INSTYTUT ŁĄCZNOŚCI
PAŃSTWOWY INSTYTUT BADAWCZY

Zakład Analiz i Rozwoju Rynku ICT (Z-2)

Analiza zmierzająca do wypracowania możliwych rozwiązań technicznych i prawnych umożliwiających wyeliminowanie/ograniczenie negatywnych zjawisk takich jak np. zjawisko simboxingu (nadużycia telekomunikacyjne)

Wersja 4

Nr zadania 02.10.1.04.06.6

Warszawa - Miedzeszyn

grudzień 2016 r.

Spis treści

1. PODSTAWY PRAWNE I MERYTORYCZNE OPRACOWANIA 7
1.1 PRZEDMIOT I PODSTAWA REALIZACJI PRACY 7
1.2 CEL PRACY 7
1.3 MATERIAŁY ŹRÓDŁOWE I SPOSÓB REALIZACJI PRACY 7
2. WSTĘP 9
2.1 WPROWADZENIE 9
2.2 DEFINICJE 10
3. SIMBOXING ORAZ INNE NADUŻYCIA TELEKOMUNIKACYJNE 12
3.1 SKALA ZJAWISKA SIMBOXINGU 12
3.2 MECHANIZM DZIAŁANIA SIMBOXINGU 13
3.3 NADUŻYCIA TELEKOMUNIKACYJNE POWIĄZANE Z SIMBOXINGIEM 14
3.3.1 GENEROWANIE SZTUCZNEGO RUCHU ATG (ANG. ARTIFICIAL TRAFFIC GENERATING) 14
3.3.2 NIEUPRAWNIONE WYKORZYSTYWANIE PŁASKICH STAWEK INTERKONEKTOWYCH PSI 14
3.3.3 WYKORZYSTYWANIE ZRÓŻNICOWANYCH STAWEK MTR W POŁĄCZENIACH WEWNĄTRZ UE I SPOZA UE 14
3.3.4 GENEROWANIE POŁĄCZEŃ NA NUMERY ZAGRANICZNE IRSF (ANG. INTERNATIONAL REVENUE SHARE FRAUD) 15
3.3.5 WYKORZYSTYWANIE ABONAMENTU TYPU NO LIMIT W INTERNECIE DO GENEROWANIA RUCHU NA ŁĄCZA MIĘDZYSIECIOWE 15
3.3.6 KLONOWANIE KART SIM I NUMERU IMEI 16
3.3.7 WŁAMANIA DO CENTRAL PBX I VPBA (PBX HACKING) 16
3.4 INNE NADUŻYCIA TELEKOMUNIKACYJNE 16
3.4.1 WYŁUDZANIE POPRZEZ SMS KODÓW DOŁADOWUJĄCYCH KARTY PRE-PAID 16
3.4.2 KOLPORTOWANIE WIRUSÓW W SIECIACH KOMÓRKOWYCH W CELU WYŁUDZENIA DANYCH, WYSYŁANIA SMS POZA KONTROLĄ UŻYTKOWNIKA, SZYFROWANIA DANYCH UŻYTKOWNIKA ORAZ SZANTAŻOWANIA (MALWARE) 16
3.4.3 WPROWADZANIE W BŁĄD ABONENTA/UŻYTKOWNIKA W CELU AKCEPTACJI PRZEZ NIEGO SUBSKRYPCJI MT (PREMIUM SMS MOBILE TERMINATED) 17
3.4.4 URUCHOMIENIE SUBSKRYPCJI MT (PREMIUM SMS MOBILE TERMINATED) ZA POMOCĄ APLIKACJI Z NIEZAUFANEGO ŹRÓDŁA 17
3.4.5 WYSYŁANIE SMS WPROWADZAJĄCYCH W BŁĄD UŻYTKOWNIKA W CELU UZYSKANIA KORZYŚCI 17

3.4.6 Prowokowanie oddzwaniania na drogie numery po rozłączeniu połączenia po jednym nieodebranym dzwonku (jap. wangiri fraud, ang. one ring one cut) 18
3.4.7 Aktywacja usługi na fałszywe lub cudze dokumenty w celu wyłudzenia sprzętu lub usług 18
3.4.8 Podmiana kont bankowych na fakturach 18
3.4.9 Podszywanie się pod dowolny numer telefoniczny za pośrednictwem portali internetowych 18
3.4.10 Kierowanie ruchu okrężną drogą z uwagi na spłaszczanie stawek w Europie do stawek jak w ruchu krajowym 19
3.4.11 Nadpisywanie numeru/adresu strony A w wiadomościach SMS 19
3.4.12 Nieuczciwa konkurencja 20
3.5 Scenariusze realizacji połączeń w przypadku simboxingu 20
3.5.1 Scenariusz realizacji połączeń obejściowych z wykorzystaniem Internetu 20
3.5.2 Scenariusz wydzwaniania na własne numery wykorzystujący asymetrię stawek MTR 23
4. Simboxing w sieci operatorów krajowych 24
4.1 Skala zjawiska simboxingu w sieci krajowej 24
4.2 Przypadki nadużyć związanych z simboxingiem potwierdzone przez operatorów 25
4.3 Sposoby działania sprawców nadużyć zidentyfikowane przez operatorów 29
4.4 Przypadek simboxingu w sieci operatora Orange Polska 30
4.4.1 Sposób rozliczania ruchu wg płaskiej stawki interkonektowej 30
4.4.2 Nadużycia spowodowane zakańczaniem połączeń międzynarodowych jako połączeń krajowych wg stawki PSI 31
4.4.3 Przypadek nadużyć ze strony operatorów grupy kapitałowej Polish Servies Group S.A przy tranzycie połączeń międzynarodowych 31
4.4.4 Działania podjęte przez operatora Orange Polska w celu zwalczania nadużyć 33
5. Przegląd działań instytucji krajowych poświęconych zwalczaniu simboxingu 34
5.1 Wprowadzenie ustawowego obowiązku rejestracji przedpłaconych kart SIM 34
5.2 Propozycje regulacji zgłoszonych przez Prezesa UKE 34
5.3 Propozycje PIIT w zakresie zmian prawnych zgłoszonych przez Prezesa UKE 36
5.3.1 Zagrożenia wynikające z nadużyć telekomunikacyjnych wskazane przez Izbę 36
5.3.2 Propozycje uszczegółowienia definicji nadużyć 37
5.3.3 Propozycje korekty założeń 39

5.3.4 Dodatkowe kwestie zgłoszone przez Izbę 39
5.4 Podsumowanie propozycji UKE i PIIT 40
6. Simboxy oraz systemy służące do wykrywania zjawiska simboxingu 42
6.1 Simboxy - urządzenia służące do realizacji simboxingu 42
6.2 Systemy służące do wykrywania simboxingu 43
6.2.1 Procedury i wspomagające zwalczanie simboxingu 43
7. Wnioski z przeglądu regulaminów świadczenia usług pod kątem identyfikacji niedozwolonych praktyk 48
8. Wnioski i propozycje działań naprawczych 49
8.1 Diagnoza 49
8.2 Propozycje działań zapobiegawczych zgłaszane przez operatorów 49
8.3 Proponowane kierunki działań dla ograniczenia nadużyć telekomunikacyjnych 51
8.3.1 Działania w zakresie przestrzegania warunków technicznych 51
8.3.2 Zwiększenie ochrony niezmienności numeru A na całej drodze połączeniowej 51
8.3.3 Działania w zakresie karania 52
8.3.4 Działania w zakresie zmiany stawek międzyoperatorskich rozliczeniowych 52
8.3.5 Propozycja zakresu modyfikacji ofert/regulaminów dostawców usług pod kątem ograniczenia nadużyć. 52
8.4 Propozycja systemu do badania niezmienności numeru abonenta A 53
8.4.1 Założenia ogólne 53
8.4.2 Założenia dotyczące scenariuszy zestawiania połączeń 53
8.4.3 Uwarunkowania implementacji systemu 54
8.5 Propozycje dalszych prac 55
9. Analiza ryzyka 57
10. Analiza SWOT 60
11. Wykaz literatury 61
12. Załącznik 1 - Przegląd metod i systemów do wykrywania simboxingu 63
12.1 Podejścia do detekcji nadużyć 63
12.2 Metody wykrywania oszustw 63
12.3 Detekcja fraudów w połączeniach międzynarodowych przy użyciu logiki rozmytej 64
12.3.1 Istota logiki rozmytej 64

12.3.2 Zasady logiki rozmytej 65
12.3.3 Wykorzystanie techniki rozmytej do wykrywania nadużyć 66
12.3.4 Wnioski 68
12.4 System Keynote SIGOS testowania parametrów QoS 68
12.5 System anty-fraudowy OCELUS 68
12.6 Optimus Fraud Management Solution (FMS) 69
12.7 System ZIRA N2B SIM BOX Detection 69
12.8 System FMSevolution firmy XINTEC 71
13. Załącznik 2 - Przegląd systemów do realizacji simboxingu 72
13.1 System firmy ANTRAX 72
13.1.1 Zastosowanie 72
13.1.2 Elementy składowe systemu 72
13.1.3 Architektura systemu 73
13.1.4 Funkcje maskujące 73
13.1.5 „Dobre praktyki" zakańczania połączeń w sieci GSM – porady producenta systemu 73
13.2 System Dinstar SIM Cloud 75
13.2.1 Charakterystyka ogólna 75
13.2.2 Public SIM Cloud 76
13.2.3 Lokalny serwer SIM 77
13.2.4 Funkcje systemu zarządzania SIM Cloud 77
13.2.5 Elementy i funkcje systemu 77
13.2.6 Główne cechy SIMbank 78
13.3 System firmy TOPEX S.A. 79
13.3.1 SIMServer 79
14. Załącznik 3 – Przykłady działań organizacji i podmiotów międzynarodowych 81
14.1 Przykłady działań wybranych zagranicznych administracji i organów regulacyjnych ... 81
14.2 Referencje CEPT 81
14.3 Rekomendacje Europejskiego Instytutu Standardów Telekomunikacyjnych ETSI 81
14.4 Rekomendacje ITU 82
14.4.1 Aspekty regulacyjne dostarczania numeru abonenta A w związku z nadużyciami w opinii ITU 83

14.4.2 PROPOZYCJE OPERATORÓW DOTYCZĄCE ROZWIĄZYWANIA KWESTII SPORNYCH ZWIĄZANYCH Z NADUŻYCIAMI TELEKOMUNIKACYJNYMI I3FORUM 83

15. ZAŁĄCZNIK 4 – PRZEGLĄD REGULAMINÓW ŚWIADCZENIA USŁUG TELEKOMUNIKACYJNYCH POD KĄTEM ZAPISÓW ZAPOBIEGAJĄCYCH ZJAWISKU SIMBOXINGU 85

15.1.1 POLKOMTEL SP. Z O.O – WYCIĄG Z UMOWY I REGULAMINÓW ŚWIADCZENIA USŁUG TELEKOMUNIKACYJNYCH NA ABONAMENT I NA KARTĘ.....85

15.1.2 ORANGE POLSKA – WYCIĄG Z REGULAMINÓW ŚWIADCZENIA USŁUG NA ABONAMENT I NA KARTĘ.....87

15.1.3 P4 SP. Z O.O. – WYCIĄG Z UMOWY I REGULAMINÓW ŚWIADCZENIA USŁUG DLA ABONENTÓW I UŻYTKOWNIKÓW 88

15.1.4 T-MOBILE – WYCIĄG Z UMOWY I REGULAMINÓW ŚWIADCZENIA USŁUG NA RZECZ ABONAMENTÓW I NA KARTĘ 90

15.1.5 VIRGIN MOBILE POLSKA SP. Z O.O. – WYCIĄG A REGULAMINU ŚWIADCZENIA USŁUG 92

1. Podstawy prawne i merytoryczne opracowania

1.1 Przedmiot i podstawa realizacji pracy

Przedmiotem pracy jest przeprowadzenie analizy zmierzającej do wypracowania możliwych rozwiązań technicznych i prawnych umożliwiających wyeliminowanie lub ograniczenie nadużyć telekomunikacyjnych, takich jak np. zjawisko simboxingu.

Podstawą realizacji pracy jest umowa dotacji celowej nr 1/DT zawartej w dniu 26 kwietnia 2016 roku pomiędzy Skarbem Państwa – Ministrem Cyfryzacji a Instytutem Łączności – Państwowym Instytutem Badawczym.

1.2 Cel pracy

Celem pracy jest zaproponowanie rozwiązań technicznych i prawnych umożliwiających wyeliminowanie lub ograniczenie nadużyć telekomunikacyjnych, takich jak np. zjawisko simboxingu.

1.3 Materiały źródłowe i sposób realizacji pracy

W pracy wykorzystano:

- krajowe i unijne akty prawne, regulacje zagraniczne, standardy ETSI oraz publicznie dostępne dokumenty krajowych i zagranicznych przedsiębiorców telekomunikacyjnych,
- informacje i opinie wybranych przedsiębiorców telekomunikacyjnych pozyskane w wyniku przeprowadzonych konsultacji,
- publikacje z prac badawczych na temat metod wykrywania simboxingu,
- opisy techniczne urządzeń służących do realizacji simboxingu,
- informacje zamieszczane na portalach i forach internetowych o nadużyciach telekomunikacyjnych, braku dostępu do usług, niskiej jakości usług i innych utrudnieniach, które mogą być spowodowane bezpośrednio lub pośrednio simboxingiem,
- notatki z konsultacji z operatorami oraz przekazane przez nich dokumenty.

Analizę nadużyć telekomunikacyjnych przeprowadzono wieloaspektowo zarówno z punktu widzenia abonentów, jak i operatorów telekomunikacyjnych oraz organów regulacyjnych w obszarach takich jak:

a) Realizacja techniczna (w tym mechanizmy i scenariusze realizacji simboxingu);
b) Środki wykorzystywane do simboxingu;
c) Instrumenty stosowane do zwalczania simboxingu (w tym metody matematyczne i urządzenia do wykrywania zjawiska simboxingu w sieci);
d) Kwestie prawnego uregulowania zjawiska simboxingu;
e) Działania regulacyjne instytucji krajowych w zakresie simboxingu;
f) Działania standaryzacyjne organizacji i podmiotów międzynarodowych;
g) Działania kontrolne (koncepcja systemu badania niezmienności numeru abonenta A)

Temat pracy przedstawiono w sposób kompleksowy z uwzględnieniem ww. kwestii oraz wyników konsultacji z operatorami, na podstawie których zdiagnozowano aktualny stan występowania zjawiska simboxingu i praktyki stosowane do jego zwalczania. Analizy z uzyskanych informacji zostały przedstawione w formie zanonimizowanej.

Oprócz simboxingu zidentyfikowano również inne negatywne zjawiska mające znamiona nadużyć telekomunikacyjnych.

W celu określenia możliwości technicznych simboxów przeanalizowano funkcjonalności wybranych urządzeń dostępnych na rynku oraz systemów do ich wykrywania.

Zaproponowano działania ukierunkowane na ograniczenie zagrożeń i wykrywanie przyczyn, a nie na usuwanie skutków, które są wynikiem nadużyć.

Przedstawiono również propozycję narzędzia do badania niezmienności numeru abonenta A przeznaczonego dla regulatora do kontroli ruchu wymienianego między operatorami.

W załączniku przedstawiono informacje uzupełniające do części głównej:

- przegląd metod i systemów do wykrywania simboxingu,
- przegląd systemów do realizacji simboxingu,
- przykłady działań organizacji i podmiotów międzynarodowych: CEPT, ETSI, ITU, i3Forum.

Niniejsze opracowanie dotyczy przede wszystkim na przedstawieniu problemów, jakie dotykają operatorów oraz strat, jakie ponoszą z tytułu fraudów telekomunikacyjnych. W trakcie prac zidentyfikowano nadużycia na szkodę użytkowników.

Potrzebę rozwinięcia tematyki, w zakresie w rozwiązywania problemów związanych z nadużyciami telekomunikacyjnymi dotykającymi użytkowników, zgłosił Departament Polityki Konsumenckiej UKE, co przedstawiono w punkcie 8.5.

2. Wstęp

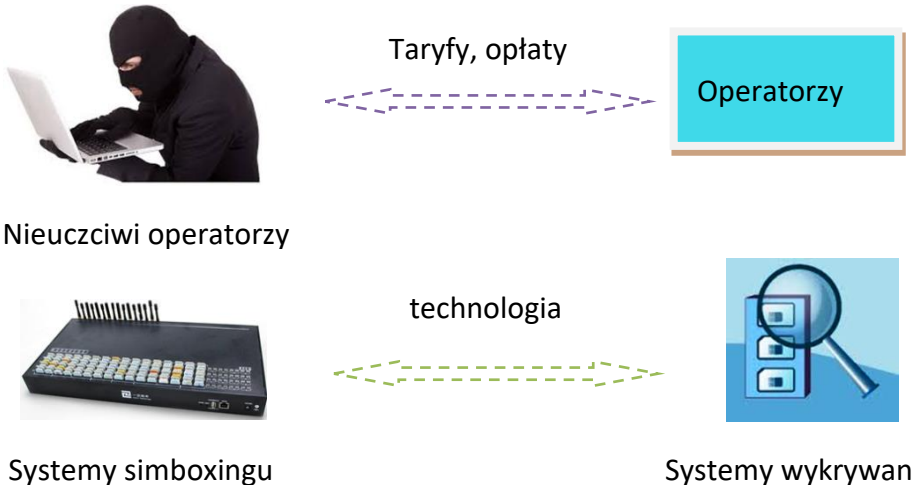
2.1 Wprowadzenie

Zróżnicowanie stawek hurtowych i detalicznych sprzyja powstawaniu nadużyć telekomunikacyjnych m.in. zjawiska simboxingu, powodowanego głównie zachowaniem anonimowości użytkowników w usłudze przedpłaconej w ruchomej publicznej sieci telefonicznej.

Stosowane przez nieuczciwych operatorów urządzenia służące do simboxingu stają się coraz bardziej wyrafinowane. Funkcjonują wbrew dobrym praktykom świadczenia usług telekomunikacyjnych i są ciągle rozwijane. Udoskonalane są także metody kamuflażu utrudniające ich wykrycie. Z analizy dostępnych opisów simboxów wynika, że nastąpił gwałtowny wzrost ich możliwości funkcjonalnych i dlatego problemy dotyczące zjawiska simboxingu wymagają rozpatrzenia w wielu aspektach.

W związku z występowaniem nadużyć rynek telekomunikacyjny stał się areną rywalizacji złych i dobrych praktyk w następujących obszarach:

- operacyjnym,
  nieuczciwi operatorzy rozszerzają asortyment nadużyć, zmieniają taktykę działania, a operatorzy prowadzący legalną działalność usiłują ukrócić te zjawiska (w szczególności simboxing) za pomocą regulaminów świadczenia usług, systemów wykrywania nadużyć itp.;
- technologicznym,
  z jednej strony obserwujemy rozwój technologii i funkcjonalności simboxów, tak aby były trudne do wykrycia i zlokalizowania, z drugiej strony pojawiają się nowe, doskonalsze urządzenia do wykrywania simboxingu.



Rysunek 2.1 Obszary rywalizacji w simboxingu

Praktyki noszące znamiona nadużyć lub będące nadużyciami w pełnym tego słowa znaczeniu dzieją się w otoczeniu prawnym instytucji unijnych i krajowych, w sektorze kontrolowanym przez krajowego regulatora rynku telekomunikacyjnego, ponieważ zjawisko nadużyć telekomunikacyjnych jest trudne do opanowania ze względu na jego globalny zasięg. Wynika to przede wszystkim z faktu, że simboxy mogą być instalowane poza granicami kraju, a więc znajdują się poza zasięgiem działania operatora krajowego oraz prawa. Krótkie serie generowanych

połączeń i częste zmiany prezentowanego numeru (pozorujące zmianę lokalizacji abonenta wywołującego) sprawia, że blokowanie numerów, z których generowane są te połączenia jest działaniem tylko na krótką metę. Obszerniejszy opis mechanizmu zjawiska simboxingu i powodów dla których jest trudne do opanowania i niełatwo jest zlokalizować winnych podano w pkt. 3.

Z konsultacji i z przeglądu ofert operatorów wynika, że wszyscy mają ofertę usługową w taryfie bez limitu w połączeniach do swojej i do wszystkich sieci, zatem wszyscy operatorzy narażeni są na oszustwa simboxingu. Dlatego uwagę zwrócono na zapisy w regulaminach i umowach (o ile występują), które mają na celu ukrócenie procederu oraz dotyczą zakresu sankcji dla abonentów wynikających ze stosowania niedozwolonych praktyk.

2.2 Definicje

CLI (ang. Calling Line Identification – identyfikacja łącza abonenckiego, wskaźnik utożsamiany najczęściej z numerem telefonicznym abonenta wywołującego.

CPND (ang. Calling Party Number Delivery) – wg ITU-T E.157 jest to usługa bazowa dla identyfikacji strony inicjującej połączenie i świadczenia usług prezentacji numeru, takich jak CLIP i MCID opisanych w zaleceniu ITU-T I.251 (dla usług) oraz w zaleceniu ITU-T Q.731 (dla sygnalizacji). CPND w ruchu międzynarodowym zapewnia przekazywanie numeru strony inicjującej połączenie w sieci poprzez granice państw.

FCT (ang. Fixed Cellular Terminal) - urządzenie komórkowe z własną kartą SIM, które może być dołączone do sieci stacjonarnej i za pośrednictwem którego można realizować w tańsze połączenia do sieci ruchomych, korzystając z niższych taryf.

Fixed Termination Rate (FTR) – stawka opłaty hurtowej za zakończenie połączenia telefonicznego w stacjonarnej sieci telefonicznej innego operatora.

Karta SIM (ang. Subscriber Identity Module) – karta chipowa różnej wielkości (mini, micro, nano) z wbudowaną pamięcią i mikroprocesorem, służąca do identyfikacji abonenta i przechowywania ograniczonej ilość danych (kontakty, SMS-y), unikalna ze względu na swój niepowtarzalny 19- lub 20-cyfrowy numer identyfikacyjny **SSN** (ang. SIM Serial Number).

MCID (ang. Malicious Call Identification) – funkcjonalność aktywowana przez abonenta, umożliwiająca identyfikację strony, która zainicjowała wywołanie złośliwe.

MT (ang. Mobile Terminated) - usługi Premium SMS świadczone są na numerach zaczynających się od cyfry 5 lub 6, dostępne z reguły w formie subskrypcji czyli prenumeraty na cykliczne dostarczanie do abonenta płatnych wiadomości.

MTR (ang. Mobile Termination Rate) - stawka rozliczeń międzyoperatorskich za zakańczanie połączeń głosowych w ruchomych publicznych sieciach telefonicznych. Nowe, obniżone stawki rozliczeń hurtowych MTRs zostały wprowadzone decyzją Prezesa UKE 14 grudnia 2012 r. Obowiązują od dnia 1 stycznia 2013 roku w rozliczeniach międzyoperatorskich na jednolitym poziomie dla wszystkich sieci telefonii komórkowej.

MVNO (ang. Mobile Virtual Network Operator) - operator wirtualnej sieci ruchomej, oferujący swoim klientom usługi telefonii komórkowej na bazie infrastruktury telekomunikacyjnej należącej do innego operatora zwanego operatorem infrastruktury lub MNO (ang. Mobile Network Operator).

Nadużycie telekomunikacyjne - wykorzystywanie usług telekomunikacyjnych niezgodnie z ich przeznaczeniem, zawartymi umowami, obowiązującymi przepisami prawa bądź normami technicznymi usług świadczonych w sieciach stron lub innych sieciach telekomunikacyjnych

(Źródło: Aneks dotyczący przeciwdziałania nadużyciom https://www.uke.gov.pl/files/?id_plik=14489.

OI (ang. Origin Identification) – identyfikacja, która pozwala określić numer telefonu, sieć, operatora oraz kraj, z którego zostało zainicjowane połączenie lub przesłana wiadomość.

Połączenie sieci – fizyczne i logiczne połączenie publicznych sieci telekomunikacyjnych użytkowanych przez tego samego lub różnych przedsiębiorców telekomunikacyjnych, celem umożliwienia użytkownikom korzystającym z usług lub sieci jednego przedsiębiorcy telekomunikacyjnego komunikowania się z użytkownikami korzystającymi z usług lub sieci tego samego lub innego przedsiębiorcy telekomunikacyjnego albo dostępu do usług dostarczanych przez innego przedsiębiorcę telekomunikacyjnego; połączenie sieci stanowi szczególny rodzaj dostępu telekomunikacyjnego realizowanego pomiędzy operatorami (art. 2 pkt 25 ustawy Pt).

Połączenie telefoniczne – połączenie ustanowione za pomocą publicznie dostępnej usługi telekomunikacyjnej, pozwalające na dwukierunkową łączność głosową (art. 2 pkt 26 ustawy Pt).

Premium Rate – usługa o podwyższonej opłacie, świadczona abonentom, obejmująca usługę telekomunikacyjną zapewniającą połączenie abonenta z dostawcą treści wraz z usługą dostępu do treści, art. 64 ust.1 ustawy Pt.

PSI (Płaska Stawka Interkonektowa) – rozliczenie z tytułu wymiany ruchu międzysieciowego inicjowanego lub zakańczanego w sieci TP wprowadzone decyzją UKE.

Simbox (zwany też SIM Bank) – urządzenie traktowane jako element bramy VoIP/GSM, umieszczony w dowolnym miejscu sieci i łączący się z tą bramą VoIP/GSM poprzez Internet. Simbox składa się z wielu interfejsów zawierających karty SIM odseparowanych od bramy VoIP/GSM. Karty SIM mogą należeć do różnych operatorów, dzięki czemu simbox może komunikować się z kilkoma bramami GSM znajdującymi się w różnych miejscach.

Brama VoIP/GSM – urządzenie zapewniająca integrację usługi VoIP z systemem telefonii komórkowej GSM, w szczególności konwersję protokołów służących do realizacji usługi VoIP (np. SIP) na protokoły stosowane do realizacji usługi głosowej w sieci GSM (definicja na potrzeby niniejszego opracowania)

Simboxing - zjawisko nielegalnego ruchu telefonicznego wykorzystywane do nieuprawnionego czerpania korzyści, polegające na masowym generowaniu drogich połączeń za pomocą instalowanych w sieci simboxów wyposażonych w wiele tanich kart przedpłaconych (pre- paid).

Sztuczny ruch ATG (ang. Artificial Traffic Generating) - ruch inicjowany w sieci telekomunikacyjnej, bądź do niej wprowadzany z wykorzystaniem urządzeń i programów mogących generować połączenia wg zaprogramowanego scenariusza tzn. o określonym czasie trwania , od jednego lub wielu numerów abonenckich do jednego lub wielu numerów, mający na celu jedynie jego zarejestrowanie w systemie bilingowym dla uzyskania nieuzasadnionych korzyści finansowych lub jego pojawienie się w punkcie styku sieci operatorskich dla wyrządzenia szkody (np. blokowania łączy, degradacji współczynników QoS) (Źrodło: Aneks dotyczący przeciwdziałania nadużyciom https://www.uke.gov.pl/files/?id_plik=14489 Generowanie sztucznego ruchu stanowi jedno ze zjawisk nadużyć telekomunikacyjnych.

3. Simboxing oraz inne nadużycia telekomunikacyjne

3.1 Skala zjawiska simboxingu

Simboxingiem popularnie określane jest nadużycie występujące przeważnie przy wymianie ruchu telefonicznego w połączeniach międzynarodowych, generowanego przy użyciu urządzeń FCT z pominięciem łączy międzyoperatorskich (połączenia sieci).

Nadużycie polega na wykorzystaniu różnicy pomiędzy cenami detalicznymi, a stawkami za zakończanie połączeń poprzez skierowanie ruchu międzyoperatorskiego do urządzenia FCT wyposażonego w karty SIM, symulujące zwykłego abonenta sieci ruchomej. W tym przypadku poszkodowanym jest najczęściej operator zakańczający połączenia, a skutkiem ubocznym zestawienia połączenia poprzez FCT jest zmiana numeru wywołującego bez wiedzy abonenta oraz obniżenie jakości świadczenia usługi.

Oszustwa związane z simboxingiem są zaliczane do grupy pięciu największych zagrożeń dla operatorów, w tym MVNO na całym świecie i według raportu stowarzyszenia Communications Fraud Control Association (CFCA) z roku 2013 powodują wysokie straty dochodów przedsiębiorców telekomunikacyjnych. Z informacji przedstawionych na konferencji i3forum 7th Annual Conference, która odbyła się w maju br. w Chicago wynika, że ogólny poziom strat przedsiębiorców na świecie z tytułu nadużyć telekomunikacyjnych może sięgać nawet około 2% wartości przychodów całego rynku telekomunikacyjnego. Z prezentowanych tam opinii, wynika również, że Europol wskazuje m.in., iż oszustwa telekomunikacyjne i cyberprzestępstwa są prowadzone obecnie na coraz większą skalę i są bardziej opłacalne dla przestępców niż handel narkotykami [1]. Z informacji podanej na stronie **http://www.xintec.com** wynika, że simboxing będący jednym z najbardziej rozpowszechnionych obecnie oszustw generuje straty rzędu 3 miliardów dolarów rocznie. Połączenia międzynarodowe wykonywane za pośrednictwem Internetu są kierowane do urządzeń zawierających karty SIM, które pod nowym zmienionym numerem abonenta A i kierują ten nielegalny ruch VoIP do sieci ruchomych jako ruch krajowy. W ten sposób nieuczciwi operatorzy skutecznie omijają stawki interkonektowe, wykorzystując różnice między wysoką stawką interkonektową i niższą stawką w połączeniu krajowym na rynku detalicznym, unikając w ten sposób oficjalnego przeliczenia zakańczanych połączeń w relacjach między operatorami, w tym MVNO.

Zjawisko simboxingu rozszerza się i istnieją co najmniej trzy powody możliwego dalszego wzrostu tego rodzaju oszustwa. Pierwszym z nich jest wykorzystanie przez oszustów przedpłaconych kart SIM bez uprzedniej rejestracji, nad którymi nadzór w zakresie śledzenia (lokalizacja, przynależność do osoby) jest znacznie trudniejszy w porównaniu do kart SIM typu post-paid. Problem jest poważny, szczególnie gdy ruch przychodzący o wysokich stawkach interkonektowych jest generowany z krajów, gdzie karty pre-paid SIM są łatwo dostępne i nie są objęte kontrolą. Drugi powód jest skutkiem przenoszeniem numerów do operatorów kuszących bardziej atrakcyjnymi ofertami. Przedsiębiorcy telekomunikacyjni działają w środowisku niskiej lojalności klienta wobec operatora. Nieuczciwi dostawcy mają zazwyczaj tańsze oferty, pozyskując w ten sposób klientów. Trzecim powodem, dla którego Simboxing staje się coraz bardziej powszechny jest szeroki wachlarz ceny simboxów, która waha się od 500 do 10 000 dolarów (przestała być zaporowa dla wielu tzw. przedsiębiorców).

Sposoby dokonywania oszustw są coraz bardziej wyrafinowane, należą do nich m.in.: często zmieniana lokalizacja, dobrze opanowana technika maskowania nierzetelnych intencji,

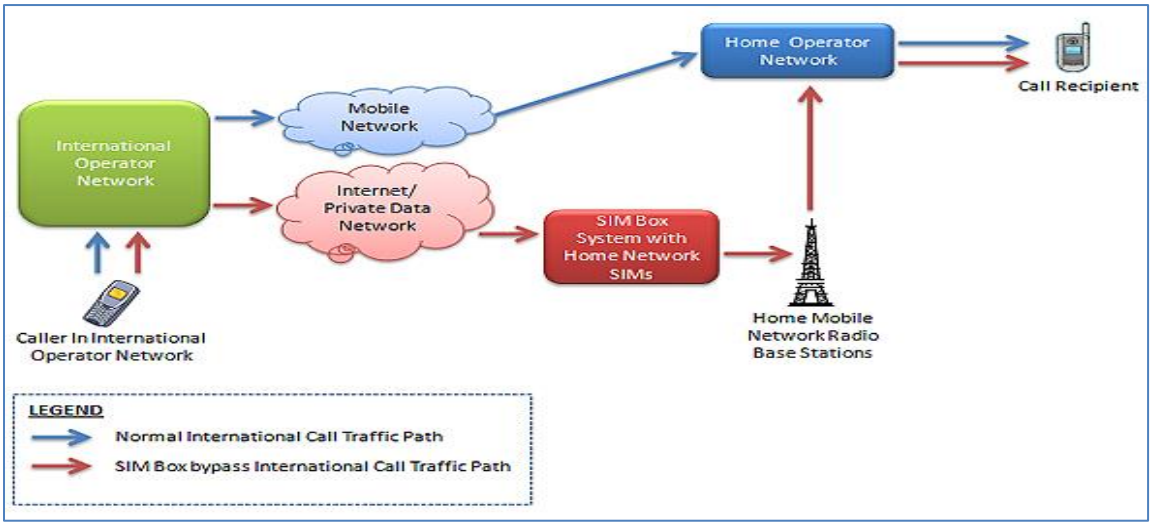
rozproszenie rozmieszczenia sprzętu w wielu miejscach skąd można wysyłać sztuczne wiadomości SMS lub przyjmować połączenia przychodzące.

W przypadku wykrycia tego zjawiska standardową procedurą operatorów telekomunikacyjnych jest zawieszenie świadczenia usług telekomunikacyjnych, następnie zerwanie umowy, a w razie większych strat – dochodzenie odszkodowania na drodze sądowej. Niewykluczone jest również skierowanie zawiadomienia do prokuratury dotyczącego popełnienia przestępstwa, np. fałszowania informacji na temat realizacji połączeń (zmiana numeru abonenta/użytkownika wywołującego).

3.2 Mechanizm działania simboxingu

Nadużycie określane mianem simboxingu stanowi nielegalną praktykę stosowaną przy tranzycie połączeń głosowych, która w przypadku ruchu międzynarodowego kierowanego do sieci stacjonarnej polega na wykorzystywaniu wiązek łączy międzycentralowych z PSI, przeznaczonych do wymiany ruchu między operatorami krajowymi. W przypadku tranzytu połączeń głosowych do sieci telefonii komórkowej proceder polega na wykorzystywaniu zróżnicowanych stawek MTR w połączeniach wewnątrz i na zewnątrz Unii Europejskiej. Nadużycie popełniane jest przy użyciu urządzeń FCT. Nazwa zjawiska pochodzi od kart SIM (ang. Subscriber Identity Module), używanych w trybie przedpłaty (pre-paid SIM) w urządzeniach zwanym FCT/Simbox pracujących jako terminale abonenckie. Simboxy transferują ruch międzynarodowy przychodzący z sieci Internet do sieci telefonii komórkowej. W ten sposób przy wykorzystaniu niskokosztowej platformy internetowej jest realizowane w sieci operatora mobilnego połączenie lokalne o niskiej opłacie, podczas gdy faktycznie abonent wywołany przez bramkę FCT/Simbox jest odbiorcą połączenia międzynarodowego, zainicjowanego w sieci operatora zagranicznego współpracującego z podmiotem, który prowadzi tę nielegalną działalność.

Schemat ideowy zestawienia połączenia w ruchu międzynarodowym z użyciem simboxów przedstawiono na rysunku 3.1.



Rysunek 3.1 Schemat zestawienia połączenia w ruchu międzynarodowym z użyciem urządzenia FCT/Simbox

Źródło: Dokument przekazany przez Orange Polska

Zasadniczym celem podmiotów uczestniczących w tym nadużyciu jest przekierowywanie ruchu telekomunikacyjnego do sieci Internet i zakańczanie połączeń międzynarodowych w sieci ruchomej z ominięciem międzynarodowych opłat interkonektowych. Tego typu połączenia realizowane są przez tzw. przedsiębiorców oferujących tanie połączenia, szczególnie na drogich kierunkach. Połączenia zakańczane są za pośrednictwem bramek FCT/Simbox, które odbierają połączenie VoIP z sieci Internet, podmieniają informację adresową i zestawiają w sieci ruchomej połączenie do abonenta żądanego, prezentując się numerem komórkowych tej sieci.

Karty SIM instalowane w bramkach FCT/Simbox należą do operatora sieci, w której zainstalowano simbox i mają odpowiednio skonfigurowaną ofertą detaliczną. Szczegółowe wykazy połączeń generowanych z wykorzystaniem tych kart SIM mylnie wskazują, iż dane połączenie zostało wykonywane pomiędzy dwoma urządzeniami końcowymi tej samej sieci, gdy w rzeczywistości połączenia zostały zainicjowane poza siecią danego operatora, w szczególności za granicą.

3.3 Nadużycia telekomunikacyjne powiązane z simboxingiem

Nadużycia telekomunikacyjne, w których jest wykorzystywane zjawisko simboxingu można podzielić na podane niżej grupy:

3.3.1 Generowanie sztucznego ruchu ATG (ang. Artificial Traffic Generating)

Nadużycie polega na generowaniu dużej liczby połączeń głosowych oraz wiadomości SMS i MMS od jednego lub wielu numerów abonenckich operatora do jednego lub grupy numerów u innego operatora, najczęściej wprowadzanych do sieci telekomunikacyjnej z wykorzystaniem urządzeń lub programów generujących połączenia, wywołania, SMS itd. o założonym czasie trwania, w celu uzyskania korzyści materialnych przez podmiot przyjmujący ruch, w związku z koniecznością zapłaty za zakończenie połączenia u danego operatora.

3.3.2 Nieuprawnione wykorzystywanie płaskich stawek interkonektowych PSI

Korzyści w tym nadużyciu wynikają z niesymetryczności stawek interkonektowych w połączeniach krajowych i zagranicznych. Największe korzyści można osiągnąć wykorzystując płaską stawkę interkonektową PSI w hurtowej usłudze zakańczania połączeń głosowych w sieci Orange, inicjowanych za granicą. Operatorzy zaangażowani w proceder zmieniają numerację zagranicznego abonenta wywołującego A na numer krajowy KNA, aby następnie połączenia głosowe zakończyć jako krajowe na wiązkach PSI przeznaczonych wyłącznie do wymiany ruchu krajowego – patrz decyzja Prezesa UKE o uchyleniu rozliczeń PSI w relacji ETelko-OPL: http://www.telko.in/uke-zablokowal-e-telko-terminacje-po-plaskich-stawkach; http://www.telko.in/files/files/DHRT.WWM.6080.7.2016.0_e-Telko_Orange_PSI.pdf.

Szerszy opis mechanizmów stosowanych w tym nadużyciu opisano w pkt 4.4,

3.3.3 Wykorzystywanie zróżnicowanych stawek MTR w połączeniach wewnątrz UE i spoza UE

W wyniku zróżnicowania stawek za zakończenie połączeń w sieci komórkowej w zależności od kraju pochodzenia (z UE i spoza UE) dochodzi do nadużycia, w którym przesyłany numer abonenta A jest zmieniany jest na numer z dowolnego kraju UE po to, aby ruch rozliczyć taniej, po stawkach operatorskich obowiązujących w UE. Dotyczy to w szczególności ruchu z kierunków spoza UE, gdzie ceny za minutę połączenia są najwyższe/znacznie wyższe.

Nadużycie jest skutkiem wydania przez UKE decyzji wprowadzającej zmiany w rozliczeniach międzyoperatorskich (MTR), w wyniku których od kwietnia 2016 w Polsce obowiązują rozliczenia po numerze abonenta A (numerze strony inicjującej połączenie). W związku z tą zmianą wprowadzono różnicowanie stawek za zakończenie połączeń w sieci komórkowej w zależności od kraju pochodzenia (z UE i spoza UE). Nadużycie polega na umyślnej ingerencji w przesyłany numer abonenta A.

W wyniku wprowadzenia w krajach UE mechanizmu RLAH (ang. Roaming Like At Home) przy jednoczesnym występowaniu różnych stawek MTR w poszczególnych krajach UE dochodzi do nadużycia np. poprzez inicjowanie połączenia w roamingu (z karty SIM polskiego operatora np. z taryfy unlimited lub z pakietem minut) na numer zagraniczny innego kraju w UE (np. w UK, Słowenia, Estonia), u którego obowiązują wyższe MTR. Zgodnie z założeniami rozliczeń międzyoperatorskich beneficjentem takiego ruchu jest operator wg numeru A. W związku z tym dużym ruchu przychód detaliczny, jaki uzyskuje polski operator może być zbyt niski, aby pokryć koszt hurtowy (tj. stawka hurtowa w roamingu na rzecz operatora, w którego sieci zalogował się klient + koszt podwyższonego MTR na numer zagraniczny).

3.3.4 Generowanie połączeń na numery zagraniczne IRSF (ang. International Revenue Share Fraud)

Nadużycie polega na generowaniu sztucznego ruchu na zagraniczne numery Premium Rate lub o wysokim koszcie. Często dla zwiększenia zysków połączenia inicjowane są, jako konferencyjne (trójstronne). Nadużycie polega na wykorzystywaniu rozliczeń międzyoperatorskich i otrzymywaniu części przychodów z tytułu opłat za zakańczanie połączeń, uzyskiwanych przez posiadacza numeru.

3.3.5 Wykorzystywanie abonamentu typu no limit w Internecie do generowania ruchu na łącza międzysieciowe

Oferta no limit (bez ograniczeń do wszystkich sieci, na liczbę i czas trwania połączenia itp.) jest powszechnie wykorzystywany przez przedsiębiorców w przekazach reklamowych. Nieuczciwym przedsiębiorcom służy do generowania dużego wolumenu ruchu na łącza międzysieciowe wszystkimi możliwymi sposobami. Mogą być zestawiane połączenia o długim czasie trwania blokujące łącza międzysieciowe prze 24 godziny na dobę. Mogą być wykorzystane simboxy do generowania dużego wolumenu ruchu lub centrale abonenckie do kierowania połączeń na łącza międzycentralowe.

Wykorzystanie central PABX w celu zakańczania ruchu z zagranicy z podmienionym numerem jest przykładowym nadużyciem typu call center. Zasadniczym celem podmiotów uczestniczących w tym nadużyciu jest przekierowywanie ruchu telekomunikacyjnego i zakańczanie połączeń międzynarodowych w danym kraju w sposób umożliwiający ominięcie wszystkich międzynarodowych opłat międzyoperatorskich. Podczas realizacji takiego połączenia następuje zmiana informacji adresowej tj. rzeczywistego numeru wywołującego abonenta A.

Ruch kierowany jest za pośrednictwem Internetu na łącza PABX z odpowiednio skonfigurowaną ofertą i następnie z wykorzystaniem przyznanej numeracji ruchu przekierowywany jest nielegalnie do docelowych sieci telekomunikacyjnych. Szczegółowe wykazy połączeń generowanych w ten sposób mylnie wskazują, iż dane połączenie zostało

wykonywane pomiędzy dwoma urządzeniami końcowymi, gdy w rzeczywistości połączenia zostały zainicjowane poza siecią danego operatora, w szczególności za granicą.

3.3.6 Klonowanie kart SIM i numeru IMEI

Nadużycie klonowania kart SIM polega na odczytaniu danych z karty SIM i przegraniu tych danych na wiele innych niezaprogramowanych kar SIM, a potem wykorzystywaniu tych kart w simboxach.

Nadużycie klonowania numerów IMEI polega na kopiowaniu legalnych numerów IMEI, które zostały wykradzione z legalnych aparatów. Klonowanie numeru IMEI zazwyczaj ma miejsce w przypadku aparatów, które pochodzą z kradzieży. Niektóre kraje, uczulone na kwestię bezpieczeństwa telekomunikacyjnego postanowiły zabronić kopiowania numerów IMEI, ale większość światowych prawodawców zdecydowanie mniej rygorystycznie podchodzi do tego rodzaju procederu. Wskazane byłoby w Polsce wprowadzić obowiązek sprawdzania prawdziwości numeru IMEI permanentnie przy każdym zestawianym połączeniu. Taka kontrola powinna zwiększyć wykrywalność telefonów z fałszywymi numerami IMEI.

3.3.7 Włamania do central PBX i VPBA (PBX hacking)

Nadużycie polega na nieuprawnionym użyciu PBX w celu wykonywania dużych wolumenów połączeń wychodzących, w tym generowania ruchu na numery o podwyższonej opłacie. Standardową procedurą operatorów telekomunikacyjnych, w przypadku wykrycia nadużycia, jest poinformowanie właściciela centralki o identyfikacji podejrzanego ruchu.

3.4 Inne nadużycia telekomunikacyjne

Nadużycia telekomunikacyjne, traktowane jako oszustwa i wyłudzenia, można podzielić na niżej wymienione przykładowe grupy.

3.4.1 Wyłudzanie poprzez SMS kodów doładowujących karty pre-paid

Nadużycie polega na próbie podszycia się pod dostawcę usługi i przesłaniu abonentowi/użytkownikowi usług przedpłaconych informacji o rzekomej korzyści (np. podwójnym doładowaniu, możliwości wygrania drogiego sprzętu itp.) po przesłaniu przez abonenta zwrotnie kodu doładowującego. Wysłany kod zostaje wykorzystany przez oszusta. Taki czyn nosi znamiona przestępstwa (oszustwa lub kradzieży impulsów) z sankcjami określonymi w ustawie z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 1997 nr 88 poz. 553 z pożn. Zmn.) (ustawa Kk).

3.4.2 Kolportowanie wirusów w sieciach komórkowych w celu wyłudzenia danych, wysyłania SMS poza kontrolą użytkownika, szyfrowania danych użytkownika oraz szantażowania (Malware)

Zagrożenia związane z malware na urządzenia mobilne (np. smartfon) stało się powszechnością. Najczęstsze wektory infekcji urządzenia mobilnego to:

- Kampanie złośliwego oprogramowania/phishingowe nakłaniające do pobrania złośliwego pliku pod przykrywką np. pobrania faktury. Złośliwy plik może być dołączony bezpośrednio do fałszywej wiadomości bądź wiadomości (w tym SMSowa) i może nakłaniać do odwiedzenia złośliwej strony, z której pobierzemy złośliwe

oprogramowanie bądź podamy swoje poufne dane (np. login i hasło) albo zostaniemy nakłonieni do wysłania SMS zapisującej do usługi Premium Rate).

- Pobranie złośliwego oprogramowania wraz z aplikacją, w przypadku pobierania jej z nieznanych źródeł w tym również zainstalowanie aplikacji z wbudowaną tylną furtką, która następnie może posłużyć do przejęcia kontroli nad urządzeniem i np. zainstalowania złośliwego oprogramowania.
- Wykorzystanie podatności systemu i oprogramowania, zwłaszcza tych znanych w przypadku braku jego bieżącej aktualizacji.

Złośliwe oprogramowanie na urządzeniu mobilnym może służyć m. in. do:

- wyłudzania poufnych danych,
- nieuprawnionego wysyłania SMS,
- szyfrowania danych użytkownika oraz szantażowania (żądania okupu), w przypadku złośliwego oprogramowania typu ransomware.

3.4.3 Wprowadzanie w błąd abonenta/użytkownika w celu akceptacji przez niego subskrypcji MT (Premium SMS Mobile Terminated)

Nadużycie podlega na tym, że osoba chcąca skorzystać z serwisu w Internecie (np. obejrzeć film, doładować telefon, wysłać e-kartkę z życzeniami) podaje swój numer telefonu w celu otrzymania kodu dla wybranej usługi, a zamiast tego otrzymuje SMS powiadamiający o uruchomieniu usługi wysyłania na jej numer wiadomości SMS wysokopłatnych przy odbiorze (nawet kilka razy w tygodniu). Abonent nie był świadomy tego, że zamawia usługę, natomiast wprowadzenie w błąd dotyczy warunków na jakich usługa jest świadczona. Można się przed tym uchronić zapoznając się z regulaminem usługi, rodzajem usługi, a w przypadku braku dostępu do treści regulaminu - niekontynuowanie transakcji. Konsekwencją dla nieświadomych abonentów/użytkowników jest konieczność zapłacenia wysokiego rachunku za usługę.

3.4.4 Uruchomienie subskrypcji MT (Premium SMS Mobile Terminated) za pomocą aplikacji z niezaufanego źródła

Nieświadome uruchomienie zamówienia na otrzymywanie SMS-ów MT może również być spowodowane ściągnięciem aplikacji z niezaufanego źródła, uruchomieniem gry, skanowaniem smartfona itp. Aplikacja bez wiedzy abonenta wysyła SMS uruchamiający subskrypcję.

3.4.5 Wysyłanie SMS wprowadzających w błąd użytkownika w celu uzyskania korzyści

Nadużycie polega na wprowadzeniu użytkownika w błąd, poprzez wysłanie (najczęściej automatycznie) wiadomości, której treść sugeruje uruchomienie płatnej subskrypcji i jednocześnie informuje o możliwości wyłączenia tej usługi poprzez wysłanie zwrotnej wiadomości z określonym kodem. Podstęp polega na tym, że wiadomość jest wysłana na numer wysoko płatny bez podania kosztów lub przy zaniżeniu stawki za SMS zwrotny. W rzeczywistości abonent/użytkownik odsyłający wiadomość, zamiast usunięcia subskrypcji, ponosi koszt korzystania z usługi o podwyższonej płatności. Osoba pokrzywdzona może dochodzić roszczeń od właściciela serwisu Premium Rate. Konsekwencją dla

nieświadomych abonentów/użytkowników jest konieczność zapłacenia za zrealizowaną usługę. Abonentowi/użytkownikowi wprowadzonemu w błąd przysługuje prawo do złożenia reklamacji (wraz z podaniem odpowiednich dowodów).

3.4.6 Prowokowanie oddzwaniania na drogie numery po rozłączeniu połączenia po jednym nieodebranym dzwonku (jap. wangiri fraud, ang. one ring one cut)

Nadużycie to polega na oszukaniu abonenta/użytkownika, który automatycznie oddzwania na numer, figurujący jako „nieodebrane połączenie". Numer ten najczęściej jest podobny do numeru krajowego, ale jest numerem zagranicznym o cenie za połączenie znacznie wyższej niż cena krajowa. Często wykorzystywane są podobieństwa początku numerów krajowych i międzynarodowych (np. 22 – Warszawa, +22 – kraje afrykańskie). Operatorzy w przypadku wykrycia nagłego przyrostu ruchu na dany kierunek międzynarodowy podejmują stosowne działania. Konsekwencją dla nieświadomych abonentów/użytkowników jest konieczność zapłacenia za zrealizowane połączenia.

3.4.7 Aktywacja usługi na fałszywe lub cudze dokumenty w celu wyłudzenia sprzętu lub usług

Wyłudzanie polega na podpisywaniu umów na sfałszowane dokumenty z intencją nieopłacania faktur za usługi i uzyskania sprzętu o dużej wartości oraz kart SIM.

3.4.8 Podmiana kont bankowych na fakturach

Oszustwo polega na dokonaniu kradzieży rachunku/faktury ze skrzynki pocztowej abonenta/użytkownika i zmianie na tym rachunku numeru konta bankowego operatora na inne. Działanie takie nosi znamiona kilku przestępstw wskazanych w ustawie Kk Należy więc zachować ostrożność w przypadku, gdy znaleziony w skrzynce pocztowej dokument zawierający logo operatora wygląda na zmieniony czy przerobiony. Numer konta do zapłaty faktury można z potwierdzić z operatorem infolinii operatora. Inną formą jest rozsyłanie, podszywając się pod operatora, sfabrykowanych faktur na skrzynki mailowe.

3.4.9 Podszywanie się pod dowolny numer telefoniczny za pośrednictwem portali Internetowych

Podszywanie się pod dowolny numer telefoniczny umożliwiają internautom nieuczciwe portale internetowe. Takie portale oferują usługi telefonii internetowej, które pozwalają osobie inicjującej połączenie wybrać dowolny ciąg cyfr jako rzekomy numer abonenta A. Podany numer jest wyświetlany abonentowi B, do którego jest zestawione połączenie. Oznacza to, że w praktyce użytkownik serwisu może zafałszować numer i przedstawić się dowolnym numerem (policji, straży, banku, instytucji publicznej itp.).

Sposób działania powyższego nadużycia można wyjaśnić na przykładzie usługi jednej z platform VoIP umożliwiającej kiedyś wybór numeru geograficznego dla dowolnie wybranej strefy numeracji oraz możliwość dowolnej konfiguracji usług dodanych z poziomu użytkownika. Zaawansowany panel konfiguracyjny użytkownika dostępny był z poziomu przeglądarki WWW (indywidualne konto użytkownika) i dawał bezpośredni dostęp do opcji dodatkowych – mowa o poprzedniej wersji usługi FreecoNet: DIAL-IN, CALL-BACK oraz AUTORYZACJA które z kolei dawały możliwości modyfikacji właściwej prezentacji połączeń między numerami w bilingu/CDR. Usługa umożliwiała świadomą modyfikację prezentacji rzeczywistego numeru abonenta wywołującego przez samego użytkownika/klienta serwisu, co powodowało również problemy w identyfikacji połączeń z urządzeń w billingu np. OPL

(rzeczywisty czas rozpoczęcia połączenia i czas jego trwania – rejestracja rekordów DATA) oraz wpływ na właściwą rejestracją połączeń w systemach billingowych dla potrzeb organów ścigania.

Podszywanie się pod dowolny numer telefoniczny umożliwiają internautom nieuczciwe portale internetowe. Takie portale oferują usługi telefonii internetowej, które pozwalają osobie inicjującej połączenie wybrać dowolny ciąg cyfr jako rzekomy numer abonenta A. Podany numer jest wyświetlany abonentowi B, do którego jest zestawione połączenie. Oznacza to, że w praktyce użytkownik serwisu może zafałszować numer i przedstawić się dowolnym numerem (policji, straży, banku, instytucji publicznej itp.).

Możliwość zafałszowania numeru może być wykorzystana do działań przestępczych (karalnych gróźb, rozbójniczych wymuszeń, anonimowych oszustw, działań terrorystycznych). Proceder podważa także wartość dowodową bilingów telefonicznych, gdyż fałszywy numer widnieje także na bilingu.

Proceder jest możliwy z powodu luki w ustawie Pt, która polega na tym, że przepis mówiący o tym, że numer telefonu musi być taki sam na całej drodze połączeniowej nie mówi jednocześnie o tym, że musi być on prawdziwy.

Podszywanie się pod dowolny numer telefonu zagraża bezpieczeństwu publicznemu, dlatego tworzenie portali umożliwiających taki proceder powinno być zakazane prawem.

3.4.10 Kierowanie ruchu okrężną drogą z uwagi na spłaszczanie stawek w Europie do stawek jak w ruchu krajowym

Można przyjąć, że ten przypadek dotyczy podobnej sytuacji jak nadużycie związane z wykorzystaniem Płaskiej Stawki Interkonektowej.

W tym modelu ruch jest celowo kierowany do operatorów sieci zagranicznych, numer A jest modyfikowany, a następnie kierowany przez kliku innych operatorów w celu zatarcia śladów i utrudnienia potencjalnych działań kontrolnych. Co więcej na rynku występują nawet firmy które oferują komercyjnie podmianę numeru wywołującego A – po przepuszczeniu ruchu przez urządzenia tych podmiotów dostaje się nową sygnalizację z numerem A.

3.4.11 Nadpisywanie numeru/adresu strony A w wiadomościach SMS

Nie każdy przypadek nadpisywania numeru/adresu strony wysyłającej wiadomości SMS jest nadużyciem, ponieważ są nadpisy uregulowane, zdefiniowane na stałe. Operatorzy mają umowy z klientami na dynamiczne nadpisywanie, które jest realizowane poprzez dostęp klientów do MSC.
W związku z brakiem regulacji dotyczących weryfikacji nadpisów przychodzących na połączeniach międzyoperatorskich, operatorzy podkreślali potrzebę uregulowań prawnych w zakresie nadpisywania adresu A w wiadomości SMS. Jakkolwiek jest to problem jest istotny, to jednak trudny do rozwiązania ponieważ wymaga uzgodnień międzyoperatorskich. Wskazane szczegółowe wyjaśnienie zjawiska i użytych pojęć, na czym polega nadpisywanie]

3.4.12 Nieuczciwa konkurencja

Działania nieuczciwych przedsiębiorców telekomunikacyjnych związane są z nieetycznym oraz niezgodnym z obowiązującym prawem zachowaniu polegającym na wprowadzaniu klientów w błąd np. sugerowaniu, że rozmowa odbywa się z przedstawicielem dotychczasowego operatora świadczącego usługę. W trakcie rozmowy z Klientem budowane jest błędne przekonanie, że dotychczasowy dostawca usług telekomunikacyjnych, który świadczył usługi danemu abonentowi, uległ likwidacji, został wykupiony przez inny podmiot lub przygotował nową ofertę na korzystniejszych warunkach.

Klienci zamiast korzystniejszych warunków otrzymują wyższe niż dotychczas rachunki, a dopiero po otrzymaniu pierwszej faktury dowiadują się również o dokonaniu zmiany dostawcy usług telekomunikacyjnych. W przypadku odstąpienia od umowy (nawet w ustawowym terminie 14 dniu w przypadku umowy zawartej na odległość abonenci obciążani są często dodatkowymi opłatami za odstąpienie od umowy.

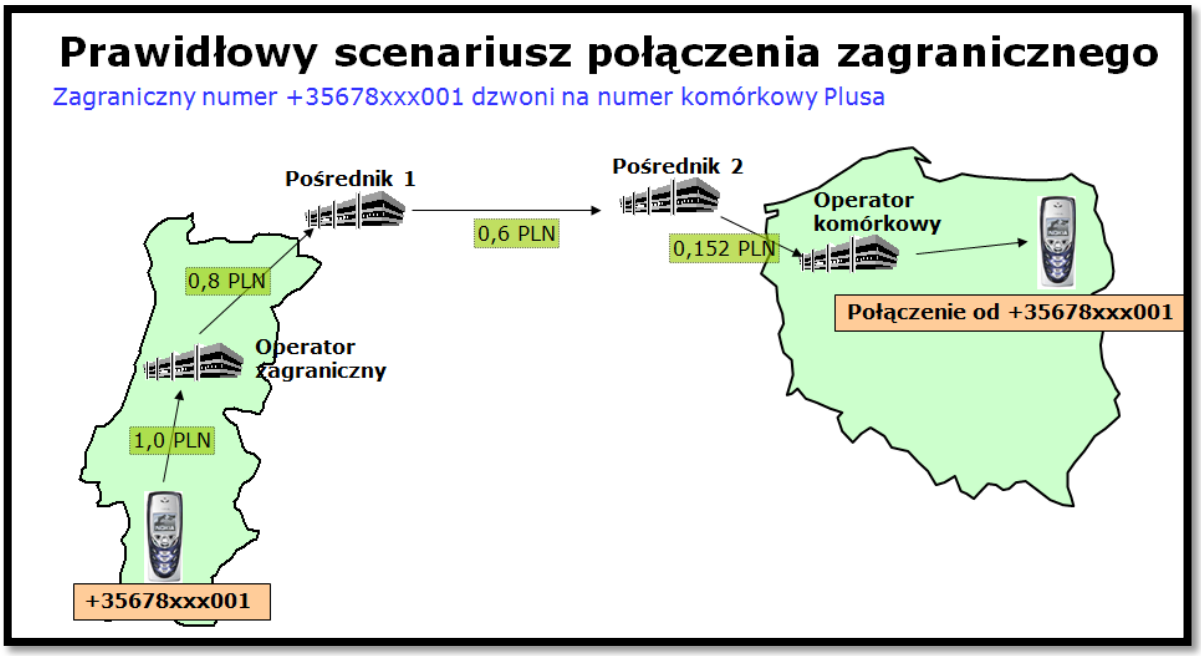
Nieuczciwa konkurencja jest zatem wynikiem umyślnego wprowadzania Klientów w błąd przy zawarciu umowy (np. w zakresie dostawcy usług), przedstawienia użytkownikom nierzetelnych lub nieprawdziwych informacji, nie pozostawienia klientowi kopii umowy i innych dokumentów związanych z umową.

3.5 Scenariusze realizacji połączeń w przypadku simboxingu

3.5.1 Scenariusz realizacji połączeń obejściowych z wykorzystaniem Internetu

Utrzymywana przez lata silna dysproporcja ceny połączeń pomiędzy publicznymi sieciami ruchomymi, w stosunku do stawek międzyoperatorskich między sieciami stacjonarnymi i komórkowymi spowodowała, że znaczna część ruchu z sieci stacjonarnych do komórkowych jest przekazywana przez nieuczciwych operatorów z zastosowaniem wielokanałowych urządzeń FCT. W Polsce powstało wiele firm zajmujących się obsługą połączeń z sieci stacjonarnych do komórkowych wykorzystujących tego typu rozwiązania. W ofertach wielu operatorów, szczególnie posługujących się techniką VoIP, połączenie takie jest często nazywane „połączeniem bez identyfikacji".

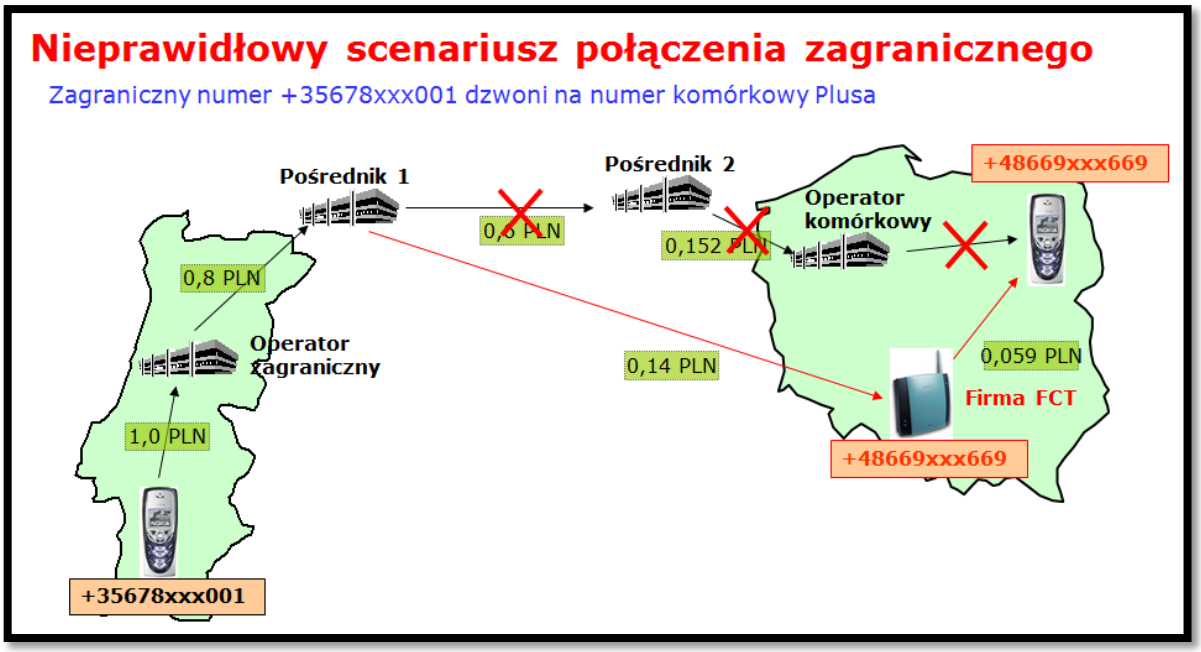
W przypadku ruchu międzynarodowego, wysokie ceny połączeń oraz wyższe regulowane stawki rozliczeń międzyoperatorskich (MTR) niż detaliczne ceny połączeń w Polsce powodują, że dochodzi do nadużyć telekomunikacyjnych, polegających na nieuprawnionym kierowaniu połączeń do sieci telekomunikacyjnej z pominięciem łączy międzyoperatorskich. Coraz częściej zamiast scenariusza pokazanego na rysunku 3.2 jest realizowany scenariusz realizacji połączenia z rysunku 3.2, noszący znamiona nadużycia telekomunikacyjnego, ponieważ motywem dla obsługi połączeń w taki sposób może być chęć uzyskania korzyści finansowych lub chęć pozyskania informacji z bilingu, z wiadomości SMS/MMS lub z podsłuchu.



Rysunek 3.2 Scenariusz realizacji połączenia w ruchu międzynarodowym, gdy nie ma nadużycia telekomunikacyjnego (Źródło: Dokument przekazany przez Polkomtel Sp. z o.o.)

W scenariuszu pokazanym na tym rysunku realizowane jest połączenie z numeru zagranicznego 356 xxx001 w sieci ruchomej do abonenta sieci Plus. Połączenie jest zestawiane poprzez dwie sieci tranzytowe oznaczone jako Pośrednik 1 i Pośrednik 2. Abonent inicjujący płaci operatorowi zagranicznemu za połączenie 1,0 zł. Pośrednik 1 inkasuje 80 gr i płaci za tranzyt 60 gr. Pośrednikowi 2, który opłaca operatora zakańczającego w wysokości 15,2 gr.

Podmioty prowadzące nieuczciwe interesy wykorzystują tę niekorzystną sytuację wynikającą z wysokich opłat tranzytowych instalując urządzenia FCT w sieci Internet, co jest prawnie dozwolone. Po przejściu przez sieć tranzytową Pośrednika 1 połączenia jest kierowane poprzez sieć Internet do urządzenia FCT z pominięciem sieci Pośrednika 2. Urządzenie FCT zestawia w sposób automatyczny połączenie do żądanego numeru, prezentując się krajowym numerem sieci ruchomej +48669xxx669 (Rysunek 3.3).



Rysunek 3.3 Scenariusz realizacji połączenia w ruchu międzynarodowym z użyciem urządzenia FCT

Źródło: Dokument przekazany przez Polkomtel Sp. z o.o.

W tym scenariuszu, w urządzeniu FCT, dokonywana jest zamiana formatu numeru abonenta wywołującego z formatu numeru międzynarodowego na krajowy. Pośrednik 1 płaci firmie dysponującej urządzeniem FCT 14 gr. zamiast 60 gr. (jak to miało miejsce w poprzednim scenariuszu). Firma dysponująca urządzeniem FCT płaci operatorowi sieci komórkowej zakańczającemu połączenie kwotę 5,9 gr. (mniejszą niż operator sieci ruchomej otrzymywał od Pośrednika 2 poprzednim scenariuszu). Ten scenariusz jest bardziej korzystny dla Pośrednika 1, mniej korzystny dla operatora sieci ruchomej. Korzyści czerpie także firma dysponująca urządzeniem FCT, która jednak uprawia niedopuszczalny proceder zamiany numeru.

Zestawienie połączeń międzynarodowych poprzez FCT wiąże się z negatywnymi konsekwencjami, takimi jak:

- zamiana faktycznego numeru na inny lub brak prezentacji numeru abonenta wywołującego,
- modyfikowanie bilingów,
- ryzyko nagrywania i podsłuchiwania połączeń przez nieuprawnione podmioty,
- gorsza jakość połączeń (z powodu przesyłania głosu przez Internet),
- dłuższy czas zestawiania połączenia.

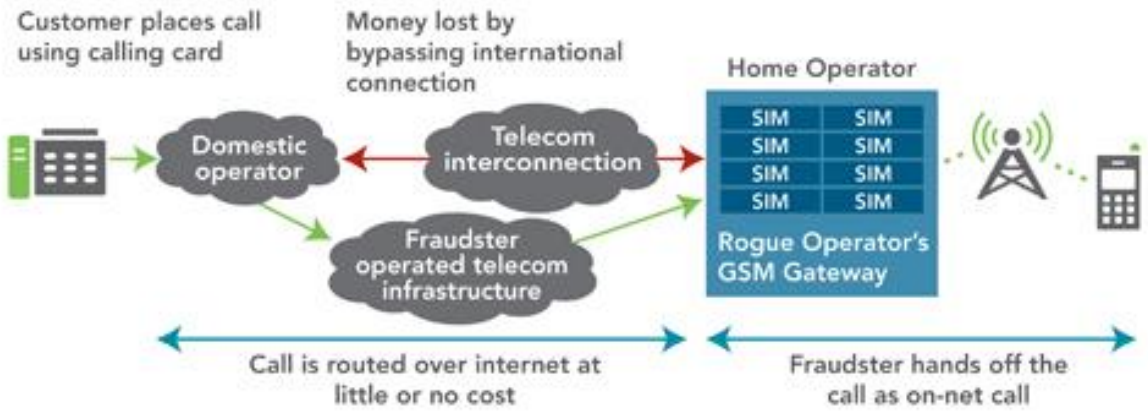
Aby nie narażać się na straty operatorzy sieci ruchomej wprowadzają w regulaminie zapisy mówiące na tym, że w przypadku uzasadnionego podejrzenia fraudu z użyciem urządzenia FCT podejrzany numer będzie zablokowany (punkt 7, załącznik 3 punt 15).

3.5.2 Scenariusz wydzwaniania na własne numery wykorzystujący asymetrię stawek MTR

Nadużycie związane z wykorzystywaniem zróżnicowanych stawek rozliczeniowych za zakańczanie (terminowanie) połączeń w sieciach operatorów komórkowych polega na wydzwanianiu przez operatora na własne numery z sieci innego operatora przy pomocy urządzeń FCT/Simbox. Pokusa do takich działań jest tym większa im większa jest różnica dotycząca tych stawek. Proceder jest opłacalny dla tego operatora, który ma wyższe stawki MTR (Mobile Termination Rate) w stosunku do innego. Korzystając z asymetrii operator o wyższych stawkach ma wyższe wpływy niż wydatki ponoszone w rozliczeniu z operatorem sieci, z którego były inicjowane połączenia związane z simboxingiem.

Operatorzy mogą przeciwdziałać tego typu nadużyciom we własnym gronie ustalając symetryczne stawki zakańczania połączeń bez względu na wielkość ruchu wymienianego w obie strony.

Wprowadzone w UE niższe stawki MTR nie rozwiązały tego problemu. Proceder jest nadal opłacalny z krajów spoza UE (np. z Ukrainy, gdzie są wyższe stawki niż w krajach UE). Operatorzy obserwują nasilenie się zjawiska unikania kosztów legalnego transferu w ruchu międzynarodowym (m. in. w ruchu przychodzącym z Ukrainy) z użyciem simboxów.



Rysunek 3.1 Schemat działania simboxingu

(Źródło: http://www.pipelinepub.com/network_and_communications_security/combating_telecom_and_VoIP_fraud/2)

4. Simboxing w sieci operatorów krajowych

W niniejszym rozdziale opisano wyniki konsultacji przeprowadzonych z operatorami, obejmujące ocenę skali zjawiska simboxingu i identyfikację problemów wynikających z tego zjawiska. Ponadto opisano przypadek nadużycia związany z simboxingiem, który wystąpił w sieci jednego z operatorów.

4.1 Skala zjawiska simboxingu w sieci krajowej

Operatorzy telekomunikacyjni podkreślali, że zjawisko simboxingu występuje w dużej skali w sieci krajowej. O dużej skali tego zjawiska świadczy fakt, że zachodzi konieczność blokowania od ok. 10 tys. do nawet 100 tys. kart SIM miesięcznie przez jednego z operatorów.

Operatorzy zwracali uwagę, że następuje zmiana działania simboxingu. Kiedyś połączenia międzynarodowe były przesyłane po IP i terminowane u operatora końcowego po lokalnej stawce. Obecnie w związku ze zróżnicowaniem stawek MTR wewnątrz UE i poza UE operatorzy obserwują wzrost wolumenu ruchu przychodzącego z krajów UE kosztem ruchu spoza UE. Obserwują także spadek ruchu międzynarodowego z innych części świata, w tym z USA. W opinii operatorów taka sytuacja wskazuje na duże prawdopodobieństwo wykorzystywania simboxów do tranzytu połączeń z zagranicy.

Zmniejszenie stawek za połączenia międzynarodowe w Unii Europejskiej spowodowało, że w połączeniach z krajów spoza UE zamieniany jest numer abonenta A i trudno jest to zjawisko zwalczyć (zob. pkt 3.5.2).

Opłacalność nadużycia simboxingu

Wg operatorów na opłacalność simboxingu mają wpływ następujące czynniki:

1. wprowadzenie niższych stawek MTR w UE przy niezmienionych wyższych stawkach za połączenia spoza UE, co stanowi zachętę do simboxingu (zob. pkt 3.6),
2. asymetria stawek MTR pomiędzy operatorami krajowymi, co powoduje wydzwanianie przez nieuczciwych operatorów na własne numery, w szczególności usług z podziałem opłaty (revenue sharing) przy korzystnej różnicy opłat wynikającej z podziału.

Operatorzy stwierdzili, że skala oddziaływania simboxingu jest znacząca i ma wpływ na parametry techniczne sieci, aspekty ekonomiczne oraz na bezpieczeństwo. Generowanie dużego ruchu w radiowej sieci dostępowej powoduje

a) natłok w sieci,
b) wysycanie się sieci radiowej w obszarach stosowania FCT (z powodu FCT trzeba rozbudowywać sieć),
c) zaburzenia procesu planowania sieci,
d) zaburzanie ciągłości numeru abonenta A na drodze połączeniowej,
e) obniżanie jakości połączeń i generowanie skarg przez klientów,
f) zaburzenia bilingu (brak lub błędne dane o połączeniu dla organów ścigania).
g) zmniejszone przychody operatora,
h) brak możliwości określenia numeru abonenta A,

i) możliwość nagrywania rozmów dla wybranych numerów lub par numerów (działanie przestępcze, dziennikarze itp.)

Skuteczność wykrywania

Połączenia realizowane przez simboxy muszą być wykrywane szybko, bo krótki jest czas na zlokalizowanie karty SIM. Rekordy CDR generowane są co 15 min., więc przeciętny czas życia karty w simboxach wynosi ok. 20 min. W związku z tym, że trzeba je wymieniać tak często, że przedsiębiorcy dopuszczający się tego procederu dysponują zwykle dużym wolumenem kart SIM typu pre-paid. Ponieważ karty pre-paid nie były wcześniej objęte obowiązkiem rejestracji, więc nie można było wpływać na ograniczenie tego procederu poprzez gospodarowanie numeracją.

Przesłankami wskazującymi, że połączenie realizowane jest przez FCT są: zmiana numeru abonenta A, brak numeru, wydłużony czas zestawiania połączenia, gorsza jakość transmisji głosu, relatywnie duża liczba wywołań z jednego numeru itp.

4.2 Przypadki nadużyć związanych z simboxingiem potwierdzone przez operatorów

Operatorzy potwierdzili, że w ich sieciach występują nadużycia powiązane z simboxingiem i generowaniem sztucznego ruchu, takie jak:

1. Generowanie połączeń do tzw. pseudoserwisów

   Mechanizm nadużycia polega na wykorzystywaniu w simboxach kart typu no-limit do dzwonienia na numery pseudo-usługowe w sieci innego operatora, co pozwala uzyskiwać dochody z opłat za ruch przychodzący. Wskutek tego, generowane są dziesiątki tysięcy minut, po kilka połączeń jednocześnie z jednej karty.

2. Wykorzystywanie pakietów płaskich ofert do generowania sztucznego ruchu, gdzie są asymetryczne stawki i obciążanie za ruch przychodzący do innego sieci operatora, który z tego tytułu czerpie korzyści.

3. Klonowanie kart SIM (dotyczy kart starego typu).

4. Klonowanie numeru IMEI.

   Niektóre kraje, uczulone na kwestię bezpieczeństwa telekomunikacyjnego postanowiły zabronić kopiowania numerów IMEI, ale większość światowych prawodawców zdecydowanie mniej rygorystycznie podchodzi do tego rodzaju procederu.

   W polskim prawodawstwie przepisy dotyczące możliwości karania za przerobienie numeru IMEI już istnieją, ewentualnie można byłoby je zmienić tak, żeby były bardziej jednoznaczne.

   Kodeks karny (art. 270 § 1 k.k.) przewiduje możliwość karania za przerobienie numeru IMEI przez osobę nieuprawnioną, traktując aparat telefoniczny trwale oznakowany numerem IMEI, jako dokument (zapisany nośnik informacji). Warunkiem niezbędnym do wymierzenia kary jest jednak ustalenie, że sprawca działał w zamiarze bezpośredniego użycia tak przerobionego telefonu, jako autentycznego.

   Drugą możliwością nałożenia kary (art. 306 k.k.) jest przyjęcie, że sprawca usuwa, podrabia lub przerabia znak indentyfikacyjny urządzenia, albowiem przypisany do telefonu komórkowego numer IMEI jest jego znakiem identyfikacyjnym.

5. Wykorzystywanie asymetrii stawek MTR i podmienianie numeru A w połączeniach międzynarodowych

   W wyniku modyfikacji informacji adresowej strony inicjującej połączenie możliwe są zagrożenia takie jak:

- Celowe zatarcie śladów źródła pochodzenia ruchu oraz utrudnienie prowadzenia działalności kontrolnej organom państwowym
- Brak wypełniania obowiązków na rzecz obronności, bezpieczeństwa Państwa oraz bezpieczeństwa i porządku publicznego
    - W wyniku oszustwa operatorzy telekomunikacyjni nie są w stanie przedstawić prawdziwych i kompletnych informacji o tym, kto faktycznie dzwonił na podany numer. Operatorzy nie są w stanie zagwarantować prawidłowego wykonania kierowanych przez uprawnione organy państwowe wezwań do przedstawienia niezbędnych danych retencyjnych
- Naruszenie zasad przetwarzania danych objętych tajemnicą telekomunikacyjną
    - Z terminowaniem połączeń wiąże się przetwarzanie danych transmisyjnych. W sytuacji, gdy podmiot ten dokonuje zmiany lub usunięcia numeru linii wywołującej, dochodzi do niedopuszczalnego przetworzenia tych danych.
- Brak możliwości prezentacji identyfikacji zakończenia sieci
    - Operatorzy nie są w stanie spełnić wymogów wynikających z Pt, czyli prezentacji identyfikacji zakończenia sieci, z którego inicjowane jest połączenie. Następuje wprowadzenie w błąd również użytkownika końcowego, któremu operator na jego życzenie jest zobowiązany świadczyć usługę prezentacji identyfikacji linii wywołującej, przed dokonaniem połączenia. Naraża to operatora na odpowiedzialność cywilną wobec użytkownika sieci, oraz na odpowiedzialność administracyjną ze strony organu regulacyjnego. Niesie to również zagrożenia (organizacje przestępcze, terroryzm).
    - Konieczne jest wprowadzenie odpowiednich przepisów oraz sankcji do ustawy Pt za naruszenie zmiany informacji adresowej oraz wprowadzenie do norm międzynarodowych zapisów zabraniających zmiany informacji adresowej.

6. Kierowania ruchu okrężną drogą z uwagi na spłaszczanie stawek w Europie do stawek jak w ruchu krajowym

   Zjawisko nosi znamiona nadużycia z wykorzystaniem stawek PSI. Podobieństwo między tymi nadużyciami wynika z faktu, że OPL identyfikuje przypadki ingerowania przez operatorów w przesyłany numer Abonenta wywołującego A dla połączeń pochodzenia międzynarodowego i jest to ten sam schemat – a wynika z różnicy stawek. Nadużycie z wykorzystaniem rozliczeń PSI polega na zakańczaniu w sieci stacjonarnej OPL międzynarodowych połączeń głosowych inicjowanych za granicą z wykorzystaniem hurtowej usługi zakańczania połączeń w sieci OPL za pomocą PSI. Operatorzy zaangażowani w proceder zmieniają numerację zagranicznego abonenta wywołującego A na numer krajowy KNA, aby następnie połączenia głosowe zakończyć jako krajowe na wiązkach PSI przeznaczonych wyłącznie do wymiany ruchu krajowego – szczegółowo zostało to opisane i wyjaśnione w decyzja Prezesa UKE o uchyleniu rozliczeń PSI w relacji ETelko-OPL:

http://www.telko.in/uke-zablokowal-e-telko-terminacje-po-plaskich-stawkach;
http://www.telko.in/files/files/DHRT.WWM.6080.7.2016.0_e-Telko_Orange_PSI.pdf.

7. Generowanie połączeń na numery zagraniczne IRSF (ang. International Revenue Share Fraud
8. Podszywanie się pod dowolny numer telefoniczny za pośrednictwem portali internetowych

   Możliwość zafałszowania numeru może być wykorzystana do działań przestępczych (karalnych gróźb, rozbójniczych wymuszeń, anonimowych oszustw, działań terrorystycznych). Proceder podważa także wartość dowodową bilingów telefonicznych, gdyż fałszywy numer widnieje także na bilingu.

   Proceder jest możliwy z powodu luki w ustawie Pt, (która polega na tym, że przepis mówiący o tym, że numer telefonu musi być taki sam na całej drodze połączeniowej nie mówi jednocześnie o tym, że musi być on prawdziwy). Wobec tego potrzebna jest pogłębiona analiza jak powinny brzmieć przepisy zabraniające dokonywania nadużyć za pomocą podmiany numeru, z którego inicjowane połączenie telefoniczne. Operatorzy już wcześniej sygnalizowali potrzebę takich przepisów oraz przepisów umożliwiających karanie za tego typu wykroczenia. Wskazane byłoby uzyskanie stanowiska oraz propozycji przedsiębiorców w tej sprawie. Jaki numer A powinien mieć abonent PABX.
9. Wykorzystywanie central PABX przez abonentów usługi call center

   Przykład 1:

   OPL zaobserwował wzrost połączeń z numeru w SN22 zakańczanych w sieci Orange w okresie jednego kwartału 2016. Według danych ze strony UKE numer należał do zakresu numeracji jednego z OA (tzw. listy Top Five Fruderów), a według danych ze strony www był to numer kontaktowy do Działu Obsługi Klienta tego OA. W wyniku interwencji OPL u operatorów tranzytujących ruch ostatecznie znikł. Połączenia z numeru zostały zakończone w sieci Orange łącznie w ilości około 12 milionów minut.

   Nadużycie w tym przypadku polegało na wykorzystaniu wymienionego numeru do tranzytowania ruchu międzynarodowego do OPL oraz zamianie informacji adresowej abonenta A wywołującego na numer Działu Obsługi Klienta tej firmy. Zdarzenia takie zostały potwierdzone w testach wykonywanych przez OPL.

   Przykład 2:

   Powszechne stało się już kierowanie ruchu przez nadużycie telekomunikacyjne związane ze świadczeniem usługi hurtowego dostępu do sieci OPL na Biurze Numerów.

   W wyniku prowadzonych analiz OPL identyfikuje, co chwila znacznie zwiększone wolumenu ruchu telekomunikacyjnego do usługi Ogólnokrajowe Biuro Numerów 118 913, inicjowane z numerów WLR należących do różnych operatorów.

   Operatorzy Alternatywni (OA) tranzytują połączenia od innych OA do usługi Ogólnokrajowego Biura Numerów świadczonej przez Orange, na warunkach przeznaczonych dla Abonentów WLR, uzyskując 40 % opust hurtowy w stawce za połączenia. Stwierdzono występowanie powiązań pomiędzy tymi firmami np. OA sprzedaje usługę telefoniczną WLR jakiemuś klientowi, który jest call-center a za tą firmą stoi ta sama

osoba z zarządu OA (obecnie po wykryciu takich przypadków te powiązania są rozpraszane).

Takie działania to już prowadzenie działalności telekomunikacyjnej w ramach umowy abonenckiej, co definitywnie jest niezgodne z prawem i musi być traktowane, jako nadużycie. Ze szczegółowej analizy połączeń wynika również, iż dochodzi do podmiany numeru abonenta A inicjującego połączenie do usługi Biura Numerów.

OPL przeprowadzał analizę wybranych połączeń przychodzących z numerów klienta WLR. Do standardowej rozmowy konsultantów było pytanie dotyczące sieci, z której dzwoni abonent A oraz przeprowadzono rejestrację takiej rozmowy. Analiza dała możliwość ustalenia rzeczywistego źródła połączenia (sieci inicjującej połączenie) i przypisania rzeczywistej sieci operatora do konkretnej rozmowy.

10. Wyłudzanie telekodów

    Nadużycie typu prześlij Twój kod zasilający kartę, to podwoimy Ci ilość środków na koncie skutkuje doładowaniem obcej karty np. do połączeń na numery Premium.

11. Malware

    Złośliwe oprogramowanie (wirusy, trojany) na smartfony i tablety. np. zamieniające numer konta bankowego w schowku i kradzież pieniędzy.

12. Wangiri (one ring one cut)

    Urywany sygnał wywołania, który ma spowodować, żeby abonent oddzwonił na numer Premium Rate lub międzynarodowy przypominający do złudzenia numer krajowy.

13. Połączenia typu SPAM realizowane na drogich numerach Premium Rate

    Wysyłanie SMS, MMS (zdjęcia, pliki dźwiękowe), inicjowanie połączeń głosowych (IVR) z komunikatem typu – wygrałeś losowanie, aby odebrać nagrodę wyślij SMS, oddzwoń itp.

14. Kierowanie ruchu drogą okrężną

    Kierowanie ruchu okrężną drogą przez inne kraje z uwagi na spłaszczanie stawek w Europie do stawek jak w ruchu krajowym.
    Można przyjąć, że temat dotyczy podobnej sytuacji jak nadużycia związane z wykorzystaniem Płaskiej Stawki Interkonektowej.

15. Kradzież rachunku ze skrzynki

    Następnie skanowanie, podstawienie fałszywego numeru konta i podrzucenie z powrotem do skrzynki wydruku podmienionej faktury.

16. Używanie skradzionych kart do wykonania dużego wolumenu ruchu.

Operatorzy przedstawili podane niżej propozycje działań naprawczych w odniesieniu do następujące nadużyć telekomunikacyjnych:

1. Wyłudzanie od operatorów sprzętu o dużej wartości oraz kart SIM na sfałszowane dokumenty

   Nadużycie polega na podpisywanie umów na sfałszowane dokumenty z intencją nieopłacania faktur. Operatorzy wnioskowali o możliwość weryfikacji online prawdziwości danych abonenta w bazach Dowodów Osobistych, PESEL, zastrzeżonych dokumentów

Ministerstwa Cyfryzacji w czasie transmisji danych (dane prawdziwe/dane nieprawdziwe). Obecnie na potwierdzenie danych w postaci papierowej Operator musi oczekiwać ponad tydzień, co uniemożliwia zastosowanie tego trybu w procesie weryfikacji potencjalnych klientów.

2. Zmienianie numeru IMEI w urządzeniach abonenckich

   Nadużycie skutkuje zafałszowaniem danych bilingach lub zupełnym ich brakiem. Operatorzy wnioskowali o wprowadzenie prawnego zakazu zmiany numerów IMEI urządzeń mobilnych. Z powodu manipulowania numerami IMEI przez przestępców podmioty uprawnione (Policja, Prokuratura) powinny w swych analizach stosować pary unikalnych numerów IMSI i IMEI.

3. Klonowanie kart SIM

   Nadużycie dotyczy kart starego typu z algorytmem COMP128-v1, nowsze karty z algorytmem COMP128-v2 są lepiej zabezpieczone. Operatorzy wnioskowali o zakazanie z mocy prawa zmiany klonowania numerów SIM.

4. Nadpisywanie adresu abonenta A w wiadomości SMS

   Nadpisy zdefiniowane na stałe są uregulowane, operatorzy mają umowy z klientami na dynamiczne nadpisywanie, które jest realizowane poprzez dostęp klientów do MSC.

   W związku z brakiem regulacji dotyczących weryfikacji nadpisów w połączeniach przychodzących na styku międzyoperatorskim, operatorzy podkreślali potrzebę uregulowań prawnych w zakresie nadpisywania adresu A w wiadomości SMS. Jakkolwiek jest to problem jest istotny, to jednak trudny do rozwiązania ponieważ wymaga uzgodnień międzyoperatorskich.

5. Podmiana numeru abonenta A

   Nadużycie zaczyna stanowić duży problem w związku z wprowadzeniem znacznych różnic w stawkach MTR wewnątrz UE i poza UE. Numery są podmieniane w sposób uniemożliwiający wykrycie takich działań. Staje się to możliwe dopiero, gdy zostanie popełniony błąd w zamianie numeru abonenta A. Operator obserwuje w ruchu przychodzącym dziwne zjawiska, mogące świadczyć o zmianach numeru przez operatorów lub pośredników, które z punktu finansowego nie mają sensu – np. ruch przychodzący z Czech prezentuje się numerami niemieckimi, a powinien czeskimi.

   Operatorzy postulowali prawne ograniczenie możliwości zmiany w łańcuchu połączeniowym numeru abonenta A oraz wprowadzenie sankcji karnych wzorem innych krajów (w Portugalii, Zimbabwe i Ghanie) (punkt 8.2), których dotknął ten problem.

4.3 Sposoby działania sprawców nadużyć zidentyfikowane przez operatorów

Przedsiębiorcy telekomunikacyjni przedstawili też sposoby działania sprawców nadużyć simboxów, które staje się coraz bardziej wyrafinowany.

1. Banki kart (powiązane z modemami) znajdują się w innych lokalizacjach niż same modemy umożliwiające przesyłanie danych między dwoma urządzeniami radiowymi. Zlokalizowanie urządzeń nadawczych w jednym miejscu pozwala na zablokowanie nadużycia w danej lokalizacji, ale nie rozwiązuje problemu zablokowania nadużycia całkowicie. W razie

wykrycia modemów są one automatycznie resetowane, co powoduje zerwanie połączenia z bankiem SIM i uniemożliwia jego lokalizację.

2. Bank SIM może obsługiwać naprzemiennie wiele lokalizacji w danym kraju, chociaż sam może znajdować się w innym kraju, co utrudnia jego wykrycie.
3. Połączenia są generowane z modemów radiowych znajdujących się w różnych lokalizacjach (w promieniu, nawet do 300 km).
4. Jednocześnie stosowane są zmiany IMEI w celu tworzenia nowych par IMSI-IMEI w systemach sieci komórkowych, co daje wrażenie kolejnego logowania się różnych abonentów. Modemy radiowe są identyfikowane numerem IMEI, a karty SIM numerem IMSI.
5. Zmiana przypisania kart SIM do poszczególnych modemów odbywa się zgodnie z regułami mobilności, co ma symulować korzystanie z karty SIM przez abonenta wyposażonego w telefon mobilny. Kiedyś były to kolejne numery IMEI, a obecnie są stosowane rzeczywiste numery, co utrudnia wykrycie nadużycia.
6. W celu utrudnienia wykrycia pośrednicy tranzytujący ruch telefoniczny przesyłają legalną drogą 98% połączeń, a jedynie 2% poprzez FCT, co powoduje, że działania trudne są do wykrycia.
7. Sprawcy nadużyć korzystają przeważnie z sieci GSM (2G), ponieważ dysponują sprzętem FCT starszej generacji, który eksploatują tak długo, jak się da.
8. Przestępcy klonują starsze karty SIM sprzed 2000 r., bo są podatne na klonowanie.

W trakcie przeprowadzanych konsultacji operatorzy nie zgłaszali propozycji zmian w swoich ofertach i umowach. Wskazywali, że niekorzystne dla nich są płaskie stawki, ale ta sytuacja została spowodowana przez rynek i nie widzą od niej odwrotu. Nie informowali jakie stosują procedury i progi, od których następuje blokowanie karty SIM.

Operatorzy poinformowali, że stosują systemy wykrywania simboxingu i zatrudniają w tym celu zewnętrze podmioty, ale nie udzielili bliższych informacji na ten temat.

4.4 Przypadek simboxingu w sieci operatora Orange Polska

W sieci operatora Orange Polska został zidentyfikowany przypadek simboxingu, którym były wykorzystywane wiązki łączy krajowych z płaską stawką interkonektową PSI do transferowania ruchu przychodzącego z zagranicy. Mechanizm realizacji tego nadużycia opisano na podstawie informacji zawartych w decyzji Prezesa UKE w sprawie umowy pomiędzy Orange i e-Telko [11]. Opisany poniżej przypadek jest jednym z wielu, jakie miały miejsce w sieci Orange i były spowodowane transferowaniem połączeń z zagranicy z naruszeniem zasad dotyczących PSI.

4.4.1 Sposób rozliczania ruchu wg płaskiej stawki interkonektowej

Płaska stawka interkonektowa PSI dotyczy rozliczania połączeń telefonicznych pomiędzy Orange i innymi operatorami sieci stacjonarnych w kraju. Rozliczenia z operatorem e-Telko w oparciu o PSI nie dotyczyły ruchu międzynarodowego, połączeń do numerów, na których świadczone są usługi sieci inteligentnej, do numerów AUS, do numerów 20x oraz ruchu inicjowanego z zagranicy. Działania takie miały na celu zapobieżenie spekulacyjnemu obrotowi ruchem telekomunikacyjnym czy też korzystaniu z usług międzyoperatorskich na zasadach rozliczeń ryczałtowych w celach

innych niż świadczenie usług detalicznych abonentom własnej sieci. Działanie takie miało również pozwolić na uniknięcie nieefektywnego wykorzystania wiązek, a także na uniknięcie nadmiernego wzrostu obciążeń kosztowych dla Orange.

4.4.2 Nadużycia spowodowane zakańczaniem połączeń międzynarodowych jako połączeń krajowych wg stawki PSI

Według operatora Orange obecnie występują w sposób regularny i zorganizowany zdarzenia polegające na zakańczaniu w sieci OPL międzynarodowych połączeń głosowych inicjowanych za granicą, jako połączeń krajowych. Występuje też celowe rozpraszanie ruchu na numeracji i kierowanie tego ruchu przez sieci innych operatorów (tranzytem) co ma świadome ukrycie skali i źródła pochodzenia ruchu. Obecnie np. prawidłowy ruch krajowy (bez podmienionego numeru A) przychodzi bezpośrednio na wiązki PSI, zaś nieprawidłowy ruch prezentujący się numeracją podmienioną jest zakańczany poprzez tranzyt i wiązki PSI innych operatorów.

Operatorzy zaangażowani w proceder simboxingu zmieniają numerację zagranicznego abonenta wywołującego A na numer krajowy A, a następnie kończą połączenia głosowe jako krajowe na wiązkach PSI przeznaczonych wyłącznie do wymiany ruchu krajowego. Wprowadzenie celowej zamiany numeru A ma na celu dodatkowe zatarcie śladów źródła pochodzenia ruchu oraz utrudnienie jakikolwiek działalności kontrolnej organom państwowym. Do operatorów którym Prezes UKE udowodnił już taką praktykę dołączają kolejni przedsiębiorcy telekomunikacyjni.

Nadużyciom sprzyja swobodne pozyskiwanie i udostępnianie numeracji, na której nie ma abonentów a która bardzo często służy do podmiany numerów. Brak w decyzjach o przydziale numeracji sposobu użytkowania przydzielonych zakresów numeracyjnych oraz zasad udostępniania ich podmiotom trzecim (np. wskazanie wprost sankcji za naruszenie tych zasad) jest sytuacją sprzyjającą zmianie informacji adresowej. Optymalnym rozwiązaniem byłby zakaz udostępniania numeracji podmiotom trzecim przez operatorów, co wymagałoby zmiany Pt.

4.4.3 Przypadek nadużyć ze strony operatorów grupy kapitałowej Polish Servies Group S.A przy tranzycie połączeń międzynarodowych

Operator Orange zaobserwował, że w połączeniach międzynarodowych kierowanych przez E-Telko do jego sieci numeracja widoczna przy terminowaniu połączeń w punkcie styku sieci Orange z E-Telko nie jest numeracją pierwotną, z której inicjowane są połączenia telefoniczne. Oznacza to, że w połączeniach głosowych inicjowanych poza granicami Polski następuje ingerencja w format przesyłanej numeracji i poinformował o tym Prezesa UKE. Okoliczność ta spowodowała uzasadnione podejrzenie, że przy terminowaniu ruchu na wiązki PSI jeden z operatorów uczestniczących w łańcuchu podmiotów terminujących połączenie i współpracująca z nim E-Telko dokonuje podmiany numeru pierwotnego na numer krajowy, co jest niezgodne z warunkami Umowy i przepisami prawa krajowego.

Połączenia międzynarodowe kierowane do sieci Orange za pośrednictwem E-Telko były terminowane z wykorzystaniem krajowej numeracji VoIP przydzielonej przez Prezesa UKE, na mocy odpowiednich decyzji administracyjnych. Taka sytuacja miało miejsce także w przypadku innych operatorów krajowych. W przypadku E-Telko numeracja ta należała do TeleTTR, przedsiębiorcy telekomunikacyjnego będącego częścią grupy kapitałowej Polish Servies Group S.A., do której należy również E-Telko. Okoliczność ta powodowała uzasadnione podejrzenie, że w czasie wymieniany ruchu telekomunikacyjnego z spoza terenu kraju (ramach podmiotów

działających w tej grupie) dochodzi do celowej podmiany numeru abonenta A w celu zakwalifikowania tych połączeń na wiązkach PSI jako połączeń krajowych.

W związku z zaistniałą sytuacją Prezes UKE przeprowadził czynności wyjaśniające z zastosowaniem narzędzi służących do sprawdzania i weryfikacji ruchu telekomunikacyjnego kierowanego na wiązki PSI do sieci Orange przez E-Telko. Głównym narzędziem weryfikacyjnym służącym do kontroli i analizy ruchu tranzytowanego było porównanie oraz analiza umów z operatorami krajowymi i zagranicznymi oraz danych bilingowych udostępnionych przez przedsiębiorców telekomunikacyjnych uwikłanych w proceder, w szczególności:

- rekordów CDR zarejestrowanych na wejściu systemu telekomunikacyjnego TeleTTR (ze zmienionym numerem międzynarodowym na numer krajowy abonenta A inicjującego połączenie za granicą) z podziałem na ruch międzynarodowy od poszczególnych operatorów zagranicznych,
- rekordów CDR na wyjściu systemu telekomunikacyjnego TeleTTR z podziałem na ten sam ruch co wejściowy kierowany do poszczególnych operatorów krajowych (w tym E-Telko),
- rekordów CDR w zakresie zarejestrowanego ruchu przychodzącego do systemu teleinformatycznego E-Telko z sieci TeleTTR,
- rekordów CDR w zakresie ruchu wychodzącego z systemu teleinformatycznego E-Telko do sieci Orange i rozliczanego w oparciu o PSI (tego samego ruchu co ruch przychodzący),
- umów zawartych przez TeleTTR z przedsiębiorcami krajowymi i zagranicznymi dotyczących wymiany ruchu telekomunikacyjnego,
- umów zawartych przez TeleTTR z przedsiębiorcami zagranicznymi, na podstawie których przesyłają oni zagraniczny ruch telekomunikacyjny do sieci TeleTTR.

Uwaga. Rekordy CDR zawierały informacje służące do naliczenia opłaty za usługę telekomunikacyjną m. in. takie jak: numer telefonu, z którego zainicjowano połączenie (numer abonenta A), numer telefonu, na który zestawiono połączenie, datę i czas zainicjowania połączenia, datę i czas trwania połączenia, informacje o dodatkowych usługach, które były wykorzystane podczas zestawiania i trwania rozmowy, informacje o taryfie oraz inne.

Po przeanalizowaniu zebranego materiału przez Prezesa UKE okazało się, że podmiany numeru abonenta A dokonywała firma OnTel BVBA, będąca podmiotem kooperującym z TeleTTR. Mechanizm podmiany polegał na tym, że informacja adresowa o numerze abonenta wywołującego była zmieniana poprzez oznakowanie numerami przydzielonymi TeleTTR wiodących wiązek łączy międzycentralowych łączących systemy telekomunikacyjne operatorów zagranicznych z systemem telekomunikacyjnym TeleTTR.

Ruch telekomunikacyjny ze zmienioną informacją adresową kierowany był następnie do sieci E-Telko, a stamtąd tranzytowany do sieci Orange przez wiązki PSI, co powodowało nieprawidłowości w funkcjonowaniu usługi świadczonej dla E-Telko przez Orange i rozliczanej w oparciu o PSI. W szczególności nieprawidłowości te dotyczyły rozliczeń międzynarodowego ruchu telekomunikacyjnego tranzytowanego przez operatorów zagranicznych do sieci TeleTTR, a następnie zakańczanego przy pomocy operatorów krajowych (w tym E-Telko) u abonentów przyłączonych do sieci Orange w oparciu o łącza z PSI. Oznaczenie wiodących wiązek łączy międzycentralowych łączących systemy telekomunikacyjne operatorów zagranicznych z systemem telekomunikacyjnym TeleTTR numerami przydzielonymi TeleTTR modyfikowało informację

zawartą w sygnalizacji SIP o źródle inicjującym połączenie. Proceder ten umożliwia E-Telko zakwalifikowanie nieuprawnionego ruchu telekomunikacyjnego pochodzącego z zagranicy na wiązki PSI przeznaczone wyłącznie do wymiany ruchu krajowego.

Ponadto w toku prowadzonego postępowania wyjaśniającego w TeleTTR i E-Telko stwierdzono, iż ruch telekomunikacyjny przychodzący z zagranicy był tranzytowany przez sieć telekomunikacyjną TeleTTR do sieci także innych operatorów krajowych. Z powodu zmiany informacji adresowej o numerze abonenta wywołującego A, kwalifikowany był przez tych operatorów jako ruch krajowy i terminowany w sieci Orange na wiązkach łączy z zastosowaniem PSI.

4.4.4 Działania podjęte przez operatora Orange Polska w celu zwalczania nadużyć

W ramach zwalczania negatywnych zjawisk występujących w sieciach telekomunikacyjnych operator Orange Polska S.A. (OPL) podejmował działania zapobiegawcze polegające na składaniu pism, zawiadomień i informacji do właściwych organów i instytucji.

OPL przekazał Prezesowi UKE pisma w sprawie SIM-BOX (FCT, rozliczeń PSI i sztucznego ruchu, w tym:

- pisma o interwencję oraz blokowanie ruchu na podstawie regulaminów świadczenia usług w związku z SIM-BOX (FCT,
- pisma w sprawie rozliczeń PSI o interwencję u Operatorów dokonujących zmiany informacji adresowej ruchu międzynarodowego na krajowy i rozliczania na PSI oraz wnioski o uchylenie rozliczeń PSI (brak możliwości blokowania ruchu na bazie zapisów decyzji UKE).
- pisma o interwencję oraz blokowanie ruchu na podstawie regulaminów świadczenia usług z powodu sztucznego ruchu.

Zdaniem operatora w większości przypadków nie były podjęte działania ze strony UKE w związku ze zgłaszanymi nieprawidłowościami.

OPL składał zawiadomienia do Prokuratury o możliwości popełnienia przestępstwa przez podmioty uczestniczące w nadużyciu (w większości umarzane). OPL zaleca wystąpienie w trybie informacji publicznej do Prokuratury Krajowej o podanie informacji ile takich spraw zakończyło się postawieniem zarzutów jakimkolwiek podmiotom.

OPL przekazał informacje do ABW o naruszeniu przez przedsiębiorców wypełniania obowiązków na rzecz obronności, bezpieczeństwa Państwa oraz bezpieczeństwa i porządku publicznego.

Zdaniem operatora, przykładowe na 20 złożonych zawiadomień o możliwości popełnienia przestępstwa związanego z simboxem nie zostały podjęte żadne działania ze strony prokuratury.

5. Przegląd działań instytucji krajowych poświęconych zwalczaniu simboxingu

Problemy z nadużyciami telekomunikacyjnymi (fraudami) są wyzwaniem na rynku telekomunikacyjnym dla działań regulacyjnych, ale brak działań w tym zakresie i sankcji powoduje, że zjawisko utrzymuje się zarówno na rynku detalicznym jak i hurtowym. Zachętą do nadużyć są atrakcyjne oferty usług telekomunikacyjnych (np. oferty no limit), asymetria stawek międzyoperatorskich, nieprecyzyjne zapisy prawa lub ich brak.

5.1 Wprowadzenie ustawowego obowiązku rejestracji przedpłaconych kart SIM

Z inicjatywy Rządu została uchwalona przez Sejm ustawa antyterrorystyczna, która zaczęła obowiązywać od lipca br. Jednym z celów tej ustawy jest zabronienie używania anonimowych numerów telefonów z tzw. kart przedpłaconych (pre-paid SIM). Ustawa wprowadza obowiązek imiennej rejestracji zakupu przedpłaconych kart SIM, co może ograniczyć nabycie dużej liczby kart przez jedną osobę.

Na mocy tej ustawy, przy zakupie karty SIM, obywatele naszego kraju wzorem społeczeństwa innych krajów Unii Europejskiej muszą podać imię, nazwisko i PESEL albo serię i numer dokumentu tożsamości, a cudzoziemcy spoza Wspólnot – numer paszportu lub karty pobytu. W przypadku zakupu telefonu na firmę konieczne jest podanie nazwy firmy oraz numeru REGON, NIP, lub KRS, a w przypadku prowadzenia działalności gospodarczej przez osobę fizyczną – numeru wpisu do ewidencji działalności gospodarczej

Każdy operator będzie mógł sprawdzić liczbę zakupionych kart przez abonentów w jego sieci. Ruch generowany przez numery powiązane z tymi kartami jako podejrzanymi może podlegać szczegółowej obserwacji.

5.2 Propozycje regulacji zgłoszonych przez Prezesa UKE

W związku z występowaniem niekorzystnych zjawisk w sieci krajowej Urząd Komunikacji Elektronicznej opublikował w dniu 13 listopada 2013 r. Stanowisko Prezesa Urzędu Komunikacji Elektronicznej w zakresie nadużyć telekomunikacyjnych w tym zjawiska generowania sztucznego ruchu telekomunikacyjnego wraz z aneksem zawierającym propozycje referencyjnych zapisów regulujących kwestie dotyczące przeciwdziałaniu nadużyciom telekomunikacyjnym (**https://www.uke.gov.pl/stanowisko-wobec-naduzyc-telekomunikacyjnych-13068**). W opinii Prezesa UKE zapisy takie powinny zostać wprowadzane na drodze cywilnoprawnych aneksów, zawieranych do umów o dostępie telekomunikacyjnym w zakresie połączenia sieci.

Aneks dotyczący przeciwdziałania nadużyciom opiera się na kilku założeniach:

- „skonkretyzowanych definicjach zjawisk nadużycia telekomunikacyjnego i sztucznego ruchu,
- możliwości zablokowania połączeń telefonicznych związanych z nadużyciem telekomunikacyjnym dopiero po uzyskaniu zgody drugiej strony umowy,
- określeniu terminów umożliwiających wyjaśnianie sytuacji dotyczących nadużyć telekomunikacyjnym,
- nie wstrzymywaniu płatności w związku z podejrzeniem nadużycia telekomunikacyjnego,
- zobowiązaniu stron do naprawienia szkód wynikłych z powodu nadużycia telekomunikacyjnego,

- ustaleniu trybu w jakim będzie pracował zespół roboczy badający sporne przypadki w zakresie nadużyć telekomunikacyjnych".

Aneks zawiera 6 artykułów oraz definicje nadużycia telekomunikacyjnego i sztucznego ruchu.

Artykuł 1 zobowiązuje strony do podejmowania działań zmierzających do wykrywania i przeciwdziałania zjawiskom Sztucznego Ruchu i Nadużycia Telekomunikacyjnego występujących w ich sieciach telekomunikacyjnych, w szczególności w zakresie opisanym w Artykule 3.

Artykuł 2 stanowi, że:

- „w przypadku wątpliwości, czy określone zjawisko jest generowaniem Sztucznego Ruchu bądź Nadużyciem Telekomunikacyjnym, strona może zwrócić się z zapytaniem do przedstawiciela drugiej strony o interpretację, wskazując jednocześnie własną interpretację danego zjawiska,
- strona zobowiązuje się do bezzwłocznego udzielenia odpowiedzi na otrzymane zapytanie,
- w przypadku uznania przez stronę zapytaną interpretacji strony pytającej za prawidłową, strony dokonają odpowiedniej korekty faktur,
- strony zobowiązane są do usunięcia wspólnie skutków Nadużycia Telekomunikacyjnego".

Artykuł 3 zobowiązuje strony do:

- „nie angażowania się w inicjowanie, tranzyt lub zakańczanie ruchu mającego cechy Sztucznego Ruchu bądź w działania mające cechy Nadużycia Telekomunikacyjnego,
- nie ułatwiania innym przedsiębiorcom lub abonentom inicjowania, tranzytu lub zakańczania ruchu mającego cechy Sztucznego Ruchu,
- nie podejmowania działania sprzyjającego Nadużyciom Telekomunikacyjnym,
- nie zatajania przed drugą stroną wiedzy o inicjowaniu, tranzycie lub zakańczaniu ruchu mającego cechy Sztucznego Ruchu, o ile działanie to dotyczy lub może dotyczyć drugiej strony lub rozliczeń tej strony prowadzonych z innymi przedsiębiorcami telekomunikacyjnymi lub abonentami,
- dochowania należytej staranności w zakresie wykrywania, identyfikacji, zapobiegania, analizy, powiadamiania drugiej strony oraz w zakresie podejmowania czynności zmierzających do wyeliminowania zjawisk mających cechy Nadużycia Telekomunikacyjnego,
- zapewnienia dochowania należytej staranności przez osoby trzecie, którymi strony posługują się w wykonaniu swoich zobowiązań w wyżej wymienionym zakresie,
- monitorowania wymiany ruchu w punktach styku sieci w celu identyfikacji zjawisk mających cechy Nadużycia Telekomunikacyjnego bądź zjawiska Sztucznego Ruchu, a w przypadku braku możliwości technicznych takiego działania, do wdrożenia funkcjonalności technicznej umożliwiającej taki monitoring".

W przypadku podejrzenia przez stronę, że określona usługa telekomunikacyjna może powodować występowanie nadużycia telekomunikacyjnego, artykuł 4 uprawnia stronę do blokowania połączeń na numery, na których świadczona jest ta usługa po uprzednim uzyskaniu zgody drugiej strony, co ogranicza działania poszkodowanego operatora.

W zależności od rodzaju nadużycia telekomunikacyjnego oraz adekwatnie i proporcjonalnie do jego wagi, blokada może mieć charakter czasowy lub stały.

Artykuł 5 stanowi, że podjęcie działań przewidzianych w niniejszym aneksie w związku z podejrzeniem wystąpienia bądź wystąpieniem zjawiska nadużycia telekomunikacyjnego, w tym także Sztucznego Ruchu, nie zwalnia stron z obowiązku zaspokojenia roszczeń wynikających z odpowiednich umów.

Artykuł 6 stanowi o powoływaniu zespołu ekspertów w celu przeprowadzenia analizy występowania niekorzystnych zjawisk. Analiza ma na celu potwierdzenie okoliczności powstania określonego zjawiska o charakterze nadużycia telekomunikacyjnego bądź sztucznego ruchu lub też okoliczności wskazującej na brak wystąpienia zdarzenia o takim o charakterze w sytuacji rozbieżności w interpretacjach, czy określone zjawisko jest generowaniem sztucznego ruchu bądź nadużyciem telekomunikacyjnym oraz w sytuacji zastosowania blokady połączeń.

Kierując się potrzebą poznania aktualnego stanowiska szeroko pojętego rynku telekomunikacyjnego, w dniach od 12 sierpnia do 12 września 2013 r. Prezes UKE przeprowadził konsultacje środowiskowe projektów opublikowanych dokumentów.

W dniu 13 listopada 2013 r. Prezes UKE opublikował uwagi zaprezentowane przez przedsiębiorców telekomunikacyjnych oraz Izby gospodarcze jakie wpłynęły w toku konsultacji do Urzędu wraz ze szczegółowym i merytorycznym odniesieniem się do kwestii podnoszonych w złożonych dokumentach.

5.3 Propozycje PIIT w zakresie zmian prawnych zgłoszonych przez Prezesa UKE

Izba podziela opinię Prezesa UKE, że nadużycia telekomunikacyjne, związane głównie z uzyskiwaniem nieuprawnionych korzyści finansowych, stanowią zjawiska zagrażające rozwojowi rynku i równoprawnej oraz skutecznej konkurencji.

Wg PIIT w nadużyciach i oszustwach telekomunikacyjnych wykorzystywany jest brak uregulowań prawnych, asymetria rozliczeń międzyoperatorskich, brak odpowiednich obowiązków regulacyjnych, różnego rodzaju oferty detaliczne i liczne promocje dla użytkowników itd. Taka działalność telekomunikacyjna jest tylko z pozoru legalna w świetle prawa. W rzeczywistości nie ma nic wspólnego z przyjętymi w obrocie gospodarczym regułami i dobrymi zwyczajami i jest nastawiona wyłącznie na cel biznesowy - odniesienie nieuzasadnionych korzyści materialnych oraz wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu działającemu „fair”.

5.3.1 Zagrożenia wynikające z nadużyć telekomunikacyjnych wskazane przez Izbę

Izba widzi następujące zagrożenia powodowane nadużyciami występującymi w sieci krajowej:

1. Straty Skarbu Państwa z tytułu niezapłaconych podatków oraz wyłudzeń.

   Działalność oszustów telekomunikacyjnych jest „utajniona” i podmioty ją prowadzące nie wykazują dochodów podlegających opodatkowaniu z tytułu działalności telekomunikacyjnej lub też wykazują duże dochody w celu wyłudzenia podatku VAT (karuzela podatkowa).

2. Brak wypełniania obowiązków na rzecz obronności, bezpieczeństwa Państwa oraz bezpieczeństwa i porządku publicznego.

   W wyniku oszustwa przez SIM-BOX operatorzy telekomunikacyjni nie są w stanie przedstawić prawdziwych i kompletnych informacji o tym, kto faktycznie dzwonił na podany numer.

Operatorzy nie są w stanie zagwarantować prawidłowego wykonania kierowanych przez uprawnione organy państwowe wezwań do przedstawienia niezbędnych danych retencyjnych.

3. Naruszenie zasad przetwarzania danych objętych tajemnicą telekomunikacyjną.

   Z terminowaniem połączeń wiąże się przetwarzanie danych transmisyjnych, w sytuacji, gdy podmiot ten dokonuje zmiany lub usunięcia numeru linii wywołującej, dochodzi do niedopuszczalnego przetworzenia tych danych.

4. Brak możliwości prezentacji identyfikacji zakończenia sieci.

   Operatorzy nie są w stanie spełnić wymogów wynikających z ustawy Pt, czyli prezentacji identyfikacji zakończenia sieci, z którego inicjowane jest połączenie. Następuje wprowadzenie w błąd również użytkownika końcowego, któremu operator na jego życzenie jest zobowiązany świadczyć usługę prezentacji identyfikacji linii wywołującej, przed dokonaniem połączenia. Naraża to operatora na odpowiedzialność cywilną wobec użytkownika sieci, oraz na odpowiedzialność administracyjną ze strony organu regulacyjnego. Niesie to również zagrożenia (organizacje przestępcze, terroryzm).

5. Przestępstw przeciwko ochronie informacji.

   Przestępstwo z art. 268 § 1 ustawy Kk polegające na niszczeniu, uszkadzaniu, usuwaniu lub zmianie zapisu istotnej informacji albo w inny sposób udaremnianie lub znaczne utrudnianie osobie uprawnionej zapoznanie się z nią, przez osoby do tego nieuprawnione - przestępstwo polegające na zmianie numeru telefonicznego linii wywołującej i zastępowanie go innym numerem.

6. Pogorszenie jakości świadczonych usług telekomunikacyjnych.

   Przeciążenie sieci telekomunikacyjnej w miejscu funkcjonowania firm zajmujących się terminowaniem połączeń przez SIM-BOX oraz spadek satysfakcji klientów z powodu tendencji do obniżania jakości usług i spadku wskaźników SLA.

7. Możliwość używania simboxów przez organizacje przestępcze i terrorystyczne.

   Zagraża bezpieczeństwu publicznemu. Bezpieczny kanał komunikacji dla organizacji przestępczych czy terrorystycznych, w znacznym stopniu utrudnia inwigilację i przeciwdziałanie aktom terrorystycznym.

8. Wprowadzenie zamiany numeru wywołującego A.

   Celowe zatarcie śladów źródła pochodzenia ruchu oraz utrudnienie jakiejkolwiek działalności kontrolnej organom państwowym.

5.3.2 Propozycje uszczegółowienia definicji nadużyć

W ocenie PIIT, „definicja nadużycia telekomunikacyjnego jest niepełna, bo nie zawiera wyszczególnionych przykładów, które określą, co strony rozumieją przez nadużycie telekomunikacyjne. Wprawdzie definicja wskazuje w szczególności, że chodzi o wykorzystanie usług telekomunikacyjnych niezgodnie z przeznaczeniem, jednakże brak dookreślenia pojęcia „niezgodnie z przeznaczeniem" może powodować spory interpretacyjne stron. W związku z powyższym Izba wnosi o zmianę definicji nadużycia telekomunikacyjnego" w propozycji Aneksu Antyfraudowego na następującą:

„Nadużycie telekomunikacyjne – jakiekolwiek nieuprawnione wykorzystanie usług telekomunikacyjnych, w sieciach Stron lub innych sieciach telekomunikacyjnych, przy zastosowaniu środków niezgodnych z prawem w dowolnym czasie i przez dowolną osobę lub urządzenie, którego głównym celem jest osiągnięcie korzyści majątkowych przez osoby/podmioty zaangażowane."

Wg PIIT „nadużycie telekomunikacyjne oznacza także taką działalność, która pomimo że nie narusza przepisów prawa i nie jest działaniem bezprawnym, Strony uznają, za niezgodną z dobrymi praktykami oraz zwyczajami handlowymi, w szczególności:

- wszelkie próby lub działania polegające na generowaniu Sztucznego Ruchu,
- przekierowania ruchu z innych sieci lub do innych sieci w celu sztucznego zwiększenia wolumenu ruchu wymienianego pomiędzy sieciami w tym zapętlanie połączeń telefonicznych,
- generowania połączeń ultra krótkich (połączenia inicjowane w celu wpłynięcia na systemy billingowe, a nie w celu skorzystania z usług telekomunikacyjnych),
- celowe przesyłanie sygnalizacji niezwiązanej ze świadczeniem usług,
- świadczenie usług telekomunikacyjnych na podstawie umów abonenckich (np. simboxing),
- wykorzystanie jakichkolwiek numerów bądź zakresów numeracji niezgodnie z ich przeznaczeniem, regulaminem świadczenia usług, regulaminem promocji bądź cennikiem usług obowiązujących u danego przedsiębiorcy telekomunikacyjnego."

Izba zgłosiła także uwagi do definicji Sztucznego ruchu podanej przez Prezesa UKE i zaproponowała zmianę definicji tego pojęcia w taki sposób, żeby rozszerzyć jego zakres, a przesłanki pozwalające na zakwalifikowanie danego ruchu jako Sztuczny były łatwiejsze do wykazania. PIIT proponuje następującą definicję tego pojęcia:

Sztuczny Ruch – rodzaj oszustwa telekomunikacyjnego polegającego na generowaniu określonej, (przez podmiot generujący), liczby połączeń, wywołań, SMS, MMS, WAPPush, kodów USSD (od jednego lub wielu numerów abonenckich do jednego lub grupy numerów), najczęściej wprowadzanych do sieci telekomunikacyjnej z wykorzystaniem urządzeń lub programów generujących połączenia, wywołania, SMS, MMS, WAPPush, kody USSD, mających na celu lub powodujących uzyskanie korzyści materialnych przez podmiot generujący lub osoby trzecie z nim współpracujące.

Zdaniem PIIT zakres definicji Sztucznego Ruchu zaproponowanej przez Prezesa UKE jest zbyt wąski, bo ogranicza zjawisko Sztucznego Ruchu jedynie do połączeń „wprowadzanych do sieci z wykorzystaniem urządzeń i programów mogących generować połączenia". Ponadto według tej definicji jest to ruch mający „(...) na celu jedynie jego zarejestrowanie na punkcie styku sieci stron bądź w platformie bilingowej w celu uzyskania nieuzasadnionych korzyści finansowych bądź wyrządzenia szkody." Takie sformułowanie definicji powoduje, że Strony w celu zakwalifikowania danego ruchu telekomunikacyjnego jako Sztuczny Ruch powinny jednoznacznie ustalić, że:

- dany ruch jest generowany z wykorzystaniem urządzeń i programów mogących generować połączenia,

- celem danego ruchu jest jedynie jego zarejestrowanie na punkcie styku sieci stron bądź w platformie bilingowej w celu uzyskania nieuzasadnionych korzyści finansowych bądź wyrządzenia szkody.

Izba uważa, że wykazanie powyższych przesłanek w ramach uzgodnień Stron może być trudne, bo strona, która odnosi korzyści ze Sztucznego Ruchu, może podnieść zarzut, iż nie można ustalić, jaki jest jedyny cel danego Ruchu oraz czy został on wygenerowany z wykorzystaniem urządzeń i programów, o których mowa w definicji. Wskutek tych komplikacji definicja zaproponowana przez Prezesa UKE może w znacznym stopniu ograniczyć skuteczność działań antyfraudowych podejmowanych na podstawie aneksu.

Ponadto, aby uszczegółowić definicję Sztucznego Ruchu i Nadużycia telekomunikacyjnego oraz aby móc stosować kryteria do oceny, czy dany ruch telekomunikacyjny może być wynikiem nadużycia, PIIT zaproponował dodanie do aneksu zapisów wskazujących czynniki, jakie strony powinny brać pod uwagę w tego typu analizie.

5.3.3 Propozycje korekty założeń

Odnośnie korekty faktur PIIT zwraca uwagę, że w Aneksie Prezesa UKE (artykuł 2) brakuje wskazania z jakiego tytułu taka korekta może następować, oraz że brakuje zapisów o wstrzymaniu płatności za generowany sztuczny ruch. Wg PIIT te sprawy należy doprecyzować, tym bardziej, że ten mechanizm został opisany w umowach na usługi Premium Rate 70X i usługi AUS z niektórymi operatorami. Zatem brak jest podstaw, by zrezygnować z tej formy bezpieczeństwa przed nadużyciami telekomunikacyjnymi.

Zdaniem PIIT zapis dotyczący uprawnienia do zablokowania połączeń na numery, na których uświadczona jest usługa mogąca powodować występowanie nadużyć (artykuł 4) jest niewystarczający, ponieważ nie określa, że fraudy są powodowane nieuprawnionym korzystaniem z usługi telekomunikacyjnej, oraz że jakiekolwiek nadużycie telekomunikacyjne powinno być eliminowane bez konieczności jednoczesnego wykazywania, że nadużycie wyniknęło z usługi telekomunikacyjnej.

Izba uważa, że zespół ekspertów ds. identyfikacji sztucznego ruchu i wykluczenia mechanizmu fraudowego (artykuł 6) powinna powoływać tylko jedna strona (ta, która zaobserwowała zjawisko nadużycia i uznała, że ruch który się pojawił jest wynikiem nadużycia), ponieważ przy powoływaniu takiego zespołu przez dwie strony może nie być to możliwe w sytuacji, gdy jedna ze stron nie wyrazi zgody.

5.3.4 Dodatkowe kwestie zgłoszone przez Izbę

Członkowie Izby wskazali, że w Aneksie brakuje kilku kwestii, które uznają za kluczowe w przypadku wystąpienia nadużyć telekomunikacyjnych, do których zaliczają:

a) rozliczenia wstępne,

b) prawo do wstrzymania zapłaty za sztuczny ruch,

c) wypowiedzenie umowy w zakresie połączenia sieci,

d) umieszczenie zapisów o nadużyciach w umowach z innymi podmiotami,

e) testy w sieciach Stron.

Ponadto Izba zwraca uwagę na konieczność podjęcia wspólnych działań dotyczących karuzeli podatkowej dla zwalczania oszustw związanych z podatkiem VAT. Złożony system rozliczeń sprzyja dokonywaniu oszustw podatkowych związanych z uchylaniem się od podatku, czy wyłudzaniem podatku VAT, z których najpoważniejszym obecnie są oszustwa karuzelowe. Mechanizm tego oszustwa składa się z wielu wariantów, przede wszystkim oszustwo typu znikający podatnik MTIC (ang. Missing Trader Intra-Community Fraud). Znikający podatnik to podmiot gospodarczy zarejestrowany, jako podatnik dla celów VAT, który nabywa towary lub usługi z potencjalnym zamiarem oszustwa, a następnie zbywa je z uwzględnieniem podatku VAT, nie przekazując należnego podatku do urzędu skarbowego.

Zdaniem Izby nadużycie telekomunikacyjne jest tak samo groźne jak każde inne oszustwo lub przestępstwo zagrożone karą kodeksu karnego i musi być tak samo piętnowane i ścigane. Operatorzy zrzeszeni w PIIT od dłuższego już czasu walczą z nadużyciami telekomunikacyjnymi i na własną rękę podejmując działania w tym zakresie. PIIT zwraca uwagę, że uczestnicy rynku telekomunikacyjnego podejmują konkretne rozwiązania w zakresie zwalczania nadużyć telekomunikacyjnych nie mając należytego wsparcia ze strony organów państwowych.

Propozycje rozwiązań legislacyjnych dla ukrócenia tego zjawiska znajdują się w dokumentach opracowanych przez UKE oraz PIIT, w szczególności w dokumencie:

- Aneks Prezesa UKE z13 listopada 2013 dotyczący przeciwdziałania nadużyciom
- Propozycje PIIT do Aneksu Antyfraudowego Prezesa UKE z 2013 (Aneks Antyfraudowy 2013 nie odpowiada na oczekiwania operatorów w zakresie zwalczania nadużyć): http://www.piit.org.pl/dokumenty/telekomunikacja/-/asset_publisher/ehjUfDM7quqd/content/piit-stanowisko-ws-projektu-stanowiska-prezesa-uke-w-zakresie-naduzyc-telekomunikacyjnych-konsultacje-aneksu-antyfraudowego)
- Propozycja PIIT do projektu rozporządzenia ws. szczegółowych wymagań dotyczących gospodarowania numeracją w publicznych sieciach telekomunikacyjnych, dotycząca kwestii nadużyć na numeracji i jej uregulowania: http://www.piit.org.pl/dokumenty/telekomunikacja/-/asset_publisher/ehjUfDM7quqd/content/piit-stanowisko-ws-projektu-rozp-maic-ws-szczegolowych-wymagan-dotyczacych-gospodarowania-numeracja-w-publicznych-sieciach-telekomunikacyjnych-art-126.

5.4 Podsumowanie propozycji UKE i PIIT

Działania na rzecz wyeliminowania lub ograniczenia różnych nadużyć telekomunikacyjnych proponowane przez Prezesa UKE, do których odniósł się w sposób wyczerpujący PIIT, należy uznać za krok w dobrym kierunku. W kwestiach, w których obydwie instytucje zajmują odmienne stanowiska, propozycje PITT są bardziej adekwatne do skali zagrożeń i szkodliwości tych negatywnych zjawisk. Chodzi tu zwłaszcza o sankcje w postaci wstrzymywania płatności za ruch, który jedna ze stron uznaje za sztuczny. Sankcja ta nie jest na tyle dotkliwa, aby nie można było jej zastosować w sytuacjach, w których są wątpliwości odnośnie do kwalifikacji zjawiska. Ewentualne rozbieżności w kwestii uznania ruchu za sztuczny mógłby rozstrzygać w drodze decyzji Prezes UKE.

Zdaniem PIIT nadużyciom i oszustwom telekomunikacyjnym sprzyjają takie właściwości polskiego rynku telekomunikacyjnego, jak

- brak uregulowań prawnych,
- brak nałożonych odpowiednich obowiązków regulacyjnych,
- asymetrię rozliczeń międzyoperatorskich,
- różnego rodzaju oferty detaliczne i liczne promocje dla użytkowników.

O ile pierwsze kwestię leżą w kompetencji ustawodawcy oraz MC i Prezesa UKE, to pozostałe mogą być rozwiązane przez samych operatorów i izby. Niemniej dotyczy tylko relacji pomiędzy operatorami krajowymi, natomiast większość nadużyć jest związania z ruchem międzynarodowym, na który krajowi operatorzy i PIIT nie mają wpływu. Potrzeba zatem działania na forum międzynarodowym, na rzecz uporządkowania rynku połączeń międzynawowych w celu ograniczenia tych szkodliwych zjawisk.

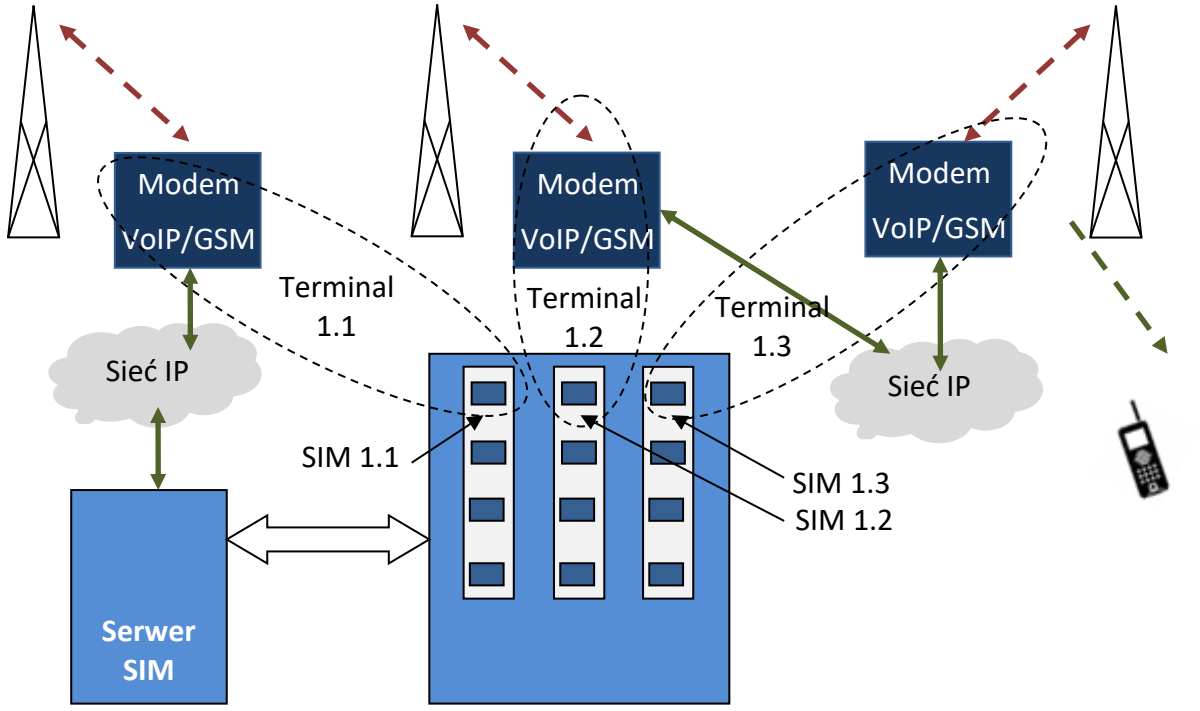
6. Simboxy oraz systemy służące do wykrywania zjawiska simboxingu

6.1 Simboxy - urządzenia służące do realizacji simboxingu

Urządzenia stosowane do uprawiania simboxingu, zwane też simboxami, są obecnie powszechnie dostępne na rynku, oferowane przez producenci jako produkt, którego koszt szybko się zamortyzuje i zapewni użytkownikowi stały, atrakcyjny dochód. Ich ceny, kształtująca się na poziomie od 500 do kilku tysięcy dolarów, są na tyle niskie, że coraz więcej podmiotów decyduje się na tego rodzaju działalność. Simboxy są wyposażone w coraz nowocześniejsze rozwiązania techniczne, które umożliwiają obejście szerokorozumianych systemów antyfraudowych stosowanych przez operatorów.

Wspólną cechą simboxów zaawansowanych technologicznie i funkcjonalnie jest ich architektura, która z reguły obejmuje 3 elementy (załącznik 2 punt 13):

- Modemy VoIP/GSM;
- Banki SIM;
- Server SIM.



Rysunek 6-1. Schemat działania simboxa rozproszonego.

Modem VoIP/GSM jest przeznaczony do fizycznego zakańczania w sieci GSM połączeń przychodzących z sieci IP przez bramkę VoIP w interfejsie radiowym. Modem pełni funkcję aparatu telefonicznego, który nie jest fizycznie wyposażony w kartę SIM.

Z reguły aparat plus karta SIM tworzą terminal w postaci jednego urządzenia, jednak zastosowanie tej reguły w simboxach uczyniłoby to urządzenie łatwym celem do namierzenia przez systemy antyfraudowe, gdyż w takim przypadku inicjowanie połączeń w sieci komórkowej odbywałoby się z

jednej lokalizacji, w sensie tej samej komórki (sektora) sieci. Aby uniknąć wykrycia każdy modem VoIP/GSM jest skomunikowany w sposób dynamiczny z kartami SIM zainstalowanymi w Banku SIM, w sensie przełączania pomiędzy kartami, tworząc z nimi terminale wirtualne. W przykładowej konfiguracji (Rysunek 6-1) karta SIM 1.1. - 1. rząd, 1. kolumna – w macierzy jest skomunikowana z pierwszym modem. Karta 1.2 – z drugim, a karta 1.3 – z trzecim, przy czym modemy są zalogowane do różnych komórek sieci.

Bank SIM zbudowany z macierzy inteligentnych gniazd SIM przeznaczonych do instalowanie kart SIM, z których każda może zostać skomunikowana lokalnie lub poprzez sieć IP z dowolnym modemem VoIP/GSM. Przełączanie kart pomiędzy modemami VoIP/GSM imituje ruch abonenta w sieci, nadając mu cechę mobilności i utrudniając wykrycie, które byłoby znacznie prostsze w przypadku terminala stacjonarnego.

Systemem zarządza **Serwer SIM**, m.in. zapewniając dynamiczną konfiguracją terminali wirtualnych. Użytkownik może zaprogramować trasę przemieszczania się wirtualnego terminala w sieci telefonii komórkowej. Wirtualna mobilność systemu sprawia, że praktyki simboxowe są trudne wykrycia i zlokalizowania, a tym bardziej do zwalczania.

Szerszy opis architektury oraz parametrów technicznych systemów służących do simboxingu zamieszczono w załączniku 2 punkt 13.

6.2 Systemy służące do wykrywania simboxingu

6.2.1 Procedury i wspomagające zwalczanie simboxingu

Operatorzy wdrażają procedury administracyjne i eksploatacyjne wspomagające wykrywanie i zwalczanie nadużyć telekomunikacyjnych, zwłaszcza zjawiska simboxingu. Na podstawie konsultacji z operatorami oraz publikowanych dokumentów zostały zidentyfikowanie takie działania, jak:

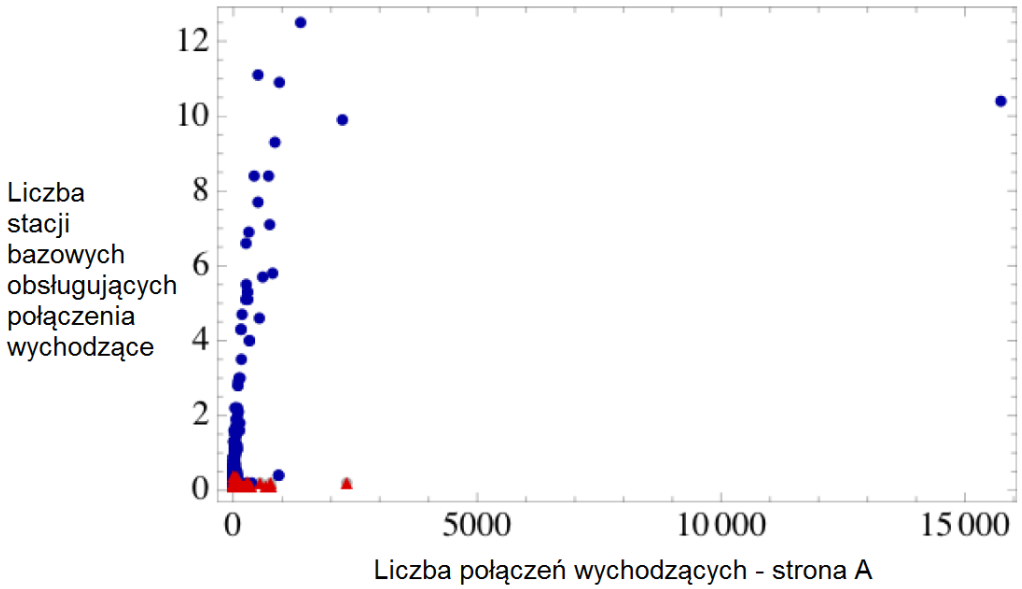
- monitorowanie sprzedaży przedpłaconych kart SIM;
- monitorowanie udziału abonentów z przedpłaconymi kartami SIM w ogólnej liczbie abonentów;
- zastrzeżenia w umowach z dystrybutorami dotyczące ograniczenia liczby kart SIM sprzedawanych jednorazowo;
- rejestracja przez Dział Obsługi Klienta skarg abonentów na jakość odbieranych połączeń międzynarodowych oraz przekazywanie tych danych do jednostki odpowiedzialnej poziom jakości usług.

Realizowane procedury stanowią istotnie uzupełnienie rozwiązań technicznych, dostarczając dane o ruchu w sieci, których analiza umożliwia identyfikację simboxów i innych szkodliwych praktyk.

W systemach technicznych wspomagających przeciwdziałanie zjawisku simboxingu wykorzystuje się algorytmy opracowane na podstawie analizy ruchu w sieciach mobilnych pod względem statystyki połączeń właściwej dla ruchu legalnego oraz ruchu pochodzącego w simboxów. Jedną z metod analitycznych jest detekcja fraudów w połączeniach międzynarodowych przy użyciu logiki rozmytej opisana w załączniku 1 – pkt 12.3, za pomocą której analizuje się dane o ruchu zawarte w rekordach CDR (ang. Call Data Record). Na bazie danych z rekordów CDR określono pięć wzorców wykrywania fraudów, w tym simboxingu:

- wysoka lub niska mobilność,
- stosunek liczby połączeń przychodzących do połączeń wychodzących,
- używanie wyłącznie usługi głosowej (bez SMS, MMS, GPRS, itp.),
- podejrzana aktywność w bliskim sąsiedztwie jednej komórki sieci,
- połączenia w nieregularnych godzinach, nietypowe długie rozmowy w nocy.

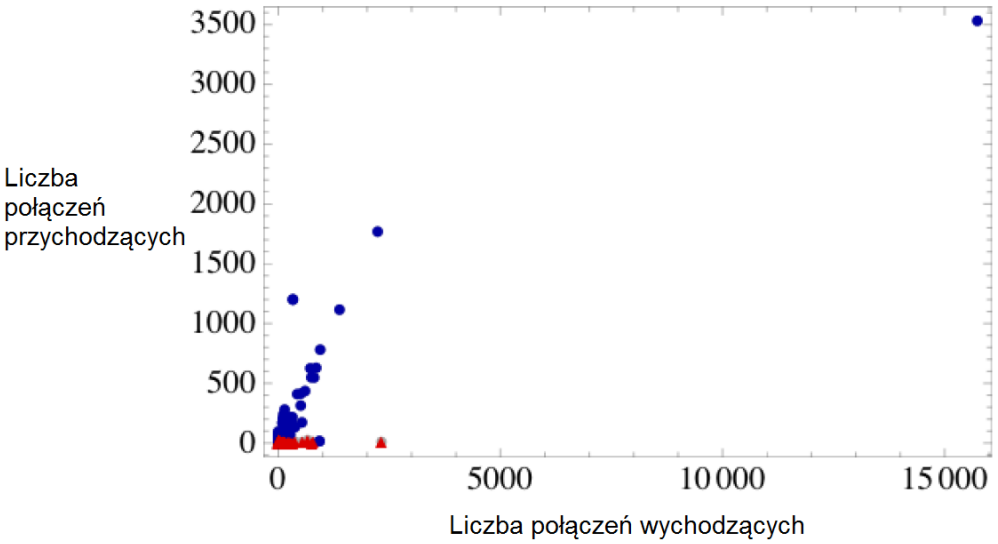
W pracy Analysis and Detection of SIMbox Fraud in Mobility Networks [12] opublikowano rezultaty analizy ruchu legalnego i nielegalnego (Rysunek 6-2 i Rysunek 6-3), gdzie niebieskie kropki odnoszą się do ruchu legalnego, zaś czerwone trójkąty do połączeń pochodzących z simboxów (Rysunek 6-4).



Rysunek 6-2. Zależność pomiędzy liczbą połączeń wychodzących a liczbą komórek sieci, z których były one inicjowane.

Źródło - Analysis and Detection of SIMbox Fraud in Mobility Networks

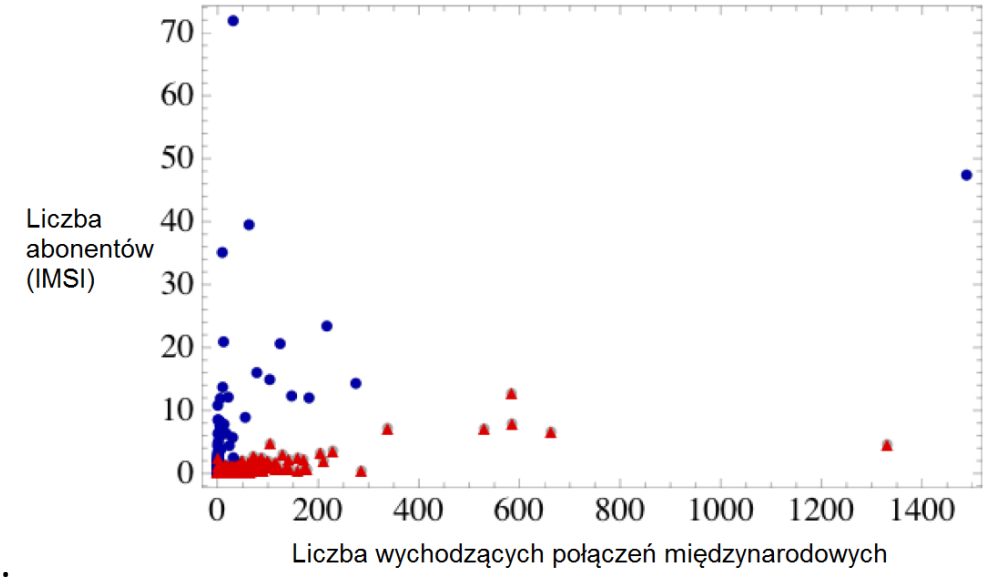
Z przytoczonych na Rysunek 6-2 danych wynika, że w przeciwieństwie do legalnego ruchu w sieci, połączenia simboxowe są inicjowane z jednej lub dwóch lokalizacji. Ta właściwość jest niestety mało użyteczna w przypadku obecnie stosownych systemów rozproszonego simboxingu, który zapewnia symulację mobilności abonenta.



Rysunek 6-3. Zależność pomiędzy liczbą połączeń wychodzących a liczbą połączeń przychodzących.

Źródło - Analysis and Detection of SIMbox Fraud in Mobility Networks

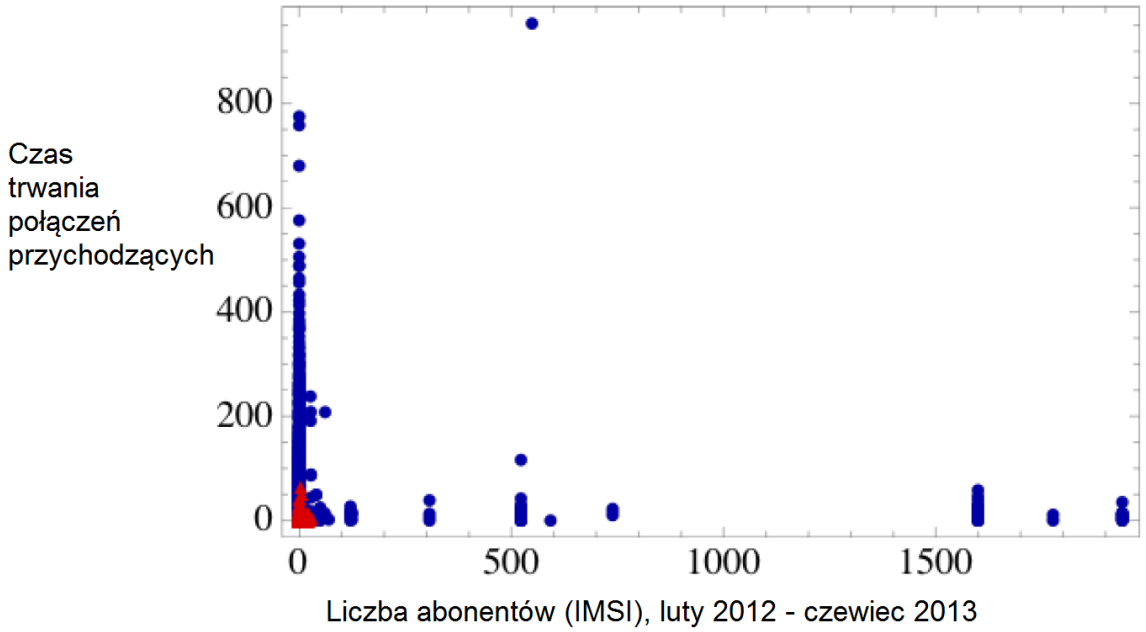
Na Rysunek 6-3 przedstawiono zależność pomiędzy liczbą połączeń wychodzących a przychodzących. W przypadki terminali legalnych jest to zależność zmienna bliska liniowej z nielicznymi wyjątkami, podczas gdy dla simboxów liczba połączeń przychodzących jest stała i bliska zeru. Tego rodzaju wzorzec może służyć jako kryterium detekcji simboxa, gdyż frauderzy, zainteresowaniu maksymalizacją zysków, nie generują na modemy simboxowe połączeń imitujących legalny ruch abonencki, które absorbują zasoby systemu.



Rysunek 6-4. Zależność pomiędzy liczbą międzynarodowych połączeń wychodzących a liczbą terminali identyfikowanych przez IMSI, z których są inicjowane.

Źródło - Analysis and Detection of SIMbox Fraud in Mobility Networks

Przedstawiona na Rysunek 6-4 zależność wskazuje, że w przeciwieństwie do terminali legalnych, w przypadku simboxów liczne połączenia były inicjowane przez nieliczne terminale abonenckie



Rysunek 6-5. Zależność pomiędzy liczbą międzynarodowych połączeń wychodzących a liczbą terminali identyfikowanych przez IMSI, z których są inicjowane.

Spośród rozwiązań technicznych oferowanych na rynku urządzeń telekomunikacyjnych i teleinformatycznych można wyróżnić 3 kategorie systemów analitycznych ruchu w sieci, realizujących algorytmy z zastosowaniem kryteriów wskazujących na działanie simboxów:

- Lokalne urządzenia sieciowe zainstalowane w sieci do monitorowania ruchu w czasie rzeczywistym oraz detekcji i blokady simboxów - systemy te na bieżąco gromadzą i analizują rekordy CDR i podejmują decyzję o blokadzie terminali, spełniających kryteria przypisane simboxom,
- Globalne systemy analityczne pracujące w czasie rzeczywistym realizują ww. funkcje skali sieci globalnej, obejmującej sieci wielu operatorów, w których zainstalowane są urządzenia testujące i monitorujące,
- Lokalne systemy do analizy w czasie nierzeczywistym plików danych CDR pod kątem funkcjonowania SIM-boxów, w tym systemy analityczne zlokalizowane w prywatnych i publicznych chmurach obliczeniowych,
- Globalne systemy analityczne pracujące w czasie nierzeczywistym realizujące ww. funkcje w skali globalnej, stosowane przez operatorów globalnych, np. Orange, T-mobile, w tym systemy analityczne zlokalizowane w prywatnych i publicznych chmurach obliczeniowych.

Zważywszy, że podmioty stosujące nadużycia korzystają w coraz bardziej zaawansowanych technologicznie i wyrafinowanych funkcjonalnie simboxów, metody analityczne zapobiegania nadużyciom w telekomunikacji mogą okazać się mało wydajne.

Opisane wyżej mechanizmy i metody (np. technika logiki rozmytej) umożliwiają wykrywanie zjawiska simboxingu w sieci. Znalazły one zastosowanie w systemach anty-fraudowych oraz w testerach służących do pomiaru parametrów QoS. Szerszy opis takiej aparatury zamieszczono w załączniku 1.

7. Wnioski z przeglądu regulaminów świadczenia usług pod kątem identyfikacji niedozwolonych praktyk

Wiodący operatorzy publicznych sieci ruchomych z reguły umieszczają w umowach abonenckich zapis stanowiący, że integralną część umowy stanowi regulamin świadczenia usług. Regulamin natomiast zobowiązuje abonenta do korzystania z sieci zgodnie z jej przeznaczeniem i zawiera szereg restrykcji, których celem jest przeciwdziałanie nadużyciom telekomunikacyjnym, w tym zjawisku simboxingu. Dokumenty te określają niedopuszczalne praktyki ze strony abonentów oraz atrybuty urządzeń, których stosowanie w sieci wymaga zgody operatora pod sankcją zablokowania karty SIM lub rozwiązania umowy.

Przykładem jest występujące w regulaminie operatora Polkomtel Sp. z o.o. pojęcie adaptera, rozumianego jako urządzenie telekomunikacyjne umożliwiające podłączenie do sieci telekomunikacyjnej i kierowanie do niej lub modyfikowanie komunikatów, połączeń telefonicznych lub sygnałów pochodzących z innych sieci telekomunikacyjnych. W tę definicję wpisują się urządzenia wykorzystywane do uprawiania simboxingu.

Spośród niedopuszczalnych praktyk opisanych w regulaminach wiodących operatorów należy wymienić przede wszystkim:

- używanie adapterów w sieci operatora bez jego zgody,
- kierowanie do sieci telekomunikacyjnej ruchu telekomunikacyjnego z innych sieci telekomunikacyjnych bez zgody operatora,
- udostępnianie innym podmiotom usług bez zgody operatora w celu uzyskiwania korzyści majątkowych dla siebie lub osoby trzeciej,
- generowania sztucznego ruchu telekomunikacyjnego w sieci,
- używania Karty SIM w celu prowadzenia działalności gospodarczej polegającej na masowym wykonywaniu połączeń,
- wykorzystywania telefonu lub Karty SIM bez zgody operatora do rozwiązań telemetrycznych.

Wprawdzie zapisy w regulaminach dają podstawę prawną operatorom, jeśli takie są, do podejmowania działań w stosunku do nieuczciwych klientów, jednak sankcje, jakimi dysponuje operator wobec sprawców nadużyć nie są adekwatne do skali zagrożeń i strat ponoszonych przez rzetelnych uczestników rynku usług telekomunikacyjnych.

Przykłady wyciągów z regulaminów świadczenia usług telekomunikacyjnych przedstawiono w załączniku3 punkt 15.

8. Wnioski i propozycje działań naprawczych

8.1 Diagnoza

Z informacji uzyskanych od operatorów i postulatów zgłaszanych w trakcie konsultacji, z analizy funkcjonalności systemów oferowanych do realizacji simboxingu oraz opisów metod i systemów wykrywania simboxingu wynika, że jest to zjawisko trudne do zwalczenia, w szczególności do wykrycia i zlokalizowania. Przede wszystkim dlatego, że charakter generowanych połączeń jest zbliżony do ruchu rzeczywistego, zjawisko ma oddziaływanie globalne, a zasięg połączeń międzynarodowy. Gdy zamiana numeru abonenta A jest realizowana za granicą (w tym w kraju UE), to nadużycie jest poza zasięgiem polskiego prawa.

Ponadto, ciągłym zmianom ulega sposób realizacji simboxingu, wynikający z nowych rozwiązań urządzeń, metod generowania simboxingu oraz zmian stawek rozliczeń międzyoperatorskich i taryf. Dlatego też regulacje powinny być dostosowane do rozwoju nowych technologii.

Skomplikowany i wyrafinowany sposób działania simboxingu powoduje trudności uzyskania dowodów nieuczciwej działalności. Karty SIM są odseparowane od części radiowej i mogą znajdować się nawet w innym kraju. Obowiązek rejestracji kart SIM powinien ograniczyć ich dostępność, a operatorzy będą mogli sprawdzić fakt nabycia wielu kart przez jedną osobę.

Operatorzy oczekują zdecydowanych działań ze strony administracji publicznej i organów ścigania oraz bardziej skutecznego karania za świadczenie usług telekomunikacyjnych niezgodnie z prawem. Problem jednak w tym, że aktualnie obowiązujące przepisy nie określają jednoznacznie takich działań ani kar. Nadużycia telekomunikacyjne nie są jasno zdefiniowane w ustawie Pt, co powoduje trudność klasyfikacji czynu, a w szczególności ściągania jego z urzędu. W tej sytuacji operatorzy mogą się zabezpieczyć przed nadużyciami jedynie za pomocą umów i regulaminów świadczenia usług, w których wprowadzają zapisy ograniczające stosowanie urządzeń FCT na postawie prawa cywilnego.

Z analizy regulaminów i umów na świadczenie usług (pkt 7) wynika, że zapisy ograniczające możliwość używania urządzeń FCT i określające działania podejmowane w związku z wystąpieniem nadużycia są niejednolite u poszczególnych operatorów, a w niektórych przypadkach nie ma ich wcale. Przedsiębiorcy telekomunikacyjni stosują różne procedury związane z blokowaniem ruchu, które wymagają ujednolicenia w umowach na świadczenie usług.

8.2 Propozycje działań zapobiegawczych zgłaszane przez operatorów

Podczas konsultacji operatorzy zgłosili szereg propozycji działań zapobiegawczych, takich jak:

1. Większa pomoc organów ścigania i karnych.
2. Szybsza ścieżka karania sprawców simboxingu.
3. Skuteczne karanie za nadużycia simboxingu.
4. Ograniczenie simboxingu poprzez konieczność rejestracji kart pre-paid.
5. Sprawdzanie w sieciach numerów IMSI i IMEI razem w procesie logowania.
6. Konieczność uregulowania kwestii nadpisywania adresu A w wiadomościach SMS.
7. Umieszczenie w ustawie Pt przepisu zakazującego stosowanie praktyk FTC i generowanie sztucznego ruchu.

Operatorzy wskazywali, że nadużycia telekomunikacyjne (fraudy) na rynku telekomunikacyjnym są ogromnym wyzwaniem i problemem. Podkreślali, że brak odpowiednich regulacji i sankcji powoduje utrzymywanie się tego zjawiska zarówno na rynku detalicznym jak i hurtowym. Dodatkową zachętą do nadużyć są atrakcyjne oferty usług telekomunikacyjnych (np. oferty unlimited), asymetria stawek międzyoperatorskich, nieprecyzyjne zapisy prawa lub ich brak.

Operatorzy wnioskowali o prawne zakazanie pośredniczenia w realizacji połączeń za pomocą simboxów oraz generowania sztucznego ruchu i odpowiednie penalizowanie takich działań. Zwracali uwagę, że obecne przepisy nie pozwalają przedsiębiorcom telekomunikacyjnym na poprawę efektywności metod walki z nadużyciami, a brak stosownych regulacji ogranicza możliwości kontrolne krajowym organom regulacyjnym. Dlatego podkreślali konieczność wprowadzenia nowych systemowych rozwiązań prawno-regulacyjnych celem wyeliminowania nadużyć telekomunikacyjnych, w szczególności poprzez jednoznaczne zdefiniowanie w ustawie Pt, aby można było określić, które działania są niezgodne z prawem. Działania te miałyby być ukierunkowane pod kątem ochrony operatorów. Należy stwierdzić, że nadużycia telekomunikacyjne z punktu widzenia operatora są trudne do precyzyjnego zdefiniowania, ponieważ podlegają zmianie w zależności od taryf, rozliczeń, możliwości technicznych, rozwoju technologii. W interesie operatorów jest aby były jasno określone w umowach i regulaminach na świadczenie usług telekomunikacyjnych oraz przestrzeganie dobrych praktyk.

Ponadto wśród propozycji zgłaszanych przez operatorów w trakcie konsultacji znalazły się takie kwestie, jak:

- poprawa efektywności stosowanych metod przeciwdziałania nadużyciom telekomunikacyjnym poprzez szybsze egzekwowanie sankcji prawnych w przypadku nadużyć,
- stworzenie warunków prawnych do stałej współpracy operatorów i Prezesa UKE, np. w zakresie wymiany informacji i przeciwdziałania nadużyciom,
- stosowanie aktywnych mechanizmów do przeciwdziałania nadużyciom w postaci: możliwości zablokowania ruchu, wstrzymania płatności, wyłączenia usługi (w uzasadnionych przypadkach), automatyzm kar dla użytkowników, dla których nadużycia telekomunikacyjne są podstawowym źródłem przychodu, a świadczone usługi nie są wykorzystywane do komunikacji, automatyzm w stosowaniu kar dla Operatorów;
- stworzenie warunków dla organów administracji państwowej, które pozwolą na ograniczenie i eliminację nadużyć telekomunikacyjnych (kontrolowanie przez UKE niezmienności numeru abonenta A na drodze połączeniowej i nakładania kar, aktywne działania Policji, ściganie z urzędu jak za przestępstwo);
- wprowadzenie mechanizmu dla skutecznego i szybkiego dostosowywania istniejących umów do zmian wynikających z decyzji SMP (decyzji Prezesa UKE w sprawie hurtowych stawek za zakańczanie połączeń).
- ujednolicenie stawki za połączenia międzyoperatorskie niezależnie od stosowanego rozwiązania technicznego (protokołu sygnalizacji) – przestrzeganie wymaganej w ustawie Pt neutralności technologicznej,
- wprowadzenie konieczności stosowania stawek symetrycznych, co spowoduje że stosowanie sztucznego ruchu będzie nieopłacalne.

Przedsiębiorcy telekomunikacyjni twierdzą, że wskutek nadużyć zostają poszkodowane te podmioty, które prawidłowo wypełniają wszystkie swoje obowiązki wobec uczestników rynku telekomunikacyjnym w Polsce oraz Skarb Państwa z tytułu potencjalnie nieodprowadzonych należności podatkowych. Obowiązek rejestracji kart prepaid może częściowo ograniczyć simboxing (FCT), ale go nie wyeliminuje.

W niektórych krajach zakazane jest kierowanie ruchu z pominięciem łączy międzyoperatorskich (w tym między innymi zakaz nielegalnego stosowania FCT) np. w Portugalii, Zimbabwe i Ghanie i grożą za to kary m. in. pozbawienia wolności.

8.3 Proponowane kierunki działań dla ograniczenia nadużyć telekomunikacyjnych

8.3.1 Działania w zakresie przestrzegania warunków technicznych

Zjawisko simboxingu nie wystąpi jeśli będą spełnione następujące warunki:

1) droga połączeniowa przebiegać będzie od abonenta A do abonenta B – nie może być segmentowana i nie może przebiegać przez styk abonencki,
2) numer abonenta A nie będzie ulegać modyfikacji na całej drodze połączeniowej, poza drobnymi wyjątkami wynikającymi z różnych formatów numerów - można dopuścić tylko elastyczność w formacie numeru wynikającą z barier technicznych implementacji protokołu SIP np. format numery krajowy lub międzynarodowy poprzedzony cyframi 0048 lub +48, ale bez zmiany KNA,
3) połączenia sieci będą realizowane za pomocą międzyoperatorskiego punktu styku – nie będą wykorzystywane w tym celu zakończenia łącza abonenckiego,
4) w rozliczeniach międzyoperatorskimi będą stosowane stawki hurtowe, a nie detaliczne,
5) wymiana ruchu będzie odbywać się tylko przez podmioty wpisane do Rejestru Przedsiębiorców Telekomunikacyjnych.

Spełnienie co najmniej jednego z powyższych warunków będzie zapobiegało przed simboxingiem oraz umożliwiało jego wykrycie.

W związku z powyższym proponuje się zmianę zapisu w Rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 12 grudnia 2014 r. w sprawie szczegółowych wymagań dotyczących zasad adresowania dla właściwego kierowania połączeń:

Proponuje się zmienić istniejący zapis:

> „§1. Informacja adresowa o numerze abonenta wywołującego powinna być niezmienna na całej drodze połączeniowej, z zastrzeżeniem § 2.”

na zapis:

> „§1. Informacja adresowa o numerze abonenta wywołującego powinna być niezmienna na całej drodze połączeniowej z zapewnieniem integralności usług i sieci, z zastrzeżeniem § 2”

8.3.2 Zwiększenie ochrony niezmienności numeru A na całej drodze połączeniowej

Operatorzy oczekują zdecydowanych działań ze strony Urzędu Komunikacji Elektronicznej i karania nieuczciwych przedsiębiorców. Aby działania UKE w zakresie ochrony niezmienności numeru abonenta A na całej drodze połączeniowej mogły być realizowane wymagane jest określenie jakie

paramenty sieci i usług powinny być przedmiotem kontroli i jaka będzie podstawa nakładania kary. Ponadto, aby Urząd Komunikacji Elektronicznej mógł stwierdzić, że usługi realizowane są niezgodnie z prawem musi być wyposażony w niezbędne narzędzie techniczne, aby mógł wykonywać badania kontrolne.

Proponuje się aby UKE prowadził w sposób ciągły badania ciągłości numeru abonenta A poprzez generowanie połączeń próbnych za pomocą specjalizowanego systemu (zob. pkt 8.4).

Dla potrzeb systemu badaniowego każdy z operatorów sieci świadczących usługi telefoniczne udostępniałby za pośrednictwem sieci Internet port badaniowy o danym numerze pracujący w sygnalizacji SIP.

Można rozważyć wykorzystanie przez UKE systemu do badania jakości połączeń telefonicznych AWP-IŁ, którym dysponuje, służącego do generowania próbnego ruchu w oparciu o próbniki badaniowe zainstalowane na centralach telefonicznych dla usługi POTS oraz próbniki badaniowe dla sieci komórkowych. Połączenia badaniowe byłyby generowane losowo, a wyniki pomiarów przetwarzane pod kątem wykrywania simboxingu za pomocą narzędzia Bussiness Intelligence.

8.3.3 Działania w zakresie karania

Prawo telekomunikacyjne nie definiuje nadużyć telekomunikacyjnych w relacjach międzyoperatorskich i nie określa karania za te przestępstwa.

W szczególności artykuł art. 209 ustawy Pt nie zawiera kar za nadużycia telekomunikacyjne. Niemniej jednak zidentyfikowano pozycję w tym artykule, która pośrednio dotyczy nadużyć telekomunikacyjnych i może stanowić podstawę karania za tego typu przestępstwa oraz instrument wykorzystany do zwalczania simboxingu.

Przykładowo, art. 209. 1. 19) ustawy Pt może stanowić podstawę karania, ponieważ mówi o tym, że podlega karze pieniężnej „kto wykorzystuje numerację niezgodnie z przeznaczeniem, o którym mowa w art. 126".

Przepis ten odnosi się do art. 126, który reguluje zasady przydziału numeracji.

8.3.4 Działania w zakresie zmiany stawek międzyoperatorskich rozliczeniowych

Można rozważyć odejście od regulacji dotyczących Płaskich Stawek Interkonektowych dla usługi zakończania połączeń w sieciach stacjonarnych, ponieważ stały się one efektem ubocznym tego rozwiązania regulacyjnego i są powodem nadużyć. Można rozważyć działania w kierunku obniżenia stawek FTR, ponieważ - zgodnie z opublikowanych ostatnio przez Komisję Europejską raportem na temat wpływu rekomendacji z 2009 r. w sprawie metodologii ustalania stawek terminacyjnych FTR/MTR na rynki telekomunikacyjne w Unii Europejskiej - stawki FTR w Polsce na poziomie ok. 0,5 eurocenta za minutę należą do najwyższych w Europie.

Można rozważyć również wyrównanie stawek rozliczeń międzyoperatorskich w sieciach ruchomych, żeby asymetria stawek MTR nie stanowiła okazji do nadużyć telekomunikacyjnych.

Odejście od stawek PSI nie proponuje się z uwagi na utrwaloną praktykę rynkową.

8.3.5 Propozycja zakresu modyfikacji ofert/regulaminów dostawców usług pod kątem ograniczenia nadużyć.

Z analizy regulaminów i umów na świadczenie usług telekomunikacyjnych wynika, że są one niejednolite u poszczególnych przedsiębiorców telekomunikacyjnych. Jednak ujednolicenie

regulaminów i umów na świadczenie usług telekomunikacyjnych nie jest zasadne, gdyż może być uznane za ograniczenie konkurencji. Dlatego też, jako postulat można zgłosić tylko upowszechnienia dobrych praktyk w zakresie postanowień umownych i regulaminowych umożliwiających zwalczanie nadużyć telekomunikacyjnych.

Sami operatorzy nie zgłaszali propozycji dotyczących zmian w regulaminach i umowach w celu ich ujednolicenia w czasie konsultacji.

8.4 Propozycja systemu do badania niezmienności numeru abonenta A

8.4.1 Założenia ogólne

Przedstawiona w tym rozdziale koncepcja systemu badaniowego powstała w wyniku konsultacji z operatorami, którzy oczekują zdecydowanych działań w zakresie zapewnienia niezmienności numeru A dla połączenia telefonicznego (od końca do końca) oraz karania winnych uwikłanych w proceder generowania nadużyć telekomunikacyjnych.

Przedstawiona propozycja jest elementem wstępnej koncepcji systemu badania ciągłości przekazywania numeru abonenta A w sieci telekomunikacyjnej i ma za zadanie określić kierunki działań w zakresie dostarczenia narzędzia badaniowego i kontrolnego dla Urzędu Komunikacji Elektronicznej.

Proponowany system byłby wykorzystywany przez Urząd Kontroli Elektronicznej jako narzędzie służące do badań kontrolnych zestawiania połączeń w ramach usługi publicznej między urządzeniami końcowymi sieci telefonicznej.

Wyniki badań potwierdzające wystąpienie nadużycia telekomunikacyjnego stanowiłyby podstawę do nakładania kar na podmioty dopuszczające się tego nadużycia.

Zakłada się, że system miałby zastosowanie do badań ciągłych oraz wyrywkowych (celowanych).

Badania ciągłe obejmowałyby testowanie ciągłości numeru A w sieciach wszystkich operatorów dołączonych do systemu. Badania wyrywkowe byłyby prowadzone w odniesieniu do podejrzanych podmiotów.

8.4.2 Założenia dotyczące scenariuszy zestawiania połączeń

Połączenia badaniowe byłyby wykonywane dla usług telefonicznych realizowanych w sieciach pracujących w różnych technologiach:

- dla usług POTS w sieciach stacjonarnych w technologii TDM - łącza analogowe w zakończeniach sieci,
- dla usług POTS w sieciach stacjonarnych w technologii IP – łącza analogowe w zakończeniach sieci,
- dla terminali technologii VoIP w sieciach stacjonarnych w technologii IP - dla sygnalizacji SIP,
- dla usług głosowych w sieciach ruchomych - terminale radiowe GSM/UMTS (bramki FTC).

Zakłada się, że połączenia będą realizowane w sposób losowy w odniesieniu do kierunku połączenia i czasu (także między różnymi rodzajami sieci).

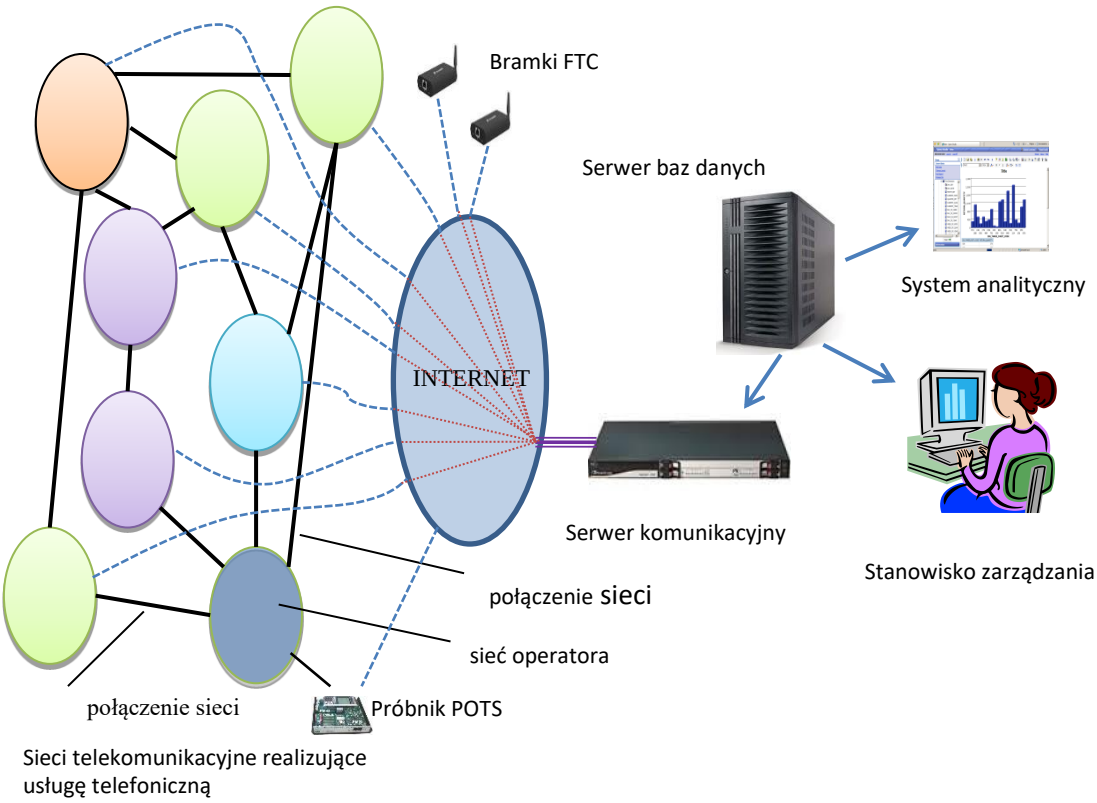
Zakłada się, że oprócz sprawdzenia zgodności numeru A wysyłanego i odbieranego na obu końcach połączenia dodatkowym parametrem będzie czas zestawienia połączenia, ponieważ każde dodatkowe przęsło na drodze połączenia (styk abonencki – sieć – styk abonencki) powoduje wydłużenie czasu zestawiania połączenia.

Fakt, że jest to system zewnętrzny - nie powiązany z systemami informatycznymi operatorów – operatorzy nie będą mieli wpływu na rodzaj i sposób realizacji badań.

Ponadto, przechodzenie przez sieci różnego rodzaju może powodować wielokrotną konwersję sygnałów (różne kodeki), co objawiać się będzie pogorzeniem jakości przesyłania sygnałów.

Rozszerzenie parametrów i zakresu pomiarów umożliwi wykorzystanie tego systemu także do badania jakości sieci telefonicznej.

System pracujący według podobnej koncepcji pod nazwą AWP-IŁ był wykorzystywany od początku lat 2000 przez Urząd Komunikacji Elektronicznej do badania jakości usługi telefonicznej. Do badania jakości połączeń były używane próbniki instalowane na zakończeniach łączy analogowych oraz próbniki dla sieci komórkowych.



Rysunek 8.1 Koncepcja systemu badania niezmienności numeru A

8.4.3 Uwarunkowania implementacji systemu

Budowę, utrzymanie i zestawienie systemu z punktu widzenia warunków technicznych ułatwi fakt, że obecnie większość platform komutacyjnych w sieciach operatorów krajowych wykonana jest w technologii IP.

Realizacja terminala badaniowego w sygnalizacji SIP może być uproszczona. Nie trzeba instalować terminali badaniowych w obiektach u operatorów, a jedynie zestawić połączenia np. z wykorzystaniem sieci Internet i terminować je w serwerze badaniowym. Każdy z operatorów będzie zobowiązany do udostępnienia zakończania łącza abonenckiego w sieci IP.

Jedynie dla zakończeń sieci analogowej i sieci radiowej GSM/UMTS wymagana będzie instalacja urządzeń badaniowych na obiektach w terenie:

- bramek FTC (ang. Fixed Cellular Terminal) dla sieci komórkowych,
- próbników ze stykiem analogowym pracujących z sygnalizacją DSS1 i SIP.

Konfiguracja systemu będzie się składać z następujących elementów:

a) serwera komunikacyjnego generującego i obierającego połączenia badaniowe pełniącego także funkcję zakończenia łącza w protokole SIP,

b) serwera baz danych przeznaczonego do gromadzenia danych badaniowych oraz danych referencyjnych, takich jak tablice przydziału numeracji, plany numeracji, plany testów itp.,

c) stanowiska zarządzania wykorzystanego do opracowania planów badań i monitorowania wykonywania połączeń badaniowych oraz konfigurowania systemu,

d) systemu analitycznego umożliwiającego analizowanie i lokalizowanie sieci, w których występuje zamiana numeru abonenta A.

Otoczenie sieci telekomunikacyjnych będzie obejmować następujące elementy:

a) sieci realizujące publiczną usługę telefoniczną działające na różnych platformach,

b) zakończenia sieci pracujące w protokole SIP lub DSS przeznaczone do celów badaniowych,

c) bramki FTC przeznaczone do wysyłania i odbierania ruchu badaniowego w sieciach komórkowych,

d) próbniki badaniowe dla analogowego zakończenia łączą abonenckiego.

Umieszczenie bramek FTC w obszarze przygranicznym i zalogowanie się do publicznych sieci ruchomych krajów sąsiednich pozwoli także na badanie połączeń w ruchu międzynarodowym.

8.5 Propozycje dalszych prac

W związku z propozycją zgłaszaną przez Departament Polityki Konsumenckiej UKE proponuje się przeprowadzenie analizy problemów związanych z nadużyciami telekomunikacyjnymi dotykającymi użytkowników.

Nadużycia, których skutki ponoszą abonenci zostały zidentyfikowane i przedstawione w punktach 3.4.1 - 3.4.7 i 3.4.12 ww. opracowania, w formie ogólnych opisów tych nadużyć. Proponuje się skoncentrowanie się w nowej pracy przede wszystkim na zaproponowaniu rozwiązań regulacyjnych bardziej adekwatnych do występujących zagrożeń, lepiej chroniących użytkowników przed nadużyciami telekomunikacyjnymi oraz przedstawieniu problemów, jakie dotykają operatorów telekomunikacyjnych oraz strat, jakie ponoszą z tytułu nadużyć telekomunikacyjnych.

Zakres prac mógłby obejmować następującą problematykę:

1. Sposoby walki z nadużyciami i ochrona abonentów przed skutkami tych nadużyć

2. Działania, jakie mogliby podjąć operatorzy w celu ochrony interesów abonentów
3. Udział i obowiązki operatorów wykrywania nieuczciwych działań
4. Wykorzystanie przez operatorów urządzeń monitorujących ruch w ich sieci w celu wykrywania nieuczciwych działań
5. Wprowadzenie rozwiązania prawnego doprecyzowującego kwestię blokowania połączeń do numerów o podwyższonej opłacie oraz usług SMS Premium Rate (np. zobowiązującego operatorów do umieszczeniu w umowie zawieranej z abonentem zapisu mówiącego o tym, że połączenia do numerów o podwyższonej opłacie oraz usług SMS Premium Rate są blokowane domyślnie, a ich odblokowanie jest realizowane na wyraźne życzenie użytkownika)
6. Wprowadzenie rozwiązania prawnego doprecyzowującego kwestię uiszczania opłaty za usługę, która w wyniku reklamacji została uznana za oszustwo (np. w odniesieniu do nadużyć opisanych w punktach 3.4.3 - 3.4.4 niniejszego opracowania usankcjonowanie nie tylko prawa do reklamacji, ale w przypadku wykazania nadużycia telekomunikacyjnego zwolnienie użytkownika obowiązku uiszczenia opłaty za usługę telekomunikacyjną stanowiącą nadużycie)
7. Propozycje rozwiązań prawnych dotyczących innych nadużyć (związanych np. z podrabianiem dokumentów abonentów, dokumentacji umownej, czy SMS Premium Rate
8. Propozycje akcji edukacyjnych

9. Analiza ryzyka

[Analizę ryzyka dla obecnego stanu przeprowadzono w oparciu o:

1. Opis i prawdopodobieństwa ryzyka wynikającego z obecnego stanu.
2. Skalę odziaływania i Skalę prawdopodobieństwa o 5-ciu progach:
    1) bardzo niskim,
    2) niskim,
    3) średnim,
    4) wysokim,
    5) bardzo wysokim.

Tabela 1: Tabela -Rejestr ryzyk

Ryzyko	Waga (oddziaływanie)	Skutki zagrożenia	Prawdopodo-bieństwo zaistnienia ryzyka	Działania zaradcze
Kierowanie połączeń za pomocą bramek FTC (simboxing)	5	niższe przychody operatorów (straty), zaburzanie ciągłości numeru abonenta A na drodze połączeniowej, obniżanie jakości połączeń i generowanie skarg przez klientów, zaburzenia danych bilingu (brak lub błędne dane o połączeniu dla organów ścigania, ujawnienie informacji SMS lub MMS, możliwość nieuprawnionego nagrywania rozmów dla wybranych numerów lub par numerów (działanie przestępcze, dziennikarze itp.	2	analiza danych bilingowych przez operatorów, stosowanie przez operatorów systemów wykrywania simboxingu, wykonywanie połączeń próbnych przez UKE, sprawna współpraca z organami ścigania.

Ryzyko	Waga (oddziaływanie)	Skutki zagrożenia	Prawdopodobieństwo zaistnienia ryzyka	Działania zaradcze
Generowanie sztucznego ruchu, np. wydzwanianie przez nieuczciwych przedsiębiorców z obcych sieci na własne numery usług – wykorzystanie podziału opłaty (revenue sharing) i niesymetrycznych stawek rozliczania, wykorzystywanie ofert bez limitu do generowania sztucznego ruchu, gdzie są asymetryczne stawki MTR lub FTR	5	Straty rzetelnych operatorów, Zaburzenie rynku telekomunikacyjnego	2	analiza danych bilingowych przez operatorów
Generowanie sztucznych połączeń do tzw. pseudoserwisów	5	Pseudoserwisy polegające na wykorzystywaniu kart typu no-limit w simboxach i dzwonienie na numery pseudo-usługowe w sieci innego operatora, który uzyskuje wpływy za opłatę za ruch przychodzący.	1	analiza danych bilingowych przez operatorów,
Generowanie połączeń w sieci ruchomej w jednej lokalizacji przy pomocy simboxa	5	Wysycanie sieci radiowej, zaburzenia procesu planowania sieci	1	analiza danych bilingowych przez operatorów, stosowanie systemów wykrywania simboxingu

Ryzyko	Waga (oddziaływanie)	Skutki zagrożenia	Prawdopodobieństwo zaistnienia ryzyka	Działania zaradcze
Kierowania ruchu krajowego drogą okrężną z uwagi na spłaszczanie stawek w Europie do stawek jak w ruchu krajowym	5	Spłaszczanie stawek w Europie do stawek jak w ruchu krajowym powoduje kierowanie ruchu również przez inne kraje	1	Wykrywanie nieciągłości numeru przy pomocy połączeń próbnych
Klonowanie kart SIM (karty starego typu)	5	Zwiększali skali nadużyć (liczby połączeń) z wykorzystaniem jednego numeru telefonicznego	1	Zastosowanie do logowania w sieci pary IMEI i IMSI
Klonowanie numerów IMEI	5	Podszywanie się pod różne prawdziwe nr IMEI	1	Zastosowanie do logowania w sieci pary IMEI i IMSI

10. Analiza SWOT

Analiza SWOT przeprowadzona została dla 3 wariantów:

a) Stan obecny – bez zmian

b) Działanie I – wprowadzenie badań kontrolnych UKE,

c) Działanie II – wprowadzenie zmian stawek rozliczeniowych,

d) Działanie III – rejestracja kart SIM.

LP.		Bez zmian	Działania kontrolne UKE	Zmiany stawek rozliczeniowych	Rejestracja kart SIM
1.	**Mocne strony**	Nie stwierdzono	Dostarczenie dowodu potwierdzonego przez regulatora	Eliminacja wykorzystania płaskich taryf ofert detalicznych oraz interkonektowych do generowania sztucznego ruchu, Eliminacja wykorzystania płaskich taryf ofert detalicznych oraz interkonektowych do simboxingu	Łatwiejsza identyfikacja użytkownika karty SIM
2.	**Słabe strony**	Niekorzystne warunki współpracy z organami ścigania Nie zdefiniowane nadużycia telekomunikacyjne Niska skuteczność karania	Konieczność wyposażenia UKE w system badaniowy Dodatkowe obciążenie personelu UKE, Konieczność udostępnienia przez operatorów portów badaniowych	Zaburzenie rynku z powodu wycofania ofert bez limitu Zaburzenie rynku z powodu likwidacji płaskich stawek interkonektowych	Dodatkowe obciążenie operatorów związane z rejestracją kart
3.	**Szanse**	Nie stwierdzono	Poczucie przez operatorów, że są kontrolowani, skłaniające ich po prawidłowych praktyk	Nie stwierdzono	Ograniczanie możliwości nabycia kart SIM w dużych ilościach przez jednego klienta, zatem wykorzystywanych do simboxingu
4.	**Zagrożenia**	Oferty detaliczne bez limitu i Płaska Stawka Interkonektowa stwarzają korzystne warunki do nadużyć	Stosowanie bardziej wyrafinowanych metod maskowania ruchu trudnych do wykrycia	Pojawienie się nowych podatności na nadużycia	Wtórny rynek kart SIM

11. Wykaz literatury

[1] i3 Forum 7 Th Annual Conference Chicaco, Ilmay12TH , 2016 Robert Benlolo http://i3forum.org/wp-content/uploads/2016/05/6%E2%80%93Fight_against_Fraud%E2%80%93Robert_Benlolo_%28Tata_Communications%29.pdf

[2] Fraud classification and recommendations on dispute handling within the wholesale telecom industry; International Interconnection Forum For Services Over IP i3 Forum (www.i3forum.org) Release 3.0 - May 2014 http://i3forum.org/wp-content/uploads/2014/05/i3F-Fraud-Classification-Release-3-2014-05-12.pdf

[3] Aneks Antyfruadowy Prezesa UKE z 2010

[4] Propozycje PIIT do Aneksu Antyfraudowego Prezesa UKE z 2013 (Aneks Antyfraudowy 2013 nie odpowiada na oczekiwania operatorów w zakresie zwalczania nadużyć): http://www.piit.org.pl/dokumenty/telekomunikacja/-/asset_publisher/ehjUfDM7qugd/content/piit-stanowisko-ws-projektu-stanowiska-prezesa-uke-w-zakresie-naduzyc-telekomunikacyjnych-konsultacje-aneksu-antyfraudowego)

[5] Propozycja PIIT do projektu rozporządzenia ws. szczegółowych wymagań dotyczących gospodarowania numeracją w publicznych sieciach telekomunikacyjnych, dotycząca kwestii nadużyć na numeracji i jej uregulowania: http://www.piit.org.pl/dokumenty/telekomunikacja/-/asset_publisher/ehjUfDM7qugd/content/piit-stanowisko-ws-projektu-rozp-maic-ws-szczegolowych-wymagan-dotyczacych-gospodarowania-numeracja-w-publicznych-sieciach-telekomunikacyjnych-art-126

[6] Stanowisko Polskiej Izby Informatyki i Telekomunikacji [PIIT] dot. szczegółowych działań w zakresie zwalczania nadużyć telekomunikacyjnych 07.10.2013r. http://www.piit.org.pl/dokumenty/telekomunikacja/-/asset_publisher/ehjUfDM7qugd/content/piit-stanowisko-dot-szczegolowych-dzialan-w-zakresie-zwalczania-naduzyc-telekomunikacyjnych

[7] ITU Workshop on „Caller ID Sppofing" ; Geneva, Switzerland, 2 June 2014

[8] ETSI TR 185 008 V2.0.0 (2008-02): Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Analysis of security mechanisms for customer networks connected to TISPAN NGN R2

[9] https://www.bu.edu/rbfl/files/2014/03/RBFL-V.-33_1_Aktas.pdf; Developments in banking law, Spoofing – Boston University

[10] http://www.xintec.com/fraud-management/what-is-simbox-fraud-and-why-is-it-so-hard-to-beat/

[11] Decyzja Prezesa Urzędu Komunikacji Elektronicznej nr DHRT.WWM.6080.7.2016.9 zmieniając umowę o połączeniu sieci z dnia 26 czerwca 2003 r., zawartą pomiędzy Orange a E-Telko dotycząca wykreślenia z Umowy postanowień umożliwiających E-Telko ryczałtowe rozlicznie ruchu międzysieciowego w oparciu o płaską stawkę interkonektową (PSI).

[12] Analysis and Detection of SIMbox Fraud in Mobility Networks – I. M. Zabarankin, R. Piqueras, J.A.Panagiaz
http://web2.research.att.com/export/sites/att_labs/techdocs/TD_101254.pdf

[13] Ustawa Prawo Telekomunikacyjne z dnia 16 lipca 2004 r. z późn. zmianami

[14] Rozporządzenie Ministra Infrastruktury z dnia 12 grudnia 2015 r. w sprawie szczegółowych wymagań dotyczących zasad adresowania dla właściwego kierowania połączeń – Dz. U. poz. 12 z dnia 5 stycznia 2015 r.

[15] Rozporządzenie Ministra Infrastruktury z dnia 19 marca 2014 r. w sprawie szczegółowych wymagań dotyczących gospodarowania numeracją w publicznych sieciach telefonicznych.(Dz. U. z dnia 10 kwietnia 2014 r. poz. 471)

12. Załącznik 1 - Przegląd metod i systemów do wykrywania simboxingu

Obecnie rynek oferuje wiele różnych systemów wykrywania simboxingu wykorzystujących coraz bardziej skomplikowane metody i funkcjonalności. Dla potrzeb niniejszego opracowania przedstawiono charakterystyki wybranych rozwiązań technicznych oraz aparat matematyczny jednej z metod wykrywania nadużyć dla zilustrowania jak bardzo wyrafinowane narzędzia muszą być zaangażowane w tym procesie.

12.1 Podejścia do detekcji nadużyć

Istnieją trzy podejścia do wykrywania oszustw za pomocą dedykowanych systemów:

1. Oparte o analizy generowanego ruchu testowego. Poprzez analizę ruchu rzeczywistego przychodzącego, ustala się czy jest to rzeczywisty ruch międzynarodowy, czy jest to ruch wewnątrz sieciowy lub czy generowany z innej sieci lokalnej.
2. Oparte o analizę baz danych. Analiza obejmuje rekordy taryfikacyjne dla każdego wywołania z karty sim danej firmy telekomunikacyjne. W tym podejściu, w procesie wykrywania fraudów mogą być wykorzystane następujące kryteria:
   - sumowanie i porównywanie stosunku połączeń wychodzących do przychodzących oraz połączeń w obrębie sieci i poza sieć,
   - brak połączeń na "dozwolone numery" (np. obsługi klienta),
   - różnorodność połączeń, w tym w obrębie sieci i poza sieć,
   - wykorzystywanie usług nie głosowych (SMS, transmisja danych, itp.),
   - mobilność, korzystanie tylko z jednej komórki sieci,
   - połączenia w nieregularnych godzinach,
   - wyszukiwanie podejrzanych komórek sieci, w tym automatyczne ich lokalizowanie.
3. Hybrydowe analizy przy użyciu obu podejść, analiz baz danych i analiz połączeń testowych, w celu opracowania bardziej efektywnych systemów wykrywania fraudów.

12.2 Metody wykrywania oszustw

Techniki wykorzystywane do wykrywania nadużyć dzielą się na dwie podstawowe klasy: techniki statystyczne i metody sztucznej inteligencji.

Statystyczne techniki analizy danych obejmują:

- wstępne przetwarzanie danych,
- obliczanie różnych parametrów statystycznych,
- łączenie, klasyfikację i przetwarzanie profilów użytkownika.

Metody sztucznej inteligencji obejmują:

- techniki uczenia maszynowego,
- sieci neuronowe,
- rozpoznawanie wzorców do wykrywania podejrzanych zachowań,

- teorię decyzji,
- analizę powiązań i logiki rozmytej.

12.3 Detekcja fraudów w połączeniach międzynarodowych przy użyciu logiki rozmytej

Opis ww. metody został opracowany na podstawie prezentacji pracy Fraud Detection in International Calls Using Fuzzy Logic, której autorami są: Abouda Abdulla A. Marah, Hussein Elrajubi i Osama Mohamed. Prezentacja została przedstawiona podczas konferencji Computer Vision and Image Analysis Applications (ICCVIA), 2015 International Conference on Sousse w Tunisie w dniach18-20 January 2015.

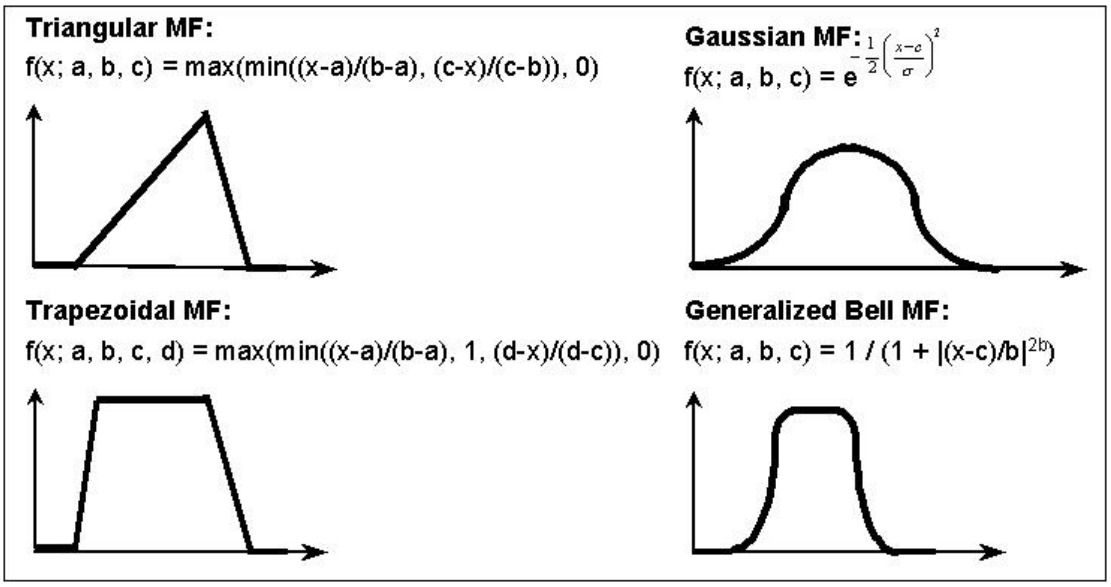
Metoda logiki rozmytej znalazła zastosowanie w nowym typie systemu do wykrywania nadużyć telekomunikacyjnych i podejmowania decyzji, wykorzystującym profile stworzone przez użytkownika. Badania systemu przeprowadzono w warunkach rzeczywistych w oparciu o pięć wybranych cech (pól) używanych jako wzorce wykrywania fraudów, do których należą: mobilność abonentów, stosunek ruchu wychodzącego i przychodzącego, gęstość użytkowników w poszczególnych komórkach sieci, nieregularność połączeń i używanie tylko usługi głosowej. Rzeczywiste bazy danych pozyskano od operatora telekomunikacyjnego Almadar Company for Telecommunication (Libia). W ramach badań oceniano możliwość zastosowania logiki rozmytej do podejmowania decyzji, które karty SIM są używane prawidłowo, a wobec których zachodzi podejrzenie oszustwa.

System został zaprojektowany i zaimplementowany przy użyciu języka C++, Microsoft Visual Studio NET. Wykorzystywano również narzędzie Fuzzy Logic w programie MatLAB do projektowania funkcji członkostwa i definiowania w systemie reguł rozmytych.

12.3.1 Istota logiki rozmytej

Technika logiki rozmytej, tak jak rachunek prawdopodobieństwa, działają w tym samym zakresie liczbowym i mają podobne wartości: 0.0 reprezentuje Fałsz (brak członkostwa w grupie), a 1.0 reprezentuje Prawdę (pełny udział w grupie). Obie metody różnią się znacząco w terminologii. Probabilistyczne podejście określa - istnieje 50% szans, że parametr X ma wartość niską (na przykład w podgrupie A), podczas gdy w terminologii logiki rozmytej odpowiada to sformułowaniu - stopień członkostwa X w podgrupie A (wartości niskie) wynosi 0,50".

Rozmyta podgrupa A jest podzbiorem wszystkich parametrów X, dla których przyznano częściowe członkostwo w podgrupie. Zbiór rozmyty A jest zdefiniowany jako uporządkowana para = {x, μ(x)}, gdzie x należy do zbioru X i 0 < = μA(x) < = 1. Funkcja członkostwa μA(x) opisuje stopień w jakim x należy do zbioru A. μA(x)=0 oznacza brak członkostwa i μA(x) = 1 oznacza pełne członkostwo. Istnieje wiele typów funkcji członkostwa, takich jak funkcja członkostwa trójkątna, trapezowa funkcja członkostwa, funkcja członkostwa Gaussa i uogólniona funkcja członkostwa Bell. W testowanym systemie zastosowano trójkątną funkcję członkostwa.



Rysunek 12.1 Przykłady rozkładu funkcji członkostwa (Internet)

12.3.2 Zasady logiki rozmytej

System decyzyjny oparty o logikę rozmytą to zbiór funkcji członkostwa i zasad, które są używane do decyzji o kwalifikacji danych. Rozmyte reguły mogą być definiowane jako instrukcje warunkowe w poniższej formie - jeśli x jest A, to y jest B - gdzie x i y są zmiennymi w postaci słownej, a A i B są odpowiednio wartościami słownymi określonymi przez rozmyty zestaw wszystkich rozpatrywanych X i Y.

W klasycznych systemach opartych na określonych regułach jeśli rozpatrywany warunek ma wartość Prawda, to w konsekwencji wynik ma również wartość Prawda. W systemach rozmytych, gdy warunki są określone jako rozmyte, wszystkie reguły są poprawne dla zdefiniowanego zakresu, to znaczy, że wszystkie wyniki są częściowo poprawne. Jeśli warunek jest dobry w pewnym stopniu członkostwa, to również wynik jest dobry w tym samym stopniu. Na przykład zasady w formie rozmytej mogą być reprezentowane jako:

- reguła 1. - jeśli "Liczba wywołań w nocy" jest mała, to wynikiem testu jest "karta Sim jest legalna".
- reguła 2. - jeśli "Liczba wywołań w nocy" jest duża, to wynikiem testu jest "karta Sim jest nielegalna".

W regule 1 warunek jest rozmyty. Wynik warunku - karta Sim jest legalna - jest poprawny w stopniu, który jest równy członkostwu w zmiennej "Liczba wywołań w nocy" w podzbiorze "mało". Również reguła 2 jest rozmyta, więc wynik warunku - karta Sim jest nielegalna - jest poprawny w stopniu, który jest równy członkostwu w zmiennej "Liczba wywołań w nocy" w podzbiorze "dużo". Słowna zmienna "Liczba wywołań w nocy" ma określony zakres, ale ten zakres może zawierać wiele zbiorów rozmytych, takich jak mało, średnio i dużo. Wartości zmiennej słownej "wynik testu" może zawierać rozmyty zbiór wartości, takich jak bardzo poprawne (bardzo legalne), poprawne (legalne) i niepoprawne (nielegalne). W ten sposób rozmyte zasady odnoszą się do zbiorów rozmytych. Rozmyte systemy eksperckie łączą ze sobą zasady i w związku z tym są w stanie obniżyć liczbę reguł w systemie o co najmniej 90%.

12.3.3 Wykorzystanie techniki rozmytej do wykrywania nadużyć

Firmy telekomunikacyjne wymagają precyzyjnych i skutecznych systemów rozliczeniowych do naliczania opłat za usługi telekomunikacyjne. Systemy płatności operatorów uwzględniają stopień wykorzystania sprzętu sieciowego, który jest używany podczas korzystania z usługi, w pojedynczym rekordzie zawierającym szczegóły połączenia (CDR). W opisywanym rozwiązaniu przewidziano wykorzystywanie jako danych źródłowych rekordów CDR dostarczanych przez firmy telekomunikacyjne. Przykładowe rekordy CDR do analizy uzyskano od firmy Aljadid Almadar, operatora komórkowego w Libii. Twórcy systemu nie znali, czy zawierają oszustwa czy nie. CDR zawiera około 65 pól, ale tylko 11 pól zostało wykorzystane w procesie wykrywania.

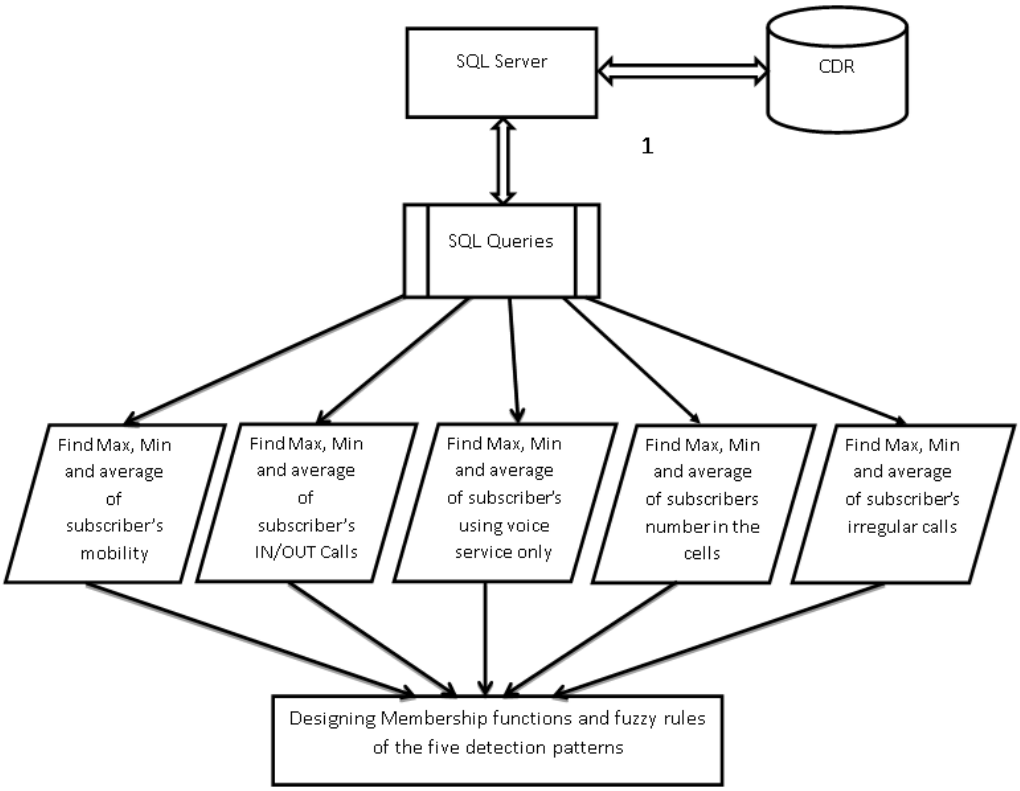
Na bazie danych z rekordów CDR określono pięć wzorców wykrywania:

- wysoka lub niska mobilność,
- stosunek liczby połączeń przychodzących do połączeń wychodzących,
- używanie wyłącznie usługi głosowej (bez SMS, MMS, GPRS, itp.),
- podejrzana aktywność w bliskim sąsiedztwie jednej komórki sieci,
- połączenia w nieregularnych godzinach, nietypowe długie rozmowy w nocy.

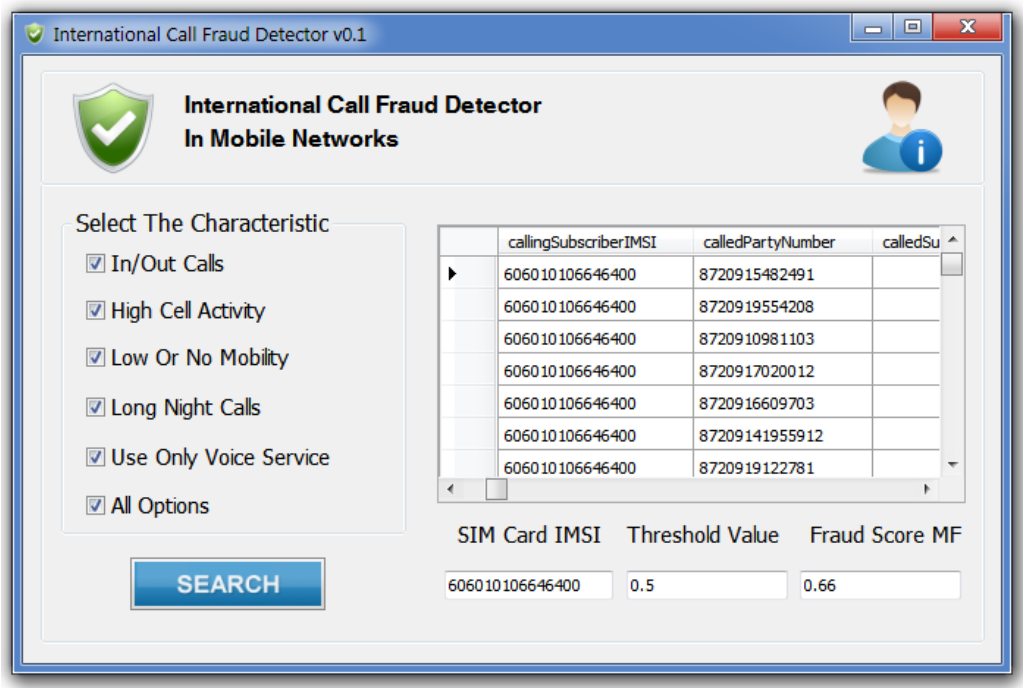
Wzorce nadużyć oraz progi zostały zaimplementowane i ustawiane przez analityków nadużyć. Są one ustalane na podstawie monitoringu ruchu w sieci i prowadzonych statystyki dla danego okresu. Jeśli próg zostanie osiągnięty, zostanie wykryte prawdopodobieństwo ewentualnych nadużyć. Analitycy mogą zdecydować w każdej sytuacji, czy jest to sytuacja prawdziwego oszustwa i jakie akcje są konieczne do podjęcia przez operatora.

Wykrywanie wzorców z rekordów CDR wykonano za pomocą języka SQL, a następnie określono wartości maksymalne i minimalne dla każdego wzorca wykrywania. Określone wartości były używane do zaprojektowania funkcji członkostwa i rozmytych reguł przy użyciu równania funkcji członkostwa.

Wartość funkcji członkostwa, dla każdego z wykrywanych wzorców może być dla niektórych przypadków minimalna a dla innych maksymalna. Jeśli dany abonent ma wszystkie wzorce wykrywania z wysoką wartością funkcji członkostwa, może to być uważane jako przypadek potencjalnych nadużyć.



Rysunek 12.2 Schemat działania systemu wykrywania simboxingu



Rysunek 12.3 Widok interfejsu graficznego system testowego

12.3.4 Wnioski

Wyniki działania systemu wykrywania nadużyć opartego na logice rozmytej zależą od jakości bazy danych, która będzie używana w systemie oraz od sposobu określenia funkcji członkostwa dla każdego wzoru wykrywania. Funkcja członkostwa może zostać zwiększona lub zmniejszona w zależności od znaczenia i skuteczności danego wzoru wykrywania.

Wyniki wykrywania wszystkich wzorców oraz wszystkie wzory i funkcje zastosowane w systemie powinny być zweryfikowane przez firmy telekomunikacyjne za pomocą testowych połączeń, tak aby potwierdzić wykrycie oszustwa.

W systemach tego typu ważna jest również dostępność dokumentów lub raportów o abonentach który popełniali oszustwa oraz o uczciwych abonentach, w celu porównywania tych danych i analizie sposobów myślenia i działania oszustów. Może to pomóc w budowie systemu i projektowaniu procesu wykrywania, aby zminimalizować ilość błędów i zwiększyć wykrywalność nadużyć.

12.4 System Keynote SIGOS testowania parametrów QoS

System Keynote SIGOS umożliwia testowanie połączeń w trybie od końca do końca i szczegółowe raportowanie parametrów QoS. Przy pomocy tego systemu można wyszukiwać drogi połączeniowe z nieuprawnionymi kartami SIM, które zostały dodane do tablicy routingu i na tej podstawie selekcjonować ścieżki o gwarantowanej jakości dla optymalizacji kosztów.

System Keynote jest stosowany przez ICSS (International Carrier Sales & Solutions) w sieci T-Mobile jako element globalnego systemu służącego do monitorowania jakości ruchu.

ICSS podpisało z firmą SIGOS porozumienie dotyczące kooperacji w zakresie detekcji i zwalczania zjawiska simboxingu. W ramach zawartego porozumienia ICSS zezwoliło firmie SIGOS na wykorzystywanie istniejącej infrastruktury systemu monitorowania do realizacji połączeń testowych w trybie od końca do końca. W zamian firma SIGOS dostarcza ICSS obszerne raporty pozwalające na szybką identyfikację dostawców stosujących niedozwoloną praktykę używania simboxów i ich sieci. Raporty są przekazywane okresowo w cyklu tygodniowym. Dla podjęcia szybkiej i skutecznej reakcji na simboxing ważne jest żeby dostarczanie raportów następowało często z uwagi na fakt, że oszuści szybko instalują nowe karty SIM w swoich urządzeniach.

12.5 System anty-fraudowy OCELUS

System antyfraudowy firmy OCELUS umożliwia operatorowi skuteczne przeciwdziałanie nadużyciom telekomunikacyjnym w tym zjawisku simboxingu. System analizuje zarówno rekordy billingowe (Charging Data Record – CDR), jak i dostępne dane biznesowe (komercyjne) i wychwytuje anomalie w ruchu w sieci pod kątem nadużyć. System monitoruje takie parametry ruchu jak: liczba połączeń, numer abonenta A, numer abonenta B, zakresy nr B, czas trwania, częstotliwość występowania numeru A, dochody, koszty, ASR (Answer-Seizure Ratio) i ACD (Average Call Duration). Użytkownik systemu może zdefiniować własne kryteria wykrywania nadużyć bez konieczności stosowania dodatkowych urządzeń, ani oprogramowania.

Opis systemu znajduje się na stronie http://www.oculeus.com/anti-fraud.html

12.6 Optimus Fraud Management Solution (FMS)

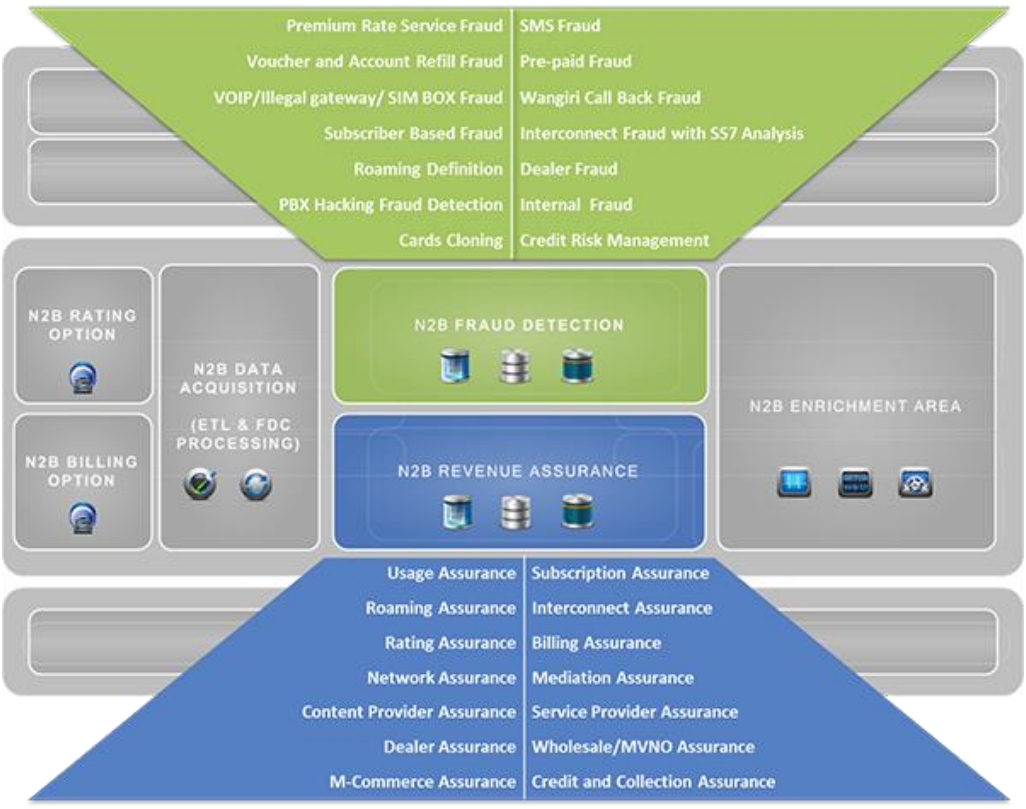
Optimus Fraud Management Solution (FMS) firmy Neutral Technologies zapewnia wszechstronną ochronę przed naruszeniami zasad wymiany ruchu, w tym przed zjawiskiem simboxingu (Bypass/SIM Box Fraud). System umożliwia operatorowi rozpoznanie rodzaju nadużycia oraz jego źródła, czy jest ono wewnętrzne, zewnętrzne, ze strony klienta, partnera lub dostawcy usług. FMS analizuje i przetwarza dane o ruchu w sieci porównując jego parametry ze stanem typowym dla poszczególnych rodzajów nadużyć.

Opis systemu znajduje się na stronie http://www.neuralt.com/73/393/optimus-fraud

12.7 System ZIRA N2B SIM BOX Detection

Pakiet oprogramowania N2B SIMBOX Detection firmy ZIRA jest częścią kompleksowego systemu N2B Risk Management obejmującego jeszcze inne pakiety i moduły antyfraudowe przedstawione na rysunku 6.4.

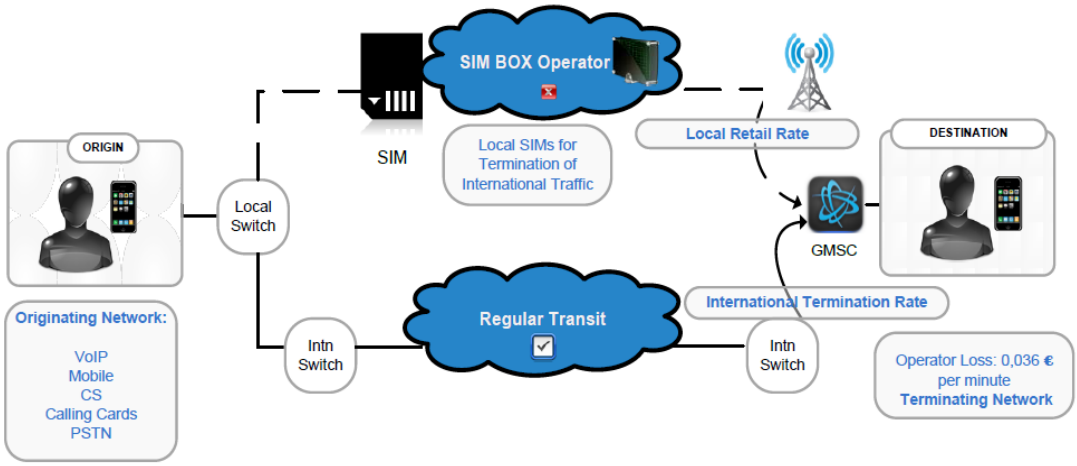
N2B SIMBOX Detection oferowany jako produkt autonomiczny, który może zostać zintegrowany z dowolnym systemem zarządzania fraudami lub osadzony w systemie ZIRA N2B Fraud Management.



Rysunek 12.4 Struktura systemu N2B Risk Management

Działanie N2B SIMBOX Detection opiera się na zaawansowanych technikach i pomiarach przepływów w sieci w celu zrozumienia zachowania abonentów. Na podstawie danych o ruchu w sieci identyfikuje użycie simboxingu. N2B SIMBOX Detection w sposób ciągły monitoruje dane o połączeniach i udostępnia szczegółowe raporty dla dalszej analizy.

Stałe monitorowanie ruchu dodatkowo gwarantuje, że nieuczciwi abonenci są łatwo rozpoznawani w sieci i ich próby wykorzystania simboksów są pomyślnie blokowane. Firma ZIRA, poprzez zaufanych partnerów, może dodatkowo zaoferować usługę Active CLI Testing Service polegającą na generowaniu połączeń głosowych do sieci klienta z dużej liczby innych sieci (stacjonarnych, ruchomych, kart telefonicznych, poprzez sieci wybranych operatorów, operatorów sieci VoIP itp.) i wykonać analizę połączeń, w celu wykrycia stosowania simboxów na drodze połączenia.



Rysunek 12.5 Funkcjonalność systemu N2B SIM BOX Detection

(Źródło www.zira.com.ba)

Funkcje oprogramowania N2B SIMBOX Detection**:**

- wykrywanie numerów telefonicznych podejrzanych o simboxing przy zastosowaniu wielu algorytmów i metod,
- zastosowanie algorytmów łączących krótkoterminowe testy z długoterminowymi analizami danych w celu osiągnięcia efektywności kosztowej i długoterminowej ochrony przychodów,
- wykrywanie podejrzanych połączeń na bazie zdefiniowanych wzorców (tylko połączenia przychodzące, bez SMS, bez MMS),
- intuicyjne wykrywanie fraudów poprzez kompleksowe podejście typu Alarm – Zdarzenie – Przypadek,
- automatyczna korelacja raportów generowanych przez testy zewnętrzne i połączeń lokalnych generowanych przez simboxy,
- analizy danych dostosowane do różnych typów klientów i ich ofert usługowych,
- wbudowane funkcje statystyczne do wykrywania simboxingu,
- narzędzia do definiowania i testowania profilów simboxingu

Korzyści z zastosowania systemu N2B SIM BOX Detection:

- zwiększenie przychodów operatora w ruchu przychodzącym poprzez zminimalizowanie stosowania simboxów,
- oszczędności dzięki szybkiej, nieinwazyjnej i efektywnej kosztowo implementacji,

- zwiększenie zdolności systemu operatora do wykrywania i eliminacji fraudów typu simbox.

Opis systemu znajduje się na stronie http://www.zira.com.ba/products/risk-managemet/n2b-fraud-management-system/sim-box/.

12.8 System FMSevolution firmy XINTEC

FMSevolution jest systemem umożliwiającym automatyzowanie procesu wykrywania oszustw. Zapewnia dostęp w czasie rzeczywistym do informacji, w jaki sposób klienci końcowi korzystają z usług w sieci operatora. Identyfikuje i poddaje kontroli wszelkie podejrzane działania w sieci.

FMSevolution jest systemem modułowym, co umożliwia konfigurowanie systemu zarządzania fraudami dostosowanego do specyficznych potrzeb danego operatora.

Fraudy wykrywane przez FMSevolution obejmują: roaming, karty pre-paid, transmisję danych, simboxing w usłudze z podziałem opłaty (ang. Revenue Share), spam SMS, klonowanie SIM, usługi Premium Rate (PMR), włamania do PBX , e-płatności, usługi typu maszyna-maszyna (M2M), oszustwa typu Wangiri, oszustwa w połączeniach międzyoperatorskich, oszustwa w usługach VoIP.

SIM Box Detector jest integralnym modułem systemu XINTEC FMSevolution, pozwalającym operatorom na neutralizację simboxów (co pośrednio przekłada się na zmniejszenie utraconych dochodów oraz zwiększenie przewagi konkurencyjnej). Analizując szczegółowe rekordy zdarzeń (xDRs) w czasie rzeczywistym przy użyciu zaawansowanych funkcji analizy danych, detektor simboxów umożliwia operatorom również pomiar strat finansowych, z którymi mają do czynienia. SIM Box Detector jest dostępny w różnych modelach wdrażania systemu FMSevolution, w tym jako instalacja lokalna, jako usługa zarządzana zewnętrznie lub jako usługa w chmurze.

Opis systemu znajduje się na stronie http://www.xintec.com/fraud-management/fmsevolution/.

13. Załącznik 2 - Przegląd systemów do realizacji simboxingu

Urządzenia używane do simboxingu są obecnie powszechnie dostępne na rynku. Producenci reklamują je w Internecie jako „maszynki do zarabiania pieniędzy". Opisy z reguły mają charakter reklamowy, a opis funkcjonalny jest ograniczony.

13.1 System firmy ANTRAX

Firma Antrax oferuje urządzenie, które odbiera połączenia przychodzące i kieruje je pod wybrany numer. Rozwiązania oferowane przez firmę Antrax omówiono na podstawie materiałów udostępnionych na stronie: **https://en.antrax.mobi**.

13.1.1 Zastosowanie

Głównym zastosowaniem systemu Antrax jest umożliwienie obchodzenia tradycyjnej ścieżki połączeń międzynarodowych realizowanej w sposób oficjalny przez operatorów telekomunikacyjnych, poprzez wykorzystanie transmisji VoIP, na przykład w sieci Internet i zakańczanie połączeń w sieci operatora lokalnego w najniższej możliwej taryfie. Oznacza to, że Antrax ignoruje trasy wyboru dróg połączeniowych w sieciach telekomunikacyjnych wyznaczane przez operatorów i kieruje połączenia międzynarodowe poprzez sieć Internet.

13.1.2 Elementy składowe systemu

SIMBOX (bank kart SIM) – sprzęt wykorzystywany przy zakańczaniu połączeń w sieci GSM. Główną funkcją tego elementu jest przechowywanie macierzy kart SIM. Simbox umożliwia funkcjonowanie bramek GSM bez zainstalowanych lokalnie kart SIM.

SIM Server

SIM Server jest elementem zarządzającym systemem ANTRAX, zapewnia sterowanie SIMBOX'ami i bramkami GSM, jednocześnie minimalizując koszty operacyjne utrzymania systemu.

Podstawowe funkcje urządzenia SIM Server.

- Generowanie połączeń przychodzących.

  Istotną cechą produktu, na którą wskazuje producent, jest generowanie połączeń wychodzących do sieci GSM w sposób symulujący typowego użytkownika sieci mobilnej. Jednym z efektywnych sposobów zaimplementowania ludzkich zachowań w systemie, jest generowanie przez sprzęt Antrax [połączeń ze swojej puli kart SIM przychodzących na własne numery kart SIM. Obchodzone są w ten sposób stereotypowe schematy stosowane do wykrywania simboxingu, przez co zwiększa się czas potrzebny do wykrycia nielegalnie stosowanej karty SIM.

- Automatyczne doładowanie SIM.

  Serwer automatycznie doładowuje karty SIM, eliminując ręczne kontrole stanu kont i ręczne doładowania. W celu doładowania kart system generuje żądania USSD (Unstructured Supplementary Service Data), wykorzystując do tego celu kody ze zdrapek wprowadzone wcześniej do systemu.

SIM Serwer umożliwia wykonywanie następujących funkcji utrzymaniowych:

- utrzymywanie aktywnego stanu kart SIM;

- automatyczną nawigację z wykorzystaniem tonowego menu DTMF;
- generowanie komunikatów o zerowym stanie kont kart SIM;
- zawiadamianie o połączeniach o zerowym czasie trwania itp.

Bramka VoIP/GSM

Bramka składa się do 15 płyt GSM montowanych w obudowie 3U. Każda płyta obsługuje dwa kanały, czyli dwa równoczesne połączenia. Urządzenie działa w paśmie częstotliwości systemu GSM i GPRS oraz umożliwia zmianę numeru IMEI. Poszczególne płyty mogą być wymieniane w trakcie pracy urządzenia, bez zakłócania pracy innych płyt.

Ilość obsługiwanych jednocześnie kanałów-(2 do 30) ma wpływ na cenę urządzenia i zależy od decyzji klienta dotyczącej liczby zakupionych kart.

13.1.3 Architektura systemu

Modularna architektura systemu umożliwia użytkownikom umieszczanie kart SIM rozdzielnie w stosunku do bramek GSM i łączenie się kart z bramkami poprzez sieć IP. Jest to ważna cecha dla podmiotów uprawiających simboxing, ponieważ usuwa ograniczenia związane z lokalizacją systemu zakańczania połączeń i utrudnia wykrycie banku kart SIM w sieci.

Modularna struktura uodparnia system na działania zewnętrzne mające na celu wykrywanie fraudów. Dzięki umieszczaniu bramek GSM w różnych lokalizacjach umożliwia równomierny rozkład i redukcję obciążenia poszczególnych stacji bazowych i kamufluje wielkość łącznej pojemności obciążenia systemu GSM.

Zastosowanie macierzy kart SIM umożliwia dołączenie do modemu GSM więcej niż jednej karty SIM, co zwiększa niezawodność systemu i zapewnia jego płynne działanie w przypadku, gdy przestaje działać jedna lub kilka kart SIM (z różnych przyczyn, np. zablokowania przez operatora).

W przypadku awarii karty SIM system automatycznie zastępuje ją inną kartą z zasobów macierzy SIM, dołączając ją do modułu GSM i zachowując pojemność systemu.

13.1.4 Funkcje maskujące

Migracja SIM – polega na stworzeniu iluzji ruchu abonenta w sieci komórkowej dzięki temu, że SIM Server powoduje, iż karty SIM inicjują połączenia z każdej bramki po kolei do bramek GSM zainstalowanych w różnych komórkach sieci. Chroni to karty SIM przed blokadą ze strony operatora sieci komórkowej.

Rotacja SIM - karty SIM w każdym Simboxie są podzielone na wiele grup. Każda grupa może być połączona z osobnym modułem bramki VoIP/GSM. System z upływem czasu zmienia kartę w grupie inicjującej połączenia. Każda karta SIM może być dołączona do bramki VoIP/GSM poprzez Internet.

13.1.5 „Dobre praktyki" zakańczania połączeń w sieci GSM – porady producenta systemu

Podane niżej przykłady, nazwane przez producenta systemu mianem „dobrych praktyk", umożliwiają zakańczanie połączeń GSM w sposób utrudniający wykrycie, a co za tym idzie zwiększający zyski podmiotów uprawiających simboxing. Wybór i zastosowanie „dobrej praktyki" zależy od kraju, operatora GSM i innych lokalnych czynników.

1. Karty SIM oddzielone od bramek GSM.

Macierze SIM powinny być oddzielone od modułów bramek VoIP/GSM. Wyodrębnienie macierzy SIM umożliwia zarządzanie wszystkimi kartami SIM z jednego miejsca.

2. Większa liczba lokalizacji zwiększa „bezpieczeństwo" zakończania połączeń w sieci GSM

Większa liczba lokalizacji zwiększa efektywność zjawiska migracji kart SIM. Jeśli bramki będą zainstalowane w sąsiednich komórkach sieci, to wtedy karty SIM będą sprawiać wrażenie, że przemieszczają się jak realni mieszkańcy (dom – biuro – supermarket – restauracja itd.), co utrudni wykrycie ich lokalizacji i zwiększy długość życia tych kart.

3. Optymalna liczba kanałów w jednej lokalizacji.

Im mniej kanałów jest w danej lokalizacji, tym mniejsze ryzyko jej wykrycia. Należy znaleźć optymalną ilość kanałów zapewniającą stabilny zysk pozostając niewidzialnym (6-12 kanałów na lokalizację jest na ogół wartością optymalną).

4. Optymalna liczba kart SIM na 1 kanał.

Liczba ta powinna zapewniać przychody, a jednocześnie oszczędzać karty SIM. Im jest więcej kart, tym mniejsze jest dzienne wykorzystanie pojedynczej karty. Duża liczba kart SIM minimalizuje ich blokadę bez zmniejszania pojemności systemu. Z doświadczeń biznesowych wynika, że 8-15 kart na kanał jest optymalnym stosunkiem, aby zapewnić codzienny zysk bez utraty karty.

5. Niezawodny softswitch.

Jest to wejściowa część systemu zakończeń sieci GSM. Przyjmuje ona wszystkie połączenia od przedsiębiorców telekomunikacyjnych. Powinno być to profesjonalne rozwiązanie operatorskie klasy 4, takie które może obsługiwać minimum 2000 połączeń równocześnie.

6. Optymalizacja przepustowości Internetu.

Stabilne połączenie internetowe jest potrzebne wszystkim elementom składowym systemu tzn. bramkom i simboxom. Tak się składa, że kraje w których zyski z simboxingu są największe, mają też największe problemy z Internetem - znalezienie połączenia 4Mb/s jest trudne. Trzeba stosować sprawdzone rozwiązania z tunelowaniem VPN i optymalizacją ruchu. Wskazuje się zastosowanie protokołu IAX2, który jest zoptymalizowany zarówno pod kątem przesyłu, jak i najmniejszej ilości niezbędnych danych.

7. Inteligentne rozwiązanie dla zminimalizowania prawdopodobieństwa blokowania kart SIM.

Inteligentne rozwiązania są traktowane jako przeciwdziałanie dla systemów antyfraudowych typu „robocalls", automatycznie generujących połączenia testowe i stanowiących potężną funkcjonalność systemów wykrywania nielegalnych kart SIM. Dlatego silnie rekomendowane jest wykorzystywanie filtrów antyspamowych, aby zapobiec wykryciu numerów kart SIM. Jednym z chytrych zabiegów podmiotów uprawiających simboxing jest przekierowywanie podejrzanych połączeń do obsługi technicznej, aby personel utrzymaniowy mógł upewnić operatora, że karta SIM należy do realnej osoby.

8. Wykorzystanie doświadczeń z działania logiki antyfraudowej operatorów GSM.

Logika „zachowywania się" karty SIM jest indywidualna, zależna od wielu lokalnych czynników. Można zaoszczędzić wiele czasu i pieniędzy podczas uruchamiania systemu korzystając z przykładów stosowanej praktycznie logiki działań antyfraudowych poszczególnych operatorów.

9. Ochrona przed podsłuchem IMSI w celu zapewnienia bezpieczeństwa zakończeń GSM.

Należy przyglądać się działaniom stosowanym przez operatora do wykrywania urządzeń Simbox. Widok poruszających się mobilnych urządzeń pomiarowych w pobliżu lokalizacji, w której są zainstalowane zakończenia GSM, świadczy o możliwym podsłuchu IMSI (ang. International Mobile Subscriber Identity). Należy wtedy sprawdzić, czy na płytach sprzętu zakończeń GSM jest uruchomiona ochrona przed podsłuchem IMSI. Z ochroną przed podsłuchem IMSI jest tak, jak z ubezpieczeniem, można go długo nie potrzebować, ale gdy okaże się potrzebne, to wtedy jego wartość jest nieoceniona.

10. Zarządzanie IMEI.

System minimalizuje czas i prawdopodobieństwo blokady kart SIM poprzez generowanie tylko poprawnych numerów SIM.

11. Automatyczna kontrola stanu i doładowanie konta karty.

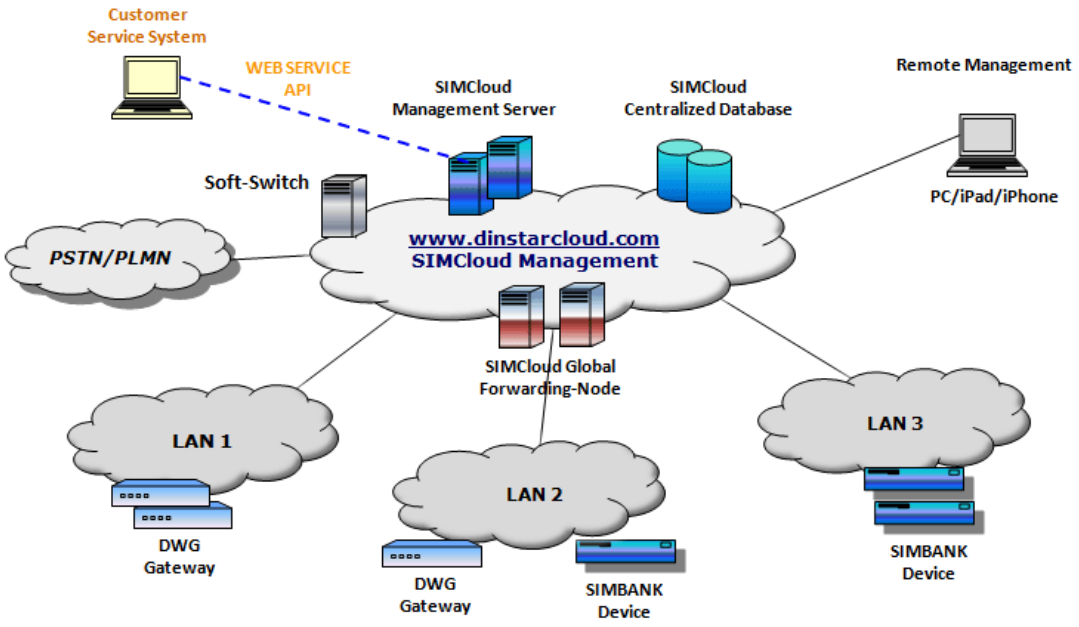
Oszczędza czas i pozwala zarabiać pieniądze dostawcy usług.

13.2 System Dinstar SIM Cloud

System SIM Cloud firmz Dinstar stanowi przykład rozwiązania simbox działającego w chmurze. Rozwiązanie omówiono na podstawie materiałów udostępnionych na stronie **http://www.dinstar.com/**.

13.2.1 Charakterystyka ogólna

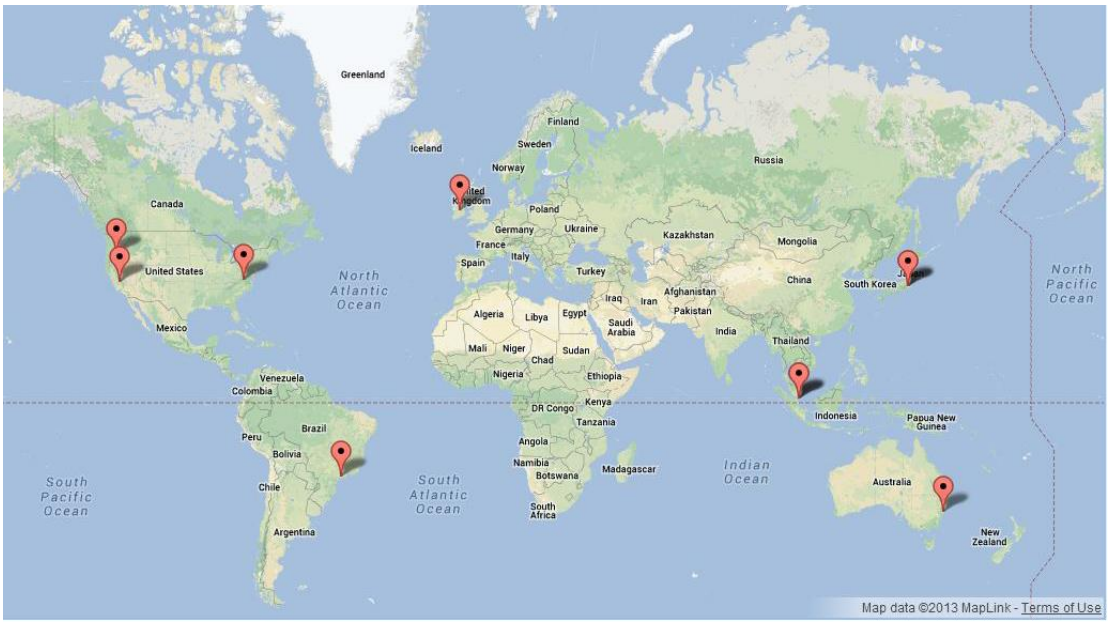
SIM Cloud jest scentralizowanym systemem zarządzania kartami SIM, który wykorzystuje najnowsze technologie internetowe. Wykonany jest w technologii Cloud computing i umożliwia sterowanie wieloma bankami SIM oraz bramkami GSM. System od razu gotowy jest do wdrożenia. Klient nie musi uruchamiać własnych serwerów, może więc łatwo rozpocząć świadczenie usług. SIM Cloud oprócz zarządzania urządzeniami i kartami SIM, realizuje symulację ludzkich zachowań w trakcie realizacji połączeń telefonicznych, dostarcza w czasie rzeczywistym statystyki działania, a także udostępnia interfejs API do oferowanych usług sieciowych. Serwer SIM Cloud udostępnia graficzny interfejs www. Za jego pomocą można przeglądać urządzenia w sieci, zarządzać kartami SIM, monitorować ich wydajność oraz identyfikować uszkodzenia w sieci. Zarządzanie systemem może być lokalne lub zdalne. Rysunek 3.7.1 przedstawia strukturę systemu.



Rysunek 13.1 Struktura systemu SIM Cloud

13.2.2 Public SIM Cloud

W wersji systemu opartej na zasobach publicznych, usługa SIM Cloud wykorzystuje chmurę Amazon oraz szereg serwerów rozrzuconych po całym świecie.



Rysunek 13.2 Serwery systemu Public SIM Cloud

Przed wykorzystaniem tego wariantu klient musi sprawdzić opóźnienia transmisji pomiędzy swoją siedzibą i poszczególnymi serwerami. Należy wybrać serwer, z którym klient uzyska najlepszy wynik (najmniejsze opóźnienie) i skontaktować się z administratorem SIM Cloud, aby powiązać swoją domenę z wybranym serwerem. Jeden serwer może zarządzać maksymalnie 16 384 kartami.

13.2.3 Lokalny serwer SIM

Jest to prywatny system SIM Cloud zainstalowany na lokalnym komputerze w sieci użytkownika (np. VPN). Rozwiązanie to zmniejsza opóźnienia i straty pakietów pomiędzy serwerem, bramkami i simboxami. Wsparcie techniczne pomaga zainstalować oprogramowanie, licencję i uruchomić serwer.

Wymagania sieciowe:

- max opóźnienie 500ms,
- przepustowość dla simboxu 192kbit/s,
- przepustowość dla bramek zależnie od ilości kanałów i użytego kodeka mowy waha się od 268kbit/s do 1216kbit/s.

13.2.4 Funkcje systemu zarządzania SIM Cloud

Funkcje zarządzania kartami są realizowane na trzech poziomach.

Funkcje zarządzania kartami na poziome I obejmują:

- migrację kart SIM pomiędzy różnymi lokalizacjami na dużym obszarze,
- rozpoznawanie numerów kart SIM poprzez automatycznie wysyłane wiadomości SMS,
- generowanie wiadomości SMS po aktywacji karty SIM (losowo na końcu połączenia),
- generowanie USSD po aktywacji SIM (losowo na końcu połączenia),
- zestawianie losowych połączeń do przypadkowych numerów oraz innych aktywnych kart SIM,
- wykrywanie blokad kart SIM poprzez niestandardowe rekordy billingowe (CDR), zablokowane powiadomienia, testowanie SMSem, testowanie próbą połączenia, testowanie stanu karty, wysyłanie promocyjnej wiadomości.

Funkcje realizowane na poziome II obejmują zarządzanie promocjami, stanem kont na kartach oraz automatycznym ich uzupełnieniem.

Poziom III obejmuje inteligentne kierowanie połączeń (np. wybieranie najtańszej karty dla danego prefiksu), tworzenie list białych i czarnych numerów, generowanie książki adresowej dla kart SIM, zarządzanie transmisją danych (zmniejszanie wymaganej przepustowości, szyfrowanie danych), generowania alarmów (SMS, e-mail).

13.2.5 Elementy i funkcje systemu

SIMbank

Urządzenie to pozwala na magazynowanie do 128 kart SIM lub innych inteligentnych kart. Razem z serwerem SIM Cloud i bramkami GSM/WCDMA/VoIP stanowi kompletne rozwiązanie radiowego systemu VoIP. Transmisja danych pomiędzy kartami SIM i innymi elementami systemu wykorzystuje prywatny protokół, zapewniający niezawodną łączność IP pomiędzy wszystkimi komponentami systemu.

Rysunek 13.3 Widok urządzenia SIMbank produkcji firmy Dinstar

Inteligentne uzupełnianie IMEI dla karty SIM

Stosuje się dwie polityki:

- stały IMEI dla określonej karty,
- zmiana IMEI przy alokowaniu karty SIM do innej bramki.

Migracja SIM w systemie

Migracja SIM wymaga w systemie wielu bramek ulokowanych przy różnych stacjach bazowych. Bramka powiązana jest z Grupą SIM, karty z Grupy po kolei współpracują z bramką. Istnieje mechanizm przenoszenia karty SIM do innej grupy.

13.2.6 Główne cechy SIMbank

SIMbank cechuje:

- wykorzystanie NAT (ang. Network Address Translation),
- 128 slotów SIM,
- dynamiczna alokacja kart SIM,
- wysoka niezawodność transmisji danych,
- zdalne karty SIM, łatwość ich zastąpienia,
- wymiana kart w „biegu” (bez przerwy w świadczeniu usług),
- zdalne zarządzanie (łatwość utrzymania urządzeń).

13.3 System firmy TOPEX S.A.

Rozwiązanie omówiono na podstawie materiałów udostępnionych na stronie **http://wiki.topex.ro/index.php/Simserver%26Simbox.**

W skład systemu simboxingu produkcji firmy TOPEX S.A. wchodzą poniżej wymienione urządzenia.

- SIMServer.

  Zawiera SIMBox, realizuje wirtualne połączenia pomiędzy bramkami z emulatorem SIM oraz SIMBoxem, zapewnia dynamiczny zdalny dostęp zapewnia do kart SIM.

- SIMBox.

  Jest częścią urządzenia SIMServer - obsługuje zainstalowane w nim karty SIM.

- multiAccess.

  Stanowi bramkę i konwerter sygnalizacji dużej pojemności (do 128 użytkowników sieci).

- QUTEX.

  Stanowi bramkę i konwerter sygnalizacji małej pojemności (do 40 użytkowników sieci).

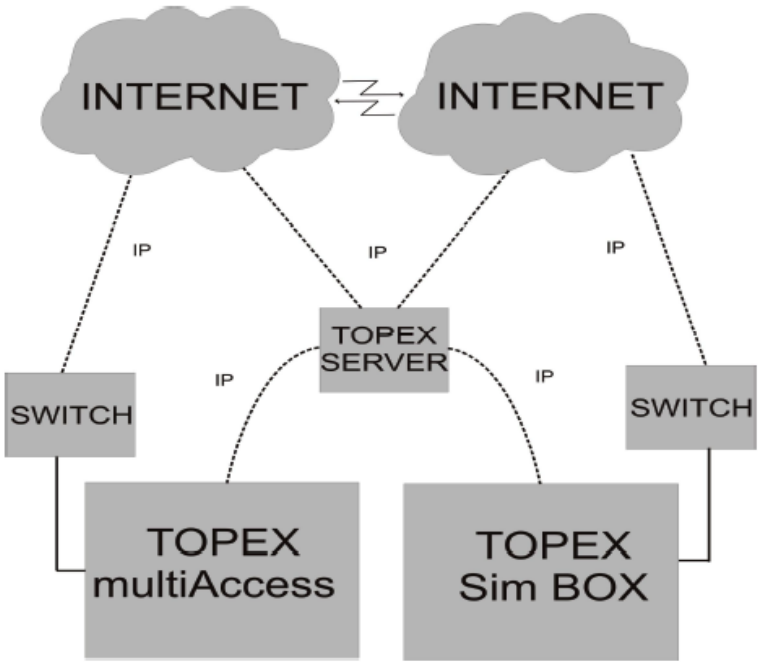
13.3.1 SIMServer

Charakterystyka urządzenia SIMServer:

- wirtualna alokacja SIM - zapewnia to uniwersalność i niższe koszty utrzymania kart SIM,
- centralne zarządzanie (dane ze wszystkich kart wszystkich SIMBoxów są przechowywane i zarządzane centralnie),
- równoczesny zdalny dostęp do kart SIM,
- alokacja kart SIM z uwzględnieniem zaawansowanej metody wyznaczania trasy rutingu po najniższych kosztach (ang. advanced LCR - Least Cost Routing Engine) - w dowolnym momencie dowolny SIM może być przydzielony dowolnej bramce w świecie,
- szczegółowy billing,
- urozmaicone algorytmy wyboru karty SIM,
- zarządzanie kartami SIM oparte na grupach (użytkownik może zdefiniować grupę mobilnych modułów, dla której będzie wyznaczona grupa kart SIM),
- zdalne zarządzanie poprzez sieci IP,
- alarmy systemu w czasie rzeczywistym (dotyczące zablokowanych SIM lub innych problemów) są wysyłane e-mailem, SMS lub telefonicznie. Użytkownik po wejściu do systemu widzi ostrzeżenia poprzez interfejs www,
- dodatkowe lokalne karty SIM mogą byś stosowane jako rezerwa (bramki na bieżąco wykorzystują wirtualne SIM z serwera, ale są w stanie współpracować z realnymi lokalnymi kartami SIM, tak się dzieje np. podczas awarii łączności IP),
- automatyczne wykrycie włożenia/wyjęcia SIM (płyty z kartami SIM można wymieniać w biegu, program skanuje SIMBox, aby wykryć zmiany i uaktualnia bazę danych),
- elastyczna integracja z modułami bramek.

Funkcje SIMServer

- wszystkie używane karty SIM są wirtualnie magazynowane i działają w ramach jednego centralnego "serwera SIM",
- serwer SIM przydziela kary SIM zdalnie w połączeniach IP,
- modemy GSM/UMTS mają dostęp do zdalnych SIM poprzez adapter terminala SIM lub emulator SIM.



Rysunek 13.4 Schemat systemu firmy Topex

SIMBox

Urządzenie SIMBox umożliwia zdalne zarządzanie i administrowanie kartami SIM zarejestrowanymi w sieciach różnych operatorów mobilnych. Poprzez interfejs www można monitorować szczegóły wszystkich operacji związanych z zarządzaniem kartami SIM. Zarządzanie urządzeniem odbywa się poprzez konsolę, która umożliwia przegląd parametrów sieciowych SIMBox takich, jak adres IP, maska, bramka, IP współpracującego serwera SIM itp. Dostęp do konsoli możliwy jest poprzez lokalnie szeregowe wejście lub poprzez Internet.

14. Załącznik 3 – Przykłady działań organizacji i podmiotów międzynarodowych

14.1 Przykłady działań wybranych zagranicznych administracji i organów regulacyjnych

Administracja Stanów Zjednoczonych podjęła działania w obszarze prawa handlowego mające na celu zwalczenie zjawiska polegającego na podszywaniu się pod numer abonenta wywołującego w transakcjach handlowych. Prezydent Obama podpisał dokument Dodd-Frank Wall Street Reform and Protection Act (Dodd-Frank Act), w którym m.in. wymieniono wykaz nadużyć związanych z tym problemem. Chociaż już wcześniej opublikowano inne dokumenty dotyczące wymiany towarów CEA (Comodies Exchange Act), umożliwiające ściganie i karanie tego zjawiska to Dodd-Frank Act jest pierwszym dokumentem adresowanym wprost do Kongresu.

Skala tego zjawiska w USA jest duża. Jeszcze zanim zaczął obowiązywać ww. akt prawny komisja CFTC (Commodity Futurres Trading Commission) nakładała kary na firmy uwikłane w ten proceder. W czerwcu 2013 r. CFTC ukarała firmę Panther za tego typu przestępstwa grzywną w wysokości 2,8 mln. dolarów. Wcześniej w grudniu 2012 r. komisja SEC (Securities ExcgangeCommission) nałożyła karę 250 tys. dolarów na firmę Biremis. We wrześniu tego samego roku, za tego typu przestępstwa została ukarana firma Hold Brothers przez regulatora FINRA (Financial Industry Regulatory Authority).

W nowym dokumencie wprowadzono poprawki w stosunku do wcześniejszych przepisów dotyczących wymiany i bezpieczeństwa wymiany danych podczas transakcji handlowych, w szczególności dodano w nim nowy rozdział zatytułowany Niedozwolone praktyki. Nadano też dodatkowe uprawnienia komisji CFTC w zakresie zapobiegania praktykom zakłócającym wymianę danych i minimalizowania wpływ tego nadużycia na funkcjonowanie rynku.

14.2 Referencje CEPT

CEPT (ang. European Conference and Postal and Telecommunications Administrations) przeprowadził analizę i przedstawił swoje stanowisko w sprawie zwalczania nadużyć związanych z podszywaniem się pod numer abonenta wywołującego w dwóch raportach:

- ECC Report 133 – Increasing Trust in Calling Line Identification and Originating Identification,
- ECC Recommendation 11/02 – Calling Line Identification and Originating Identification.

Zadaniem CEPT opisane tam problemy mogą być użyteczne dla ITU przy podejmowaniu w przyszłości inicjatyw i decyzji w sprawie polityk przyjętych w tym zakresie.

CEPT proponuje zastosowanie ewolucyjnego podejścia do używania wskaźnika CLI, polegającego m.in. na zogniskowaniu działań wokół scenariuszy, w których numery użyte jako wskaźniki CLI dla usług nie są bezpośrednio powiązane z tym numerem.

14.3 Rekomendacje Europejskiego Instytutu Standardów Telekomunikacyjnych ETSI

ETSI przedstawiło swoje rekomendacje dotyczące implementacji mechanizmów bezpieczeństwa komunikacji zapobiegające szeroko pojętym zagrożeniom oraz fraudom m.in. związanym ze zjawiskiem podszywania się pod inny numer niż rzeczywisty w dokumencie ETSI TR 185 008 V2.0.0 (2008-02).

W szczególności rozdział 6.5, zatytułowany Antispoofing, poświęcony jest zagrożeniom i funkcjonalnościom przeciwdziałającym tym zagrożeniom. Zarówno w tym rozdziale jak i w całym dokumencie nie ma odniesień bezpośrednio do zjawiska simboxingu, lecz do szerzej pojętego nadużycia, jakim jest podszywanie się pod numer abonenta wywołującego.

Zagrożeniami dla bezpieczeństwa komunikacji związanymi z tym zjawiskiem są m.in. nieautoryzowany dostęp, inicjowanie niezamawianej informacji, ukrywanie numeru abonenta A. Natomiast funkcjonalności m.in. takie jak autoryzowany dostęp, protokoły bezpieczeństwa oraz filtrowanie pakietów pozwalają zapobiegać i pomagają chronić zasoby sieci NGN przed atakami inicjowanymi z innych sieci. Jako mechanizmy związane z bramą w sieci użytkownika CNG (ang. Customer Network Gateway) rekomendowane są: autentykacja i autoryzacja, zarządzanie bezpieczeństwem Firewalling, Antispoofing oraz NAT (ang. Network Address Translation).

14.4 Rekomendacje ITU

Zagadnienie podszywania się pod numer abonenta wywołującego jest sprawą bardzo ważną dla ITU, o czym świadczy fakt, że ta kwestia została uwypuklona w wielu dokumentach, w szczególności w rezolucjach:

- WTSA-12 Resolution 65 on Calling Party Number Delivery, calling Line identification and origin identification,
- WTSA-12 Resolution 29 on Alternative Calling Procedure,
- PP-06 Resolution 21 on Alternative Calling Procedures on Telecommunication Networks,
- WTDC-10 Resolution 22 on Alternative Calling Procedures on Telecommunication Networks, Identification of Origin and Apportionment of Revenues, in Providing International Telecommunication Services.

Dla zapewnienia dostarczania informacji CLI, zgodnie z odpowiednimi zaleceniami ETSI we wszystkich krajach członkowskich UE, te zagadnienia znalazły się także w dokumencie International Telecommunication Regulations.

Ponadto zostały utworzone grupy robocze ITU-T SG2, SG3 oraz SG17, których zadaniem było prowadzenie prac studialnych dotyczących wpływu, jaki na koszty i bezpieczeństwo komunikacji wywiera brak identyfikacji strony inicjującej połączenie oraz podszywanie się pod numer abonenta A.

W wyniku prac grupy roboczej ITU-T SG2 zostało opublikowane zalecenie ITU-T E.157, w którym wymaga się dostarczania numeru strony inicjującej połączenia poprzez całą sieć i granice państw w formacie zgodnym z zaleceniem E.164. Prace grupy ITU-T SG2 w ramach zalecenia E.157 musiały być skorelowane z działaniami grupy ITU-T SG11 (np. w zakresie wymagań zawartych w zaleceniu Q.931) oraz z działaniami grupy ITU-T SG16 (np. w zakresie wymagań na protokół H.323), dla zapewnienia zgodności z postulatami zgłoszonymi w ww. rezolucjach.

Międzynarodowa Unia Telekomunikacyjna przedstawiła swoje działania, mające na celu zapobieganie przed podszywaniem się pod cudzy numer, na warsztatach ITU Workshop on „Caller ID Spoofing" zorganizowanych w Genewie 2 czerwca 2014 r. Warsztaty były połączone z sesją Grupy Roboczej ITU-T Study Group 2.

14.4.1 Aspekty regulacyjne dostarczania numeru abonenta A w związku z nadużyciami w opinii ITU

Na konferencji ITU Workshop on „Caller ID Spoofing" w Genewie zwrócono uwagę na problemy związane z obsługą CPND (ang. Calling Party Number Delivery), w szczególności na to, że:

- niektóre kraje nie mają możliwości zapewnienia dostarczania wskaźnika CLI,
- istotne zalecenia nie powinny być narzucane odgórnie, lecz ustalane na poziomie krajowym,
- może być trudne narzucenie wymagań na VoIP, w tym zakresie który nie podlega powszechnie obowiązującym wymaganiom,
- operatorzy potrzebują elastyczności w zarządzaniu swoimi sieciami i stosowaniu zaleceń,
- Prawo stosowane przez Państwa Członkowskie nie powinno być restrykcyjne ze względu na ewolucję technologii.

Postawiono też pytanie retoryczne, czy należy ograniczać wolność działania operatorów?

Ponadto zaproponowano żeby właściwa agencja określiła, które drogi rutingu będą używane dla połączeń międzynarodowych oraz dla ruchu wychodzącego biorąc pod uwagę koszty tranzytu.

Państwa Członkowskie powinny zapewnić, żeby były wykorzystywane tylko przydzielone do tego zasoby sieci w ruchu międzynarodowym.

14.4.2 Propozycje operatorów dotyczące rozwiązywania kwestii spornych związanych z nadużyciami telekomunikacyjnymi i3Forum

Operatorzy na zgromadzeniu i3Forum przeprowadzili analizę kilku ważnych ich zdaniem nadużyć telekomunikacyjnych z punktu widzenia scenariuszy realizacji fraudów. Przedstawili oni swoje konstatacje w dokumencie Fraud classification and recommendations on dispute handling within the wholesale telecom industry Release 3.0-May 2014 udostępnionym na stronie i3forum: http://i3forum.org/wp-content/uploads/2014/05/i3F-Fraud-Classification-Release-3-2014-05-12.pdf.

W dokumencie przedstawiono kwestie dotyczące postępowania w przypadku wystąpienia nadużyć na hurtowym rynku usług głosowych.

W dokumencie opisano scenariusze realizacji nadużyć oraz działania, które pozwalają uniknąć pewnych rodzajów nadużyć, przedstawiono podejście do detekcji nadużyć i do rozwiązywania wynikających z nich spornych problemów , przeanalizowano wpływ nadużyć na straty finansowe operatorów oraz ocenę nadużyć w kategoriach „zwycięzca", „przegrany".

Dokument potwierdza, że operatorzy posiadają odpowiednie struktury, kompetencje i środki, aby we własnym zakresie inicjować interaktywne pomiary i prowadzić analizy przepływu ruchu powiązanego z nadużyciami, a w razie konieczności blokować numery, na których dochodzi do nadużyć.

Zdaniem autorów, dokument powinien stanowić podstawę odniesienia przy podpisywaniu przez operatów klauzul kontraktowych z dostawcami usług, w odniesieniu do zidentyfikowanych typów nadużyć oraz warunków ukierunkowanych na blokowanie przepływów pieniężnych, które wzbogacają stronę realizującą nadużycie.

Ogólne rekomendacje podjęte na na zgromadzeniu i3Forum:

- Służby powołane przez operatorów do zwalczania nadużyć powinny analizować przepływ ruchu w sieci oraz obserwować miejsca w sieci, które mogą być potencjalnym źródłem sztucznego ruchu. Powinien być obserwowany ruch zarówno po stronie inicjującej połączenia, jak i po stronie docelowych gdzie połączenia są zakańczane.
- W razie potrzeby powinny być inicjowane sesje pomiarowe, podejmowane rozmowy dla wyjaśnienia zdarzenia, a nawet blokowany ruch o podejrzanym pochodzeniu.
- Informacja o zaistniałym zdarzeniu powinna być kolportowana do wszystkich stron mających związek z przepływem podejrzanego ruchu.
- Dla osiągnięcia jak najlepszego efektu rekomenduje się wdrożenie centralnej skrzynki mailowej, dostępnej dla wszystkich operatorów i dostawców usług.
- Powinny być generowane dwa odrębne komunikaty, zawierające co najmniej informacje dotyczące ram czasowych wystąpienia nadużycia (ang. timeframe), miejsca docelowego (ang. destination) i liczby minut trwania zdarzenia (ang. volume at that time).
- Kluczową sprawą przy wyjaśnianiu spornych kwestii związanych z nadużyciami jest przestrzeganie postanowień i harmonogramów, dla uniknięcia dodatkowych komplikacji w przypadku wyłamywania się jednej ze stron z poczynionych uzgodnień.

15. Załącznik 4 – Przegląd regulaminów świadczenia usług telekomunikacyjnych pod kątem zapisów zapobiegających zjawisku simboxingu

Operatorzy krajowych publicznych sieci ruchomych w regulaminach świadczenia usług telekomunikacyjnych umieszczają zapisy dotyczące zakazu stosowania w sieci urządzeń pozwalających na realizację simboxingu. Określają też działania restrykcyjne, które mogą być podjęte ze strony operatora w przypadku naruszenia postanowień regulaminu. Z przedstawionych poniżej przykładów wynika, że dotyczą one operatorów infrastruktury, ale także wirtualnych.

Celowo przytoczono obszerne fragmenty regulaminów w wersji źródłowej dla zobrazowania, w jaki sposób operatorzy krajowi formułują zapisy dotyczące zapobiegania nadużyciom telekomunikacyjnym w swoich sieciach oraz w jaki sposób różnią się te zapisy.

Wnioski

Zapisy w regulaminach dają podstawę prawną operatorom do podejmowania działań w stosunku do klientów.

Czterej główni operatorzy mogą, na podstawie zapisów (głównie w regulaminach świadczenia usług,) rozwiązywać umowy (blokować karty SIM) w przypadku wykorzystywania kart SIM w procederze simboxingu.

Polkomtel wprowadził definicję adaptera (urządzenia) umożliwiającego komunikację pomiędzy różnymi sieciami.

15.1.1 Polkomtel sp. z o.o – wyciąg z umowy i regulaminów świadczenia usług telekomunikacyjnych na abonament i na kartę

Pełny tekst Umowy o świadczenie usług telekomunikacyjnych („Umowa") – osoby fizyczne jest dostępny pod adresem (http://www.plus.pl/documents/16/ade5b062-133a-44a6-b845-1d90a319f903?title=Umowa_o_%C5%9Bwiadczenie_us%C5%82ug_telekomunikacyjnych_(Abonament).pdf)

W §5 Postanowienia końcowe znajduje się zapis, że:

1. Integralną częścią Umowy jest:

   a. Załącznik nr 1 – Regulamin świadczenia usług telekomunikacyjnych przez POLKOMTEL Sp. z o.o. - Abonament

W przytoczonym regulaminie operator zdefiniował pojęcie adaptera, który może być użyty do simboxingu:

„Adapter - urządzenie telekomunikacyjne umożliwiające podłączenie do sieci telekomunikacyjnej i kierowanie do niej lub modyfikowanie komunikatów, połączeń telefonicznych lub sygnałów pochodzących z innych sieci telekomunikacyjnych."

W Regulaminie świadczenia usług telekomunikacyjnych przez POLKOMTEL sp. z o.o. - Abonament, w szczególności w § 6 Wykonywanie Umowy. Odpowiedzialność znajdujemy (ew. są) następujące zapisy:

„9. Abonent zobowiązany jest do:

a. niepodejmowania jakichkolwiek działań powodujących zakłócenia pracy infrastruktury sieci telekomunikacyjnej i teleinformatycznej POLKOMTEL oraz sieci Internet lub zakłócenia pracy urządzeń aktywnych podłączonych do tych sieci,

b. niekorzystania z Usług niezgodnie z obowiązującym prawem, w tym nierozpowszechniania szkodliwych treści, w szczególności naruszających dobra osobiste, prawa autorskie lub prawa pokrewne,

c. nieużywania karty SIM z wykorzystaniem urządzenia kradzionego lub bez wymaganej homologacji lub certyfikatu,

d. nieużywania Adapterów bez zgody POLKOMTEL,

e. nieużywania Kart SIM aktywowanych w sieci POLKOMTEL w Adapterach bez zgody POLKOMTEL,

f. niekierowania do sieci telekomunikacyjnej (w tym do sieci POLKOMTEL) ruchu telekomunikacyjnego z innych sieci telekomunikacyjnych bez zgody POLKOMTEL,

g. niewykorzystywania Urządzenia telekomunikacyjnego lub Karty SIM niezgodnie z przepisami prawa lub z zawartą Umową lub w celu realizacji działań na szkodę POLKOMTEL lub osób trzecich,

h. nieudostępniania innym podmiotom Usług bez zgody POLKOMTEL w celu uzyskiwania korzyści majątkowych dla siebie lub osoby trzeciej,

i. niewysyłania niezamówionych informacji handlowych (spam),

j. niegenerowania sztucznego ruchu telekomunikacyjnego w sieci POLKOMTEL, to jest w szczególności ruchu, który nie służy nadawaniu, odbiorowi lub transmisji informacji kierowanych od lub do Abonenta, bądź którego głównym celem jest osiągnięcie korzyści majątkowej poprzez uzyskanie pewnej puli (liczby lub czasu trwania) połączeń pomiędzy siecią POLKOMTEL a innymi sieciami telekomunikacyjnymi,

k. nieużywania Karty SIM w celu prowadzenia działalności gospodarczej polegającej na masowym wykonywaniu połączeń (w tym połączeń telefonicznych, SMS, MMS) do wybranych osób lub grup osób (w tym tzw. „call center"), w szczególności poprzez automatyczną dystrybucję połączeń lub automatyczną, interaktywną obsługę osoby dzwoniącej lub integrację systemu telekomunikacyjnego i informatycznego,

l. niewykorzystywania telefonu lub Karty SIM bez zgody Polkomtel do rozwiązań telemetrycznych polegających na przesyłaniu informacji z/do systemów: pomiarowych, zdalnego sterowania, alarmowych, w tym w systemach monitoringu osób, budynków, pojazdów, a także informacji dodatkowych wysyłanych/ odbieranych przez te systemy"

Z kolei Regulamin świadczenia usług telekomunikacyjnych przez POLKOMTEL sp. z o.o. – „Na Kartę", w szczególności w § 6 Wykonywanie Umowy. Odpowiedzialność, zawiera następujące zapisy:

9. Abonent Na Kartę zobowiązany jest do:

a. niepodejmowania jakichkolwiek działań powodujących zakłócenia pracy infrastruktury sieci telekomunikacyjnej i teleinformatycznej POLKOMTEL oraz sieci Internet lub zakłócenia pracy urządzeń aktywnych podłączonych do tych sieci,

b. niekorzystania z Usług niezgodnie z obowiązującym prawem, w tym nierozpowszechniania szkodliwych treści, w szczególności naruszających dobra osobiste, prawa autorskie lub prawa pokrewne,

c. nieużywania karty SIM z wykorzystaniem urządzenia kradzionego bez wymaganej homologacji lub certyfikatu,

d. nieużywania Adapterów bez zgody POLKOMTEL,

e. nieużywania Kart SIM aktywowanych w sieci POLKOMTEL w Adapterach bez zgody POLKOMTEL,

f. niekierowania do sieci telekomunikacyjnej (w tym do sieci POLKOMTEL) ruchu telekomunikacyjnego z innych sieci telekomunikacyjnych bez zgody POLKOMTEL,

g. niewykorzystywania Urządzenia telekomunikacyjnego i Karty SIM niezgodnie z przepisami prawa lub z zawartą Umową lub w celu realizacji działań na szkodę POLKOMTEL lub osób trzecich,

h. nieudostępniania innym podmiotom Usług bez zgody POLKOMTEL w celu uzyskiwania korzyści majątkowych dla siebie lub osób trzecich,

i. niepodejmowania jakichkolwiek działań z użyciem Karty SIM służących skorzystaniu z Usług mimo braku w chwili inicjowania połączenia wystarczającej Wartości konta,

j. niewysyłania niezamówionych informacji handlowych (spam),

k. niegenerowania sztucznego ruchu telekomunikacyjnego w sieci POLKOMTEL, to jest w szczególności ruchu, który nie służy nadawaniu, odbiorowi lub transmisji informacji kierowanych od lub do Abonenta Na Kartę, bądź którego głównym celem jest uzyskiwanie pewnej puli (liczby lub czasu trwania) połączeń telekomunikacyjnych pomiędzy siecią POLKOMTEL a innymi sieciami telekomunikacyjnymi,

l. nieużywania Karty SIM w celu prowadzenia działalności gospodarczej polegającej na masowym wykonywaniu połączeń (w tym połączeń telefonicznych, SMS, MMS) do wybranych osób lub grup osób (w tym tzw. „call center"), w szczególności poprzez automatyczną dystrybucję połączeń lub automatyczną, interaktywną obsługę osoby dzwoniącej lub integrację systemu telekomunikacyjnego i informatycznego,

m. niewykorzystywania telefonu lub Karty SIM bez zgody POLKOMTEL do rozwiązań telemetrycznych polegających na przesyłaniu informacji z/do systemów: pomiarowych, zdalnego sterowania, alarmowych, w tym w systemach monitoringu osób, budynków, pojazdów, a także informacji dodatkowych wysyłanych/odbieranych przez te systemy,

n. Abonent Na Kartę będący konsumentem zobowiązany jest do korzystania z Usług wyłącznie w celach niezwiązanych bezpośrednio z jego działalnością gospodarczą lub zawodową,".

15.1.2 Orange Polska – wyciąg z regulaminów świadczenia usług na abonament i na kartę

Operator nie udostępnia na swojej stronie internetowej wzoru umowy, natomiast regulaminy są łatwo dostępne.

Regulamin świadczenia usług telekomunikacyjnych w Mobilnej Sieci Orange dla Abonentów ofert na abonament z dnia 13 listopada 2015 r. jest dostępny pod adresem:

(http://www.orange.pl/ocp-http/PL/Binary2/1997333/4090538941.pdf)

W regulaminie dla klientów z abonamentem, zastrzeżenie odnośnie do wykorzystania karty SIM jest ogólnikowe. W § 18 - Odpowiedzialność Abonenta zapisano, że:

„Abonent zobowiązuje się przestrzegać postanowień Regulaminu, zawartej umowy oraz szczególnych warunków oferty, w szczególności korzystać z usług zgodnie z ich przeznaczeniem".

W regulaminie dla klientów na kartę przypadek simboxingu jest precyzyjnie zdefiniowany i zabroniony. Regulamin świadczenia usług telekomunikacyjnych dla Abonentów ofert na kartę z dnia 01.01.2014 r. jest dostępny pod adresem: http://www.orange.pl/ocp-http/PL/Binary2/2004902/4106041121.pdf.

Regulamin w §18 Ograniczenie, rozwiązanie i wygaśnięcie Umowy zawiera następujące zapisy:

„1. Operator zastrzega sobie prawo do ograniczenia świadczenia usług telekomunikacyjnych lub rozwiązania Umowy w każdym czasie ze skutkiem natychmiastowym, bez odszkodowania oraz wcześniejszego uprzedzenia w razie:

1.1. podania przez Abonenta nieprawdziwych danych do Rejestracji;

1.2. nieuprawnionego dostępu do Sieci telekomunikacyjnej przez Abonenta;

1.3. **wykorzystywania numerów abonenckich** aktywowanych w Sieci telekomunikacyjnej Operatora **do kierowania do sieci** telekomunikacyjnej Operatora lub sieci innych przedsiębiorców telekomunikacyjnych, **ruchu pochodzącego z innych sieci telekomunikacyjnych, za pomocą urządzeń telekomunikacyjnych przy użyciu abonenckiej karty SIM;**

1.4 innego rażącego naruszenia przez Abonenta postanowień Regulaminu lub warunków Umowy, w szczególności w przypadku generowania sztucznego ruchu telekomunikacyjnego (tj. ruchu niesłużącego wymianie informacji; ruchu którego wyłącznym celem jest uzyskiwanie pewnej puli połączeń telekomunikacyjnych); używania karty SIM w celu prowadzenia działalności gospodarczej polegającej na masowym wykonywaniu połączeń telefonicznych, tzw. rozwiązań „call center"; używania karty SIM w systemach i urządzeniach służących do zautomatyzowanego przesyłania danych pomiarowych lub zdalnego sterowania, w tym w systemach monitoringu osób, budynków, pojazdów (tzw. rozwiązania telemetryczne) lub do generowania ruchu maszynowego (ruchu typu „maszyna do maszyny" lub „maszyna do Abonenta"); używania karty SIM do masowej dystrybucji SMS i/lub MMS, niebędącej standardową wymianą komunikatów np. rozsyłanie informacji handlowej; rozsyłania wiadomości SMS/MMS typu SPAM z numeru Abonenta; wykonywania połączeń, które są w dalszej kolejności przekierowywane za pomocą dowolnej technologii, a w szczególności w technologii POTS oraz transmisji danych VoIP (Voice over Internet Protocol); bądź w innych przypadkach udostępnienia usług Operatora innym osobom w celu uzyskania korzyści majątkowych bez zgody Operatora;".

15.1.3 P4 sp. z o.o. – wyciąg z umowy i regulaminów świadczenia usług dla abonentów i użytkowników

Operator umieścił jasny zakaz wykorzystania kart SIM do simboxingu zarówno w umowie jak i w regulaminie.

Pełny tekst umowy o świadczenie usług telekomunikacyjnych dla osób indywidualnych znajduje się pod adresem internetowym:

(http://www.play.pl/resources/pdf/2016/UMOWA-O-SWIADCZENIE-USLUG-TELEKOMUNIKACYJNYCH-indyw-nowy-numer-umowa-na-odl.pdf)

Postanowienia Ogólne zawierają następujące zapisy:

„pkt 16. Operator może, według własnego wyboru, rozwiązać Umowę w każdym czasie ze skutkiem natychmiastowym, bez zachowania okresu wypowiedzenia lub zawiesić świadczenie Usług Telekomunikacyjnych bez odszkodowania w przypadku:

e) gdy **Abonent będzie kierował do Sieci** Telekomunikacyjnej lub sieci innych przedsiębiorców telekomunikacyjnych, **za pomocą jakichkolwiek urządzeń telekomunikacyjnych, przy użyciu Karty SIM/USIM otrzymanej przez Abonenta, ruch pochodzący z innych sieci telekomunikacyjnych** bez zgody Operatora,

f) udostępniania usług Operatora innym osobom w celu uzyskania korzyści majątkowych bez zgody Operatora,

19. W ramach niniejszej Umowy, Abonent zobowiązuje się:

a) nie generować sztucznego ruchu nie służącego wymianie informacji, miedzy innymi z wykorzystaniem automatycznych systemów wywołujących,

b) nie używać Karty SIM/USIM w rozwiązaniach telemetrycznych,

c) nie używać Karty SIM/USIM do ruchu generowanego maszynowo, w szczególności ruchu typu „maszyna do maszyny" lub „maszyna do użytkownika",

d) nie używać Karty SIM/USIM do generowania ruchu, który ma charakter ataku Denial of Service,

e) nie wykorzystywać kart SIM/USIM do masowego rozsyłania informacji (SMS lub MMS) przeznaczonych bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku Abonenta lub innego podmiotu, lub w inny sposób służący osiągnieciu efektu handlowego (zakaz dotyczy Abonenta działającego jako przedsiębiorca lub na rzecz innego przedsiębiorcy),

f) nie wykorzystywać Kart SIM/USIM bez zgody P4 do inicjowania ruchu, polegającego na masowym wykonywaniu połączeń, w szczególności w przypadku automatycznej dystrybucji połączeń lub automatycznej interaktywnej obsługi numeru wywołanego lub w przypadku integracji systemu telekomunikacyjnego i informatycznego w celu obsługi tego ruchu lub przy wykorzystaniu kart w marketingu bezpośrednim (zakaz dotyczy Abonenta działającego jako przedsiębiorca lub na rzecz innego przedsiębiorcy)."

W części dotyczącej Oświadczenia Abonenta znajdują się następujące zapisy:

„Abonent oświadcza, ze otrzymał i akceptuje następujące dokumenty, które stanowią integralna cześć Umowy:

- Regulamin świadczenia Usług Telekomunikacyjnych przez P4 sp. z o.o. dla Abonentów

  Regulamin świadczenia Usług Telekomunikacyjnych przez P4 Sp. z o.o. dla Abonentów znajdujący się pod adresem:

(http://www.play.pl/resources/pdf/2016/Regulamin-swiadczenia-Uslug-Telekomunikacyjnych-dla-Abonentow_08062016.pdf)

zawiera następujące zapisy:

„§ 10. Zobowiązania Abonenta

1. Abonent zobowiązuje się:

a) do niepodejmowania jakichkolwiek działań powodujących albo mogących powodować zakłócenia pracy urządzeń aktywnych podłączonych do Sieci Telekomunikacyjnej lub sieci teleinformatycznej Operatora oraz sieci Internet;

b) nie kierować bez zgody Operatora do Sieci Telekomunikacyjne lub sieci innych przedsiębiorców telekomunikacyjnych za pomocą jakichkolwiek urządzeń telekomunikacyjnych przy użyciu Karty SIM/USIM otrzymanej przez Abonenta ruchu pochodzącego z innych sieci telekomunikacyjnych;

c) do korzystania z usług zgodnie z obowiązującym prawem;”

- Regulamin o Świadczeniu Usług Telekomunikacyjnych dla Użytkowników

  Regulamin o Świadczeniu Usług Telekomunikacyjnych dla Użytkowników znajduje się pod adresem:

  (**http://www.play.pl/resources/pdf/2016/Regulamin-swiadczenia-Uslug-Telekomunikacyjnych-dla-Uzytkownikow_15072016.pdf**)

  Regulamin w § 6. Zobowiązania Użytkownika zawiera następujące postanowienia:

  „1. Użytkownik zobowiązuje się:

  a) do niepodejmowania jakichkolwiek działań powodujących albo mogących powodować zakłócenia pracy urządzeń aktywnych podłączonych do Sieci Telekomunikacyjnej lub sieci teleinformatycznej Operatora oraz sieci Internet;

  b) **nie kierować bez zgody Operatora do Sieci Telekomunikacyjnej lub sieci innych przedsiębiorców telekomunikacyjnych za pomocą jakichkolwiek urządzeń telekomunikacyjnych przy użyciu Karty SIM/ USIM otrzymanej przez Użytkownika ruchu pochodzącego z innych sieci telekomunikacyjnych**; realizowanie połączeń za pomocą urządzeń końcowych przeznaczonych do przyłączenia do sieci stacjonarnej lub działających na podobnej zasadzie (zwanych dalej Urządzeniami FCT), w których wykorzystywane będą karty SIM/USIM działające w Sieci Telekomunikacyjnej, wymaga uzyskania od Operatora uprzedniej pisemnej zgody;

  c) do korzystania z usług zgodnie z obowiązującym prawem.”

15.1.4 T-Mobile – wyciąg z umowy i regulaminów świadczenia usług na rzecz abonamentów i na kartę

Operator udostępnia umowę o świadczenie usług telekomunikacyjnych pod adresem:

(**http://www.t-mobile.pl/r/repo1/tm/documents/doc_00003/D_003_0006102.pdf**).

Na mocy tej umowy, zgodnie z §3 2. Abonent nie może korzystać z Usług Telekomunikacyjnych w sposób naruszający prawo lub Umowę, a w szczególności nie może używać wydanych mu przez Operatora kart SIM:

„2.2 do innych działań powodujących lub mogących powodować zakłócenia pracy Sieci, urządzeń podłączonych do Sieci lub sieci Internet,

2.3 do kierowania do Sieci lub do innych sieci telekomunikacyjnych połączeń pochodzących z innych sieci telekomunikacyjnych, w szczególności w celu świadczenia usług telekomunikacyjnych osobom trzecim, bądź do udostępniania w inny sposób usług telekomunikacyjnych innym podmiotom, w tym w celu uzyskania korzyści majątkowej,

2.4 w urządzeniu telekomunikacyjnym realizującym funkcje zakończenia sieci stałej lub działającym na podobnej zasadzie, chyba ze Operator wyraził na to uprzednia pisemna zgodę,

2.5 do generowania automatycznego ruchu, w szczególności ruchu pomiędzy urządzeniami lub automatycznych połączeń pomiędzy urządzeniami a Abonentem,

2.6 do wspomagania lub budowania rozwiązań typu „call center", w tym do wykonywania połączeń telefonicznych w takich rozwiązaniach (nie oznacza to zakazu wykonywania połączeń do call center),

2.7 do masowego rozsyłania informacji (SMS lub MMS) przeznaczonych bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku Abonenta lub innego podmiotu, jak również przeznaczonych do osiągniecia jakiegokolwiek innego efektu handlowego (zakaz ten dotyczy Abonenta działającego jako przedsiębiorca),

2.8 do generowania sztucznego ruchu w Sieci, to jest w szczególności ruchu, który nie służy nadawaniu, odbiorowi lub transmisji informacji, bądź którego celem jest wygenerowanie pewnej ilości lub czasu połączeń."

Regulamin Świadczenia Usług Telekomunikacyjnych na rzecz Abonentów T-Mobile jest dostępny pod adresem:

(**http://www.t-mobile.pl/r/repo1/tm/documents/doc_00003/D_007_0005528.pdf.**

W tym regulaminie brak jest stosownych zapisów (przyjęto, że zapisy w umowie wystarczą).

Karta rejestracyjna T-Mobile na kartę - osoba fizyczna znajduje się pod adresem (**http://www.t-mobile.pl/r/repo1/tm/documents/doc_00008/D_003_0012846.pdf**. W Karcie umieszczono następujący zapis:

„Akceptuje warunki świadczenia usług telekomunikacyjnych określone w „Regulaminie Świadczenia Usług Telekomunikacyjnych przedpłaconych w systemie T-Mobile na kartę" „Regulaminie Świadczenia Usług Telekomunikacyjnych przedpłaconych Heyah na rzecz Użytkowników" „Regulaminie Świadczenia Usług Telekomunikacyjnych Przedpłaconych w Usłudze tuBiedronka".

Regulamin Świadczenia usług Telekomunikacyjnych Przedpłaconych w systemie T-mobile na kartę jest dostępny pod adresem:
(**http://www.t-mobile.pl/r/repo1/tm/documents/doc_00003/D_007_0000413.pdf**)

O przyczynach wygaśnięcia i rozwiązanie umowy mówią następujące zapisy §15 tego regulaminu:

„2. Operator może według własnego wyboru rozwiązać Umowę ze skutkiem natychmiastowym bez wcześniejszego uprzedzenia Użytkownika lub zawiesić świadczenie Usług Telekomunikacyjnych bez odszkodowania w przypadku, gdy Użytkownik rażąco narusza przepisy prawa lub postanowienia Umowy, w szczególności:

2.1. wykorzystuje Usługi Telekomunikacyjne świadczone przez Operatora w sposób naruszający prawo lub postanowienia Umowy;

2.3. podejmuje działania powodujące lub mogące powodować zakłócenia pracy urządzeń podłączonych do Sieci lub sieci Internet;

2.4. **kieruje do Sieci lub do innych sieci telekomunikacyjnych, za pomocą Karty SIM, połączenia pochodzące z innych sieci telekomunikacyjnych, w szczególności w celu świadczenia usług telekomunikacyjnych innym podmiotom;**

2.5**. wykorzystuje Kartę SIM w urządzeniach, które mogą być wykorzystywane do przekierowywania połączeń przychodzących z sieci innych operatorów, w szczególności w celu świadczenia usług telekomunikacyjnych innym podmiotom.**

2.6. generuje sztuczny ruch w Sieci, to jest w szczególności ruch, który nie służy nadawaniu, odbiorowi lub transmisji informacji, bądź którego celem jest wygenerowanie pewnej ilości lub czasu połączeń”

15.1.5 Virgin Mobile Polska Sp. z o.o. – wyciąg a regulaminu świadczenia usług

Zastrzeżenia zawarte w regulaminie blokują wykorzystanie karty SIM w bramce VoIP/GSM.

Regulamin Promocji „pakiety za #PółDarmo” zawiera informacje:

„44. W ramach korzystania z niniejszej Oferty Promocyjnej Abonent zobowiązuje się:

„a. nie generować sztucznego nie służącego do wymiany informacji;

b. nie używać Karty SIM/USIM w rozwiązaniach telemetrycznych, nie używać karty SIM/USIMw systemach i urządzeniach służących do zautomatyzowanego przesyłania danych pomiarowych lub zdalnego sterowania, w tym w systemach monitoringu osób, budynków, pojazdów;

c. nie używać Karty SIM/USIM do ruchu generowanego maszynowo, w szczególności ruchu typu „maszyna do maszyny” lub „maszyna do użytkownika”;

d. nie używać Karty SIM/USIM do generowania ruchu, który ma charakter Denial of service;

e. nie wykorzystywać Karty SIM/USIM bez zgody Virgin Mobile Polska do rozwiązań typu „call of center”;

f. nie używać Karty SIM/USIM do masowej dystrybucji SMS i/lub MMS nie będącej standardową wymianą komunikatów, nie rozsyłać wiadomości SMS/MMS typu SPAM stanowiących działania niezgodne z obowiązującymi przepisami.

45. W ramach oferty **abonent nie może wykonywać połączeń. które są w dalszej kolejności przekierowywane za pomocą dowolnej technologii**, a w szczególności w technologii POTS (konwencjonalnej analogowej linii telefonicznej) oraz **transmisji VoIP** (ang. Voice over Internet Protocol – Głos przez Protokół Internetowy).

46. W przypadku naruszenia przez abonenta któregokolwiek z postanowień określonych w punktach 44-45 niniejszej Oferty Promocyjne lub gdy do Virgin Mobile Polska wpłyną uzasadnione

skargi innych Abonentów w związku z otrzymywaniem wiadomości typu SMS typu SPAM z numeru abonenta stanowiącymi działania niezgodne z obowiązującymi przepisami, Operator może według własnego wyboru rozwiązać Umowę w każdym momencie ze skutkiem natychmiastowym (bez wcześniejszego uprzedzenia Abonenta) lub ograniczyć bądź zawiesić świadczenie Usług Telekomunikacyjnych. Pisemne potwierdzenie o rozwiązaniu umowy zostanie wysłane w formie wiadomości SMS."