

WOJSKOWA AKADEMIA TECHNICZNA

im. Jarosława Dąbrowskiego

WYDZIAŁ CYBERNETYKI



IPSEC

Przedmiot: **MODELOWANIE SYSTEMÓW TELEINFORMATYCZNYCH**

Autorzy:

Łukasz CZERNISZEWSKI

Prowadzący:

dr inż. Andrzej Stasiak

Warszawa 2022

1. Ogólny wstęp do dokumentacji projektowej,

Dokumentacja projektowa będzie wykorzystywana w celu zbudowania demonstratora technologii. Zostanie zaimplementowany protokół IPsec wraz z wymianą kluczy szyfrowania pomiędzy komputerami.

2. Potrzeba używania protokołu,

- Zapewnienie możliwości bezpiecznej wymiany danych
- Umożliwienie monitorowania ruchu przechodzącego przez sieć
- Zapewnienie poufności
- Uniknięcie przypadków sfałszowania transportowanych danych

3. Ogólny opis protokołu.

Architektura IPSec udostępnia różne usługi zabezpieczające transferowane dane w warstwie sieciowej przez niezabezpieczone łącza. Może być wykorzystywana w środowisku wykorzystującym protokół IP w wersji 4 i w wersji 6. Daje systemowi możliwość wyboru odpowiedniego protokołu i algorytmów do zabezpieczenia transmisji przy wykorzystaniu kluczy kryptograficznych. Architektura IPSec może być wykorzystywana do zabezpieczania jednej lub wielu ścieżek pomiędzy hostami, pomiędzy bramami bezpieczeństwa albo pomiędzy hostem, a taką bramą. IPSec jest zbiorem otwartych standardów zapewniających bezpieczną prywatną komunikację w sieciach. IPSec umożliwia realizację następujących operacji:

- weryfikowanie źródła pochodzenia datagramu protokołu IP (eliminacja możliwości zamiany adresu źródłowego pakietu);
- beipołączeniowe weryfikowanie integralności datagramu IP (zabezpieczenie przed modyfikacją zawartości pakietu);
- zabezpieczenie zawartości pakietu przed odczytaniem (stosowanie różnych metod kryptograficznych);
- zapobieganie wielokrotnego wysyłania do odbiorcy poprawnego takiego samego pakietu, który wcześniej został przechwycony (unikanie zablokowania działania usług).

Z tego względu, że IPSec funkcjonuje w warstwie sieciowej, mechanizmy IPSec mogą być wykorzystane do zabezpieczania wszystkich pakietów protokołów wyższych warstw, np. TCP, UDP, ICMP, BGP, itd.

IPSec stanowi połączenie kilku różnych technologii zabezpieczeń, dzięki czemu tworzy pełny system chroniący dane. W szczególności IPSec używa:

- algorytmu wymiany kluczy Diffie'go-Hellmana;

- infrastruktury klucza publicznego do negocjacji klucza sesji;
- algorytmów szyfrowania danych typu DES;
- algorytmów generowania skrótów typu MD5 i SHA;
- cyfrowych certyfikatów.

Na pełen zestaw zabezpieczeń oferowanych w środowisku IPSec składają się dwa komponenty:

- definicja danych dodawanych do standardowego pakietu IP w celu zapewnienia poufności, integralności, autentyczności pakietu (nagłówki AH i ESP) i definicja sposobu kodowania zawartości pakietu;
- mechanizm wymiany kluczy przez łącza publiczne IKE (ang. Internet Key Exchange) niezbędnych do negocjacji parametrów bezpiecznego połączenia pomiędzy dwoma węzłami sieci i wymiany kluczy sesji.

4. Wymagania w stosunku do protokołu,

- Minimalizacja konsekwencji wycieku klucza
- Uwierzytelnianie pochodzenia danych
- Zapewnienie integralności danych w pakiecie
- Poufność transmisji
- Ograniczone zabezpieczenie przed analizą ruchu

5. Założenia w stosunku do protokołu,

- Protokół musi szyfrować transmisje.
- Protokół musi zapewnić integralność danych w pakiecie.
- Protokół uwierzytelnia pochodzenie danych.

6. Ograniczenia protokołu.

- Obciążenie procesora – protokół IPsec wymaga dużej mocy obliczeniowej procesora, do stałego szyfrowania i odszyfrowania danych
- Kompatybilność – brak spójnego standardu własnej kompatybilności
- Szeroki zakres dostępu – przyznanie dostępu jednemu urządzeniu może dać dostęp również innym urządzeniom
- Dostępność – użytkownik, który zainstalował klienta IPsec, nie będzie mógł uzyskać dostępu do Internetu w sieci innej firmy

7. Aktor:

UŻYTKOWNIK

- Użytkownik - aktor, korzystający z aplikacji, może wysyłać i odbierać zaszyfrowane wiadomości od innych użytkowników aplikacji.

ADMINISTRATOR

- Administrator - aktor, nadzorujący działanie aplikacji, może...

8. Przypadki użycia

Użytkownik

- Zarządzaj kontaktami
 - Wpisz do listy kontaktów
 - Wyłącz z listy kontaktów
- Wyślij wiadomość
 - Wybierz adresata
 - Zaszyfruj wiadomość
- Odbierz wiadomość
 - Odszyfruj wiadomość
- Wyświetl okno aplikacji
- Zakończ konwersację

Administrator

- Uruchom terminal
 - Monitoruj połączenie
 - Monitoruj dane aplikacji

| | | |
|--|--|--------------------|
| Identyfikator: | UC1 | |
| Nazwa przypadku użycia: | Zarządzaj kontaktami | |
| Opis przypadku użycia: | Zarządzanie osobami, z którymi mamy możliwość kontaktu | |
| Aktor inicjalizujący: | Użytkownik | |
| Warunki wstępne: | Użytkownik musi mieć połączenie z siecią | |
| Scenariusz główny: | Użytkownik dodaje nową osobę do kontaktów | |
| Scenariusz alternatywny: | Użytkownik usuwa kontakt | |
| Wyjątki: | System informuje użytkownika o braku połączenia z siecią | |
| Po spełnieniu warunków i wykonaniu scenariusza głównego: | Liczba kontaktów powiększa się lub pomniejsza | |
| | Usuń kontakt | Dodaj nowy kontakt |

| | | |
|---|--|--|
| Zawarte i rozszerzone przypadki użycia: | | |
|---|--|--|

| | | |
|--|---|---------------------|
| Identyfikator: | UC2 | |
| Nazwa przypadku użycia: | Wyślij wiadomość | |
| Opis przypadku użycia: | Wysyłanie zaszyfrowanej wiadomości tunelem IPsec | |
| Aktor inicjalizujący: | Użytkownik | |
| Warunki wstępne: | Użytkownik musi mieć połączenie z siecią | |
| Scenariusz główny: | Użytkownik wysyła wiadomość do innego użytkownika tunelem IPsec | |
| Scenariusz alternatywny: | Użytkownikowi nie udaje się wysłać wiadomości do innego użytkownika tunelem IPsec | |
| Wyjątki: | System informuje użytkownika o braku połączenia z siecią | |
| Po spełnieniu warunków i wykonaniu scenariusza głównego: | Wiadomość zaszyfrowana protokołem IPsec zostanie wysłana do drugiego użytkownika | |
| Zawarte i rozszerzone przypadki użycia: | Wybierz adresata | Zaszyfruj wiadomość |
| | | |

| | | |
|--|--|--|
| Identyfikator: | UC3 | |
| Nazwa przypadku użycia: | Wyświetl okno aplikacji | |
| Opis przypadku użycia: | Uruchomienie aplikacji do kontaktowania się między dwoma użytkownikami | |
| Aktor inicjalizujący: | Użytkownik | |
| Warunki wstępne: | Użytkownik musi mieć połączenie z siecią | |
| Scenariusz główny: | Użytkownik uruchamia aplikację i wyświetla się jej okno główne | |
| Scenariusz alternatywny: | System informuje użytkownika o braku połączenia z siecią | |
| Wyjątki: | System informuje użytkownika o braku połączenia z siecią | |
| Po spełnieniu warunków i wykonaniu scenariusza głównego: | Uruchomione zostanie okno aplikacji | |
| Zawarte i rozszerzone przypadki użycia: | | |
| | | |

| | | |
|--|--|--|
| Identyfikator: | UC4 | |
| Nazwa przypadku użycia: | Zakończ konwersację | |
| Opis przypadku użycia: | Użytkownik kończy konwersację z drugim użytkownikiem | |
| Aktor inicjalizujący: | Użytkownik | |
| Warunki wstępne: | Użytkownik musi mieć połączenie z siecią | |
| Scenariusz główny: | Użytkownik kończy konwersację (wymianę kluczy) z innym użytkownikiem | |
| Scenariusz alternatywny: | System informuje użytkownika o braku połączenia z siecią i samoczynnie rozłącza go z konwersacji | |
| Wyjątki: | System informuje użytkownika o braku połączenia z siecią i samoczynnie rozłącza go z konwersacji | |
| Po spełnieniu warunków i wykonaniu scenariusza głównego: | Użytkownik kończy konwersację (wymianę kluczy) z innym użytkownikiem | |
| Zawarte i rozszerzone przypadki użycia: | | |
| | | |

| | | |
|--|---|--|
| Identyfikator: | UC5 | |
| Nazwa przypadku użycia: | Odbierz wiadomość | |
| Opis przypadku użycia: | Użytkownik odbiera zaszyfrowaną wiadomość od drugiego użytkownika | |
| Aktor inicjalizujący: | Użytkownik | |
| Warunki wstępne: | Użytkownik musi mieć połączenie z siecią | |
| Scenariusz główny: | Użytkownik odbiera tunelem IPsec zaszyfrowaną wiadomość od drugiego użytkownika | |
| Scenariusz alternatywny: | Użytkownik nie odebrał tunelem IPsec zaszyfrowanej wiadomości od drugiego użytkownika | |
| Wyjątki: | System informuje użytkownika o braku połączenia z siecią | |
| Po spełnieniu warunków i wykonaniu scenariusza głównego: | Użytkownik odbiera tunelem IPsec zaszyfrowaną wiadomość od drugiego użytkownika | |
| Zawarte i rozszerzone przypadki użycia: | Odszyfruj wiadomość | |
| | | |

| | | |
|--|--|--|
| Identyfikator: | UC6 | |
| Nazwa przypadku użycia: | Monitoruj połączenie zewn | |
| Opis przypadku użycia: | Administrator uruchamia terminal i monitoruje połączenie | |
| Aktor inicjalizujący: | Administrator | |
| Warunki wstępne: | Administrator musi mieć połączenie z siecią | |
| Scenariusz główny: | Użytkownik uruchamia terminal i kontroluje przesyłane pakiety IPsec | |
| Scenariusz alternatywny: | Administrator nie uruchamia terminala | |
| Wyjątki: | Administrator nie ma dostępu do sieci | |
| Po spełnieniu warunków i wykonaniu scenariusza głównego: | Administrator uruchamia terminal i kontroluje przesyłane pakiety IPsec | |
| Zawarte i rozszerzone przypadki użycia: | Uruchom terminal | |
| | | |

| | | |
|--|---|--|
| Identyfikator: | UC7 | |
| Nazwa przypadku użycia: | Monitoruj dane aplikacji | |
| Opis przypadku użycia: | Administrator uruchamia terminal i monitoruje przesyłane dane aplikacji | |
| Aktor inicjalizujący: | Administrator | |
| Warunki wstępne: | Administrator musi mieć połączenie z siecią | |
| Scenariusz główny: | Użytkownik uruchamia terminal i kontroluje przesyłane dane aplikacji | |
| Scenariusz alternatywny: | Administrator nie uruchamia terminala | |
| Wyjątki: | Administrator nie ma dostępu do sieci | |
| Po spełnieniu warunków i wykonaniu scenariusza głównego: | Użytkownik uruchamia terminal i kontroluje przesyłane pakiety IPsec | |
| Zawarte i rozszerzone przypadki użycia: | Uruchom terminal | |
| | | |

9. Specyfikacja opisów sytuacji

| OPIS SYTUACJI | JAKO | CHCĘ | ABY |
|---------------------------|---------------|---|--|
| Komunikacja użytkowników | Użytkownik | Wysyłać wiadomości | Komunikować się z innymi użytkownikami |
| | Użytkownik | Odbierać wiadomości | Komunikować się z innymi użytkownikami |
| | Użytkownik | Wysyłać wiadomości do osoby z katalogu | Wysyłać wiadomości na konkretny adres |
| | Użytkownik | Blokować użytkownika | Nie otrzymywać niechcianych wiadomości |
| | Użytkownik | Wyrejestrować użytkownika | Edytować listę kontaktów |
| | Użytkownik | Zarejestrować użytkownika | Edytować listę kontaktów |
| Zabezpieczenie połączenia | Użytkownik | Szyfrowania wiadomości | Nie było możliwości podsłuchania jej między dwoma urządzeniami |
| | Użytkownik | Posiadać system wymiany kluczy | Szyfrowanie działało automatycznie |
| | Administrator | Posiadać możliwość weryfikacji połączenia | Sprawdzić poprawność połączenia |
| | Użytkownik | Wykorzystywać protokół IPsec | Zabezpieczyć połączenie |
| Dostęp do aplikacji | Użytkownik | Posiadać system wymiany kluczy | System działał w określonym interwale czasowym |
| | Użytkownik | Uruchamiać system w przeglądarce | Niepotrzebne było instalowanie dodatkowego oprogramowania |
| | Administrator | Mieć możliwość przeglądania logów | Weryfikować poprawność działania aplikacji |
| | Użytkownik | Płynnego działania aplikacji | Nie było opóźnień podczas konwersacji |

| | | |
|--|---|--|
| <div>3131</div> <div>JAKO użytkownik CHCE wyrejestrować użytkownika</div> <div>Krzysztof Krasecki</div> <div>High</div> <div>Normal</div> <div>Blocked</div> | <div>3134</div> <div>JAKO użytkownik CHCE wysłać wiadomości do osoby</div> <div>Łukasz Czerniszewski</div> <div>Medium</div> <div>Normal</div> <div>Blocked</div> | <div>3155</div> <div>Jako użytkownik CHCE uruchamiać system w</div> <div>Aleksander Paczeńskiowski</div> <div>Medium</div> <div>Normal</div> <div>Blocked</div> |
| <div>3133</div> <div>JAKO użytkownik CHCE zarejestrować użytkownika</div> <div>Krzysztof Krasecki</div> <div>High</div> <div>Normal</div> <div>Blocked</div> | <div>3136</div> <div>JAKO użytkownik CHCE blokować użytkownika ABY</div> <div>Łukasz Czerniszewski</div> <div>Medium</div> <div>Normal</div> <div>Blocked</div> | <div>3156</div> <div>JAKO administrator CHCE mieć możliwość przeglądania</div> <div>Aleksander Paczeńskiowski</div> <div>Medium</div> <div>Normal</div> <div>Blocked</div> |
| <div>3135</div> <div>JAKO użytkownik CHCE szyfrowania wiadomości ABY</div> <div>Krzysztof Krasecki</div> <div>High</div> <div>Normal</div> <div>Blocked</div> | <div>3147</div> <div>JAKO użytkownik CHCE wyrejestrować użytkownika</div> <div>Łukasz Czerniszewski</div> <div>Medium</div> <div>Normal</div> <div>Blocked</div> | <div>3149</div> <div>JAKO użytkownik CHCE zarejestrować użytkownika</div> <div>Łukasz Czerniszewski</div> <div>Low</div> <div>Normal</div> <div>Blocked</div> |
| <div>3137</div> <div>JAKO użytkownik CHCE posiadać system wymiany</div> <div>Krzysztof Krasecki</div> <div>High</div> <div>Normal</div> <div>Blocked</div> | <div>3154</div> <div>JAKO użytkownik CHCE posiadać system wymiany</div> <div>Aleksander Paczeńskiowski</div> <div>Medium</div> <div>Normal</div> <div>Blocked</div> | |
| <div>3157</div> <div>JAKO użytkownik CHCE płynnego działania aplikacji</div> <div>Aleksander Paczeńskiowski</div> <div>High</div> <div>Normal</div> <div>Blocked</div> | <div>3155</div> <div>Jako użytkownik CHCE uruchamiać system w</div> <div>Aleksander Paczeńskiowski</div> <div>Medium</div> <div>Normal</div> <div>Blocked</div> | |

10. Specyfikacja komunikatów wymienianych podczas komunikacji w modelowanym protokole komunikacyjnym

1. Wysłanie wiadomości

Użytkownik szyfruje wiadomość oraz tworzy nowy pakiet ESP do wysłania, następnie użytkownik przesyła stworzony pakiet z zaszyfrowaną wiadomości do 2 użytkownika.

Wysłanie wiadomości = Użytkownik + zaszyfrowanie wiadomości + stworzenie pakietu ESP + wysłanie pakietu + użytkownik.

2. Zarządzaj kontaktami

Użytkownik otwiera listę kontaktów, w tym czasie komputer administratora udziela dostępu do jego bazy kontaktów. Następnie użytkownik może dokonać edycji, wprowadzone zmiany zostają przesłane oraz zapisane na komputerze administratora. Na koniec komputer administratora wyświetla informacje o wyniku przeprowadzonej operacji.

Zarządzanie kontaktami = użytkownik + wysłanie zapytania o listę kontaktów + komputer administratora + przesłanie listy kontaktów + użytkownik + wprowadzenie zmian + przesłanie zmian + komputer administratora + zapisanie zmian + użytkownik + wyświetlenie komunikatu o wyniku operacji.

3. Uruchom terminal

Administrator wysyła żądanie o przedstawienie wybranych danych do komputera administratora. Komputer administratora sprawdza, czy są jakieś nowe komunikaty do wyświetlenia oraz wyświetla te, które są dostępne. Komputer administratora wysyła komunikat o zamknięciu monitora danych.

Uruchom terminal = interfejs administratora + wyślij żądanie o przedstawienie danych + komputer administratora + sprawdź dostępność nowych komunikatów + wyświetl dostępne komunikaty + interfejs administratora + komunikat o wyniku operacji.

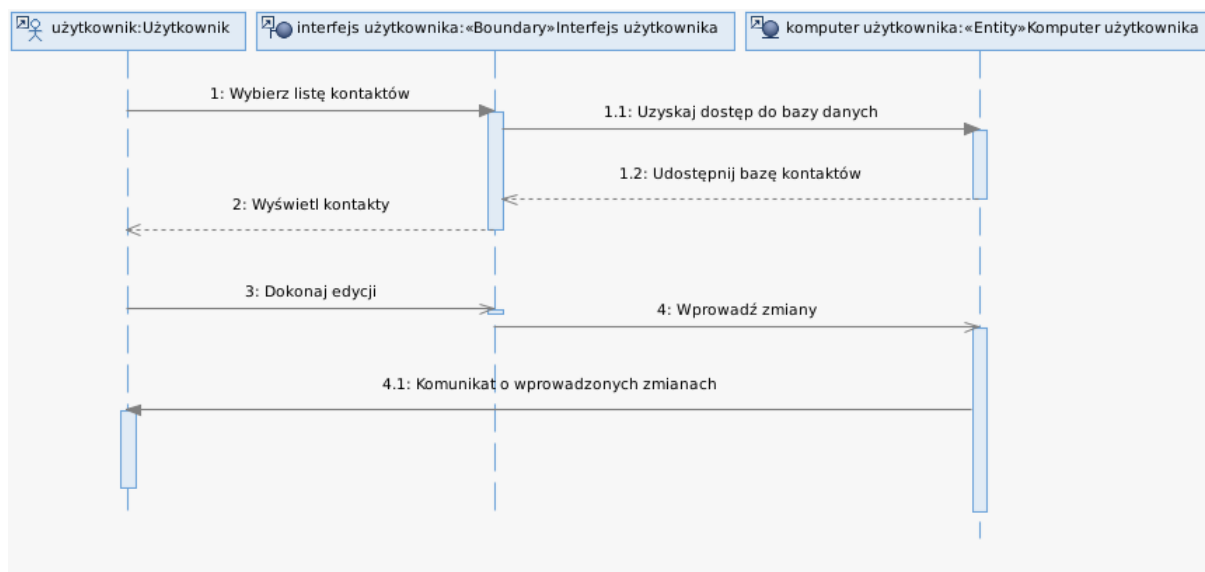
4. Odebranie wiadomości

Użytkownik odszyfrowuje wiadomość a, następnie ją wyświetla.

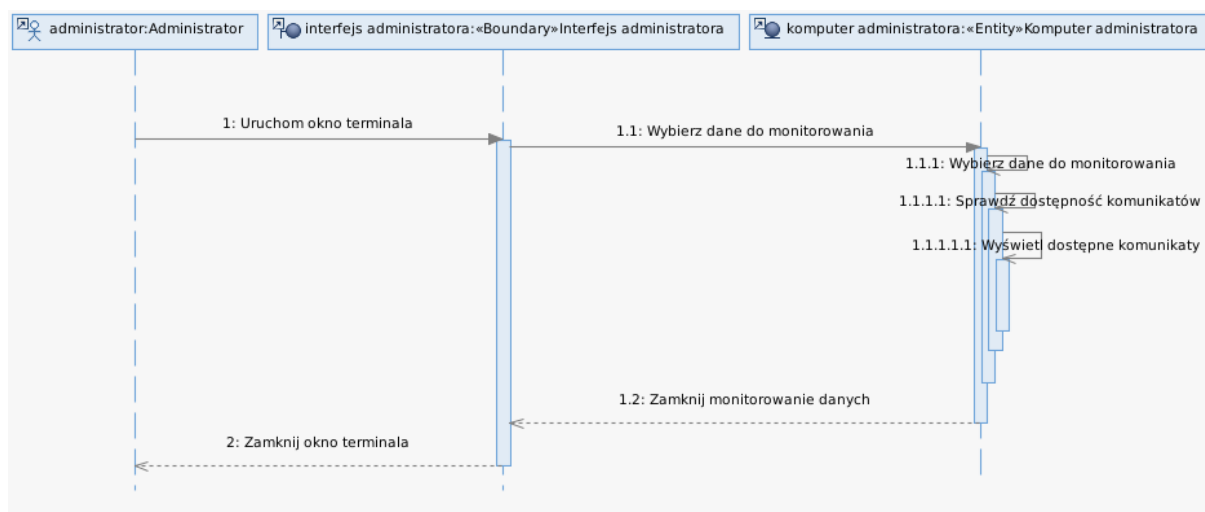
Odebranie wiadomości = Użytkownik + odszyfrowanie wiadomości + wyświetlenie wiadomości

11. Diagramy sekwencji

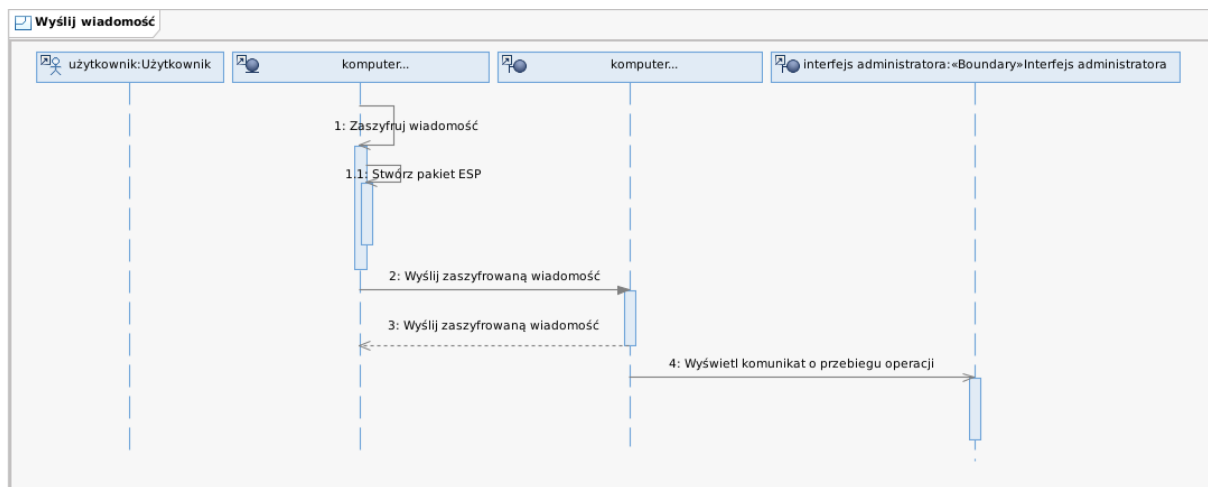
Zarządzaj kontaktami:



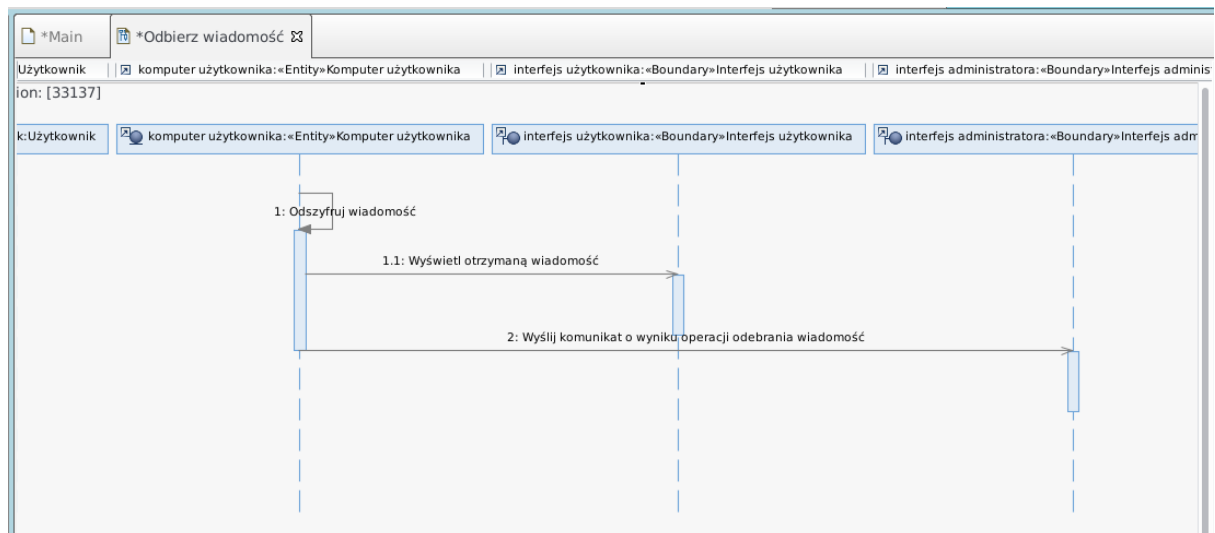
Uruchom terminal:



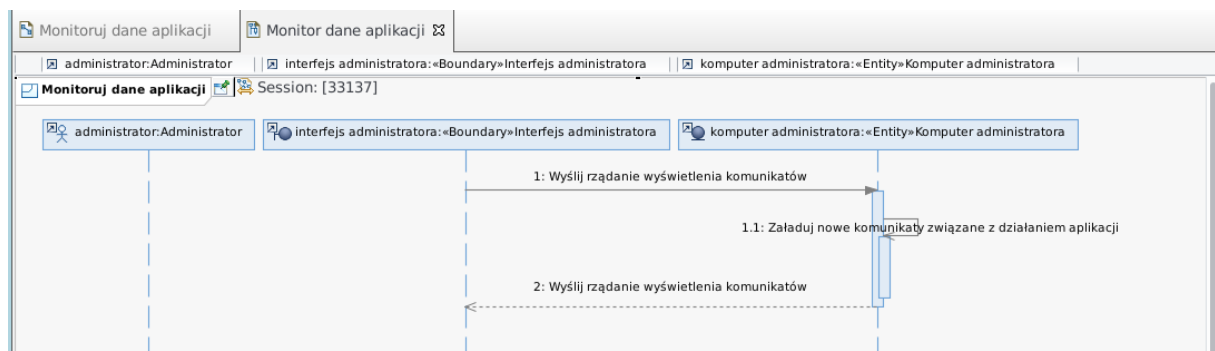
Wyślij wiadomość:



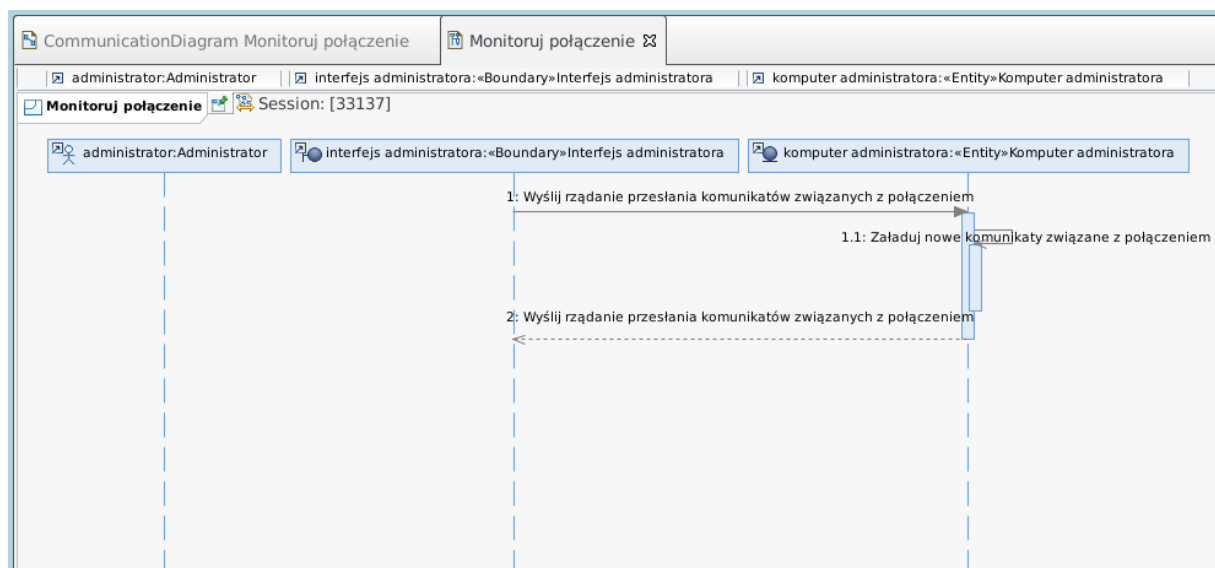
Odbierz wiadomość



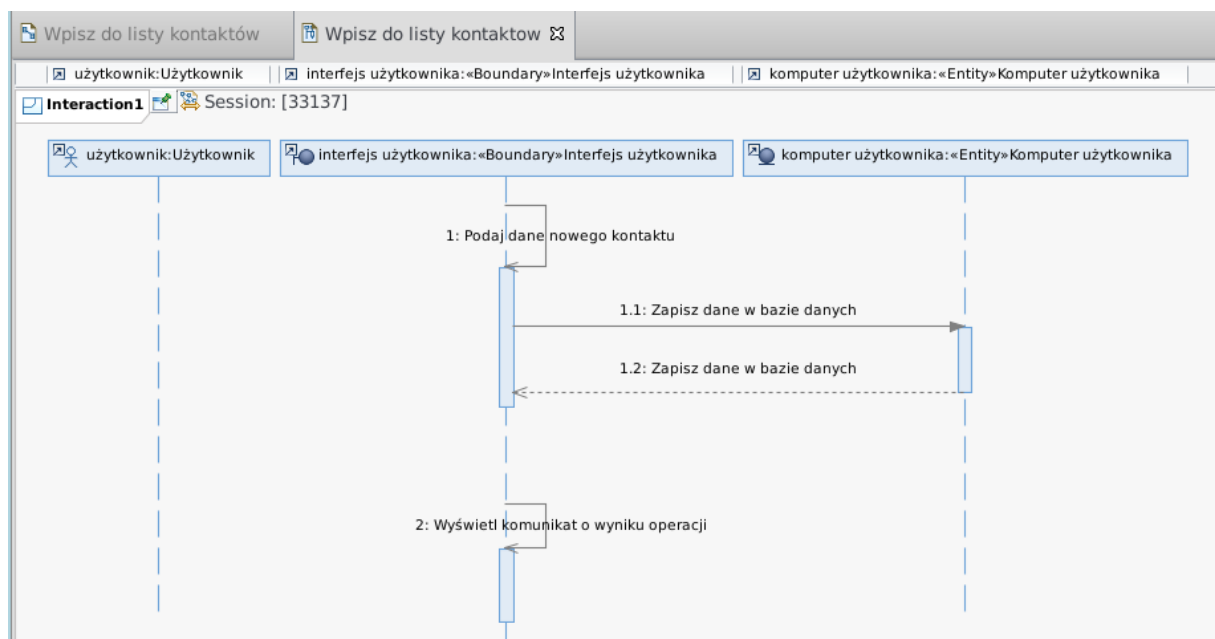
Monitoruj dane aplikacji



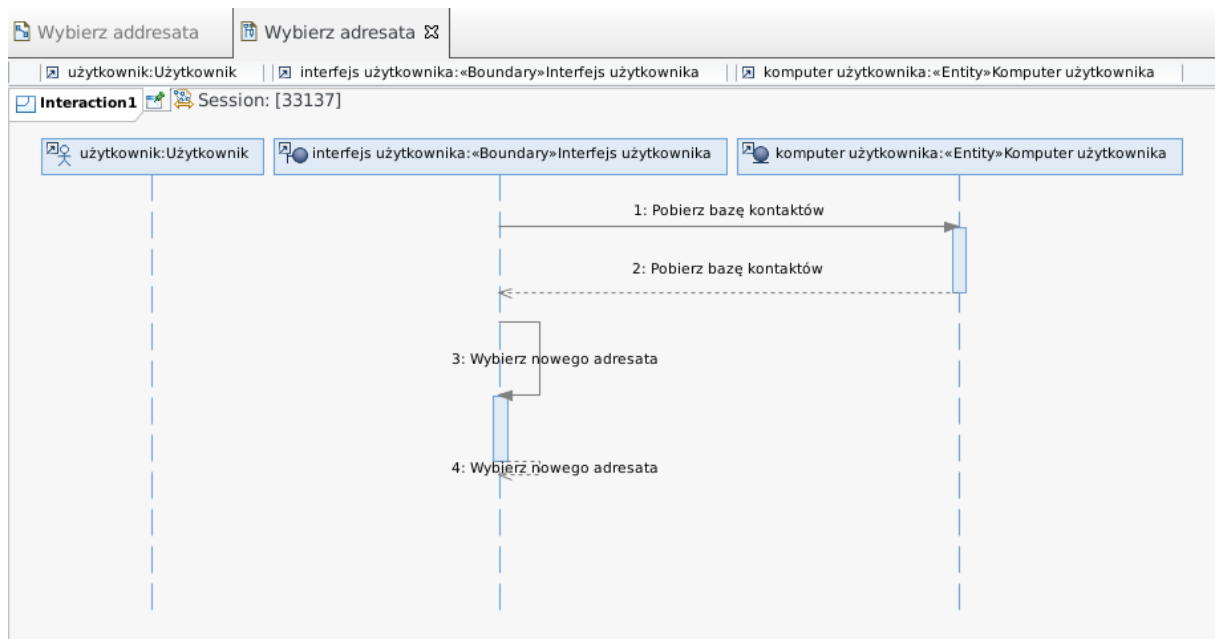
Monitoruj połączenie



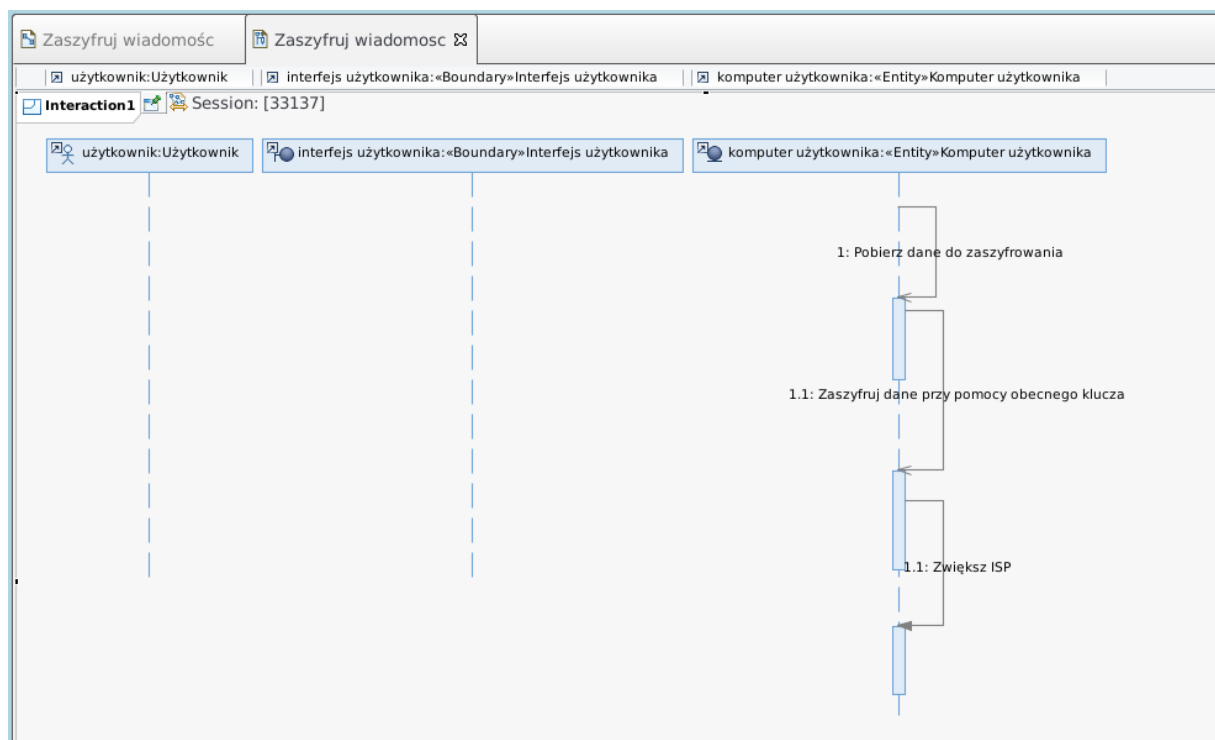
Wpisz do listy kontaktów.



Wybierz adresata

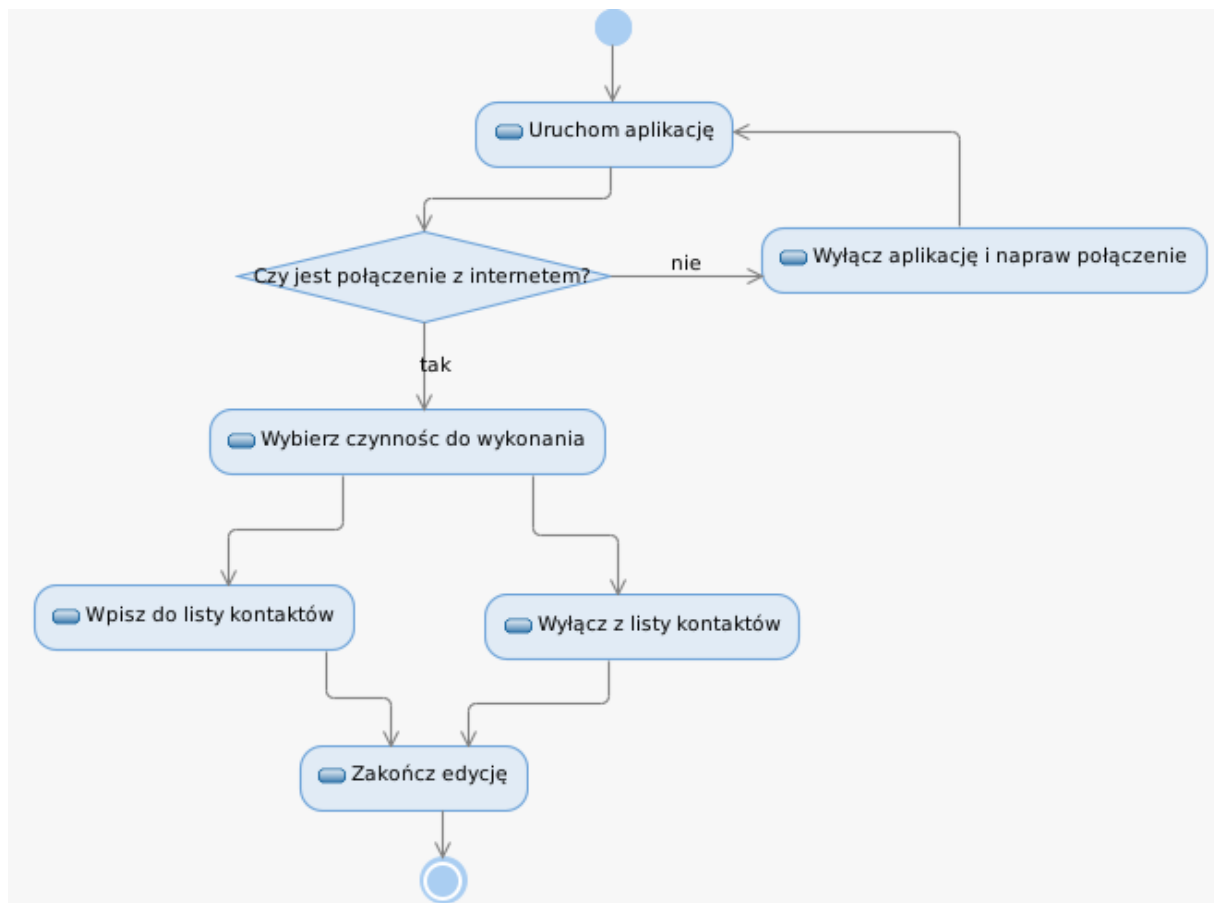


Zaszyfruj wiadomość

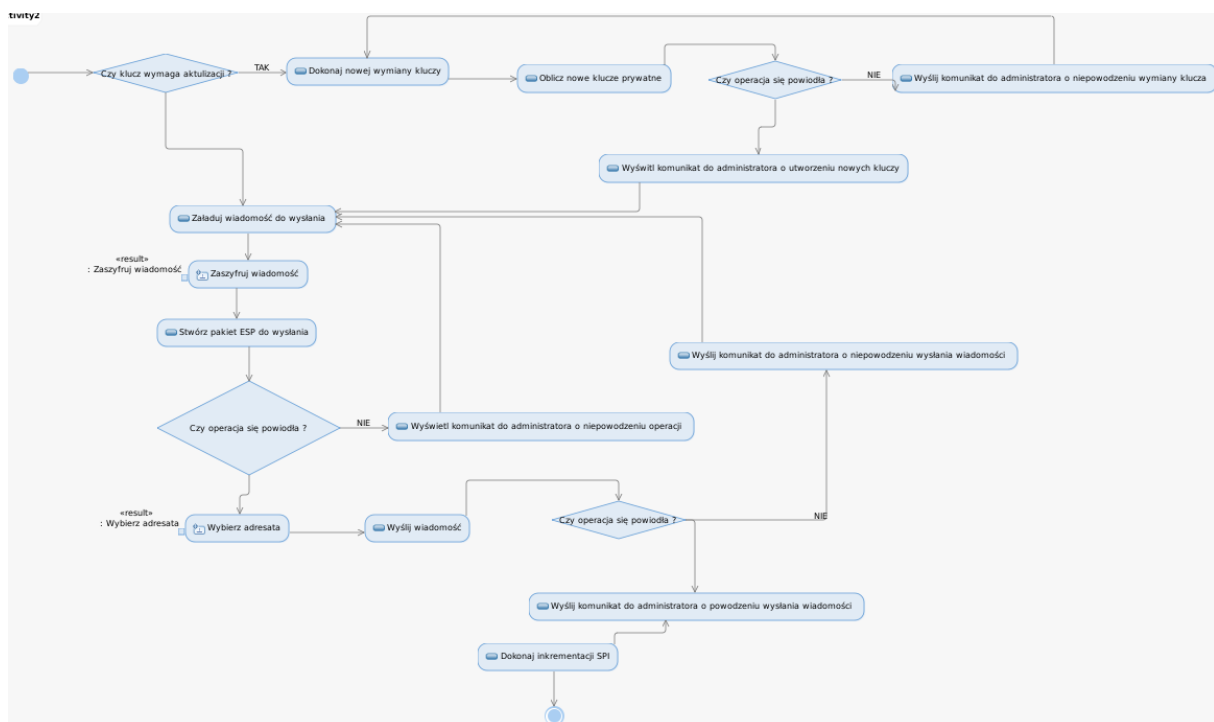


12. Diagramy aktywności:

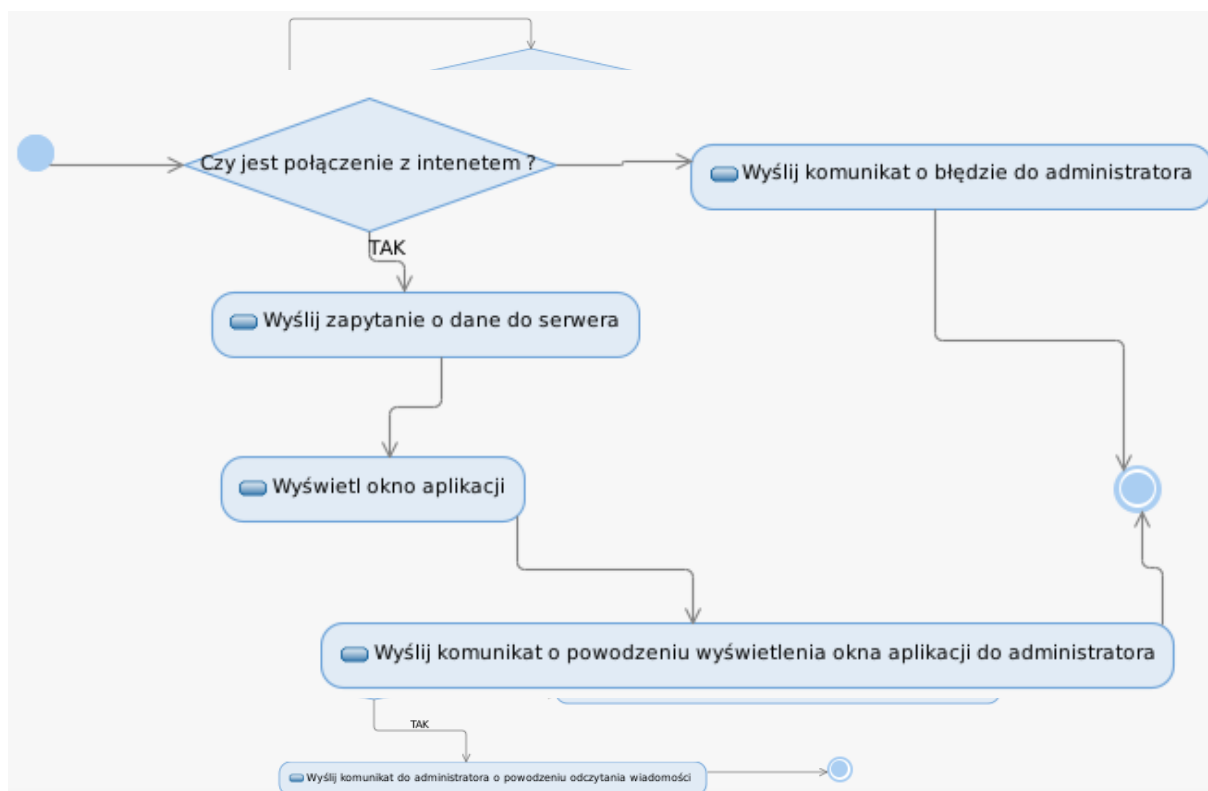
Zarządzaj kontaktami:



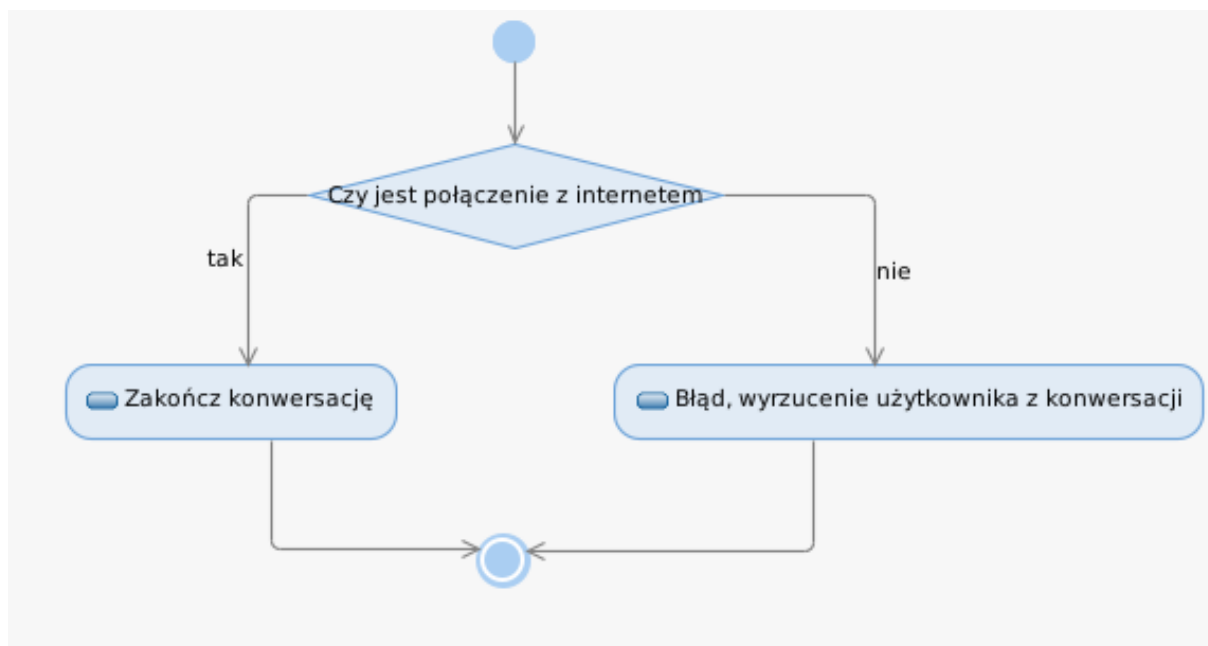
Wyślij wiadomość:



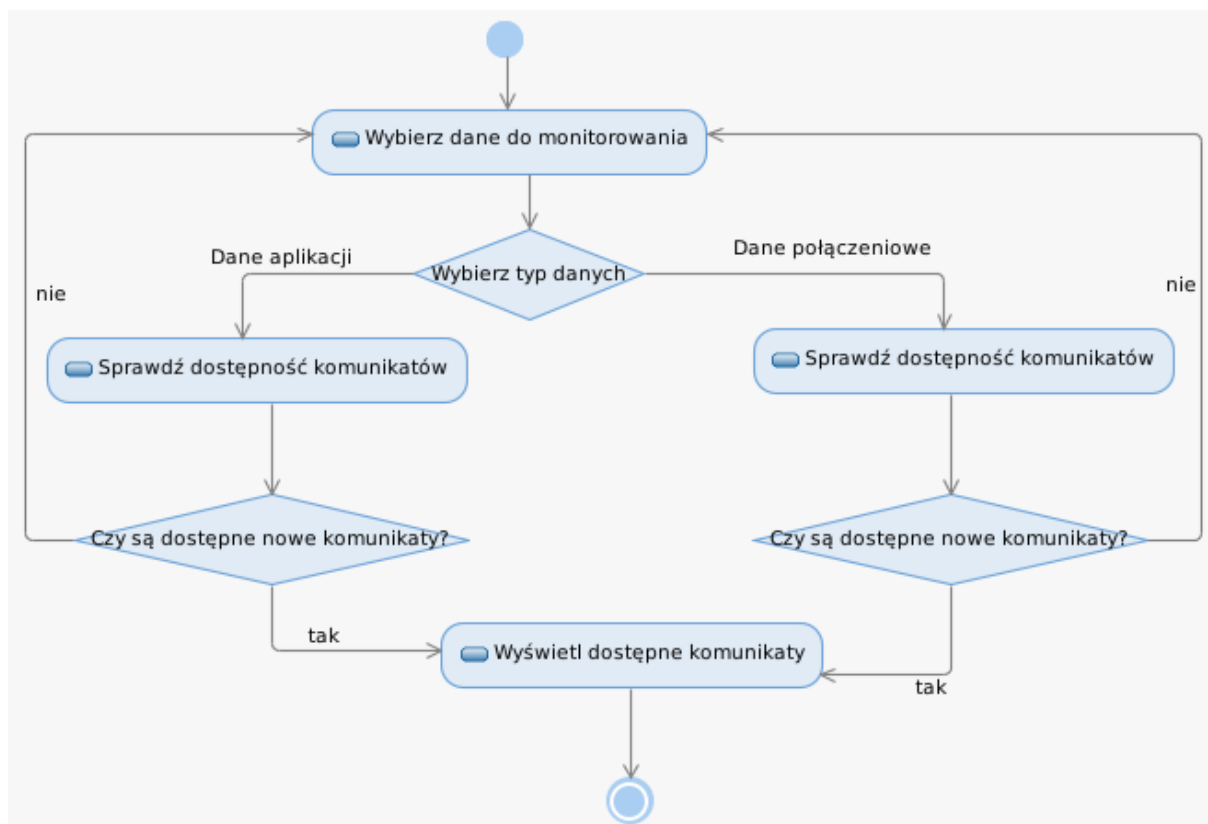
Odbierz wiadomość:



Zakończ konwersację:

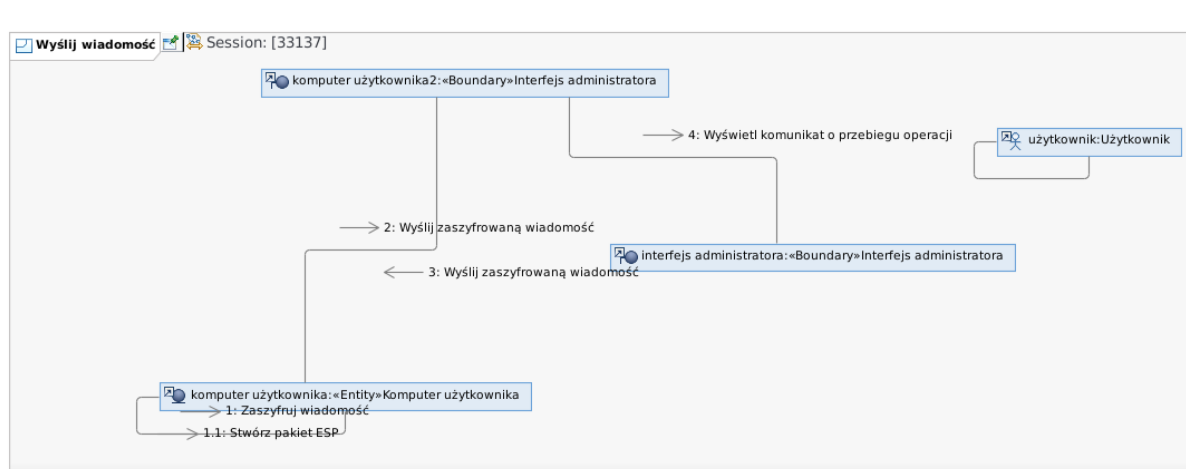


Uruchom terminal:

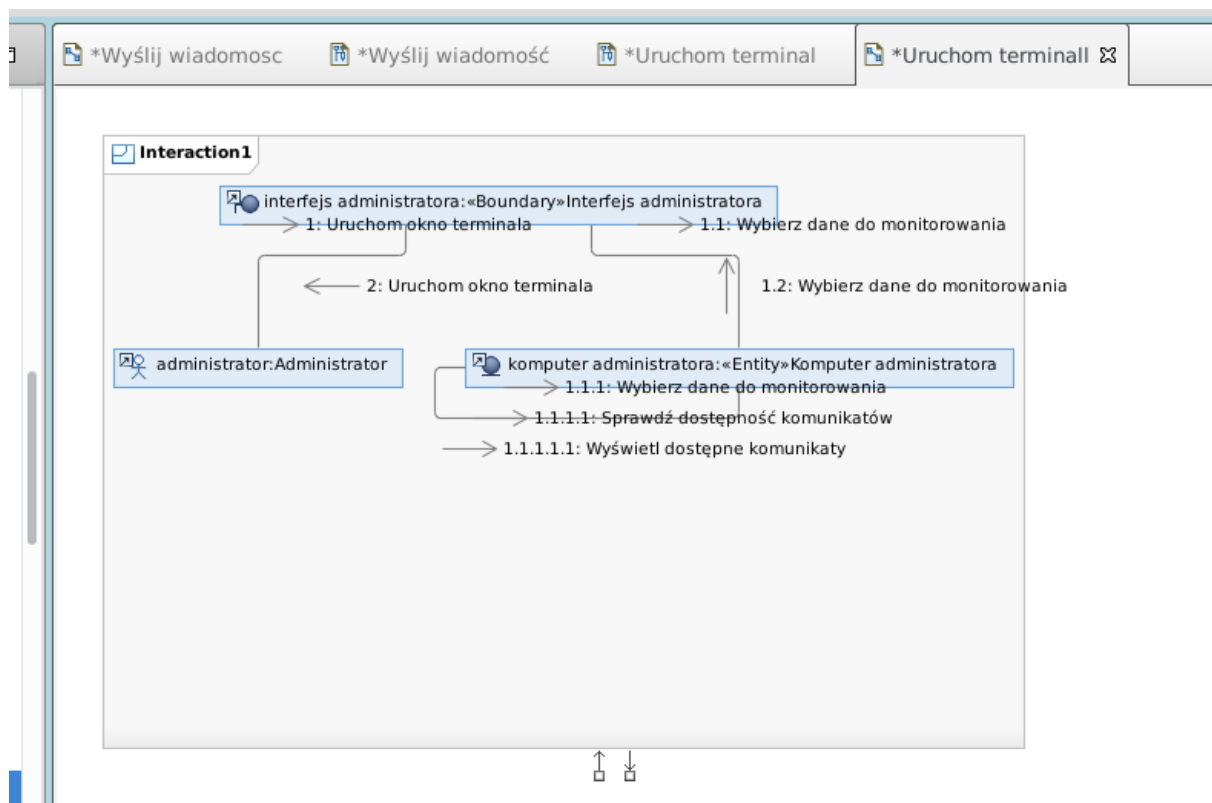


13. Diagramy komunikacji

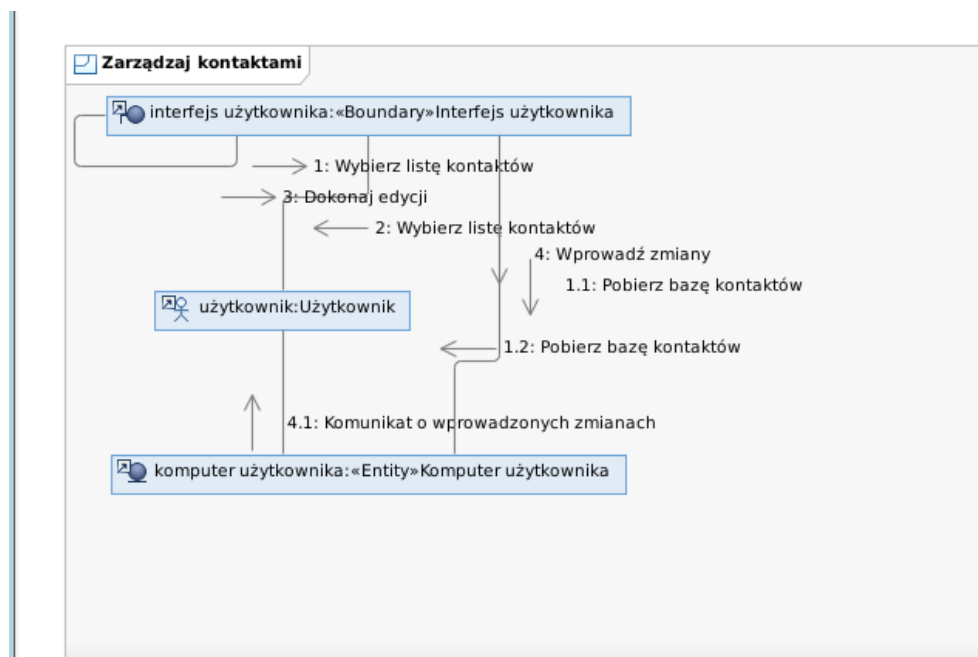
Wyślij wiadomość:



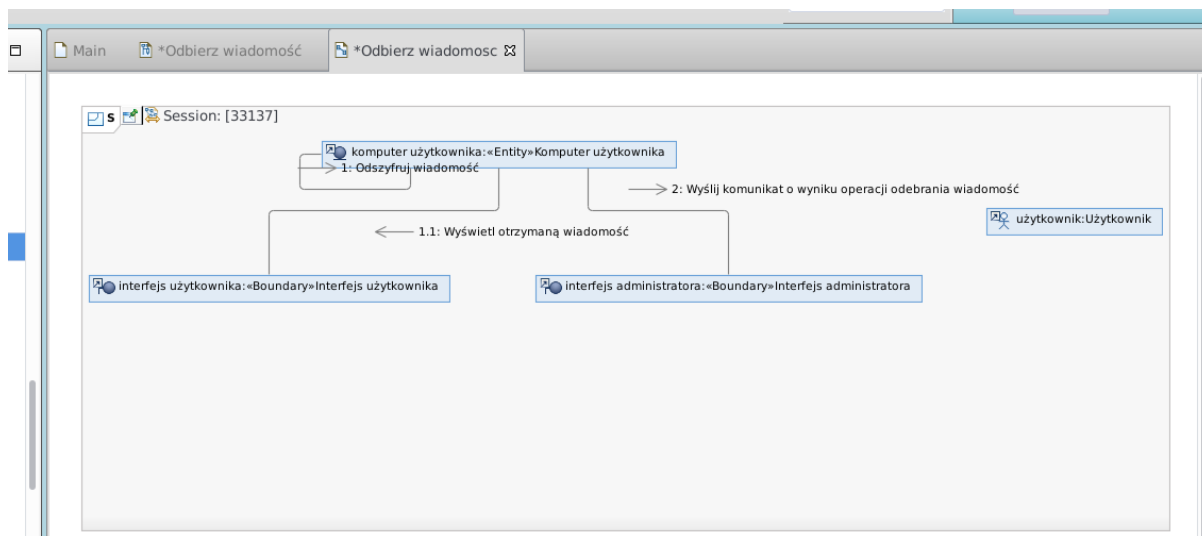
Uruchom terminal:



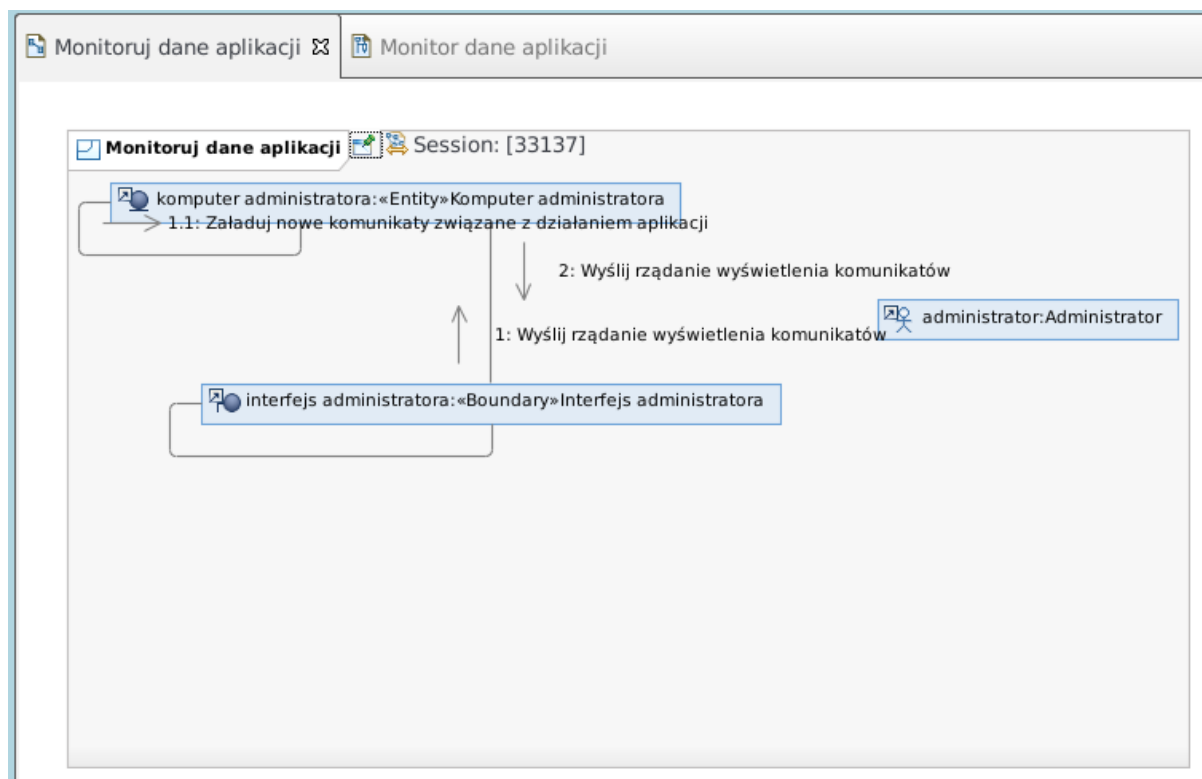
Zarządzaj kontaktami:



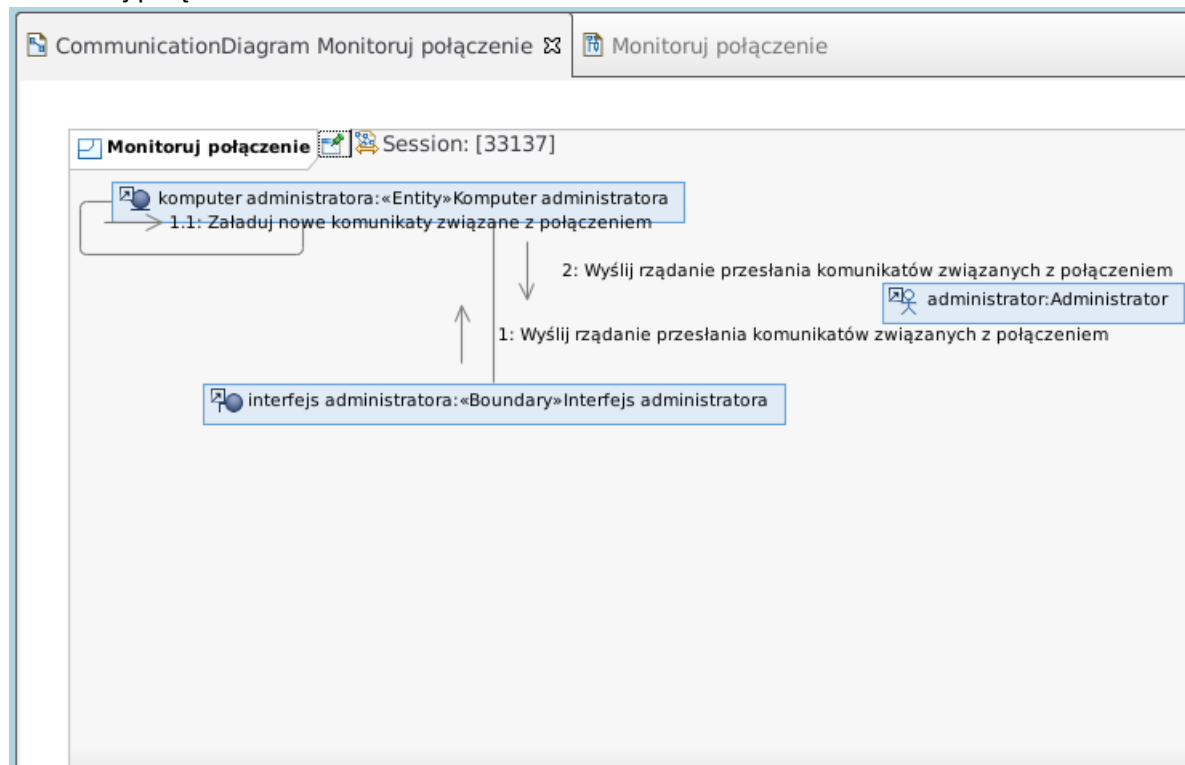
Odbierz wiadomość:



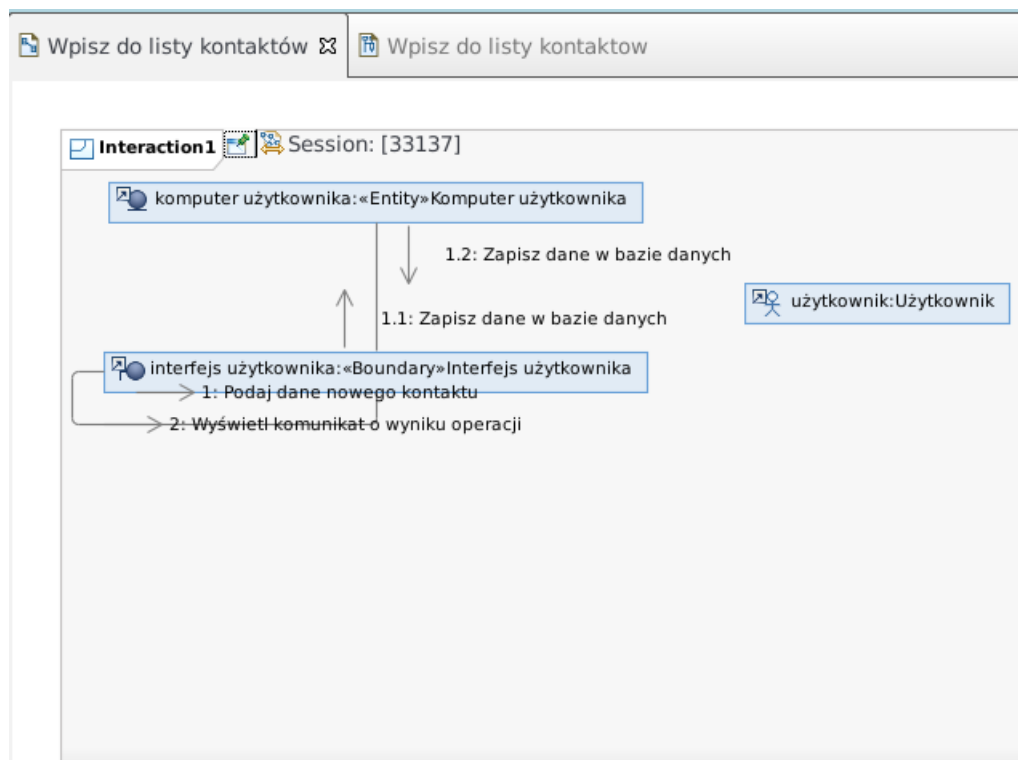
Monitoruj dane aplikacji



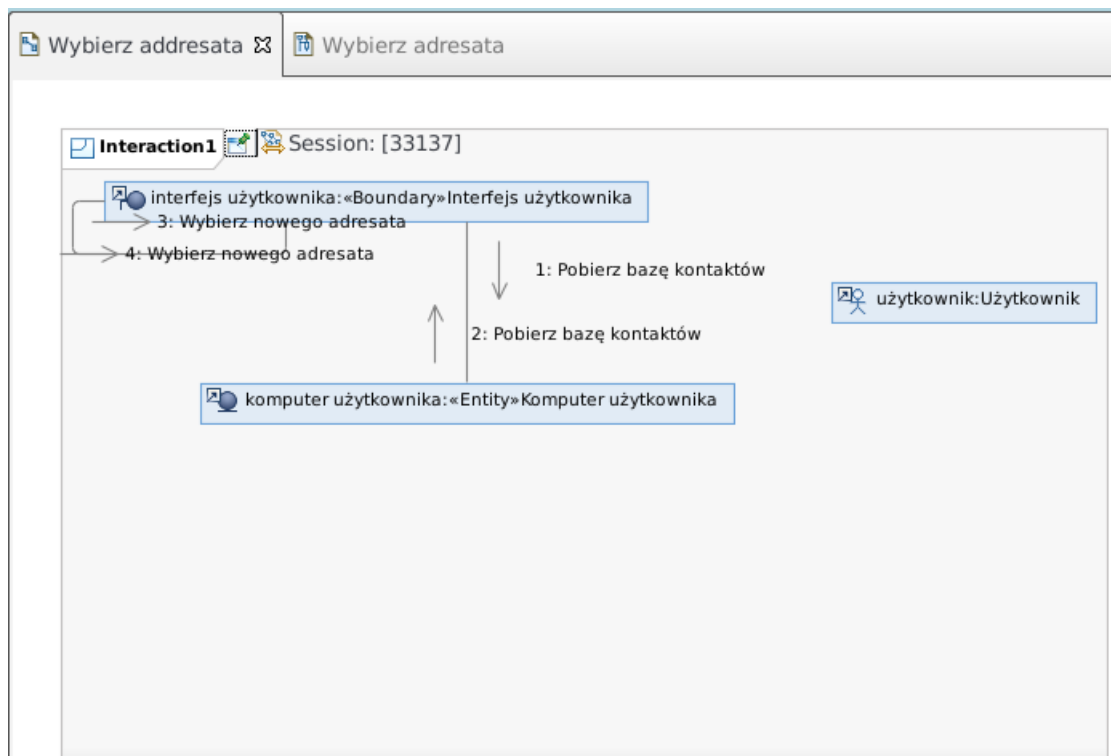
Monitoruj połączenie



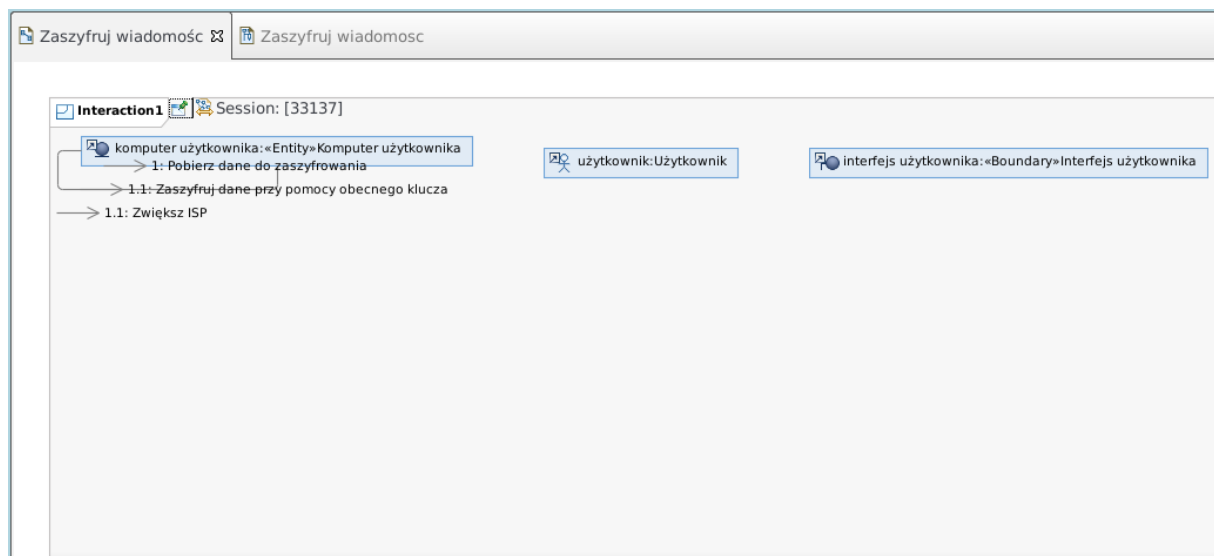
Wpisz do listy kontaktów



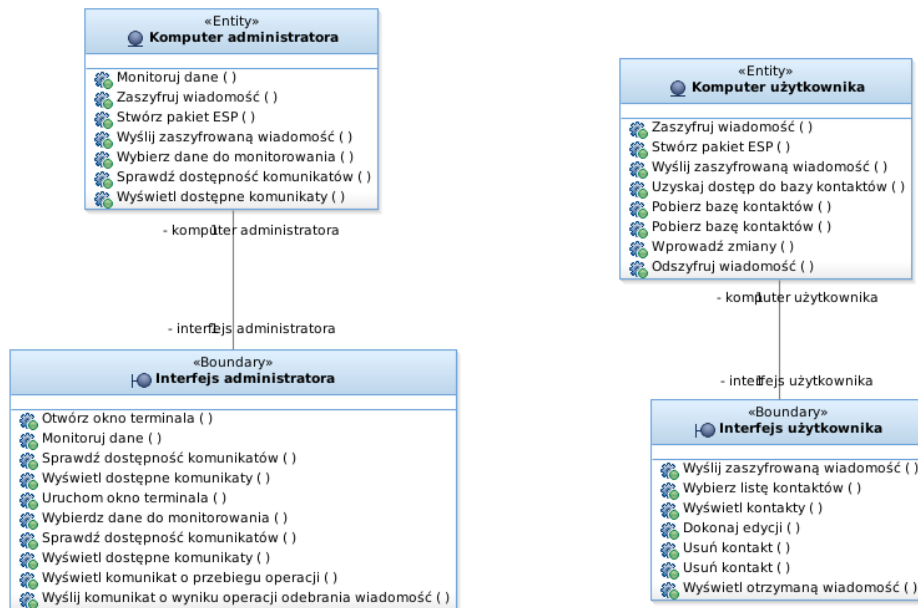
Wybierz adresata



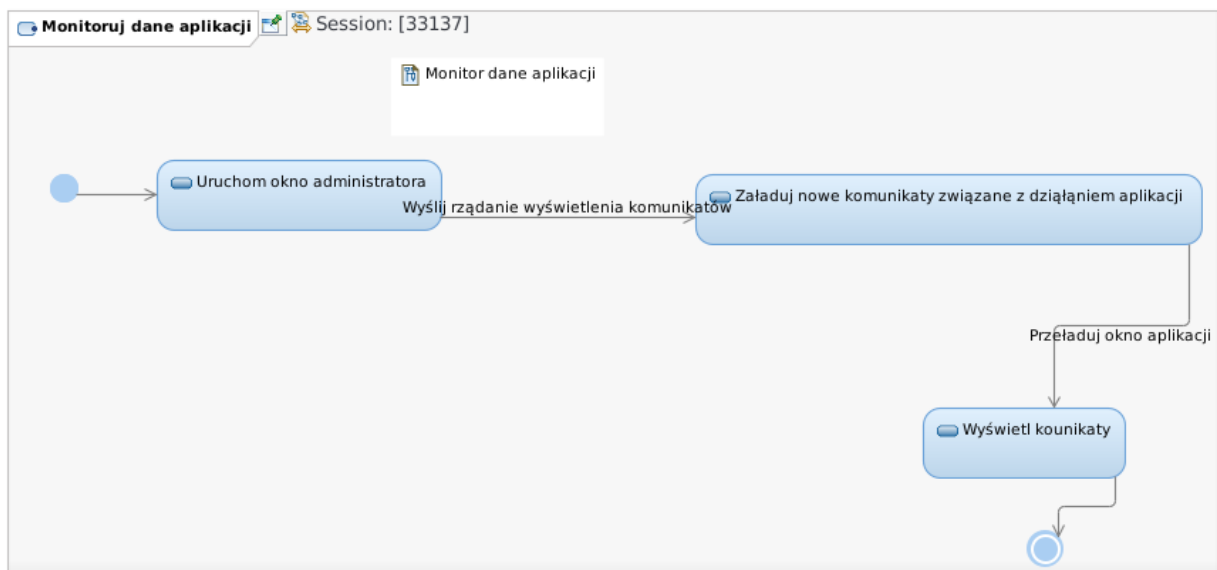
Zaszyfruj wiadomość



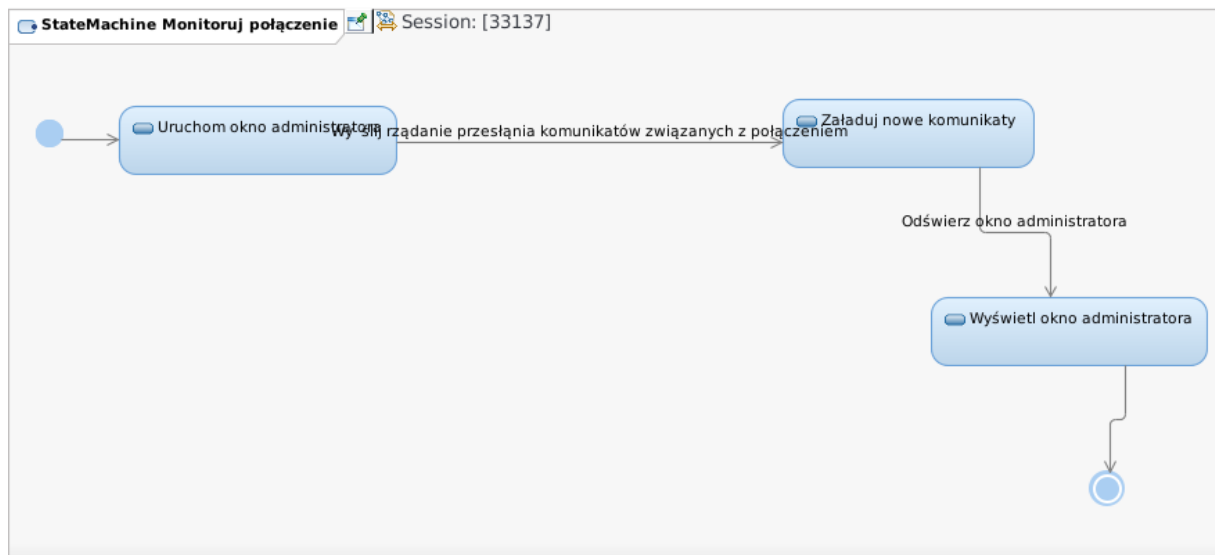
14. Diagram klas



15. Diagramy stanów



Rysunek 1SM Monitoruj dane aplikacji



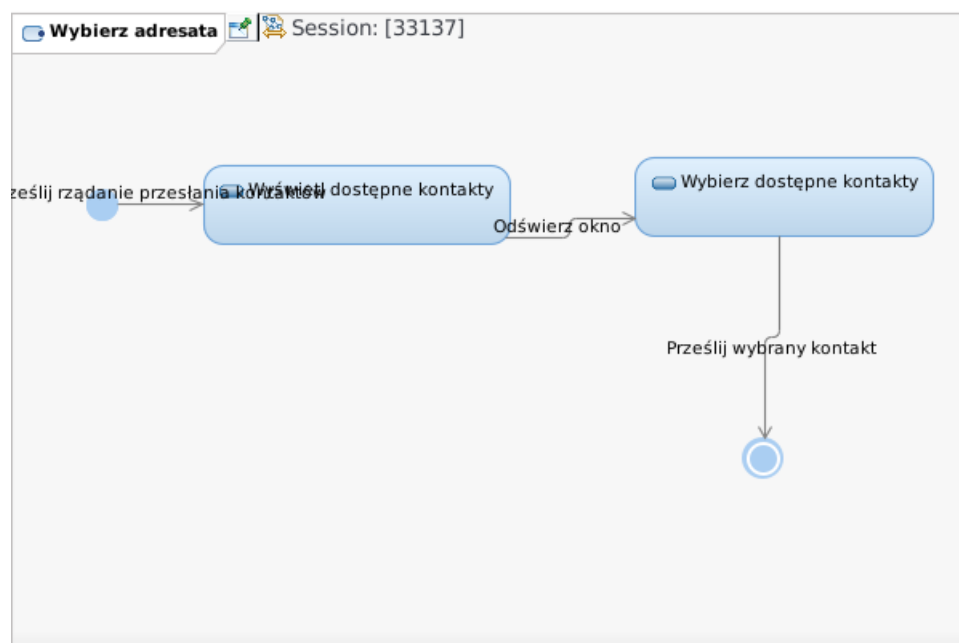
Rysunek 2 SM Monitoruj połączenie



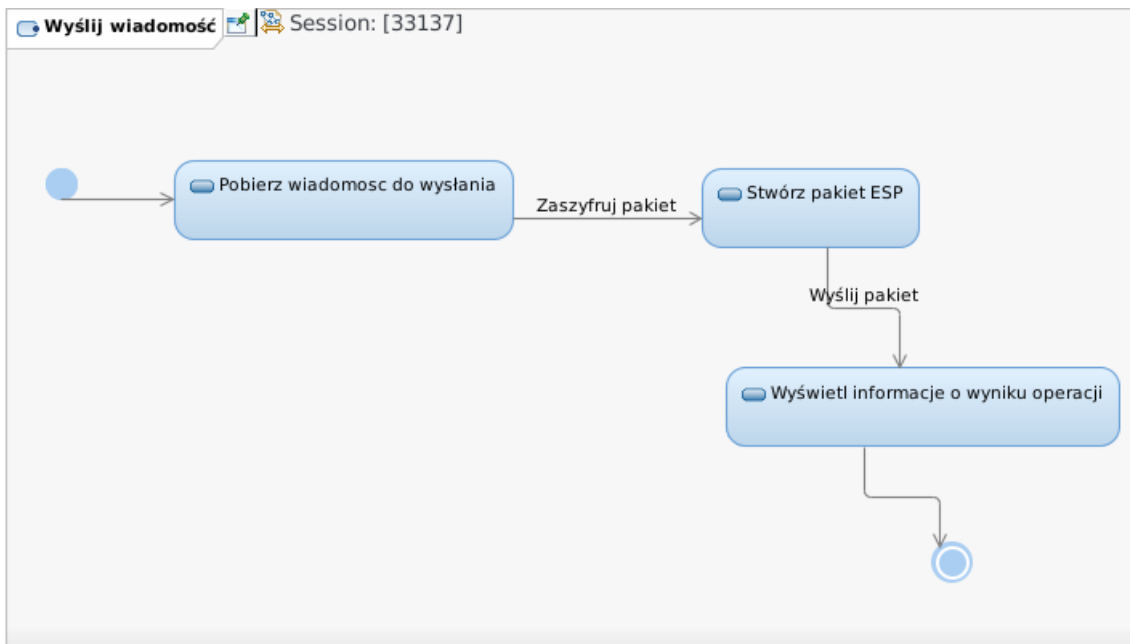
Rysunek 3 SM Odbierz wiadomość



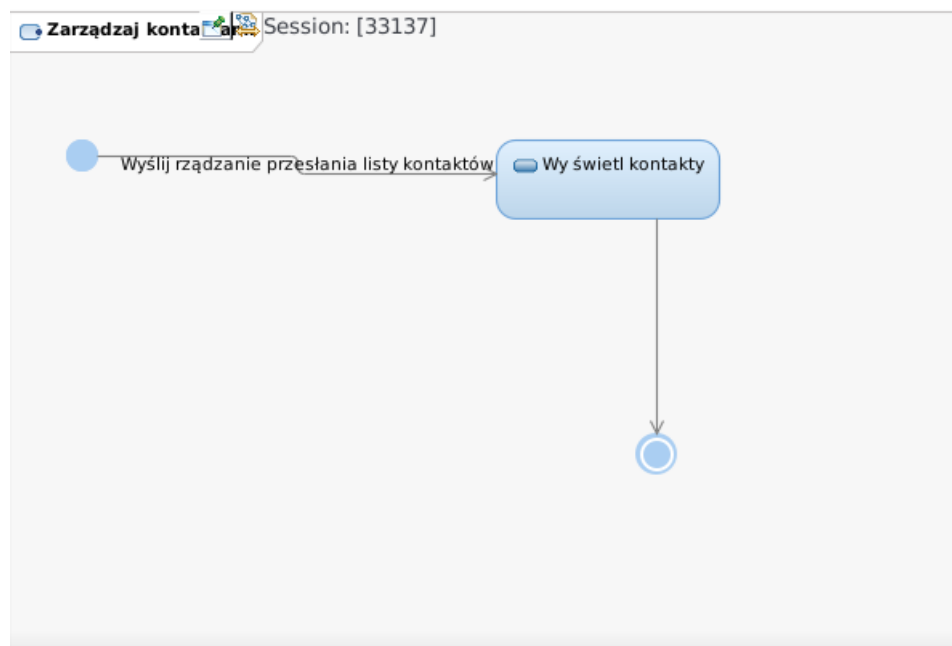
Rysunek 4 SM Uruchom terminal



Rysunek 5 SM Wybierz adresata



Rysunek 6 SM wyślij wiadomość

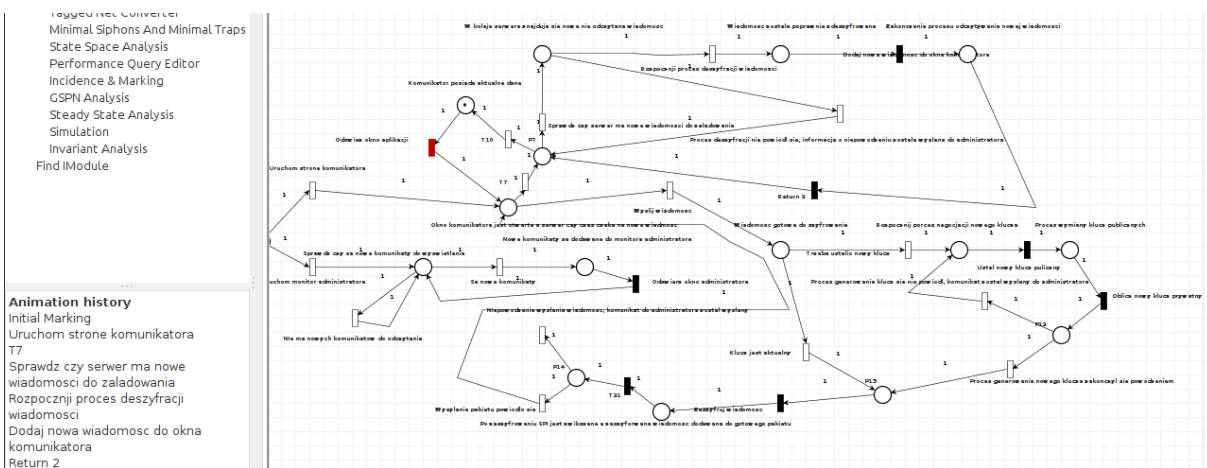
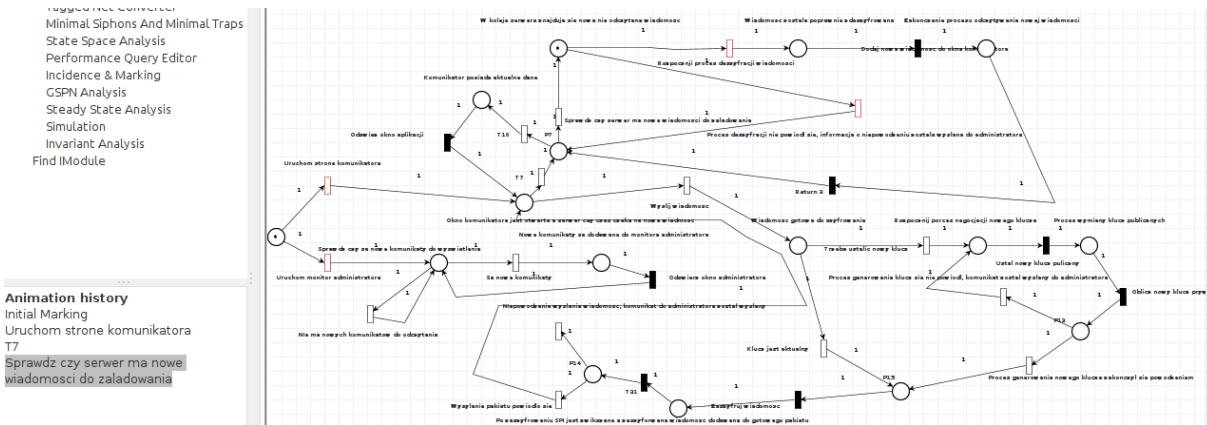
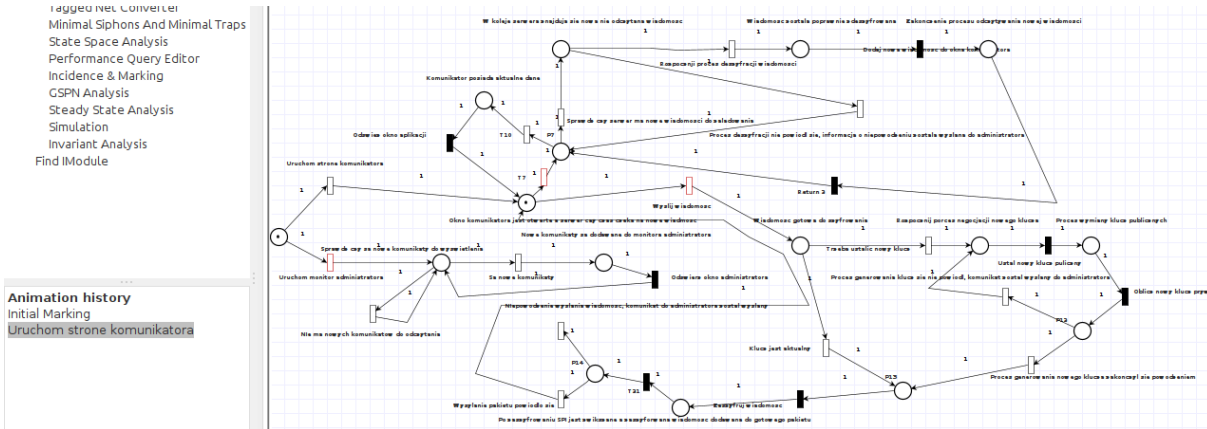


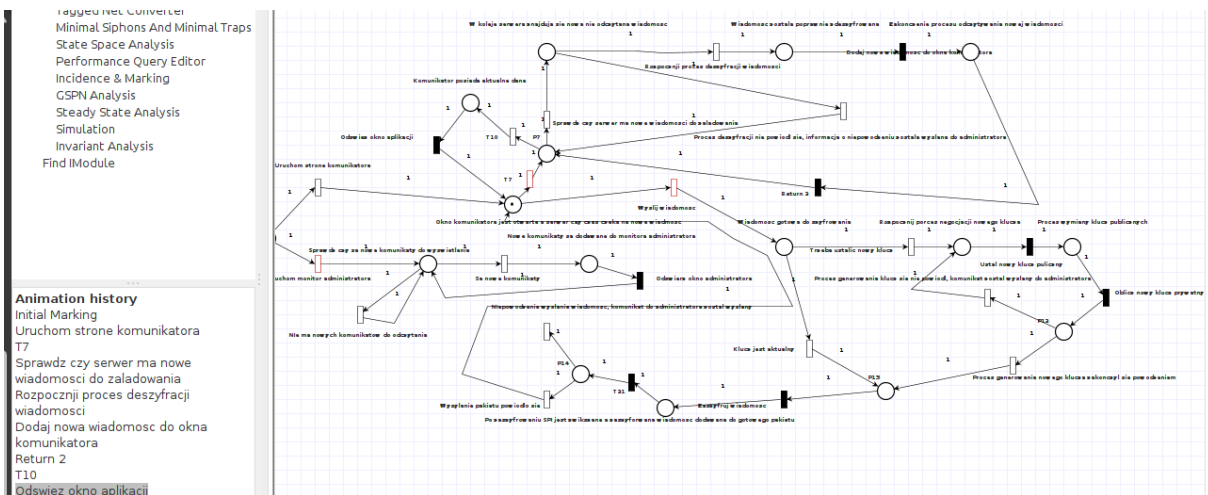
Rysunek 7 SM zarządzaj kontaktami

17. TESTY

1. TEST 1

Test pierwszy polega na sprawdzeniu czy użytkownik po uruchomieniu programu będzie domyślnie sprawdzał czy nie dostał żadnej nowej wiadomości. W przypadku pojawienia się nowych wiadomości powinny być one odczytane oraz wyświetlone użytkownikowi.



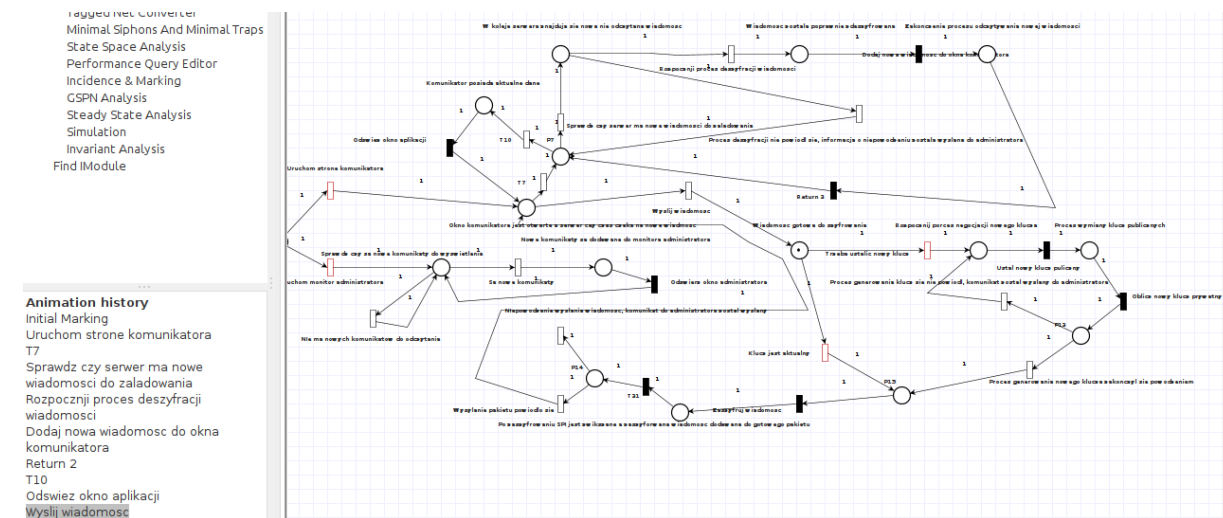


Wynik:

W teście 1 zostało pokazane, że po uruchomieniu aplikacji zostają załadowane nowe wiadomości a następnie wyświetlone użytkownikowi. Test zakończony **POZYTYWNIE**

2. TEST 2

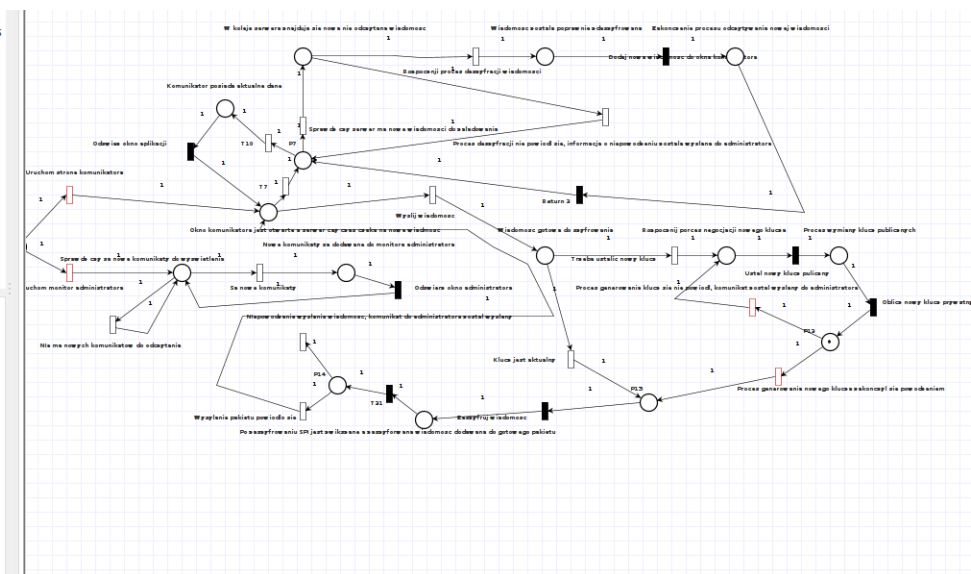
Przed wysłaniem wiadomości użytkownik powinien ustalić nowy klucz do używania w procesie szyfrowania/ deszyfrowania wiadomości.



Tagged Net Converter
Minimal Siphons And Minimal Traps
State Space Analysis
Performance Query Editor
Incidence & Marking
GSPN Analysis
Steady State Analysis
Simulation
Invariant Analysis
Find IModule

Animation history

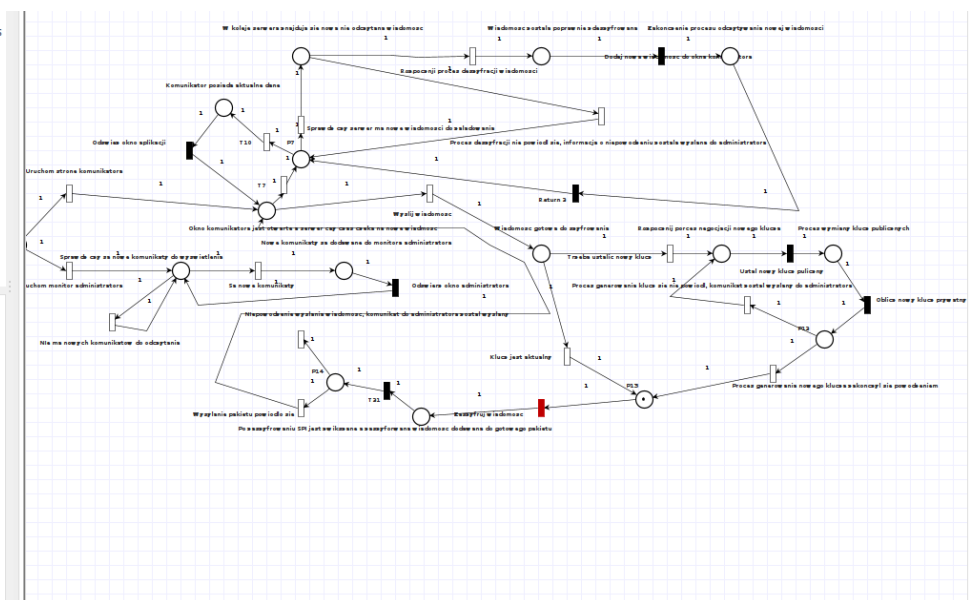
Initial Marking
Uruchom stronę komunikatora
T7
Sprawdz czy serwer ma nowe wiadomości do załadowania
Rozpocznij proces deszyfracji wiadomości
Dodaj nowa wiadomość do okna komunikatora
Return 2
T10
Odśwież okno aplikacji
Wyslij wiadomość
Trzeba ustalić nowy klucz
Ustal nowy klucz publiczny
Oblicz nowy klucz prywatny



Tagged Net Converter
Minimal Siphons And Minimal Traps
State Space Analysis
Performance Query Editor
Incidence & Marking
GSPN Analysis
Steady State Analysis
Simulation
Invariant Analysis
Find IModule

Animation history

Initial Marking
Uruchom stronę komunikatora
T7
Sprawdz czy serwer ma nowe wiadomości do załadowania
Rozpocznij proces deszyfracji wiadomości
Dodaj nowa wiadomość do okna komunikatora
Return 2
T10
Odśwież okno aplikacji
Wyslij wiadomość
Trzeba ustalić nowy klucz
Ustal nowy klucz publiczny
Oblicz nowy klucz prywatny
Proces generowania nowego klucza zakończył się powodzeniem

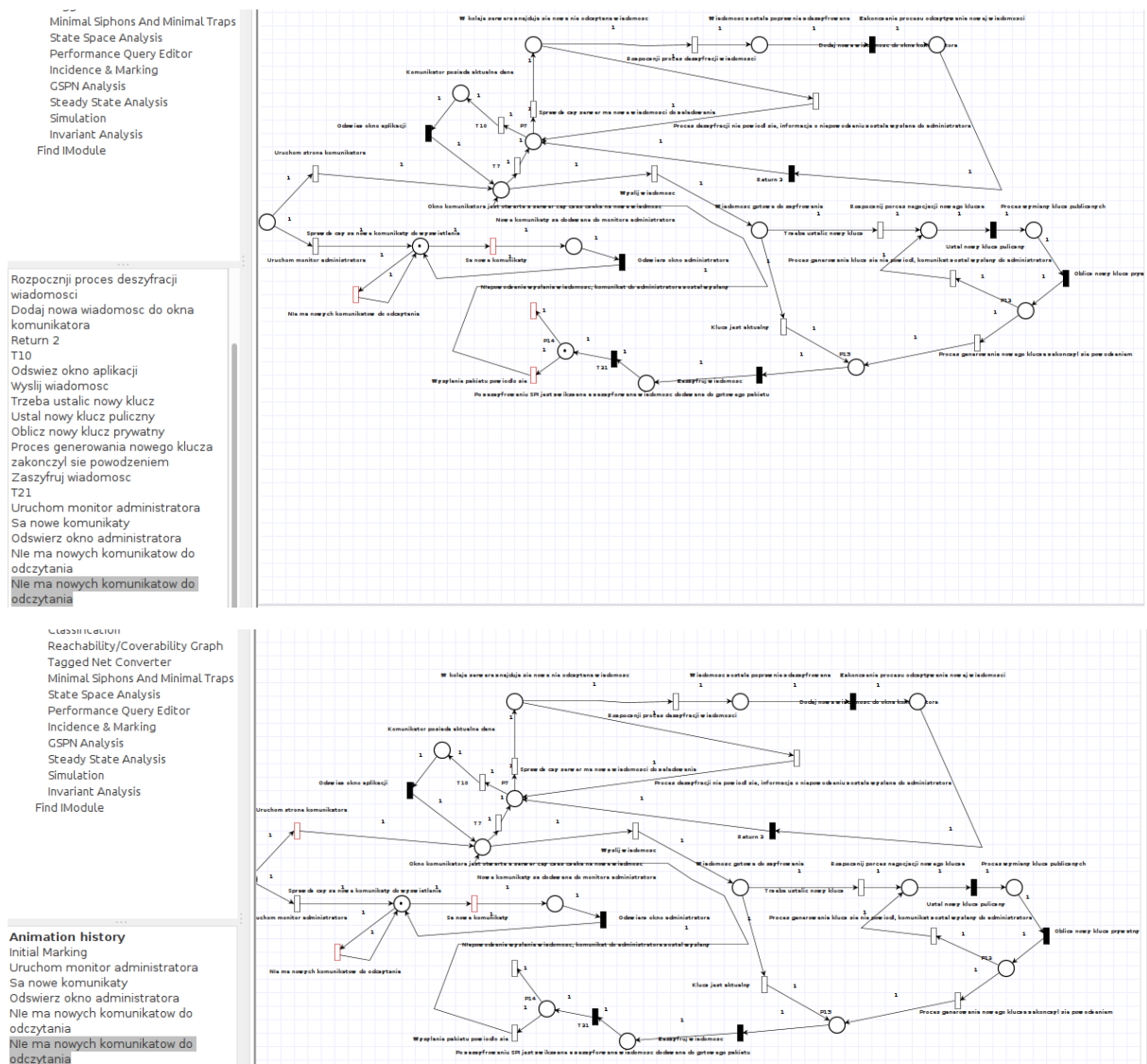


Wynik:

W teście 2 zostało pokazane, że po przed wysłaniem wiadomości w razie potrzeby można wygenerować nowy klucz. Test zakończony **POZYTYWNIEM**

3. TEST 3

Administrator powinien mieć możliwość włączenia monitora oraz okresowe sprawdzanie dostępności nowych komunikatów w trakcie działania aplikacji. S



Wynik:

W teście 3 zostało pokazane, że administrator może otworzyć swój monitor nie tylko na początku działania aplikacji oraz, że może na bieżąco pobierać nowe komunikaty. Test zakończony **POZYTYWNI**

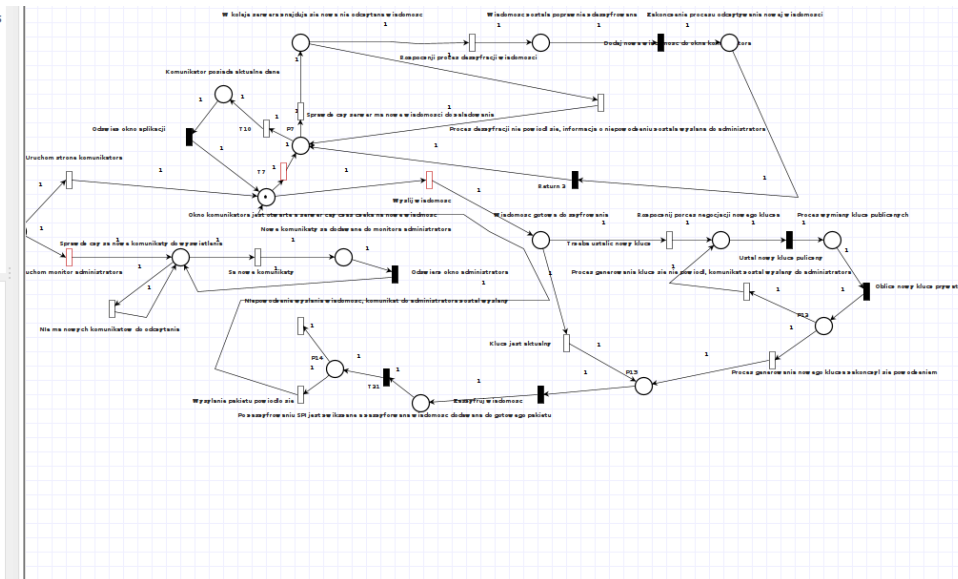
4. TEST 4

Użytkownik powinien mieć możliwość wysłania wiadomości bez konieczności generowania nowego klucza.

Minimal Siphons And Minimal Traps
State Space Analysis
Performance Query Editor
Incidence & Marking
GSPN Analysis
Steady State Analysis
Simulation
Invariant Analysis
Find IModule

Animation history

Initial Marking
Uruchom stronie komunikatora
Wyslij wiadomosc
Klucz jest aktualny
Zaszyfruj wiadomosc
T21
Wysylanie pakietu powiodlo sie
T7
Sprawdz czy serwer ma nowe wiadomosci do zaladowania
Rozpoczni proces deszyfracji wiadomosci
Dodaj nowa wiadomosc do okna komunikatora
Return 2
T10
Odswiez okno aplikacji



Wynik: W teście 4 zostało pokazane, że użytkownik może wysyłać wiadomości bez konieczności każde razowego generowania nowych kluczy (tylko w zadanym interwale). Test zakończony **POZYTYWNIIE**

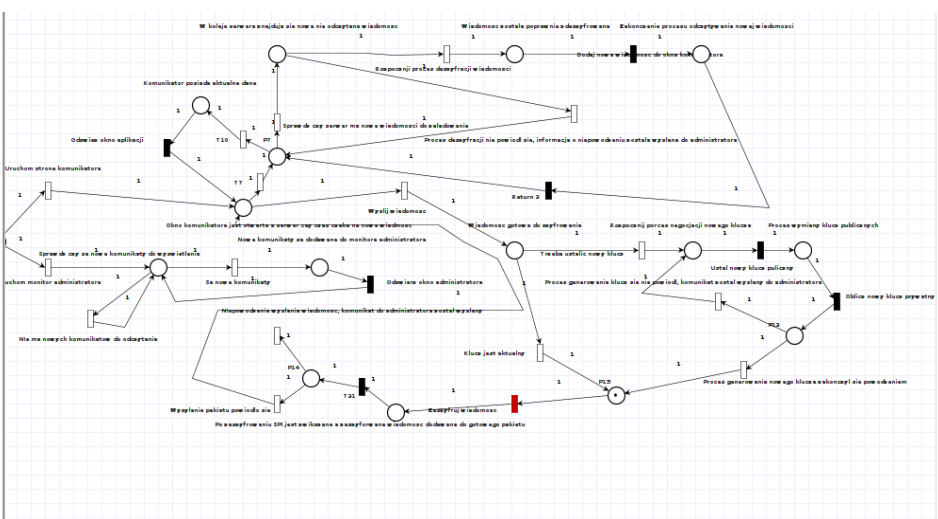
5. TEST 5

W przypadku kiedy nie udałaby się generacja kluczy, aplikacja powinna samodzielnie przystąpić do ponownej generacji.

Minimal Siphons And Minimal Traps
State Space Analysis
Performance Query Editor
Incidence & Marking
GSPN Analysis
Steady State Analysis
Simulation
Invariant Analysis
Find IModule

Animation history

Initial Marking
Uruchom stronie komunikatora
Wyslij wiadomosc
Trzeba ustalic nowy klucz
Ustal nowy klucz publiczny
Oblicz nowy klucz prywatny
Proces generowania klucza sie nie powiodl, komunikat zostal wyslany do administratora
Ustal nowy klucz publiczny
Oblicz nowy klucz prywatny
Proces generowania nowego klucza zakonczyl sie powodzeniem



Wynik: W teście 5 zostało pokazane, że aplikacja samoczynnie przystąpi do ponownej generacji kluczy w przypadku niepowodzenia poprzedniej generacji. Test zakończony **POZYTYWNIIE**

18. Wyniki testów możliwych do przeprowadzenia w PIPE.

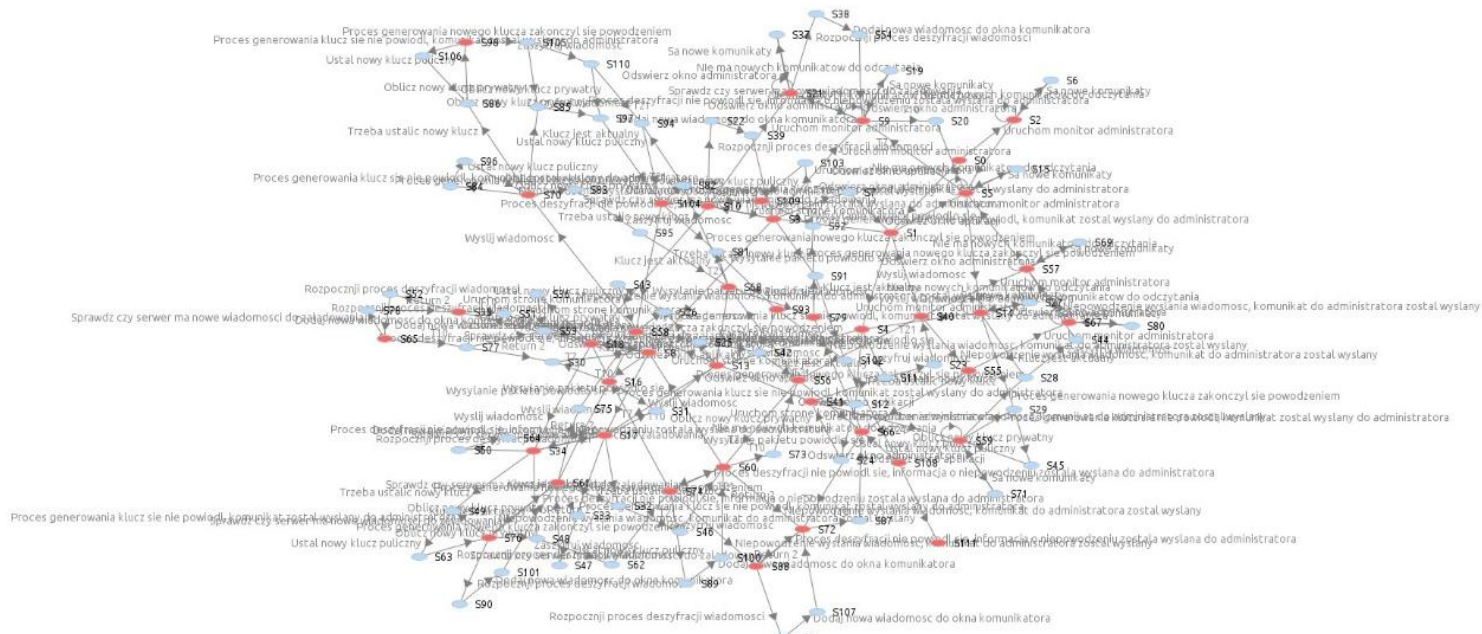
| Steady State Distribution of Tangible States | | Sojourn times for tangible states | | Steady State Distribution of Tangible States | |
|--|---------|-----------------------------------|---------|--|---------|
| Marking | Value | Marking | Value | Marking | Value |
| M0 | -0 | M0 | 0.5 | M0 | -0 |
| M1 | -0 | M1 | 0.0625 | M1 | -0 |
| M2 | -0 | M2 | 0.00989 | M2 | -0 |
| M3 | -0 | M3 | 0.22727 | M3 | -0 |
| M4 | -0 | M4 | 0.07692 | M4 | -0 |
| M5 | 0.00181 | M5 | 0.00869 | M5 | 0.00181 |
| M6 | 0 | M6 | 0.13514 | M6 | 0 |
| M7 | 0.00907 | M7 | 0.00976 | M7 | 0.00907 |
| M8 | -0 | M8 | 0.0098 | M8 | -0 |
| M9 | -0 | M9 | 0.0098 | M9 | -0 |
| M10 | -0 | M10 | 0.0098 | M10 | -0 |
| M11 | 0 | M11 | 0.04762 | M11 | 0 |
| M12 | 0.00082 | M12 | 0.009 | M12 | 0.00082 |
| M13 | 0 | M13 | 0.06667 | M13 | 0 |
| M14 | 0 | M14 | 0.07463 | M14 | 0 |
| M15 | 0 | M15 | 0.0087 | M15 | 0 |
| M16 | 0.00004 | M16 | 0.005 | M16 | 0.00004 |
| M17 | -0 | M17 | 0.5 | M17 | -0 |
| M18 | 0 | M18 | 0.06662 | M18 | 0 |
| M19 | 0.00009 | M19 | 0.005 | M19 | 0.00009 |
| M20 | 0 | M20 | 0.00869 | M20 | 0 |
| M21 | 0.00001 | M21 | 0.005 | M21 | 0.00001 |
| M22 | 0 | M22 | 0.00976 | M22 | 0 |
| M23 | 0 | M23 | 0.00976 | M23 | 0 |
| M24 | 0 | M24 | 0.00901 | M24 | 0 |
| M25 | 0 | M25 | 0.0098 | M25 | 0 |
| M26 | 0.00928 | M26 | 0.06667 | M26 | 0.00928 |
| M27 | 0.46379 | M27 | 0.00999 | M27 | 0.46379 |
| M28 | 0 | M28 | 0.00901 | M28 | 0 |
| M29 | 0 | M29 | 0.00901 | M29 | 0 |
| M30 | 0.04638 | M30 | 0.41667 | M30 | 0.04638 |
| M31 | 0 | M31 | 0.005 | M31 | 0 |
| M32 | 0 | M32 | 0.005 | M32 | 0 |
| M33 | 0 | M33 | 0.41667 | M33 | 0 |
| M34 | 0.00422 | M34 | 0.09091 | M34 | 0.00422 |
| M35 | 0 | M35 | 0.01 | M35 | 0 |
| M36 | 0 | M36 | 0.005 | M36 | 0 |
| M37 | 0 | M37 | 0.01 | M37 | 0 |
| M38 | 0.00019 | M38 | 0.01 | M38 | 0.00019 |
| M39 | 0.00046 | M39 | 0.01 | M39 | 0.00046 |
| M40 | 0.00004 | M40 | 0.01 | M40 | 0.00004 |
| M41 | 0.46379 | M41 | ∞ | M41 | 0.46379 |

| Throughput of Timed Transitions | | Average Number of Tokens on a Place | |
|--|------------|---|------------------|
| Transition | Throughput | Place | Number of Tokens |
| Rozpoczni proces deszyfracji wiadomosci | 0.02218 | Komunikator posiada aktualne dane | 0 |
| Sprawdz czy serwer ma nowe wiadomosci do zaladowania | 0.02218 | Okno komunikatora jest otwarte a serwer cay czas czeka na nowe wiadmosc | 0.01109 |
| Uruchom monitor administratora | 0 | Start | 0 |
| Uruchom strone komunikatora | 0 | W koleje serwera znajduja sie nowa nie odczytana wiadomosc | 0.00022 |
| Wyslij wiadomosc | 0.05545 | Wiadomosc zostala poprawnie zdeszyfrowana | 0 |
| T7 | 0.1109 | Zakonczenie procesu odczytywania nowej wiadomosci | 0 |
| Proces deszyfracji nie powiodl sie, informacja o niepowodzeniu zostala wyslana do administratora | 0 | P7 | 0.05545 |
| T10 | 0.1109 | Wiadomosc gotowa do szyfrowania | 0.00504 |
| Trzeba ustalio nowy klucz | 0.00504 | Rozpoczni porces negocjacji nowego klucza | 0 |
| Klucz jest aktualny | 0.05041 | Proces wymiany klucz publicznych | 0 |
| Proces generowania klucz sie nie powiodl, komunikat zostal wyslany do administratora | 0 | P12 | 0.00005 |
| Proces generowania nowego klucza zakonczyl sie powodzeniem | 0.00504 | P13 | 0 |
| Niepowodzenie wyslania wiadomosc, komunikat do administratora zostal wyslany | 0.00001 | Po zaszyfrowaniu SPI jest zwikszone a zaszyfrowana wiadomosc dodawana do gotowego pakietu | 0 |
| Wysylanie pakietu powiodlo sie | 0.05545 | P14 | 0.00055 |
| Sa nowe komunikaty | 47.56365 | Sprawdz czy sa nowe komunikaty do wyswietlenia | 0.47564 |
| Nie ma nowych komunikatow do odczytania | 0.04756 | Nowe komunikaty sa dodawane do monitora administratora | 0 |

Petri net simulation results

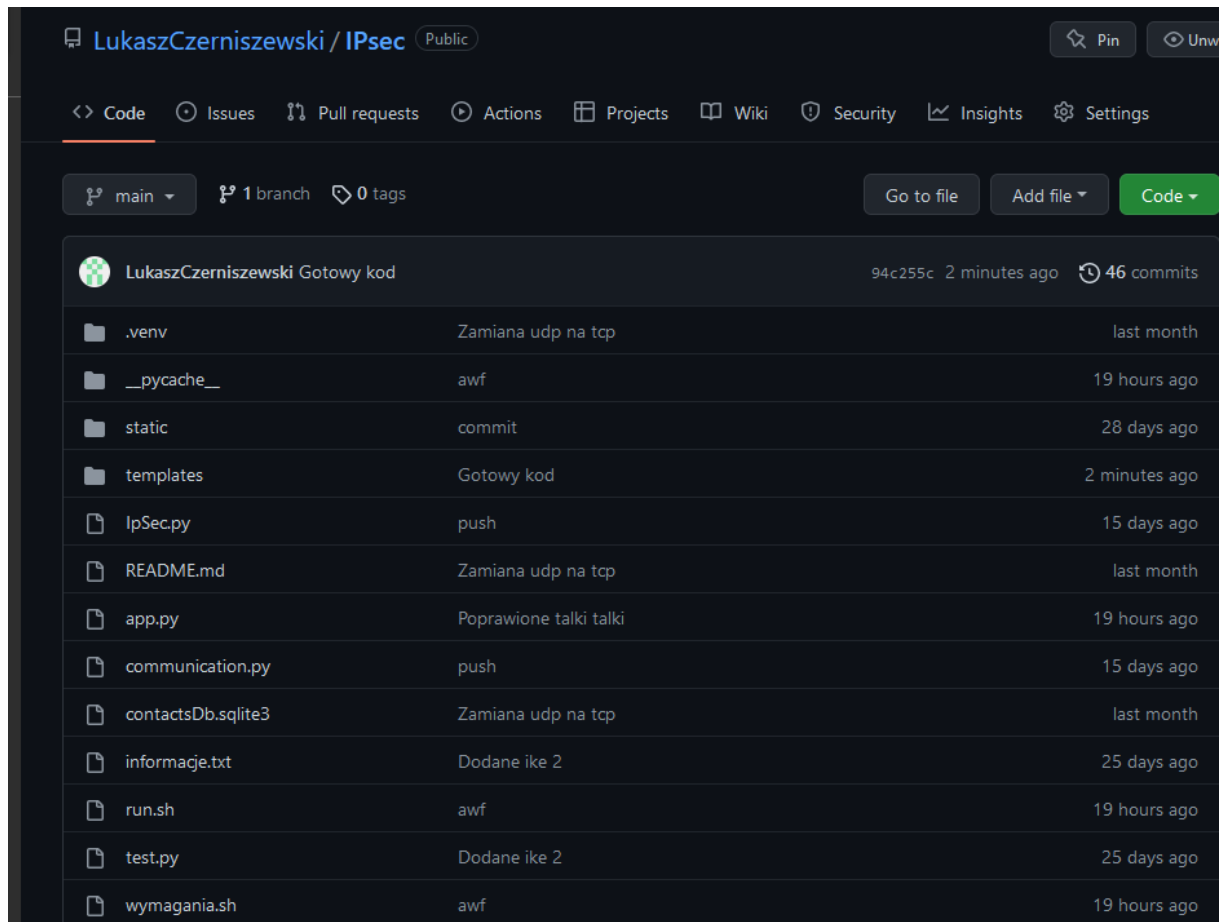
| Place | Average number of tokens 95% confidence interval (+/-) | |
|---|--|---------|
| Komunikator posiada aktualne dane | 0.0099 | 0.06185 |
| Okno komunikatora jest otwarte a serwer czy czas czeka na nowe wiadomosc | 0.52475 | 0.33777 |
| Start | 0.0198 | 0.72001 |
| W koleje serwera znajdują sie nowa nie odczytana wiadomosc | 0.0297 | 0.03247 |
| Wiadomosc zostala poprawnie zdeszyfrowana | 0.0099 | 0.02263 |
| Zakonczenie procesu odczytywania nowej wiadomosci | 0.0099 | 0.02263 |
| P7 | 0.42574 | 0.47337 |
| Wiadomosc gotowa do szyfrowania | 0 | 0.20668 |
| Rozpocznij porces negocjacji nowego klucza | 0 | 0.03383 |
| Proces wymiany klucz publicznych | 0.0099 | 0.03383 |
| P12 | 0.0099 | 0.03383 |
| P13 | 0 | 0.11899 |
| Po zaszyfrowaniu SPI jest zwikszone a zaszyfrowana wiadomosc dodawana do gotowego pakietu | 0.0099 | 0.12849 |
| P14 | 0.0099 | 0.18104 |
| Sprawdz czy sa nowe komunikaty do wyswietlenia | 0.52475 | 0.485 |
| Nowe komunikaty sa dodawane do monitora administratora | 0.45545 | 0.4602 |

19. Graf osiągalności



20. Opis demonstratora

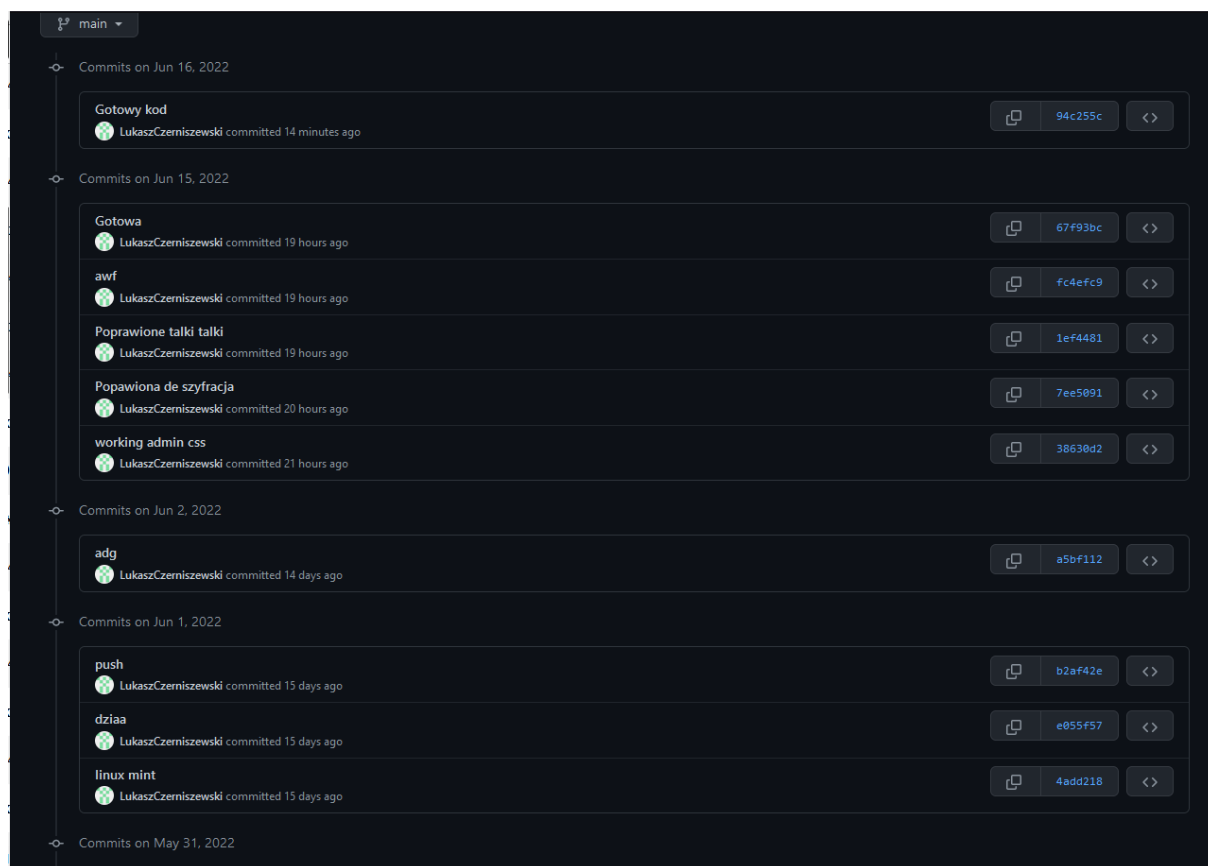
1 . Link do repozytorium: <https://github.com/LukaszCzerniszewski/IPsec>



The screenshot shows the GitHub interface for the repository 'LukaszCzerniszewski / IPsec'. The repository is public and has 46 commits. The file list includes:

| File/Folder | Commit Message | Time |
|--------------------|------------------------|---------------|
| .venv | Zamiana udp na tcp | last month |
| __pycache__ | awf | 19 hours ago |
| static | commit | 28 days ago |
| templates | Gotowy kod | 2 minutes ago |
| IpSec.py | push | 15 days ago |
| README.md | Zamiana udp na tcp | last month |
| app.py | Poprawione talki talki | 19 hours ago |
| communication.py | push | 15 days ago |
| contactsDb.sqlite3 | Zamiana udp na tcp | last month |
| informacje.txt | Dodane ike 2 | 25 days ago |
| run.sh | awf | 19 hours ago |
| test.py | Dodane ike 2 | 25 days ago |
| wymagania.sh | awf | 19 hours ago |

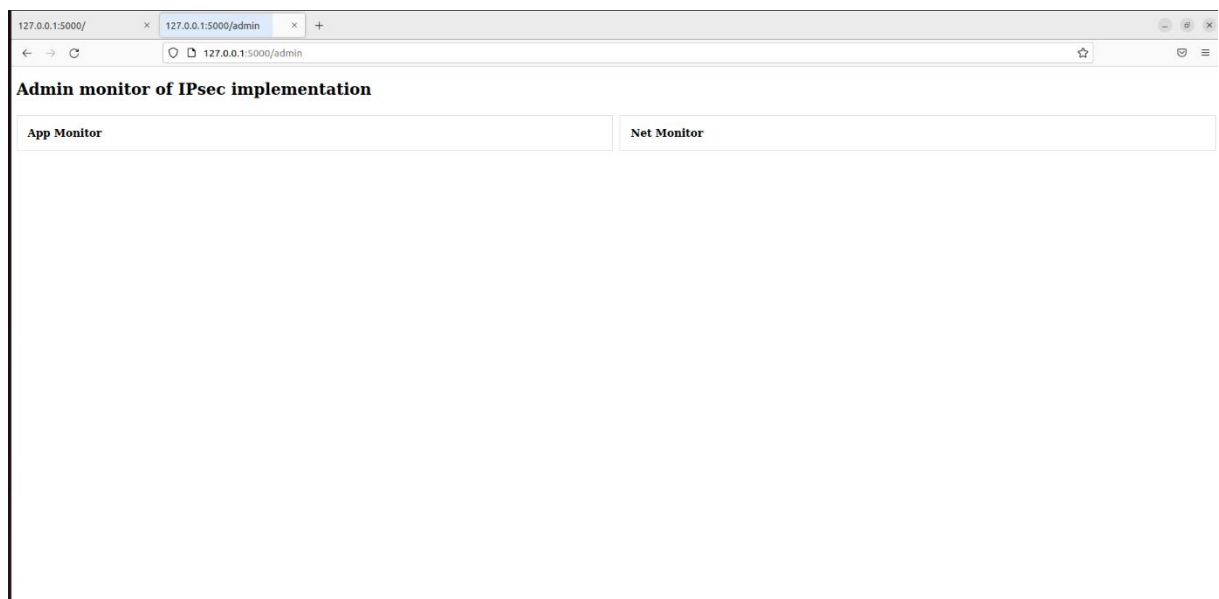
Link do historii zmian: <https://github.com/LukaszCzerniszewski/IPsec/commits/main>



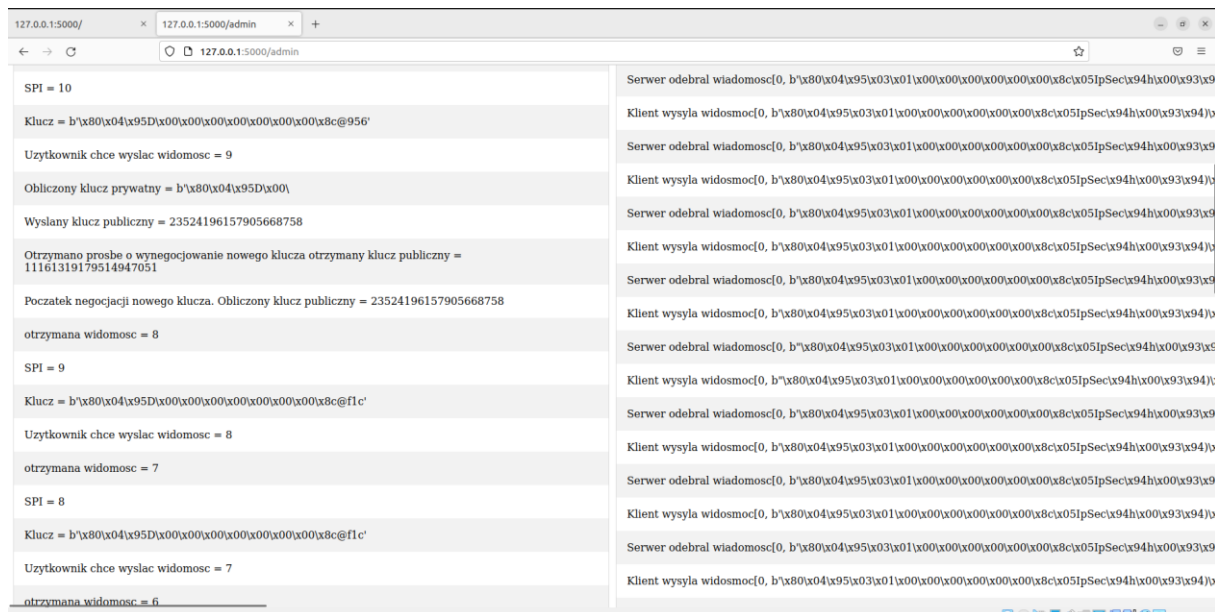
21. Obecnie działające elementy:

- Serwer do odbierania wiadomości;
- Klient do wysyłania wiadomości;
- Interfejs graficzny zaimplantowany w flasku;
- Generowanie pakietów ESP przy pomocy biblioteki scapy;
- Wysyłanie oraz odbieranie wiadomości.
- Generowanie kluczy publicznych/ prywatnych
- Protokół diffiego/ hellmana pełniący role IKE2
- Strona pozwalająca administratorowi na monitorowanie parametrów
- Skrypt pozwalający na automatyczne zainstalowanie wymaganych plików
- Skrypt każdorazowo sprawdzający aktualność bibliotek oraz uruchamiający aplikację.

22. Obrazy przedstawiające działanie aplikacji



[illegible]



23. User guide

1. Linux (Zalecany)

1. Na urządzeniu powinien być zainstalowany Python3 (domyślnie znajdują się na większości systemów z tej rodziny)
2. Proszę pobrać kod oprogramowania z strony <https://github.com/LukaszCzerniszewski/IPsec.git>
3. Folder oraz wszystkie pliki znajdujące się w nim powinny posiadać uprawnienia do uruchamiania. W tym celu proszę wykonać polecenie `sudo chmod -R 777 IPsec`
4. Proszę wejść do folderu **IPsec** oraz uruchomić skrypt **run.sh** jako użytkownik sudo (`sudo ./run`)
5. W dowolnej przeglądarce proszę otworzyć adres <http://127.0.0.1:5000/>
6. W celu otwarcia monitora administratora należy otworzyć stronę <http://127.0.0.1:5000/admin>. W tym oknie możemy obserwować działania na poziomie aplikacji oraz przesyłania pakietów.
7. W oknie po lewej stronie znajduje się pole do wpisania danych osoby, z którą chcemy rozmawiać. Domyślnie rozmawiamy z samym sobą.
8. W centralnej części głównego okna znajduje się okno umożliwiające wysyłanie wiadomości oraz jest wyświetlana historia czatu.

2. Windows (Niezalecany)

1. Na urządzeniu powinien być zainstalowany Python3 (domyślnie znajdują się na większości systemów z tej rodziny)
2. Najprościej jest zainstalować jądro Linuxa oraz wykonać kroki zawarte w 1. Linux.
3. Inaczej po zainstalowaniu pythona3 wraz z pip3 proszę wykonać kolejno komendy:
 1. pip install flask
 2. pip install pyDH
 3. pip install scapy
4. Proszę uruchomić plik app.py jako administrator
5. Proszę wykonać kroki 5 – 8 z punktu 1.Linux

W systemie Windows mogą wystąpić problemy spowodowane z konfiguracją zapory sieciowej.