Programowanie Sieciowe
Projekt wstępny

Zespół nr 34:
Igor Matynia
Wiktor Topolski
Bartłomiej Pełka
Andrii Gamalii

Treść zadania

Stworzyć prosty system anonimizujący, będący uproszczeniem rozwiązania Tor.

Klient pozyskuje listę węzłów pośredniczących.

Klient łączy się z wybranym węzłem pośredniczącym, tunelując ruch za pomocą wybranego rozwiązania (TLS? IPSec?). Proszę ograniczyć się do tunelowania ruchu TCP.

Węzeł pośredniczący łączy się z oryginalną lokalizacją docelową (nie korzystając z kolejnych węzłów pośredniczących jak w oryginalnym rozwiązaniu Tor).

Węzeł pośredniczący powinien wprowadzać pseudolosowe opóźnienia i dokonywać zmiany rozmiaru/segmentacji przesyłanego strumienia ruchu.

Założenia

- Realizacja projektu w Pythonie
- Nadawca przesyła plik binarny do odbiorcy
- Centralny serwer dystrybucyjny przechowuje listę węzłów pośredniczących
- Klient może wybrać, czy chce też być węzłem pośredniczącym
- Tunelowanie ruchu TCP [klienci, węzły, serwer dystrybujący] za pomocą TLS
- Jeden węzeł pośredniczący może obsługiwać wiele klientów
- Węzeł pośredniczący jest wybierany przez nadawcę
- Odbiorca nie wie od kogo otrzymuje plik

Protokół komunikacyjny

W protokole będą występowały pakiety odpowiedzialne za między innymi:

- Rejestracja nowego węzła w sieci
- Zapytanie o listę węzłów w sieci
- Zapytanie o status węzła, w celu weryfikacji czy jest wciąż aktywny
- Odłączenie węzła z sieci
- Anonimizowany przesył danych poprzez pośrednika do odbiorcy

- Anonimizowany odbiór danych - nasłuchiwanie pakietów przychodzących z sieci
- Przesyłanie błędów przy transmisji danych (między węzłem pośredniczącym a nadawcą)

Zakres realizacji

- Implementacja struktury listy węzłów, mechanizm jej przesyłania
- Realizacja protokołu
- Ustawienie systemu CA, stworzenie certyfikatów do korzystania z TLS
- Implementacja węzła centralnego
    - Komunikacja z węzłem pośredniczącym
        - Utrzymywanie aktualności listy węzłów pośredniczących
    - Komunikacja z klientem
        - Nadanie listy węzłów pośredniczących
- Implementacja węzła pośredniczącego
    - Komunikacja z punktem docelowym
        - Wprowadzenie pseudolosowego opóźnienia
        - Sztuczna segmentacja strumienia ruchu
    - Komunikacja z węzłem centralnym
        - Powiadomienie o statusie węzła
        - Rejestracja/usuwanie węzła
    - Komunikacja z klientem
        - Obsługa TLS
        - Odbiór danych
- Implementacja klienta
    - Komunikacja z węzłem centralnym
        - Odpytywanie o listę dostępnych węzłów pośredniczących
    - Komunikacja z węzłem pośredniczącym
        - Obsługa klienta TLS
        - Anonimizowany przesył danych

Przypadki użycia

Anonimowy przesył danych do adresata

Przypadek użycia: Użytkownik chce wysyłać poufne informacje lub komunikować się bez obawy o przechwycenie danych.
Scenariusz:

1. Użytkownik pyta się węzła centralnego o listę węzłów pośrednich
2. Użytkownik wybiera losowy węzeł z listy
3. Użytkownik wysyła do wybranego węzła pośredniego wiadomość z danymi binarnymi i informacją o adresacie - nasłuchując przy tym komunikatów o możliwych błędach.
4. Węzeł pośredni wysyła do adresata wiadomość
5. Węzeł pośredni informuje użytkownika o sukcesie/niepowodzeniu

Dodanie komputera jako węzeł sieci

Przypadek użycia: W celu rozwoju sieci anonimizującej użytkownik może przyłączyć swój komputer jako nowy węzeł sieci.

Scenariusz:

1. Użytkownik prosi węzeł centralny o rejestrację podając swój adres, klucz publiczny i port
2. Węzeł centralny zapisuje informacje podane przez użytkownika i odsyła informację o zapisaniu do bazy węzłów pośredniczących
3. Użytkownik otwiera port do nasłuchiwania

Odbieranie danych

Przypadek użycia: Użytkownik chce obierać dane od innego użytkownika, który korzysta z systemu anonimizującego.

Scenariusz: Użytkownik otwiera port do nasłuchiwania jak w zwykłej sieci i obsługuje przychodzące pakiety ustalonego protokołu

Utworzenie nowego systemu anonimuzającego

Przypadek użycia: Użytkownik chce dać możliwość innym użytkownikom na anonimizację w sieci

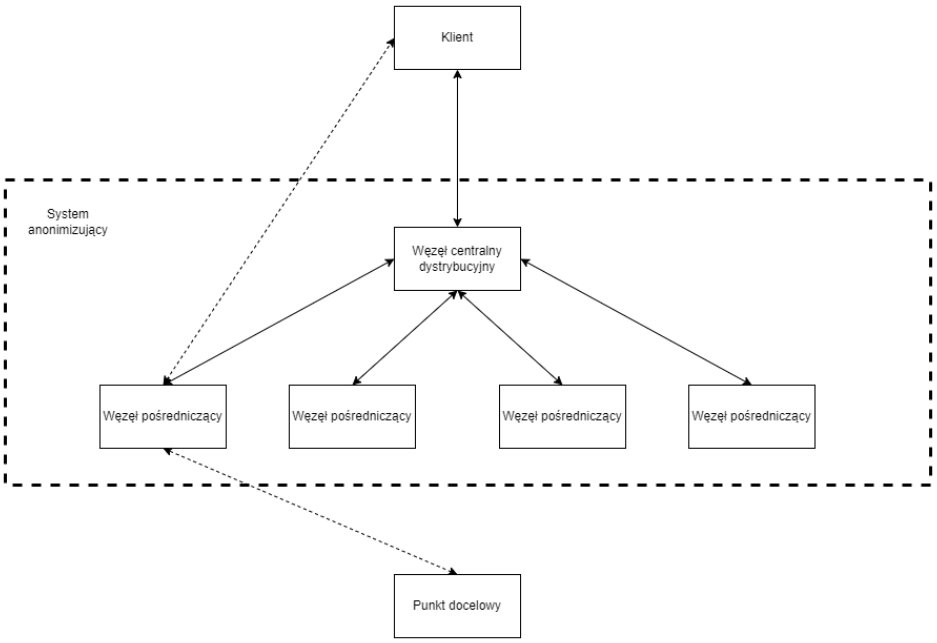
Scenariusz:

1. Użytkownik uruchamia centralny serwer dystrybucyjny
2. Użytkownik przekazuje interesantom adres serwera dystrybucyjnego
3. Użytkownik dodaje komputery działające jako węzły do sieci

Architektura

W sieci anonimizującej występują 4 główne elementy:

- Centralny serwer dystrybucyjny
- Węzeł, który podczas komunikacji pełni rolę pośrednika
- Nadawca wysyłający plik przez sieć do odbiorcy
- Odbiorca nie korzystający z sieci, ale obsługujący protokół



Obsługa sytuacji błędnych

Sytuacja “awaria używanego węzła pośredniczącego”

Węzeł pośredniczący przestaje działać mając otwarte połączenie z klientem.

Obsługa: klient przestaje próbować nadawać dane do tego węzła, próbuje łączyć się do innych węzłów pośredniczących z poprzednio otrzymanej listy i łączy się z jednym z działających węzłów.
Dodatkowo, węzeł dystrybucyjny cyklicznie odpytuje węzły o ich status, czy są wciąż aktywne. Jeśli któryś nie jest aktywny, zostaje on usunięty z listy.

Sytuacja “cicha awaria węzła”

Węzeł pośredniczący przestaje działać, lecz sieć się o tym nie dowiaduje.

Obsługa: Węzeł dystrybucyjny cyklicznie odpytuje węzły o ich status, czy są wciąż aktywne. Jeśli któryś nie jest aktywny, zostaje on usunięty z listy. W przypadku gdy to nadawca nie może się połączyć z wybranym węzłem pośrednim, ignoruje ten węzeł i wybiera inny z listy.

Sytuacja “otrzymana lista nie zawiera działających węzłów”

Lista, którą ma klient, nie zawiera działających węzłów.

Obsługa: klient żąda aktualnej listy od węzła centralnego.

Sytuacja “awaria węzła centralnego dystrybucyjnego”

Węzeł centralny przestaje działać.

Obsługa: Brak, system nie jest w stanie obsłużyć klientów.

Sytuacja “awaria odbiorcy/niedostępny odbiorca”

Węzeł pośredni nie może wysłać wiadomości do odbiorcy

Obsługa: węzeł informuje nadawcę o braku możliwości wysłania i zrywa połączenie z odbiorcą i nadawcą.

Sytuacji “pusta lista węzłów”

Klient dostaje pustą listę węzłów od węzła centralnego

Obsługa: timeout i ponowne żądanie.

Sytuacji “lista węzłów zawierająca jedynie siebie samego”

Klient dostaje listę węzłów, która zawiera tylko jego

Obsługa: timeout i ponowne żądanie.

Przypadki testowe

Przypadek testowy “pobieranie listy węzłów pośredniczących”

Cel: sprawdzenie poprawności przesyłanych danych o węzłach

Kroki:

1. Wysłanie zapytania o listę węzłów.
2. Sprawdzenie czy dane o węzłach (IP, porty) otrzymane przez klienta są wiarygodne.

Przypadek testowy “pobieranie pustej listy węzłów pośredniczących”

Cel: test obsługi sytuacji błędnej z pustą listą

Kroki:

1. Wysłanie zapytania o listę węzłów.
2. Jak jest pusta lista, to klient czeka i powraca do kroku 1.
3. Otrzymano niepustą listę.

Przypadek testowy “pobieranie listy węzłów pośredniczących, zawierającej tylko ten węzeł, który jest klientem”

Cel: test obsługi sytuacji błędnej

Kroki:

1. Wysłanie zapytania o listę węzłów.
2. Jak jest taka lista, to klient czeka i powraca do kroku 1.
3. Otrzymano dobrą listę.

Przypadek testowy “nawiązywanie połączenia z wybranym węzłem pośredniczącym”

Cel: upewnienie się, że klient jest w stanie połączyć się z węzłem

Kroki:

1. Wysłanie zapytania o listę węzłów.
2. Wybranie jednego z węzłów.
3. Nawiązanie połączenia z wybranym węzłem.

4. Potwierdzenie udanej komunikacji.

Przypadek testowy “szyfrowanie danych”

Cel: upewnienie się, że ruch pomiędzy klientem i węzłem jest szyfrowany

Kroki:

1. Pobieranie przez klienta listy węzłów.
2. Łączenie się z wybranym węzłem.
3. Włączenie nasłuchiwania pakietów (np. Wireshark).
4. Przesyłanie danych do wybranego węzła.
5. Sprawdzenie, czy przesłane pakiety były szyfrowane.

Przypadek testowy “anonimowość”

Cel: upewnienie się, że odbiorca nie zna adresu IP rzeczywistego nadawcy.

Kroki:

1. Pobieranie przez nadawcę listy węzłów.
2. Łączenie się z wybranym węzłem.
3. Włączenie nasłuchiwania pakietów na odbiorcy (np. Wireshark).
4. Przesyłanie danych do wybranego węzła.
5. Sprawdzenie, czy przesłane pakiety nie zawierają IP nadawcy w nagłówku.

Podział prac w zespole

Centralny serwer dystrybucyjny – Igor Matynia
Węzeł pośredniczący - Andrii Gamalii
Klient - Bartłomiej Pełka
Odbiorca – Wiktor Topolski
Opis projektu i implementacji – Igor Matynia
Opis scenariuszy komunikacji – Andrii Gamalii
Definicja komunikatów (protokół) - Wiktor Topolski
Opisy zachowania podmiotów komunikacji – Wiktor Topolski
Przeprowadzenie testów - Igor Matynia
Wyniki testów - Igor Matynia
Podsumowanie – Andrii Gamalii
Przygotowanie demonstracji - Bartłomiej Pełka

Scenariusz demonstracji

Przedstawienie podstawowego działania sieci

- Uruchomienie węzła centralnego, klienta, odbiorcy i dwóch pośredników
- Transmisja danych między klientem a odbiorcą

Awaria węzła

- Transmisja kolejnych danych na tym samym połączeniu

- Wyłączenie węzła pośredniczącego w transmisji
- Następuje przełączenie na nowy węzeł pośredniczący i kontynuacja transmisji

Ciche awarie węzłów i brak działających węzłów

- Wyłączane są wszystkie węzły pośredniczące i włączane są dwa nowe, z nowymi adresami, nieznane klientom w sieci
- Następuje próba transmisji danych, klient żąda od serwera nowej listy węzłów pośredniczących
- Następuje udana transmisja danych

Wyłączenie odbiorcy danych

- Wyłączony zostaje odbiorca
- Następuje próba transmisji danych ze strony nadawcy
- Węzeł pośredniczący informuje nadawcę, że odbiorca aktualnie nie działa

Ponowne włączenie odbiorcy danych

- Następuje udana transmisja danych

Co jeszcze ewentualnie: pokazanie w logach węzła pośredniczącego, że następuje szatkowanie pakietów