Bezpieczeństwo systemów komputerowych

Tunele wirtualne, kryptograficzne zabezpieczanie komunikacji

Marcin Peczarski

Instytut Informatyki Uniwersytetu Warszawskiego

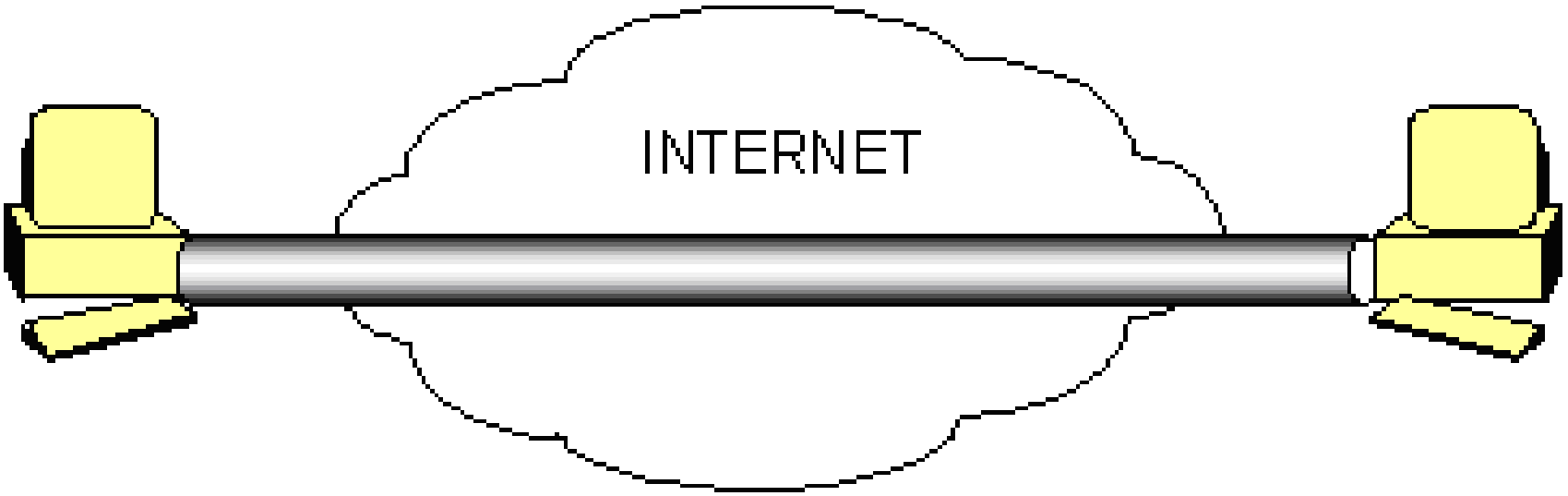
5 grudnia 2011

Na podstawie materiałów Michała Szychowiaka
z *http://wazniak.mimuw.edu.pl*

VPN – tunele wirtualne

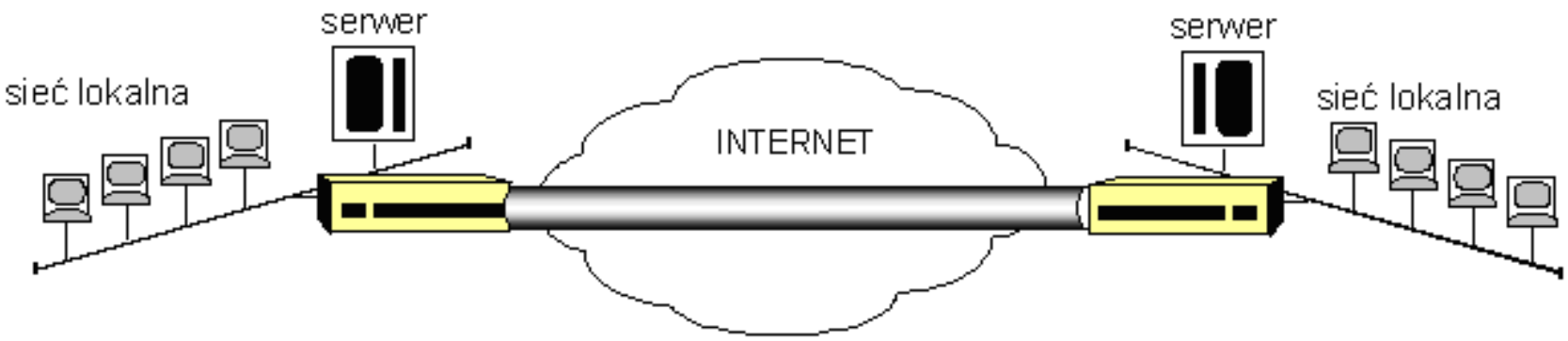
- VPN (ang. *Virtual Private Network*) polega na tworzeniu tuneli komunikacyjnych w istniejącej sieci w celu stworzenia sieci wirtualnej.
- Tunel jest przeźroczysty dla komunikujących się węzłów.
- VPN pozwala utworzyć sieć prywatną za pomocą sieci publicznej (np. Internetu), łączącą różne siedziby firmy lub organizacji, często odległe geograficznie.
- W sieci publicznej należy się liczyć z potencjalnymi naruszeniami poufności, integralności i autentyczności transmitowanych danych.
- W celu realizacji bezpiecznego połączenia tunel chroni się za pomocą kryptografii.
- Dane przesyłane tunelem mogą też być kompresowane.

Tunel komputer-komputer



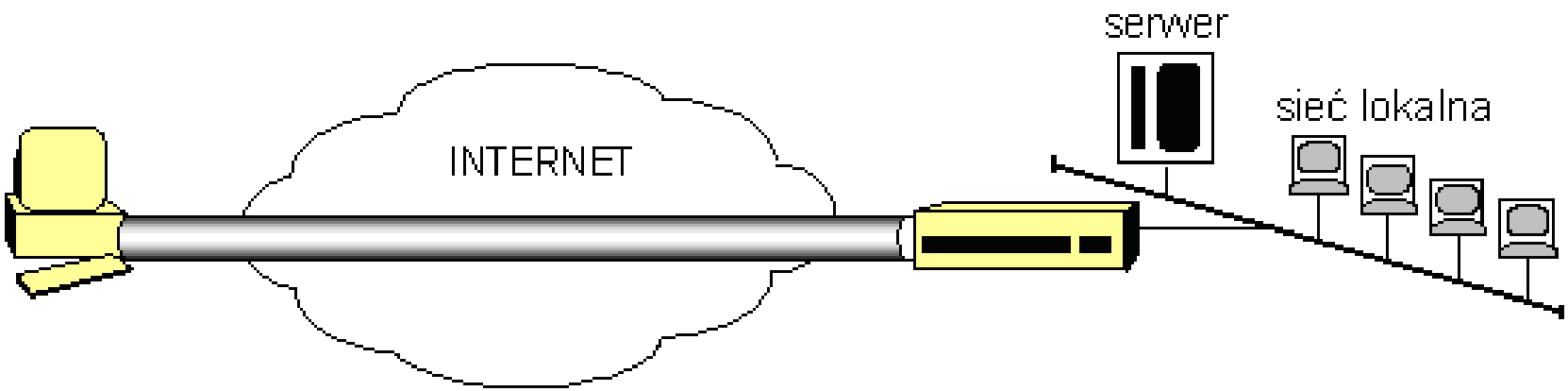
- Po angielsku *host-to-host*
- Końcami tunelu są pojedyncze stanowiska, wyposażone w odpowiednie oprogramowanie lub sprzęt do szyfrowania transmisji pomiędzy nimi.

Tunel sieć-sieć



- Po angielsku *net-to-net*
- Końcami tunelu są pojedyncze węzły międzysieciowe, np. dedykowane urządzenia szyfrujące, rutery brzegowe z modułami kryptograficznymi.
- Szyfrowana może być cała transmisja wychodzącą z sieci lokalnych lub tylko wybrane usługi.
- Transmisja odbywająca się wewnątrz poszczególnych sieci nie jest szyfrowana.

Tunel komputer-sieć



- Po angielsku *host-to-net*
- Jednym z końców tunelu jest pojedyncze stanowisko, które uzyskuje dostęp do zasobów pewnej sieci lokalnej, np. korporacyjnej.
- Cała komunikacja lub wybrany ruch (wybrane usługi) poddawane są szyfrowaniu.
- Jest to model typowy dla środowisk pracy zdalnej.

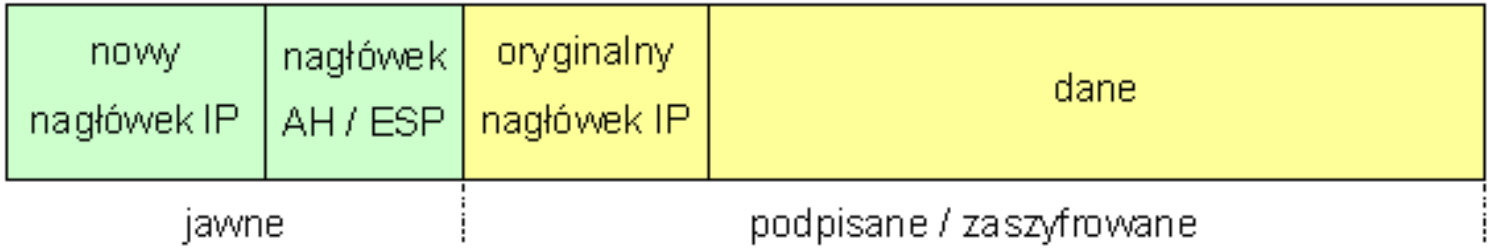
IPsec

- Oferuje:
  - uniwersalny tunel wirtualny w warstwie sieciowej.
  - wzajemne uwierzytelnianie,
  - szyfrowanie datagramów IP.
- Jest wymaganą częścią IPv6.
- Tryby pracy:
  - transportowy,
  - tunelowy.

Tryb transportowy

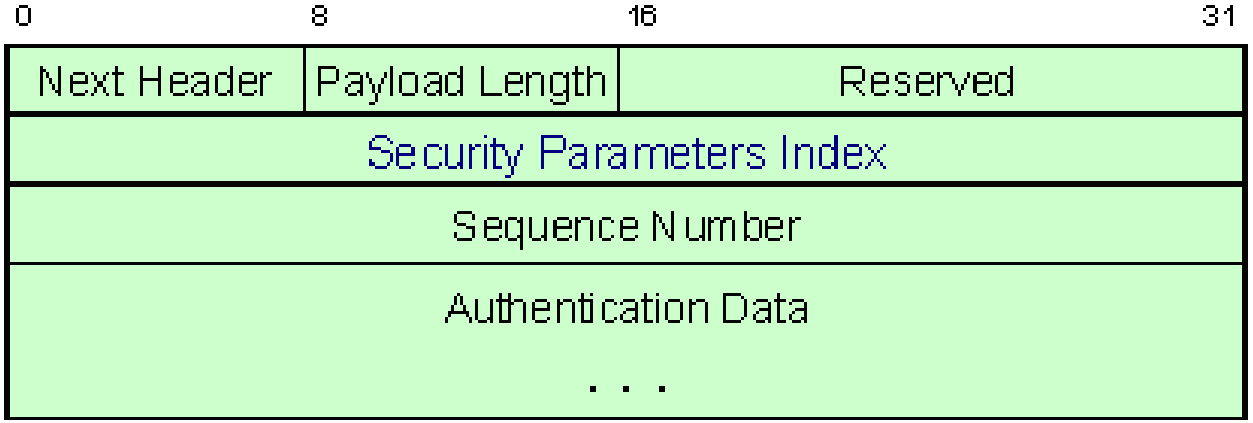
- Po angielsku *transport mode*
- Pole danych, niosące ramkę protokołu wyższej warstwy, np. TCP, UDP, ICMP itd., może zostać podpisane – do datagramu dodawany jest nagłówek AH (ang. *Authentication Header*).
- Pole danych może też zostać zaszyfrowane – do datagramu dodawany jest nagłówek ESP (ang. *Encapsulating Security Payload*).

Tryb tunelowy



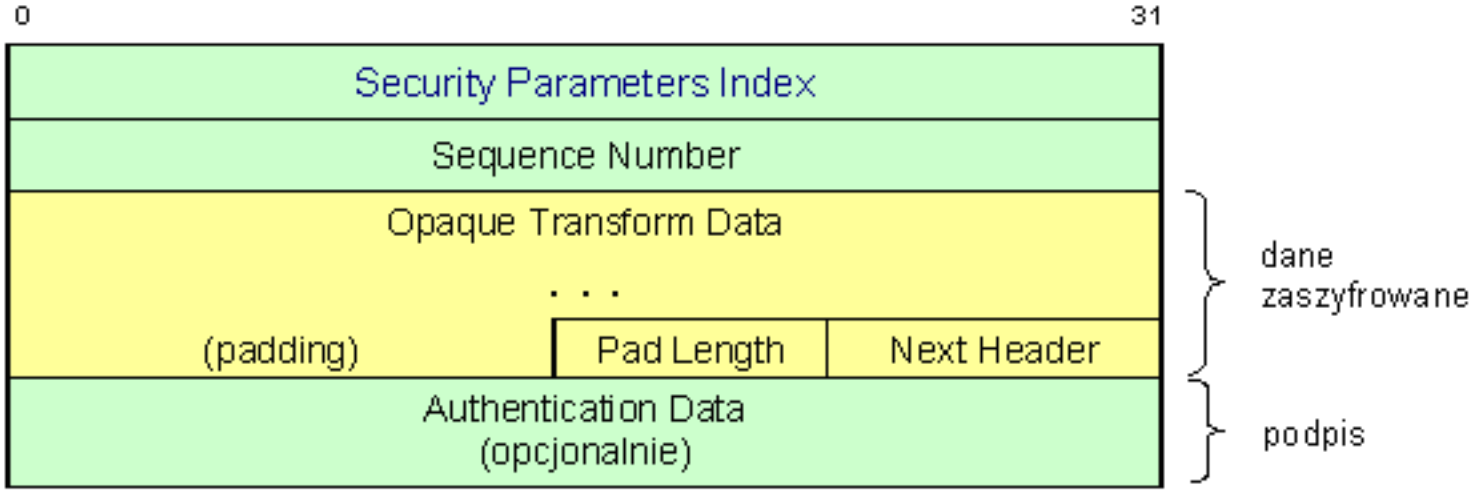
- Po angielsku *tunnel mode*
- Cały oryginalny datagram IP, łącznie z nagłówkiem, jest podpisywany lub szyfrowany.
- Do datagramu dodawane są odpowiednie nagłówki: AH, ESP, nowy nagłówek IP.

Authentication Header (AH)



- Zapewnia integralność zawartości datagramu i uwierzytelnianie źródła pochodzenia datagramu.
- Działa na wierzchu IP, używając numeru protokołu 51.
- Sequence Number – monotonicznie zwiększana wartość, chroniąca przed atakiem powtórzeniowym.
- Authentication Data – zawiera podpisany skrót zawartości.
- Fukcja skrótu, oprócz pola danych, obejmuje też stałe pola nagłówka (zarówno w trybie transportowym, jak i tunelowym).
- Ewentualna fragmentacja datagramu musi być wykonana wcześniej (podpisywany jest każdy fragment oddzielnie).

Encapsulating Security Payload (ESP)



- Zapewnia integralność i poufność zawartości datagramu oraz uwierzytelnianie źródła pochodzenia datagramu.
- Działa na wierzchu IP, używając numeru protokołu 50.
- Można używać tylko samego
  - szyfrowania (ang. *encryption-only*) – niezalecane,
  - uwierzytelniania (ang. *authentication-only*).
- Nie chroni zawartości nagłówka IP (choć w trybie tunelowym chroni nagłówek oryginalnego datagramu).
- Payload Data, Pad Length – wypełnienie dla szyfrów blokowych.

AH i ESP

- Możliwe jest połączenie mechanizmów AH i ESP.
- Przykładowo, najpierw szyfrowane są dane za pomocą ESP, a następnie cały datagram jest podpisywany za pomocą AH.
- Alternatywnie, najpierw wyznacza się nagłówek AH i umieszcza się go w datagramie, a następnie szyfruje w całości z użyciem ESP (tuneluje).

Security Parameters Index

- Identyfikuje parametry bezpieczeństwa.
- W połączeniu z adresem IP identyfikuje asocjację bezpieczeństwa SA (ang. *Security Association*) używaną dla danego datagramu.
- SA tworzy pewnego rodzaju kanał wirtualny.

Asocjacja bezpieczeństwa

- Zbiór parametrów charakteryzujących bezpieczną komunikację między nadawcą a odbiorcą (kontekst):
  - algorytm AH,
  - klucze AH,
  - algorytm szyfrowania ESP,
  - klucze szyfrowania ESP,
  - dane inicjujące algorytm szyfrowania,
  - algorytm uwierzytelniania ESP,
  - klucze algorytmu uwierzytelniania ESP,
  - czas ważności kluczy,
  - czas ważności asocjacji,
  - adresy IP mogące współdzielić asocjację,
  - etykieta poziomu bezpieczeństwa: poufne, tajne, ściśle tajne, ...
- Parametry asocjacji bezpieczeństwa nie są przesyłana przez sieć – przesyłany jest tylko numer SPI.
- Asocjacja bezpieczeństwa jest jednokierunkowa – w każdym kierunku może być używany inny zestaw parametrów.

Schemat działania stacji IPsec wysyłającej

- Sprawdź, czy i w jaki sposób wychodzący pakiet ma być zabezpieczony:
  - sprawdź politykę bezpieczeństwa w SPD (ang. *Security Policy Database*);
  - jeśli polityka bezpieczeństwa każe odrzucić pakiet, odrzuć pakiet;
  - jeśli pakiet nie musi być zabezpieczany, wyślij pakiet.
- Ustal SA, które powinno być zastosowane do pakietu:
  - odszukaj SA w bazie SAD (ang. *SA Database*) lub
  - jeśli nie ma jeszcze odpowiedniego SA, uzyskaj odpowiednie SA.
- Zabezpiecz pakiet, wykorzystując algorytmy, parametry i klucze zawarte w SA:
  - stwórz nagłówek AH, ESP;
  - jeśli tryb tunelowy, stwórz nowy nagłówek IP;
- Wyślij pakiet.

Schemat działania stacji IPsec odbierającej

- Sprawdź nagłówki:
  - odszukaj SA w SAD na podstawie SPI zawartego w nagłówku;
  - jeśli SA wskazywany przez SPI nie istnieje, odrzuć pakiet;
  - postępuj zgodnie z informacjami zawartymi w SA.
- Sprawdź, czy i jak pakiet powinien być zabezpieczony:
  - sprawdź politykę bezpieczeństwa w SPD;
  - jeśli polityka bezpieczeństwa każe odrzucić pakiet, odrzuć pakiet;
  - jeśli zabezpieczenia pakietu nie odpowiadają polityce bezpieczeństwa, odrzuć pakiet;
  - jeśli pakiet był zabezpieczony prawidłowo, przekaż go do warstwy wyższej.

Zarządzanie kluczami IPsec

- IPsec nie definiuje sposobów zarządzania i dystrybucji kluczy.
- Klucze mogą być przypisane do:
  - użytkownika,
  - komputera.
- Sposoby dystrybucji kluczy:
  - wyznaczenie wszystkich kluczy przez administratora (małej sieci lokalnej);
  - wykorzystanie istniejących systemów dystrybucji, np. Kerberosa;
  - specjalizowane protokoły dla serwerów kluczy (niezależne od IPsec), np. SKIP (Sun), Photuris, IKE (Internet Key Exchange);
  - integracja serwerów kluczy z usługami katalogowymi, np. DNSsec, LDAP.

Protokoły zarządzania kluczami IPsec

- Służą do
  - wzajemnego uwierzytelniania podmiotów nawiązujących asocjację IPsec;
  - uzgadniania kluczy na potrzeby kanałów SA.
- Obie te funkcje realizowane są na podstawie skonfigurowanych na stałe danych uwierzytelniających:
  - hasło wspólne dla pary stacji (ang. *shared secret*),
  - certyfikaty X.509,
  - klucze PGP.
- Niektóre implementacje (SKIP, Photuris) umożliwiają wyłącznie uwierzytelnienie na podstawie haseł.
- Popularny protokół IKE obsługuje natomiast wszystkie wyżej wymienione metody i umożliwia jeszcze prywatne rozszerzenia.

Protokół IKE (Internet Key Exchange)

- Obejmuje dwa składniki:
  - ISAKMP (Internet Security Association and Key Management Protocol) – faktyczny protokół negocjacji parametrów IPSec;
  - Oakley – kryptograficzny protokół wymiany kluczy za pomocą schematu Diffiego–Hellmana.
- ISAKMP stanowi trzon całości i z tego powodu nazwy tej używa się niekiedy zamiennie z IKE.
- Protokół ISAKMP korzysta z UDP (port 500).
- Wymiana kluczy następuje dwuetapowo:
  - ustalenie tożsamości komunikujących się węzłów i utworzenie bezpiecznego kanału (tzw. ISAKMP SA), utrzymywanego przez cały czas trwania sesji;
  - właściwa negocjacja parametrów asocjacji.
- Negocjacja obejmuje m.in. listę obsługiwanych algorytmów szyfrujących, co ułatwia obsługę środowisk heterogenicznych.

Protokół IKE, cd.

- Uwierzytelnianie może być realizowane na dwa sposoby:
  - każda para węzłów ma ustalone wspólne hasło, które służy do obliczania kluczy metodą Diffiego–Hellmana; oznacza to konieczność konfigurowania haseł na wszystkich węzłach, co jest istotnym ograniczeniem i może okazać się zbyt pracochłonne w przypadku dużych sieci;
  - zastosowanie kluczy publicznych podpisanych przez nadrzędny urząd certyfikujący CA (np. certyfikatów X.509); wolne od ograniczeń ręcznej definicji haseł.
- Protokół ISAKMP jest łatwo rozszerzalny, można zdefiniować
  - własny zestaw szyfrów,
  - własne mechanizmy uwierzytelnienia.

IKE i PKI (Public Key Infrastructure)

- Protokół IKE pozwala wykorzystać możliwości PKI.
- Po nawiązaniu komunikacji, ale przed uzgodnieniem ISAKMP SA, węzeł może zweryfikować autentyczność certyfikatu drugiej strony dzięki podpisowi CA.
- W skrajnym przypadku węzeł nie musi nic wiedzieć o innych węzłach, z którymi będzie się łączył, lub które będą się łączyć z nim.
- Wymaga to jedynie lokalnego dostępu (zainstalowania w tym węźle) klucza publicznego urzędu CA – będzie to jeden i ten sam klucz na wszystkich węzłach.
- Znacznie ułatwia to realizację złożonych topologii.

IKE

- Umożliwia automatyczną renegocjację kluczy kryptograficznych co określony interwał czasu.
- W przypadku złamania bieżącego klucza dane zaszyfrowane poprzednimi kluczami nie są narażone.
- Cecha ta, określana jako Perfect Forward Security, chroni przed sytuacją, gdy atakujący zapisuje wszystkie przechwycone w przeszłości dane w nadziei, że kiedyś uda mu się zdobyć klucz do ich rozszyfrowania.
- Implementacja jest obligowana, aby w przypadku renegocjacji klucza poprzedni klucz został usunięty z pamięci.
- Wówczas włamywacz nie znajdzie go nawet w przypadku opanowania systemu operacyjnego węzła.

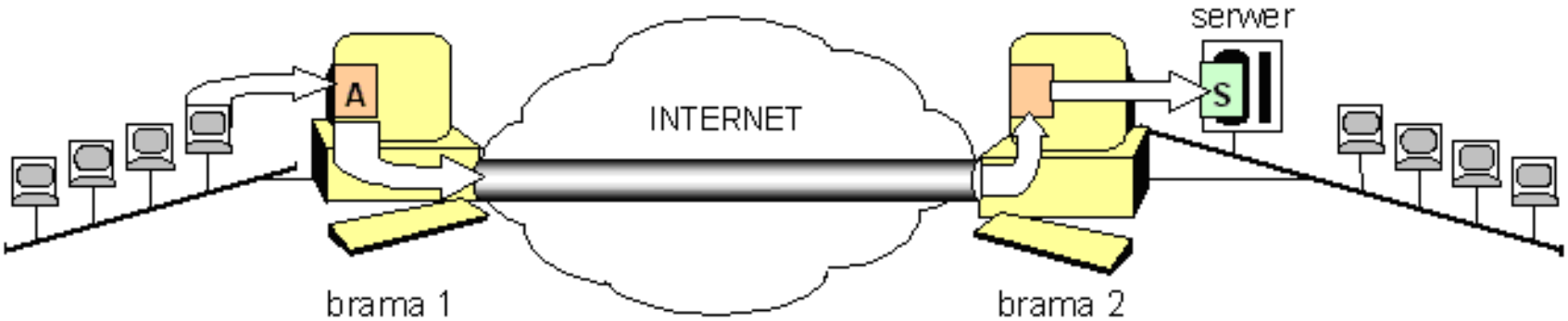
PPTP i MPPE

- PPTP – Point to Point Tunneling Protocol
  - standardowo dostępny w systemach Windows
  - dostępne też implementacje dla systemów uniksowych
  - RFC 2637
- MPPE – Microsoft Point-to-Point Encryption
  - szyfrowanie danych przesyłanych za pomocą PPTP
  - RFC 3078, RFC 3079

L2TP

- Layer Two Tunneling Protocol
- Przeznaczony do tworzenia prywatnych sieci wirtualnych w warstwie łącza (warstwa druga) modelu OSI.
- Umożliwia kapsułkowanie w sieci IP protokołów PPP, Frame Relay, Ethernet, ATM, ...
- W rzeczywistości protokół warstwy sesji (warstwa piąta).
- Jako warstwy transportowej (warstwa czwarta) używa UDP.
- Nie szyfruje i nie uwierzytelnia przesyłanych danych – bazuje na bezpiecznej komunikacji w warstwie sieciowej (warstwa trzecia), np. IPsec.
- Wersja 3 (L2TPv3) jest opisana w RFC 3931.

Tunel SSH (ang. *port forwarding*)

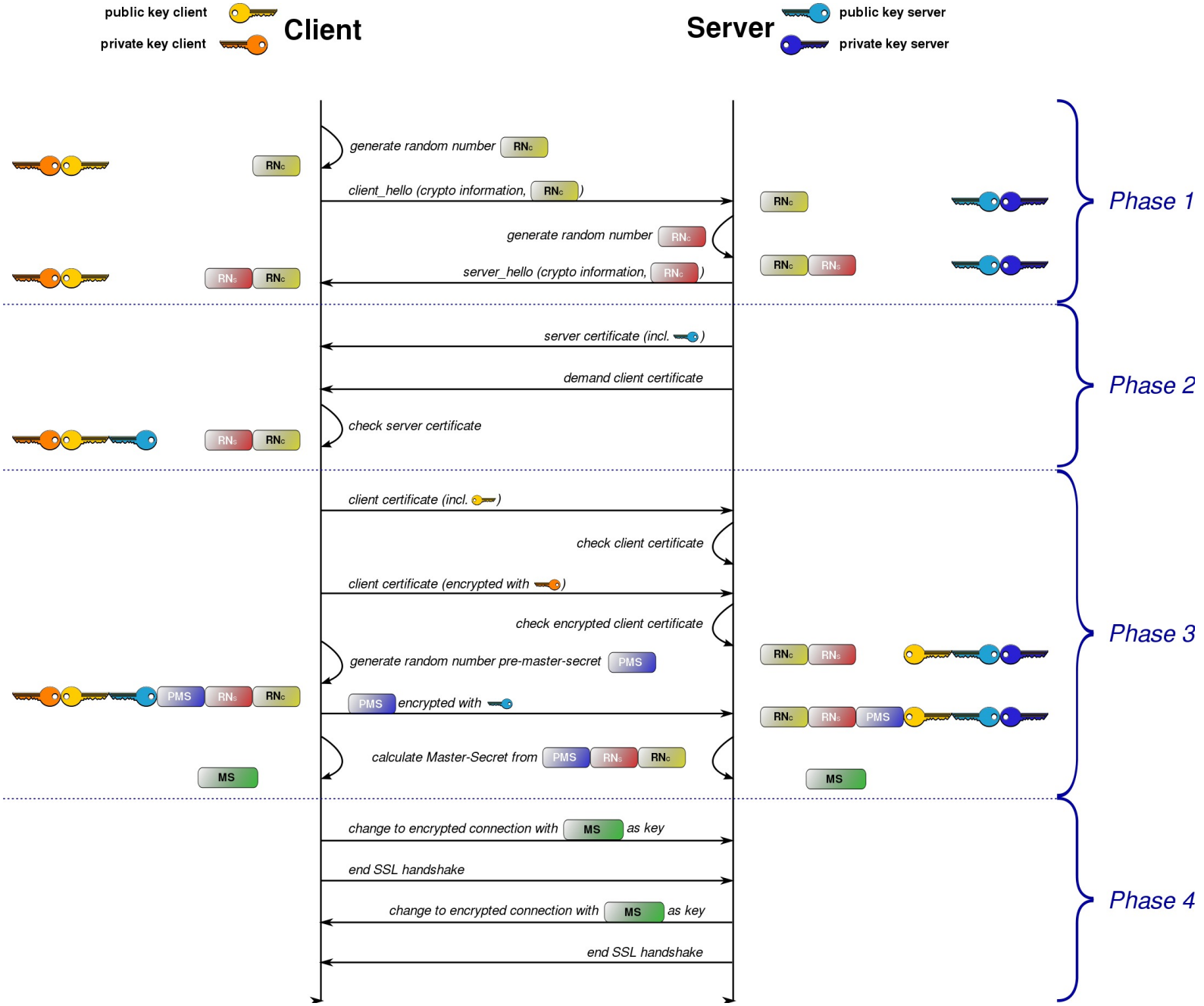


- SSH oferuje możliwość realizacji tuneli wirtualnych w warstwie transportowej.
- Działanie mechanizmu propagowania połączeń:
  - połączenia na port A bramy 1 są tunelowane do bramy 2
  - i dalej propagowane na port S serwera w sieci lokalnej za bramą 2;
  - tunel między bramą 1 a bramą 2 jest szyfrowany;
  - komunikacja poza tunelem (w obu sieciach lokalnych, czyli od klienta do bramy 1 oraz od bramy 2 do serwera) nie jest szyfrowana.

Tunele SSL

- SSL (Secure Socket Layer):
  - działa w warswie aplikacji modelu internetowego – warstwy sesji (5) i prezentacji (6) modelu ISO/OSI,
  - protokół połączeniowy,
  - dwupunktowy tunel kryptograficzny z certyfikatami,
  - ochrona poufności, integralności i autentyczności,
  - zaprojektowany z myślą o ochronie protokołów aplikacyjnych.
- Wersje popularnych protokołów korzystające z tunelu SSL:
  - HTTPS port 443,
  - SMTPS port 465,
  - TELNETS port 992,
  - IMAPS port 993,
  - IRCS port 994,
  - POP3S port 995.
- SSL potrafi tunelować dowolny ruch (stunnel, OpenVPN).
- Następcą SSL w wersji 3.0 został protokół TLS (Transport Layer Security) w wersji 1.0, aktualna wersja TLS to 1.2.

Negocjacja połączenia SSL



Protokół SSL

- Faza 1.
  - Klient wysyła do serwera komunikat client_hello (wersja protokołu, identyfikator sesji, lista obsługiwanych szyfrów i metod kompresji, losowe dane).
  - Serwer odsyła komunikat server_hello (wersja protokołu, identyfikator sesji, wybrany szyfr i metoda kompresji, losowe dane).
- Faza 2.
  - Serwer wysyła swój certyfikat X.509.
  - Serwer opcjonalnie żąda certyfikatu klienta (wraz z losowym zawołaniem).
  - Klient uwierzytelnia serwer na podstawie odebranego certyfikatu i w razie niepowodzenia przerywa połączenie.

Protokół SSL, cd.

- Faza 3.
  - Jeśli serwer żądał uwierzytelnienia klienta, to klient wysyła też swój certyfikat oraz podpisane zawołanie odebrane wcześniej od serwera.
  - Po pomyślnym uwierzytelnieniu klient tworzy pierwotny sekret główny PMS (ang. *premaster secret*), który szyfruje kluczem publicznym serwera i wysyła do serwera.
  - Po ewentualnym uwierzytelnieniu klienta serwer deszyfruje pierwotny sekret główny i na jego podstawie uzyskuje sekret główny MS (ang. *master secret*).
  - Klient oblicza sekret główny.
- Faza 4.
  - Z wygenerowanego sekretu głównego obie strony tworzą (zależny od ustalonego algorytmu szyfrującego) klucze szyfrowania i podpisywania.
  - Klient i serwer wysyłają do siebie nawzajem zaszyfrowany kluczem sesji komunikat o zakończeniu fazy uzgadniania.
  - Protokół uzgadniania kończy się i (o ile wzajemna weryfikacja przebiegła pomyślnie) rozpoczyna się sesja SSL.

Protokół SSL, poprawność

- Jeśli serwer nie posiadałby klucza prywatnego odpowiadającego kluczowi publicznemu ze swojego certyfikatu:
  - nie rozszyfruje poprawnie sekretu i nie wygeneruje tego samego klucza sesji co klient,
  - połączenie zastanie przerwane.
- Jeśli klient nie posiadałby klucza prywatnego odpowiadającego kluczowi publicznemu ze swojego certyfikatu:
  - serwer pobierze jego klucz publiczny z certyfikatu i rozszyfruje zapytanie podpisane kluczem prywatnym klienta,
  - nie otrzyma zawołania, które wysłał,
  - zatem klient nie jest tym, czyją autentyczność poświadcza certyfikat.
- Newralgiczna w tym procesie jest weryfikacja certyfikatów.

OpenVPN

- Program uożliwiający tworzenie wirtualnych sieci prywatnych
- Oparty na SSL/TLS i bibliotece OpenSSL
- Dostępny dla systemów uniksowych i Windows

DTLS

- Datagram Transport Layer Security
- Jest przeznaczony dla protokołów pakietowych.
- Ma zapewnić podobne usługi, co TLS dla protokołów strumieniowych: poufność, integralność i autentyczność przesyłanych danych.
- RFC 4347