Union internationale des télécommunications

INITIATIVE MONDIALE EN FAVEUR DE L'INCLUSION FINANCIÈRE (FIGI)

Groupe de travail sur la sécurité, l'infrastructure et la confiance

Test de sécurité des applications de services financiers numériques fondés sur les technologies USSD et STK

Rapport sur l'axe de travail "Sécurité"

DÉCHARGE DE RESPONSABILITÉ

L'Initiative mondiale en faveur de l'inclusion financière (FIGI) est un programme triennal mis en œuvre dans le cadre d'un partenariat entre le Groupe de la Banque mondiale, le Comité sur les paiements et les infrastructures de marché (CPMI) et l'Union internationale des télécommunications (UIT), et financé par la Bill and Melinda Gates Foundation. Il vise à faciliter et à accélérer l'application de réformes nationales en vue d'atteindre les objectifs nationaux en matière d'inclusion financière et, à terme, l'objectif mondial consistant à garantir un accès universel aux services financiers à l'horizon 2020. La FIGI finance des initiatives dans trois pays – la Chine, l'Égypte et le Mexique – et lutte contre trois obstacles distincts à l'accès financier universel, à travers le soutien qu'elle apporte aux trois groupes de travail suivants:
1) le Groupe de travail sur l'acceptation des paiements électroniques (dirigé par le Groupe de la Banque mondiale);
2) le Groupe de travail sur l'identité numérique pour les services financiers (dirigé par le Groupe de la Banque mondiale); et
3) le Groupe de travail sur la sécurité, l'infrastructure et la confiance (dirigé par l'UIT).

La FIGI organise trois colloques annuels rassemblant les autorités nationales, le secteur privé et d'autres parties prenantes compétentes afin de partager les nouvelles idées des groupes de travail et de faire le point sur l'avancée de la mise en œuvre au niveau national.

Le présent rapport a été élaboré par le Groupe de travail de la FIGI sur la sécurité, l'infrastructure et la confiance, dirigé par l'UIT. Les résultats, interprétations et conclusions exprimés dans ce rapport ne reflètent pas nécessairement les opinions des partenaires de la FIGI, notamment le CPMI, la Bill and Melinda Gates Foundation, l'UIT ou la Banque mondiale (y compris son Conseil d'administration ou les gouvernements qu'il représente). Les références éventuelles à certaines sociétés ou aux produits de certains fabricants ne signifient pas que l'UIT approuve ou recommande ces sociétés ou ces produits de préférence à d'autres de nature similaire, mais dont il n'est pas fait mention. Sauf erreur ou omission, les noms des produits propriétaires comprennent une lettre majuscule initiale. Les partenaires de la FIGI ne garantissent pas l'exactitude des données figurant dans le présent rapport. Les frontières, couleurs, dénominations et autres informations figurant sur les cartes de ce document n'impliquent aucune prise de position de la part des partenaires de la FIGI concernant le statut juridique d'un pays, d'un territoire, d'une ville ou d'une région ou de ses autorités, ni aucune reconnaissance ou acceptation de ces frontières.

Test de sécurité des applications de services financiers numériques fondés sur les technologies USSD et STK

Axe de travail "Sécurité"

À propos du présent rapport

Ce rapport a été rédigé par Kevin Butler, de l'université de Floride, ainsi que Vijay Mauree et Arnold Kibuuka, de l'UIT. Les auteurs souhaitent remercier Assaf Klinger, de Vaulto, pour l'aide et le soutien qu'il a apporté à la relecture et à la révision de ce document. Les auteurs tiennent en outre à remercier les membres du Groupe de travail de la FIGI sur la sécurité, l'infrastructure et la confiance. Vijay Mauree, de l'UIT, a assuré la supervision générale de ce rapport.

Si vous souhaitez nous communiquer des informations complémentaires, veuillez contacter Vijay Mauree à l'adresse tsbfigisit@itu.int.

Abréviations et acronymes

A2P	De l'application à la personne
AuC	Centre d'authentification
BSC	Contrôleur de station de base
BSS	Sous-système radio
BTS	Station d'émission-réception de base
DFS	Service financier numérique
EIR	Registre d'identité de l'équipement
GSM	Système mondial de communication mobile
HLR	Registre de localisation de rattachement
IMEI	Identité internationale de l'équipement mobile
IMSI	Identité internationale de station mobile
KiC	Identifiant de la clé et de l'algorithme de chiffrement
KiD	Identifiant de la clé et de l'algorithme de contrôle de redondance/CC/de signature numérique
MNO	Opérateur de réseau mobile
MSC	Centre de commutation pour services mobiles
MSISDN	Numéro d'annuaire d'abonné international de station mobile[1]
OTA	Par voie hertzienne
PCB	Carte de circuit imprimé
PCSC	Personal Computer/Smart Card
PIN	Numéro d'identification personnel
SAT	Kit d'application SIM
SIM	Module d'identification de l'abonné
SMPP	Protocole de messages courts entre homologues
SMS	Service de messages courts
SMSC	Centre de services de messages courts
STK	Boîte à outils SIM
TAR	Référence d'application d'utilitaire
USIM	Module universel d'identité de l'abonné
USSD GW	Passerelle de données de service complémentaire non structurées

[1] Numéro utilisé pour identifier un numéro de téléphone mobile au niveau international composé d'un indicatif de pays ainsi que d'un code de destination national qui identifie l'opérateur de l'abonné.

Table des matières

1 Introduction

Les fournisseurs de services financiers numériques (DFS) ont de plus en plus souvent recours aux canaux de données de service complémentaire non structurées (USSD) et de boîte à outils SIM (STK) pour favoriser la croissance et l'adoption des DFS, principalement dans les pays en développement. La Global System Mobile Association (GSMA) a estimé qu'en Afrique, plus de 90 % des transactions d'argent mobile sont effectuées par USSD[2]. Plusieurs opérateurs de DFS à grande échelle – bKash au Bangladesh, Wing au Cambodge, Easy Paisa au Pakistan, Tigo et M-Pesa en Tanzanie et au Kenya, EcoCash au Zimbabwe, MTN Mobile Money en Afrique et dans les pays du Moyen-Orient, Airtel money en Afrique et en Asie, etc. – utilisent l'USSD comme principal mécanisme de communication entre les clients et leurs plateformes de DFS.

Ce document met en évidence les menaces et les vulnérabilités auxquelles les DFS fondés sur les technologies USSD et STK sont exposés. Il établit une liste de bonnes pratiques à l'attention des fournisseurs de DFS, des opérateurs de réseaux mobiles ainsi que des utilisateurs de DFS qui utilisent ces environnements.

Les canaux USSD et STK rendent possible l'utilisation des services d'ouverture de comptes, de transfert d'argent, de paiement de factures, de consultation de soldes, etc. Les banques traditionnelles peuvent désormais étendre leurs activités à l'aide des canaux USSD et STK par le biais de leurs réseaux d'agents bancaires.

L'adoption et l'utilisation de canaux USSD et STK dépendent principalement des facteurs suivants:

1. La compatibilité avec les appareils mobiles. Les solutions de DFS fondées sur les technologies USSD et STK sont indépendantes des appareils. Elles s'utilisent efficacement et sans difficulté sur les smartphones, les téléphones fixes et les téléphones mobiles de base sans qu'il soit requis de changer d'appareil mobile.
2. La rapidité et la réactivité de la technologie USSD répondent au besoin de simultanéité des DFS.
3. Le coût et l'efficacité. Le déploiement des DFS sur STK et USSD nécessite l'utilisation des protocoles de réseau en vigueur. Le fournisseur de DFS ou l'opérateur de réseau mobile peuvent utiliser la passerelle USSD existante pour déployer des DFS sans avoir à mettre le réseau à niveau.
4. L'interactivité. Les canaux USSD et STK sont basés sur des sessions et peuvent alimenter des applications conviviales pilotées par des menus, lesquelles sont essentielles pour garantir le fonctionnement du catalogue de produits des DFS.
5. Les messages USSD sont acheminés via le réseau domestique de l'abonné; les services USSD dont dispose l'abonné restent disponibles en itinérance sans frais supplémentaires.
6. Les protocoles USSD et STK ne stockent aucune information confidentielle sur le poste mobile.

L'utilisation des canaux USSD et STK, en particulier pour les DFS, a soulevé des préoccupations en matière de sécurité. Par leur biais, les attaquants peuvent en effet compromettre la confidentialité, l'intégrité et la disponibilité des services ainsi que le caractère privé des transactions. Le présent document décrit les différents scénarios d'attaque qui peuvent être suivis pour exploiter les

[2] https://www.gsma.com/r/wp-content/uploads/2019/05/GSMA-State-of-the-Industry-Report-on-Mobile-Money-2018-1.pdf

vulnérabilités des canaux USSD et STK, et recommande plusieurs bonnes pratiques à l'attention des opérateurs de réseaux mobiles, des fournisseurs de DFS et des utilisateurs.

2 Principaux composants des écosystèmes de DFS fondés sur les technologies USSD et STK

Il existe de nombreux points d'interaction entre les différentes parties d'un écosystème de DFS fondé sur les technologies USSD et STK. Les attaquants peuvent donc attaquer le système de nombreuses façons différentes. Les attaques réussies ont souvent des conséquences sur les parties prenantes exploitées, mais également sur d'autres acteurs de l'écosystème.

Le tableau 2-1 présente les éléments critiques d'un écosystème de DFS fondé sur les technologies USSD et STK, les menaces et les vulnérabilités annexes ainsi que des propositions de tests et de scénarios d'attaque.

Tableau 2-1 Éléments d'un écosystème de DFS

Composants	Menaces et vulnérabilités relatives aux technologies USSD et STK	Tests/scénarios d'attaque
Appareil mobile	• Accès non autorisé à l'appareil mobile/vol. • Modification de l'appareil pour compromettre la sécurité de la plateforme sous-jacente, par exemple en y installant des logiciels malveillants et de routage. • Modification physique de l'appareil mobile consistant à placer du matériel supplémentaire pouvant être utilisé comme logiciel espion.	• Exécution du code USSD à distance
Carte SIM	• Permutation et recyclage de cartes SIM • Attaques Simjacker • Algorithmes faibles utilisés sur les cartes SIM; par exemple, on sait que les algorithmes COMP128 v1 et v2 utilisés par la carte SIM et le centre d'authentification pour générer la demande d'authentification chiffrée initiale peuvent être cassés.	• Test de la carte SIM à l'aide du testeur de carte SIM. • Test de la STK à l'aide du traceur SIM. • Tests de clonage SIM. • Test de validation de l'identité internationale de station mobile et d'équipement mobile (IMSI et IMEI).
Station de base	• Attaques par intercepteur: il a été démontré que les algorithmes de chiffrement des réseaux GSM tels que A5/1 et A5/2 sont vulnérables. Les réseaux existants qui utilisent le chiffrement GSM sont exposés aux attaques par intercepteur	• Interception à l'aide d'une BTS malveillante. • Traçage et capture du trafic au niveau des passerelles et des

Composants	Menaces et vulnérabilités relatives aux technologies USSD et STK	Tests/scénarios d'attaque
	des stations de base malveillantes. Celles-ci y sont placées par les attaquants, qui se présentent comme des tours de fournisseurs officielles (il s'agit donc de fausses stations de base, souvent nommées "IMSI-catcher"). • Les attaques par répétition de session: les algorithmes faibles permettent aux attaquants de déchiffrer les communications avant de les renvoyer dans le réseau de l'opérateur mobile. Il est ainsi possible d'accéder à l'intégralité des informations communiquées, y compris les données de transaction et les données financières. • Les écoutes clandestines: la clé secrète Kc générée à l'aide des valeurs Ki et RAND de l'algorithme A5 peut être cassée, et le signal entre le champ modifié et le sous-système radio est susceptible de faire l'objet d'une écoute clandestine afin d'en extraire des transactions financières. • Déni de service: la valeur RAND envoyée au champ modifié lors de l'authentification initiale peut être attaquée et modifiée par l'intrus, provoquant ainsi un déni de service au sein du DFS.	nœuds des opérateurs de réseaux mobiles tels que le centre de commutation pour services mobiles (MSC), le canal USSD ou le centre de services de messages courts (SMSC).
Réseau infrastructurel (passerelle USSD, MSC, SMSC)	• Vulnérabilités inhérentes au protocole SS7: en l'absence de contrôles internes réguliers, il est possible d'accéder aux données des clients en interne. Le protocole GSM MAP utilisé pour autoriser la communication entre les nœuds infrastructurels de l'opérateur mobile transmet en texte clair, ce qui peut, en l'absence de chiffrement de bout en bout, offrir la possibilité de prendre connaissance en interne des informations relatives aux codes PIN ainsi qu'aux transactions. • Ces informations peuvent être falsifiées par des utilisateurs internes, en particulier dans les protocoles comme USSD, qui n'assurent pas l'intégrité des messages. • L'accès simplifié au réseau SS7 permet aux attaquants d'utiliser les opérations du sous-système application mobile (MAP) pour insérer ou modifier les données de l'abonné, de situer son emplacement ou d'intercepter ses communications mobiles.	

La figure 1 illustre les différents éléments du réseau ainsi que certains des points vulnérables de l'écosystème sur lesquels les attaques ci-dessus peuvent être lancées.

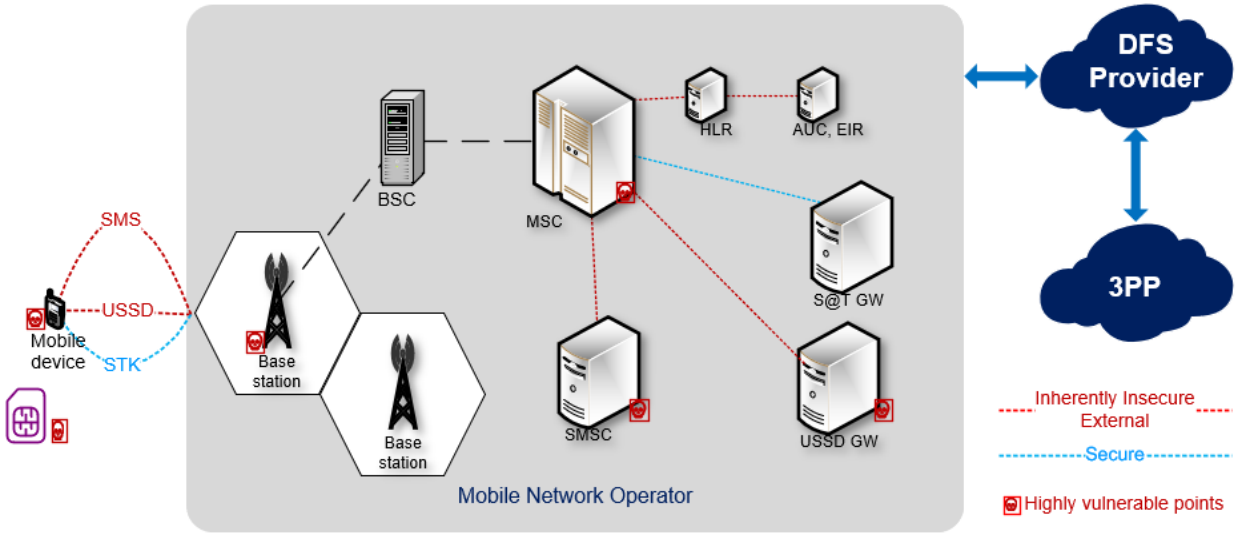

Figure 1 – Éléments de réseau et points vulnérables

3 Test des attaques contre les applications de DFS fondées sur les technologies USSD et STK

Les attaques et scénarios suivants permettent de tester la sécurité des transactions DFS fondées sur les technologies USSD et STK.

i. Attaques passives et actives contre les transactions de compte
ii. Tests d'authentification de l'appareil
iii. Tests des attaques par permutation de cartes SIM en vérifiant l'IMSI
iv. Tests des STK à l'aide de SIMtrace
v. Tests de la sécurité de la carte SIM à l'aide du testeur SIM
vi. Attaques par clonage SIM

3.1 Attaques passives et actives contre les transactions financières numériques

Le but de ce test est de déterminer si un attaquant peut réaliser une attaque passive ou active contre des transactions de DFS. La procédure et l'équipement nécessaires pour effectuer ces deux attaques sont identiques. Toutefois, les attaques passives consistent principalement à espionner les transactions DFS, c'est-à-dire à capturer et déchiffrer les messages des DFS pendant qu'ils traversent le réseau. Au cours d'une attaque active, l'attaquant interfère directement avec la transaction DFS. Cela peut se traduire par une attaque par déni de service ou par la transmission de transactions malveillantes visant à susciter une réaction chez le client DFS qui ne se doute de rien.

Les attaques passives et actives sont décrites ci-après en fonction du niveau d'accès du testeur.

a. La capture de données/paquets au niveau de la station d'émission-réception de base (BTS) désigne l'écoute clandestine et l'acquisition d'informations sur un compte par une personne extérieure ayant accès à un intercepteur GSM pendant l'activation.

b. La capture des journaux dans le réseau du fournisseur (par exemple, SMSC, passerelle USSD) désigne la capacité d'un attaquant à espionner une transaction DFS.
c. La modification des demandes des utilisateurs au niveau de la BTS désigne la capacité d'un adversaire à utiliser la BTS pour lancer des attaques par intercepteur.
d. La modification des données au niveau d'autres nœuds du sous-système de commutation de réseau (par exemple, SMSC, passerelle USSD) désigne la capacité d'un adversaire (utilisateur interne malveillant ou cyberattaquant distant) à modifier les données des DFS au sein du réseau du fournisseur.
e. La création de faux messages USSD au moyen du protocole SS7 pour manipuler autrui et solliciter le code PIN de l'utilisateur de DFS.

Ces tests permettent d'évaluer la vulnérabilité d'une transaction DFS à une attaque par intercepteur et peuvent être effectués en réalisant les actions suivantes:

a. Intercepter les données DFS lorsqu'elles passent par l'appareil mobile et la BTS à l'aide de systèmes de radiocommunication pilotés par un logiciel (SDR).
b. Capturer le trafic au niveau de la BTS dans le réseau des fournisseurs de réseau d'opérateurs de réseaux mobiles en l'absence d'intercepteur GSM.
c. Capturer le trafic et les journaux au niveau du MSC, du registre de localisation de rattachement (HLR), du SMSC et du serveur DFS.

3.1.1 Interception du trafic à l'aide d'un système SDR

Ce test montre que les attaquants qui ont accès à un périphérique radio logiciel universel, désormais appelé système de radiocommunication piloté par un logiciel (SDR), peuvent réaliser une attaque par intercepteur. Ce faisant, ils peuvent écouter clandestinement et acquérir des informations sur une transaction DFS telles que le code PIN de l'utilisateur.

L'algorithme de chiffrement GSM A5/1 est réputé faible[3]. Si l'opérateur mobile n'utilise pas l'algorithme de chiffrement A5/0 ou qu'il utilise l'algorithme de chiffrement faible A5/1, les services USSD et les SMS transitant par voie aérienne sont susceptibles d'être interceptés.

De plus, un système SDR agissant comme une fausse BTS peut forcer l'équipement de l'utilisateur ou l'appareil mobile à fonctionner avec un modem A5/0, qui ne bénéficie d'aucun chiffrement. Le cas échéant, il est possible de manipuler l'utilisateur pour solliciter son code PIN associé aux DFS.

Le système SDR peut être utilisé pour capturer les informations de transaction DFS de l'utilisateur telles que son code PIN, son mot de passe à usage unique ou ses SMS lorsqu'elles traversent l'interface aérienne (interface Um) pendant une session USSD.

Ce type de système peut également permettre à un attaquant de modifier des données de transaction et de les répéter dans le réseau.

[3] https://www.zdnet.com/article/gsm-a51-encryption-cracked-but-theres-no-need-to-panic/

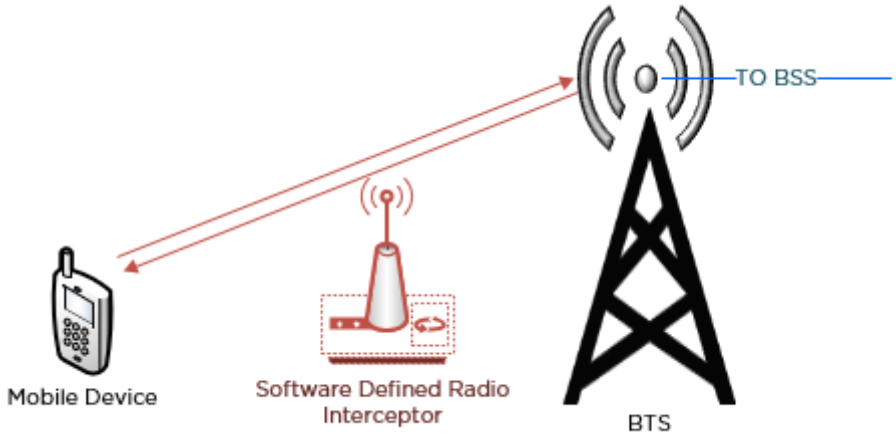

Figure 2 – Interception du trafic à l'aide d'un système SDR

3.1.2 Suivi du trafic au niveau de la BTS

Ce test envisage un scénario dans lequel un acteur malveillant a accès au site de la station de base du fournisseur de réseau mobile. La fonction de mise en miroir copie les paquets des ports d'écoute vers les ports d'observation sans affecter les capacités de traitement des paquets des appareils. Les administrateurs réseau l'utilisent pour analyser les paquets et surveiller les appareils, notamment pour veiller au bon fonctionnement des services réseau. Cependant, un utilisateur interne malveillant pourrait abuser de ce privilège pour espionner les transactions DFS.

Les tests peuvent être effectués soit en capturant les paquets directement depuis le terminal de maintenance local de la BTS, soit en configurant un port d'écoute sur un commutateur en suivant les étapes ci-dessous.

a. La figure 3 montre comment configurer le reniflage de paquets dans un port d'écoute.
b. Capturer la transmission entre la BTS et l'unité centrale de traitement et de transmission universelle.

Pour effectuer ce test, le fournisseur doit de préférence utiliser une BTS de faible puissance qui ne transporte aucun trafic commercial.

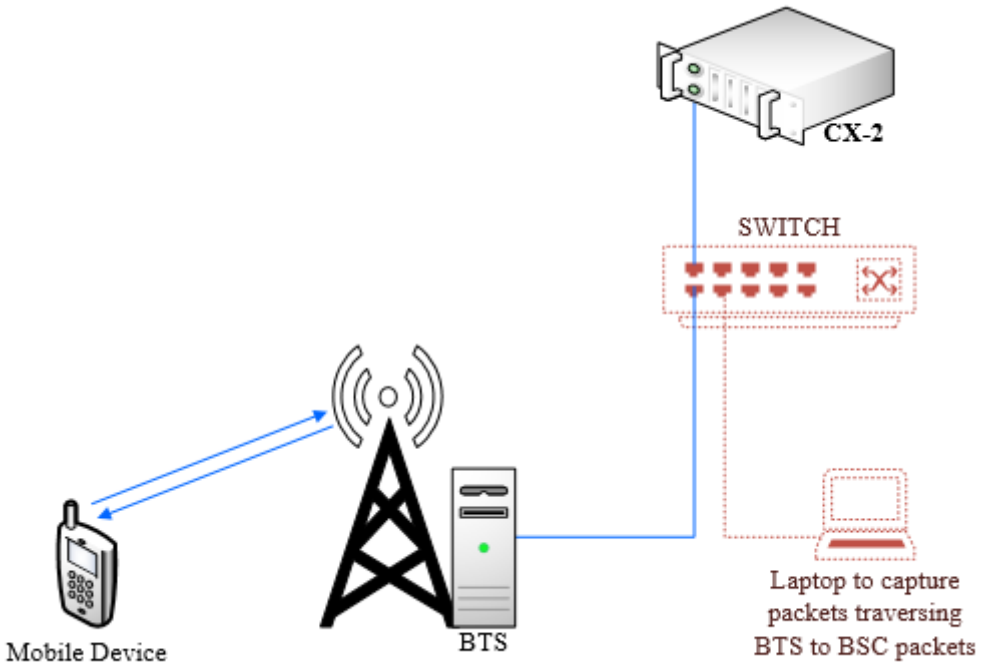

Figure 3 – Capture du trafic au niveau de la BTS

c. Comme indiqué sur la figure 3 ci-dessus, trois ports sont configurés sur un commutateur au sein du même réseau, dont un port configuré pour refléter le trafic.
d. Wireshark permet de capturer le trafic des ports d'écoute.
e. Effectuer des transactions DFS USSD et STK tout en capturant les paquets au point d'interception.
f. Il est possible d'analyser les paquets à l'aide d'outils comme Wireshark afin de vérifier si les données DFS sont transmises en toute sécurité de l'appareil de l'utilisateur vers le serveur DFS.

3.1.3 Suivi du trafic au niveau du MSC, du HLR, du SMSC et du serveur DFS

Ce test montre qu'il est possible qu'une opération d'un utilisateur interne ou qu'une cybercampagne[4] visant à lire les données DFS dans le réseau du fournisseur de services de télécommunication ou de DFS prenne place dans l'un des nœuds du réseau. Ces attaques peuvent être exécutées par le biais de connexions de maintenance à distance ou à l'aide des outils de surveillance des fournisseurs généralement utilisés par les opérateurs pour permettre aux fournisseurs de réseaux infrastructurels de résoudre les problèmes techniques.

La figure 4 montre les différents points de capture des données DFS dans l'écosystème.

Les tests permettent de déterminer si le fournisseur de DFS ou de services de télécommunication transmet les données DFS entre les différents nœuds du réseau de manière sécurisée.

La procédure ci-dessous permet de capturer le trafic du réseau.

a. Enregistrer la carte SIM et l'activer sur le réseau.

[4] https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

b. Une fois la carte SIM connectée au réseau, lancer la capture de paquets au niveau du SMSC, de la passerelle USSD, du HLR, du MSC et du serveur DFS.
c. Capturer les journaux au niveau de la station de base, du SMSC et du serveur DFS tout en effectuant des transactions DFS sur le téléphone.

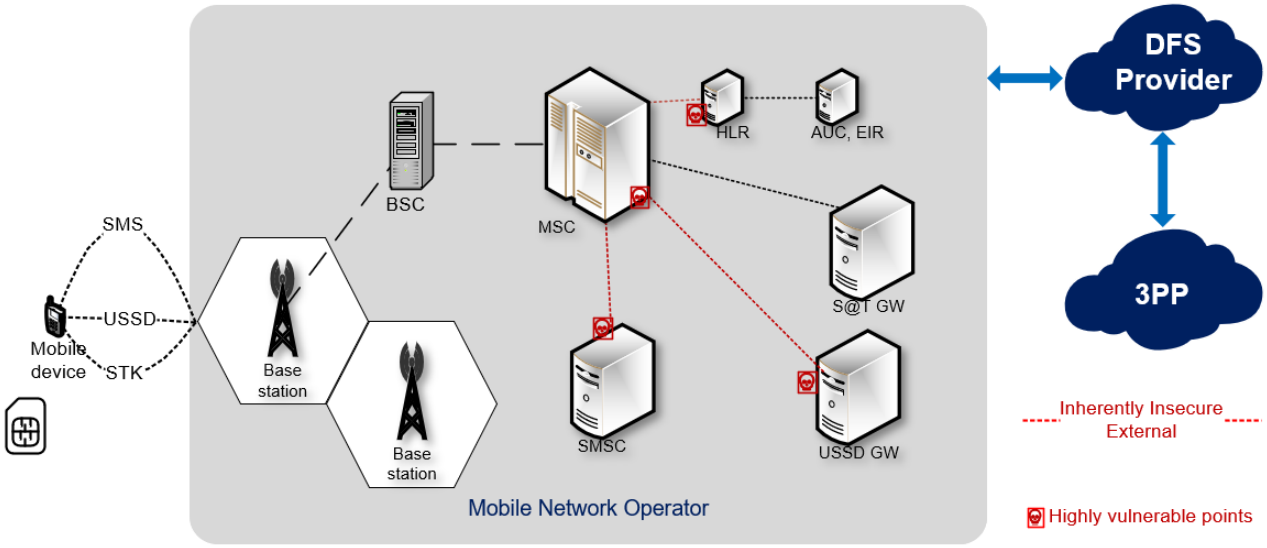

Figure 4 – Interception de transactions DFS

d. Analyser les journaux et les traces afin de récupérer l'activation du compte DFS et les informations de transaction telles que le code PIN du client à partir des captures de paquets au niveau du SMSC, du HLR, du serveur DFS et de la passerelle USSD.

3.1.4 Exploitation des attaques passives et actives

Il est également possible d'exécuter des attaques par intercepteur actives en compromettant les femtocellules, qui sont bien plus accessibles[5].

3.2 Validation du dispositif

Le but de ce test est de déterminer s'il existe un processus de validation de l'appareil mobile qui permet d'accéder au service d'argent mobile. Ce test vise à vérifier si l'opérateur du DFS ou l'opérateur de réseau mobile valide ou détecte un changement sur l'appareil lors de la vérification de son IMEI.

Une carte SIM est utilisée pour effectuer des transactions depuis deux appareils différents (possédant chacun un IMEI). L'utilisateur peut vérifier si des informations d'identification ou une étape de validation supplémentaires sont requises par le système DFS pour que la carte SIM puisse être utilisée afin d'effectuer des transactions DFS sur un autre appareil.

3.3 Validation et vérification de l'IMSI

Les fournisseurs de DFS identifient le client DFS par son numéro de réseau numérique à intégration de services d'abonné mobile (MSISDN), c'est-à-dire le numéro de téléphone du téléphone portable. Toutefois, dans le cas d'une permutation de carte SIM, l'IMSI associée à la carte SIM change.

[5] http://www.cs.ru.nl/~fabianbr/pub/thesis_fabian_vd_broek.pdf

L'authentification IMSI permet d'identifier la carte SIM et fournit à l'abonné un accès sécurisé à ses comptes de DFS.

Le but de ce test est de déterminer si le fournisseur DFS valide la carte SIM de l'utilisateur avant toute transaction DFS.

Si le fournisseur DFS valide la carte SIM en vérifiant l'IMSI utilisée, tout attaquant qui permute une carte SIM de DFS se voit alors refuser l'accès aux transactions effectuées avec ladite carte SIM.

Pour réaliser ce test, il faut effectuer deux transactions: l'une avec la carte SIM d'origine et l'autre avec une carte SIM permutée afin de déterminer si le DFS ou l'opérateur mobile demandent d'autres informations d'identification ou requièrent de suivre une étape de validation supplémentaire avant l'utilisation de la carte SIM permutée.

3.4 Attaques par intercepteur sur les SIM STK

Ce test démontre la confidentialité des transactions DFS à l'interface entre la carte SIM et le téléphone mobile. L'outil Osmocom SIMtrace2[6] est utilisé pour suivre de manière passive les communications entre la carte SIM et l'équipement mobile.

Ce test démontre le cas pratique suivant:

a) Un attaquant bénéficiant d'un accès physique à un appareil mobile utilisé pour des DFS pourrait insérer un proxy ou une carte SIM mince, comme la Turbo SIM[7], entre la carte SIM de l'utilisateur de DFS et l'interface du téléphone pour renifler le code PIN du mobile.
b) Ce test démontre également que la communication entre l'équipement mobile et la carte SIM n'est pas chiffrée et révèle les menaces associées aux cartes SIM minces.

3.4.1 Configuration du test

Configurer le matériel SIMtrace à l'aide des schémas et étapes ci-dessous.

a) Placer la carte SIM à tester dans le matériel SIMtrace.

b) Connecter le câble flexible au matériel SIMtrace et l'extrémité SIM à la prise du téléphone.
c) Connecter le matériel SIMtrace par USB à la machine hôte.

[6] https://osmocom.org/projects/simtrace2/wiki
[7] https://en.wikipedia.org/wiki/Turbo_SIM

La figure suivante illustre schématiquement cette configuration.

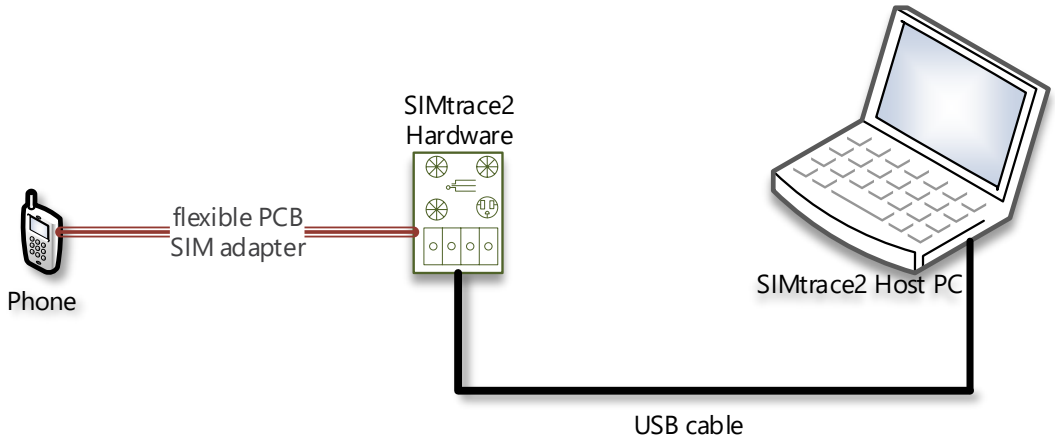

Figure 5 – Connexion schématique de SIMtrace

La figure 6 montre une configuration physique du dispositif SIMtrace.

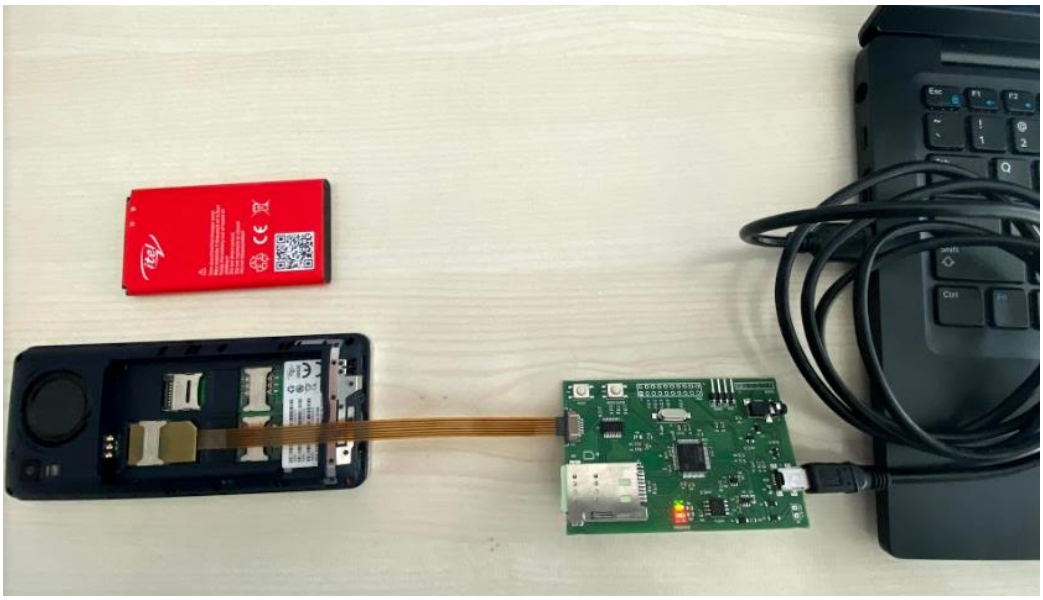

Figure 6 – Configuration physique de SIMtrace

d) Lancer Wireshark et écouter l'interface localhost.
e) Lancer SIMtrace et effectuer des transactions DFS sur la STK tout en capturant les paquets à l'aide de Wireshark.

```
$ ./simtrace
```

```
figisit@DFSLAB: ~
File  Edit  View  Search  Terminal  Help
^Cfigisit@DFSLAB:~$ simtrace2-sniff
simtrace2-sniff - Phone-SIM card communication sniffer
(C) 2010-2017 by Harald Welte <laforge@gnumonks.org>
(C) 2018 by Kevin Redon <kredon@sysmocom.de>

Using USB device 1d50:60e3 Addr=4, Path=1-2, Cfg=1, Intf=0, Alt=0: 255/1/0 (SIMtrace Sniffer)
Entering main loop
TPDU: 80 f2 00 00 44 62 42 82 02 78 21 84 10 a0 00 00 00 87 10 02 ff ff f0 01 89 00 00 01 ff a5 11 80 01 71 81 03 0
1 0a 32 82 01 0a 83 04 00 00 e1 d4 8a 01 05 8b 03 2f 06 02 c6 09 90 01 40 83 01 01 83 01 81 81 04 00 00 14 d0 90 00

TPDU: 80 f2 00 00 00 6c 44
TPDU: 80 f2 00 00 44 62 42 82 02 78 21 84 10 a0 00 00 00 87 10 02 ff ff f0 01 89 00 00 01 ff a5 11 80 01 71 81 03 0
1 0a 32 82 01 0a 83 04 00 00 e1 d4 8a 01 05 8b 03 2f 06 02 c6 09 90 01 40 83 01 01 83 01 81 81 04 00 00 14 d0 90 00

TPDU: 80 f2 00 00 00 6c 44
TPDU: 80 f2 00 00 44 62 42 82 02 78 21 84 10 a0 00 00 00 87 10 02 ff ff f0 01 89 00 00 01 ff a5 11 80 01 71 81 03 0
1 0a 32 82 01 0a 83 04 00 00 e1 d4 8a 01 05 8b 03 2f 06 02 c6 09 90 01 40 83 01 01 83 01 81 81 04 00 00 14 d0 90 00

TPDU: 80 f2 00 00 00 6c 44
Card state change: reset de-asserted
ATR: 3b 9e 96 80 1f c7 80 31 e0 73 fe 21 1b 66 d0 01 a0 81 0f 00 2f
PPS: ff 10 96 79
PPS: ff 10 96 79
Fi/Di switched to 512/32
Card state change: reset asserted
Card state change: reset de-asserted
ATR: 3b 9e 96 80 1f c7 80 31 e0 73 fe 21 1b 66 d0 01 a0 81 0f 00 2f
PPS: ff 10 96 79
PPS: ff 10 96 79
Fi/Di switched to 512/32
TPDU: 00 a4 00 04 02 3f 00 61 2e
TPDU: 00 c0 00 00 2e 62 2c 82 02 78 21 83 02 3f 00 a5 09 80 01 71 83 04 00 00 e1 d4 8a 01 05 8b 03 2f 06 02 c6 09 9
0 01 40 83 01 01 83 01 81 81 04 00 04 15 d6 90 00
TPDU: 00 a4 00 04 02 2f 00 61 21
TPDU: 00 c0 00 00 21 62 1f 82 05 42 21 00 32 04 83 02 2f 00 a5 03 80 01 71 8a 01 05 8b 03 2f 06 03 80 02 00 c8 88 0
1 f0 90 00
TPDU: 00 b2 01 04 32 61 18 4f 10 a0 00 00 00 87 10 02 ff ff f0 01 89 00 00 01 ff 50 04 55 53 49 4d ff ff ff ff ff f
f ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 90 00
TPDU: 00 a4 04 04 10 a0 00 00 00 87 10 02 ff ff f0 01 89 00 00 01 ff 61 44
TPDU: 00 c0 00 00 44 62 42 82 02 78 21 84 10 a0 00 00 00 87 10 02 ff ff f0 01 89 00 00 01 ff a5 11 80 01 71 81 03 0
1 0a 32 82 01 0a 83 04 00 00 e1 d4 8a 01 05 8b 03 2f 06 02 c6 09 90 01 40 83 01 01 83 01 81 81 04 00 00 14 d0 90 00

TPDU: 00 20 00 01 00 63 c3
TPDU: 00 20 00 81 00 63 c3
```

Figure 7 – Exemple de sortie SIMtrace

f) Analyser les traces SIM Wireshark des paquets capturés relatifs aux transactions STK entre la carte SIM et l'équipement mobile.

```
405  125.…  lo…  lo… GSM …  65 ETSI TS 102.221 STATUS : Terminal should repeat command, Lengt… 38229 (38229),gsmtap (4729)
 54  32.8…  lo…  lo… GSM …  83 ETSI TS 102.221 TERMINAL PROFILE                               38229 (38229),gsmtap (4729)
349  85.5…  lo…  lo… GSM …  77 ETSI TS 102.221 TERMINAL RESPONSE DISPLAY TEXT                 38229 (38229),gsmtap (4729)
393  105.…  lo…  lo… GSM …  77 ETSI TS 102.221 TERMINAL RESPONSE DISPLAY TEXT                 38229 (38229),gsmtap (4729)
407  128.…  lo…  lo… GSM …  77 ETSI TS 102.221 TERMINAL RESPONSE DISPLAY TEXT                 38229 (38229),gsmtap (4729)
434  149.…  lo…  lo… GSM …  77 ETSI TS 102.221 TERMINAL RESPONSE DISPLAY TEXT                 38229 (38229),gsmtap (4729)
345  80.2…  lo…  lo… GSM …  84 ETSI TS 102.221 TERMINAL RESPONSE GET INPUT                    38229 (38229),gsmtap (4729)
403  121.…  lo…  lo… GSM …  84 ETSI TS 102.221 TERMINAL RESPONSE GET INPUT                    38229 (38229),gsmtap (4729)
157  33.4…  lo…  lo… GSM …  81 ETSI TS 102.221 TERMINAL RESPONSE POLL INTERVAL                38229 (38229),gsmtap (4729)
351  86.0…  lo…  lo… GSM …  87 ETSI TS 102.221 TERMINAL RESPONSE PROVIDE LOCAL INFORMATION    38229 (38229),gsmtap (4729)
409  129.…  lo…  lo… GSM …  87 ETSI TS 102.221 TERMINAL RESPONSE PROVIDE LOCAL INFORMATION    38229 (38229),gsmtap (4729)
332  62.8…  lo…  lo… GSM …  80 ETSI TS 102.221 TERMINAL RESPONSE SELECT ITEM                  38229 (38229),gsmtap (4729)
336  65.0…  lo…  lo… GSM …  77 ETSI TS 102.221 TERMINAL RESPONSE SELECT ITEM                  38229 (38229),gsmtap (4729)
338  68.3…  lo…  lo… GSM …  80 ETSI TS 102.221 TERMINAL RESPONSE SELECT ITEM                  38229 (38229),gsmtap (4729)
340  71.5…  lo…  lo… GSM …  80 ETSI TS 102.221 TERMINAL RESPONSE SELECT ITEM                  38229 (38229),gsmtap (4729)
396  111.…  lo…  lo… GSM …  80 ETSI TS 102.221 TERMINAL RESPONSE SELECT ITEM                  38229 (38229),gsmtap (4729)
401  116.…  lo…  lo… GSM …  80 ETSI TS 102.221 TERMINAL RESPONSE SELECT ITEM                  38229 (38229),gsmtap (4729)
370  89.9…  lo…  lo… GSM …  77 ETSI TS 102.221 TERMINAL RESPONSE SEND SHORT MESSAGE           38229 (38229),gsmtap (4729)
428  133.…  lo…  lo… GSM …  77 ETSI TS 102.221 TERMINAL RESPONSE SEND SHORT MESSAGE           38229 (38229),gsmtap (4729)
121  33.2…  lo…  lo… GSM …  77 ETSI TS 102.221 TERMINAL RESPONSE SET UP EVENT LIST            38229 (38229),gsmtap (4729)

  ˅ Command details: 012304
        Command Number: 0x01
        Command Type: GET INPUT (0x23)
        Command Qualifier: 0x04
  ˅ Device identity: 8281
        Source Device ID: Terminal (Card Reader) (0x82)
        Destination Device ID: SIM / USIM / UICC (0x81)
  ˅ Result: 00
        Result: Command performed successfully (0x00)
  ˅ Text string: 0435343533
        Text String Encoding: GSM default alphabet, 8 bits (0x04)
        Text String: 5453
Status Word: 911c Normal ending of command with info from proactive SIM
```

Figure 8 – Exemple de sortie Wireshark de SIMtrace – cette trace Wireshark montre que le PIN a été capturé en texte clair par SIMtrace.

La capture Wireshark ci-dessus montre un des résultats possibles; un attaquant peut lire le code PIN et les données lorsqu'ils sont saisis sur l'appareil avec la trace SIM.

3.4.2 Exploitation des vulnérabilités de la carte SIM

Ce test démontre le risque associé aux cartes SIM minces et aux appareils dont l'accès aux composants matériels qui contiennent la carte SIM ne présente aucune difficulté.

Une attaque par intercepteur peut être réalisée à l'aide de la Bladox Turbo SIM[8], qui est insérée entre la carte SIM et le téléphone. Tous les paquets qui traversent la carte SIM sont transmis à l'attaquant.

3.5 Attaques utilisant un message hertzien binaire[9]

Ce test démontre la vulnérabilité d'une carte SIM aux attaques d'acteurs malveillants qui visent à envoyer des messages hertziens binaires comprenant des commandes spécifiques. Ce test fait passer une carte SIM par un lecteur de carte à puce compatible PCSC afin de déterminer si elle est sensible aux attaques Simjacker[10] ou WIB[11].

Ces dernières permettent aux attaquants d'envoyer un message binaire hertzien aux applications SIM qui s'exécutent sur la carte SIM et d'interagir avec l'appareil mobile afin d'effectuer les actions suivantes:

a) Lancer un appel, envoyer un SMS et envoyer des demandes SS.

b) Lancer des demandes USSD.

c) Lancer un navigateur Internet avec une URL spécifique.

d) Afficher du texte sur l'appareil.

e) Rentrer en contact avec les utilisateurs.

L'attaque WIB et l'attaque Simjacker se distinguent par les applications de la carte SIM qu'elles ciblent. Simjacker exécute des commandes via l'application S@T Browser. En revanche, les attaques WIB ciblent l'application Wireless Internet Browser (WIB).

La possibilité d'exécuter ces attaques à distance sur une carte SIM constitue un risque pour les utilisateurs de DFS.

Les fournisseurs utilisent des messages binaires hertziens pour envoyer des mises à jour et des modifications aux menus SIM sans qu'il soit nécessaire de rééditer la carte SIM. L'utilisateur final reçoit un message binaire de l'opérateur pour télécharger ou activer de nouveaux services sur sa carte SIM sans qu'il ait à se rendre dans un point de vente. Les fournisseurs de DFS qui offrent des DFS avec STK mettent à jour le menu d'application STK de la liste de services financiers à l'aide de

[8] https://www.bladox.com/
[9] https://opensource.srlabs.de/projects/simtester/wiki#TAR-Scanner
[10] https://simjacker.com/downloads/technicalpapers/AdaptiveMobile_Security_Simjacker_Technical_Paper.pdf
[11] https://ginnoslab.org/2019/09/21/wibattack-vulnerability-in-wib-sim-browser-can-let-attackers-globally-take-control-of-hundreds-of-millions-of-the-victim-mobile-phones-worldwide-to-make-a-phone-call-send-sms-to-any-phone-numbers/

messages hertziens binaires. L'exécution est souvent indétectable et, dans la plupart des cas, ne génère aucune notification à l'utilisateur et aucune action n'est requise.

Un attaquant peut faire usage de cette fonctionnalité pour envoyer un SMS binaire comprenant des commandes ciblant les DFS de l'utilisateur.

Ce test utilise l'application SIMtester pour vérifier si une carte SIM est vulnérable et exploitable par des attaques hertziennes par SMS. Il vérifie pour cela si le fournisseur a activé les fonctions de sécurité adéquates sur la carte SIM pour les esquiver.

Chaque application est dotée d'un niveau de sécurité minimal qui spécifie le contrôle de sécurité minimal dont les paquets sécurisés envoyés à l'application font l'objet. La carte SIM vérifie le niveau de sécurité avant de traiter la commande binaire. Si le test échoue, elle rejette les messages. Si l'application SIM est configurée avec un niveau de sécurité minimal = 0 ou ne vérifie pas les identifiants de la clé et de l'algorithme de chiffrement (KiC) et de la clé et de l'algorithme de contrôle de redondance/CC/de signature numérique (KiD), un attaquant peut envoyer une commande SMS hertzienne pour contrôler l'application SIM sans même connaître la clé hertzienne, le KiC ou le KiD. Le KiC est utilisé pour chiffrer la commande sécurisée, et le KiD sert à générer la somme de contrôle cryptographique, qui permet de vérifier que la commande provient d'une identité valide.

3.5.1 Configuration du test

Pour effectuer les tests, dézippez le fichier d'application SIMtester et exécutez la commande ci-dessous.

```
$ unzip SIMTester_v1.9.zip

$ java -jar SIMTester.jar
```

L'application s'exécute en envoyant des messages à chacune des références d'application d'utilitaire afin de tester la vulnérabilité des commandes SMS hertziennes sans jeu de clés.

La sortie des résultats indique si la carte SIM est vulnérable ou non.

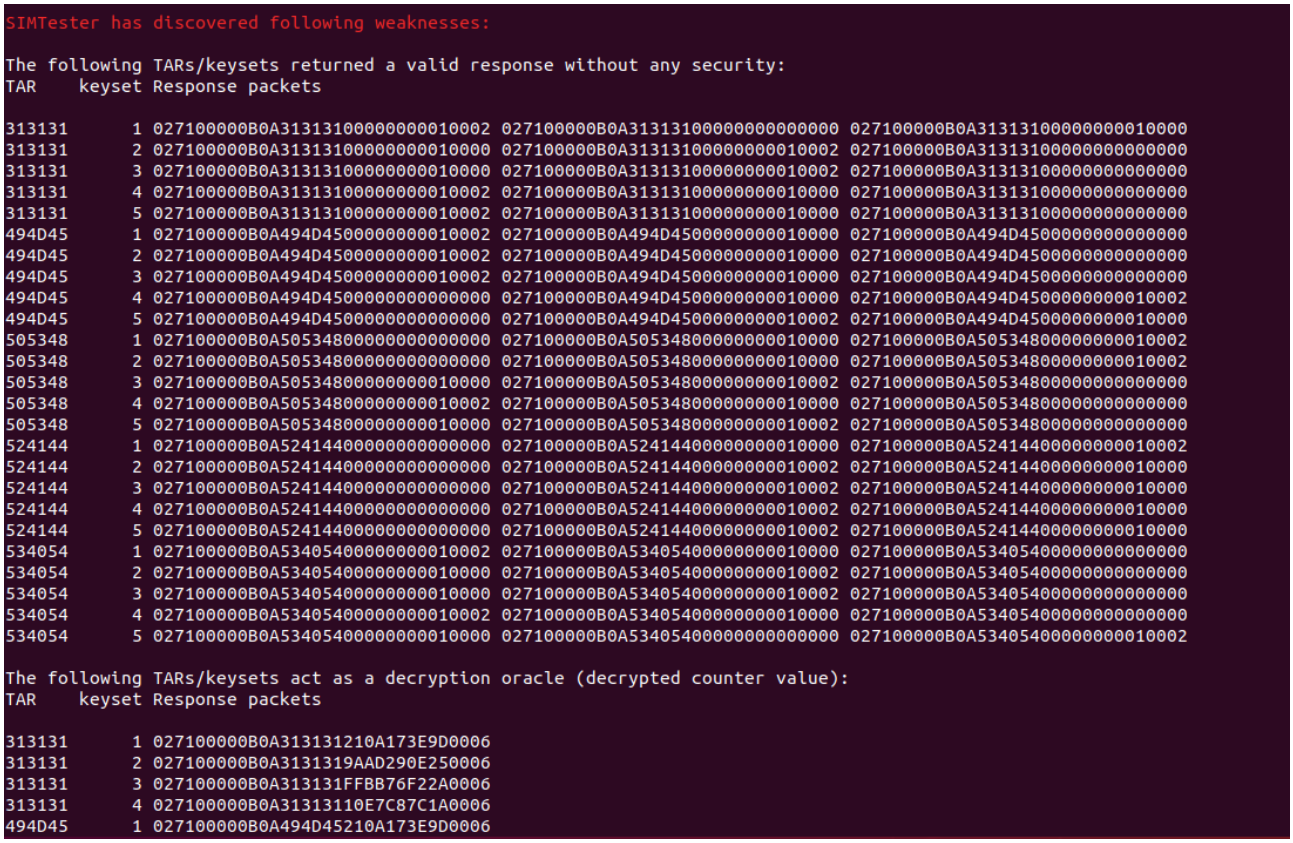

Figure 9 – Sortie du SIMtester d'une carte SIM vulnérable

3.5.2 Exploitation de la vulnérabilité Simjacker

Les trois conditions suivantes doivent être réunies pour exploiter la vulnérabilité de Simjacker:

a. Le centre SMS accepte et relaie des messages binaires.
b. La capacité de l'appareil cible à recevoir des messages binaires SMS qui contiennent des commandes (U)SIM Application Toolkit.

c. La technologie S@T Browser déployée sur la carte SIM avec le niveau de sécurité minimal défini sur "No Security".

3.6 Exécution du code USSD à distance sur l'appareil avec ADB

Le but de ce test est de démontrer que les attaquants distants peuvent exécuter des transactions DFS en utilisant le code USSD sur un appareil rooté. Ce test est réalisé à l'aide d'un ordinateur sur lequel sont installés les outils de la plateforme Android Debug Bridge (ADB)[12]. L'appareil Android rooté est connecté à l'ordinateur par un câble USB.

Le test nécessite que l'appareil mobile et la machine hôte soient connectés au même point d'accès Wi-Fi.

Les instructions suivantes détaillent la configuration du test.

a) La commande suivante doit être exécutée afin d'identifier l'adresse IP de l'appareil mobile sur la machine hôte.

[12] https://www.xda-developers.com/quickly-install-adb/

./adb shell ifconfig wlan0 *l'IP de l'appareil mobile est listée, par exemple 192.168.1.104*

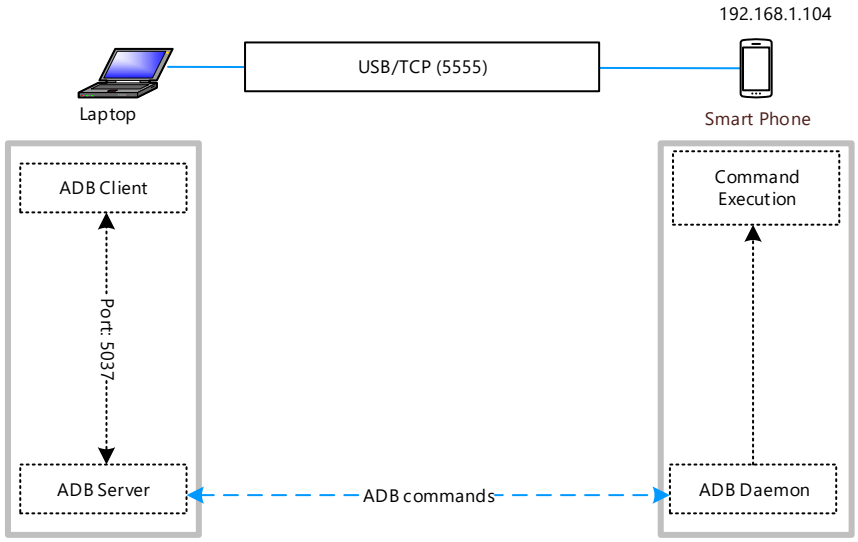

Figure 10 – Configuration schématique de la connexion ADB

b) Se connecter à l'appareil mobile avec son adresse IP à l'aide de la commande suivante:

./adb connect 192.168.1.104

c) Confirmer que l'ordinateur hôte est connecté à l'appareil cible par Wi-Fi à l'aide de la commande:

./adb devices

d) Une fois le câble USB retiré, tester l'exécution des commandes USSD mobiles à distance sur un appareil en exécutant les commandes ci-dessous sur l'interface système de l'ordinateur:

./adb shell

am start -a android.intent.action.CALL -d tel:*185*1*1%23

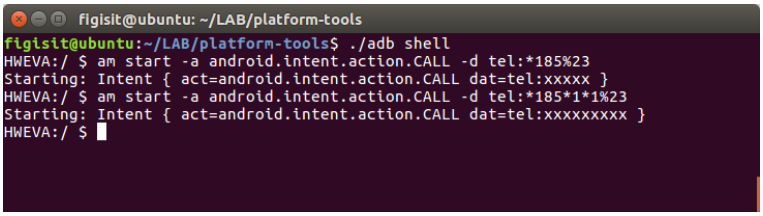

Figure 11 – Commande USSD à distance à l'aide de

Ce test montre qu'un attaquant distant qui a eu accès à l'appareil peut ensuite émettre des commandes USSD à distance et effectuer une transaction DFS.

3.7 Exécution du code USSD à distance avec SS7

En raison du haut niveau de confiance des utilisateurs lors de la réception de messages USSD, l'attaque la plus simple à exécuter et reproduire consiste à utiliser le code USSD pour envoyer un message frauduleux à l'utilisateur en usurpant l'identité du fournisseur de services financiers et en incitant l'utilisateur à divulguer des informations sensibles telles que son numéro de compte et son code PIN.

Par exemple, pour hameçonner ces informations d'identification, l'attaquant envoie un message USSD d'hameçonnage comme dans la figure 12 ci-dessous.

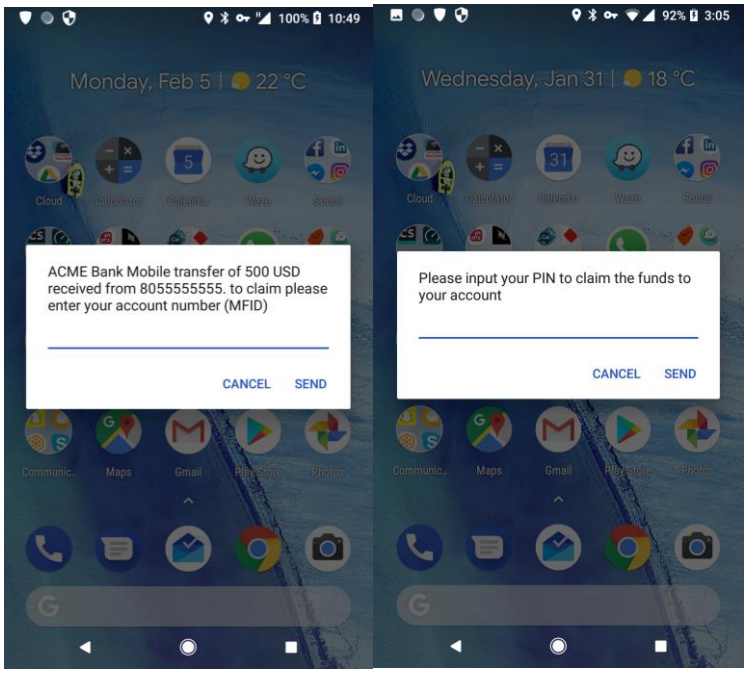

Figure 12 – Utilisation d'un message USSD pour hameçonner l'utilisateur et le manipuler

Un attaquant ayant accès au réseau SS7 peut envoyer des messages USSD à n'importe quel réseau.

Étant donné que le message USSD ne contient aucune identification et que l'utilisateur est habitué à recevoir ces messages du réseau, l'utilisateur divulgue son numéro de compte et son code PIN en toute confiance. L'attaquant se connecte ensuite au compte et intercepte les fonds.

3.8 Attaques par clonage SIM

Le but de ce test est d'évaluer si un attaquant capable de cloner une carte SIM peut réussir à authentifier la SIM clonée auprès du service d'argent mobile et effectuer des transactions frauduleuses. Cette attaque n'est possible que sur les cartes SIM compatibles avec l'algorithme obsolète COMP128v1.

Il est possible de simuler le clonage de la carte SIM à l'aide du logiciel libre pySIM[13].

[13] https://github.com/osmocom/pysim

4 Bonnes pratiques d'atténuation des menaces USSD et STK

Cette section présente les bonnes pratiques que les fournisseurs de DFS et les opérateurs de réseaux mobiles peuvent suivre afin de contourner les menaces et les attaques visant les implémentations DFS fondées sur les technologies USSD et STK.

4.1 Bonnes pratiques d'atténuation des risques de récupération des données de l'utilisateur

- Utiliser un protocole TLS v1.2 ou supérieur pour sécuriser la connexion entre le SMSC GW, la passerelle USSD et le serveur d'application DFS.
- L'opérateur mobile doit veiller à utiliser un chiffrement radio sécurisé entre les appareils des utilisateurs et les stations de base.
- Utiliser le délai d'expiration de la session côté client pour limiter le nombre de demandes/réponses altérées.
- Déployer le masquage du code PIN USSD dans la mesure du possible.
- Suivre le développement de technologies permettant de sécuriser les paiements mobiles grâce au chiffrement (et au déchiffrement ultérieur du côté de l'opérateur mobile) des messages USSD. Avec l'émergence de nouvelles exigences de faible performance et de schémas de chiffrement résistant à l'informatique quantique, il est désormais possible de crypter les messages USSD de bout en bout, même dans les réseaux 2G existants. La commission d'étude 11 de l'UIT-T, qui porte son intérêt sur les exigences de signalisation, les protocoles et les spécifications de test, travaille actuellement à la rédaction d'un rapport technique (qui sera publié en mars 2021) qui passera ces technologies en revue et soumettra une liste d'applications à intégrer dans la signalisation USSD, tant du côté du réseau infrastructurel que de l'équipement de l'utilisateur (dans la carte SIM).
- S'assurer qu'il existe un processus vérifiable permettant d'examiner l'accès aux traces ainsi qu'aux journaux dans les interfaces qui utilisent des protocoles intrinsèquement peu sûrs.
- Offrir aux clients la possibilité de ne pas utiliser les canaux USSD ou STK dans le cadre de leurs transactions financières, en particulier ceux qui peuvent accéder au DFS depuis une application.
- Fixer des limites de transaction pour les retraits et les transferts des clients par le canal USSD, par client et par jour selon les besoins.

4.2 Bonnes pratiques d'atténuation des risques liés à la permutation et au recyclage de cartes SIM[14]

- L'authentification des appareils consiste à suivre les numéros IMEI des appareils utilisés pour accéder à l'argent mobile afin d'améliorer la sécurité des points d'extrémité. Il est ainsi possible de signaler les comptes qui changent d'appareil.
- Le processus de vérification de l'identité doit s'appuyer à la fois sur quelque chose que l'utilisateur est, sur quelque chose qu'il a et sur quelque chose qu'il sait. L'utilisateur devra par exemple présenter une pièce d'identité valide, se soumettre à une vérification biométrique et fournir des informations sur son compte avant de pouvoir procéder à un échange ou un remplacement de carte SIM.
- Les fournisseurs de DFS et de services de paiement doivent être en mesure de détecter en temps réel l'échange ou le remplacement d'une carte SIM associée à des DFS. Ils doivent également procéder à des vérifications supplémentaires avant d'autoriser la nouvelle

[14] https://www.issms2fasecure.com/assets/sim_swaps-04-16-2020.pdf

carte SIM à effectuer des transactions de valeur élevée ou à apporter des modifications au compte de DFS.

- L'opérateur de réseaux mobiles doit concevoir un processus de recyclage des numéros mobiles qui requiert de communiquer avec les fournisseurs de DFS par le biais des MSIDN échangés ou recyclés. [Ici, le recyclage de numéro désigne la réattribution d'un MSIDN dormant/inactif à un nouveau client par l'opérateur de réseaux mobiles]. Lorsqu'une carte SIM est recyclée, l'opérateur de réseaux mobiles signale un changement de numéro IMSI pour le numéro de téléphone du compte correspondant. Le fournisseur de DFS doit alors bloquer l'accès au compte en attendant de vérifier que le nouveau propriétaire de la carte SIM est bien le titulaire du compte.
- L'opérateur de réseau mobile doit sauvegarder et stocker de manière sécurisée les données de carte SIM telles que le numéro IMSI et les valeurs de clé secrète (valeurs Ki).

4.3 Bonnes pratiques à suivre pour éviter l'exécution du code USSD à distance sur les appareils

- Les propriétaires d'appareils Android doivent désactiver l'interface ADB et les fournisseurs d'appareils ne doivent pas livrer de produits en laissant ADB activé sur le réseau.
- Les utilisateurs de DFS doivent être informés des dangers liés aux connexions aux réseaux Wi-Fi publics ainsi que de la manière dont ils doivent gérer les risques associés aux autorisations des applications. Les utilisateurs de DFS doivent notamment être conscients des risques de confidentialité auxquels ils s'exposent lorsqu'ils accordent leur autorisation à une application sur un appareil. Si les autorisations demandées sont trop invasives, il leur est recommandé de ne pas télécharger l'application.
- Éviter d'utiliser des appareils rootés dans le cadre de transactions DFS et veiller à ce que les logiciels des appareils soient régulièrement mis à jour. Cela les protège des logiciels malveillants et des logiciels espions.

4.4 Bonnes pratiques d'atténuation des risques d'exploitation de la carte SIM à l'aide de technologies hertziennes binaires

- Filtrage des SMS: les attaquants à distance passent par les réseaux mobiles pour envoyer des SMS binaires vers et depuis les téléphones des victimes. Les opérateurs mobiles doivent empêcher l'envoi et la réception de messages binaires comme les SMS hertziens. Ces SMS ne devraient être autorisés qu'à partir de sources figurant sur une liste blanche.
- Les messages hertziens avec codage STK provenant d'abonnés domestiques doivent être limités à l'envoi à/par la plateforme d'opérateurs de réseaux mobiles et non à d'autres abonnés.
- Les fournisseurs de contenu envoient généralement du texte sous la forme de messages SMS A2P. Leur trafic ne doit pas contenir de messages avec codage STK.
- Routage SMS domestique: il s'agit de l'interdiction de l'ensemble des SMS sortants et entrants, à l'exception de ceux qui sont acheminés par les hôtes du réseau domestique.