POLITECHNIKA OPOLSKA

Wydział Elektrotechniki Automatyki i Informatyki

Kierunek: Informatyka

Specjalność : Informatyka Stosowana

Temat pracy magisterskiej:

Bezpieczeństwo sieci. Analiza zagrożeń

Network security. Threat analysis

Wykonawca:

inż. Bartłomiej Gierucki

Promotor:

dr inż. Joanna Kolańska

Opole 2019

Spis treści

Cel pracy

Celem mojej pracy magisterskiej jest przedstawienie zagrożeń wynikających z dzisiejszej ery możliwości zagrożeń cyfrowych. Wiadomo nie od dzisiaj, że postęp w dziedzinie elektroniki oraz możliwości cyfryzacji w globalnej sieci INTERNET jest nieunikniony. Jest to z jednej strony dobry symptom gdyż w wielu dziedzinach ery cyfryzacji dają ogromne możliwości rozwoju oraz ulepszają elementy oraz produkty już dostępne na rynku. W dziedzinie medycyny postęp jest tak szybki, że era komputerów stwarza ogromne możliwości wyeliminowania chorób oraz szerzenia się epidemii poprzez bieżące monitorowanie sytuacji. Dzięki cyfryzacji jesteśmy w stanie na bieżąco kontrolować swoje zdrowie dzięki aparaturze pomiarowej np. rezonans magnetyczny czy tomograf oraz jakże popularne EEG do badania fal mózgu. Możliwości zakupu towarów gdzie użytkownik jest w stanie dzięki swojemu komputerowi wybrać najwłaściwszy i konkurencyjny cenowo produkt daje możliwość zaoszczędzenia dużej sumy pieniędzy. Dzięki rozwojowi Internetu także branża mediów społecznościowych osiągnęła ogromny sukces. Dzięki portalom typu: facebook, nasza-klasa, instagram czy twitter jest możliwość odnaleźć dawnych znajomych czy odnowić z nimi stare znajomości. Dzięki portalom randkowym wiele osób znalazło tą przysłowiową drugą połówkę. Ja osobiście pamiętam jeszcze czasy gdzie aby napisać pismo urzędowe należało korzystać z maszyny do pisania i nie było tak prosto jak obecnie. Komputer dzięki programom wbudowanym w system operacyjny ma ogromne możliwości. Należy tylko potrafić tą wiedzę wykorzystać aby móc zarabiać pieniądze czy tworzyć nowe produkty. Dzięki oprogramowaniu typu Solid Works można budować konstrukcję, wymiarować elementy. A takie oprogramowanie jak EPLAN daje ogromne możliwości w dziedzinie projektowania szaf sterowniczych. Oprogramowanie Autocad znalazło zastosowanie w dziedzinach typu: Elektryczne, Wentylacyjne i wiele innych. Również architekci oraz designer wnętrz korzystają z możliwości wizualizacji oraz renderowania stworzonego obrazu. Dzięki postępowi cyfryzacji również księgowi nie potrzebują żmudnej i czasochłonnej pracy związanej z pisaniem i wyliczaniem na kartce papieru. Praktycznie każda branża dzięki cyfryzacji jest ułatwiona.

Powstawanie oraz era pojawienia się komputerów klasy PC oraz wyścigu firmy Microsoft oraz Apple doprowadziła według mojego mniemania do obecnego stanu

stabilności komputerów. Oprogramowanie Microsoft gdzie obecnie wiedzie prym Windows 10 jest ponoć najbardziej stabilnym w całej historii Microsoftu, którym założycielem był Bill Gates, który zaczynał swoją przygodę w garażu tworząc pierwsze środowisko imitacji systemu operacyjnego DOS. Natomiast Steve Jobs niestety już nieżyjący dążył do tego aby zastosować sprzęt idealnie dopasowany do oprogramowania. Zależało mu na stabilności systemu. Microsoft jeszcze 15 lat temu dawał możliwość inwencji twórczej dzięki konfiguracji podzespołów w komputerze klasy PC. Niestety odbijało się to na stabilności działania komputera. Do dnia dzisiejszego komputery klasy Apple czy to MacBook, iMac są świetnie dopasowane hardware-owo oraz software-owo. Coraz większą zyskują popularność w Polsce dzięki prostemu interfejsowi, stabilności oraz bezpieczeństwu użytkowania. Oczywiście alternatywą do tych dwóch systemów jest jeszcze system operacyjny Linux stworzony przez Linusa Torvaldsa fińskiego programistę. Jest to system darmowy, wykorzystywany do użytkowników bardziej zaawansowanych. W tym środowisku przedstawię metody „hakowania" wykorzystując środowisko Kali Linux 2.0. System ten opiera się na konsoli, w której należy posługiwać się komendami. Służy również do stawiania serwerów.

Od samego początku zbudowania komputera pojawiały się wirusy. Jednym z pierwszych wirusów, który został zidentyfikowany o nazwie Brain atakował pierwszy sektor dyskietek włożonych do zarażonych komputerów. Został odkryty w 1986 roku. Autorami byli dwaj Pakistańczycy , bracia AmjadFarooq i BasitFarooqAlvi [1]. Jako jednego z pierwszych uważa się ElkCloner napisany przez Richarda Skrentę w roku 1986. Miał 400 linii kodu i udawał program bootujący. Wirus działał na systemie operacyjnym DOS 3.3 i również rozprzestrzeniał się na dyskietki. Wirus ten został napisany na sprzęcie Apple. Gdy komputer został zainfekowany, co 50 uruchomień wyświetlał wierszyk: [2]

Elk Cloner: The program with a personality
It will get on all your disks
It will infiltrate your chips
Yes, it's Cloner!
It will stick to you like glue
It will modify RAM too
Send in the Cloner!

Pierwszy wirus w 1971 roku pojawił się Creeper kiedy zaczął powstawać Internet. Była to sieć typu ARPANET. Został stworzony przez programistę Boba Thomasa. Jego celem miało być wyświetlanie komunikatu o treści – Jestem Creeper, złap mnie jeśli potrafisz? Od tamtej pory ilość wirusów znacząco wzrosła. W 1990 roku sklasyfikowano 1300 wirusów a w roku 2000 było ich 50 tysięcy. W chwili obecnej szacuje się że jest obecnych ponad 200 milionów wersji różnego rodzaju złośliwego oprogramowania. [3]

Natomiast pierwszy program antywirusowy powstał w roku 1983 i napisał go Czech Pavel Baudisz na komputerze Olivetti M24.

Rys.1. Stary computer-avast-olivetti-m24

[1]https://blog.avast.com/pl/7-rzeczy-kt%C3%B3rych-prawdopodobnie-nie-wiedzieli%C5%9Bcie-o-ava%C5%9Bcie z dnia 7.07.2019 r.

W 1999 roku powstał pierwszy robak o nazwie Mellissa, który atakował pliki pakietu biurowego Microsoft Word. Rozprzestrzeniał się dzięki programowi pocztowemu Outlook gdzie wykorzystywał kontakty zapisane w programie. Jego działanie polegało na szyfrowaniu plików i żądaniu zapłaty 100 dolarów jeśli chce się odzyskać dane.

Bardzo niebezpiecznym wirusem stworzonym najprawdopodobniej na potrzeby agencji wywiadowczej Izraela był wirus Stuxnet, który został odkryty 15 lipca 2010 roku przez specjalistów IT z Białorusi. Był to rootkit, który wykorzystywał lukę typu 0-day. Wirus był rozpowszechniany za pomocą zainfekowanych pamięci USB. Atakował sterowniki PLC z rodziny Siemensa SIMATIC S7-300 oraz S7-400. Zmieniał ustawienia częstotliwości prądu wirówek gazowych Irańskiej elektrowni atomowej. Celem wirusa było przejęcie kontroli oraz dostęp zdalny do systemu. Ten wirus uważa się za najbardziej zaawansowany i przełomowy kod w historii. [4 5]

W miarę postępu rozwoju komputerów klasy PC Internet stał się łakomym kąskiem zarobku dla hakerów. Hakerzy to osoby, które znakomicie orientują się w świecie IT. Są specjalistami w budowie komputera oraz oprogramowania. Często są to programiści, którzy są w stanie napisać program typu exploit do uzyskania dostępu do komputera. Świetnie znają system operacyjny Linux dzięki wbudowanym programom oraz znajomości konsoli są w stanie realizować swoje praktyki. Obecnie, dzięki wbudowanemu oprogramowaniu typu metasploit w systemi Linux nawet małoletni uczniowie (Script Kids) gimnazjum są w stanie uzyskać nieautoryzowany dostęp do czyjegoś niezaktualizowanego komputera. Aby temu przeciwdziałać należy bezwzględnie aktualizować system, korzystać z programu zabezpieczającego system w czasie rzeczywistym (połączenie programu antywirusowego oraz zapory sieciowej zwanej firewallem). No i oczywiście aktualizacja tyczy się wszystkich programów wykorzystywanych do pracy, gdyż hakerzy mogą uzyskać dostęp nie tylko przez lukę w systemie. Najgroźniejsza jest jednak podatność ludzka, która w największym stopniu ma wpływ na działanie osób trzecich. Nieklikanie w linki nieznanych wiadomości przychodzących na adres mailowy. Uważne przeglądanie forów internetowych i nieklikanie w podejrzane linki.

W przypadku bankowości internetowej zabezpieczenia banków są bardzo dobre. I tutaj hakerzy wykorzystują podatność użytkownika a nie serwera banku. W tym celu są wysyłane emaile praktycznie identyczne do prawdziwej witryny banku. W wysłanym przez hakerów formularzu proszą o identyfikator, hasło i jednorazowy kod. Kiedyś bardzo popularne były kody w zdrapce, obecnie wykorzystywane są hasła smsowe. Po otrzymaniu tych danych haker za pomocą jednego kodu smsowego jest w stanie zrobić przelew na maksymalną kwotę dostępną na koncie ofiary. Bardzo popularny był również atak na podszywanie się pod konsultant telefonii banku. W sieci istnieją serwisy w których można

podszyć się po dany numer telefonu i za pomocą socjotechniki uzyskać w przypadku większości użytkowników wszystkie potrzebne dane do realizacji kradzieży pieniędzy. Osoby mniej techniczne również udawało się nabrać wysyłając sms-a z prośbą o podanie hasła jednorazowego i przesłanie go sprawcy w celu weryfikacji. Przestępca dzięki programowi keyloggerowi zainstalowanemu na komputerze ofiary jest w stanie odczytać sekwencję znaków wpisywanych na komputerze ofiary. Dzięki połączeniu z serwerem udaje mu się uzyskać login i hasło ofiary. Prośba natomiast o kod smsowy daje mu możliwości przelewu na swoje konto.

Bardzo popularne były również kradzieże pieniędzy za pomocą skimmingu czyli kopiowania kart bankomatowych. Działo się tak gdyż, przestępcy instalowali skimmery w bankomatach i dzięki wbudowanej kamerze odczytywali numer pin. W ten sposób byli w stanie wypłacić pieniądze które były na koncie. Oczywiście kwotę, która była limitowana lub też i nie.

Rys.2. Zielony skimmer imitujący anti-simmerową nakładkę

[2] https://niebezpiecznik.pl/post/nowy-ultracienki-skimmer-niepostrzezenie-odczytuje-paski-kart-w-bankomatach z dnia 7.07.2019 r.

W internecie bardzo popularne są płatności kartą kredytową. Umożliwia to numer karty, kod CVC2 oraz data wydania. Niestety nie wszystkie serwisy (według mojej wiedzy mniej niż połowa) udostępniają metodę płatności 3D-Secure, która polega na dodatkowej autoryzacji kodem smsowym lub wygenerowanym przez token. Dzięki oprogramowaniu szpiegującemu można uzyskać dane: numer karty, data wydania i kod CVC2. Wtedy drzwi dla hakera są otwarte.

Niestety często oprogramowanie antywirusowe nie wykrywa oprogramowania szpiegującego, gdyż haker infekując komputer wgrywa backdoora i dobrze maskuje w komputerze ofiary. Dzięki maskowaniu system antywirusowy nie jest w stanie go zidentyfikować. Jedynie takie oprogramowanie można zidentyfikować programami typu sniffer. Bardzo dobrym programem tego typu jest np. Wireshark. Umożliwia on identyfikację całego ruchu sieciowego. Niestety jest to zadanie trudne i wymaga wiedzy dotyczącejprotokołów całej strefy OSI, portów TCP i UDP. W przypadku identyfikacji oprogramowania szpiegującego należy przeinstalować system operacyjny.

Dlatego w celu bezpieczeństwa należy wykonywać regularnie backupy danych na dysku twardym. Nie instalować programów pochodzących z nie zaufanego źródła oraz zachować rozwagę przy korzystaniu z cudzych nośników danych (wspomniana infekcja wirusem Stuxnet). Dla zapewnienia większego bezpieczeństwa swoich danych zalecane jest stosowanie szyfrowania danych. Umożliwiają to wbudowane programy zarówno na Windowsa jak i Linuxa. IOS marównież wbudowaną funkcję szyfrowania danych w system. Popularnym programem jest Bitloker, który stosuje algorytm szyfrowania AES 128 lub 256 bitowy. AES 128 bit jest tak bezpieczny, że gdyby trylion maszyn, z których każda mogła analizować miliard kluczy na sekundę, pracowała dwa miliardy lat, to klucz AES-128 zostałby złamany.[6] Dotyczy to ataku typu bruteforce czyli sprawdzania każdej możliwej kombinacji znaków. Natomiast algorytm został złamany przez profesora z Shanghai Jiao Tong University w Chinach, o pseudonimie YuYu. Wykorzystał on metodę typu side-channel. Do łamania haseł wykorzystuje się również metodę słownikową oraz tablice tęczowe.

W celu zapewnienia bezpieczeństwa bardzo ważne jest stosowanie innych haseł w różnych serwisach internetowych. Bywa to bardzo uciążliwe ale na szczęście istnieją programy typu Lastpass, które umożliwiają tworzenie bazy haseł w chumurze. Hasła są szyfrowane i na pewno bardziej bezpieczne niż zapisane w naszym komputerze czy na kartce papieru. W celu ochrony środków dostępnych na koncie bankowym zaleca się ustawienie limitów.

2. Wprowadzenie

2.1 Opis środowiska Kali Linux

Do przeprowadzenia testów penetracyjny wykorzystano środowisko testowe Kali Linux 2018, który został uruchomiony za pomocą maszyny wirtualnej VirtualBox. Jest to środowisko wykorzystywane przez specjalistów IT do przeprowadzania:

1) Rekonesansu
2) Skanowania
3) Wykorzystania luk
4) Utrzymania dostępu
5) Zacierania śladów

Kali Linux to otwarty projekt open source. Bazujący na systemie Debianie wykorzystywany do łamania zabezpieczeń i testów penetracyjnych. Poprzednia wersja nazywała się BackTrack. Obecnie Kali Linux zawiera dużo programów do przeprowadzania audytów. [7]

Rys.3. Środowisko testowe Kali Linux

Kali Linux jest wspierany przez organizację Offensive Security specjalizującą się w testach zabezpieczeń, szkolenie oraz wydawaniem certyfikatów. Czy testy penetracyjne są legalne?Jeśli wykonujemy testy penetracyjne w sieci w której jesteśmy administratorami to tak.Jeśli natomiast wykorzystamy naszą wiedze do przełamania zabezpieczenia bez zgody właściciela i uzyskania dostępu jest to przestępstwo karane grzywną, ograniczeniem wolności albo pozbawieniem wolności do lat 2. Jest to art. 267 § 1 i 2 kodeksu karnego. [8]

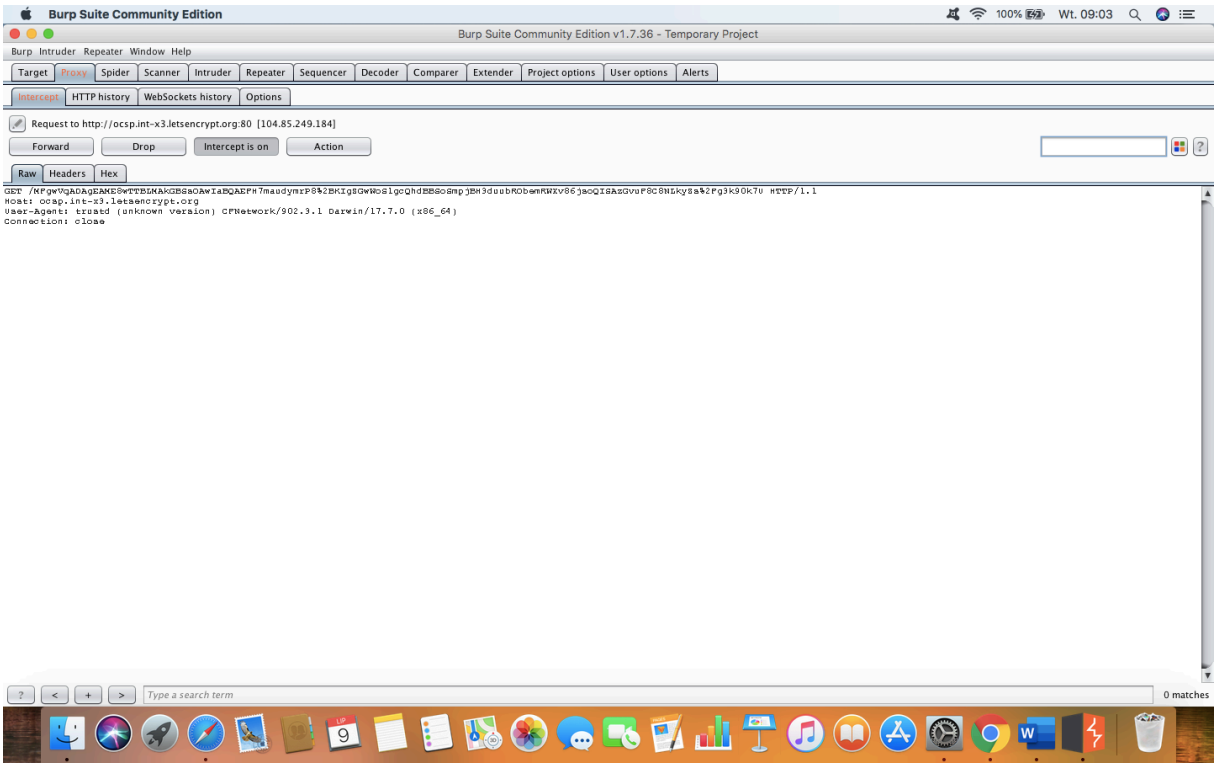
2.2 Wykorzystanie niezbędnego oprogramowania w systemie Kali Linux

1. **Hydra** popularny łamacz hasełktóry może być użyty z różnych źródeł: http, ftp, telnet etc. Wykorzystuje do łamania procesor. To niestety w dużym stopniu opóźnia proces odnajdywania hasła.
2. **Aircrack-ng** – narzędzie sieciowe służące do detekcji, przechwytywania pakietów i analizy sieci Wi-Fi. Umożliwia łamanie zabezpieczeń WEP, WPA/WPA2-PSK. Do prawidłowego działania aplikacji potrzebna jest karta sieciowa obsługująca tryb monitor (RFMON). Aircrack-ng dostępny jest na platformę Linux (posiada wsparcie techniczne) oraz Microsoft Windows (brak wsparcia technicznego). [9]
3. **Metasploit** – otwarte narzędzie służące do testów penetracyjnych i łamania zabezpieczeń systemów teleinformatycznych. Metasploit zawiera bazę gotowych exploitów oraz udostępnia interfejs, dzięki któremu można przygotowywać własne, korzystając z gotowych komponentów.

   Metasploit został przygotowany w 2003 roku w języku Perl. Od wersji 3.0 został całkowicie przepisany w języku Ruby. Środowisko może być uruchamiane na wielu wersjach systemu Unix i Linux oraz w systemie Windows.

   W październiku 2009 projekt Metasploit został przejęty przez firmę Rapid 7 specjalizującą się w oprogramowaniu do zarządzania podatnościami systemów [10]
4. **Hashcat-** program do łamania haseł, umożliwia wykorzystanie karty graficznej do łamania hasła. Dzięki temu proces odnajdywania hasła jest dużo szybszy.
5. **Nmap-** najpopularniejszy dostępny skaner portów. Wykorzystywany przy procesie skanowania otwartych portów danego celu (adresu IP). Jego wersją GUI jest Zenmap dla początkujących użytkowników.
6. **BurpSuite-** graficzne środowisko do testowania zabezpieczenia stron WWW. Pozwala testować ruch http/https pomiędzy przeglądarką a serwerem. Prostota, duża funkcjonalność stawia te oprogramowanie wysoko cenione przez specjalistów IT.

7. **Nikto-** skaner podobny do Nessusa do przeprowadzania sieciowych testów penetracyjnych. Narzędzie szuka przestarzałych wersji oprogramowania i błędów konfiguracji.
8. **DirBuster-** jedno z lepszych narzędzi do wyszukiwania ukrytych katalogów aplikacji sieciowych.
9. **OpenVas-** skaner sieciowy, który jest gałęzią programu Nessus.
10. **WPScan –** to skaner podatności systemu typu CMS WordPress, który jest bardzo popularny.



Rys.4. BurpSuite Community Edition

2.3 Najpopularniejsze rodzaje ataków internetowych oraz przeprowadzanie rekonesansu

W celu przeprowadzeniu testu penetracyjnego działania należy zacząć od Rekonesansu czyli uzyskania danych z subdomen, aderów IP czy innych ogólnodostępnych informacji. Podstawą rekonesansu jest wykorzystanie przeglądarki internetowej w celu zdobycia informacji. Za pomocą zaawansowanego algorytmu wyszukiwania jesteśmy w stanie uzyskać naprawdę sporo informacji o danym celu.

Wyszukiwanie za pomocą przeglądarek nazywa się rekonesansem pasywnym co oznacza, że nie zostawiamy śladu. Trzy filtry, które są najczęściej używane do Google hackingu to:

intitle – wyszukiwanie określonych fraz w opisie tytule strony

inurl – wyszukiwanie określonych fraz w adresie URL

filetype – wyszukiwanie wybranych rodzajów plików dla danej frazy[11]

Wpisanie frazy cameralinksysinurl:main.cgiumożliwia przykładowy podgląd kamery „na żywo”

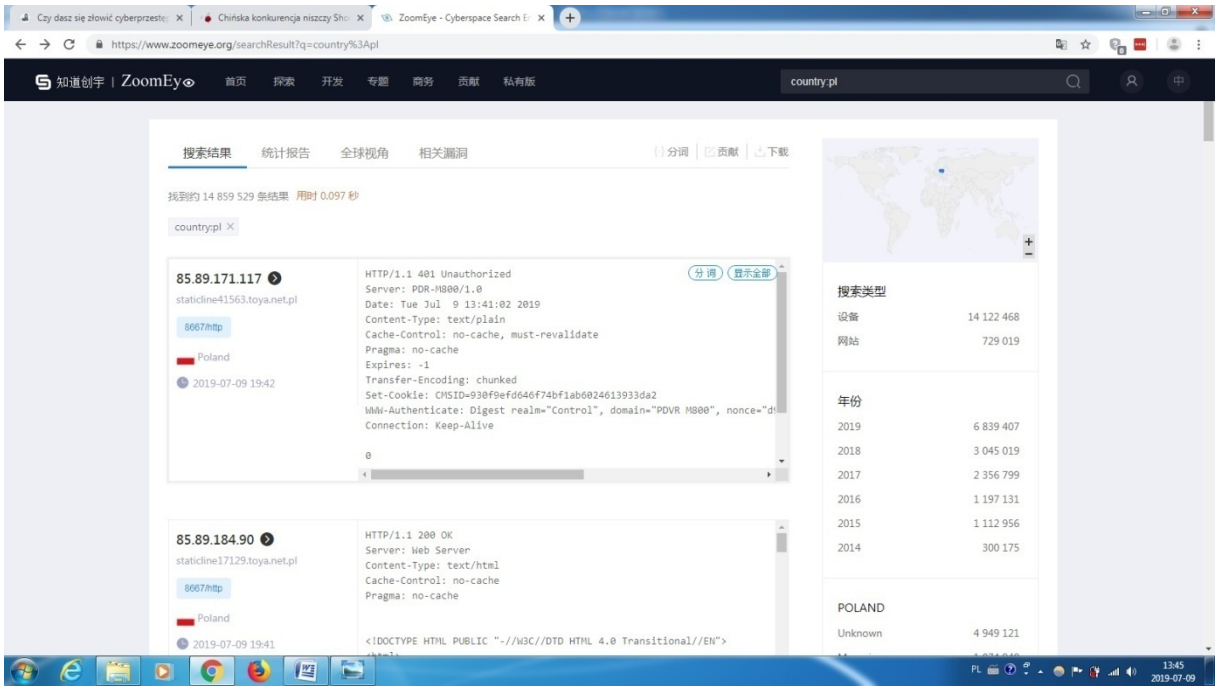
Z ciekawszych dostępnych w sieci informacji można znaleźć:

- Dostęp do urządzeń firmowych np. kamer VOIP (live),
- Pliki konfiguracyjne serwerów i aplikacji których ujawnienie może być potencjalnie niebezpieczne,
- Prywatne pliki użytkowników, które nie powinny znajdować się w sieci,
- Pliki z hasłami zapisanymi jawnym tekstem,

Ciekawym serwisem jest http://exif.regex.info w którym użytkownik jest w stanie sprawdzić czy zdjęcie nie zostało spreparowane oraz kiedy faktycznie je wykonano. Dodatkowo serwis oferuje histogram. Serwis jest darmowy.

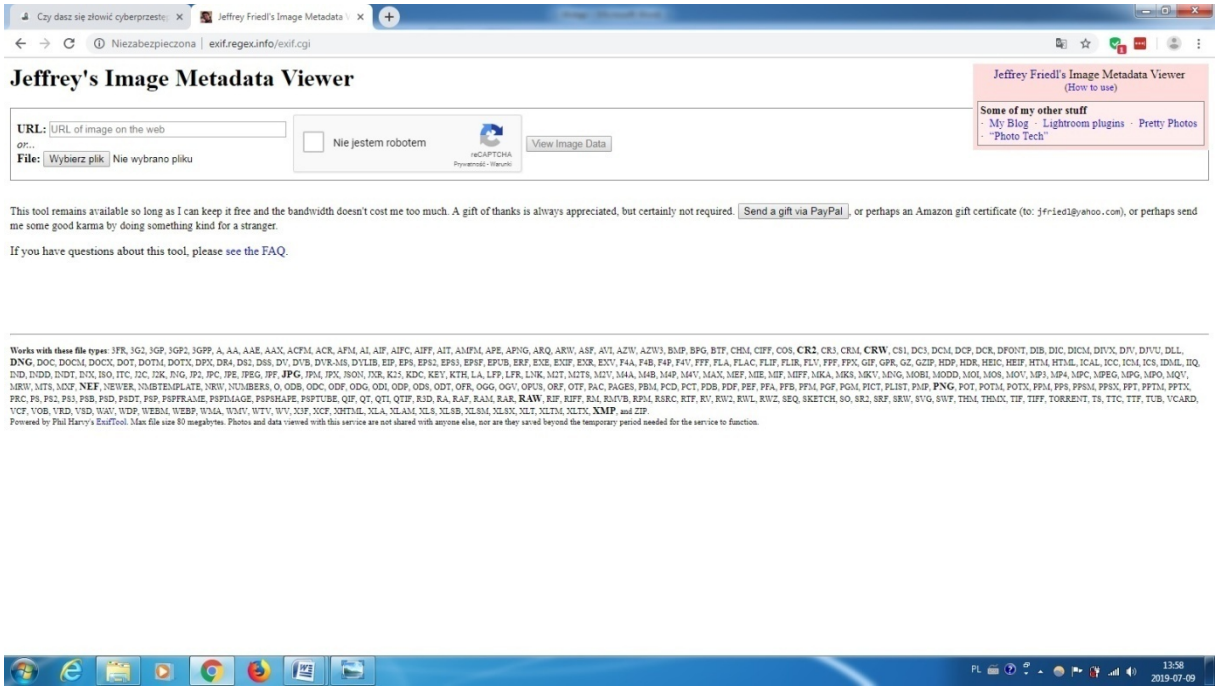
Kolejnym interesującym serwisem jest https://tineye.com, który umożliwia sprawdzenie czy dane zdjęcie znajduje się w zasobach Internetu. Ma obszerną bazę danych w której można sprawdzić czy ktoś nie wykorzystał zdjęcia w celach nieuprawnionych.

Dostępny Chiński serwis: www.zoomeye.org umożliwia ogromne możliwości rekonesansu pasywnego, w którym mamy możliwość zobaczyć infrastrukturę dostępną na publicznych adresach IP. Rozpoznać – czyli poznać dostępne tam domeny, urządzenia (wraz z ich typami) czy nawet aplikacje z konkretnymi (czasem podatnymi) wersjami. Serwis podobno lepszy od Shodana, który również oferuje wyszukiwanie komputerów, urządzeń sieciowych czy urządzeń pracujących na specyficznych wersjach oprogramowania. [12]



Rys.5. Zoomeye.org

[5]https://www.zoomeye.org/searchResult?q=country%3Apl z dnia 7.07.2019 r.



Rys.6. exif.regex.info serwis do sprawdzania meta danych fotografii

[6]http://exif.regex.info/exif.cgi z dnia 7.07.2019 r.

W celu przeprowadzania rekonesansu haker zainteresowany jest następującymi danymi:

- adres IP oraz adres MAC celu
- spis stron internetowych ofiary i dane w nich publikowane (sprawdzenie ukrytej zawartości za pomocą oprogramowania DirBuster)
- wersja systemu na którym pracuje ofiara bądź serwer
- informacje o użytkowniku lub użytkownikach danego systemu
- czy serwer korzysta z IDS (intrusionprevention system)
- fizyczna budowa Siecie
- otwarte porty w komputerze ofiary bądź serwerze
- exploity umożliwiające dostęp do komputera ofiary, ofiar [13]

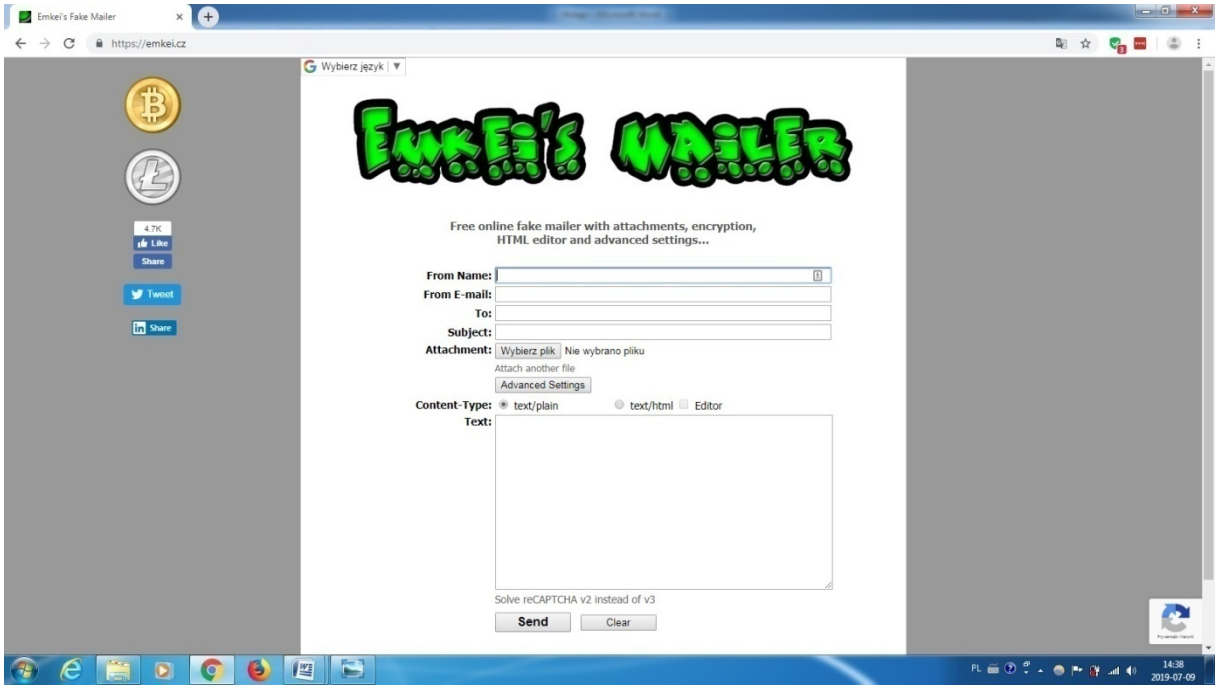
Aby przeprowadzić skan pasywny można wykorzystać do tego serwis hardenize.com. Umożliwia on przeprowadzenie audytu w obszarach: DNS, mail czy problemów z certyfikatami SSL. Dużą zaletą jest to, że jest darmowy.

Phishing

Phishing to inaczej fishing czyli „łowienie ryb" oznacza to, iż haker zamiast wykonywać zaawansowane metody uzyskania niepowołanego dostępu do komputera „zarzuca przynętę" i czeka, aż użytkownik da się zmanipulować. Celem hakera jest podszycie się np. pod Urząd Skarbowy, Bank, osobę której ufasz czy inną instytucję rządową. Kiedy ofiara otrzyma wiadomość i kliknie w nią (może to być wiadomość email wraz z linkiem lub załącznikiem). Może to być wiadomość email łudząco podobna do wiadomości przychodzących z danego Banku. I co najważniejsze wiadomość wysłana przez hakera jest wysłana z adresu prawdziwego Banku!!! Tak to nie żart, istnieją serwisy, które to umożliwiają. Tak więc ciężko odróżnić jest wiadomość spreparowaną przez oszusta. Serwisem oferującym wysłanie emaila z dowolnym adresem np. listy@prezydent.pl jest czeski portal www.emkei.cz.

Jeśli otworzysz wspomniany załącznik z obcej wiadomości lub też nie to w konsekwencji pozwoli przestępcy kontrolować komputer, podsłuchiwać komunikację co oznacza, że jest w stanie przejąć Twoje loginy i hasła.Domenę na która przestępca skłania

nas przekserować i uzyskać dostęp do loginu i hasła może być również przypominać prawdziwą domenę. Oto 2 przykłady: https://rnBank.pl, https://mbank.pl [14]



Rys.7. emkei.cz, portal, który umożliwia wysłanie wiadomości z dowolnego adresu

[7] https://emkei.cz z dnia z dnia 7.07.2019 r.

Jeszcze jednym ciekawym serwisem jest pipl.com, który oferuje gigantyczną bazę danych kontaktów (w tym numerów telefonów i kont w mediach społecznościowych) Wyświetla również informację o zdjęciach danego użytkownika w celu identyfikacji. Niestety od niedawna nie jest darmowym serwisem. Można znaleźć parę rekordów rejestrując się do demo wersji serwisu. Bardzo ciekawa alternatywa dla poszukiwania kogoś w Internecie.

W Internecie również można sprawdzić drzewo genealogiczne swoich przodków, istnieje w tym celu parę serwisów jak np. findmypast.com czy myheritage.pl

Niekwestionowaną bazą danych w Polsce jest system CEPIK czyli Centralna Ewidencja Pojazdów i Kierowców, od niedawna w wersji 2.0. Korzystać z niego mogą: Policja, Straż Graniczna, Żandarmeria Wojskowa, Służby Specjalne, prokuratura, Okręgowe Stacje Kontroli Pojazdów czy kancelarie komornicze. System został od niedługiego czasu również udostępniony każdej osobie, która chce otrzymać informację o samochodzie (ważność polisy OC oraz badania technicznego pojazdu). Za pomocą systemu Cepik 2.0 możemy również

sprawdzić ilość punków karnych oraz przebieg auta jak również czy Autobus, którym udaje się nasza pociecha na wakacje jest sprawny.

Do uzyskania tych informacji potrzebny jest Profil Zaufanylub e-dowód (dotyczy to punktów karnych oraz usługi Mój Pojazd).
W celu weryfikacji potencjalnego zakupu samochodu potrzebny jest nam tylko numer rejestracyjny pojazdu, numer VIN oraz pierwsza rejestracja.

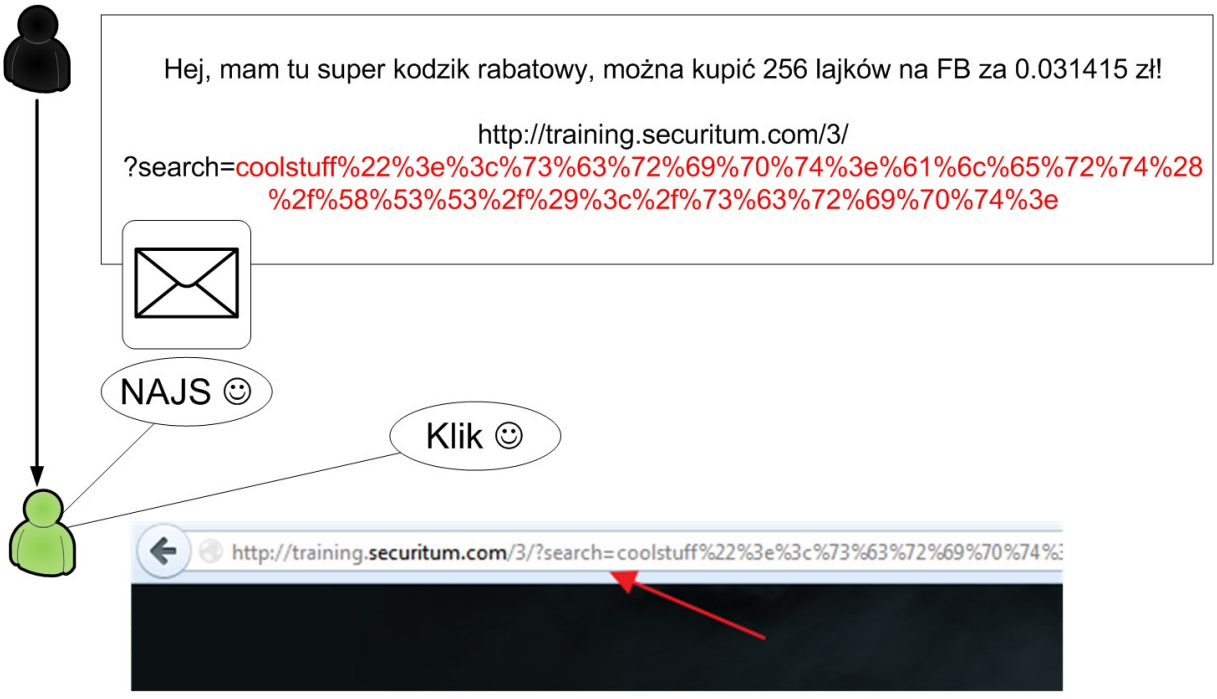
Innym ogromnym źródłem danych jest system KSIP- Krajowy System Informacji Policji. Jest tosystem zamknięty i odseparowany od sieci Internetowej. Instytucje Wojskowe oraz firmy które narażone są na ataki hakerów są odseparowane od sieci INTERNET w celu nie wypłynięcia tajnych danych.

Na koniec informacji o rekonesansie należy wspomnieć o darknecie, potocznie zwanej siecią TOR. Jest to odseparowana sieć, w której użytkownik łączy się poprzez kilka serwerów. A że transmisja jest szyfrowana do niedawna uważano sieć Tor za pełni anonimową. Obecnie rząd Stanów Zjednoczonych ma możliwość monitorowania dowolnego szerokopasmowego połączenia z Internetem dzięki urządzeniom wprowadzonym na podstawie Communications Assistance for Law EnforcementAct (CALEA) i dlatego może kontrolować oba punkty końcowe połączeń Tora, wykonywanych na terytorium USA. O ile Tor chroni przed analizą ruchu, nie może zapobiec potwierdzeniu komunikacji [15]. Sieć tor posiada adresy w domenie (jakiś_adres.onion). Znajduję się wiele for dyskusyjnych gdzie można zakupić skradzione bazy danych użytkowników, kart kredytowych, dane personalne. Zakupić substancję psychoaktywne czy nawet broń. Jest to również raj dla pornografii dziecięcej, gdzie pedofila i osoby z nią powiązane czują się bezpiecznie. TOR powstał w celu anonimizacji użytkownika i miał zamysł być stosowany w krajach gdzie demokracja delikatnie rzecz biorąc kuleje. Jak wygląda to dzisiaj, każdy może wypracować swoje indywidualne zdanie na ten temat. Aby uzyskać dostęp do sieci Tor potrzebna jest tylko przeglądarka dostępna w sieci INTERNET oraz znajomość adresy serwisu w sieci TOR.

2.4 Najważniejsze wady aplikacji webowych

Za czynnik największego ryzyka uważa się luki bezpieczeństwa w warstwie dostępu do danych, ponieważ grożą one ujawnieniem całego zbioru danych, mogącego zawierać ważne dane osobowe i hasła. Dlatego dostęp do bazy danych musi być wyjątkowo dobrze chroniony i zabezpieczony przed atakami. Najwięcej danych znajduje się w warstwie aplikacji, a za ich występowanie odpowiadają programiści. Serwer sieciowy łączy użytkownika z resztą aplikacji. Dlatego serwer musi być dobrze chroniony przed ujawnieniem newralgicznych danych[16]

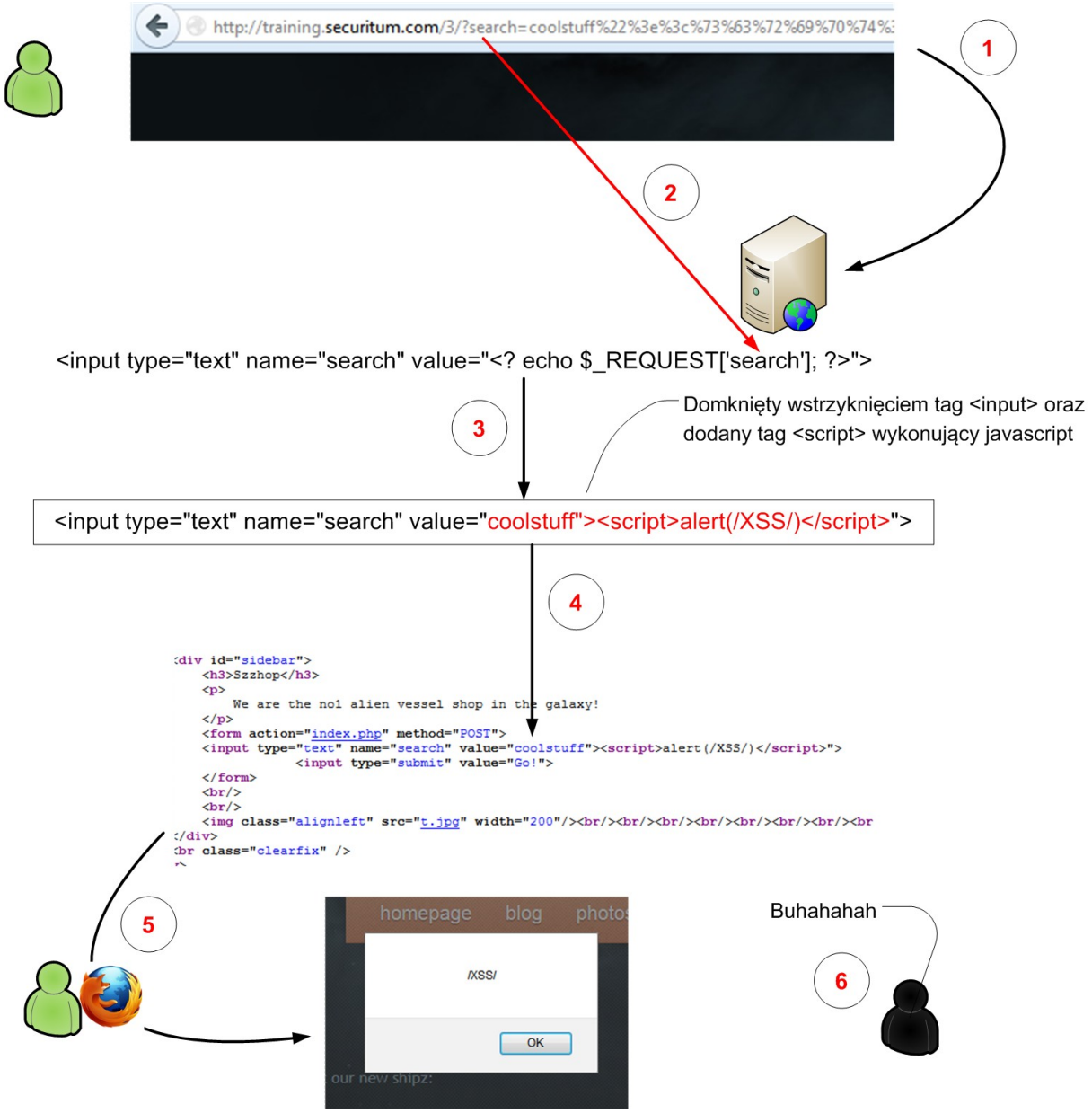
a) Atak typu XSS- (Cross-sitescripting) polega na przekazywaniu wrogich skryptów pomiędzy stronami WWW a przeglądarkami użytkowników. Dzięki temu atakowi haker jest w stanie uzyskać dostęp do konta użytkownika oraz uzyskać informację dotyczącą jego loginu i hasła do serwisu. Może również odczytać zawartość Cookiem. Dzięki atakowi XSS haker jest w stanie przekierować nieświadomego użytkownika do kontrolowanych przez siebie witryn internetowych. Przestępca wykorzystuje podatności w skryptach np. Javascript, AJAX, JSON czy Flash. Poniżej



przykładowy atak podatności XSS

Rys.8. Atak typu XSS

[8]https://sekurak.pl/czym-jest-xss z dnia 7.07.2019 r.



Rys.9. Atak typu XSS c.d

[9]https://sekurak.pl/czym-jest-xss z dnia 7.07.2019 r.

b) Wstrzykiwanie kodu SQL

Jest to atak na bazę danych znajdującą się po stronie serwera. Atak bazuje na nieautoryzowanej modyfikacji kodu SQL co wynika z tego, że język ten jest językiem interpretowanym. Oznacza to, że każdy przesłany do baz danych, poprawny składniowo ciąg znaków zostanie przez serwer wykonany. [17]

c) Przepełnienie bufora

Przepełnienie bufora ma na celu zmianę sposobu działania programu tak aby program wykonał kod przygotowany przez atakującego. Atak jest możliwy dzięki modyfikacji wartości rejestrów, który pozwala na zmianę programu.

Jeżeli atakujący wyśle do bufora za pomocą debuggera własny kod i zmieni wartość rejestru EIP, uruchomiony zostanie w buforze wrogi kod.

2.5 Ataki CSRF

Atak typu CSRF (cross-siterequestforgery) polega na wykonaniu przez ofiarę pewnej czynności ale bez użycia skryptu jak w przypadku XSS. Celem jest przeglądarka internetowa, w której ofiara jest uwierzytelniona. W przypadku ataku CSRF luka pozwala przejąć napastnikowi tożsamość ofiary i w jej imieniu wykonać różne czynności. Technika ta jest często wykorzystywana w celu zmiany w podatnej witrynie danych użytkownika, np. adresu email, numeru telefonu lub adresu pocztowego. [17]

2.6 Algorytmy szyfrowania w Internecie

Aby zapewnić bezpieczeństwo danych w Internecie stosuje się zabezpieczenia, które mają zapewnić poufność danych. Przeglądarka WWW powinna zapewniać bezpieczny kanał wymiany danych między użytkownikiem a serwerem, do którego nie powinien mieć dostępu nikt inny. Przechowywane na serwerze dane również powinny być zaszyfrowane w celu uniemożliwienia zdobyć ich przez hakerów. Niestety algorytm MD5 w dalszej części zostanie zaprezentowany jako możliwy do złamania.

Szyfrowanie to najpowszechniej akceptowana forma kryptografii wykorzystywana do ochrony informacji. Zapewnia ochronę między innym przed sniffigiem- czyli podsłuchaniem. Niestety cały czas trwa wyścig pomiędzy hakerami a specjalistami w dziedzinie IT, gdzie Ci drudzy są o krok dalej przed hakerami. Dlatego tak ważne są aktualizacje systemów

operacyjnych oraz urządzeń (nawet drukarki czy telewizora) w celu uniemożliwienia nieautoryzowanego dostępu.

Najpopularniejszym systemem zapewniającym bezpieczeństwo danych w połączeniu(między użytkownikiem a serwerem) jest łącze SSL (SecureSocketLayer).

Protokół został opracowany w 1994 r. w firmie Netscape. W 1999 r organizacja IETF opublikowała protokół Transport Layer Security (TLS) będący rozwinięciem protokołu SSL w wersji 3. Obecnie jest uważany za niebezpieczny a najlepszym środkiem zaradczym jest korzystanie z wersji 1.2. Podczas przesyłania tak newralgicznych danych jak numery kart kredytowych czy dane personalne zawsze powinno korzystać się z najnowszej wersji protokołu TLS.

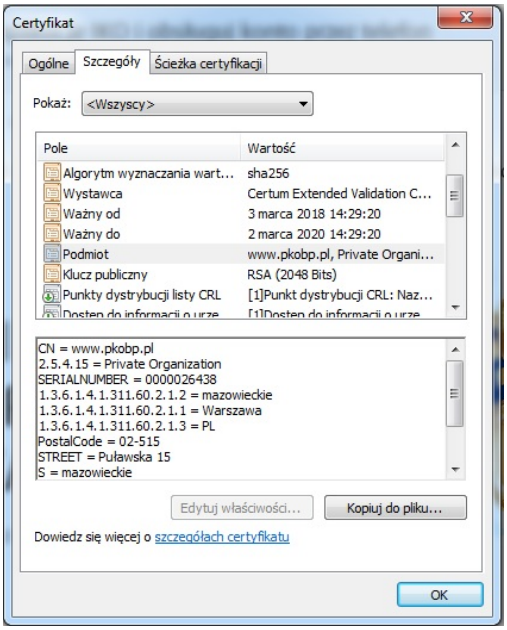
Szyfrowanie symetryczne polega na wykorzystaniu tego samego klucza do szyfrowania jak i rozszyfrowania danych w związku z czym należy znaleźć bezpieczny sposób przekazu klucza drugiej stronie. Wykorzystywane jest do szyfrowania dużych porcji danych w przeciwieństwie do szyfrowania asymetrycznego. Algorytm szyfrowania symetrycznego dzieli się na dwie grupy: szyfry blokowe oraz szyfry strumieniowe. Najpopularniejszealgorytmyszyfrowania to DES- Data Encryption Standard, AES- Advance EncryptionStandard, RC4- Rivest Cipher 4.

Szyfrowanie asymetryczne polega na wykorzystaniu dwóch kluczy tzn. klucza publicznego i prywatnego. Szyfrowanie to jest bezpieczniejsze od szyfrowania symetrycznego. Klucz publiczny jest dostępny dla każdego natomiast klucz prywatny już nie. Dane zaszyfrowane za pomocą jednego klucza można rozszyfrować tylko przy użyciu drugiego.

Proces szyfrowania odbywa się wieloetapowo, ale dla użytkownika przebiega niepostrzeżenie. Proces można podzielić na 2 etapy. W pierwszej fazie następuje szyfrowanie asymetryczne a w drugiej symetryczne.

1) Następuje komunikacja pomiędzy klientem a serwerem, w której klient przedstawia numer wersji SSL i obsługiwane algorytmy szyfrowania

2) W odpowiedzi serwer wysyła informację o obsługiwanych przez siebie wersjach SSL i algorytmach szyfrowania, po czym strony wybierają wspólną najnowszą wersję. Serwer dostarcza klientowi również certyfikat SSL zawierający klucz publiczny i ogólne informacje o serwerze.
3) Klient uwierzytelnia serwer, weryfikuje certyfikat, który znajduje się na komputerze lokalnym. Klient sprawdza czy certyfikat jest zaufany, czyli czy organ certyfikacyjny podpisał dany certyfikat
4) Następuje wygenerowanie przez klienta tajnego klucza sesji a następnie zaszyfrowanie tego klucza za pomocą publicznego klucza serwera i wysłanie go do serwera
5) Serwer jest w stanie rozszyfrować informację dzięki kluczowi prywatnemu (dzieje się tak gdyż klucz prywatny został zaszyfrowany kluczem publicznym serwera). Następnie następuje generowanie przez klienta i serwer w kilku etapach klucz sesji. Klucz sesji ma za zadanie szyfrować dane podczas sesji (jest to szyfrowanie symetryczne). Dodatkowo w celu weryfikacji obliczany jest skrót, który dodawany jest do wiadomości. Jest to tak zwana funkcja mieszająca, która dodatkowo wzmacnia bezpieczeństwo algorytmu szyfrowania. W protokole SSL wykorzystuje się algorytm SHA- (SecureHashAlgorithm) obejmującą całą rodzinę funkcji mieszających. [16 17]



Rys.10. Certyfikat PKO BP

[10] www.pkobp.pl z dnia 14.09.2019 r.

2.7 Atak Man in the Middle

Atak typu Man In the middle na SSL (w tłumaczeniu człowiek pośrodku) to typ ataku, który polega na przepuszczeniu informacji przez komputer napastnika aby ten mógł podejrzeć i zmanipulować te dane przed przesłaniem ich w miejsce docelowe.

Przeprowadzenie tego ataku jest możliwe tylko jak haker znajduje się w środku połączenia użytkownika i serwera sieciowego. Haker jest w stanie deszyfrować dane pomiędzy użytkownikiem a serwerem tylko jeśli przedstawi użytkownikowi fałszywy certyfikat. Taki certyfikat oczywiście jest inny od certyfikatu instytucji z która chce się połączyć klient. Klient otrzyma ostrzeżenie w oknie przeglądarki. Po zaakceptowaniu fałszywego certyfikatu haker jest w stanie manipulować w połączeniu pomiędzy ofiarą i np. Bankiem.

3. System podmiany SMS-a w telefonie komórkowym

Zdecydowana większość użytkowników jest nieświadoma możliwości podmiany zawartości SMS-a w ich telefonie. Zmiana treści SMS jest możliwa poprzez modyfikację ustawień w PDU w programie PDUspy. Inną metodą jest wysyłanie komend za pomocą terminala połączonego za pomocą modemu GSM z komputerem. W celu przeprowadzenia przykładowego ataku, wybrano metodę z wykorzystaniem programu PDUspy. W tym celu spreparowano dwie wiadomości wysłane w przeciągu 2 minut, o zmienionej treści.

Interpretujemy:
- zwykły SMS- Standardowa wiadomość SMS,
- Flash SMS- Wiadomość wyświetlana w formie "alertu" /komunikatu,
- Silent / Ping SMS- Typ wiadomości, który nie wyświetla się na telefonie odbiorcy ale pozwalają m.in. na odebranie raportu.

Za pomocą PDU- "surowy" format wiadomości, jesteśmy w stanie spreparować SMS- a. TPDU- Transport Protocol Data Unit jest to format enkapsulacji wiadomości.

Wybrane pola TPDU:

1. SCA (Service-Center-Address) Numer SMS Centrum. Istnieje możliwość wprowadzenia wartości 00, aby SMSC zostało wybrane automatycznie.
2. TP-MTI- Określanie typu wiadomości, tj. SMS-DELIVERY, SMS-DELIVERY-REPORT, SMS-SUBMIT, SMS-SUBMIT-REPORT, SMS-COMMAND, SMS-STATUS-REPORT, Reserved.
3. TP-DCS(TP-Data-Coding-Scheme) Określenie schematu kodowania, m.in. wielkości alfabetu, tj. 7-bit(text), 8-bit(binaty) oraz 16-bit (UCS-2 / text).
4. TP-VP Ważność wiadomości.
5. TP-UD (TP-User-Data) Zawiera dane użytkownika, np. tekst wiadomości.
6. TP-UDL (TP-User-Data-Lenght) Określa długość TP-UD.
7. TP-DA Adres docelowy.
8. TP-PID (TP-Protocol-Identifier) Pozwala na odniesienie się do wyższej warstwy protokołu, m.in. dzięki niemu możemy wysyłać "inne typy" wiadomości. [18]

Przykładowy format PDU wiadomości: 07918497908916F0040B918497090458F70000917031713465800550F95B1C06

Do przeprowadzenia operacji podmiany SMS-a niezbędny jest modem GSM oraz Konwerter USB- UART. Poniżej znajdują się dane sprzętu zakupionego u sprzedawcy w popularnym Polskim serwisie aukcyjnym.

Moduł GSM GPRS GA6

Moduł zbudowany na układzie GA6, jest znakomitą alternatywą dla układów z serii SIM900, SIM800. Komunikacja z mikrokontrolerami odbywa się poprzez interfejs UART oraz polecenia AT. Idealnie nadaje się do współpracy z Arduino, Raspberry Pi bądź innymi mikrokontrolerami z interfejsem UART.

- Chip: GA6,
- Częstotliwości sieci GSM 850/900/1800/1900MHz (praca w polskich sieciach GSM),
- Napięcie zasilania przez złącze microUSB: 5V,
- Napięcie zasilania - pin VCC_IN: 5V - 9V,
- Interfejs UART TTL - poziomy dopuszczalne napięć 3.3V,
- Domyślna prędkość transmisji : 115200bps, istnieje możliwość zmiany komendami AT,
- Wbudowany mikrofon,
- Supportvoicecalls,
- Support SMS messages,
- Support GPRS data service, maximum data rate, download 85.6Kbps, upload 42.8 Kbps,
- Support standard GSM07.07, 07.05 the AT command,
- Złącze katy: micro SIM,
- 2 x złącze anteny SMA oraz IPEX,
- Złącze do podłączenia mikrofonu elektretowego,
- Złącze do podłączenia słuchawek,
- Diody LED sygnalizujące pracę modułu,
- W zestawie antena 2dbi,
- Wymiary: 45*45mm.

ZASILANIE: Moduł GSM posiada wbudowana przetwornicę DCDC, dzięki temu może być zasilany napięciem 5V przez złącze microUSB, lub od 5V do 9V przez pin Vcc_IN, o wydajności prądowej ok 2A. Tak duży prąd jest pobierany tylko chwilowo, np w momencie logowania się do sieci GSM, przy normalnej pracy układ zadowala się kilkudziesięcioma mA, a w trybie uśpienia nawet 3mA. Dlatego jeżeli układ nie będzie odnajdywał sieci, bedzie miał problem z zalogowaniem, lub sam się resetował, w pierwszej kolejności należy sprawdzić zasilanie.

Port UART: Do dyspozycji mamy dwa porty UART. Oznaczony jako H_TXD oraz H_RXD, służy wyłącznie do aktualizacji oprogramowania układu GA6, natomiast piny opisane jako U_RXD oraz U_TXD, służą do komunikacji np z mikrokontrolerem, przez ten port sterujemy modułem przez komendy AT. [19]

Rys.11. Moduł GSM GPRS GA6

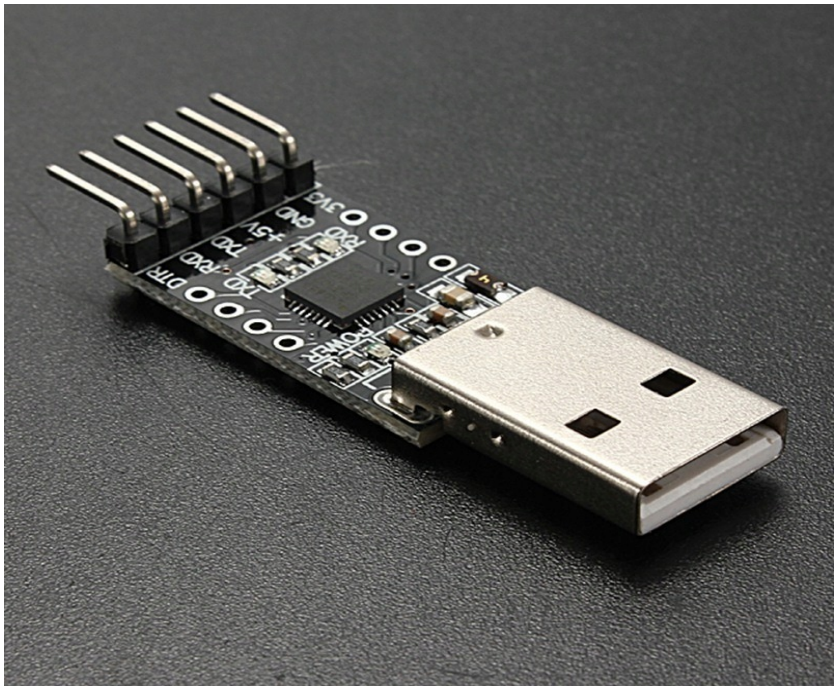
[11] https://allegro.pl/oferta/modul-gsm-gprs-a6-sms-antena-arduino-sim900-8002890305 z dnia 12.04.2019 r.

USB - UART CP2102

Konwerter USB - UART. Moduł przydatny wszędzie tam gdzie potrzebne jest połączenie komputera z układem za pomocą interfejsu UART (RS232 TTL)., np. moduły GPS, GSM, mikrokontrolery. CP2102 może być podłączony bezpośrednio z układami ARDUINO mini , umożliwia ich programowanie lub zostać wykorzystany do transmisji danych przez interfejs UART. Konwerter można bezpośrednio podłączyć z układami o logice 3.3V lub 5V, wybór napięcia nie wymaga żadnych zmian w ustawieniach konwertera.

- Zastosowany układ: CP2102
- Wtyk USB - typ A
- Współpraca z układami 3.3V oraz 5V
- Wydajność prądowa pinu 3.3V to tylko max 50mA
- Diody LED sygnalizujące zasilanie
- Diody LED sygnalizujące wysyłanie oraz odbieranie danych
- Sygnały na listwie goldpin: RX, TX, DTR, CTS, GND , VCC
- Obsługiwany w systemach: Windows XP/Server 2003/Vista/7/8/8.1/10/WinCE/Macintosh OSX/Linux/Android

[20]



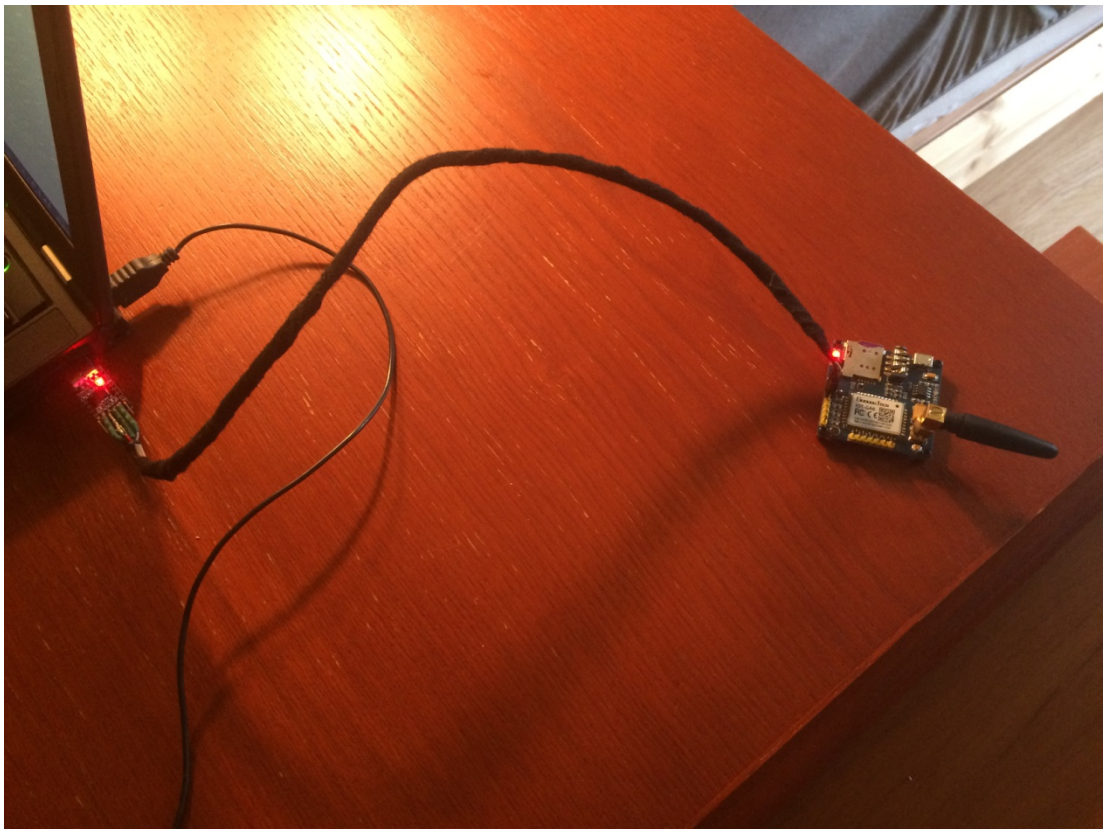
Rys.12. UART CP2102

[12] https://allegro.pl/oferta/cp2102-usb-uart-konwerter-rs232-arduino-7477037761] z dnia 12.04.2019 r.

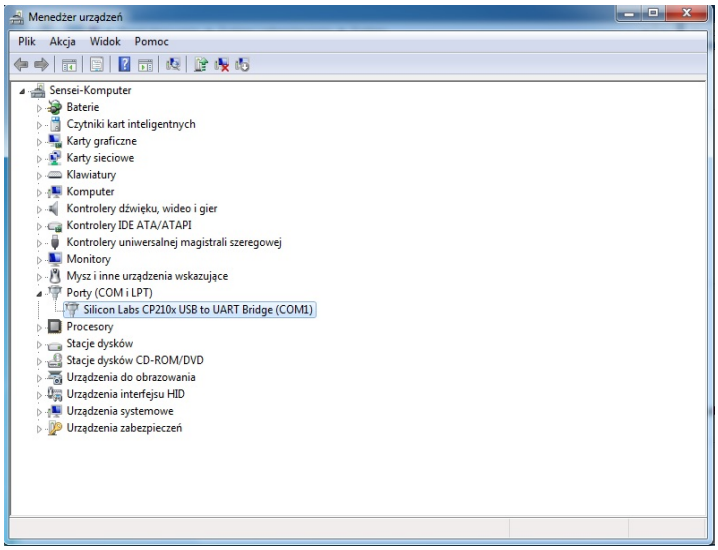
Prezentacja podmiany SMS-a

1.1 Instalacja sterownika

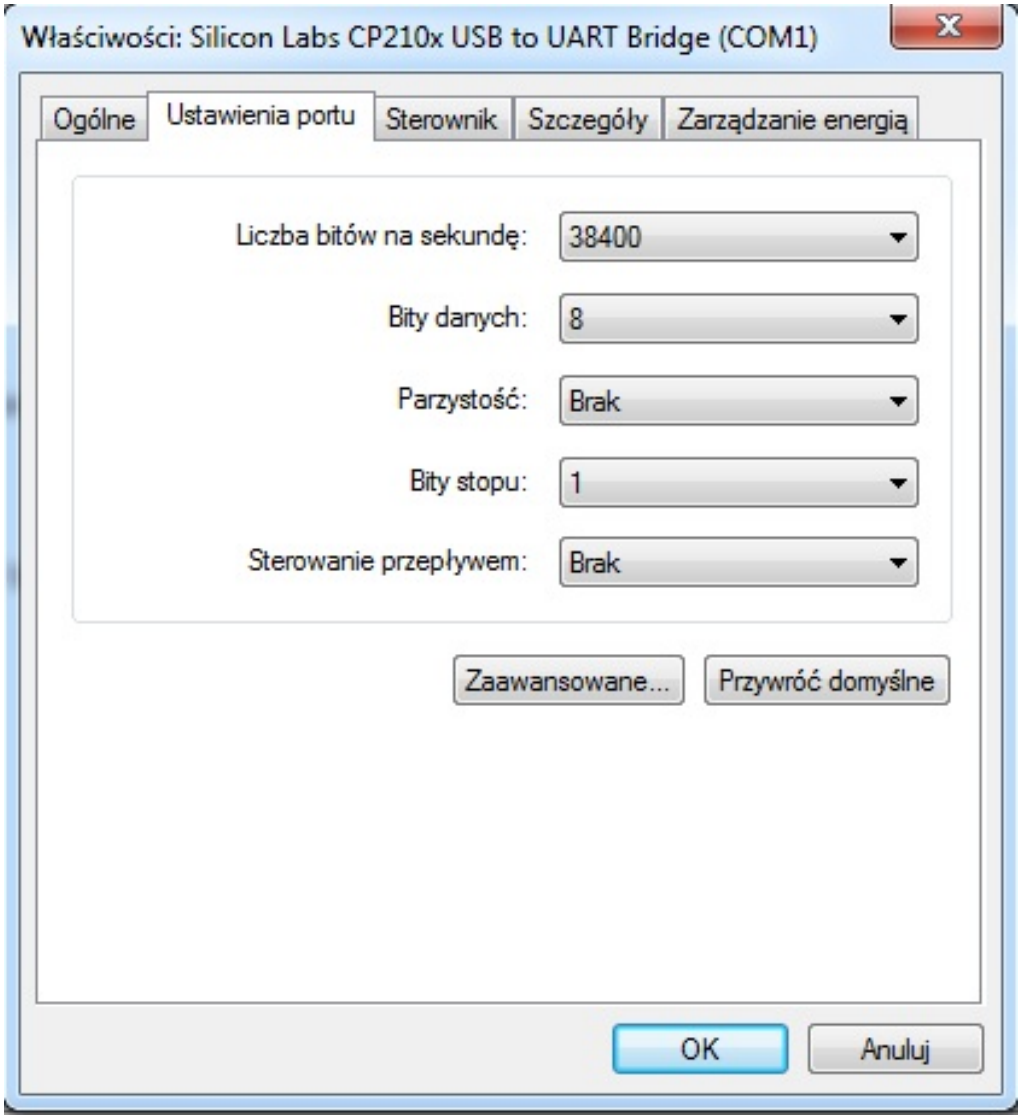
a) W pierwszej kolejności należy zainstalować sterownik USB konwertera USB-UART. Ustawić wartość przesyłu danych oraz połączyć się z programem PDUSpy.



Rys.13. Modem GSM GPRS GA6 podłączony z komputerem



Rys.14. Sterownik umożliwiający komunikację z modemem- w tym przypadku port COM**1**



Rys. 15. Modem GSM GPRS GA6- ustawienie prędkości przesyłu danych

1.2 Podłączanie modemu

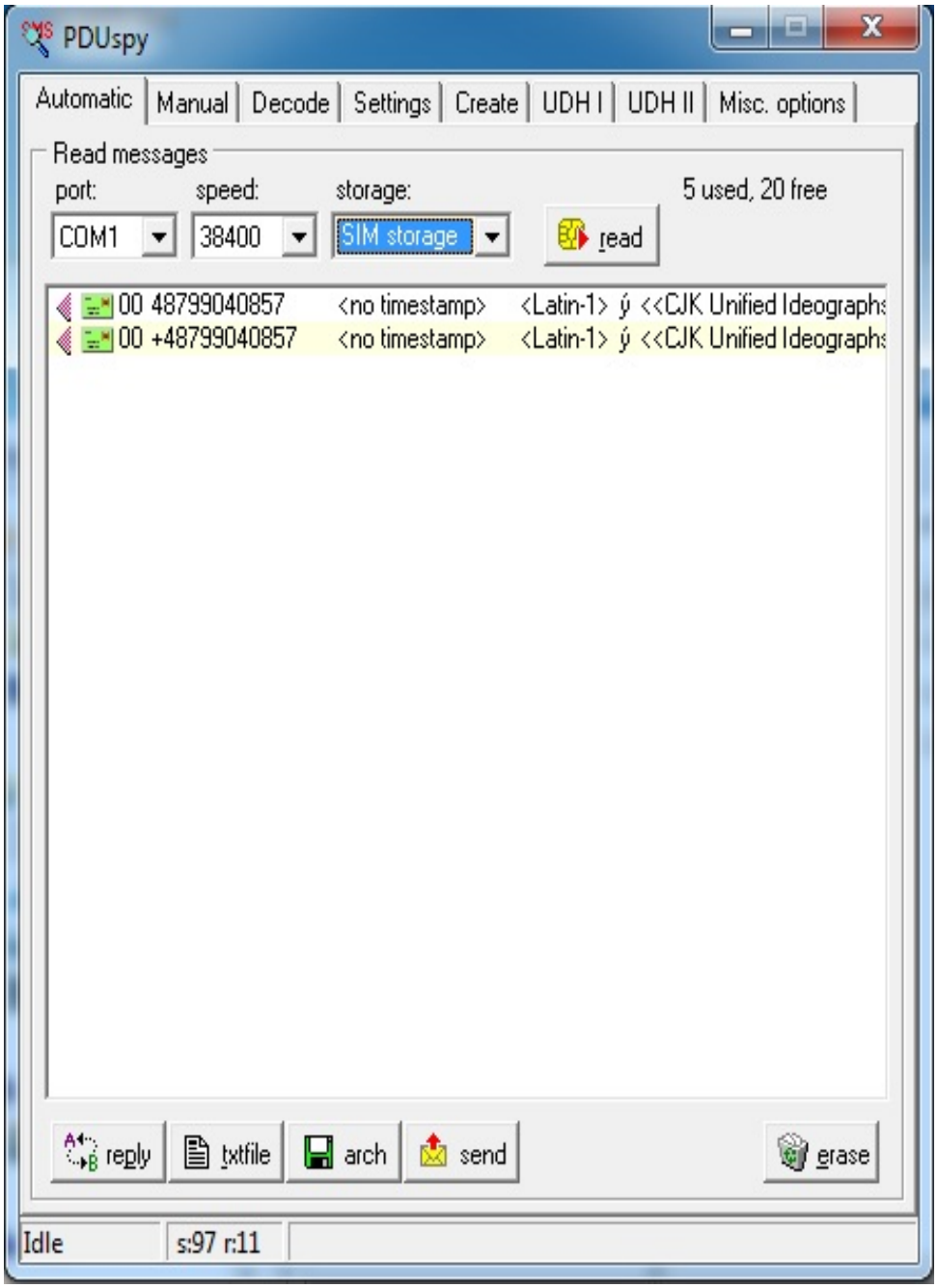
a) następuję podłączenie z modemem za pomocą programu PDUSpy- odczyt karty SIM, która znajduje się w czytniku modemu

b) W dalszej części należy ustawić program według poniższego klucza zawartego w rysunkach poniżej

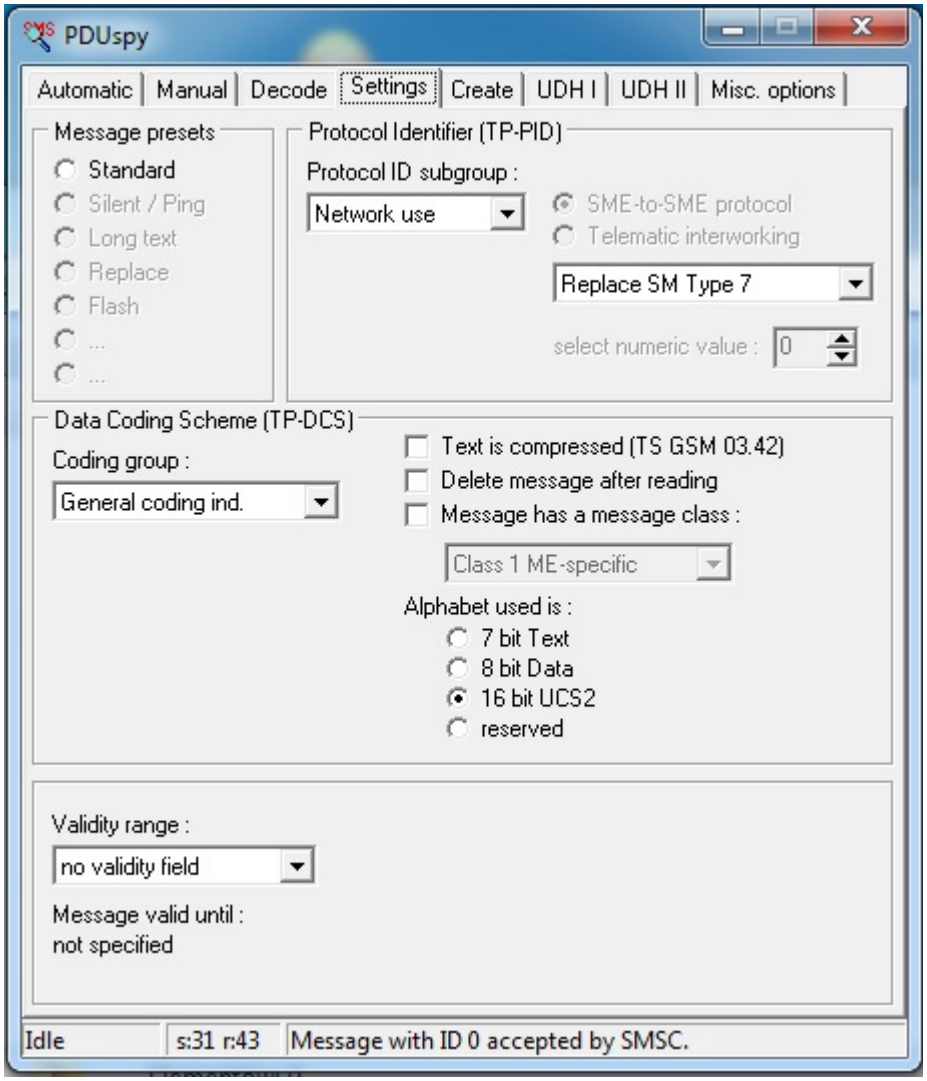
- ustawiamy wiadość SM typu 7,

- wiadomość ma wartość 16-bit UCS2,

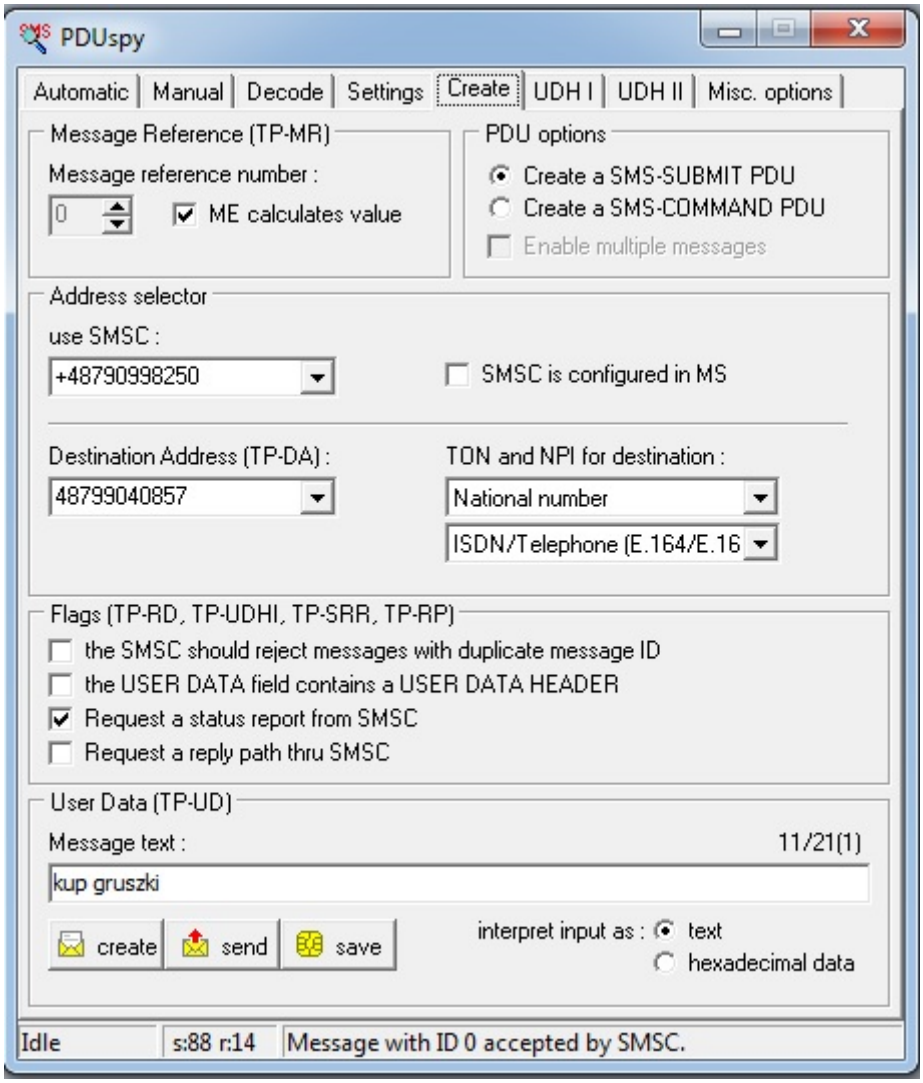
- należy ustawić numer operatora karty SIM- SMSC (Centrum Zarządzania SMS), pośredniczypomiędzy abonentami przy przesyłaniu wiadomości SMS.



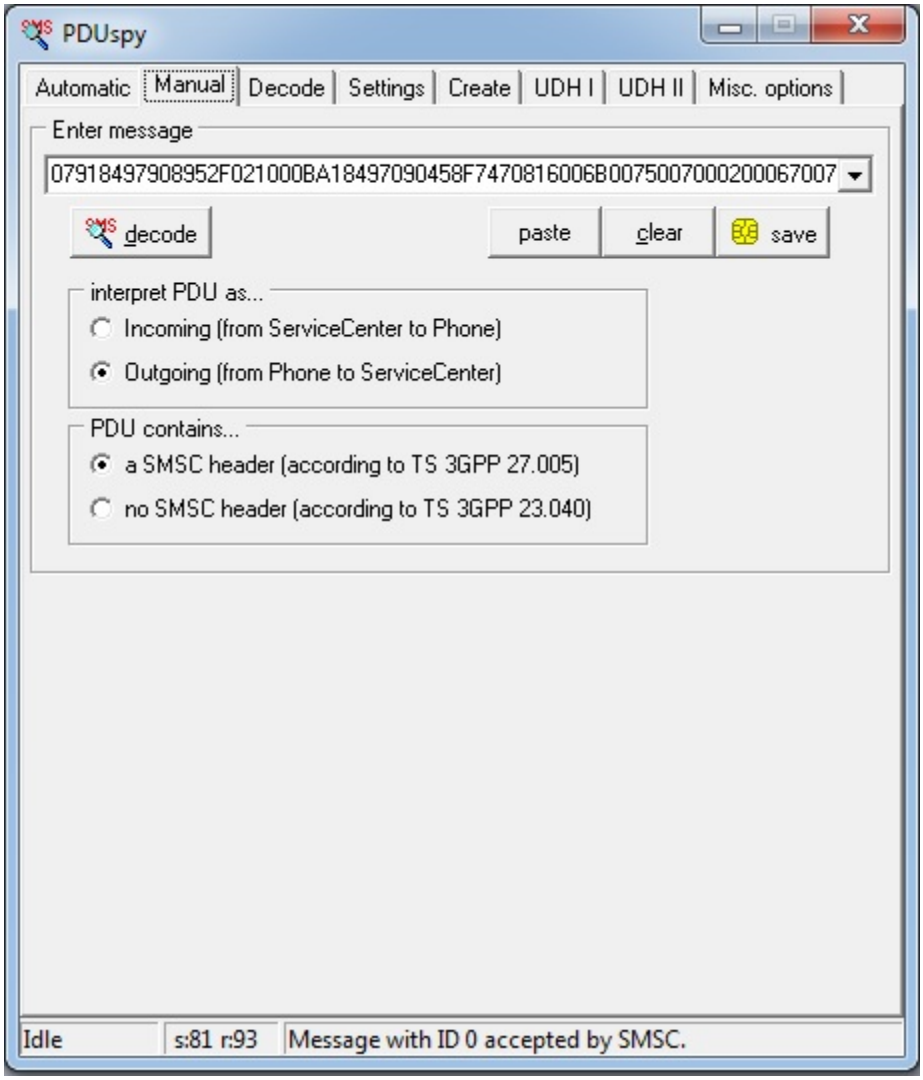
Rys.16. Ustawienie Modemu GSM GPRS GA6 w programie PDUSpy



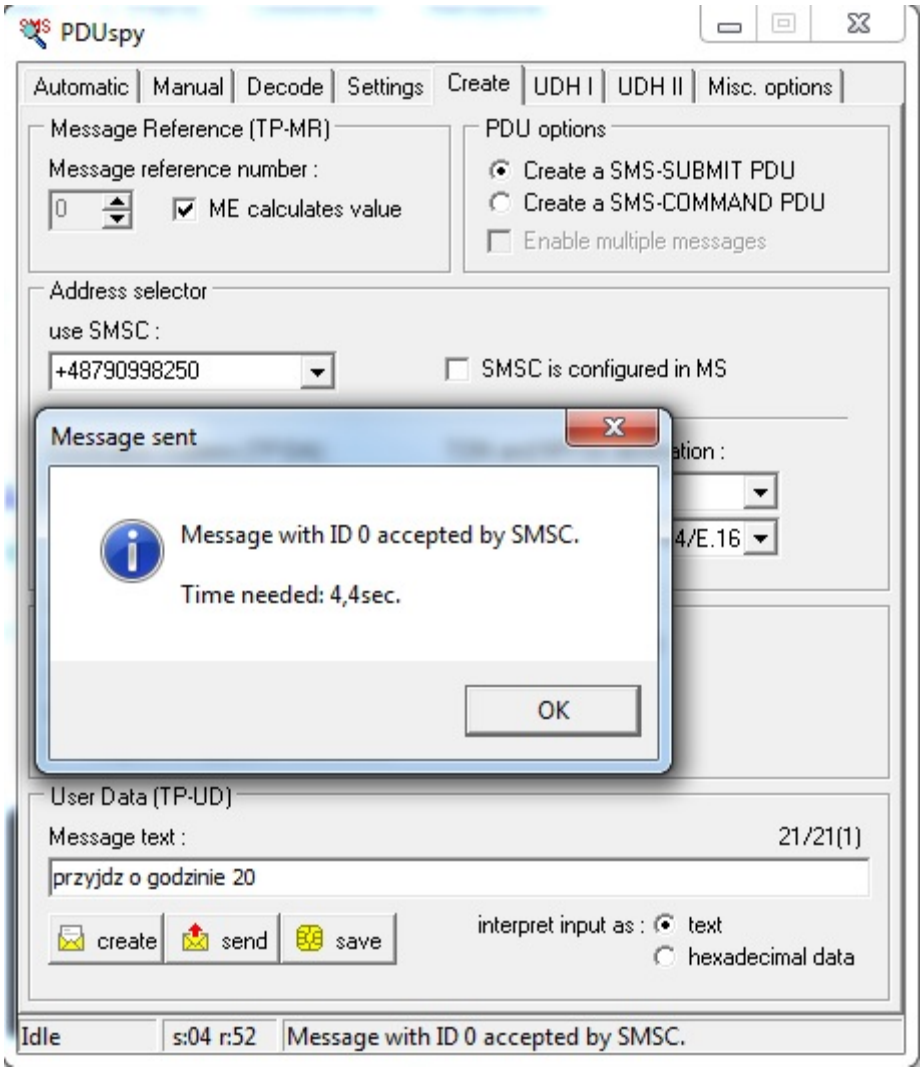
Rys.17. Konfiguracja modemu w programie PDUSpy



Rys.18. Tworzenie wiadomości w programie PDUSpy



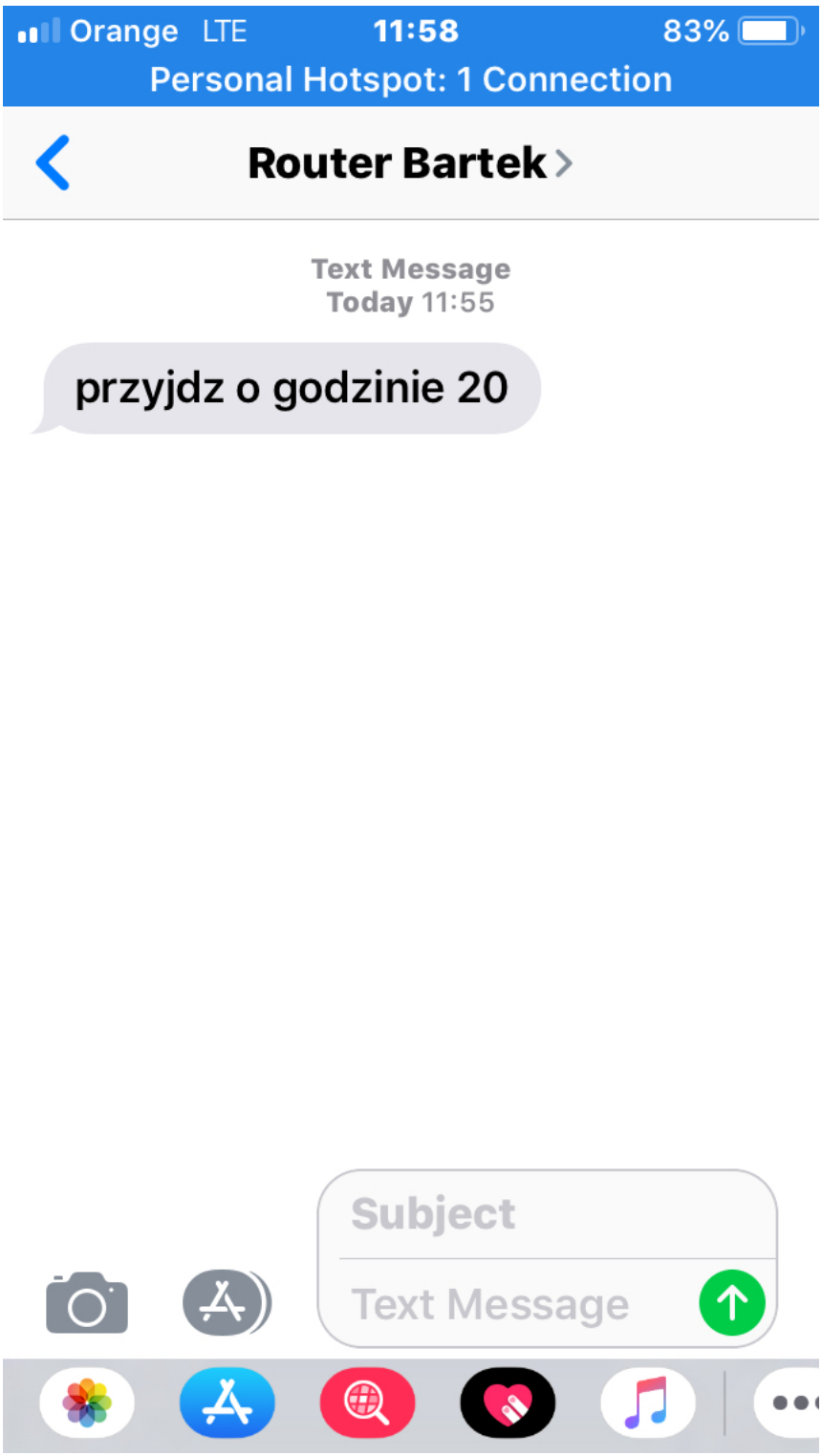
Rys. 19. Konfiguracja wiadomości w programie PDUSpy- otrzymana wartość PDU



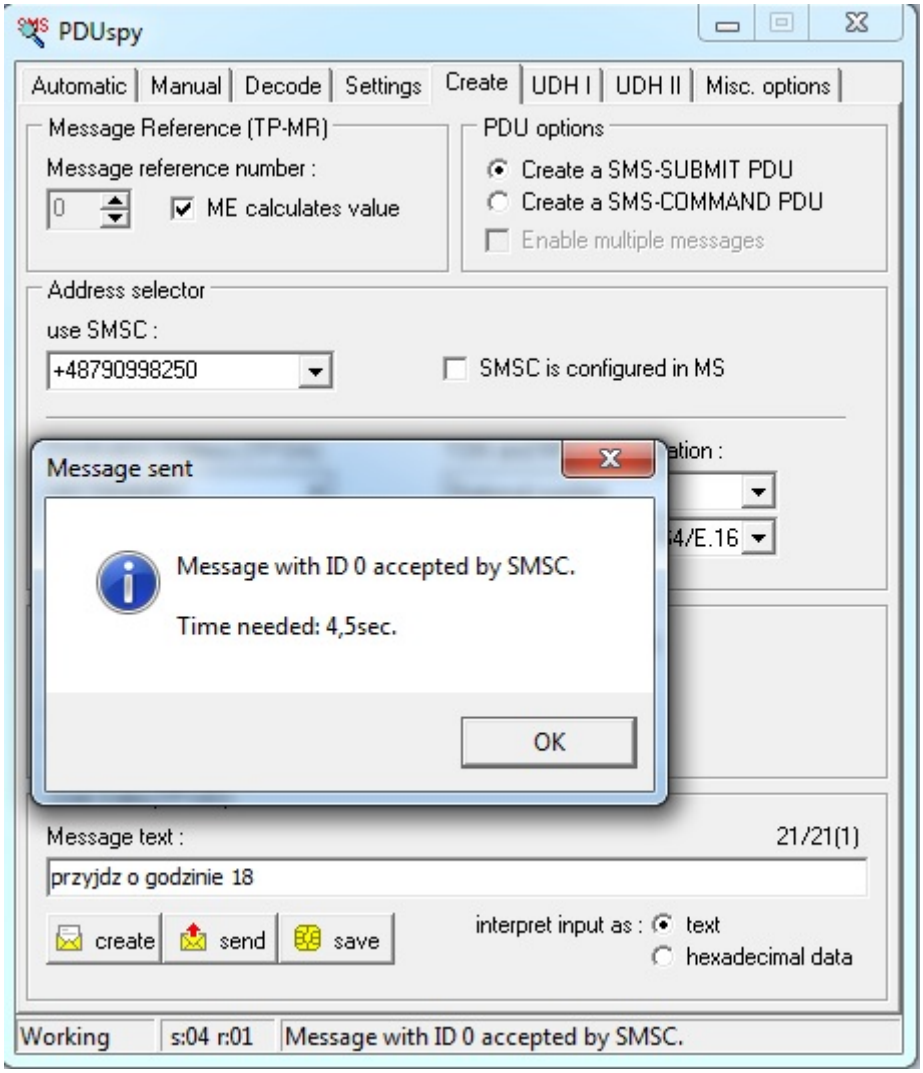
Rys. 20. Wysłanie pierwszej wiadomości w programie PDUSpy o treści-"przyjdz o godzinie 20"

1.3 Przykład podmiany SMSa

a) oryginalny

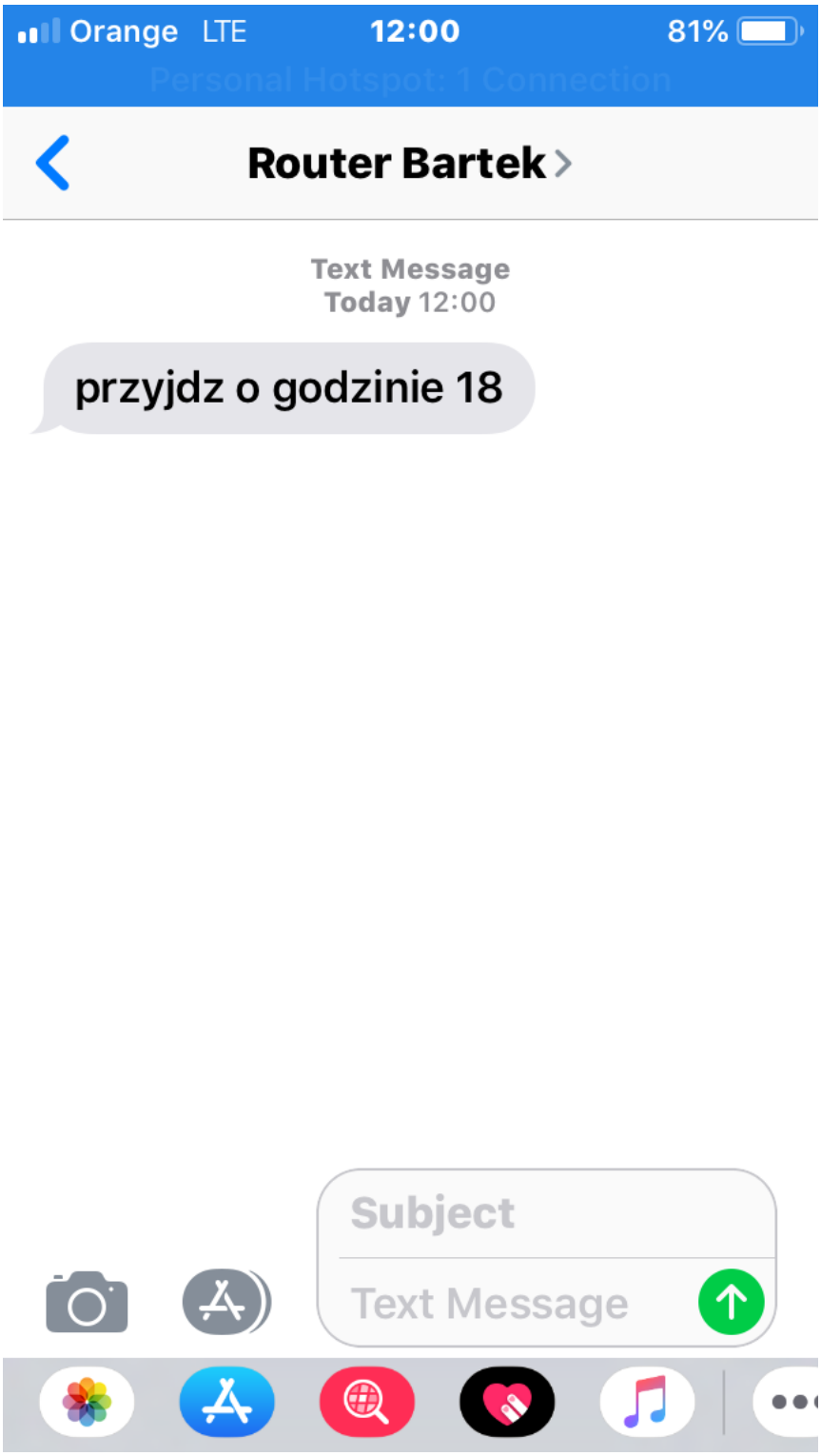


Rys. 21. Otrzymany SMS o treści- "przyjdz o godzinie 20".



Rys.22. Wysłanie pierwszej wiadomości w programie PDUSpy o treści- "przyjdz o godzinie 18"

b) podmieniony



Rys.23. Otrzymany SMS o treści- "przyjdz o godzinie 18"

Można zauważyć, że podmiana nastąpiła z treści- "przyjdz o 20" na "przyjdz o 18" w przeciągu 2 minut. W obecnych czasach istnieje dużo możliwości technologicznych na oszukiwanie ludzi nie tylko w internecie ale i za pomocą SMS-ów, socjotechniki psychologicznej jak np. (metoda na wnuka)- tyczy się to osób starszych. Pokazana metoda jest możliwa dzięki zastosowaniu odpowiedniego sprzętu połączonego z oprogramowaniem. Istnieje również możliwość podszycia się pod dowolny numer telefonu, który wygląda jak numer telefonu od wiarygodnych instytucji. W tym celu oszust ma nieograniczoną możliwość inwencji twórczej uzyskania praktycznie wszystkich danych i nie tylko danych.

4. Bezpieczeństwo znaków zmiennej treści VMS wyświetlających informację na autostradzie

System sterowania znakami zmiennej treści VMS, monitoring czujników pogody, kamery systemu wizyjnego, kamery automatycznego rozpoznawania tablic rejestracyjnych oraz pomiar parametrów pojazdów transportowych jak wiele innych systemów sterowania realizuje (GDDKiA)—przez system Krajowy System Zarządzania Ruchem- ITS. Dzięki temu systemowi możliwe jest integrowanie różnych rozwiązań związanych z ułatwieniami podczas podróży drogami w kraju. Kierowca informowany jest dzięki KSZR o korkach, temperaturze, prędkości oraz pogodzie i wielu innych informacja potrzebnych do komfortowej podróży. Dzięki zastosowaniu Systemu zmiennej treści VMS możliwa jest dynamiczna zmiana treści wyświetlającej informacji w czasie rzeczywistym dzięki rozwiązaniom programowym, które sterowane są za pomocą głównego programu integrujące systemy działające w terenie różnych firm realizujących dany projekt. Integracja możliwa jest dzięki zastosowaniu szyny ESB. Do pomiaru natężenia ruchu stosowane są między innymi dedykowane czujniki pętlowe (zmiana pola magnetycznego wywołana przejazdem pojazdem). Z takich czujników pobierane są między innymi takie dane jak:

- prędkość pojazdu
- klasa pojazdu (zgodnie z klasyfikacją 8+1 - motocykle, auta, busy, autobusy, itd.)
- czas rejestracji
- długość pojazdu
- odległość pomiędzy pojazdem poprzedzającym
- wizualizacja aktualnej sytuacji na drodze za pomocą aplikacji operatorskiej, którą zasilają algorytmy sterujące.

Algorytmy służą do wywołania zatwierdzonej tymczasowej organizacji ruchu, mogą wywoływać treści na znakach np. dotyczące sugerowanych objazdów, warunków meteorologicznych, zdarzeń itd.

Większość systemów działa na jednym serwerze ze względu na rozmiar. Oczywiście możliwe jest rozwiązanie chmurowe z zaawansowanym balansowaniem zasobów/zadań.

Oprogramowanie napisane jest w różnych językach w zależności od potrzeb: C++, C#, PHP, Python, Java, LUA.

Sterowanie znakami zmiennej treści VMS odbywa się za pomocą dedykowanych protokołów komunikacji. W przypadku autostrad płatnych istnieje narzucony standard budowy światłowodów wzdłuż autostrady do wykorzystania w systemach ITS. Znaki VMS wykorzystują połączenie za pomocą przewodów światłowodowych lecz w terenie gdzie nie ma takiej możliwości ze względów technicznych stosowane są rozwiązania bezprzewodowe takie jak:

- połączenie satelitarne,
- połączenie bezprzewodowe GSM/GPRS,
- sieci Radiowe WI-FI,
- radiolinie.

Komunikacja znaków VMS odbywa się za pomocą zamkniętych sieci LAN (często są stosowane sieci VLAN) bez dostępu do internetu. Jest to połączenie przewodowe za pomocą budowy sieci typu Ethernet. Używa się również protokół komunikacyjny SOAP, który stosuje XML do kodowania wywołań i protokół HTTP do ich przenoszenia. Wykorzystuje się również:

- REST API.
- MODBUS.
- Komunikacja z wykorzystaniem gniazdek sieciowych najczęściej z dedykowanym protokołem binarnym.
- Dość często stosowany jest również interfejs RS232/485.

Wykorzystywane są bezpieczne połączenia (szyfrowane) w sieciach Wi-Fi jak i LAN. Dostępne metody zwiększające bezpieczeństwo to:

- Uwierzytelnianie (hasło dostępu do panelu administracyjnego).
- Firewall czyli zapora ogniowa, która odpowiedzialna jest za ruch przychodzący oraz wychodzący z urządzenia.
- Szyfrowanie dysków (np. Bitlocker, Truecrypt, VeraCrypt).
- VPN czyli wirtualna sieć prywatna, jest to tunel szyfrowany pomiędzy użytkownikiem a celem w celu zmniejszenia ryzyka podsłuchu (zwiększa anonimowość w sieci).

- Stosowanie VLAN-ów.
- Uwierzytelnianie Radius.
- Szyfowanie połączenia SSL.
- SSH.
- Szyfrowanie WEP, WPA, WPA2 w sieciach Wi-fi.

Problem pojawia się przy braków możliwości połączenia Znaków VMS w sieć LAN, wtedy następuje podłączenia za pomocą GSM/GPRS. I tutaj pojawiają się problemy z bezpieczeństwem, gdyż za pomocą wysyłania komunikatów GSM (transmisja jednokierunkowa) jest obawa o przechwycenie treści wiadomości SMS z informacją wyświetlaną przez znak VMS. Można przeprowadzić taki wykorzystując platformę radia programowalnego USRP do przechwytywania informacji o użytkownikach GSM.

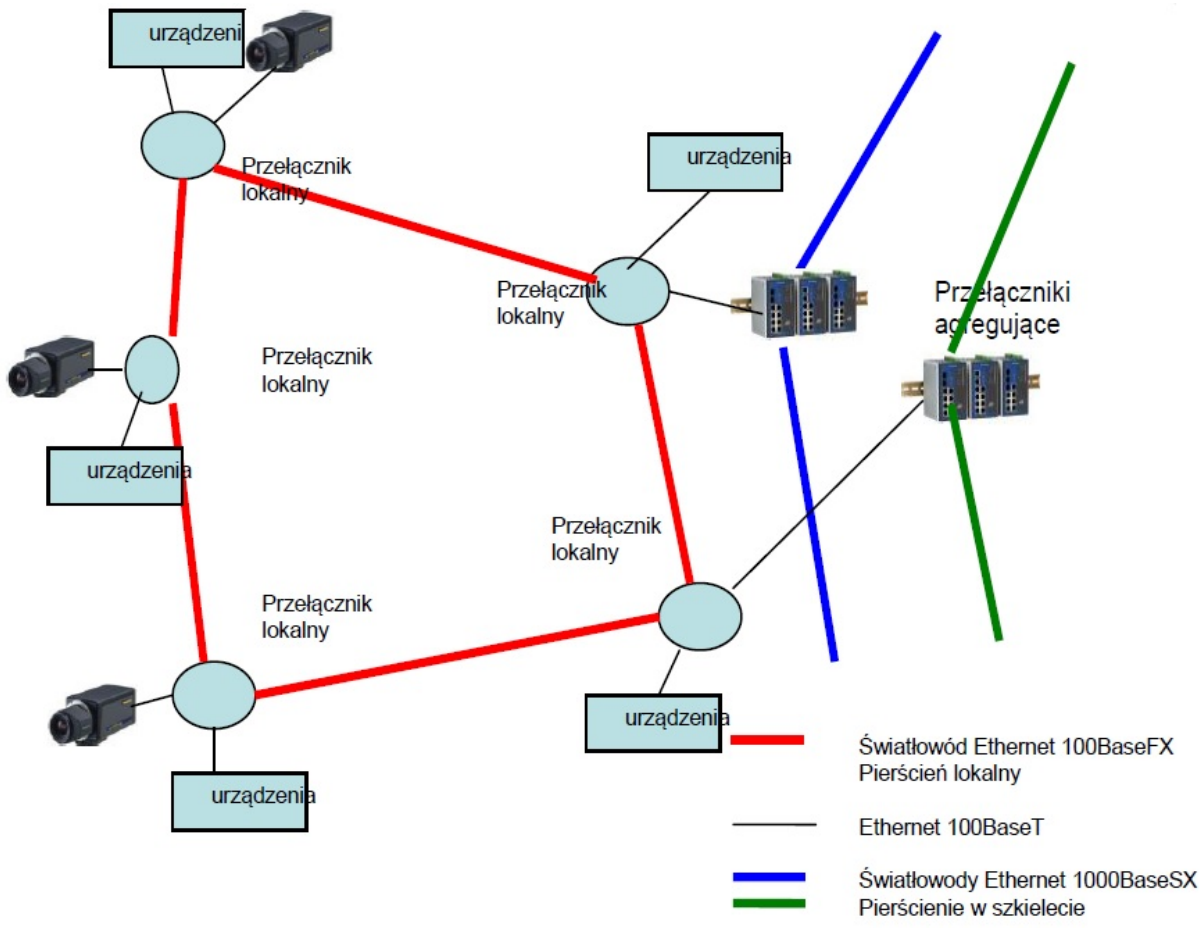
Moduł radia programowalnego USRP N210 (ang. *Universal Software RadioPeripheral*), przedstawiony poniżej, jest uniwersalną platformą oferowaną przez
firmę Ettus Research LLC, która umożliwia implementację systemów radiowych
pracujących w paśmie do 6 GHz.

Rys.24. Moduł radia programowalnego USRP

[24] www.ettus.com z dnia 14.09.2019 r.

[21]

Za pomocą tego urządzenia można przechwycić transmisję w różnych częstotliwościach (urządzenia GSM wykorzystują 1800Mhz). Dzięki oprogramowaniu i podłączeniu do komputera urządzenie jest w stanie imitować BTS-a i przechwycić transmisję pomiędzy klientem a urządzeniem. Przechwytuje między innymi takie informację jak IMSI oraz IMEI użytkownika. Dostępne są również tańsze urządzenia, które umożliwiają podsłuch transmisji GPRS.



Rys.25. Przykład sieci warstwowej

[25] Standard mediów- dokumentacja ze strony GDDKiA z dnia 1.09.2019 r.

Na rysunku przedstawiony został przykład takiej sieci. Typowo mogą to być warstwy sieci umownie nazywane:

- dostępowa,

- agregacyjna,
- szkieletowa.

Zakłada się, że podsystem komunikacyjny będzie budowany jako system co najmniej dwuwarstwowy:

- sieć szkieletowa,
- sieć dostępowa.

Warstwa dostępowa służy do realizacji połączeń pomiędzy obiektami leżącymi w niedalekiej odległości od siebie. Przykładem takiego segmentu sieci może być realizacja połączeń do urządzeń na autostradzie leżących w pobliżu węzła autostradowego takich jak znaki zmiennej treści, urządzenia pomiaru ruchu, kamery itp. W każdym punkcie jest zainstalowany przełącznik Ethernetowy pracujący w płaskim pierścieniu. Z pętli do warstwy wyższej sieci są wyprowadzone co najmniej dwa wyjścia z różnych przełączników lokalnych (zabezpiecza to przed odcięciem połączeń w przypadku awarii pojedynczego przełącznika – zawsze jest droga obejściowa). Warstwa agregacyjna jest zbudowana również w architekturze pierścienia łączącego ze sobą pewną liczbę węzłów na odcinku autostrady. Warstwa szkieletowa łączy ze sobą wiele pierścieni warstw niższych. [22]

Urządzenia lokalne będą mogły łączyć się z urządzeniami centralnymi i z urządzeniami centrum zarządzania poprzez sieć WAN drogą wybraną automatycznie przez odpowiednie protokoły wyboru ścieżki. W przypadku uszkodzenia któregokolwiek urządzenia lub interfejsu w węźle sieci WAN nastąpi przełączenie i wybór nowej ścieżki dla pakietów.

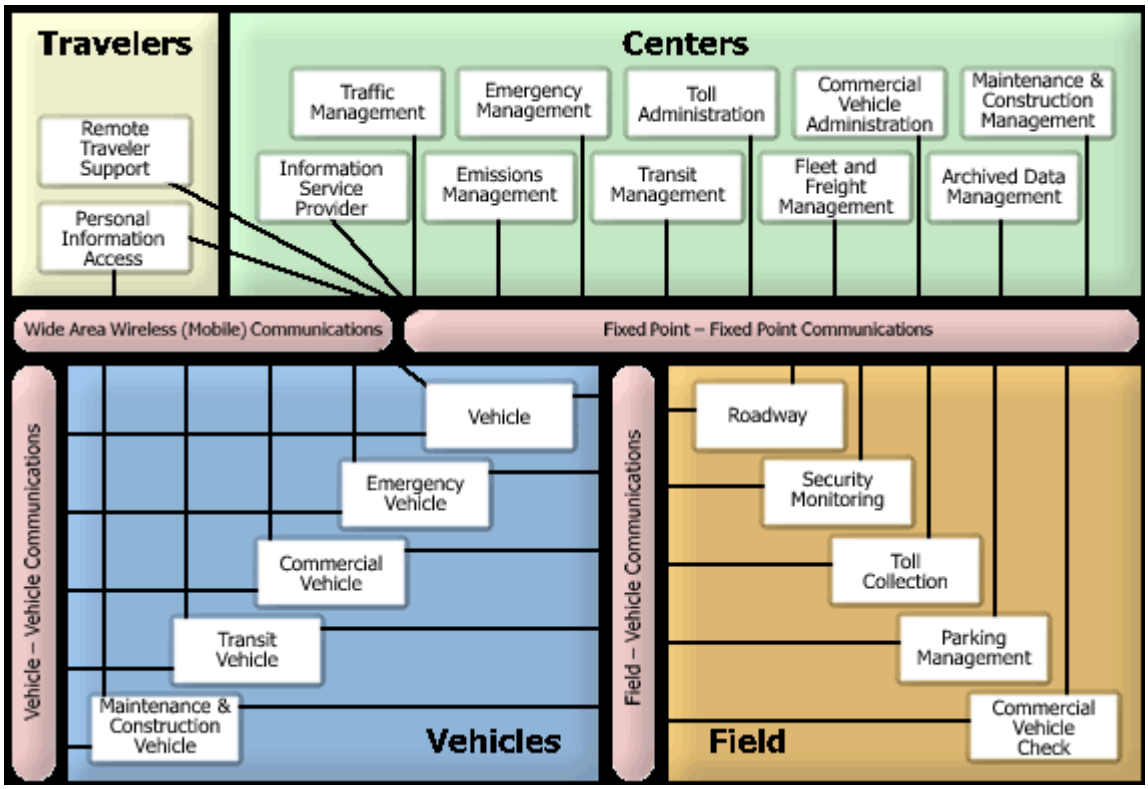
W celu ułatwienia eksploatacji, a także diagnostyki systemów należy wirtualnie separować od siebie ruch generowany poprzez urządzenia wchodzące w skład różnych podsystemów ITS. Należy stosować przełączniki pozwalające na tworzenie VLAN (wirtualnych LAN), separujących ruch pomiędzy nimi, mechanizmy uprzywilejowania pakietów, mechanizmy kontroli przepływu - co umożliwia planowanie ruchu i jego kontrolę. Podział na wirtualne sieci pozwala także, w przypadkach awarii, na ustalenie priorytetu przesyłanych danych przez drogi obejściowe (których przepływność może być mniejsza).

Jako preferowane topologie sieci należy przyjąć:

- liniową,
- pierścień,
- drzewo. [22]

Rys. 26. System Znaków zmiennej treści VMS firmy APM z dnia 01.07.2019 r.

Rys.27. System Znaków zmiennej treści VMS firmy APM 01.07.2019 r.



Rys.28. Architektura ITS wg. RITA (Research and Innovative Technology Administration)

[28] http://www.its.dot.gov/arch/arch_longdesc.htm z dnia 01.09.2019 r.

Diagram przedstawia cztery klasy systemów ITS, wraz z ich podsystemami:

- Travelers – podróżni (żółty): zdalna informacja podróżnych i dostęp do informacji personalnych

- Centers - centra (zielony): dostawca informacji, zarządzanie ruchem, zarządzanie emisją zanieczyszczeń, zarządzanie kryzysowe, zarządzanie tranzytami, pobór opłat, zarządzanie

- flotą i ładunkami, administrowanie pojazdami komercyjnymi, zarządzanie danymi archiwalnymi oraz zarządzanie i utrzymywanie infrastruktury

  - Vehicles – pojazdy (niebieski): pojazdy utrzymania i serwisowe, pojazdy tranzytowe, pojazdy komercyjne, pojazdy ratunkowe oraz pojazdy.

  - Field – infrastruktura terenowa (pomarańczowy): drogi, monitoring bezpieczeństwa, pobór opłat, zarządzanie parkingami, monitorowanie pojazdów komercyjnych.

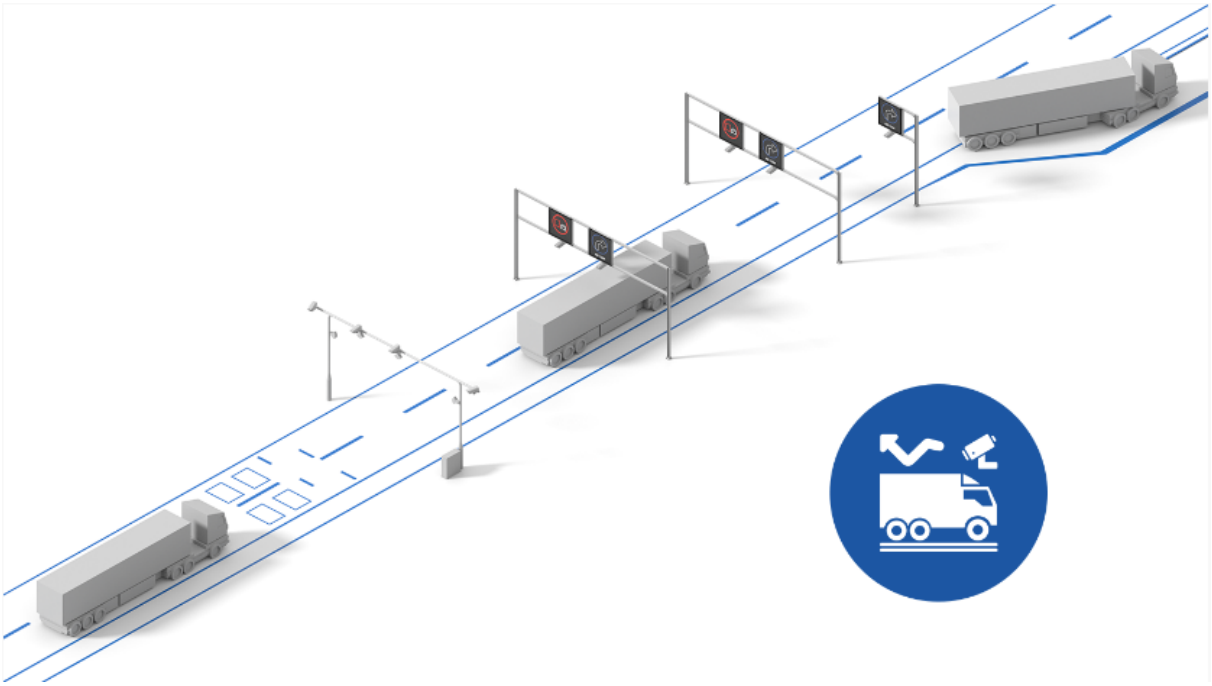
Wszystkie te podsystemy są połączone za pomocą kanałów przepływu informacji. Ponadto na diagramie znajdują się pola reprezentujące typy systemów łączności:

- Wide area wireless (mobile) – łączność mobilna,

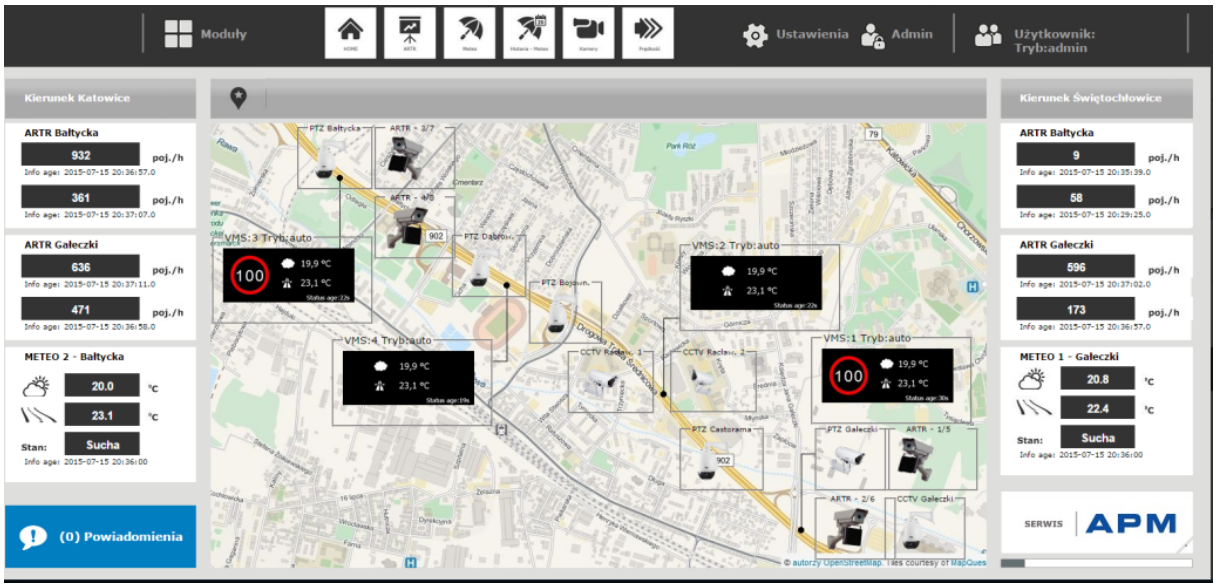
- Fixed-point to fixed-point - połączenia stacjonarne,

- Vehicle to vehicle – połączenia pomiędzy pojazdami (bezprzewodowe),

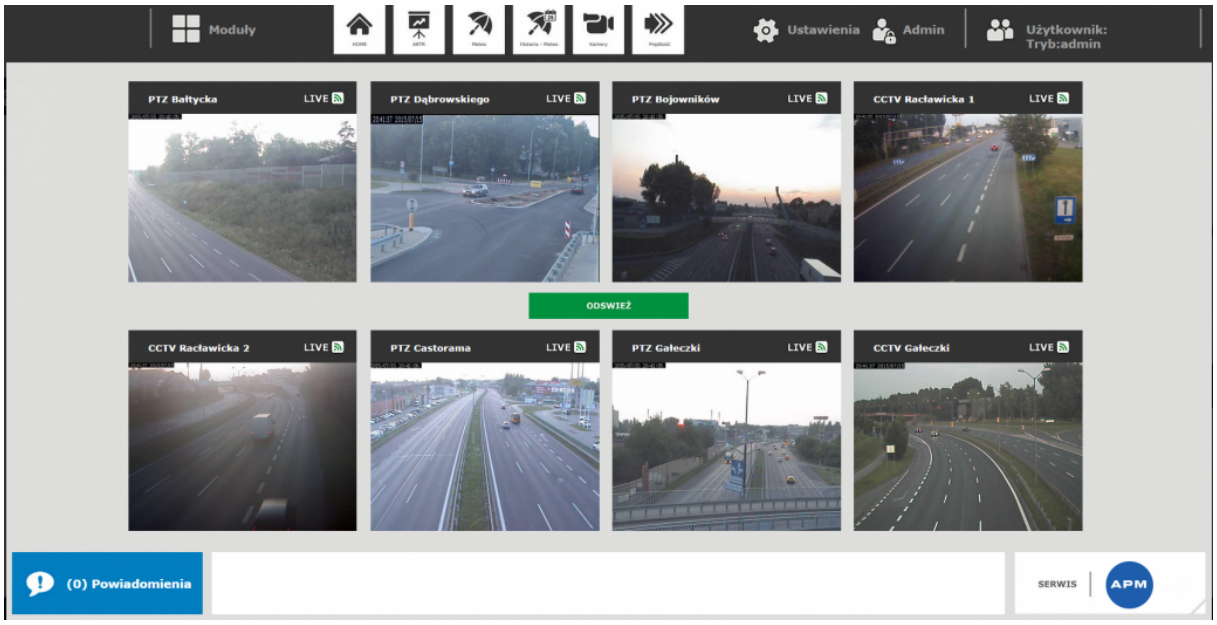
- Field – Vechicle Communication – połączenia pojazd - infrastruktura. [22]



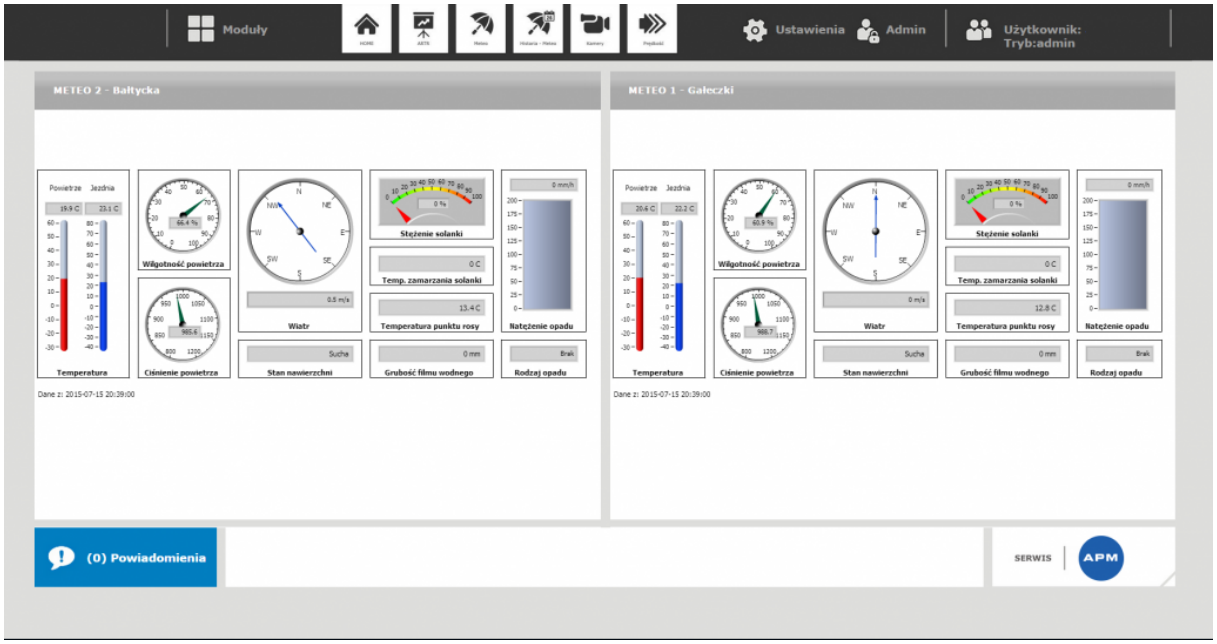
Rys. 29. System WIM PRO 2.0 firmy APM 01.07.2019 r.



Rys.30. System Control PRO firmy APM- parametry drogi 01.07.2019 r.



Rys. 31. System Control PRO firmy APM- podgląd kamer 01.07.2019 r.



Rys. 32. System Control PRO firmy APM- podgląd parametrów temperatury 01.07.2019 r.

5. Podsumowanie

W podsumowaniu zawarte informacje aby były przydatne przy zachowaniu ostrożności w Internecie jak również w życiu codziennym, gdzie kradzież portfela przechodzi do lamusa. Możemy zostać okradzeni w bardziej "kulturalny" sposób. Podczas przeprowadzania badania realizacji oszustwa brania kredytu w Internecie, prócz takich danych jak PESEL, data urodzenia, miejsce zamieszkania, numer dowodu osobistego, nazwisko panieńskie matki, nazwisko rodowe matki ojca, ewentualnie numer karty kredytowej lub bankomatowej należy przesłać numeru telefonu oraz skan dowodu (przednia i tylnia) następuję weryfikacja konta bankowego pożyczkodawcy. W tym celu wpłacany jest jeden złoty. Po weryfikacji następuje zwrot wpłacanej kwoty. Niestety haker mając dane wskazane jak wyżej po wcześniejszej opisanej metodzie phishingu jest w stanie "dorobić" bardzo autentyczny dowód kolekcjonerski. Koszt wyrobienia takiego dowodu to około 800 zł. Na szczęście niedawno 12.07.2019 r. weszła Nowa Ustawa o dokumentach publicznych, która zabrania wytwarzania dowodów kolekcjonerskich. Eksperci ChronPESEL.pl wskazują, w jaki sposób można odróżnić tzw. kolekcjonerski dowód osobisty od prawdziwego dokumentu. Falsyfikat ma zdecydowanie bardziej nasycone kolory i posiada powłokę, która daje mocniejsze wrażenie odblasku. Imitacje hologramu są jednak niskiej jakości. W przeciwieństwie do oryginału nie dają wrażenia trójwymiarowości. Rozmieszczenie poszczególnych nadruków jest jednak niemal identyczne jak w przypadku prawdziwego dowodu osobistego. Jednak już w pierwszym kontakcie powinien wzbudzić podejrzenia u oglądającego. Niestety, różnice te zacierają się w przypadku zeskanowania kolekcjonerskiego dowodu osobistego. Może je dostrzec jedynie uważny obserwator. [23]

Tak więc mając dane, dowód kolekcjonerski, podobny adres mailowy (zbliżony do nazwiska), numer telefonu (przy badaniu uzyskałem informację, że nie jest weryfikowany na kogo jest zarejestrowany) założone konto internetowe na dane w dowodzie kolekcjonerskim można bez ograniczeń korzystać z czyjejś zdolności kredytowej. Również wszelkiego rodzaju pożyczki typu "chwilówki" są użyczane osobom w przedziale wiekowym 18-74 lat bez weryfikacji w BIK- (Biuletyn Informacji Kredytowej). Potrzebny jest dowód osobisty lub paszport oraz w przypadku nowego typu dowodu osobistego również dokument poświadczający adres zamieszkania, może to być np. faktura za prąd. Wiąże się to z tym, iż w nowym dowodzie nie ma adresu zamieszkania. Tak więc przy osobach o nieuczciwych

zamiarach i współpracy oszustów jak i socjotechnice można w łatwy sposób okraść daną osobę. Jedyną obecnie dostępną formą zabezpieczenia jest system SMS-owy BIK-u płatny 23 złote, który generuje informację o próbie zawarcia pożyczki na nasze dane. Wtedy jest czas na reakcję. Niestety uzyskując informację nie wszystkie firmy oferujące pożyczki współpracują z BIK. Nie otrzymałem informacji jak to wygląda procentowo. Natomiast po uzyskaniu kredytu otrzymałem informację z BIK-u w postaci SMS-a o kredycie w jednej z instytucji kredytowej. Według ChronPESEL.pl tylko w 2017 r. dokonano 47 000 wyłudzeń na skradzione dane osobowe o łącznej wartości nawet 3 mld zł. Średnia kwota, którą próbowano wyłudzić to ponad 65 tys. zł.

Lepszym środkiem ochrony byłoby używanie nowych e-dowodów w postaci uwierzytelniania w technologii NFC gdzie prócz weryfikacji danych należy wprowadzić PIN. Dzięki e-dowodowi również możemy podpisać się cyfrowo. Niestety w tym celu potrzebny jest specjalny czytnik, który obecnie bardzo szybko tanieje lecz nawet niewiele instytucji korzysta z tej metody.

Bezpieczeństwo cyfrowe w obecnych czasach to priorytet nie tylko dla Państwa Polskiego. Każde Państwo liczy się z zagrożeniami cyberterroryzmu czy ataków przez obce mocarstwa w celu dezinformacji, uzyskania tajnych danych czy wpływania i manipulacji w danym kraju. Bardzo istotne jest ostatnio "trolowanie" czyli tworzenie grup ludzi, którzy mają na celu dyskredytację danej osoby lub osób czy polityki danego rządu. Miało to miejsce chociażby podczas wyborów prezydenckich w USA. Obecny rząd bardzo wysoko stawia sobie bezpieczeństwo nie tylko militarne ale i informatyczne czego dowodem ma być utworzenie w lutym 2019 r. Wojsk Obrony Cyberprzestrzeni. Obecnie szefem tej jednostki jest generał brygady Karol Molenda i cały czas trwa proces rekrutacji, gdyż można wnioskować, że jest duże zapotrzebowanie na ochronę w sieci.

Istnieje również CERT- organizacja, której zadaniem jest między innymi rejestrowanie oraz obsługa zdarzeń naruszających bezpieczeństwo w sieci, aktywne reagowanie na incydenty powstające w sieci. W tej organizacji możemy zgłosić naruszenie w Internecie. Znajduje się na stronie internetowej CERT Polska bardzo wiele interesujących artykułów praktycznych, które często przewyższają internetowe publikacje.

Obecnie infrastruktura internetowa wspomagana jest za pomocą sztucznej inteligencji. Nawet infolinia Orange korzysta już ze wspomagania klienta za pomocą sztucznej inteligencji. Niestety testowanie wypadło słabo gdyż asystent źle odczytał numer

wprowadzony ustnie. Lecz tylko kwestią czasu jest kiedy sztuczna inteligencja będzie w stanie przewyższyć ilorazem inteligencji Leonardo DaVinci czy Einsteina. O ile już nie przewyższa. Należy tylko mieć nadzieję, że słowa Stevena Hawkinga o sztucznej inteligencji nie będą prawdziwe. Bo twierdził on, że sztuczna inteligencja to największe zagrożenie dla ludzkości. No cóż nawet w nowej powieści Dana Browna- Początek sztuczna inteligencja jest w stanie zrealizować scenariusz przewyższający schemat strategii zwykłego człowieka o kilkanaście ruchów w przód (porównując do gry w szachy).

Natomiast aby względnie bezpiecznie móc korzystać z bankowości oraz przeglądania Internetu zaleca się aby:

- korzystać z aktualnego programu antywirusowego z wbudowanym firewallem oraz VPN-em który gwarantuje anonimowość oraz szyfrowanie i ukrywanie adresu IP,
- regularne aktualizacje oprogramowania systemu operacyjnego jak również innych programów jak np. Acrobat Reader, Microsoft Office,
- w przypadku firm należy stosować IPS,
- ale przede wszystkim należy zachować zdrowy rozsądek, nie klikać w nieznanego pochodzenia załączniki i nie odbierać poczty z załącznikami od nieznanych,
- wskazane jest również stosowanie szyfrowania dysków,
- stosowanie różnych haseł, zastosowanie menadżera haseł w celu archiwizacji wielu haseł,
- uwierzytelnianie dwuskładnikowe.

Spis rysunków:

Wszystkie rysunki firmy APM zawarte w pracy zostały udostępnione do publikacji za zgodą firmy APM PRO sp. z o.o. (https://apm.pl)

Bibliografia:

[1] https://pl.wikipedia.org/wiki/Brain_(wirus_komputerowy) z dnia 7.07.2019 r.

[2] https://www.komputerswiat.pl/aktualnosci/wydarzenia/pierwszy-wirus-komputerowy-stworzono-35-lat-temu/3dm58jt z dnia 7.07.2019 r.

[3] https://www.spidersweb.pl/2011/03/wszystkiego-najlepszego-wirus-komputerowy-ma-40lat.html z dnia 7.07.2019 r.

[4] https://www.newsweek.pl/swiat/stuxnet-wirus-robak-stuxnet/z4zeec3 z dnia 7.07.2019 r.

[5] https://niebezpiecznik.pl/post/stuxnet/ z dnia 7.07.2019 r.

[6] https://www.chip.pl/2011/08/algorytm-szyfrowania-aes-zostal-zlamany z dnia 7.07.2019 r.

[7] www.kali.org z dnia 14.09.2019 r.

[8] https://niebezpiecznik.pl/post/nieautoryzowane-testy-penetracyjne-opinia-prawnika z dnia 7.07.2019 r.

[9] https://www.aircrack-ng.org z dnia 14.09.2019 r.

[10] https://www.metasploit.com z dnia 14.09.2019 r.

[11] https://sekurak.pl/rekonesans-infrastruktury-it-czesc-1-google-hacking/.

[12] https://sekurak.pl/shodan-czyli-google-dla-urzadzen-sieciowych z dnia 14.09.2019 r.

https://sekurak.pl/chinska-konkurencja-niszczy-shodana-uniwersalne-narzedzie-do-rekonesanu z dnia 14.09.2019 r.

[13] https://haker.edu.pl/2014/03/15/czym-jest-footprinting z dnia 14.09.2019 r.

[14] Szkolenie niebezpieczni.pl w Katowicach.

[15] One cell is enough to break Tors anonymity. 2009-02-18. [dostęp 2009-03-18].

[16] Kali Linux Testy penetracyjne Wydanie II Juned Ahmed Ansari.

[17] Certyfikowany IT Specjalista Securit, Akademia Bezpieczeństwa Marcin Szeliga.

[18] Szkolenie sekurak.pl w Katowicach.

[19] https://allegro.pl/oferta/modul-gsm-gprs-a6-sms-antena-arduino-sim900-8002890305 z dnia 12.04.2019 r.

[20] https://allegro.pl/oferta/cp2102-usb-uart-konwerter-rs232-arduino-7477037761 z dnia 12.04.2019 r.

[21] www.ettus.com z dnia 14.09.2019 r.

[22] Generalna Dyrekcja Dróg Krajowych i Autostrad oraz Stowarzyszenie ITS Polska- „Standard realizacji mediów do łączności i transmisji danych KSZR”

[23] https://prnews.pl/odroznic-kolekcjonerski-dowod-osobisty-prawdziwego-dokumentu-442319 z dnia 14.09.2019 r.