Kryptografia w Internecie

SSL, PGP, SSH
VPN, bezpieczeństwo DNS

Bezpieczne usługi sieciowe

- Cechy wspólne:
  - Algorytm hybrydowy
  - Kompresja danych

SSL - Security Socket Layer
TLS – Transport Layer Security

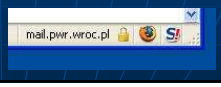
- Protokół służący do szyfrowania sesji z serwerami
- Pozwala na zestawianie szyfrowanych połączeń internetowych wykorzystujących takie protokoły jak: http (strony WWW), ftp, smtp, telnet

SSL/TLS

- Połączenie się ze stroną WWW poprzez SSL jest oznaczane w przeglądarkach następująco:

  https://

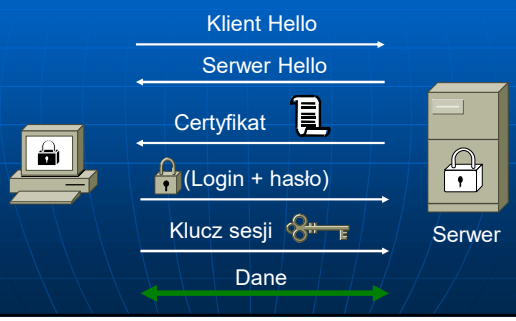
- Bezpieczna wymiana informacji z serwerem jest oznaczana kłódeczką



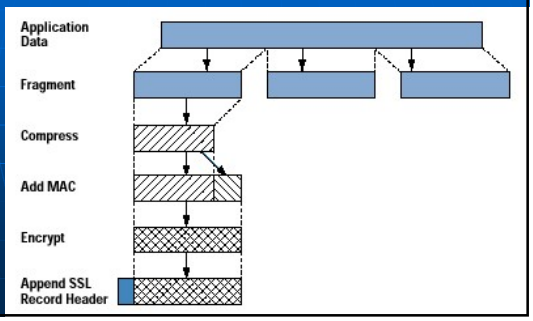
Moc szyfrowania SSL

- Klucze asymetryczne:
  1024 - stosunkowo bezpieczne,
  2048 - zalecane,
  4096 - silne bezpieczeństwo.
- Klucze symetryczne:
  40, 56, 64 - zbyt mało,
  128 - bezpieczne, zalecane
  256 - silne bezpieczeństwo.

Działanie SSL

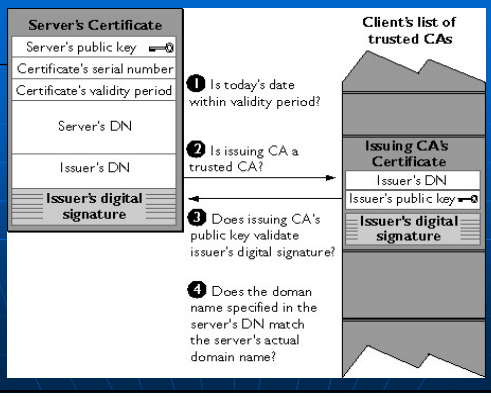


Transmisja SSL



Certyfikat SSL

- Klucz publiczny serwera
- Numer seryjny certyfikatu
- Okres ważności certyfikatu
- Nazwę domenową serwera (pwr.edu.pl)
- Nazwę domenową wystawcy certyfikatu
- Podpis wystawcy



Ważność certyfikatu

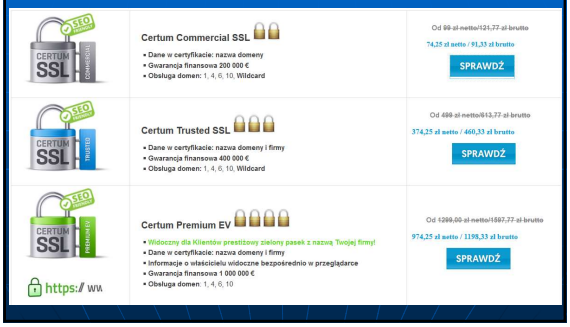
Ważność certyfikatu wygasa:

- W momencie upływu jego terminu ważności.
- Gdy certyfikat zostanie unieważniony przed datą wygaśnięcia ważności.
  - listy unieważnień (*certificate revocation lists*), przechowywane na serwerach wszystkich CA.

Certyfikaty zaufanych CA

- Są dołączone do większości przeglądarek internetowych
- Ze względu na wygasanie i unieważnienia certyfikatów należy pamiętać o aktualizacji przeglądarki
- Jak to wygląda w praktyce ?

Jak uzyskać certyfikat SSL



Historia SSL

- Security Socket Layer
  - SSL 1.0 (1993)
  - SSL 2.0
  - SSL 3.0
- Transport Layer Security
  - TLS 1.0 (SSL 3.1)
  - TLS 1.1
  - TLS 1.2 (sierpień 2008)

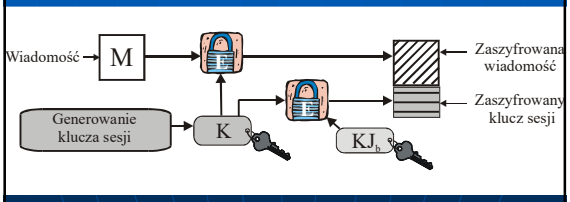
PGP – *Pretty Good Privacy*

- Pierwsza wersja PGP powstała w 1991
- PGP zapewnia poufność, integralność i uwierzytelnienie w poczcie elektronicznej oraz przy przechowywaniu plików
- Algorytmy: konwencjonalny (IDEA), asymetrycznych (RSA) i haszowania (MD5)

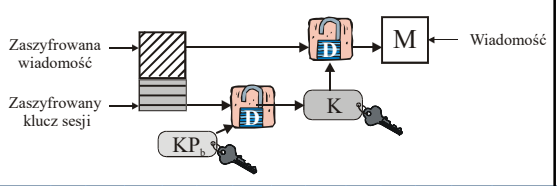
PGP

- Wersje dla systemów: DOS/Windows, UNIX, Macintosh, Linux
- Możliwość zintegrowania PGP z większością programów pocztowych
- Darmowe wersje - OpenPGP
- Nie jest kontrolowany przez żadną instytucję rządową ani standaryzacyjną, co utrudnia służbom wywiadowczym kontrolę poczty elektronicznej

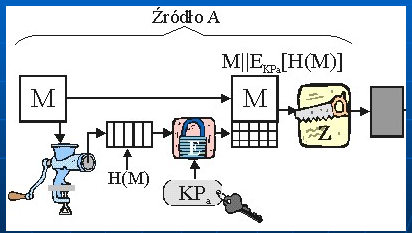
PGP – przygotowanie wiadomości



PGP – odbieranie wiadomości

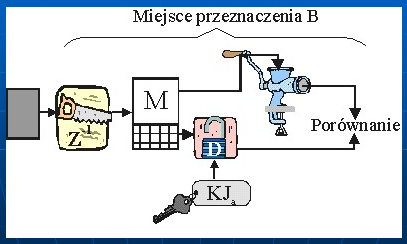


PGP – podpisywanie



(skrót MD5 – 128 bitów)

PGP – weryfikacja podpisu



Uwierzytelnianie w PGP

Sygnatury mogą być:

- dołączane do sygnowanego komunikatu
- przesyłane oddzielnie (np. gdy prowadzi się dziennik sygnatur, w celu wykrywania wirusów, gdy dokument sygnowany jest przez więcej niż jedną osobę.

PGP - baza kluczy prywatnych

- Indeksowana przez ID użytkownika lub ID klucza.
- Klucz prywatny zaszyfrowany za pomocą wartości H(P_i) - hasła użytkownika (P_i) przekształconego operacją hashowania.
- Każdy dostęp do klucza prywatnego wymaga podania hasła. Dlatego bezpieczeństwo całego systemu PGP zależy od bezpieczeństwa hasła.

PGP - baza kluczy prywatnych

Datownik	ID Klucza	Klucz jawny	Zaszyfrowany klucz prywatny	ID użytkownika
.	.	.	.	.
T_i	$KJ_i \bmod 2^{64}$	KJ_i	$E_{H(P_i)}[KP_i]$	Użyt i
.	.	.	.	.

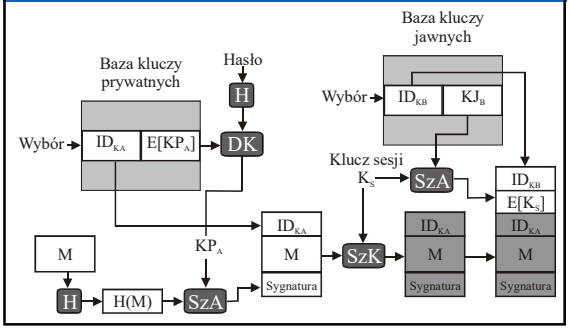
PGP – baza kluczy jawnych

- Każda pozycja w bazie kluczy jawnych to certyfikat klucza jawnego.
- Pole zaufania sygnatury wskazuje stopień zaufania użytkownika do osoby/firmy sygnującej certyfikat.

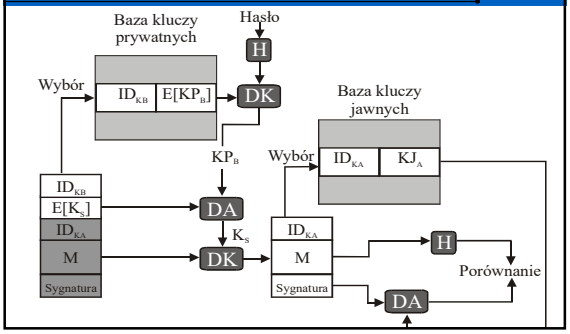
PGP – baza kluczy jawnych

Datownik	ID Klucza	Klucz jawny	Zaufanie do właściciela	ID użytko-wnika	Legalność klucza	Sygna tura	Zaufanie do sygnatury
.	.	.	.	.	.	.	.
T_i	$KJ_i \bmod 2^{64}$	KJ_i	$flaga_i$ zaufania	Użyt i	$flaga_i$ zaufania		
.	.	.	.	.	.	.	.

Generowanie komunikatu PGP



Odbiór komunikatu PGP



Dystrybucja kluczy jawnych

- Jedną z przyczyn powstania PGP było ograniczenie możliwości naruszania prywatności korespondencji przez agencje rządowe.
- Dlatego nie istnieją centralne ośrodki certyfikacji, nad którymi ktoś mógłby przejąć kontrolę.
- Użytkownicy sieci uwierzytelniają nawzajem swoje klucze jawne

Zarządzanie kluczami jawnymi w PGP

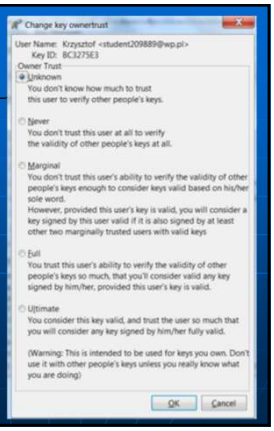
- Poświadczenia oryginalności kluczy dokonywane nie przez zaufanego wystawcę certyfikatów, lecz przez użytkowników tworzących rozproszoną sieć zaufania (*Web of Trust*).
- W bazie kluczy jawnych w polu zaufania wpisywane jest zaufanie użytkownika do właściciela danego klucza. Można ufać całkowicie (w pełni) lub częściowo.

Web of Trust – PGP i OpenPGP

- Każdy użytkownik weryfikuje (podpisuje) klucze użytkowników, do których ma zaufanie
- Po wygenerowaniu swojego klucza użytkownik przekazuje go do podpisania swoim ‘znajomym’
- Klucz jest wysyłany innym razem z podpisami
- Istnieją serwery kluczy

Web of Trust

Czy możesz uwiarygodnić czyjś klucz dzięki podpisowi użytkownika X ?



SSH

Secure Shell

SSH (*Secure Shell*)

- Zapewnia mechanizm szyfrowania danych w warstwie transportowej
- Program został napisany przez Tatu Ylonena z Uniwersytetu w Helsinkach
- Połączenie jest realizowane po stronie klienta przez program *ssh*, a po stronie serwera przez demona *sshd*

Algorytmy SSH

- Szyfrowanie wiadomości:
  AES (SSH2)
  DES, 3DES – tryb CBC
  IDEA - CFB
  Blowfish-CBC
  RC4
- Asymetryczne uwierzytelnianie: RSA

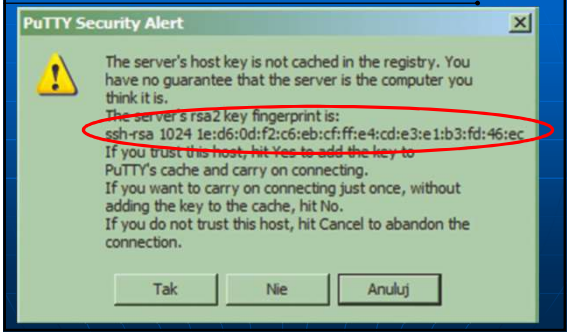
Zasada działania SSH

- Każdy z komputerów posiada parę kluczy, tzw. *Public Host Key*
- Podczas uruchamiania demona *sshd* generowana jest dodatkowa para kluczy serwera. Klucz publiczny nazywa się *Server Key*. Klucze są zmieniane co godzinę.

Zasada działania SSH

- Kiedy użytkownik A chce się zalogować na serwer B, to B przesyła do A dwa klucze publiczne *Server Key* i *Public Host Key*. A sprawdza czy *Public Host Key* jest poprawny (zgadza się z kluczem zapisanym w pliku lokalnym)

Pierwsze logowanie - *Putty*



Uwierzytelnienie w SSH

- Protokół Kerberos.
- Rhosts - uwierzytelnienie komputera.
- RhostsRSA - uwierzytelnienie komputera z użyciem RSA.
- Public-Key - uwierzytelnienie na podstawie kluczy asymetrycznych użytkowników.
- User-password - uwierzytelnienie na podstawie hasła przesyłanego w formie zaszyfrowanej.

Zastosowania SSH

- Praca na zdalnym terminalu (np. *Putty*)
- Zdalne wykonywanie poleceń
- Kopiowanie plików (*scp*)

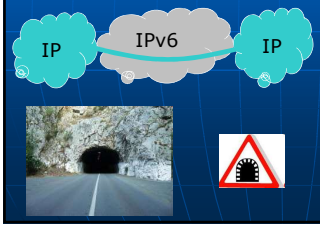
Virtual Private Networks

VPN

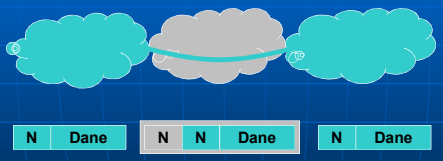
- Dla prywatnych sieci rozległych
- Zamiast tworzenia własnych łączy
- Wirtualne tunele
- Potrzeba zapewnienia bezpieczeństwa
- Rodzaje:
  - Zaufany VPN (trusted VPN)
  - Bezpieczny VPN (secure VPN)
  - Hybrydowy VPN (hybrid VPN)

Tunelowanie

- Tunele budowane są w celu połączenia dwóch podobnych środowisk, rozdzielonych odmiennym środowiskiem



Tunelowanie w sieciach

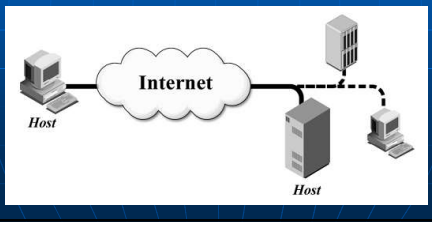


VPN

- VPN to:
  - Tunelowanie
  - Tunelowanie + uwierzytelnianie
  - Tunelowanie + szyfrowanie
  - Tunelowanie + uwierzytelnianie + szyfrowanie
- Kontrola integralności
- Kontrola przepływu

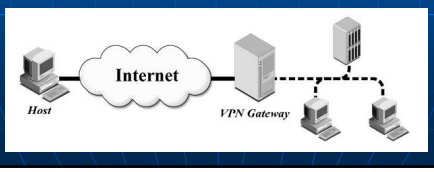
Modele VPN

- VPN typu HOST-HOST
  - Łączenie dwóch urządzeń za pośrednictwem sieci publicznej



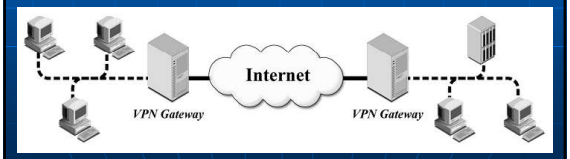
Modele VPN

- VPN zdalnego dostępu
  - Łączenie zdalnych użytkowników z siecią firmową
  - Network Access Servers
  - Weryfikacja, np. login/hasło



Modele VPN

- VPN typu LAN-LAN
  - Łączenie odległych sieci lokalnych
  - Duże natężenia ruchu w sieci VPN

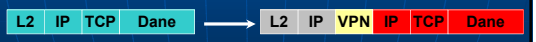


VPN

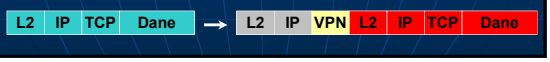
- W warstwie aplikacji

- W warstwie transportowej

- W warstwie sieci



- W warstwie łącza danych



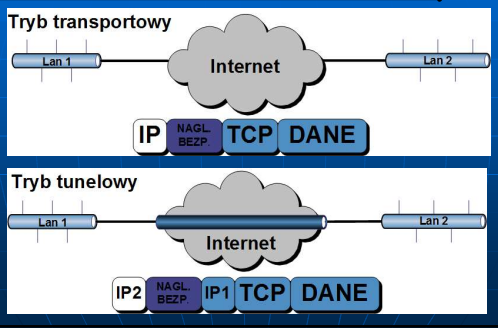
Technologie VPN

- IPSec
- L2TP
- SSL
- PPTP

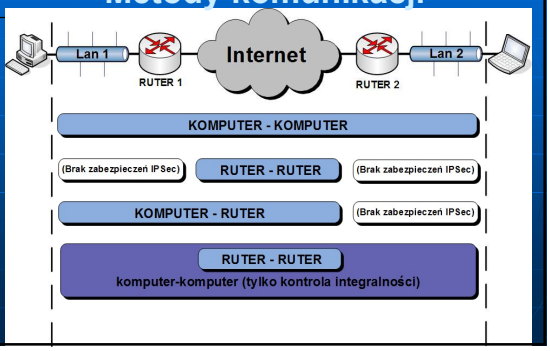
IPSec

- IP Secure, RFC 2401-2412
- Złożony zbiór protokołów zapewniających ochronę transmisji danych w warstwie sieciowej
- Przezroczysty dla aplikacji
- Pierwotnie był częścią składową IPv6
- Konkurencyjny standard CET (Cisco Encryption Technology), obecnie wyparty przez IPSec

Tryby pracy IPSec



Metody komunikacji



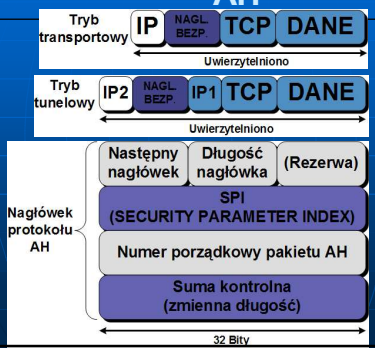
IPSec

- AH (Authentication Header)
  - Zapewnienie integralności pakietu
  - Uwierzytelnienie
  - Ochrona przed atakami powtarzającymi

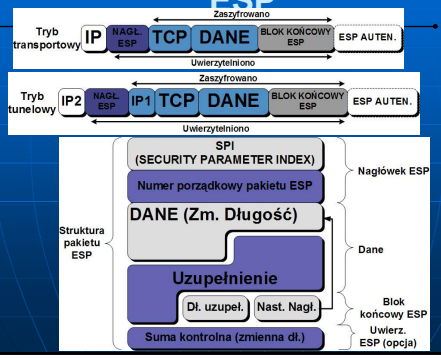
IPSec

- ESP (Encapsulation Security Payload)
  - Szyfrowanie danych
  - Opcjonalnie zadania AH
- ISAKMP (Int. Sec. Associaton-Key Managm. Prot.)
  - Wymiana danych kryptograficznych i konfiguracyjnych zabezpieczających połączenie

AH



ESP



Protokół ISAKMP

- Protokół aplikacyjny służący do wypełniania tablic przechowujących dane kryptograficzne
- Port 500 protokołu UDP
- Specyficzny tryb pracy określany jako żądanie – odpowiedź danych w warstwie sieciowej

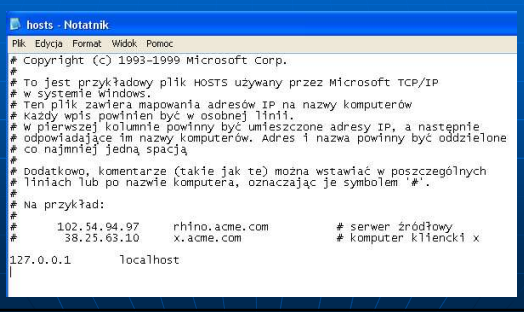
Bezpieczeństwo systemu DNS

Systemy tłumaczenia nazw

- ARPANET – adresy liczbowe (IP)
- Plik *hosts.txt* oraz */etc/hosts*
  - Jeden serwer - NIC w Stanford Research Institute
  - Administratorzy uaktualniali pliki we własnych systemach
  - Problemy: nieefektywność, niedokładność, zależność od administratorów
  - Funkcjonuje nadal

Hosts.txt i lmhosts.sam

- WINDOWS\system32\drivers\etc



Systemy tłumaczenia nazw

- RFC 882 i RFC 883 (1984) – początek DNS
  - Łatwość zapamiętywania i 'odgadywania' nazw domen
  - Można odgadnąć funkcje serwera znając jego adres domenowy, np.:
    dn.xyz.com
    db.xyz.com
    www.xyz.com
    smtp.xyz.com

Zapytania DNS

- Zapytania proste
  - *Load balancing*
- Zapytania odwrotne
  - Wygoda użytkownika
  - Ułatwienia konfiguracji filtrów
  - Domena *in-addr.arpa*

Zapytania DNS

- Zapytania rekurencyjne
  - zadaniem serwera jest udzielenie prawidłowej odpowiedzi
  - pytania użytkownik -> serwer DNS
- Zapytania iteracyjne
  - serwer zwraca adres serwera DNS, który ma udzielić odpowiedzi
  - pytania serwer DNS -> serwer DNS

Odpowiedzi DNS

- Resource record zawierający odpowiedź na nasze zapytanie (Answer RR), np rekord A 193.59.201.40 dla zapytania o adres IP dla domeny *www.xyz.pl*,
- Resource record zawierający informacje o serwerach autorytatywnych (Authority RR),
- Resource record zawierający wszelkie dodatkowe informacje (Additional RR), czasem zwany "glue recordem".

Bezpieczeństwo DNS

- Serwery DNS - małe wymagania, często instalowane na przestarzałym sprzęcie
- Stare wersje systemów operacyjnych – podatność na ataki
- Brak dbałości o bezpieczeństwo kont administratorów DNS

Zagrożenia

- Konsekwencje przejęcia kontroli nad serwerem DNS:
  - Podmiana adresów zaufanych serwerów, przekierowanie klientów do stron konkurencji (poczta, www)
  - Wciągnięcie komputera intruza na listę zaufanych komputerów
  - Bezużyteczność certyfikatów SSL

Zagrożenia

- Przekierowanie usług: podmiana adresów stron informacyjnych, serwerów poczty, banków, składnic oprogramowania, itp.
- DoS:
  - przekierowanie na nieistniejący adres IP
  - zalanie niewielkiego serwera lawiną przekierowanych pakietów

Zagrożenia

- Wyciek informacji
  - Napastnik może uzyskać informacje o funkcjach serwerów i ich adresach:

    dn.xyz.com
    www.xyz.com
    smtp.xyz.com
  - Ciągłe przestrzenie puli adresów publicznych

Zagrożenia

- Podszycie się pod serwer DNS
- Przekazanie fałszywych informacji poprzez Additional Resource Record
- Wymuszenia transferu stref

Transfery stref

- Początkowe wersje serwerów DNS pozwalały na zdobycie pełnej informacji o konfiguracji stref każdemu pytającemu: programy *nslookup*, *dig*
- Wymuszenie częstego transferu stref (rekordy do 64kB) znacznie zwiększa ruch w sieci

Identyfikatory zapytań

- Jeden port dla zapytań DNS
- Identyfikacja zapytania i odpowiedzi na podstawie identyfikatora (*query ID*) – 16-bitowego
- Identyfikatory zwiększane o 1 dla kolejnego zapytania
- Zatruwanie pamięci podręcznej (*cache poisoning*)

DNS *cache poisoning*

1. Napastnik wysyła do serwera zapytanie o wybrany adres
2. Serwer odpytuje serwer niższego poziomu – zapytanie otrzymuje *query ID*
3. Napastnik zasypuje serwer spreparowanymi odpowiedziami, próbując trafić w przyjęty *query ID*
4. Serwer przyjmuje spreparowaną odpowiedź, odrzuca prawidłową, która przychodzi później

DNS spoofing

Podszywanie pod serwer DNS:

1. Użytkownik wysyła zapytanie do serwera DNS
2. Napastnik wysyła zafałszowaną odpowiedź podszywając się pod serwer DNS
3. Użytkownik odrzuca drugą odpowiedź – od prawdziwego serwera – gdyż przychodzi ona później

DNS spoofing

- Łatwo przechwycić ruch do serwera DNS (dobrze znane adresy tych serwerów, port 53)
- Napastnik jest z reguły szybszy od serwera DNS, który musi znaleźć odpowiedź odpytując inne serwery

Bezpieczeństwo transferów stref

- Obecnie transfery stref tylko do wybranych komputerów – najczęściej według adresów IP
- Transaction Signatures (TSIG) – uwierzytelnianie na podstawie sygnatur kryptograficznych

Transaction Signatures (TSIG)

- Stosowany wspólny tajny klucz
- Stosowana funkcja hashująca, np. SHA lub MD5
- Żądanie transferu stref musi być podpisane
- Zalety: większa elastyczność (DHCP)
- Wady: odkrycie tajnego klucza narusza bezpieczeństwo całego systemu

DNSSEC

- DNS Security Extensions – bezpieczna wersja DNS
- Kryptografia klucza publicznego
- Odpowiedzi DNS podpisane przez serwer
- Do transferów stref i do podpisywania odpowiedzi

Projektowanie DNS

- Strefa wewnętrzna i zewnętrzna
- Separacja stref
- Serwer wewnętrzny zapewnia obsługę zapytań rekurencyjnych wyłącznie od użytkowników lokalnych
- Serwer zewnętrzny obsługuje zapytania zewnętrzne i nie obsługuje zapytań rekurencyjnych
- Ochrona przed zatruciem pamięci podręcznej serwera wewnętrznego