FIGI
FINANCIAL INCLUSION
GLOBAL INITIATIVE

АЮУЛГҮЙ БАЙДАЛ, ДЭД БҮТЭЦ, ИТГЭЛИЙН АЖЛЫН ХЭСЭГ

USSD болон STK суурилсан дижитал санхүүгийн үйлчилгээний аюулгүй байдлын шалгалт, туршилт

Аюулгүй байдлын ажлын хэсгийн тайлан

Аюулгүй байдал, дэд бүтэц, итгэлцлийн ажлын хэсэг

USSD БОЛОН STK-Д СУУРИЛСАН ДИЖИТАЛ САНХҮҮГИЙН ҮЙЛЧИЛГЭЭНИЙ АЮУЛГҮЙ БАЙДЛЫН ШАЛГАЛТ, ТУРШИЛТ

АНХААРУУЛГА

Санхүүгийн үйлчилгээний хүртээмжийг нэмэгдүүлэх олон улсын санаачлага (FIGI)-ын хүрээнд Дэлхийн банк (WBG), Төлбөр тооцоо болон зах зээлийн дэд бүтцийн хороо (CPMI)-ны хамтарсан 3 жилийн хөтөлбөрийн хүрээнд зохион байгуулагдсан арга хэмжээ юм.

Дэлхий даяарх санхүүгийн үйлчилгээний хүртээмж 2050 үндсэн зорилтод хүрэхийн тулд улс орон бүрийн санхүүгийн үйлчилгээний хүртээмжийг нэмэгдүүлэх зорилтод дэмжлэг үзүүлэх зорилгоор Билл ба Мелинда Гейтсийн сан (BMGF), Олон улсын цахилгаан холбооны байгууллага (ITU) хамтран түс арга хэмжээнд дэмлэг туслалцаа үзүүлэн хамтран ажилладаг бөгөөд түс сангаас Бүгд Найрамдах Хятад Ард Улс, Египт, Мексик зэрэг улсуудтай хамтран ажиллаж байна. Хамтын ажиллагаа болон ерөнхий зохион байгуулалтын хувьд (1) Цахим төлбөр тооцоог нутагшуулах ажлын хэсэг (ДБАА удирдлагаар), (2) Дижитал санхүүгийн үйлчилгээн дэх танилт бүртгэл, хаяг ID -н ажлын хэсэг (ДБАА удирдлагаар), (3) Дэд бүтэц аюулгүй бадлыг бэхжүүлэх ажлын хэсэг (ОУЦХБ удирдлагаар)-үүд ажиллаж тухайн улсын бодлого, зохицуулалтын байгууллага болон хувийн хэвшил, олон нийтийн санаа, санаачлагыг тусган уялдуулж хамтран ажиллаж байна.

Энэхүү тайлан нь Олон улсын цахилгаан холбооны байгууллагаар ахлуулсан FIGI аюулгүй байдал, дэд бүтэц, итгэлцлийн ажлын хэсгийн бүтээгдэхүүн юм.

Энэхүү тайланд илэрхийлсэн дүгнэлт, тайлбар, дүгнэлтүүд нь Төлбөр ба зах зээлийн дэд бүтцийн хороо, Билл ба Мелинда Гейтсийн сан, Олон улсын цахилгаан холбооны байгууллага, Дэлхийн банк зэрэг Санхүүгийн хүртээмжийг дэмжих санаачилгыг идэвхижүүлэгчдийн шууд санал санаачлагын хүрээнд гарсан зүйлс бөгөөд шууд ашиглах, баримт бичигт түсгах албагүй.

Мөн тодорхой компаниуд эсвэл тодорхой үйлдвэрлэгчдийн бүтээгдэхүүнийг дурьдсан нь тэдгээрийг дурдаагүй ижил төстэй шинж чанартай бусад бүтээгдэхүүнээс илүү, ОУЦХБ-аас зөвшөөрсөн эсвэл санал болгосон гэсэн үг биш юм.

FIGI-ийн түншүүд энэ ажилд орсон мэдээллийн үнэн зөвийг баталгаажуулахгүй бөгөөд хил хязгаар, өнгө, нэр томъёо болон бусад мэдээлэл нь аливаа улс орон, нутаг дэвсгэр, хот, бүс нутгийн эрх зүйн байдлын талаарх FIGI-ийн түншүүдийн дүгнэлт, түүний эрх бүхий байгууллагуудын дүгнэлтийг илэрхийлэхгүй мөн анхаарна уу.

Энэ тайлангийн талаар

Энэхүү тайланг Флоридагийн их сургуулийн Кевин Батлер, ОУЦХБ-ын Вижэй Мори, Арнольд Кибуука нар бичсэн. Тайланг хянаж, засварлахад дэмжлэг, туслалцаа үзүүлсэн Ассаф Клингер, Ваулто нарт талархал илэрхийлье. Зохиогчид болон FIGI аюулгүй байдлын дэд бүтэц, итгэлцлийн ажлын хэсгийн гишүүдэд талархал илэрхийлье. Энэхүү тайлангийн ерөнхий удирдамжийг ОУЦХБ-ын Вижай Маури өгсөн.

Хэрэв та нэмэлт мэдээлэл өгөхийг хүсвэл Vijay Mauree тай холбогдоно уу. tsbfigisit @ itu .int


SIM1
SIM2

Агуулга

Товчлол

AuC Authentication Centre
A2P Application-to-Person
BSC Base Station Controller
BSS Base station Subsystem
BTS Base Transceiver Station
DFS Digital Financial Services
EIR Equipment Identification Register
GSM Global System for Mobile Communications
HLR Home Location Register
IMEI International Mobile Equipment Identity
IMSI International Mobile Subscriber Identity
KIc Key and algorithm Identifier for ciphering
KID Key and algorithm Identifier for Redundancy Check/CC/Digital Signature
MSC Mobile Switching Centre
MSISDN Mobile Station International Subscriber Directory Number Number.
(Note – A number used to identify a mobile phone number internationally, it includes a country code and a National Destination Code which identifies the subscriber's operator)
MNO Mobile Network Operator
OTA Over the Air
PCB Printed Circuit Board
PCSC Personal Computer/Smart Card
PIN Personal Identification Number
SAT SIM Application Toolkit
SIM Subscriber Identification Module
SMPP Short Message Peer-to-Peer Protocol
SMS Short Messaging Service
SMSC Short Message Service Centre
STK SIM Tool Kit
TAR ToolKit Application Reference
USIM Universal Subscriber Identity Module
USSD GW Unstructured Supplementary Service Data Gateway

AuC -баталгаажуулалтын төв
A2P -програмаас хүн рүү
BSC -бааз станцын хяналт
BSS -бааз станцын дэд систем
BTS -үндсэн дамжуулагч станц
DFS- Дижитал санхүүгийн үйлчилгээ
EIR -тоног төхөөрөмжийн таних бүртгэл
GSM Гар утасны холбооны дэлхийн систем
HLR -гэрийн байршлын бүртгэл
IMEI -олон улсын хөдөлгөөнт төхөөрөмжийн таних тэмдэг
IMSI -олон улсын гар утасны захиалагчийн таних тэмдэг
KIc -Түлхүүр ба алгоритмын танигч
KID - шууд нөөцөөр давхар ажиллаж дижитал гарын үсийн Түлхүүр ба алгоритмын танигч.
MSC -Mobile Switching Center
MSISDN - мобайл станц дахт олон улсын захиалагчийн лавлах дугаар .
(Тэмдэглэл – Гар утасны дугаарыг олон улсад танихад ашигладаг дугаар бөгөөд үүнд улсын код болон захиалагчийн операторыг тодорхойлсон Үндэсний очих газрын код)
MNO - үүрэн холбооны үйлчилгээ эрхлэгч
OTA -Over the Air
PCB -хэвлэсэн хэлхээний самбар
PCSC-хувийн компьютер/ухаалаг карт
PIN -хувийн таних дугаар
SAT -SIM суурилсанпрограмын хэрэгсэл
SIM -захиалагчийг таних модуль
SMPP Богино Мессежийн ижил түвшинд дэх шууд холболтын протокол
SMS богино мессежийн үйлчилгээ
SMSC богино мессеж үйлчилгээний төв
STK SIM хэрэгслийн багц
TAR Програм дахь хэрэгслүүлрүүдийн лавлагаа
USIM Нийтзахиалагчди йг таних модуль
USSD GW Бүтэцгүй нэмэлт үйлчилгээний өгөгдөл дамжуулах гарц

USSD болон STK дээр суурилсан дижитал санхүүгийн үйлчилгээний програмуудын аюулгүй байдлын туршилт

1 ТАНИЛЦУУЛГА

Дижитал санхүүгийн үйлчилгээ (ДСҮ) үзүүлэгчид, ялангуяа хөгжиж буй орнуудад тухайн үйлчилгээний өсөлт, хэрэглээг нэмэгдүүлэхийн тулд Бүтэцгүй Нэмэлт Үйлчилгээний Өгөгдөл (USSD) болон Sim Tool Kit (STK) сувгуудыг ихээр ашиглаж байна.

GSMA-ийн тооцоолсноор Африкт гар утасны цахим гүйлгээний 90 гаруй хувь нь USSD-г ашигладаг бол Бангладеш дахь ДСҮ-ний оператор bKash, Камбож дахь Wing, Пакистан дахь Easy Paisa, Танзани, Кени дэх Tigo болон M-Pesa, Зимбабвегийн EcoCash, Африк болон Ойрхи Дорнодын MTN Mobile Money, Африк, Ази дахь Airtel зэрэг томоохон оролцогчид цахим мөнгөний болон дижитал санхүүгийн харилцаанд USSD-г үндсэн суваг болгон ашигладаг.

Энэхүү баримт бичиг нь USSD болон STK дээр суурилсан ДСҮ-ний аюулгүй байдал, эмзэг байдлыг онцолсон бөгөөд энэ сонголтыг ашиглаж буй ДСҮ үзүүлэгч, мобайл сүлжээний операторууд болон ДСҮ-ний хэрэглэгчдэд зориулсан шилдэг туршлагыг санал болгож байна.

USSD болон STK сувгуудыг ашиглан үзүүлж буй үйлчилгээнүүдэд данс нээх, мөнгө шилжүүлэх, төлбөр тооцоо, үлдэгдэл лавлагаа авах зэрэг багтана.

Уламжлалт банкууд өөрийн агент, банкны сүлжээгээр дамжуулан USSD болон STK сувгуудаар үйлчилгээг үзүүлэх боломжтой болсон.

USSD болон STK-ийн хэрэгцээ, хэрэглээ нь дараахь зүйлээс шалтгаална.

1. Мобайл төхөөрөмж: USSD болон STK дээр суурилсан ДСҮ-ний шийдэл нь төхөөрөмжөөс хамааралгүй. Тэдгээрийг ухаалаг гар утас болон энгийн товчтой гар утсанд ашиглах боломжтой бөгөөд ингэснээр хөдөлгөөнт төхөөрөмжийг өөрчлөхгүйгээр үйлчилгээ үзүүлэх, сонголт хийх боломжийг олгоно.
2. USSD нь шуурхай, хурдан хариу үйлдэл үзүүлдэг бөгөөд дижитал санхүүгийн үйлчилгээнд нэн шаардлагатай бодит цаг хугацааны боломжийг олгодог.
3. Зардал ба үр ашиг: ДСҮ-г STK болон USSD дээр үзүүлэхэд одоо байгаа сүлжээний протоколуудыг шууд ашигладаг. ДСҮ үзүүлэгч эсвэл үүрэн холбооны оператор нь дижитал санхүүгийн үйлчилгээг нэвтрүүлэхийн тулд сүлжээнд ямар нэгэн шинэчлэлт хийх шаардлагагүйгээр аль хэдийн байгаа USSD гарцыг шууд ашиглах боломжтой.
4. Интерактив байдал: USSD болон STK нь тухай бүр холбогдсон холболт дээрээ суурилдаг бөгөөд хэрэглэгчдэд үйлчилгээ авах ойлгомжтой бүтэц цэс, өөрөө удирдах боломжийг олгодог давуу талтай.
5. USSD үйлчилгээ авах захиалагчийн хүсэлтийг үүрэн холбооны үйлчилгээ эрхлэгч нь өөрийн сүлжээгээр дамжуулдаг; Захиалагчийн ашиглах USSD үйлчилгээг роуминг хийх үед нэмэлт төлбөргүйгээр ашиглах боломжтой.
6. USSD болон STK протоколууд нь гар утасны төхөөрөмж дээр ямар ч нууц мэдээллийг хадгалдаггүй.

USSD, STK болон ДСҮ-ний хооронд үүсэх үндсэн хэрэглээ нь гүйлгээ хийх юм. Энэхүү баримт бичиг нь USSD болон STK сувгуудын сул, эмзэг талыг тодорхойлох, эрсдэл, халдлагын хувилбарууд, аюулгүй байдлын асуудлыг тайлбарлаж, халдлага нууцлалын талаарх хамгийн сайн туршлагыг санал болгоно. Үүрэн холбооны үйлчилгээ эрхлэгч, ДСҮ-ний үйлчилгээ үзүүлэгч, хэрэглэгчид хоорондын уялдаа холбоо, бүрэн бүтэн байдал, үйлчилгээний хүртээмж, нууцлал зэрэг орно.

2 USSD, STK ДСУ-НИЙ ҮНДСЭН БҮРДЭЛ БА ЭКОСИСТЕМ

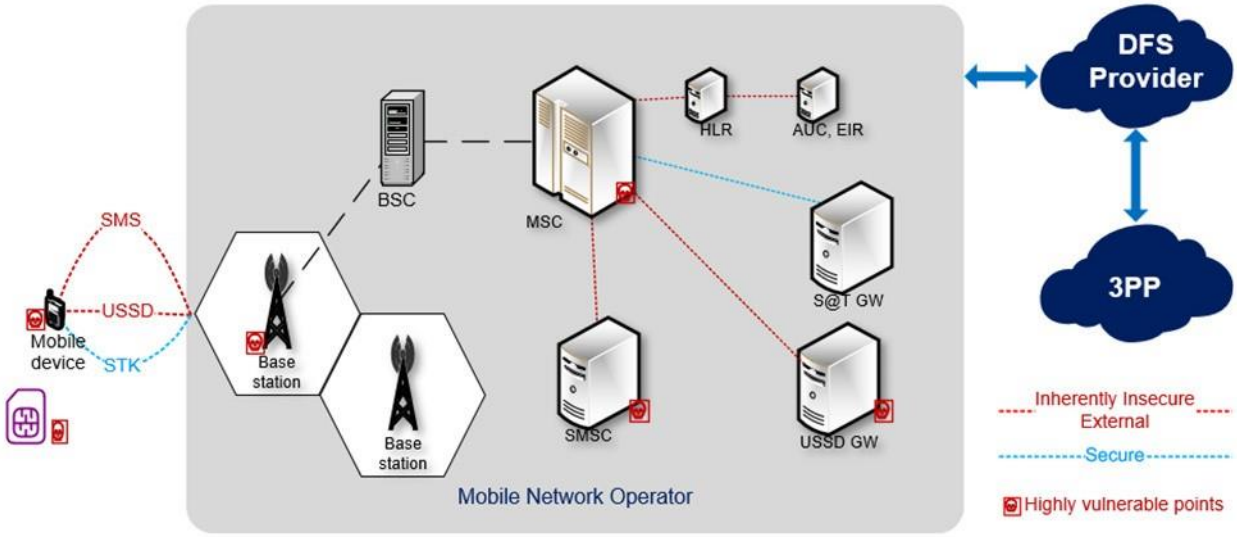
USSD болон STK дээр суурилсан ДСУ-ний экосистемд өөр өөр талуудын харилцан үйлчлэлийн цэгүүд байдаг. Иймээс/Энэ нь халдагчдад эдгээр интерфейсийг ашиглан систем рүү довтлох боломжуудыг үүсгэдэг, ~~энэ нь~~ ба оролцогч талуудад төдийгүй экосистемийн бусад хэсгүүдэд ч нөлөөлөх үр дагавартай байдаг. “Хүснэгт 2-1”-д USSD болон STK дээр суурилсан ДСУ экосистемийн чухал элементүүд, эдгээр цэгүүдийн аюул, эмзэг байдал, санал болгож буй туршилтууд болон халдлагын хувилбаруудыг харуулав.

Хүснэгт 2-1 ДСУ-ний экосистем болон бүрдэл хэсэг

Бүрэлдэхүүн хэсгүүд	USSD болон STK-тэй холбоотой аюул занал, эмзэг байдал	Туршилт/халдлагын хувилбарууд
Гар утас	• Хөдөлгөөнт төхөөрөмжид зөвшөөрөлгүй нэвтрэх / хулгайлах. • Үндсэн платформын аюулгүй байдлыг алдагдуулахын тулд төхөөрөмжид хөндлөнгөөс нөлөөлөх оролцох, жишээлбэл, хортой програм суулгах, төхөөрөмжид гаднаас чиглүүлэлт хийх. • Тагнуулын програм болгон ашиглаж болох нэмэлт техник хангамжийг байрлуулах замаар хөдөлгөөнт төхөөрөмжид шууд хөндлөнгөөс оролцох.	• Алсын зайнаас USSD гүйцэтгэх
SIM карт	• SIM солих болон SIM дахин боловсруулах • SIMJacker дайралт • SIM картанд ашигладаг сул алгоритмууд; жишээ нь, анхны Signed RES үүсгэхийн тулд SIM болон Authentication Center ашигладаг COMP128 v1 ба v2 алгоритмууд эвдэрсэн нь мэдэгдэж байна.	• SIM шалгагч ашиглан SIM тест хийх. • SIM замыг ашиглан STK тест хийх. • SIM клон тест. • IMSI болон IMEI баталгаажуулалтын тест.
Суурь станц	• Man-in-the-middle халдлага: A5/1, A5/2 гэх мэт GSM сүлжээний шифрлэлтийн алгоритмууд эмзэг болох нь батлагдсан. GSM шифрлэлтэд тулгуурласан уламжлалт сүлжээнүүд нь халдагчийн байрлуулсан хуурамч суурь станцуудын 'Man-in-the-middle' халдлагад өртөх явдал гардаг. Энэ нь өөрсдийгөө хууль ёсны үйлчилгээ үзүүлэгчийн цамхаг (жишээ нь, ихэвчлэн 'IMSI Catcher гэж нэрлэдэг хуурамч суурь станц) сүлжээнд оролцон халдлага хийдэг. • Replay attacks: Сул алгоритмууд нь халдагчдад үүрэн холбооны үйлчилгээ эрхлэгчийн сүлжээнд дахин илгээхийн өмнө шифрийг тайлах боломжийг олгодог. Ийм схем нь халдагчид гүйлгээ, санхүүгийн мэдээлэл зэрэг бүх дамжуулсан мэдээлэлд бүрэн нэвтрэх боломжийг олгоно. • Eavesdropping: A5 алгоритм Ki болон RAND утгуудыг ашиглан үүсгэсэн Kc нууц түлхүүрийг эвдэж болох ба MS болон BSS хоорондын санхүүгийн гүйлгээний дохиог чагнаж/тайлж чаддаг. • Үйлчилгээнээс татгалзах: Анхны баталгаажуулалтын үед MS руу илгээсэн RAND утгыг халдагч халдаж, өөрчилж, DFS-д үйлчилгээ үзүүлэхээс татгалзах шалтгаан болгодог.	• Хуурамч BTS ашиглан саатуулах. • MSC, USSD, SMSC зэрэг мобайл сүлжээний операторын гарц болон зангилаа цэгүүдэд ачааллын урсгалд хяналт хийх, бүртгэх.
Үндсэн сүлжээ (USSD GW, MSC, SMSC)	• SS7 протоколын сул талууд: Дотоод хяналт хангалтгүй байгаа нь хэрэглэгчийн мэдээлэлд нэвтрэх боломжийг олгодог. Үүрэн холбооны операторын үндсэн зангилаа хооронд харилцахад ашигладаг GSM MAP протокол нь тодорхой текстээр дамждаг бөгөөд энэ нь төгсгөлөөс төгсгөл хүртэл шифрлэлт байхгүйн улмаас PIN болон гүйлгээний мэдээлэл зэрэг дотоод мэдээллийг ил болгох, харах боломжийг олгодог. • Ашиглаж буй хэрэглэгчийн мэдээлэлгүй байдал, ялангуяа USSD гэх мэт мессежийн үйлчилгээний бүрэн бүтэн байдлын талаар ойлголтгүй тохиолдолд хууран мэхлэх боломжтой. • SS7 сүлжээнд нэвтрэх хялбар байдал нь халдагчид MAP (Mobile Application Part) үйлдлүүдийг ашиглан захиалагчийн өгөгдлийг оруулах, өөрчлөх, гар утасны холбоо барих, захиалагчийн байршлыг тодорхойлох боломжийг олгодог.	•

“Зураг 1” -ээр сүлжээний өөр өөр элементүүд болон дээр дурдсан халдлагад өртөж болох экосистемийн зарим эмзэг цэгүүдийг харуулав.

Зураг 1 - Сүлжээний элементүүд ба эмзэг цэгүүд



3 USSD БОЛОН STK СУУРИЛСАН ДСҮ-НИЙ ХЭРЭГЖИЛТҮҮД, ТУРШИЛТЫН ХАЛДЛАГА

USSD болон STK ашиглан хийгдсэн ДСҮ-ний гүйлгээний аюулгүй байдлыг шалгах халдлагын хувилбарууд

i. Дансны гүйлгээний эсрэг идэвхтэй болон идэвхгүй халдлага
ii. Төхөөрөмжийн баталгаажуулалтын туршилт
iii. IMSI баталгаажуулалтаар SIM солих халдлагыг турших
iv. SIM trace ашиглан STK тест хийх
v. SIM шалгагч ашиглан SIM картын аюулгүй байдлын туршилт
vi. SIM клон халдлага

3.1. ДСҮ-ний гүйлгээний эсрэг идэвхтэй, идэвхгүй халдлага

Энэхүү тестийн зорилго нь халдагч ДСҮ-ний гүйлгээний эсрэг идэвхгүй эсвэл идэвхтэй халдлага хийж чадах эсэхийг тодорхойлох явдал юм. Хоёр халдлагыг гүйцэтгэх үндсэн арга зарчим, тоног төхөөрөмж ижил боловч идэвхгүй халдлагад халдагч голчлон ДСҮ-ний гүйлгээг чагнаж/тагнах, сүлжээгээр дамжих үед мессежийг барьж, шифрийг нь тайлдаг бол идэвхтэй халдлагыг ДСҮ-ний гүйлгээнд шууд саад учруулан ДСҮ-ээр үйлчлүүлэгчийн зан үйлийг өдөөх, үйлчилгээ үзүүлэхээс татгалзах эсвэл хортой гүйлгээг дамжуулах хэлбэрээр илэрдэг.

Идэвхгүй болон идэвхтэй халдлагуудыг шалгах боломжтой түвшинд үндэслэн доор тайлбарлав.

a. GSM саатуулагч төхөөрөмжөөр дамжуулан халдагч BTS буюу үндсэн дамжуулагч станцаас өгөгдөл/пакет авах, идэвхжүүлэх, бүртгэл, мэдээллийг чагнаж/тагнах боломжийг хязгаарлах чадварыг тогтоодог.
b. Үйлчилгээ үзүүлэгчийн сүлжээн дэх логуудыг (жишээ нь, SMSC, USSD GW) барьж авах нь халдагч этгээдийн ДСҮ-ний гүйлгээг чагнах боломжийг илэрхийлдэг.

c. BTS дээрх хэрэглэгчийн хүсэлтийг өөрчлөх боломжтой байдал нь халдагчид BTS-ийг “man-in the-middle” дайралтанд ашиглах боломжтойг харуулж байна гэсэн үг юм.
d. Бусад сүлжээний дэд системийн зангилаа (жишээ нь, SMSC, USSD GW) дээрх өгөгдлийг өөрчлөх нь үйлчилгээ үзүүлэгчийн сүлжээн дэх ДСУ-ний өгөгдлийг өөрчилдөг халдагч (malicious insider or remote cyber attacker) юм.
e. Нийтийн сүлжээнд инженерчлэл хийх, DFS хэрэглэгчийн ПИН код авах зорилгоор SS7 ашиглан хуурамч USSD мессеж үүсгэх.

Мөн ДСУ-ний гүйцэтгэлийг “man-in-the-middle” халдлагад өртөмтгий эсэхийг шалгадаг бөгөөд туршилтыг дараах байдлаар хийж болно.

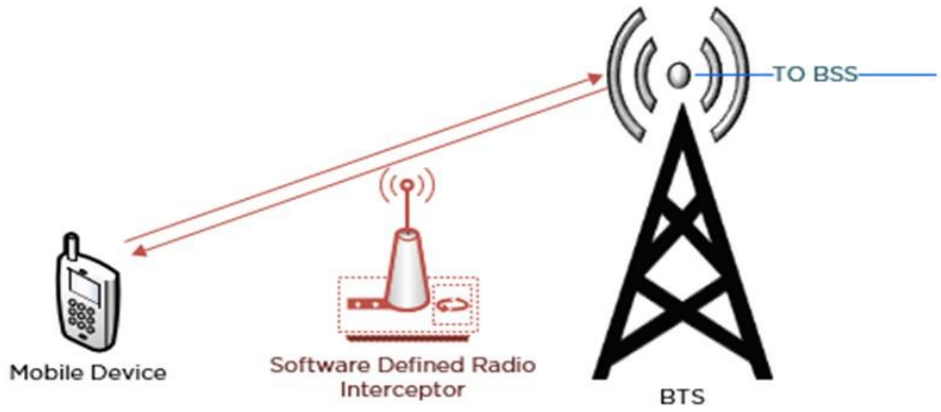
a. Програм хангамжаар тодорхойлогдсон радио (SDR) нөлөөлөл ашиглан хөдөлгөөнт төхөөрөмж болон BTS-ийг дайран өнгөрөх ДСУ-ний өгөгдлийг саатуулах.
b. GSM саатуулагч байхгүй үед үүрэн холбооны үйлчилгээ эрхлэгчийн сүлжээн дэх BTS дээрх урсгалыг авах
c. MSC, HLR, SMSC болон ДСУ-ний сервер дээрх урсгалын мэдээлэл болон бүртгэлийг авах

3.1.1. Програм хангамжаар тодорхойлогдсон радио (дохио) ашиглан ачааллын урсгалыг таслах, зогсоох

Програм хангамжаар тодорхойлогдсон радио ашиглан ачааллын урсгалыг таслан зогсоох буюу дундаас нь халдлага хийх боломжтой гэдгийг харуулж байна. Халдагч нь хэрэглэгчийн ПИН код гэх мэт ДСУ-ний гүйлгээний талаарх мэдээллийг чагнаж, мэдэж авдаг. GSM A5/1 шифрлэлтийн алгоритм сул байгаа нь мэдэгдэж байна. Хэрэв гар утасны оператор нь A5/0 шифрлэлт эсвэл сул A5/1 шифрлэлтийн алгоритмыг ашиглаагүй бол USSD үйлчилгээ болон агаараар дамжуулж буй SMS нь сааталд өртөмтгий байдаг.

Цаашилбал, хуурамч BTS-ийн үүрэг гүйцэтгэдэг SDR нь хэрэглэгчийн төхөөрөмж эсвэл хөдөлгөөнт төхөөрөмжийг шифрлэлтгүй A5/0 модем дээр ажиллуулахад хүргэдэг. Энэ тохиолдолд ДСУ ПИН кодыг хэрэглэгчээс авахын тулд нийтийн хэрэглээний сүлжээний инженерчлэлийг ашиглаж болно.
USSD алхамын үеэр ПИН, OTP, эсвэл SMS зэрэг хэрэглэгчийн ДСУ-ний гүйлгээний мэдээллийг авахын тулд SDR-г ашиглаж болно. Халдагчид мөн гүйлгээний өгөгдлийг өөрчилж, SDR ашиглан сүлжээнд дахин ачааллах боломжтой.

Зураг 2- Програм хангамжаар тодорхойлсон радио төхөөрөмж ашиглан ачааллыг саатуулах доголдуулах, таслах



3.1.2. BTS дээрх ачааллын урсгалыг булаах, барьж авах

Энэ туршилт нь халдагчид гар утасны сүлжээний үйлчилгээ үзүүлэгчийн үндсэн станцын сайт руу нэвтрэх боломжийг олгодог.

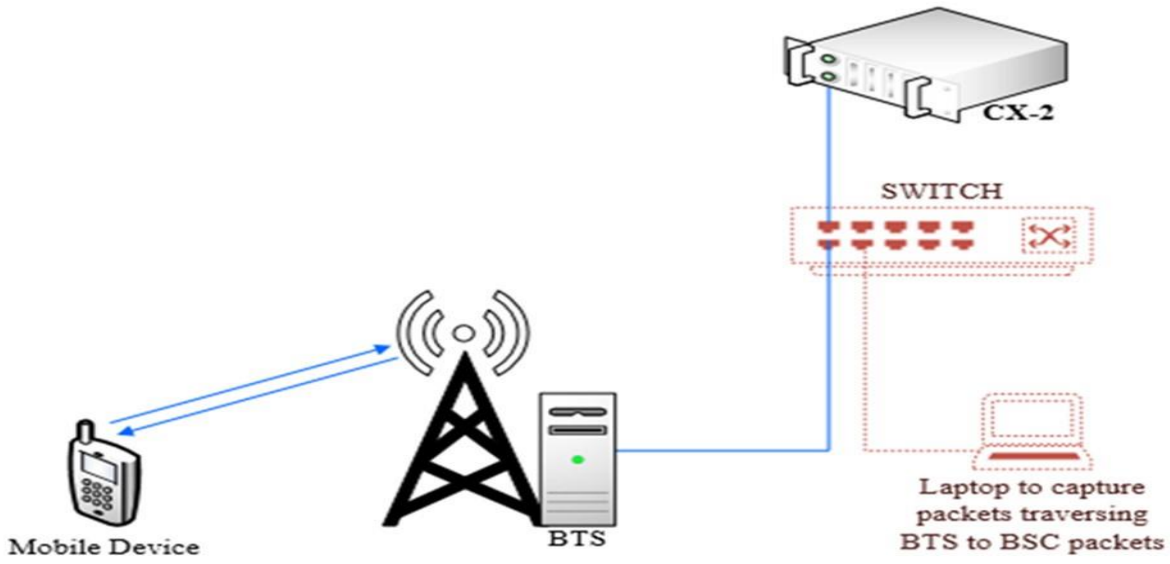
Толин тусгал хийх функц нь төхөөрөмжүүдийн пакет боловсруулах чадварт нөлөөлөхгүйгээр толин тусгалтай портууд дээрх пакетуудыг ажиглагч портууд руу хуулдаг.

Сүлжээний администраторууд төхөөрөмжид хяналт тавих, ялангуяа сүлжээний үйлчилгээ хэвийн ажиллаж байгаа эсэхийг тодорхойлохын тулд пакетуудад дүн шинжилгээ хийх замаар уг функцийг ашигладаг.

Гэсэн хэдий ч халдагч нь ДСУ-ний гүйлгээг чагнах, тагнахын тулд давуу эрхээ урвуулан ашиглаж болно. Туршилтыг BTS-ийн "Local Maintenance Terminal" (LMT) шууд багцыг авах эсвэл доорх алхмуудыг дагаж шилжүүлэгчээр дамжуулан порт толин тусгалыг тохируулах замаар хийж болно.

Туршилтыг BTS-ийн LMT - ээс шууд багцыг авах замаар хийж болно.

Зураг 3 - BTS-ийн ачааллын урсгалыг булаах, барьж авах.



a. Зураг 3-т пакетийн портод толин тусгалыг хэрхэн тохируулахыг харуулав.
b. BTS болон Universal Main Processing and Transmission Unit (UMPT) хооронд дамжуулалтыг авах.

Энэ туршилтыг хийхийн тулд үйлчилгээ үзүүлэгч нь арилжааны урсгалыг дамжуулдаггүй, бага чадалтай BTS тестийг ашиглах нь тохиромжтой.

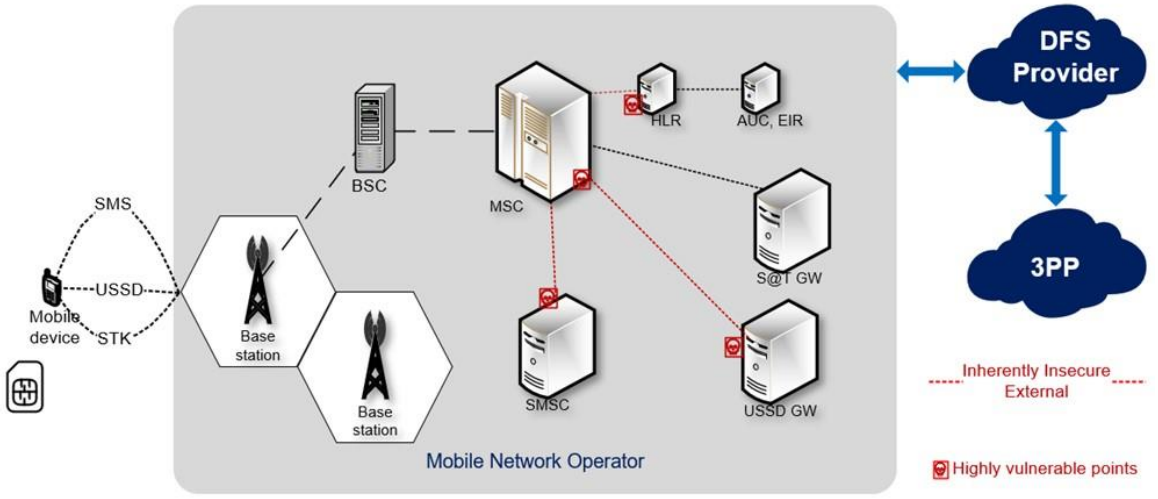
c. Дээрх 3-р зурагт үзүүлсэн шиг шилжүүлэгч нь нэг сүлжээний гурван порттой, урсгалыг тусгах нэг порттой тохируулагдана.
d. Wireshark-ийг ашигласнаар толин тусгалтай портуудын урсгалыг авдаг.
e. Таслах цэг дээр пакетуудыг барьж байхдаа USSD болон STK ДСУ-ний гүйлгээг хийнэ үү.
f. ДСУ-ний өгөгдлийг хэрэглэгчийн төхөөрөмжөөс ДСУ-ний сервер рүү найдвартай дамжуулж байгаа эсэхийг шалгахын тулд пакетуудыг Wireshark гэх мэт шинжилгээний хэрэгслүүдээр шинжилдэг.

3.1.3. MSC, HLR, SMSC, DFS сервер дээрх ачааллын урсгалыг барих, бүртгэх.

Энэхүү туршилт нь харилцаа холбоо эсвэл ДСУ үзүүлэгчийн сүлжээн дэх өгөгдлийг уншихын тулд өөр өөр сүлжээний аль ч цэг дээр дотоод эсвэл кибер кампанит ажил явуулах боломжийг харуулж байна.

Энэхүү халдлагыг алсын зайнаас засвар үйлчилгээний холболтоор дамжуулан гүйцэтгэх боломжтой. Олон операторууд үндсэн сүлжээний үйлдвэрлэгчдэд техникийн асуудлыг шийдвэрлэх боломжийг олгодог.

Зураг 4 - DFS гүйлгээг замаас нь барих



Зураг 4-т ДСУ-ний экосистем дотор өгөгдлийг дундаас нь авах, цуглуулах боломжит цэгүүдийг харуулав.

Туршилтууд нь ДСУ үзүүлэгч эсвэл харилцаа холбооны үйлчилгээ үзүүлэгч нь өөр өөр сүлжээний зангилааны хооронд ДСУ-ний өгөгдлийг найдвартай дамжуулдаг эсэхийг харуулсан.

Сүлжээний урсгалыг барих(халдаж турших)ын тулд доорх аргачлалыг дагаж мөрдөнө.

a. SIM картыг бүртгүүлээд сүлжээнд идэвхжүүлнэ.
b. SIM сүлжээнд холбогдсоны дараа SMSC, USSD GW, HLR, MSC, HLR болон ДСУ серверээс пакет авах ажиллагааг эхлүүлнэ.
c. Утсан дээр ДСУ-ний гүйлгээг хийж байхдаа үндсэн станц, SMSC, ДСУ-ний сервер дээр бүртгэлийг авна.
d. SMSC, HLR, ДСУ-ний сервер, USSD GW-ээс авсан багцаас ДСУ-ний дансны идэвхжүүлэлт, хэрэглэгчийн PIN код зэрэг гүйлгээний мэдээллийг авахын тулд бүртгэл, мөрийг шинжилнэ.

3.1.4. Идэвхгүй болон идэвхтэй довтолгоог ашиглах

Халдагч нь халдагчид илүү хүртээмжтэй байдаг фемтоцеллүүдийг эвдэж, дундын идэвхтэй дайралтуудыг хийж болно [4]. (Жижиг оврын үүрэн станц хувь хэрэгцээний)

3.2. Төхөөрөмжийн баталгаажуулалт

Энэхүү тестийн зорилго нь мобайл мөнгөний үйлчилгээнд нэвтэрч бүй гар утасны төхөөрөмжид баталгаажуулалт байгаа эсэхийг тодорхойлох явдал юм. Энэхүү шалгалт нь ДСУ-ний оператор эсвэл үүрэн холбооны оператор ашигласан төхөөрөмжийн Олон улсын хөдөлгөөнт төхөөрөмжийн таних тэмдэг (IMEI)-ийг шалгах замаар төхөөрөмжид өөрчлөлт орсон эсэхийг шалгах юм.

SIM карт нь хоёр өөр төхөөрөмж (IMEI-ээр тодорхойлогддог) ашиглан гүйлгээ хийхэд ашиглагддаг. Хэрэглэгч өөр төхөөрөмж дээр ДСУ-ний гүйлгээнд SIM карт ашиглахыг зөвшөөрөхөөс өмнө ДСУ-ний системээс нэмэлт итгэмжлэл/баталгаажуулалт шаардлагатай эсэхийг шалгах боломжтой.

3.3. IMSI итгэмжлэл ба баталгаажуулалт

ДСУ үзүүлэгчид өөрийн хэрэглэгчийг гар утасны дугаар болох гар утасны захиалагчийн нэгдсэн үйлчилгээний дижитал сүлжээний (MSISDN) дугаараар тодорхойлдог. Гэхдээ SIM солих тохиолдолд SIM карттай холбоотой IMSI (Олон улсын гар утасны захиалагчийн таних тэмдэг) өөрчлөгддөг. IMSI нэвтрэлт танилт нь SIM картыг таньж, захиалагчийг ДСУ-ний данс руугаа аюулгүй нэвтрэх боломжийг олгодог.

Энэхүү туршилтын зорилго нь ДСУ үзүүлэгч нь санхүүгийн гүйлгээ хийхээс өмнө хэрэглэгчийн SIM картыг баталгаажуулсан эсэхийг тодорхойлох явдал юм.

Хэрэв ДСУ үзүүлэгч нь IMSI ашигласан эсэхийг баталгаажуулж SIM картын баталгаажуулалтыг хэрэгжүүлбэл ДСУ-ний орчинд SIM сольсон халдагч сольсон SIM-г ашиглан гүйлгээ хийх эрхгүй болно.

Энэ тестийг хийхийн тулд хоёр гүйлгээг гүйцэтгэнэ үү: нэг нь эх SIM, нөгөө нь сольсон SIM картаар солигдсон SIM картыг ашиглахын өмнө ДСУ/мобайл оператор нэмэлт итгэмжлэл/ баталгаажуулалт шаардаж байгаа эсэхийг тодорхойлох.

3.4. Man-in-the-middle attacks on STK SIMs

Энэхүү тест нь ДСУ-ний гүйлгээний нууцлалыг SIM карт болон гар утасны хоорондох интерфейс гэдгийг харуулж байна. Osmocom SIMtrace2 [5] нь SIM-ME холболтыг хянахад ашиглагддаг. Энэхүү туршилт нь дараахь практик тохиолдлыг харуулж байна.

a) ДСУ-д ашигладаг мобайл төхөөрөмжид физик хандалттай халдагчид ДСУ-ний хэрэглэгчийн SIM карт болон утасны интерфейсийн хооронд Turbo SIM [6] гэх мэт прокси эсвэл нимгэн SIM-г оруулж, гар утасны PIN кодыг хуулбарлах боломжтой.
b) Энэхүү тест нь мөн ME болон SIM карт хоорондын холбоо шифрлэгдээгүй болохыг харуулж, нимгэн SIM-тэй холбоотой аюулыг харуулж байна.

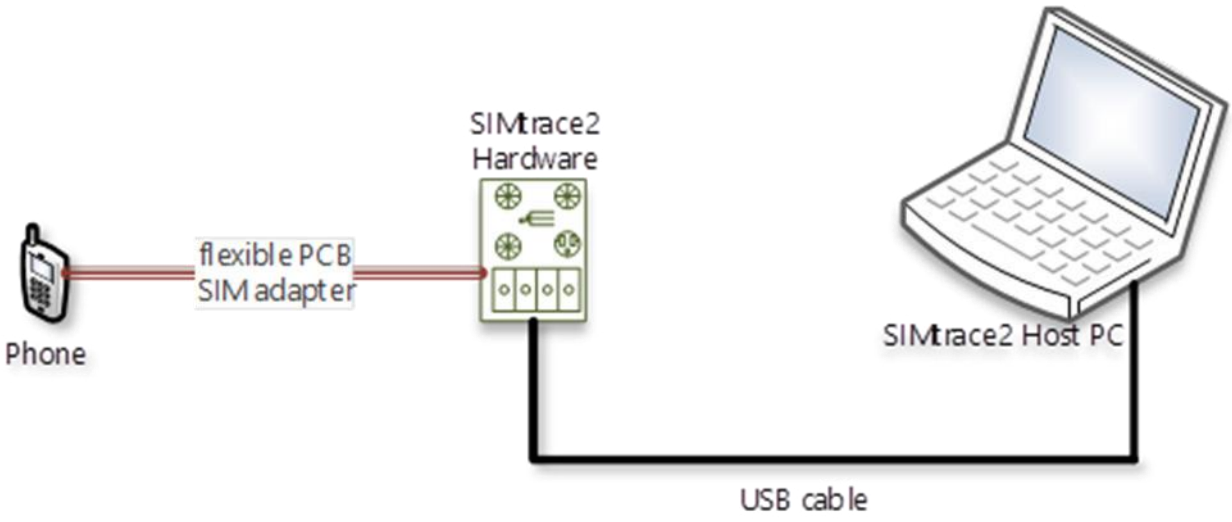
3.4.1. Туршилтын тохиргоо

Доорх диаграмм болон алхмуудыг ашиглан SIMtrace техник хангамжийг тохируулна уу.

a) SIM картыг SIMtrace тоног төхөөрөмжид байрлуулна уу.
b) Flexi-кабелийг SIMtrace төхөөрөмжид, SIM төгсгөлийг утасны залгуурт холбоно.
c) SIMtrace тоног төхөөрөмжийг USB-ээр дамжуулан хост машин руу холбоно уу .

Доорх зурагт тохиргооны схемийн дүрслэлийг харуулав.

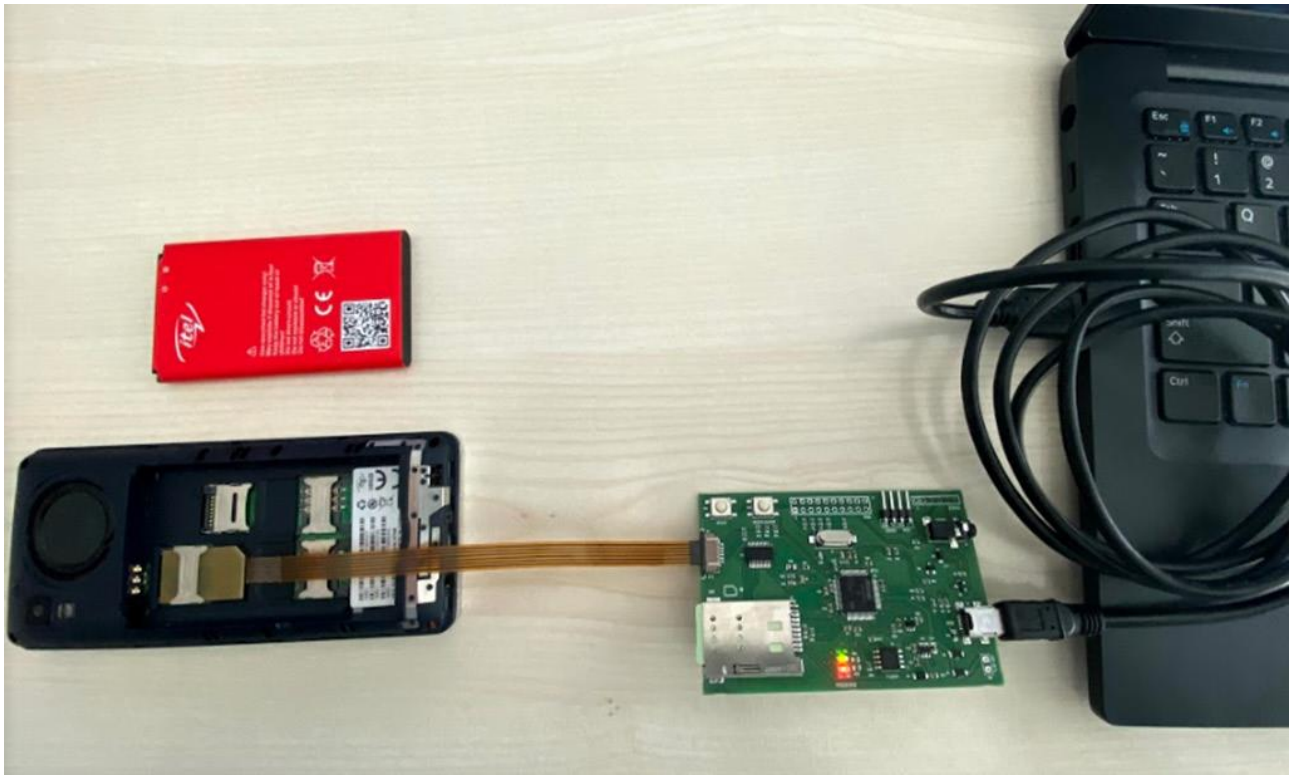
Зураг 5 – SIMtrace схемийн холболт



Доорх зураг 6-д SIMtrace төхөөрөмжийн физик тохиргоог харуулав.

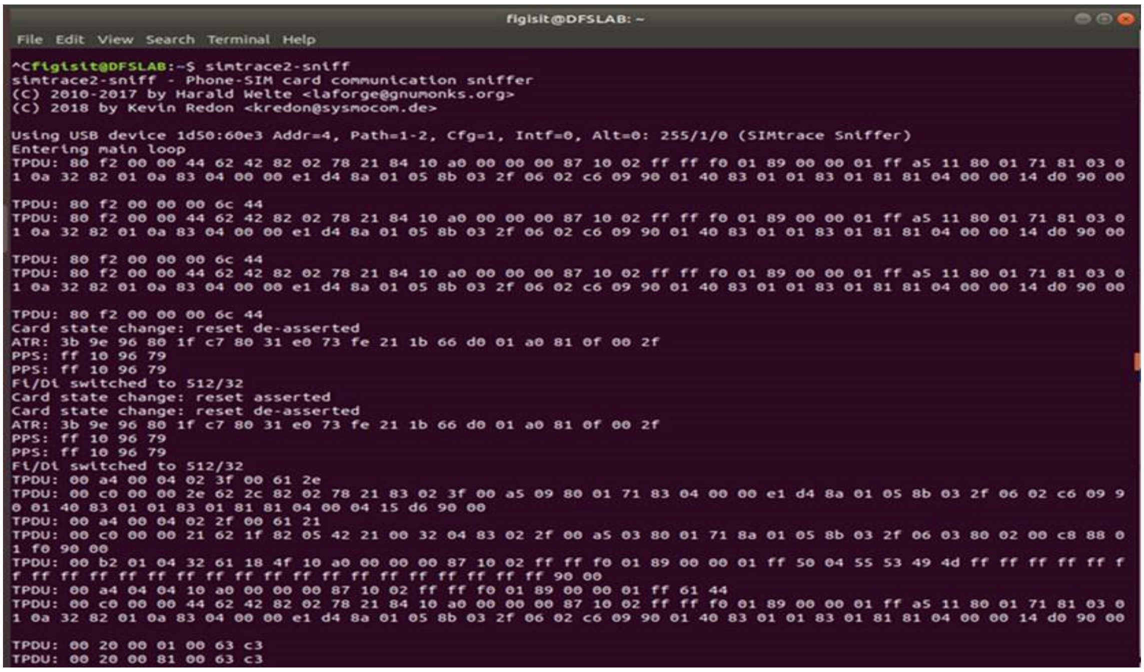
d) Wireshark-г ажиллуулаад localhost интерфейсийг сонсож эхлээрэй.
e) SIMtrace - г ажиллуулж , Wireshark ашиглан пакетуудыг барьж байхдаа STK дээр DFS гүйлгээг хийнэ үү. *$* . / simtrace
f) Пакетуудын Wireshark SIM ул мөрийг шинжилнэ үү

Зураг 6 - SIMtrace тоног төхөөрөмжийн тохиргоо

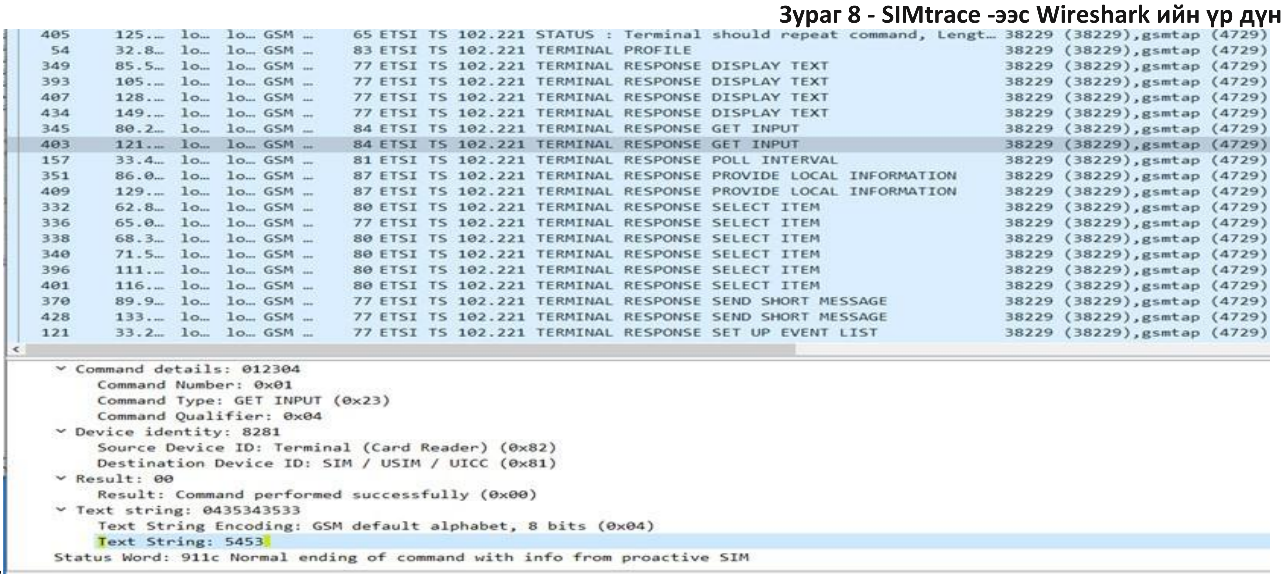


SIM карт болон ME хоорондын STK гүйлгээтэй холбоотой.

Зураг 7 - SIMtrace гаралтын жишээ



Зураг 8 - SIMtrace -ээс Wireshark ийн үр дүн



.

Энэхүү Wireshark үл мөр нь PIN кодыг SIMtrace -ээр тодорхой текстээр авсан болохыг харуулж байна. Дээрх Wireshark-ийн зураг авалт нь жишээ үр дүн бөгөөд халдагч нь PIN код болон өгөгдлийг төхөөрөмжид SIM кодоор залгах үед уншиж чаддаг болохыг харуулж байна.

3.4.2. SIM картны сул талыг ашиглах нь

Энэ туршилт нь SIM карт ашигладаг техник хангамжийн бүрэлдэхүүн хэсгүүдэд хялбар хандах боломжтой төхөөрөмжүүдтэй холбоотой эрсдэл болон нимгэн SIM-тэй холбоотой эрсдэлүүдийг харуулдаг.

Энэ халдлагыг Bladox Turbo SIM [7] ашиглан хийж болох бөгөөд үүгээр SIM болон утасны хооронд залгагдсан “Man-in-the-Middle” халдлагыг гүйцэтгэх боломжтой ба SIM-ээр дамжиж буй аливаа пакетуудыг халдагч руу дамжуулдаг.

3.5. Хоёртын OTA мессежийг ашиглан халдлага хийх[8]

Энэхүү туршилт нь SIM карт халдлагад өртөмтгий байдгийг харуулж байгаа бөгөөд энэ нь халдагч этгээдэд тусгай түшаал бүхий хоёртын OTA мессежийг эмзэг SIM рүү илгээх боломжийг олгодог. Энэхүү тест нь SIM картыг PCSC -тэй ухаалаг карт уншигчаар дамжуулан бүдгэрүүлж, SIM нь simjacker [9] эсвэл WIB халдлагад өртөмтгий эсэхийг мэдэх юм[10].

Simjacker болон WIB халдлага нь халдагчид SIM карт дээр ажилладаг SIM програмууд руу хоёртын OTA мессеж илгээж, гар утас, төхөөрөмжтэй харилцаж дараах үйлдлүүдийг хийх боломжийг олгодог.

a. *Дуудлага эхлүүлэх, SMS илгээх, SS хүсэлт илгээх.*
b. *USSD хүсэлтийг эхлүүлэх.*
c. *Тодорхой URL хаягтай интернет хөтөч ажиллуулах.*
d. *Төхөөрөмж дээрх текстийг харуулах.*
e. *Хэрэглэгчидтэй харилцах*

Simjacker халдлагын хоорондох ялгаа нь тэдний зорилтот SIM карт дээр ажиллаж байгаа програмууд байдаг. Симжакер нь S@T Browser програмаар дамжуулан тушаалуудыг гүйцэтгэдэг. Үүний эсрэгээр, WIB халдлага нь 'Wireless Internet Browser' (WIB) програмыг чиглүүлдэг. Дээрх халдлагыг SIM картанд алсаас хийх чадвар нь дижитал санхүүгийн үйлчилгээний хэрэглэгчдэд учирч болзошгүй эрсдэл юм.

"Over-the-air" (OTA) хоёртын мессежийг үйлчилгээ үзүүлэгчид SIM картыг дахин гаргах шаардлагагүйгээр SIM цэс рүү шинэчлэлт, өөрчлөлт оруулахад ашигладаг. Эцсийн хэрэглэгч нь үүрэн холбооны үйлчилгээний цэгт очих шаардлагагүйгээр SIM-дээ шинэ үйлчилгээг татаж авах эсвэл идэвхжүүлэхийн тулд оператороос хоёртын мессеж хүлээн авдаг.

STK бүхий ДСҮ-г санал болгодог үйлчилгээ үзүүлэгчид хоёртын OTA мессежийг ашиглан хэрэглэгчдээ STK програмын цэсээр дамжуулан санхүүгийн үйлчилгээний жагсаалтыг илгээдэг.

Гүйцэтгэл нь ихэвчлэн илрэхгүй буюу ихэнх тохиолдолд хэрэглэгчдэд мэдэгдэлгүй аливаа төрлийн арга хэмжээ авдаггүй.

Халдагчид энэ функцийг ашиглан хэрэглэгчийн дижитал санхүүгийн үйлчилгээнд чиглэсэн команд бүхий хоёртын SMS илгээх боломжтой.

Энэхүү тест нь SIMtester програмыг ашиглан а OTA SMS халдлагад өртөмтгий, ашиглагдах боломжтой эсэхийг шалгахын тулд үйлчилгээ үзүүлэгч нь энэ халдагчаас сэргийлэхийн тулд SIM картын хамгаалалтын функцийг идэвхжүүлсэн эсэхийг шалгадаг.

Аппликэйшн бүр нь хамгийн бага аюулгүй байдлын түвшинтэй (MSL) бөгөөд энэ нь програм руу илгээсэн хамгаалагдсан пакетуудад хэрэглэгдэх хамгийн бага аюулгүй байдлын шалгалтыг тодорхойлдог. Хоёртын командыг боловсруулахын өмнө SIM нь аюулгүй байдлын түвшинг шалгадаг бөгөөд хэрэв туршилт амжилтгүй болвол SIM нь мессежээс татгалздаг.

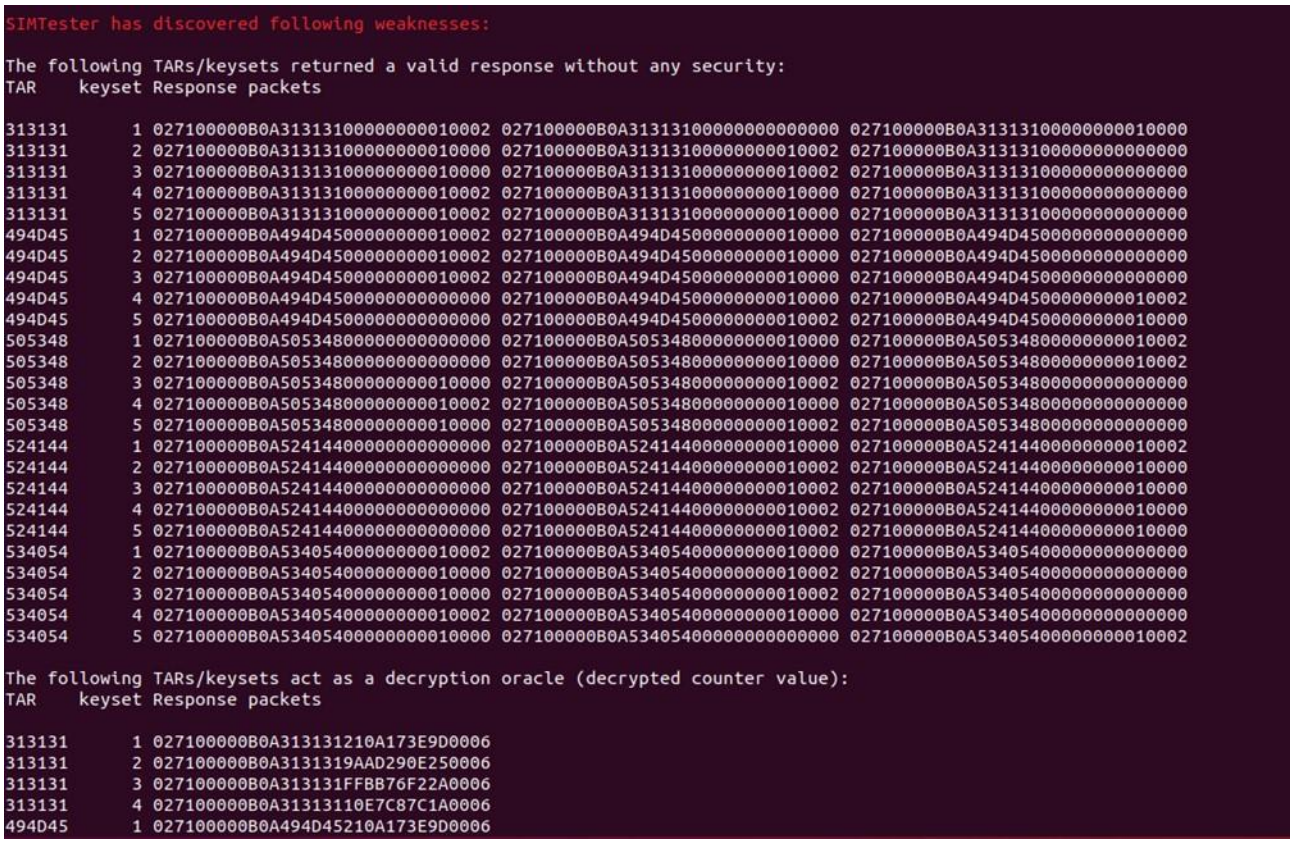
Хэрэв SIM програмыг MSL = 0-ээр тохируулсан эсвэл KiC болон KiD-г шалгаагүй бол халдагч нь OTA товчлуур болох KiC , KiD - г мэдэлгүйгээр SIM програмыг удирдах OTA SMS командыг илгээж болно. KiC нь аюулгүй командыг шифрлэхэд, KiD нь криптограф шалгах нийлбэрийг үүсгэхэд ашиглагддаг бөгөөд энэ нь түшаал нь хүчинтэй болон таних эсэхийг баталгаажуулдаг .

3.5.1. Туршилтын тохиргоо

Туршилтыг хийхийн тулд SIMtester програмын файлыг задлаад доорх командыг ажиллуулна уу.

$ SIMTester_v1.9.zip задлах
$ java -jar SIMTester.jar

Түлхүүр багцгүйгээр OTA SMS командуудад мэдрэмтгий эсэхийг шалгахын тулд хэрэглүүрийн лавлагаа (TARs) болгонд мессеж илгээх замаар програм ажиллуулдаг.
Үр дүнгийн гаралт нь SIM карт эмзэг эсэхийг харуулах болно.



Зураг 9 - Эмзэг SIM-ээс SIMtester гаралт

3.5.2. Симжакерын эмзэг байдлыг ашиглах

Дараах гурван нөхцөл нь симжакерын эмзэг байдлыг ашиглах боломжийг олгоно.

a. SMS төв нь хоёртын мессежийг хүлээн авч, дамжуулдаг
b. Зорилтот төхөөрөмжийн (U)SIM Application Toolkit командуудыг агуулсан хоёртын SMS мессеж хүлээн авах чадвар.
c. SIM карт дээр суурилуулсан S@T Browser технологи нь аюулгүй байдлын доод түвшинг "Аюулгүй байдал-0" гэж тохируулсан.

3.6. ADB ашиглан төхөөрөмж дээр алсын USSD гүйцэтгэл

Энэхүү туршилтын зорилго нь алсын халдлага үйлдэгч нь төхөөрөмж дээр үндэслэн USSD ашиглан ДСҮ-ний гүйлгээг гүйцэтгэх чадварыг харуулах явдал юм.

Энэ туршилтыг “Android Debug Bridge” ADB платформын хэрэгслүүд [11] суулгасан компьютер ашиглан гүйцэтгэдэг. Rooted android төхөөрөмж нь USB кабелиар дамжуулан компьютерт холбогдсон байна.

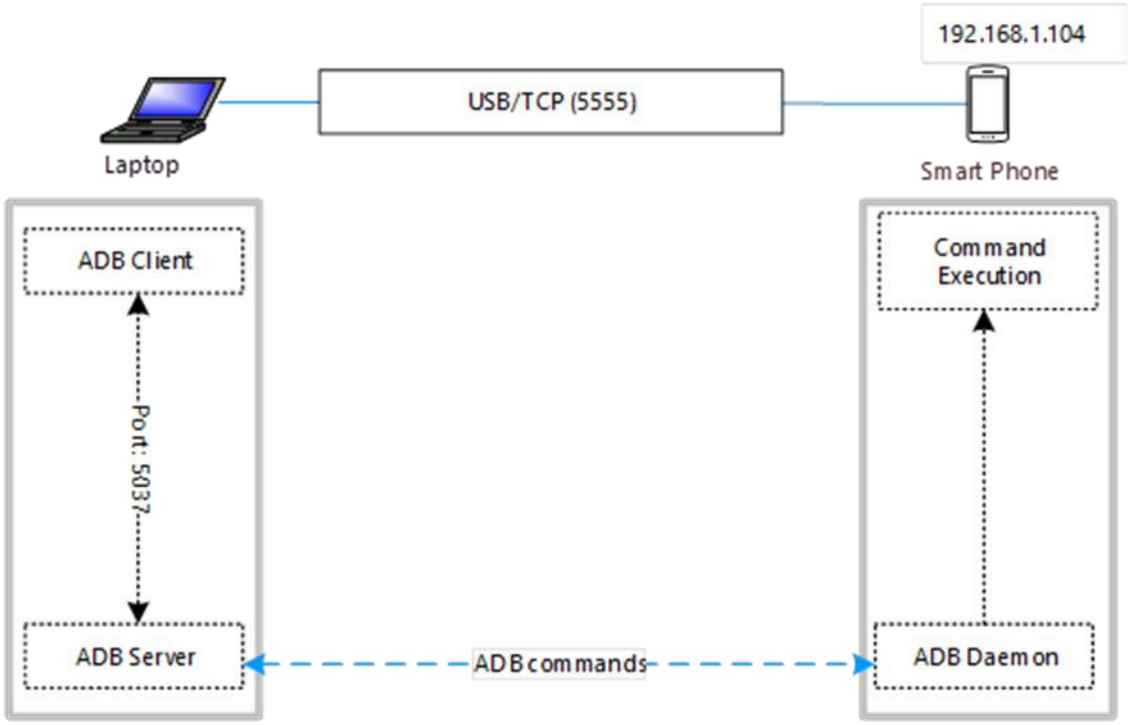
Туршилт нь хөдөлгөөнт төхөөрөмж болон хост машиныг ижил Wi-Fi сүлжээний цэгт холбосон байхыг шаарддаг.

Дараах заавар нь туршилтын тохиргооны талаарх мэдээллийг харуулсан.

a) Мобайл төхөөрөмжийн IP хаягийн командыг гүйцэтгэх замаар хост машин дээр тодорхойлно.

./ adb shell ifconfig wlan0 хөдөлгөөнт төхөөрөмж IP жагсаалтад 192.168.1.104 гэж харуулав

Зураг 10 - АХБ-ны холболтын схемийн тохиргоо

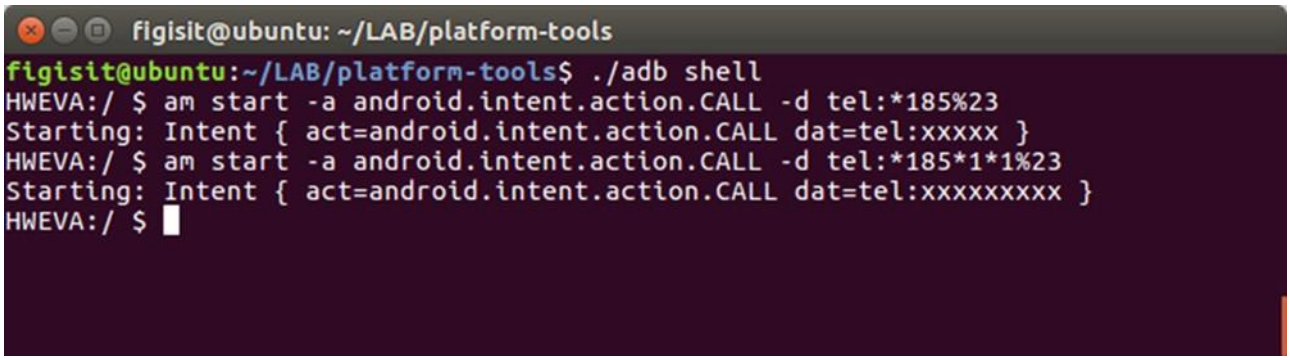


b) Доорх командыг ашиглан мобайл төхөөрөмжид IP хаягаар нь холбогдоно уу
./ adb connect 192.168.1.104

c) Энэ командыг ашиглан хост компьютер Wi-Fi-аар дамжуулан зорилтот төхөөрөмжид холбогдсон эсэхийг баталгаажуулна уу.
./ adb төхөөрөмжүүд

d) USB-г салгасны дараа компьютерийн бүрхүүл дээр ажилладаг доорх командуудыг ашиглан гар утасны USSD командын гүйцэтгэлийг төхөөрөмжид алсаас шалгана уу. *./ adb бүрхүүл am start -a android.intent .action.CALL -d ymac :* 185*1*1%23*

Зураг 11 - АХБ бүрхүүл ашиглан алсын USSD команд

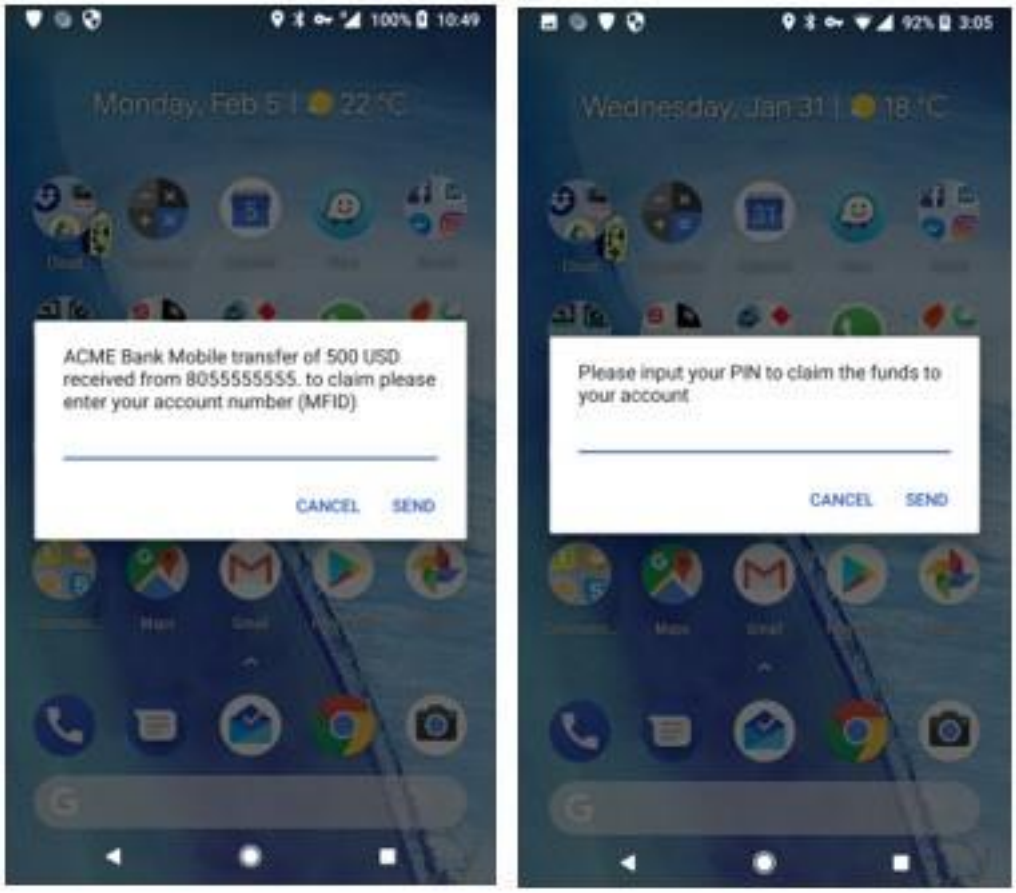


Энэхүү туршилт нь төхөөрөмжид нэвтэрсэн халдлага үйлдэгч нь алсын зайнаас USSD команд өгч, ДСУ-ний гүйлгээг хийж болохыг харуулж байна.

3.7. SS7 ашиглан алсаас USSD гүйцэтгэх

USSD мессеж хүлээн авах үед хэрэглэгчдийн итгэл үнэмшил, эргэлзэлгүй итгэх байдалд үндэслэн халдлагыг гүйцэтгэх, өргөжүүлэх болон хамгийн энгийн USSD ашиглан санхүүгийн үйлчилгээ үзүүлэгчийн хувийн мэдээллийг авах, хэрэглэгчийн дансны дугаар, ПИН код гэх мэт нууц мэдээллийг цуглуулах, задруулах хуурамч мессеж илгээх явдал юм.

Зураг 12 - USSD ашиглан хэрэглэгчийг итгүүлэх



SS7 сүлжээнд нэвтрэх эрхтэй халдагч ямар ч сүлжээнд USSD мессеж илгээх боломжтой. USSD мессежэнд таних тэмдэг байхгүй бөгөөд хэрэглэгч сүлжээнээс эдгээр мессежийг хүлээн авахад дассан тул итгэл үнэмшилтэйгээр өөрийн дансны дугаар болон ПИН-код зэргийн нууцлалаа задалдаг. Үүнийг нь ашиглан халдагчид данс руу нь нэвтэрч гадагшаа чиглэсэн шилжүүлгийг хийдэг.

3.8. SIM клон халдлага

Энэхүү туршилтын зорилго нь SIM картыг хуулбарлаж чадах халдагчид үйлчилгээнд хуулбарласан SIM картыг амжилттай баталгаажуулж, хуурамч гүйлгээ хийж чадах эсэхийг үнэлэх явдал юм. Энэ халдлага нь зөвхөн хуучирсан COMP128v1 алгоритмыг дэмждэг SIM картууд дээр байж болно .

SIM клончлолыг нээлттэй эх сурвалжийн pySIM [12] ашиглан загварчилж болно .

4. USSD болон STK-ийн аюулыг саармагжуулах туршлагууд

Энэ хэсэгт DFS үйлчилгээ үзүүлэгчид болон үүрэн холбооны операторууд USSD болон STK дээр суурилсан ДСУ-ний хэрэгжүүлэлтүүдэд аюул, халдлагаас урьдчилан сэргийлэхийн тулд ашиглаж болох шилдэг туршлагуудыг тоймлон харуулав.

4.1. Хэрэглэгчийн мэдээллийг татаж авахаас сэргийлэх туршлагууд

i. SMSC GW, USSD GW болон ДСУ програмын сервер хоорондын холболтыг хамгаалахын тулд TLS v1.2 буюу түүнээс дээш хувилбарыг ашиглана уу.
ii. Үүрэн холбооны оператор нь хэрэглэгчдийн төхөөрөмж болон үндсэн станцуудын хооронд аюулгүй радио шифрлэлтийн хэрэглээг хангах ёстой.
iii. Өөрчлөгдсөн хүсэлт/хариултыг хязгаарлахын тулд үйлчлүүлэгчийн тал дээр сессийн завсарлагыг ашиглана уу.
iv. Боломжтой бол USSD PIN маскыг байрлуул.
v. USSD мессежийг шифрлэх (мөн дараа нь УХУЭ талд шифрлэлтийг тайлах) замаар гар утасны төлбөрийг аюулгүй байлгах технологийн зааварчилгааг дагаж мөрдөөрэй. Бага гүйцэтгэлтэй шинэ

шаардлага гарч ирснээр квант тооцоололд тэсвэртэй шифрлэлтийн схемүүд гарч ирсэн. USSD -ийн төгсгөлийн шифрлэлт нь одоо байгаа 2G сүлжээнүүдэд ч боломжтой болж байна. Дохионы шаардлага, протокол, туршилтын үзүүлэлтүүдэд анхаарлаа хандуулдаг ITU-T судалгааны бүлэг 11 одоогоор эдгээр технологиудыг судалж, USSD дохиололд нэгтгэх програмуудыг санал болгох техникийн тайлан *(03/2021 онд хэвлэгдэх)* дээр ажиллаж байна. үндсэн сүлжээний тал ба хэрэглэгчийн төхөөрөмж *(SIM карт дотор).*

vi. Аюулгүй протокол ашигладаг интерфэйс дээрх ул мөр, бүртгэлд хандах хандалтыг шалгах аудитын процесс байгаа эсэхийг шалгаарай.

vii. Санхүүгийн гүйлгээ, ялангуяа програм ашиглан ДСҮ-д хандах боломжтой USSD эсвэл STK сувгуудаас татгалзах сонголтыг үйлчлүүлэгчдэд санууллаарай.

viii. Хэрэглэгчийн USSD сувгаар мөнгө авах, шилжүүлэхэд шаардагдах гүйлгээний хязгаарыг үйлчлүүлэгч тус бүрээр тохируулна уу.

4.2. SIM солих болон SIM дахин боловсруулах эрсдлийг бууруулах туршлага [13]

i. Төхөөрөмжийн баталгаажуулалт нь гар утасны мөнгө рүү нэвтрэхэд ашигладаг төхөөрөмжүүдийн IMEI-г хянах замаар эцсийн цэгийн аюулгүй байдлыг сайжруулах нэг арга юм. Ийм байдлаар төхөөрөмжийг өөрчилдөг бүртгэлийг онцлох явдал юм.

ii. Хэрэглэгчийн таних, баталгаажуулахдаа өөрт байгаа тухайн хүнийг таних бүх хувилбарыг ашиглах, баталгаажуулах ёстой. Жишээлбэл, SIM солихоос өмнө хүчинтэй ID, биометрийн баталгаажуулалт, ДСҮ-ний дэлгэрэнгүй мэдээллийг ашиглах боломжтой.

iii. ДСҮ болон төлбөрийн үйлчилгээ үзүүлэгч нь ДСҮ бүхий SIM карт солих эсвэл солигдсон тохиолдолд илрүүлэх боломжтой байх ёстой. Мөн шинэ SIM-ээр өндөр дүнтэй гүйлгээ хийх эсвэл дансны өөрчлөлтийг хүлээн зөвшөөрөхөөс өмнө нэмэлт баталгаажуулалт хийнэ үү.

iv. Үүрэн холбооны үйлчилгээ эрхлэгч нь гар утасны дугаарыг дахин боловсруулах үйл явцыг зохион байгуулах ёстой бөгөөд үүнд ДСҮ үзүүлэгчид гацсан эсвэл дахин боловсруулсан Гар утасны захиалагчийн таних дугаар (MSIDN) дээр холбогдох хэрэгтэй. (Энэ хүрээнд: дугаарын дахин боловсруулалт гэдэг нь ДСҮ дээрх идэвхитэй/идэвхгүй байгаа гар утасны захиалагчийн таних дугаарыг (MSISDN) шинэ хэрэглэгч рүү дахин хуваарилах явдал юм). SIM картыг дахин боловсруулах үед гар утасны оператор данс, утасны дугаартай холбоотой шинэ IMSI-г ДСҮ үзүүлэгчид мэдэгдэх, ДСҮ үзүүлэгч нь SIM картыг эзэмшиж буй шинэ хүний данс эзэмшигч болохыг баталгаажуулах хүртлээ дансыг хязгаарлах ёстой.

v. Мобайл оператор нь IMSI болон SIM-н нууц түлхүүрийн утгууд (KI утгууд) гэх мэт SIM өгөгдлийг хамгаалж, найдвартай хадгалах ёстой.

4.3. Төхөөрөмж дээр алсын зайнаас USSD ажиллуулахгүй байх туршлага

i. Андройд төхөөрөмж эзэмшигчид ADB-н интерфэйсийг идэвхгүй болгох ёстой бөгөөд төхөөрөмжийн борлуулагчид сүлжээгээр дамжуулан Android дибаг хийх гүүрийг идэвхжүүлсэн бүтээгдэхүүнийг дамжуулж болохгүй.

ii. DFS-ийн хэрэглэгчид нийтийн Wi-Fi сүлжээнд холбогдохын аюул болон програмын зөвшөөрөлтэй холбоотой эрсдлийг хэрхэн зохицуулах талаар мэдлэгтэй байх ёстой. Ялангуяа DFS хэрэглэгчид төхөөрөмж дээрх аппликейшнд зөвшөөрөл олгохдоо нууцлалын нөлөөллийн талаар мэдэж байх ёстой. Хэрэв зөвшөөрөл нь хэтэрхий халдан түрэмгийлэх шинжийг агуулсан, эрсдэлтэй байвал програмыг татаж авахаас зайлсхийх хэрэгтэй.

iii. ДСҮ-ний гүйлгээнд үндэслэгдсэн төхөөрөмж ашиглахаас зайлсхийж, төхөөрөмжийн программ хангамжийг байнга шинэчилж байх хэрэгтэй. Тогтмол шинэчлэлтүүд нь төхөөрөмжийг хортой програм болон чагнах, тагнах програмаас хамгаалдаг.

4.4. Хоёртын OTA ашиглан SIM-н ашиглалтыг багасгах туршлага

i. SMS шүүлтүүр: Алсын халдагчид хохирогчийн утас руу хоёртын мессежийг хүргэхийн тулд гар утасны сүлжээг ашигладаг. Мобайл операторууд OTA SMS гэх мэт хоёртын мессеж илгээх, хүлээн авах боломжийг хаах хэрэгтэй. Ийм мессежийг зөвхөн зөвшөөрөгдсөн жагсаалтад орсон эх сурвалжаас авахыг зөвшөөрөх ёстой.

ii. Үндсэн захиалагчдын STK кодтой OTA мессежийг бусад захиалагчдад биш, зөвхөн үүрэн холбооны үйлчилгээ эрхлэгчийн платформ руу илгээхээр хязгаарлах ёстой.
iii. Контент нийлүүлэгчид ерөнхийдөө A2P SMS мессеж хэлбэрээр текст илгээдэг. Тэдний траффик нь STK кодтой мессеж агуулах ёсгүй
iv. SMS гэрийн чиглүүлэлт: Энэ нь гэрийн сүлжээний хостуудаар дамжсанаас бусад бүх чиглэлийн SMS-г хориглох явдал юм.

Төгсгөлийн тайлбарууд

1. https://www.gsma.com/r/wp-content/uploads/2019/05/GSMA-State-of-the-Industry-Report-on-Mobile-Money-2018-1.pdf
2. https://www.zdnet.com/article/gsm-a51-encryption-cracked-but-theres-no-need-to-panic/
3. https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers
4. http://www.cs.ru.nl/~fabianbr/pub/thesis_fabian_vd_broek.pdf
5. https://osmocom.org/projects/simtrace2/wiki
6. https://en.wikipedia.org/wiki/Turbo_SIM
7. https://www.bladox.com/
8. https://opensource.srlabs.de/projects/simtester/wiki#TAR-Scanner
9. https://simjacker.com/downloads/technicalpapers/AdaptiveMobile_Security_Simjacker_Technical_Paper.pdf
10. 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/
11. https://www.xda-developers.com/quickly-install-adb/
12. https://github.com/osmocom/pysim
13. https://www.issms2fasecure.com/assets/sim_swaps-04-16-2020.pdf

International Telecommunication Union
Place des Nations
CH-1211 Geneva 20
Switzerland