Metody zabezpieczania transmisji w sieci Ethernet

na przykładzie protokołu PPTP

Paweł Pokrywka

Plan prezentacji

- Założenia
- Cele
- Problemy i ich rozwiązania
- Rozwiązanie ogólne i jego omówienie

Założenia

- Sieć osiedlowa
  - Typowa, amatorska sieć komputerowa wykonana w technologii Ethernet. Kable sieciowe nie są specjalnie zabezpieczone. Urządzenia aktywne (koncentratory, przełączniki) znajdują się często w mieszkaniach użytkowników.
- Dostęp do Internetu
  - Sprzedajemy użytkownikom sieci usługę jaką jest możliwość korzystania z zasobów globalnej sieci

Cele

- W miarę bezawaryjny i cechujący się dobrą przepustowością dostęp do Internetu.
  - Większość operatorów na tym poprzestaje
- Dobra autoryzacja użytkowników.
  - Nie chcemy aby użytkownici kradli jedni drugim usługę za którą zapłacili, tym samym zmniejszając nasze przychody. Przykładem kradzieży usługi jest korzystanie z Internetu przez osobę która nie opłaciła abonamentu, natomiast podszywa się pod osobę, która go zapłaciła.
- Bezpieczeństwo transmisji internetowych.
  - Chcemy aby przynajmniej na drodze od użytkownika do naszego routera przesyłanie danych było bezpieczne.

Problemy i ich rozwiązania

- Problem
  - Podsłuch transmisji ethernetowych.
  - Jeśli korzystamy z koncentratorów to użytkownicy mogą się nawzajem podsłuchiwać przez przełączenie karty sieciowej w tryb promiscuous i uruchomienie analizatora pakietów.
- Rozwiązanie.
  - Korzystajmy z przełączników.

Problemy i ich rozwiązania

- Problem
  - Podsłuch transmisji ethernetowych (2)
  - Jeśli korzystamy z przełączników ethernetowych, podsłuch nie jest to już tak trywialny, ale cały czas prosty w realizacji, jeśli użytkownik dysponuje odpowiednimi narzędziami i wiedzą o atakach w sieci Ethernet (np. arp-spoofing, mac-flooding etc.)
- Rozwiązanie.
  - Szyfrujmy transmitowane dane. Służą do tego np. protokoły HTTPS (oparty na SSL), SSH.

Problemy i ich rozwiązania

- Problem.
  - Podszywanie się.
  - Przez zmianę IP i numeru MAC karty sieciowej (nie jest wymagane do tego specjalne oprogramowanie) atakujący jest w stanie podszyć się pod innego użytkownika, i w jego imieniu np. korzystać z Internetu (lub co gorsza dokonać włamania odpowiedzialnością obciążając tego użytkownika).
- Rozwiązanie.
  - Jedynym wyjściem jest zakup zaawansowanych przełączników ethernetowych i skonfigurowanie ich w ten sposób, aby do każdego portu był przypisany konkretny adres IP i MAC. Jest to rozwiązanie nieelastyczne oraz przede wszystkim – drogie.

Problemy i ich rozwiązania

- Problem.
  - Ataki typu człowiek w środku (ang. man in the middle).
  - Te ataki bazują na takiej ingerencji w transmisję, że użytkownik komunikuje się z atakującym myśląc, że połączył się z serwerem, zaś atakujący łączy się z serwerem w imieniu użytkownika.
  - Takie ataki buduje się wykorzystując np. arp-spoofing, dns-spoofing w połączeniu ze specjalizowanymi narzędziami. Istnieją aplikacje automatyzujące ataki nawet na połączenia szyfrowane.
- Rozwiązanie.
  - Różne rozwiązania dla różnych protokołów. W większości przypadków niezbędna jest świadomość zagrożenia u użytkownika. Przykład – HTTPS.

Problemy i ich rozwiązania

- Problem.
  - Przerywanie transmisji danych.
  - Atak polega na wykorzystaniu wiedzy zdobytej z podsłuchu sieciowego (adresy i porty pakietów oraz numery sekwencyjne TCP) do resetowania sesji TCP i zakończania połączeń UDP przez podszywanie się pod użytkownika. W przypadku połączeń TCP wystarczy wysłać odpowiedni pakiet z ustawioną flagą RST, w przypadku UDP pakiet ICMP. Istnieją narzędzia automatyzujące ten atak.
  - Efekt – klient nie może nawiązać połączenia z Internetem lub połączenia się rwą (i dzwoni do nas, bo „Internet się zepsuł”).
- Rozwiązanie.
  - Stosujmy protokoły odporne na resetowanie – ale jednocześnie musimy zapewnić łączność użytkowników z usługami internetowymi, które bazują na protokołach TCP i UDP. Konieczna jest jakaś forma tunelowania.

Rozwiązanie ogólne

Wirtualna Sieć Prywatna (VPN)

- VPN pomiędzy każdym użytkownikiem a routerem
- Spośród dostępnych rozwiązań wybrałem protokół PPTP (Point to Point Tunneling Protocol).
- Został on opracowany przez firmę Microsoft i (mimo tego ;-) posiada następujące zalety:

5. Jest dostępny standardowo na każdym komputerze z zainstalowanym systemem Windows.
6. Jest sprawdzony przez profesjonalistów z branży bezpieczeństwa komputerowego i z zachowaniem pewnych środków ostrożności przy wdrażaniu zapewnia wysokie bezpieczeństwo.

Diagram typowej sieci

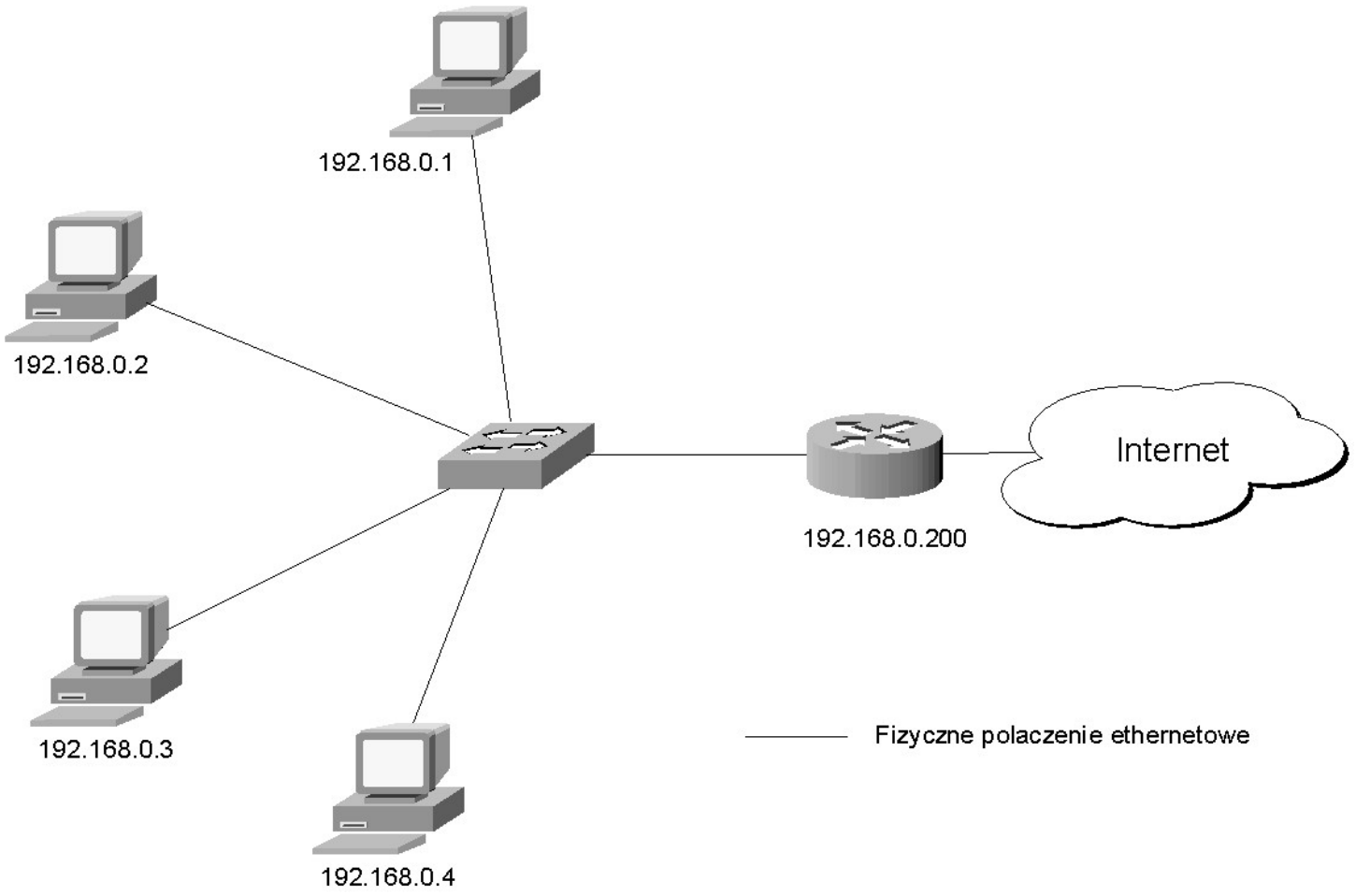


Diagram sieci z VPN

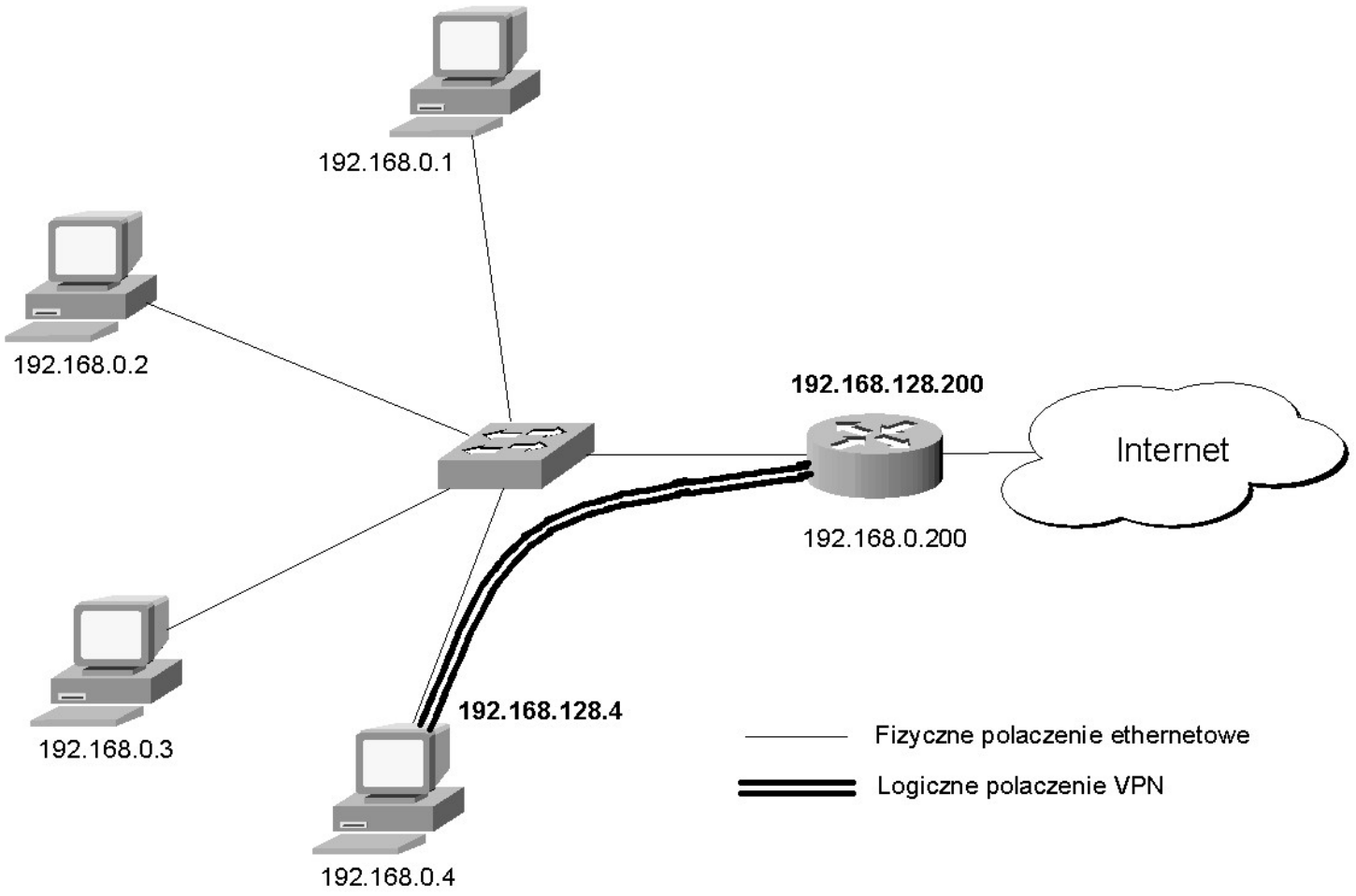
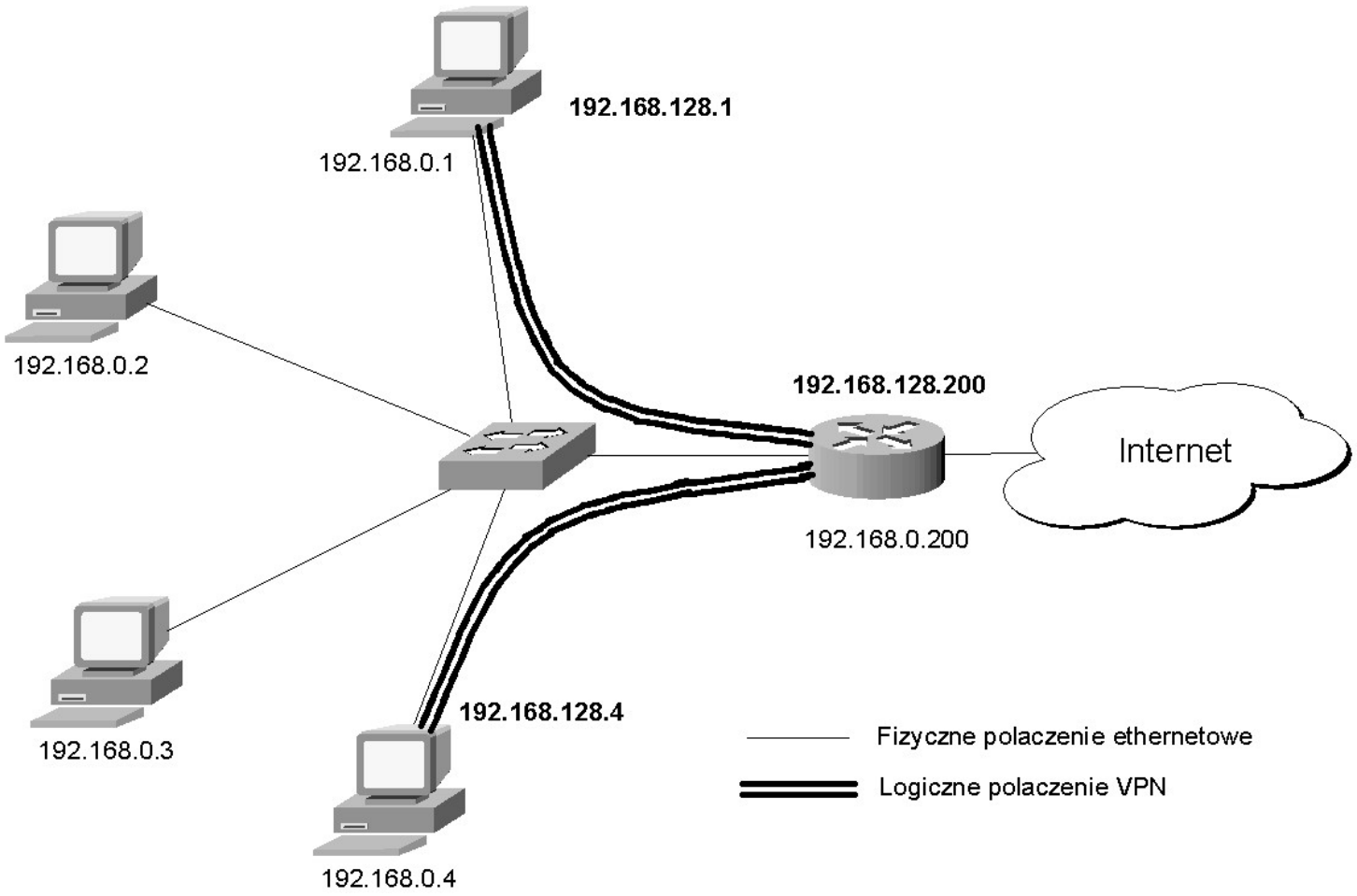


Diagram sieci z VPN

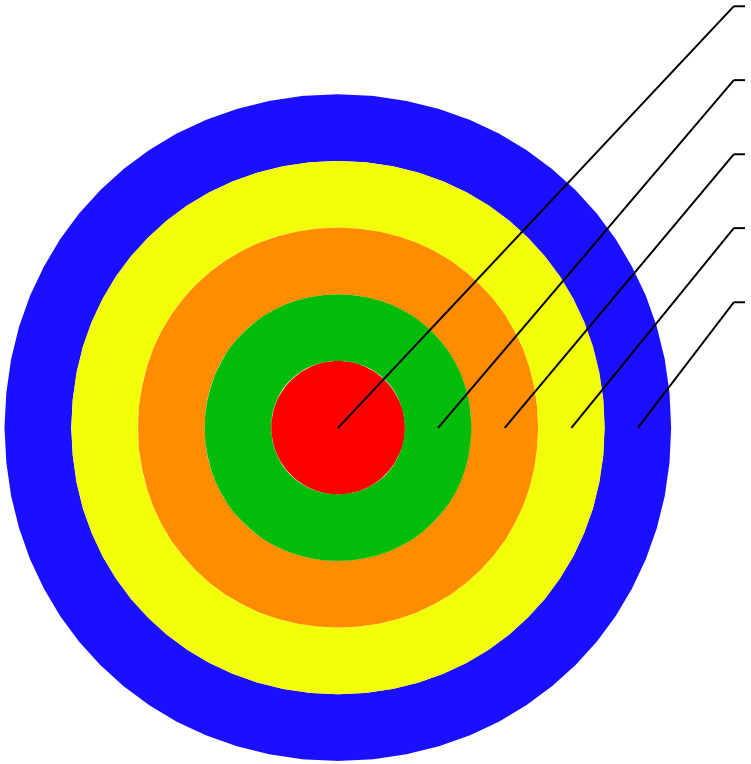


Protokół PPTP

Sesja PPTP składa się z dwóch połączeń:

- połączenia kontrolnego
  - port 1723/TCP, służy do nawiązywania sesji oraz jej kończenia
- połączenia tunelowego
  - wykorzystuje protokoły GRE i PPP do enkapsulowania pakietów danych użytkownika

Enkapsulacja



Ethernet

Pakiet IP z danymi

PPP (szyfrowanie)

GRE

IP

Ochrona przed zagrożeniami

- Podsłuch jest niewykonalny bez znajomości klucza szyfrującego.
- Nie jest możliwe podszycie się pod użytkownika bez znajomości jego hasła.
- Ataki MitM nie są możliwe do przeprowadzenia przy prawidłowej konfiguracji klienta i serwera (wymuszanie szyfrowanej autoryzacji i szyfrowania transmisji).
- PPTP wykorzystuje do transmisji właściwej protokół GRE, którego nie da się zresetować. Protokół TCP jest używany tylko na początku i końcu połączenia VPN.