas en interconexión**.

Mejores Prácticas y Estrategias de Mitigación

- Implementación de **Zero Trust en redes Telco**.
- Segmentación y protección del Core 5G.
- Hardening en elementos de red y API Security.
- Monitoreo continuo con **SIEM y AI para detección de ataques**.
- Modelos de **Threat Intelligence aplicados a Telco**.

Casos de estudio y brechas de seguridad

- Ataques recientes en redes móviles.
- Casos de fraude en telecomunicaciones.
- Ejemplo de explotación de fallos en SS7/SIGTRAN.

SS7 Firewall

Category 1

Messages should not be expected at the interconnect level unless there is a prior agreement between operators.

- SendRoutingInfo
- SendIMSI
- AnyTimeInterrogation
- AnyTimeSubscriberInterrogation
- AnyTimeModification
- SendIdentification
- ResumeCallHandling
- FailureReport
- CheckIME
- NoteSubscriberDataModified

Category 2

Messages should only be expected for an inbound roamer from their home network.

- ProvideSubscriberInfo
- ActivateTraceMode
- DeactivateTraceMode
- ProvideRoamingNumbers
- SetReportingState
- RemoteUserFree
- AlertServiceCentre
- CancelLocation
- ProvideSubscriberLocation
- BeginSubscriberActivity

Category 3

Messages should only be expected on interconnects between mobile operators for outbound roamers.

- UpdateLocation
- UpdateGPRSLocation
- PurgeMS
- RegisterSS3
- EraseSS
- ActivateSS
- DeactivateSS
- InterrogateSS
- ProcessUnstructuredSSRequest
- SendAuthenticationInfo

MONIEM TECH

GRACIAS

Gracias.