|  |
| --- |
| Warszawa,20.01.2010  Mateusz Drzymała  Robert Strulak |
| Steganograficzny komunikator w sieci LAN oparty o metodę PadSteg. |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |

Spis treści

[1. Opis systemu PadSteg. 2](#_Toc283330407)

[2. Decyzje projektowe. 3](#_Toc283330408)

[3. Opis aplikacji 3](#_Toc283330409)

[4. Podsumowanie 4](#_Toc283330410)

# Opis systemu PadSteg.

Steganografia jest nauką, której celem jest przekazywanie informacji w taki sposób aby sam fakt wymiany informacji był ukryty. W przeciwieństwie do kryptografii nauka ta nie koncentruję się na szyfrowaniu wiadomości jednak na zapewnieniu poufności poprzez niejawną komunikację.

Spektrum doboru nośników steganograficznych jest ogromne. Mogą to być obrazy, dźwięki, pliki tekstowe czy nawet głowy niewolników(tatuowano informację na zgolonej głowie, następnie czekano aż włosy odrosną i wysyłano dany „nośnik” do odbiorcy). Ostatnia metoda jednak dawno już wyszła z użycia. W prezentowany przez nas systemie skupiamy się na tzw. Steganografi sieciowej, która jako nośnik informacji używa protokołów sieciowych.

System PadSteg jest przykładem steganografii sieciowej międzyprotokołowej. Jego działanie oparte jest o błędne dopełnianie ramek Ethernetowych. W sieciach LAN minimalna długość ramki wynosi 64B, stąd też każda krótsza ramka musi zostać dopełniona. Początkowo ustalono, że brakujące bajty będą zastępowane zerami, jednak jak się okazało, w zależności od producenta karty sieciowej czy jej sterownika dopełnienie to często zawiera różne znaki w szczególności części pamięci jądra systemu operacyjnego. Błędy związane z dopełnianiem wymienionych powyżej ramek stwarzają pewne możliwości, które mogą zostać użyte przez steganografie międzyprotokołową.

Działanie systemu PadSteg oparte jest o dopełnianie ramek Ethernetowych. W celu ustanowienia komunikacji należy wykonać następujące kroki:

1. **Inicjalizacja ukrytych węzłów – węzeł, który chce rozpocząć komunikację rozsyła wiadomość ARP-Request . W dopełnienie ramki tej wiadomości znajdują się informację, które pozwalają innym węzłom dowiedzieć się o istnieniu rozsyłającego węzła. Dopełnienie zawiera:**
2. **Losową liczbę RD,**
3. **Wynik funkcji skrótu obliczanej na podstawie wartości RD, adresu MAC nadawcy oraz identyfikatora protokołu – nośnika PID.**

**Następnie, każdy węzeł analizuje zawartość odebranej ramki, obliczana jest ta sama funkcja skrótu. Jeżeli wynik jest zgodny, to węzły są gotowe do rozpoczęcia komunikacji.**

1. **Wymiana danych – po ustalenie protokołu po którym będzie następowała komunikacja, wymiana danych może zostać rozpoczęta. Przykładowo jeżeli ustalono protokół TCP, ukryte informację mogą być umieszczane w dopełnieniach wiadomości ACK wysyłanych np. podczas transferu plików między węzłami.**

# **Decyzje projektowe.**

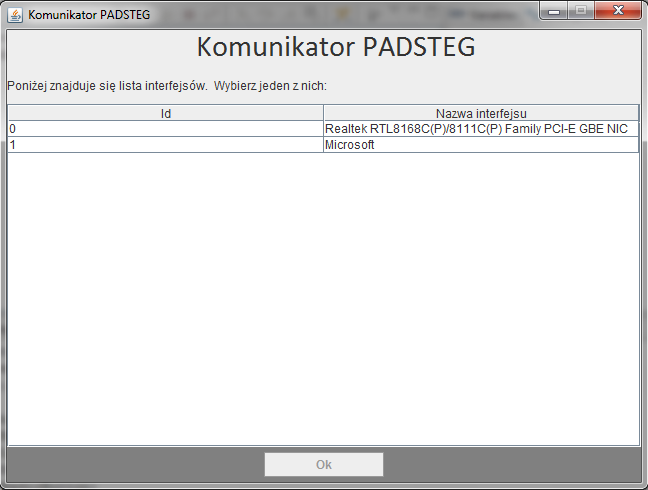
Projekt został napisany w języku JAVA przy użyciu biblioteki jNetPcap, która umożliwia niskopoziomowy dostęp do zawartości ramek. Jako nośnik

# Opis aplikacji

Aplikacja została napisana w języku JAVA przy użyciu biblioteki SWING. W celu uzyskanie możliwości dostępu do ramek skorzystaliśmy z biblioteki jNetPcap, która jest „wrapperem” biblioteki LibPcap/WinPcap.

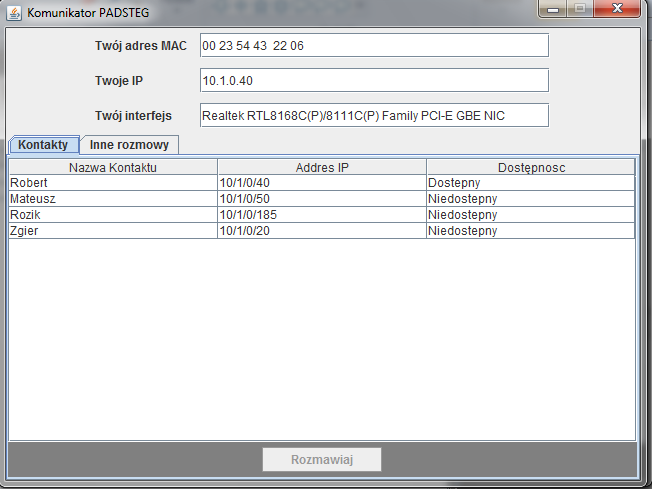
Po uruchomieniu aplikacji pojawia się następujący ekran:

Ekran nr.1



Ekran wyświetla wszystkie interfejsy kart sieciowych zainstalowane w danym komputerze. Po wyborze jednego z interfejsów należy zatwierdzić swoją decyzję przyciskiem OK. Przed przełączeniem się na następny ekran pojawi się komunikat, który umożliwia rezygnację z wyboru bądź jej zatwierdzenie.

Ekran nr.2

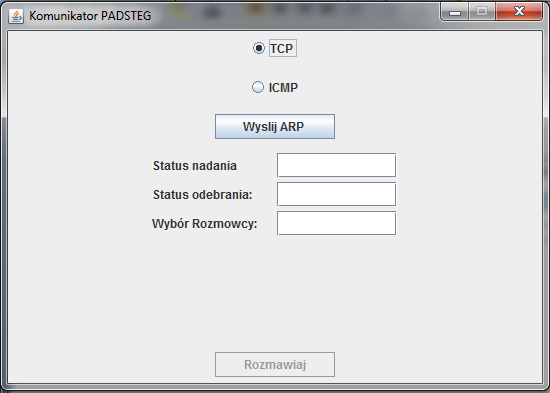


Ekran składa się z dwóch części. Pierwsza przedstawia parametry wybranej karty sieciowej, druga natomiast prezentuję tabele zawierająca listę użytkowników wczytaną z pliku konfiguracyjnego. Tabela zawiera trzy kolumny, z których godną szczególnej uwagi jest trzecia ponieważ wyświetla aktualny status użytkowników. Status „Dostepny” oznacza, że użytkownik posiada włączoną aplikację oraz jest gotowy na inicjację komunikacji.

Zakładka „Inne rozmowy” przedstawia inne rozmowy prowadzone przez użytkowników z naszej listy.

Po wybraniu użytkownika z listy a następnie naciśnięciu przycisku „Rozmawiaj” pojawia się następujący ekran.

Ekran nr.3



Ekran przedstawia odpowiednio statusy nadania oraz odebrania oraz protokół, który został wybrany naszego rozmówcę. Po odebraniu a następnie wysłaniu wiadomości ARP można rozpocząć rozmowę. Po kliknięcie przycisku „Rozmawiaj” pojawia się następujący ekran.

Ekran nr.4

# Podsumowanie