Bezpieczeństwo:

Tylko 51 stron o bezpieczeństwie

Bezpieczeństwo

stan który daje poczucie pewności istnienia i gwarancje jego zachowania oraz szansę na doskonalenie. Brak utraty czegoś dla podmiotu szczególnie cennego. Jego brak wywołuje niepokój i poczucie zagrożenia.

Czemu bezpieczeństwo jest istotne?

bo system może zawierać prywatne dane które nie powinny wychodzić na zewnątrz, bo przez wyciek informacji i nieuprawniony dostęp mogą być straty pieniężne. Bezpieczeństwo jest istotne bo systemy komputerowe są praktycznie wszędzie.

Definicja: poufność, integralność, dostępność, identyfikacja, uwierzytelnianie, odpowiedzialność, autoryzacja, safety, security, ryzyko, zagrożenie, haker, cracker:

Poufność - informacje zabezpieczone są przed nieuprawnionym dostępem

Integralność - informacje nie zostały zmienione (dodane lub usunięte) przez nieupoważniony podmiot

Dostępność - autoryzowani użytkownicy mają ciągły dostęp do informacji

Identyfikacja - jesteśmy w stanie zidentyfikować użytkownika

Uwierzytelnianie - po identyfikacji weryfikujemy czy to jest ta osoba

Odpowiedzialność - *? zmiana uprawnień … ?,* obowiązek odpowiadania za coś

Autoryzacja - następstwo identyfikacji i uwierzytelniania

Safety – o systemie mówimy że jest safety gdy mamy pewność, iż nie stwarza on zagrożenia dla podmiotów (m.in. ludzi) znajdujących się poza systemem

Security – system posiada cechę security wówczas, gdy mamy pewność, iż można go ochronić przed zagrożeniami. W szczególności ochrona przed utratą poufności, integralności i dostępności

Ryzyko - prawdopodobieństwo wystąpienia niepożądanego zdarzenia i skutku, który może spowodować straty

Zagrożenie - możliwość niewłaściwego wykorzystania pewnego słabego punktu systemu, możliwe do wykorzystania przez osoby 3cie.

Haker - osoba o bardzo dużych umiejętnościach informatycznych. Celem jej działania nie jest zaszkodzenie innym osobom. Działa wyłącznie w celach poznawczych

Cracker - osoba, której działania są niezgodne z prawem i prowadzą np. do nieautoryzowanego pozyskania informacji lub uniemożliwienia świadczenia pewnych usług.

Wiarygodność systemu:

System jest wiarygodny, gdy jest:

- dyspozycyjny - powinien umożliwić dostęp
- niezawodny - bezawaryjny
- bezpieczny - patrz wyżej

Podział zagrożeń:

- miejsce wystąpienia
    - zewnętrzne - ataki z zewnątrz
    - wewnętrzne - dzieją się z wnętrza naszego systemu (pracownik)
- świadomość
    - celowe pasywne - osoba działa świadomie i świadomie stanowi zagrożenie dla systemu, pasywność oznacza brak ingerencji w system.
    - celowe aktywne - osoba działa świadomie i świadomie stanowi zagrożenie dla systemu, aktywność oznacza ingerencję w system (łamanie zabezpieczeń).
    - przypadkowe - osoba atakująca nie zrobiła tego celowo, to był przypadek
- fizyczne - wszelkie zagrożenia dotyczące infrastruktury fizycznej
    - pożar
    - zakłócenia elektryczne
    - wandalizm, włamanie
    - zalanie
    - duże przegrzanie
- logiczne - niezwiązane z infrastrukturą fizyczną
    - nieuprawnione uzyskanie dostępu do systemu
    - nieuprawnione uzyskanie informacji
    - podmiana danych (zaburzenie integralności)
    - zakłócenie pracy usługi
    - szpiegostwo lub infiltracja

Zasady tworzenia bezpiecznych haseł:

Nie używać:

- własnych identyfikatorów
- imienia
- nazwiska
- danych osobowych(PESEL, data urodzin
- samych liter lub samych cyfr
- haseł krótszych niż 6 znaków

Należy:

- używać małych i dużych liter, znaków alfanumerycznych

- okresowo zmieniać hasło
- hasło powinno dać się szybko wpisać

Etapy tworzenia zabezpieczeń:

1. **Analiza wymagań** - etap początkowy, gdzie zastanawiamy się co mamy chronić, jak mamy to chronić, ustalamy z klientem detale na niskim poziomie bez wygórowanych szczegółów technicznych
2. **Projektowanie** - najważniejszy etap tworzenia zabezpieczeń. Na tym etapie odpowiadamy szczegółowo i technicznie co chronić, jakie są potencjalne zagrożenia, jakie jest ich źródło, i ile czasu możemy poświęcić na ochronę. Błąd popełniony na tym etapie może spowodować poważne problemy w kolejnych etapach.
3. **Wdrożenie**
4. **Zarządzanie**

Co chronić?

identyfikacja zasobów: dane wrażliwe, sprzęt komputerowy, infrastruktura sieciowa. Chronimy nie tylko zasoby cyfrowe ale i fizyczne - komputery, dyski twarde itd.

Definicja: szyfrowanie, kodowanie, kryptologia, szyfrogram, klucz szyfrujący, klucz deszyfrujący:

szyfrowanie - zapis danych w taki sposób żeby tylko uprawnione osoby były w stanie je przeczytać,

kodowanie - ma na celu taki zapis informacji, aby była ona zrozumiała dla jak największej liczby osób. Do konwersji wykorzystywana jest tablica kodów,

kryptologia - dziedzina wiedzy o przekazywaniu informacji tak, aby uchronić ją przed nieuprawnionym dostępem. dzieli się na:

- kryptografię - utajnianie danych
- kryptoanalizę - łamanie szyfrów

szyfrogram (kryptogram) - zaszyfrowana wiadomość

klucz szyfrujący - dane służące do szyfrowania

klucz deszyfrujący - dane służące do deszyfrowania

Klasyczne algorytmy szyfrujące: przestawieniowe, podstawieniowe (monoalfabetyczne, homofoniczne, wieloalfabetowe, poligramowe), mieszane:

Algorytmy klasyczne

używane przed rokiem 1975, algorytm musiał być chroniony, łatwy do złamania, wyjście dla współczesnych metod

Podział:

- przestawieniowy - mieszamy kolejność
- podstawieniowy - podstawiamy inne znaki
- mieszany - to i to

Przestawieniowe

polegają na zamianie kolejności znaków, zamieniają porządek znaków zgodnie z wybraną figurą geometryczną, figura geometryczna oraz sposób zapisu i odczytu stanowią klucz, najprostsza metoda - macierz.

BEZPIECZEŃSTWOSK >

B	E	Z	P
I	E	C	Z
E	Ń	S	T
W	O	S	K

Podstawieniowe

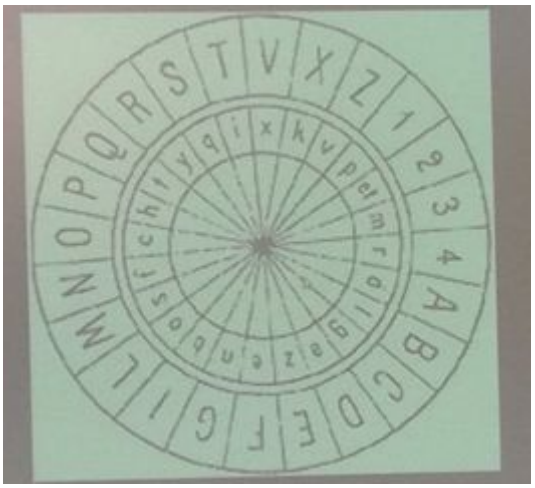
- **monoalfabetyczne** - zamieniają pojedynczy znak tekstu jawnego w znak alfabetu szyfrogramu, np. szyfr Cezara → ROT13

A	Ą	B	C	D	E	Ę	F	G	H	I	J	K	L	Ł	M	N	Ń	O	Ó	P	R	S	Ś	T	U	V	W	Y	Z	Ź	Ż
R	S	Ś	T	U	V	W	Y	Z	Ź	Ż	A	Ą	B	C	D	E	Ę	F	G	H	I	J	K	L	Ł	M	N	Ń	O	Ó	P

  BEZPIECZEŃSTWOSK → ŚVOHŻVTOVĘJLNFJĄ

- **homofoniczne** - każdy znak tekstu jawnego posiada własny zbiór symboli zwanych homofonami. Liczba homofonów zależy od częstości występowania znaków w tekście jawnym. Wybór poszczególnych homofonów powinien być losowy. Pozwoli to uniknąć łamania metodą statyczną.
- **wieloalfabetowe** - wiele niezależnych podstawień monoalfabetycznych. Przykład: tarcza Albertiego – dwie tarcze ze znakami, jedna z tarcz jest obrotowa. Osoba

deszyfrująca musiała znać znak początkowy i sekwencję obrotów.



- **poligramowe** - w jednym kroku szyfrujemy więcej niż jeden znak, np. szyfr Playfaira

Szyfr Playfair'a.

- Kluczem szyfru jest macierz kwadratowa
- Alg szyfrowania:

1. Wybierz dwa znaki tekstu jawnego
2. Jeśli obydwa znaki są w tym samym wierszu to znaki szyfru odczytujemy z prawej strony znaków tekstu jawnego
3. Jeśli obydwa znaki są w tej samej kolumnie, to znaki szyfu odczytujemy poniżej znaków txt jawnego
4. Jeśli znaki znajdują się w różnych wierszach i kolumnach, to wyznaczny jest prostokąt, którego rogi wyznaczają znaki szyfrogramu
5. Jeśli oba znaki są identyczne wówczas w tekście jawnym wstawiany jest dodatkowy znak
6. W przypadku nieparzystej długości dopisywany jest nieznaczący znak.

Przykład: Alokacja (dzielimy na bloki dwuznakowe) -> AL OK AC JA

D	W	G	R	C
A	L	O	P	B
E	H	K	S	W
T	M	U	J	N
F	I	Y	Z	X

AL -> OP

D	W	G	R	C
A	L	O	P	B
E	H	K	S	W
T	M	U	J	N
F	I	Y	Z	X

OK -> UY

D	W	G	R	C
A	L	O	P	B
E	H	K	S	W
T	M	U	J	N
F	I	Y	Z	X

AC->BD

D	W	G	R	C
A	L	O	P	B
E	H	K	S	W
T	M	U	J	N
F	I	Y	Z	X

JA -> TP

Kryteria Shannona.

Pięć kryteriów Shannona:

1. Ilość tajności zaoferowanej - wewnętrzna moc algorytmu
2. Rozmiar klucza - powinien być możliwie mały
3. Łatwość - prostota i jak najmniejsza złożoność procesu szyfracji i deszyfracji
4. Propagacja błędów - powinna być zminimalizowana
5. Powiększanie się wiadomości - nie jest wskazane

Szyfry symetryczne (strumieniowe, blokowe) i asymetryczne:

Szyfry symetryczne:

- do szyfrowania i deszyfracji używamy jednego klucza
- klucz nie może zostać ujawniony
- nadawca i odbiorca muszą znać klucz

Szyfry symetryczne dzielą się na strumieniowe i blokowe.

Strumieniowe:

- każdy bity szyfrowany osobno
- do szyfrowania i deszyfracji wykorzystuje się ten sam klucz
- większość systemów opiera się na generatorach ciągów pseudolosowych (klucz)
- strumień bitu tekstu jawnego łączony jest z kluczem przy użyciu operacji XOR

Blokowe:

- szyfrują bloki wejściowe w oparciu o zadany klucz
- długość bloku wyjściowego jest równa długość bloku wejściowego
- mają 3 tryby pracy n/w.

Szyfry asymetryczne:

- wykorzystywane są dwa klucze: tajny i jawny.
- klucz tajny zna tylko właściciel, używany jest do deszyfracji,
- klucz jawny powszechnie znany, używany do szyfrowania,
- klucza prywatnego nie da się w prosty sposób odtworzyć z klucza publicznego
- algorytmy wykorzystują operacje jednokierunkowe (jesteśmy w stanie w jedną stronę przeprowadzić w prosty sposób operację, a w drugą już nie tak łatwo)

Tryby pracy szyfrów blokowych:

- ECB (Electronic Code Block)
- CBC (Cipher Block Chaining)
- CFB (Cipher Feedback)

ECB - tekst jest dzielony na bloki o ustalonej długości. Bloki szyfrowane są niezależnie przy użyciu tego samego klucza. Utrata pojedynczego bloku nie uniemożliwia deszyfracji pozostałych bloków. Zaleta - szybkość. Wada - bezpieczeństwo.

CBC - każdy blok szyfrogramu zależy zarówno od aktualnie szyfrowanej informacji oraz od wszystkich wcześniejszych. Wykonywana jest operacja XOR bloku aktualnie szyfrowanego z blokiem zaszyfrowanym wcześniej.

CFB - wiadomość przesyłana jest znak po znaku. Wykorzystuje rejestr przesuwny. Rejestr przesuwny wypełniony jest pewną sekwencją inicjującą. Aby rozpocząć szyfrowanie, musi zostać odebrany cały blok tekstu jawnego.

DES, 3DES, IDEA, AES, Blowfish, RC5, RSA, algorytm Diffiego-Hellmana, ElGamal:

Algorytm DES (Data Encryption Standard):

- algorytm symetryczny, blokowy
- dane długości 64 bitów
- klucz 56 bitowy utworzony z 64 bitowego klucza wejściowego
- 8 bitów klucza wejściowego traktuje się jako bity parzystości
- klucz musi być chroniony
- podatny jest na ataki typu *brute force*
- modyfikacją tego algorytmu jest 3DES.

Algorytm 3DES:

- oparty na DES
- wykorzystanie 3 operacji i 3 kluczy
- pierwszy krok - szyfrujemy pierwszym kluczem
- drugi krok - deszyfrujemy drugim kluczem
- trzeci krok - szyfrujemy trzecim kluczem

Algorytm IDEA (International Data Encryption Algorithm):

- symetryczny, blokowy
- dane długości 64 bitów
- klucz długości 128 bitów
- opiera się na operacjach arytmetycznych takich jak: sumo modulo 2, dodawanie modulo 2^16, mnożenie modulo 2^16+1

Algorytm AES (Advanced Encryption Standard):

- symetryczny, blokowy
- dane długości 128/192/256 bitów,
- klucz 128/192/256 bitów
- długość danych = długość klucza
- następca DES
- składa się z kilkunastu iteracyjnie wykonywanych rund
- liczba run zależy od rozmiaru klucza 10-128b, 12-192b, 14-256b

Algorytm Blowfish:

- symetryczny, blokowy
- dane długości 64 bitów
- klucz od 32 do 448 bitów
- 16 rund

Algorytm RC5:

- symetryczny, blokowy

- dane długości 32,64,128 bitów
- klucz od 0 do 1040 bitów
- ilość rund od 1 do 255
- następcą RC5 jest RC6
- **RC4 nie ma nic wspólnego z RC5**

Nazwa	Długość danych [bity]	Długość klucza [bity]	Ilość rund
DES	**64**	**56, 8 bitów parzystości**	**1**
3DES	**64**	**168, 24 bity parzystości**	**3**
IDEA	**64**	**128**	**8.5 (pół rundy tak!)**
AES	**128/192/256**	**128/192/256**	**10/12/14**
Blowfish	**64**	**32 - 448**	**16**
RC5	**32/64/128**	**0-2040**	**1-255**

Algorytm RSA:

- asymetryczny
- wykorzystywany do szyfrowania i podpisów cyfrowych
- opiera się na faktoryzacji dużych liczb
- oba klucze są parą dużych liczb pierwszych
- klucz prywatny można obliczyć znając liczby pierwsze użyte przy tworzeniu klucza publicznego,
- jest wolniejszy niż DES
- wykorzystywany do wymiany klucza, a szyfrowanie tym samym kluczem odbywa się przy użyciu algorytmu DES

Algorytm Diffiego-Hellmana:

- służy do ustalenia klucza szyfrującego,
- wymiana może odbywać się niezabezpieczonym kanałem
- odporny na podsłuch
- obliczanie logarytmów dyskretnych w ciałach skończonych
- klucz może posłużyć do szyfrowania komunikacji
- nie nadaje się do szyfrowania
- zasada działania:
    - obie strony wykorzystują generatory g, korzystające z takiego samego zbioru danych
    - Strona A losuje liczbę naturalną a i wysyła stronie B g^a
    - Strona B losuje liczbę naturalną b i wysyła stronie A g^b
    - Strona A oblicza (g^b)^a
    - Strona B oblicza (g^a)^b
      W ten sposób obie strony posiadają **g^(ab)** - tajny klucz

Algorytm ElGamal:

- algorytm asymetryczny
- umożliwia szyfrowanie oraz obsługę podpisów cyforwych
- wykorzystuje algorytm Diffiego-Hellmana
- opiera się na obliczaniu logarytmów dyskretnych w ciele licz całkowitych modulo duża liczba pierwsza
- różne modyfikacje tego algorytmu są bardzo szeroko stosowane

Funkcje skrótu (MD2, MD4, MD5, SHA-1, SHA-2, SHA-3, zastosowania):

Funkcje skrótu:

- haszujące, mieszające
- na podstawie porcji danych wyznacza się krótki ciąg o stałej długości
- funkcja jednokierunkowa
- dla pewnej wiadomości w prostu sposób można utworzyć skrót
- ze skrótu trudno jest wyznaczyć wiadomość
- trudno jest znaleźć wiadomość, dla której skrót będzie identyczny (kolizja)

Algorytm MD2:

- stworzona w 1989 roku przez Rona Rivesta
- Losowe permutowanie bajtów.
- Wada: szybkość działania
- Nie powinna być wykorzystywana

Algorytm MD4:

- stworzona przez ROna Rivesta
- skrót długości 128 bitów
- blok 512 bitowy (448+64 na pierwotną długość), uzupełniany jeśli trzeba (jedynką i ciągiem zer)
- wynik uzyskiwany jest po przetworzeniu wszystkich bajtów
- 4 zmienne łańcuchowe
- transformacja ma 3 rundy (48 kroków)
- do wyniku każdego kroku dodawana jest stała zależna od numeru kroku
- nie jest wystarczająco bezpieczna - kolizje występują przy wykonaniu 2^20 operacji wyznaczania funkcji skrótu.

Algorytm MD5:

- ulepszona wersja MD4
- skrót o długości 128 bitów
- zmiany (ulepszenia):
    - cztery cykle (64 kroki), każdy oparty o inną funkcję nielionową, 16 operacji w każdym kroku
    - do wyniku dodawana jest stała zależna od numeru cyklu
    - zmieniona funkcja w cyklu drugim

    - wiadomosc pierwotna - koniecznośćwykonania 2^64 operacji skracania losowych wartości

Algorytm SHA-1:

- Zaprojektowany przez NIST i NSA.
- Blok 512 bitów (448+64), uzupełnienia jak w MD5.
- Skrót ma długość 160 bitów,
- bazuje na MD4
- Pięć 32 bitowych zmiennych łańcuchowych
- 4 cykle każdy po 20 operacji
- konwersja wejściowego ciągu: Big-endian.
- Niebezpieczny.

Algorytm SHA-2:

- SHA-224, SHA-256, SHA-384, SHA-512 – długość skrótu
- maksymalny rozmiar wiadomości
    - 2^64 - 1 (SHA-224, SHA-256),
    - 2^128 - 1 (SHA-384, SHA-512)
- rozmiar bloku
    - 512 bity (SHA-224, SHA-256) 16x32 bity,
    - 1024 bity (SHA-384, SHA-512) 16x64 bity
- ilość rund
    - 64 rundy (SHA-224, SHA-256),
    - 80 rund (SHA-384, SHA-512)

Algorytm SHA-3:

- alogrytm Keccak, w 2012 wygrał konkurs na funkcję haszującą NIST
- wyższa wydajność niż SHA-2
- jest alternatywą dla innych funkcji haszujących
- 24 rundy x 5 funkcji
- konstrukcja gąbki

Funkcje skrótu – podsumowanie

Funkcja		Długość skrótu [b]	Blok [b]	Max wielkość wiadomości	Kroki	Operacje
MD4		128	512	$2^{64} - 1$	48	and, or, xor, not
MD5		128	512	$2^{64} - 1$	64	and, or, xor, not
SHA-1		160	512	$2^{64} - 1$	80	and, or, xor, not
SHA-2	SHA -224	224	512	$2^{64} - 1$	64	and, or, xor, shr, rot
	SHA-256	256				
	SHA-384	384	512	$2^{128} - 1$	80	
	SHA-512	512				
SHA-3		224 256 384 512	1152 10880 832 576		24	and, xor, not, rot

Zastosowania:

Weryfikacja integralności plików bądź wiadomości

Istotnym zastosowaniem funkcji skrótu jest weryfikacja spójności danych. Porównanie skrótów dwóch plików umożliwia stwierdzenie, czy w pliku zostały dokonane jakiekolwiek zmiany.

Z tego powodu, większość algorytmów podpisu cyfrowego działa na zasadzie wygenerowania skrótu wiadomości, dzięki czemu można w dowolnym momencie sprawdzić, czy wiadomość jest autentyczna.

Funkcje skrótu używane są również do weryfikacji haseł. W celu zwiększenia bezpieczeństwa, w bazie danych przechowuje się skrót hasła, zamiast tekstu jawnego. Hasło wprowadzone przez użytkownika jest haszowane i dopiero wtedy porównywane ze skrótem w bazie danych. Taki sposób przechowywania haseł utrudnia ich odzyskanie, ze względu na jednokierunkowość funkcji haszujących.

Identyfikacja plików lub danych

Skrót może również służyć do identyfikacji plików; Systemy kontroli wersji, takie jak Git lub Mercurial używają funkcji skrótu SHA do identyfikacji różnego rodzaju zawartości (zawartość plików, drzewa katalogów).

Innym zastosowaniem jest używanie skrótów w tablicach z haszowaniem w celu szybkiego wyszukiwania danych.

Enigma, skytale:

Enigma

niemiecka przenośna, elektromechaniczna maszyna szyfrująca, oparta na zasadzie obracających się wirników. Tak jak inne maszyny oparte na rotorach, Enigma jest połączeniem systemów elektrycznego i mechanicznego. Część mechaniczna składa się z alfabetycznej 26 znakowej klawiatury, zestawu osadzonych na wspólnej osi i obracających się bębnów nazywanych rotorami lub wirnikami oraz mechanizmu obracającego jeden lub kilka rotorów naraz za każdym naciśnięciem klawisza.

Skytale

to metoda szyfrowania używana w starożytnej Grecji w szczególności przez Spartan. Na laskę nawijano pasek pergaminu, a tekst pisano na stykających się brzegach. Posiadacz laski o identycznej grubości mógł szybko odczytać tekst.

Podpis cyfrowy, podpis elektroniczny:

Podpis cyfrowy

służy do zagwarantowania:

- autentyczności - pochodzenie
- niezaprzeczalności - nie da się wyprzeć autorstwa
- integralności - podpisana informacja nie może zostać zmieniona

Podpis cyfrowy to kombinacja kryptografii asymetrycznej i jednokierunkowej funkcji skrótu. Jest funkcją podpisywanej wiadomości i pewnej informacji znanej autorowi (klucz prywatny). Może zostać zweryfikowany przy użyciu klucza publicznego.
Wykorzystujemy różne mechanizmy, kryptografii asymetrycznej.

Podpis elektroniczny

wniosek elektroniczny i nanoszony zeskanowany podpis odręczny

Niezaprzeczalny podpis cyfrowy, niepodrabialny podpis cyfrowy, podpis ślepy, podpis symetryczny z arbitrem:

Niezaprzeczalny podpis cyfrowy:

- nadawca nie może wyprzeć się wiadomości
- nadawca musi zgodzić się na weryfikację podpisu
- algorytm:
    - nadawca wysyła odbiorcy dokument z podpisem
    - odbiorca generuje losową liczbę i przesyła ją nadawcy

    - nadawca przy użyciu klucza prywatnego przekształca liczbę
    - nadawca przesyła wynik odbiorcy
    - odbiorca weryfikuje podpis

Niepodrabialny podpis cyfrowy:

- pozwala wykryć fałszerstwo
- dla klucza publicznego istnieje wiele kluczy prywatnych
- ciężko jest znaleźć właściwy klucz prywatny
- dokument podpisany z wykorzystaniem podrobionego klucza prywatnego to inny podpis
- oznacza to że można w prosty sposób wykryć próbę podrobienia wiadomości

Podpis ślepy:

- podpisujący nie powinien poznać treści dokumentu
- Przykład: Osoba podpisująca ma potwierdzić dostarczenie wiadomości a nie jej treść
- Wykorzystanie czynnika zaciemniającego - *nadawca mnoży przez losową zmienną wiadomość która ma być podpisana i daje ją do podpisu, tamten podpisuje i odsyła, a tamten sobie odciemnia.*
- Problem: skąd osoba podpisująca wie co podpisuje? *Wymyślono taką metodę: wykonano n kopii wiadomości zaciemnionych różnymi sposobami. Odbiorca prosi o n-1 czynników zaciemniających. Jeśli odbiorca przeprowadzi odpowiednie operacje i zobaczy że dokumenty są prawidłowe to podpis jest składany pod jednym nie odszyfrowanym plikiem (czyli tym bez czynnika nie zaciemniającego) Odbiorca prosi o losowe czynniki.*

Podpis symetryczny z arbitrem:

- w transmisji uczestniczy osoba będąca arbitrem (zaufana osoba, poświadczająca wiadomość - pośrednik)
- arbiter dzieli klucz nadawcy KN z nadawcą i klucz odbiorcy KO z odbiorcą
- Algorytm:
    - nadawca szyfruje wiadomość dla odbiorcy i przesyła do arbitra
    - arbiter odszyfrowuje wiadomość używając klucza KN
    - arbiter łączy odszyfrowaną wiadomość z zaszyfrowaną od nadawcy. Całość szyfruje kluczem KO
    - odbiorca deszyfruje wiadomość przy użyciu klucza KO. Otrzymuje w ten sposób wiadomość i poświadczenie źródła wiadomości od arbitra.

Podpis jest niepodrabialny, autentyczny. Wygenerowany dokument jest niezmienialny, niezaprzeczalny.

PKI (elementy, funkcje, cykl życia klucza, proces certyfikowania, przechowywanie certyfikatów, zastosowania):

PKI (Public Key Infrastructure)

- służy do zarządzania kluczami publicznymi użytkowników,
- pozwala wiązać klucz publiczny z daną osobą
- właściciel tworzy parę kluczy, skrót klucza publicznego jest certyfikowany
- PKI służy do zapobiegania fałszerstwom polegającym na podmianie klucza

Elementy PKI:

- Centra Certyfikacji (CA)
- Urzędy rejestrujące (RA)
- Posiadacze certyfikatów
- Klienci
- Repozytoria

PKI cykl życia klucza:

- utworzenie
- certyfikacja
- rozprowadzenie - *przez właściciela pierwszego centrum certyfikacji****
- użytkowanie aktywne - *służy do szyfrowania****
- użytkowanie pasywne (dany klucz już nie powinien być stosowany ale jest)
- unieważnienie klucza - *umieszczany na liście CRL - liczba odwołań certyfikatu.****

*** - niepotwierdzone*

Proces certyfikowania

użytkownik zgłasza się do CA ze swoim kluczem publicznym. Do weryfikacji wykorzystywany jest klucz publiczny CA.

Przechowywanie certyfikatów

- serwery LDAP
- serwery WWW
- serwery FTP
- serwery DNS
- X.500
- bazy danych
- OSCP

Standard X.509 (definicja, składowe certyfikatu, CRL):

X.509 v3

najpopularniejszy standard certyfikatów PKI, definiuje schemat certyfikatu unieważnień (CRL) i atrybutu. Nadzorowany przez ITU-T. Pierwsza wersja standardu opublikowana w 1988 r.

Składowe certyfikatu X.509 v3

- wersja
- numer seryjny
- sygnatura
- informacja o wystawcy
- identyfikator algorytmu
- data ważności
- informacja o właścicielu
- klucz publiczny właściciela
- rozszerzenia

X.509 v3 - CRL

Certificate Revocation List, jest to lista unieważnionych certyfikatów publikowana przez CA. Zawiera wyłącznie numery seryjne unieważnionych certyfikatów. Posiadacz klucza zwraca się do CA w celu unieważnienia certyfikatu.

X509 v3 - certyfikaty atrybutów

Atrybuty opisujące uprawnienia. Rozdzielenie autoryzacji od uwierzytelniania.

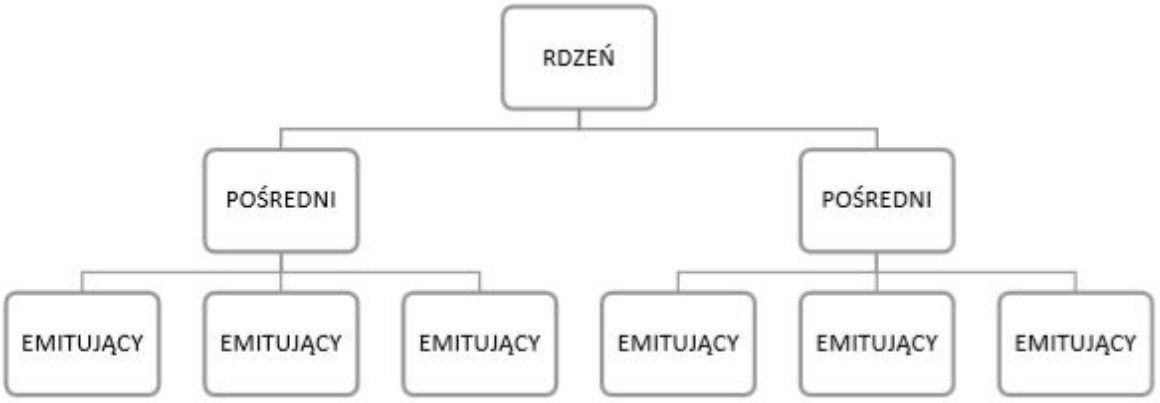
Urząd certyfikacji (rodzaje certyfikacji, model hierarchiczny, centra certyfikujące):

CA (Certificate Authority)

- Wewnętrzna
    - Prostsze zarządzanie **+**
    - Brak kosztów certyfikatów **+**
    - Tańsza rozbudowa systemu **+**
    - Bardziej skomplikowana implementacja **-**
    - Kwestie bezpieczeństwa spoczywają na właścicielu **-**
    - Brak zaufania
- Zewnętrzna
    - Bezpieczeństwo i odpowiedzialność spoczywają na CA **+**
    - Zaufanie **+**

- Konieczność płacenia za każdy certyfikat **-**
- Mniejsza elastyczność w przypadku konfiguracji i zarządzania **-**
- Skomplikowana integracja **-**

Model hierarchiczny:



Poziom emitujących powinien być weryfikowany przez nasz poziom pośredni.
Emitujący to osoba/firma, która wystawia konkretny certyfikat dla klienta.
Rdzeń musi być naprawdę dobrze chroniony.

Centra certyfikujące:

- komercyjne
  - Symantec - kiedyś VeriSign
  - Comodo Group - prywatna firma z USA
  - Go Daddy - prywatna firma z USA
  - GlobalSign
- komercyjne Polska
  - KIR (Szafir) - krajowa izba rozliczeniowa (rozliczenia pomiędzy bankami)
  - PWPW (Sigillium) - państwowa wytwórnia papierów wartościowych
  - Unizeto Technologies
- NIekomercyjne
  - OpenCA
  - OpenSSL
  - TinyCA

Model OSI-7 (definicja, warstwy, działanie każdej warstwy, protokoły, urządzenia):

MODEL OSI-7

standard zdefiniowany przez ISO oraz ITUT opisujący strukturę komunikacji sieciowej. Model OSI opisuje drogę danych od aplikacji w systemie jednej stacji roboczej do

aplikacji w systemie drugiej. Przed wysłaniem dane wraz z przekazywaniem do niższych warstw sieci zmieniają swój format, co nosi nazwę procesu kapsułkowania (enkapsulacji).

Warstwy:

- aplikacji
  - definiuje interfejs transmisji danych przez aplikację
  - protokoły
    - FTP, TFTP
    - DNS
    - SMTP, POP3, IMAP
    - SIP
    - HTTP
    - SNMP
    - SSH
    - telnet
    - DHCP
  - urządzenia
    - brama
    - host (komputer)
    - serwer
- prezentacji
  - odpowiada za szyfrowanie, kodowanie, kompresję, konwersję danych
  - protokoły
    - ssl,
    - mime
- sesji
  - odpowiada za negocjację i nawiązywanie połączenia
  - protokoły
    - L2TP,
    - PPTP,
    - NetBIOS
- transportowa
  - odpowiada za przekazywanie danych między urządzeniami
  - dane dzielone są na części
  - port
  - protokoły
    - TCP,
    - UDP
    - SPX
- sieciowa
  - odpowiada za trasowanie pakietów
  - zna topologię sieci
  - adres logiczny
  - protokoły
    - IP
    - ICMP

            - ARP
            - RARP
            - IPsec
        - urządzenia
            - router
- łącza danych
    - nadzoruje błędy w warstwie fizycznej
    - enkapsulacja w ramki
    - adres fizyczny
    - protokoły
        - PPP
        - ATM
        - HDLC
        - ARP
        - X.25
        - Ethernet
    - urządzenia
        - most
        - przełącznik
- fizyczna
    - obsługa fizycznego wysyłania i odbierania sygnałów
    - sygnały elektryczne, radiowe, optyczne
    - przesył danych binarnych
    - brak mechanizmów kontroli
    - protokoły
        - Ethernet
        - RS-232
        - RS-459
        - DSL
        - PDF
        - Bluetooth
    - urządzenia
        - konwerter mediów
        - modem
        - transceiver - nadajnik-odbiornik
        - karta sieciowa
        - wzmacniak
        - koncentrator

Rodzaje ataków (pasywne, aktywne):

Rodzaje ataków:

- pasywne - atakujący nie modyfikuje fizycznej transmisji, transmisja trwa a atakujący ją np. podgląda, podsłuchuje, monitoruje
- aktywne - wszystkie te gdzie zachodzi fizyczna ingerencja w transmisję

Techniki ataków (sniffing, scanning, spoofing, poisoning, DoS, DDoS, DRDoS, zastosowania):

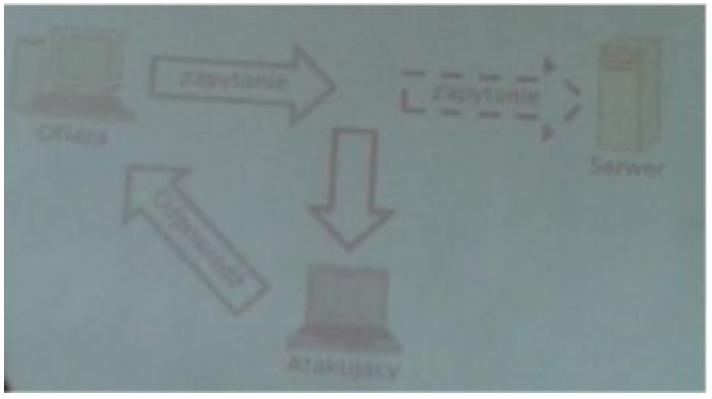
Techniki ataków:

- sniffing
    - wykorzystujemy ogólnodostępne oprogramowanie do monitorowania ruchu sieciowego
    - podsłuchujący musi ustawić kartę sieciową w odpowiedni tryb
    - karta przetwarza wówczas wszystkie pakiety które trafiają do niej
    - wszystko zależy też od budowy sieci komputerowej
    - podstawowe bezpieczeństwo daje zastosowanie switcha.

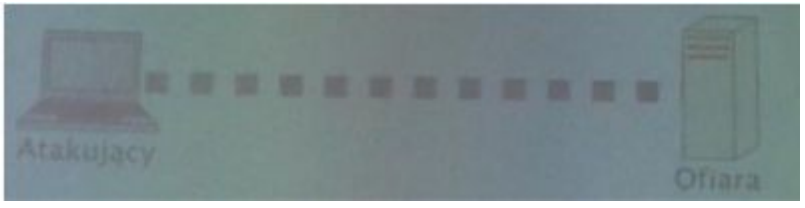
- scanning
    - atakujący skanuje ofiarę
    - służy to do weryfikacji usług jakie działają na danym serwerze jakie usługi udostępnia
    - skanowanie daje nam pogląd które porty otwarte i wtedy możemy szukać podatności danych portów na ataki
    - wykorzystuje specyfikę działania konkretnych protokołów

- spoofing
    - sytuacja, gdy atakujący powoduje, że ofiara wysyłając zapytania do serwera tak naprawdę zamiast tego przesyła je do atakującego
    - pojawia się coś na ścieżce transmisji co przechwytuje ten ruch
    - ofiara myśli że wszystko wysyła do serwera prawidłowo

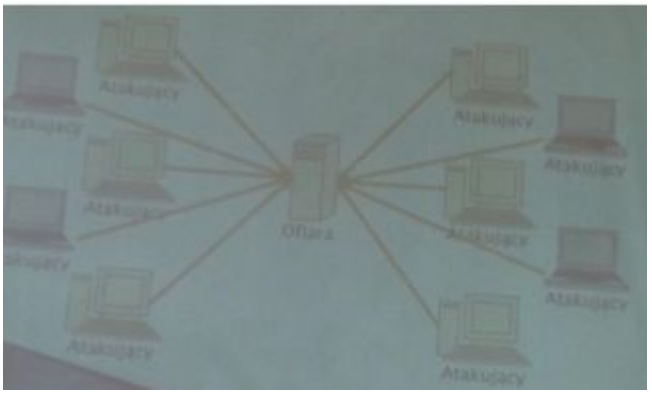
- poisoning
    - Podobnie jak spoofing, ofiara również myśli że komunikuje się prawidłowo,
    - w tym wypadku atakujący nie musi stosować technik przekierowania ruchu tylko spowodować, że ofiara będzie się komunikowała np. ze złym adresem (zamiast serwer prawidłowy to adres atakującego bo np. została oszukana na etapie uzyskiwania parametrów DNS)



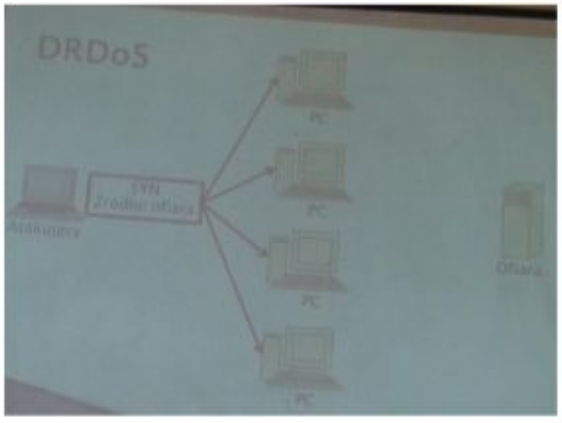
- DoS
    - Denial of Service
    - Atakujący stara się „zalać” ofiarę zapytaniami/pakietami, aby ofiara przestała świadczyć daną usługę.

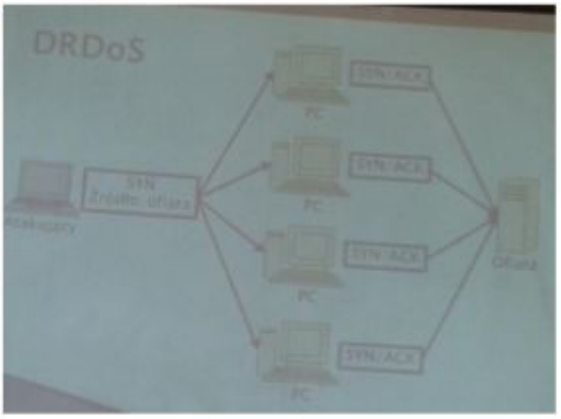


- DDoS
    - Distributed Denial of Service
    - rozproszony DoS.
    - Atakujących jest wielu, atakują równocześnie.
    - Może być nawet przypadkowy.



- DRDoS
    - Distributed Reflection Denial of Service
    - atak rozproszony, wykorzystujący specyfikę działania pewnych protokołów.
    - Ukrywamy faktyczne źródło ataku.
    - Atakujący wysyła pakiet z ustawioną pewną flagą, ale jako źródło podaje nie swój adres.
    - Wysyła to do X maszyn a świecie, maszyny wysyłają odpowiedź nie do atakującego ale do ofiary (jej adres był podstawiony w miejsce adresu atakującego).





nmap:

Nmap (ang. “Network Mapper”) jest narzędziem **open source** do **eksploracji** sieci i audytów bezpieczeństwa. Został zaprojektowany do szybkiego **skanowania** dużych sieci, ale również działa dobrze w stosunku do pojedynczych adresów. Nmap wykorzystuje **niskopoziomowe pakiety IP** do wykrywania które adresy są dostępne w sieci, jakie udostępniają usługi (nazwa aplikacji i wersja), na jakich systemach operacyjnych pracują (wersja systemu), jakie typy systemów zaporowych (firewall) są wykorzystywane i dziesiątek innych cech. Nmap jest powszechnie wykorzystywany do **audytów bezpieczeństwa**, również wielu administratorów sieci i systemów wykorzystuje go wykonywania rutynowych czynności, takich jak

inwentaryzacja zasobów sieci, zarządzanie aktualizacjami oprogramowania i **monitorowania** systemów oraz ich czasu działania (uptime).
Oprogramowanie nmap:

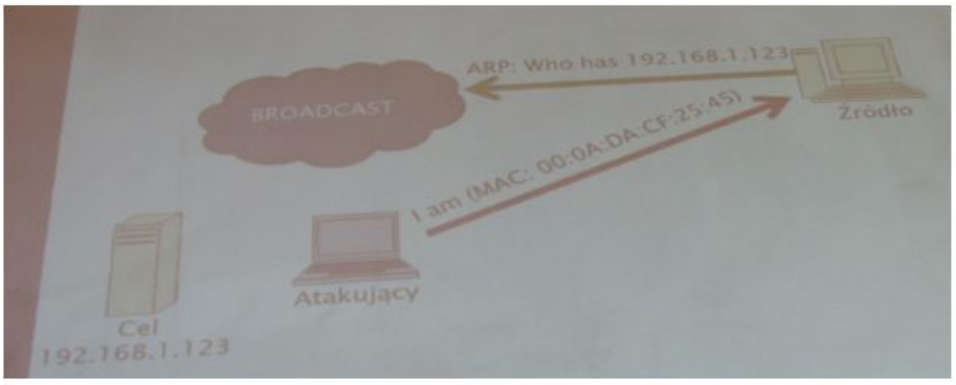
- TCP (nmap sT)
- UDP (nmap sU)
- SYN (nmap sS)
- ACK (nmap sA)
- FIN (nmap sF)
- Ping (nmap sP)

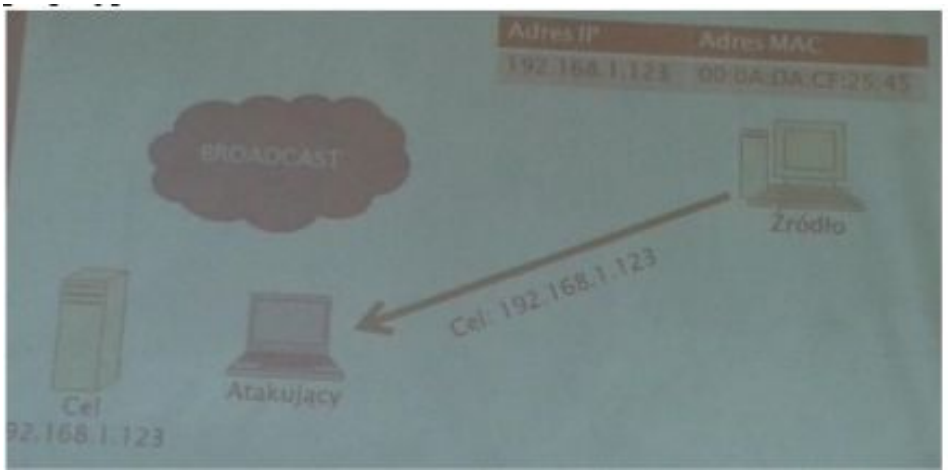
Zagrożenia i techniki w poszczególnych warstwach modelu OSI i protokołach:

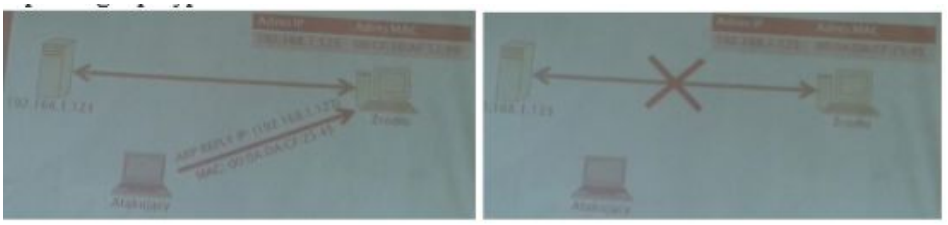
Zagrożenia:

- warstwa sieciowa
    - adresacja IP
        - możliwość modyfikacji adresu źródłowego
        - IP spoofing (podszywanie się pod IP - modyfikacja nagłówka)
    - routing
        - przekazywanie pakietów w oparciu o zdefiniowane reguły
        - za trasowanie odpowiedzialny jest router
        - router w przypadku przeciążenia odrzuca pakiety
        - retransmisja zależy od protokołu warstwy niższej
    - rozgłoszenia
        - w każdej sieci IP występuje adres broadcast
        - wysyłanie pakietu na taki adres spowoduje rozesłanie go do wszystkich urządzeń w sieci
        - również w warstwie łącza danych istnieje adres broadcast
    - ARP - mapowanie adresów sieciowych na fizyczne. ARP ma za zadanie dokonać translacji adresu IP na adres MAC
    - Jak działa ARP?
        - 1. W momencie gdy urządzenie źródłowe chce rozpocząć komunikację z innym urządzeniem w pierwszej kolejności sprawdza pamięć podręczną ARP pod katem docelowego adresu MAC. Gdy wpis zostanie znaleziony następuje transmisja.
        - 2. Gdy wpis nie zostanie znaleziony, źródło wygeneruje ARP request. ARP request zawiera adres IP i MAC źródła oraz IP celu. Mac celu jest pusty.
        - 3. ARP request zostaje wysłany jako rozgłoszenie do wszystkich urządzeń w sieci.
        - 4. Każde urządzenie odbiera pakiet i porównuje docelowy adres IP ze swoim adresem. Jeśli adresy się nie zgadzają pakiet zostanie odrzucony.

- 5. Gdy adresy się zgadzają to urządzenie generuje ARP reply. Celem jest adres źródła (IP i MAC) z ARP request.
- 6. Aby wysłać ARP reply urządzenie dodaje do swojej pamięci podręcznej ARP odpowiedni wpis (cel transmisji). Odpowiedź wysyłana jest bezpośrednio do źródła ARP request (unicast).
- 7. Źródło przetworzy pakiet i doda do swojej pamięci podręcznej odpowiedni wpis.

- umożliwia mapowanie adresów logicznych na fizyczne
- opisuje sposób utrzymywania tablic ARP (przez pewien czas przechowywana jest informacja o translacji adresu)
- zagrożenia ARP spoofing:
  - 

  - 

  - 
- ARP i Windows
  - dotyczy systemów od Visty
  - Jeżeli wpis w tablicy ARP ma status **Reachable** to transmisja odbywa się zgodnie z tym wpisem
  - Jeżeli wpis nie jest używany przez określony czas to status zmieniany jest na **Stale**

- Jeśli wpis w tablicy ma status **Stale**
    - Czas osiągalności określony jest wzorem BaseReachable * losowa wartość z przedziału MIN-MAX
    - BaseReachable 30 000 ms
    - MIN: 0,5
    - MAX: 1,5
    - Jeśli wpis nie jest używany przez 15-45 sekund to zostanie ustawiony status **Stale**
- Sprawdzanie aktualnego czasu osiągalności dla interfejsu:
    - netsh interface ipv4 show interfaces – wyświetlona zostanie lista dostępnych interfejsów
    - netsh interface ipv4 show interface INDEX – info na temat czasu osiągalności
    - netsh interface ipv5 set interface INDEX basereachable=CZAS[ms] – zmiana referencyjnego czasu osiągalności
- Domyślny rozmiar pamięci podręcznej: 256
    - Aby zmienić rozmiar należy skorzystać z polecenia: netsh interface ipv4 set global neighborcachelimit = 4096
- Wyświetlenie tablicy arp: arp –a
- Dodanie statycznego wpisu arp –s IP MAC
- Tak dodane wpisy są ważne tylko do ponownego uruchomienia komputera
- Usuniecie pojedynczego wpisu: arp –d IP
- Usunięcie wszystkich wpisów: arp –d * lub netsh interface ip delete arpcache

■ **ARP Poisoning** w Win 7

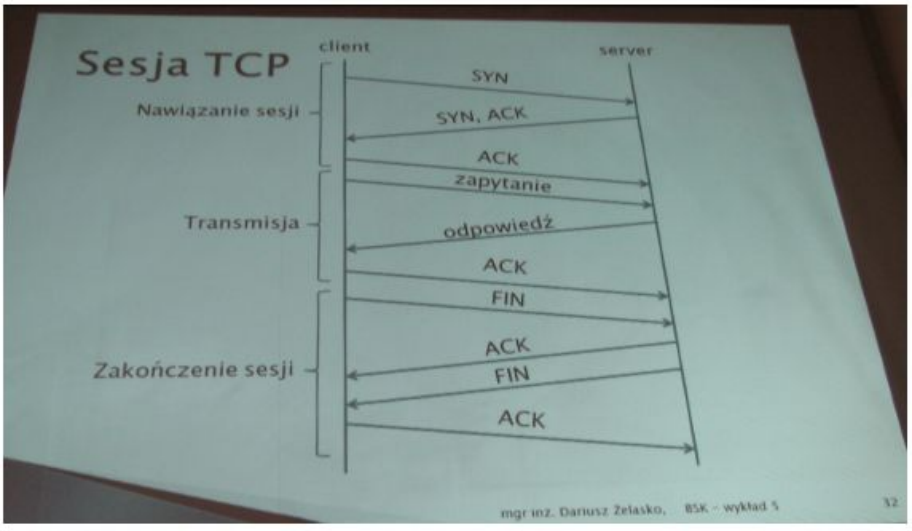
I

- Wysłanie ARP Reply do urządzenia z Windows 7 nie spowoduje zmiany w tablicy. Firewall w Windows zablokuje taki pakiet.
- W momencie gdy ofiara wykryła i zignorowała ARP Reply nastąpi wysłanie pakietu ARP Request. Docelowym adresem IP będzie adres źródłowy otrzymanego ARP Reply. ARP Request zostanie wysłany w formie unicast.
- Następnie system nie otrzyma odpowiedzi wyśle ARP Request w formie rozgłoszenia. Uzyskana odpowiedź będzie potwierdzeniem prawidłowości wpisu. **CO JEŻELI ATAKUJĄCY ODPOWIE NA PYTANIE SYSTEMU???**

II

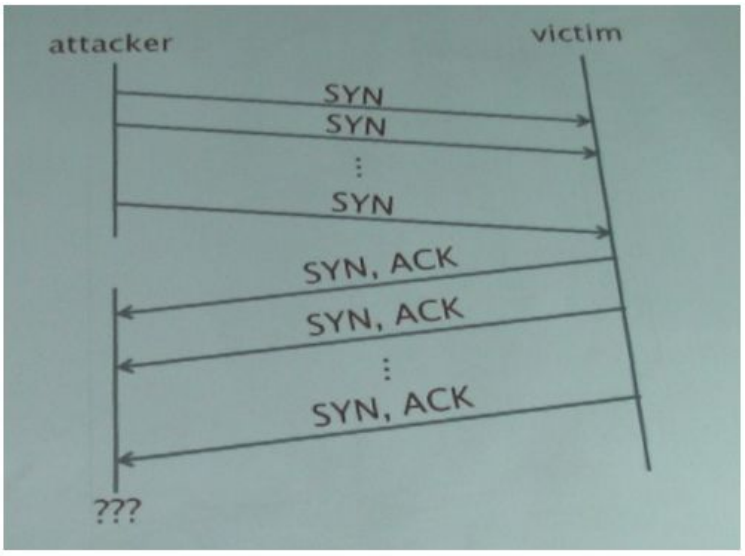
- Wysłanie pakietu ARP request ze sfałszowanym adresem źródłowym i prawidłowym docelowym IP spowoduje dodanie wpisu do tablicy ARP ofiary
- Komputer ofiary odpowie ARP Reply

            - Następnie ofiara wyśle pakiet ARP request pytając o adres źródła dla którego utworzony został wpis
            - Gdy atakujący nie odpowie ofiara wyśle ARP request w formie rozgłoszenia. Uzyskana odpowiedź spowoduje zmianę wpisu w tablicy ARP. **CO JEŚLI WPIS JUŻ ISTNIEJE?**
- warstwa łącza danych
    - **MAC flooding**
        - Tablica CAM przełącznika przechowuje adresy MAC i skojarzone z nimi porty
        - Atak polega na wysłaniu wielu pakietów z różnymi adresami źródłowymi MAC
        - Przełącznik stara się przypisać źródłowe MAC do portu
        - W momencie przepełnienia tablicy CAM przełącznik zaczyna działać jak koncentrator
        - Atakujący uzyskuje w ten sposób dostęp do wszystkich pakietów przekazywanych w sieci
- warstwa transportowa
    - UDP
        - Protokół bezpołączeniowy (bez nawiązania połączenia)
        - Brak kontroli przepływu i retransmisji
        - Zaletą jest szybkość działania (brak narzutów)
        - Wykorzystywany wszędzie tam gdzie ważna jest szybkość działania a nie koniecznie dokładność
        - Zagrożenia: **UDP spoofing, UDP flood, DoS**
    - TCP
        - Połączeniowy i niezawodny protokół komunikacyjny
        - Kontrola przepływu i retransmisja
        - Wolniejszy od UDP
        - Wykorzystywany wszędzie tam gdzie ważna jest dokładność a nie szybkość
        - sesja TCP:



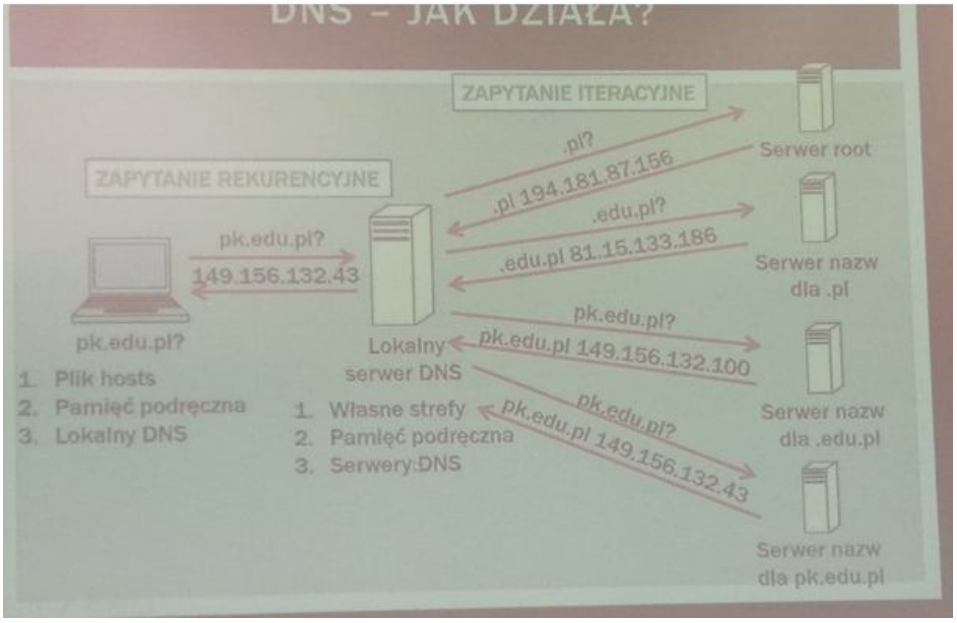
        - **TCP spoofing:**
            - celem jest zestawienie połączenia z ofiarą ataku podszywając się pod zaufany system

        - wymaga sfałszowania adresu i znalezienia prawidłowego ISN
    - **SYN Flood:**
        - do ofiary wysyłamy wiele pakietów SYN ze sfałszowanym adresem źródłowym.
        - Ofiara zacznie odpowiadać z SYN ACK do nas (bo źródło zostało podstawione).



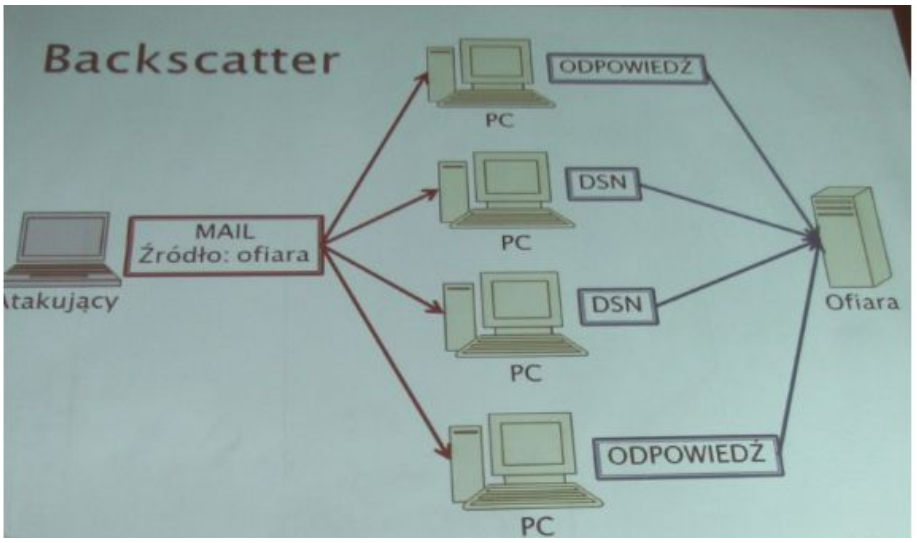
    - **ping**
        - Program do diagnozowania połączeń sieciowych
        - Podaje liczbę zagubionych pakietów oraz opóźnienie transmisji
        - Wykorzystuje protokół ICMP (ICMP Echo Request i ICMP Echo Reply)
    - **ping flood**
        - Duża liczba pakietów ICMP
        - Ma za zadanie przeciążyć łącze ofiary
        - Atakujący musi posiadać łącze o wyższej przepustowości niż ofiara
        - Atak może zostać przeprowadzony z wielu maszyn równocześnie
    - **smurf attack**
        - Następca Ping flood
        - Atakujący nie musi posiadać wyższej przepustowości łącza niż ofiara
        - ICMP Echo Request wysyłane jest ze zmienionym adresem źródłowym – adres ofiary
        - Pakiety wysyłane są na adres rozgłoszeniowy dużej sieci
        - Komputery, które odebrały pakiety wysyłają ICMP Echo Reply na adres ofiary
- warstwa aplikacji

- DNS



  - Domain Name System
  - Służy do zamiany nazw domenowych zrozumiałych dla użytkownika na adresy zrozumiałe dla urządzeń sieciowych
  - Struktura hierarchiczna
  - Rozproszona baza danych
  - **Zagrożenia**:
    - **DNS korzysta z protokołu UDP – DdoS**
    - **Brak mechanizmów autoryzacji – Man in the middle**
    - **Zatruwanie pamięci cache – cache poisoning**
  - **Zapobieganie**
    - **DNSSec**
  - Drive-by pharming
    - Ma za zadanie podmianę serwerów DNS na routerze ofiary
    - Konsekwencją jest to, że użytkownik może zostać skierowany na spreparowane strony internetowe
    - Główna przyczyna opiera się na zbyt słabym haśle routera
- SMTP
  - Simple Mail Transfer Protocol
  - Przekazywanie poczty elektronicznej
  - Zagrożenia
    - **Brak weryfikacji nadawcy**
    - **Backscatter**
    - **Sniffing**
    - **Spoofing**
    - **phishing**
    - **Man in the middle**
  - **zapobieganie:**
    - SMTP-AUTH - niweluje problem open relay, żeby wysłać wiadomość musi zostać dokonana autoryzacja (login, hasło)
    - TLS/SSL - protokół szyfrowania
  - **E-mail spoofing**

        - E-mail ze sfałszowanym nagłówkiem
        - Umożliwia to podszycie się pod np. zaufane źródło
    - **Backscatter -** Atakujący wysyła wiadomość podszywając się adresem pod kogoś innego. Przesyła wiadomość do wielu serwerów.



    - SMTP komendy
        - Inicjacja sesji (np. telnet 25 localhost)
        - EHLO/HELO – powitanie i uzyskanie informacji o serwerze
        - MAIL FROM: adres_email – źródło wiadomości
        - RCPT TO: adres_email – cel wiadomości
        - DATA: 1. SUBJECT TEMAT 2. Treść wiadomości 3. Znak ‘ . ‘ – koniec wiadomości
        - QUIT – zakończenie połączenia
    - **SPAM**
        - Wszelkiego rodzaju niechciane lub niepotrzebne wiadomości elektroniczne (brak wyraźnej zgody na otrzymywanie)
        - Treść wiadomości niezależna od odbiorcy
        - Nadawca może odnieść zysk większy niż korzyść odbiorcy

- FTP
    - Protokół wymiany plików
    - Klient-serwer
    - Port 21 (polecenia – port stały) i 20 (dane – nie zawsze ten sam port) TCP
    - RFC 959
    - Tryby pracy:
        - aktywny – port 21 do wysyłania poleceń i 20 do przesyłu danych, połączenie zestawiane przez serwer
        - pasywny – port 21 do wysyłania poleceń i port powyżej 1024 dla transmisji danych, połączenia zestawiane przez klienta
    - Zagrożenia:
        - **Błędne uprawnienia,**
        - **DoS**
    - //Komendy kontrolne FTP
        - USER – nazwa użytkownika

                - PASS – hasło
                - CWD – zmień katalog (np. na zgodny z uprawnieniami)
                - CDUP – przejdź do katalogu nadrzędnego
                - QUIT – przerwanie połączenia
    - telnet
        - Obsługa terminala w architekturze klient-serwer
        - Połączenie nie jest szyfrowane
        - Zagrożenia:
            - **spoofing,**
            - **sniffing**
        - **Zapobieganie**
            - SSH – „rozwiązanie dla niebezpiecznego telnetu”
    - LDAP
        - Lightweight Directory Access Protocol
        - Bazuje na standardzie X.500
        - Protokół usług katalogowych
        - Wykorzystuje TCP/IP
        - **Nie jest szyfrowany**
        - Zagrożenia:
            - **man in the middle,**
            - **sniffing**
    - **Decompression bomb**
        - Archiwum (np. zip), które może spowodować:
            - Wygenerowanie nieskończenie dużego pliku
            - Wygenerowanie bardzo dużego pliku (poprzez wysoki stopień kompresji)
        - Łatwy do wykrycia przez oprogramowanie antywirusowe
    - **Fork-bomb**
        - Polega na utworzeniu wielu kopii programu w celu wypełnienia tablicy procesów
        - Nie ma możliwości wywołania nowego procesu
        - Zabezpieczenie:
            - limit procesów, które mogą zostać utworzone przez użytkownika
    - **Brute force**
        - Może zostać wykorzystany w ataku na dowolny system kryptograficzny
        - Systematyczne sprawdzenie wszystkich możliwych kombinacji (kluczy, haseł)
        - Dla krótkich haseł metoda działa dość szybko
        - Przy dłuższych hasłach czas szukania jest nieakceptowalny
        - Zasoby
    - **Atak słownikowy**
        - Metoda zbliżona do brute force
        - Wykorzystywany jest słownik, który może być np. lista słów najczęściej występujących w danym języku
    - **Tablice tęczowe**
        - Baza zawierająca skróty

        - Wykorzystywane w łamaniu haseł zahaszowanych jednokierunkową funkcją skrótu
        - Baza tworzona jest przez zapisywanie łańcuchów ze skrótów z haseł
        - Mniej mocy obliczeniowej niż brute force
    - **Sól**
        - Pozwala zabezpieczyć się przed próbami złamania hasła
        - Sól to losowo generowana wartość dodawana do skrótu

SSL/TLS:

SSL/TLS:

- Zapewnia poufność, integralność i uwierzytelnianie
- 1994 – pierwsze wersja protokołu SSL (Netscape)
- 1995 – SSL 3
- 1996 – grupa TLS zaczęła pracę nad rozwinięciem SSL
- Klucze 40 bitowe nie zapewniały bezpieczeństwa
- Obecnie min. 128 bitowe klucze
- Działa w warstwie prezentacji
- Wykorzystywany m.in. przez HTTPS, POP3, IMAP, SMTP, FTPS
- Wykorzystuje symetryczne i asymetryczne algorytmy szyfrowania
- Pod-protokoły: SSL Handshake, SSL Change Cipher Specification, SSL Alert Protocol, SSL Record Layer

SSL Handshake

- Służy do zabezpieczenia:
    - Uwierzytelniania serwera, klienta (nieobowiązkowe)
    - Wymiana informacji niezbędnych do wyliczenia wspólnego sekretu
- Dwa rodzaje komunikatów: nazwiązanie nowej sesji, odnowienei sesji

SSL Change Cipher Specification

- Jeden komunikat
- Sygnalizacja, że zmienione zostały parametry zabezpieczenia
- Zmiana przeprowadzana jest niezależnie (klient i serwer)

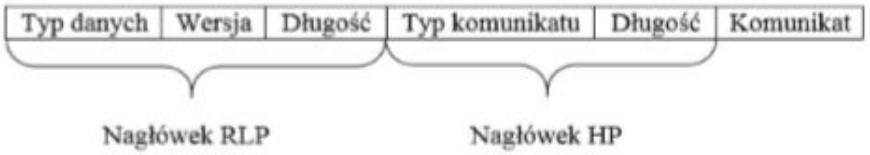
SSL Alert Protocol

- Informuje o błędach w komunikacji
- Dwa poziomy ważności:
    - Warning – komunikacja może przebiegać dalej
    - Critical error - komunikacja zostaje zakończona

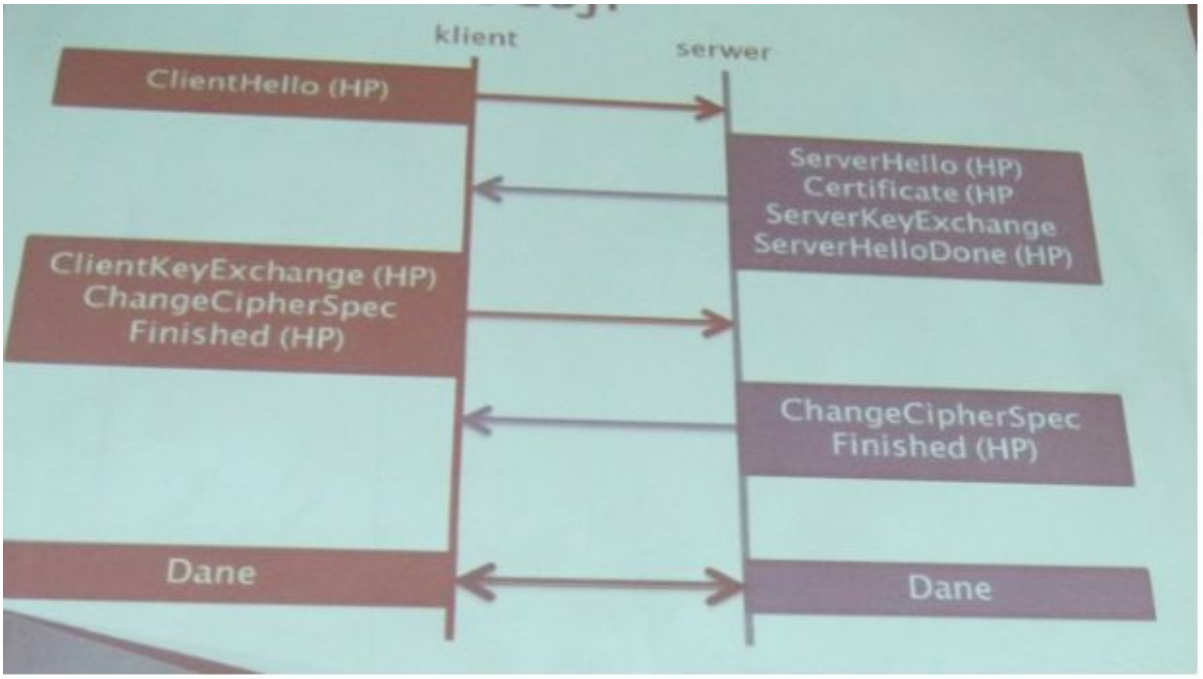
SSL Record Layer

- Dzieli dane na fragmenty mniejsze niż 2^14 B
- Przeprowadza kompresję danych (o ile obie strony się zgodziły)
- Oblicza sumę kontrolną
- Uzupełnia blok gdy dane zajmują mniej niż przewiduje blok szyfru

Nagłówek:

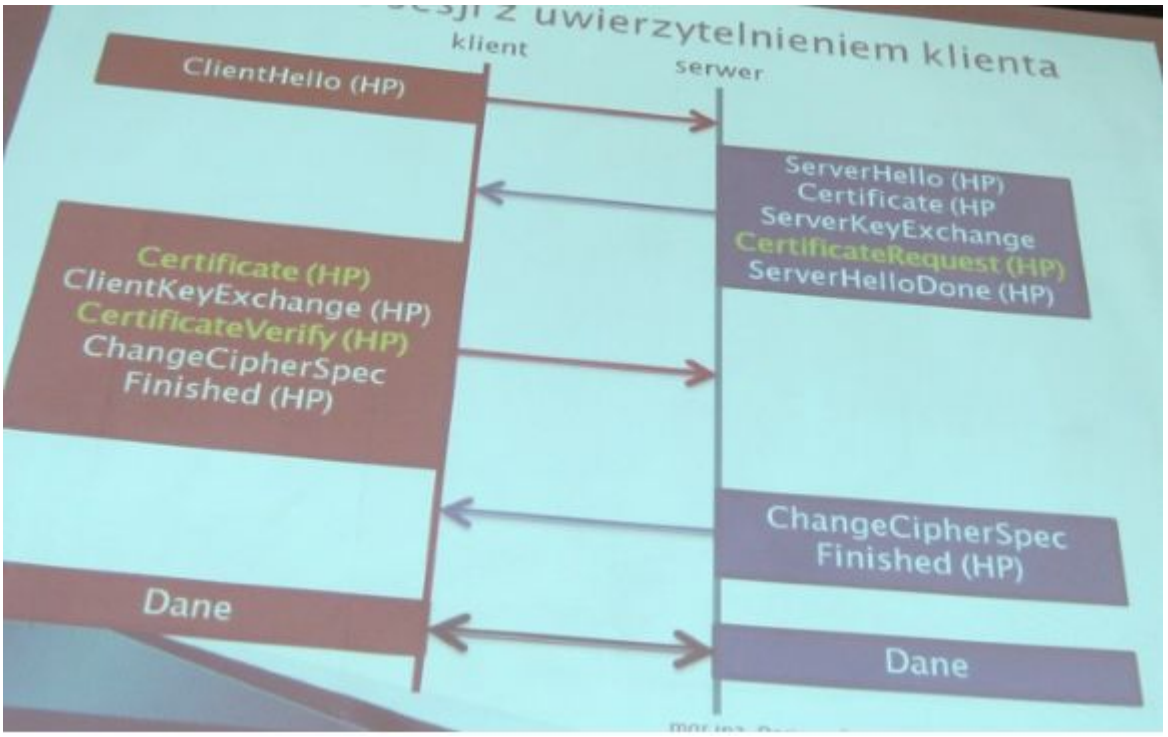


Utworzenie sesji



1. Klient: ClientHello(HP) à serwer
2. Serwer: ServerHello(HP), Certificate(HP), ServerKeyExchange, ServerHelloDone(HP) à klient
3. Klient: ClientKeyExchange(HP), ChangeCipherSpec, Finished(HP) à serwer
4. Serwer: ChangeCipherSpec, Fihisned(HP) à klient
5. Dane klientßàserwer

Utworzenie sesji z uwierzytelnieniem klienta



- To samo co utworzenie sesji normalnie (to wyżej)
- przy „2.” Dodajemy CertificateRequest(HP)
- przy „3.” Certificate(HP), CertificateVerify(HP)

Firewall (definicja, zadania, rodzaje, typy, rozwiązania, konfiguracja, zastosowania):

Firewall

- System bezpieczeństwa służący do kontroli ruchu przychodzącego i wychodzącego
- Działa w oparciu o reguły
- Pakiety filtrowane są pod kątem spełniania reguł
- Znajduje się pomiędzy bezpieczną siecią wewnętrzną a siecią zewnętrzną
- Pracują w dolnych warstwach modelu OSI (nie do końca prawda)
  [LAN] --- [Firewall] --- [WAN]

Zadania:

- Filtrowanie pakietów
- Proxy
- NAT
- VPN

Rodzaje

- Sprzętowy
  - dedykowane urządzenie podpięte kablami

- Programowy
    - maszyna, na której instalujemy odpowiednie oprogramowanie

Typy

- bezstanowy
    - Pojawiły się w latach 80 XX wieku (routery)
    - Pierwszy dokument – 1988 rok
    - Filtrowały wyłącznie pakiety
    - Jeśli dany pakiet spełnia którąś z reguł jest blokowany:
        - DROP – zablokowanie
        - REJECT – drop z informacją zwrotną
    - Firewall tego typu nie sprawdza czy pakiet jest fragmentem już trwającej transmisji
    - Wykorzystywane informacje:
        - docelowy i źródłowy adres,
        - protokół,
        - port docelowy i źródłowy (w przypadku TCP, UDP)
    - Zazwyczaj pracują w warstwie fizycznej, łącza danych i sieciowej
    - Z warstwy transportowej pochodzi informacja dotycząca portu
    - **Zalety**: szybki, małe wymagania sprzętowe
    - **Wady**: brak definicji kierunku ruchu, brak śledzenia sesji, analiza nagłówków protokołu
    - *//Zalety i wady bezstanowych nie są takie oczywiste. Np. szybki, ale brak mechanizmów śledzenia sesji. Więc coś za coś*
    -
    -
- stanowy
    - Przechowuje informacje o zestawionych sesjach i połączeniach – stan łącza, sesja TCP
    - Monitorowanie pakietów przychodzących i wychodzących
    - Informacje przechowywane są w tablicy dynamicznej
    - Decyzje podejmowane są nie tylko na podstawie reguł ale również kontekstu
    - Pakiety należące do sesji są przesyłane natychmiast
    - Three-way handshake
    - Pakiety z flagą SYN traktowane są jako próba nawiązania nowej sesji/połączenia
    - **Zalety**: weryfikacja kierunku ruchu, śledzenie sesji, analiza kontekstowa nagłówków, dodatkowe funkcje np. proxy
    - **Wady**: wolniejszy, większe wymagania sprzętowe

**** - NIEKONIECZNIE TYP, może chodzić o konfiguracje!**

- programowy**
    - Pracuje w warstwie aplikacji
    - Kontroluje informacje przychodzące i wychodzące oraz próby dostępu do aplikacji lub usługi

    - Typy: network-based, host-based (działa na naszym OS, zabezpiecza tylko nasz komputer)
- network-based**
    - Może działać np. na hoście przez który przechodzi cały ruch sieciowy
    - Nadzoruje ruch, filtruje zawartość
    - Tego typu firewall może zostać tak skonfigurowany aby kontrolował tylko konkretne usługi
- host-based**
    - Oprogramowanie zainstalowane na komputerze
    - Badane są wywołania systemowe
    - Chroni wyłącznie aplikacje zainstalowane na tym komputerze
    - Mogą blokować reklamy
    - Tryb interaktywnego uczenia się po instalacji
    - Często ze zintegrowaną ochroną antywirusową

**** - NIEKONIECZNIE TYP, może chodzić o konfiguracje!**

Rozwiązania

- sprzętowe
    - Cisco,
    - Checkpoint,
    - Juniper,
    - PaloAltoNetworks,
    - Watchguard
- systemowe
    - IPFilter (Unix),
    - Ipfw (FreeBSD),
    - NPF (NetBSD),
    - PF (OpenBSD),
    - nftables/iptables/ipchains (Linux)
        - IPTABLES:
            - Iptables od linuxa 2.4, wcześniej ipchains
            - Program do konfiguracji reguł firewalla
            - Umożliwia tworzenie tabel zawierających łańcuchy regul przetwarzania pakietów
            - Tabele: Filter, Nat
            - Reguly: PREROUTING (nat), INPUT(filter), FORWARD (filter), OUTPUT (filter, nat), POSTROUTING(nat)
            - Akcje: ACCEPT, DROP, REJECT
            - Firestarter – graficzna nakładka na iptables
            - Następca iptables: nftables (kernel 3.13) //bazuje na wirtualnej maszynie
    - zapora systemu Windows
- darmowe firewalle
    - Endian firewall
    - IPCop
    - IPFire

    - Vyatta (potem skomercjalizowana – teraz na jej podstawie /?? Pisownia/ VOS)

Konfiguracja

- z routowaniem
- drop-in
- bridge

Zastosowania

Do jego podstawowych zadań należy filtrowanie połączeń wchodzących i wychodzących oraz tym samym odmawianie żądań dostępu uznanych za niebezpieczne.

Proxy:

Proxy:

- Pośredniczą w transmisji
- Użytkownik wysyła zapytanie do proxy
- Proxy przesyła zapytanie do odpowiedniego serwera
- Zastosowania:
    - Filtrowanie zawartości
    - Podmiana źródła transmisji
    - Analiza ruchu w sieci
    - Cache

OpenProxy

- Dostępne dla każdego
- Zapewniają anonimowość (zaleta dla użytkownika, wada dla administratora)
- Open proxy są często blokowane przez serwery
- Przykład: https://hidemyass.com/proxy-list/

ReverseProxy

- Zapytania pochodzą z Internetu
- Proxy kieruje zapytania do odpowiednich serwerów
- Serwery znajdują się w sieci wewnętrznej
- Zalety:
    - Ukrywanie informacji o serwerze, który udzielił odpowiedzi
    - Ochrona przed atakami
    - Równoważenie obciążenia
    - Cache
    - Redukcja adresów IP

NAT:

NAT (Network Address Translation)

- Zmieniany jest adres źródłowy w nagłówku IP
- Pozwala na ukrycie adresu źródłowego (sieć lokalna)
- Dynamicznie tworzona jest tablica translacji
- Statyczna tablica – port forwarding
- Typy:
    - **1:1**
    - **1:wielu**
    - **1:wielu z translacją portów**

NAT 1:1

- Translacja 1:1 adresów prywatnych na publiczne, i na odwrót
- Każdy adres prywatny musi mieć odpowiadający mu adres publiczny
- Ukrycie źródła
- Główna wada: liczba niezbędnych adresów publicznych

NAT 1:wielu

- Zdefiniowana jest pewna pula adresów publicznych
- Translacja adresów odbywa się dynamicznie
- Router zapisuje informację o każdej translacji (odpowiedź)

NAT1:wielu z translacją portów

- Wystarczy jeden adres publiczny
- W nagłówku oprócz adresu źródłowego IP zmieniany jest również port źródłowy
- Tworzona jest tablica translacji (adres + port)
- Pozwala ograniczyć liczbę wykorzystywanych adresów publicznych

NAT vs IPv6

- Na chwilę obecną nie ma konieczności stosowania

IPv4	IPv6
2^32	2^128
4.3*10^9	~3.4*10^38

DMZ (demilitarized zone)

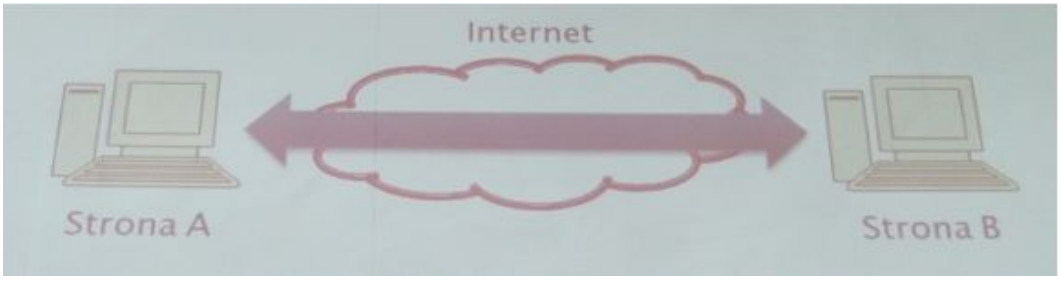
- Strefa zdemilitaryzowana
- Urządzenia znajdujące się w strefie są widoczne z sieci WAN
- Strefa ta jest odizolowana od sieci LAN

- W routerach SOHO urządzenie DMZ jest w tej samej sieci LAN co zwykłe urządzenia

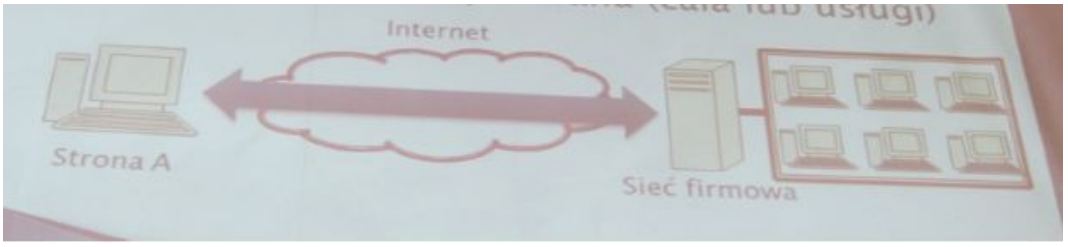
VPN:

VPN

- Virtual Private Network
- Umożliwia transmisję danych poprzez sieć publiczną przy użyciu bezpiecznego kanału
- Zestawienie połączenia point-to-point
- Umożliwia udostępnienie zasobów z sieci prywatnej użytkownikowi znajdującemu się poza siecią prywatną
- Przykład: firmowe VPN
- Podział:
    - Remote-Access
    - Site-to-Site
- Typy:
    - host-to-host



        - Tunel zestawiany jest pomiędzy komputerami //bezpośrednio
        - Strony muszą być wyposażone w odpowiednie oprogramowanie //lub sprzęt (sprzęt już niekoniecznie)
        - Zadania oprogramowania/sprzętu – szyfrowanie i deszyfrowanie
    - host-to-net



        - Jedną stronę stanowi komputer kliencki, drugą odpowiednie urządzenie
        - Strona kliencka uzyskuje dostęp do zasobów sieci korporacyjnej
        - Komunikacja jest szyfrowana (cała lub usługi)

    - net-to-net

        - Obie strony stanowią dedykowane urządzenia sieciowe
        - Mogą szyfrować całą transmisję ze swoich sieci lokalnych lub pewne wybrane usługi
        - Szyfrowana jest wyłącznie transmisja między lokalizacjami
        - Transmisja w obrębie sieci lokalnych nie jest szyfrowana
- Bezpieczeństwo:
    - Poufność
    - Uwierzytelnianie
    - Integralność
    - Protokoły:
        - IPSec
        - SSL/TLS
        - DTLS
        - SSTP
    - szyfrowanie
        - Zazwyczaj wykorzystywane są następujące metody szyfrowania: PGP, IDEA
- tunelowanie
    - VPN często opiera się na tunelowaniu:
    - Protokoły: Carrier Protocol, Tunneling Protocol, Passenger
- uwierzytelnianie
    - Strony muszą zostać uwierzytelnione
    - Różne metody uwierzytelniania

PGP:

PGP

- Oparty na MD5, RSA i IDEA
- Autor: Philip Zimmermann
- Początkowo bezpłatny
- Od wersji 5.0 bezpłatny do zastosowań niekomercyjnych
- W 2010 firma PGP została przejęta przez Symantec

PGP - szyfrowanie

1. Generowany jest losowy klucz
2. Dane wejściowe są szyfrowane przy użyciu wygenerowanego klucza
3. Klucz szyfrowany jest przy użyciu klucza publicznego odbiorcy
4. Zaszyfrowane dane i klucz przesyłane są odbiorcy

PGP - deszyfracja

1. Z zaszyfrowanej wiadomości wyodrębniane są zaszyfrowane dane i klucz
2. Klucz jest deszyfrowany przy użyciu klucza prywatnego odbiorcy
3. Dane deszyfrowane są przy użyciu odszyfrowanego klucza

IPSec (definicja, protokoły, tryby pracy, bazy danych, wysłanie/odebranie pakietu, zarządzanie kluczami, zastosowania):

IPS

- Stworzony w celu zabezpieczenia protokołu IP
- Zbiór otwartych standardów
- Wykorzystywany w IPv4 i IPv6
- Dostarcza mechanizmy uwierzytelniania i szyfrowania
- Szyfrowanie i uwierzytelnianie odbywa się dla każdego pakietu
- Wykorzystywany przez VPN
- Wykorzystanie IPSec nie wymusza stosowania specjalnego sprzętu/oprogramowania
- IPSec może zabezpieczać dowolny protokół warstwy wyższej (np. TCP UDP ICMP)
- Dawniej tworzono dedykowane łącza punkt-punkt
- Nie gwarantuje identyfikacji nadawcy
- IPSEC wykorzystuje:
    - Algorytm Diffiego-Hellmana – do wymiany kluczy
    - PKI – do negocjacji klucza
    - DES - do szyfrowania danych
    - MD5 i SHA - do generowania skrótów
    - Certyfikatów cyfrowych
- Składa się z dwóch podstawowych komponentów:
    - Danych dodawanych do pakietu IP zapewniających autentyczność, poufność i integralność – nagłówek AH lub ESP
    - IKE – mechanizm wymiany kluczy wykorzystywanych w trakcie negocjacji bezpiecznego połączenia

IPSec – security association (SA)

- Określa zależności bezpieczeństwa pomiędzy stronami
- Jest jednokierunkowym kanałem
- Jeśli komunikacja ma być dwukierunkowa muszą być dwa kanały
- Każdy kanał posiada swój własny SPI, licznik sekwencyjny i klucze kryptograficzne
- SA definiowana jest przez losowy SPI, docelowy adres IP oraz identyfikator protokołu zabezpieczeń (AH lub ESP)

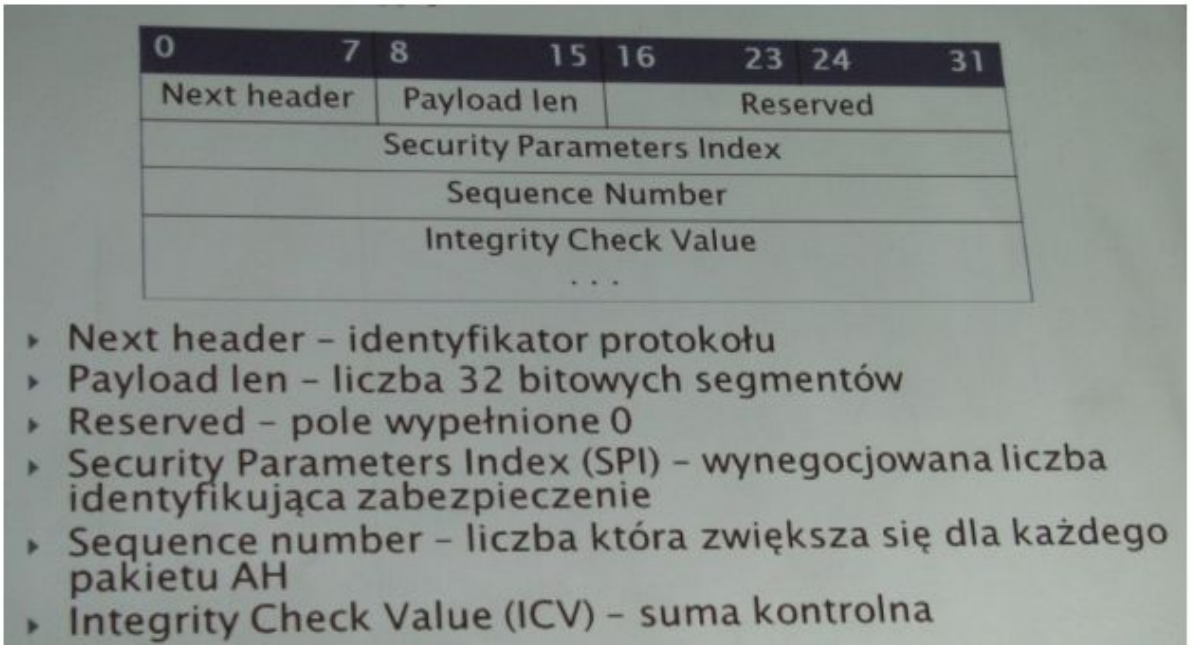
- W momencie wysłania pakietu, który wymaga zabezpieczenia przez IPSec system sprawdza w bazie relacje zabezpieczeń u umieszcza SPI w nagłówku IPSec
- Parametry zabezpieczeń negocjowane są w trakcie zestawienia połączenia
- Obowiązuję przez cały czas działania relacji

AH:

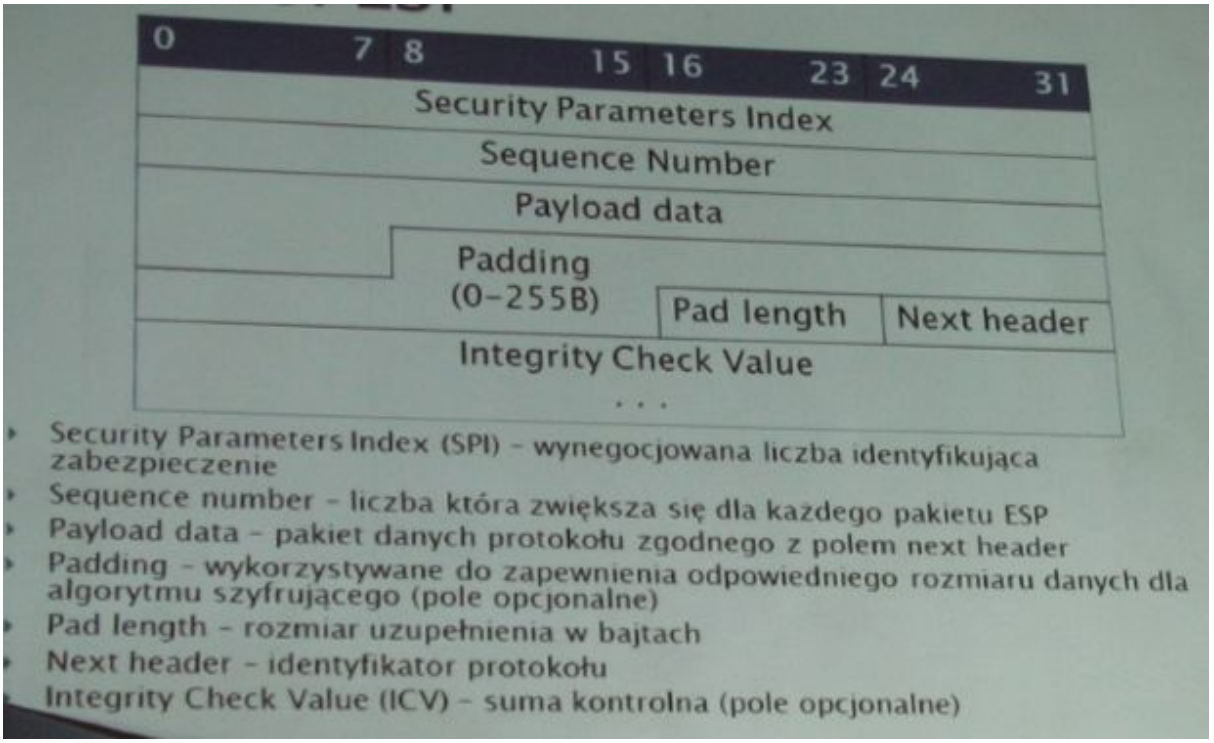
- Zapewnia integralności uwierzytelnianie
- Nie zapewnia poufności
- Protokół numer 51
- Tworzony jest skrót z pakietu (MD5, SHA-1 lub inne w zależności od negocjacji)
- Niezaprzeczalność: np. RSA
-

Protokoły

- AH:
    - Zapewnia integralności uwierzytelnianie
    - Nie zapewnia poufności
    - Protokół numer 51
    - Tworzony jest skrót z pakietu (MD5, SHA-1 lub inne w zależności od negocjacji)
    - Niezaprzeczalność: np. RSA



- ESP
    - Zapewnia szyfrowanie całego pakietu
    - Podpisywanie pakietu – funkcje skrótu
    - Szyfrowanie – szyfry blokowe w trybie CBC



Tryby Pracy

- IPSEC – tryb **transportowy**
    - Szyfrowana jest wyłącznie zawartość
    - Nie zapewnia integralności danych
    - Dodawany jest nagłówek AH/ESP
    - Bezpieczne łącze między hostami
- IPSEC - tryb **tunelowania**
    - Cały pakiet jest szyfrowany (nagłówek + dane)
    - Następnie tworzony jest nowy pakiet z nowym nagłówkiem
    - Wspiera NAT traversal
    - Stosowany gdy chociaż jedna strona to brama
    - Może być również stosowany do komunikacji host-host

Bazy Danych

- Dwie bazy danych:
    - SPD (Security Policy Database)
        - Baza SPD pozwala klasyfikować ruch sieciowy na
            - Inbound,
            - Outbound,
            - To be protected,
            - Not to protected
        - Możliwe decyzje:
            - Reject,
            - zastosuj IPSec,
            - nie stosuj IPSec
    - SAD (Security Association Database)

- Rekord w bazie SAD – aktywna relacja zabezpieczeń
- Indeksowanie – adres docelowy, typ protokołu IPSec, SPI
- Zawiera:
    - Licznik numeru sekwencyjnego
    - Wskaźnik przepełnienia licznika
    - Anti reply
    - Algorytm uwierzytelniania, klucze (dla AH)
    - Algorytm szyfrowania, klucze, algorytm uwierzytelniania (dla ESP)
    - Czas życia
    - Czas pracy

Wysłanie/Odebranie pakietu

1. Sprawdzenie konieczności zabezpieczenia i sposobu
    - Sprawdzenie polityki w SPD odrzucenie pakietu, przesłanie lub dalsze przetworzenie
2. Ustalenie Security Association
    - Przeglądanie bazy SAD
    - Nawiązanie SA
3. Zastosowanie zabezpieczeń
    - Utworzenie nagłówka AH lub ESP
    - W trybie tunelowym utworzenie nowego nagłówka IP
4. Wysłanie gotowego pakietu

1. Weryfikacja nagłówka IPSec
    - Sprawdzana jest baza SAD w poszukiwaniu SA zgodnego z SPI z nagłówka, dalsze przetwarzanie zgodne z SA
    - Odrzucenie gdy SA nie istnieje
2. Sprawdzenie konieczności zabezpieczenia i sposobu
    - Sprawdzenie polityki w SPD odrzucenie pakietu, dalsze przetworzenie

zarządzanie kluczami

- Dystrybucja kluczy nie należy do specyfikacji IPSec
- Możliwe metody dystrybucji:
    - Ręczna
    - Automatyczna
        - Systemy dystrybucji
        - Integracja z usługami katalogowymi
        - Niezależne od IPSec protokoły i serwery

zastosowania

- zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrowania pomiędzy komputerami. Protokoły tej grupy mogą być wykorzystywane do tworzenia Wirtualnej Sieci Prywatnej (ang.VPN). Może zabezpieczać dowolny protokół.

NAT Traversal:

NAT Traversal

- Gdy wykorzystywany jest IPSec wykorzystują NAT Traversal aby pakiety ESP przeszły przez NAT
- Umożliwia urządzeniom znajdującym się za NAT zestawienie bezpiecznego połączenia
- Najpierw następuje sprawdzenie, czy na drodze pomiędzy źródłem a celem znajdują się urządzenia NAT
- W tym celu każda ze stron wysyła pakiet NAT-D zawierający skrót z IP i portu
- Urządzenie, które odbierze pakiet NAT-D oblicza swój własny skrót i porównuje z tym otrzymanym
- Różne skrótu oznaczają, że po drodze znajduje się urządzenie NAT
- Następnie wykorzystywany jest NAT-T
- Pakiety IPSec są enkapsulowane w datagramy UDP i przesyłane do urządzenia docelowego
- W Windows XP NAT Traversal domyślnie jest włączony
- Od Windows XP SP2 jest domyślnie wyłączony

IKE (definicja, zasada działania):

IKE

- Internet Key Exchange
- Zaprojektowany przez NSA
- Służy do wymiany kluczy oraz zestawiania bezpiecznych połączeń
- Składa się z dwóch części:
    - ISAKMP – specyfikacja formatu pakietów i stanów
    - Oakley – kryptograficzne metody uwierzytelniania i negocjacji kluczy
- W przypadku IPSEC:
    - ISAKMP – negocjacja parametrów IPSec
    - Oakley – wymiana kluczy przy użyciu algorytmu Diffiego-Hellmana
- ISAKMP umożliwia definiowanie własnych parametrów (DOI) – zestaw szyfrów i mechanizmy uwierzytelniania

Zasada działania

1. Uwierzytelnienie stron
2. Zestawienie bezpiecznego kanału ISAKMP SA
3. Uzgodnienie kluczy i parametrów IPSec
4. Renegocjacja co określony czas

Kerberos (definicja, składniki systemu, zastosowania, algorytm uwierzytelniania):

Kerberos:

- Protokół uwierzytelniania i autoryzacji
- Powstał na uniwersytecie MIT w ramach projektu Athena
- Wykorzystuje port 88 UDP
- Jest bazą danych zawierającą dane dotyczące tożsamości oraz hasła
- Ze względu na rodzaj przechowywanych danych trzeba zapewnić odpowiedni poziom bezpieczeństwa
- Służy do wydawania biletów będących przepustkami do usług
- **Uwierzytelnianie:**
    -

Składniki systemu

- Składniki systemu:
    - Klient – źródło identyfikatora i hasła
    - Authentication server – przechowuje hasła i weryfikuje tożsamość użytkownika, TGT
    - Ticket-granting server – dostarcza klientowi bilet umożliwiający wykorzystanie usługi dostępnej na serwerze usług
      Serwer usług – świadczy pewną usługę, chce mieć pewność co do tożsamości klienta

Zastosowania

- Protokół uwierzytelnienia i weryfikacji
- Port 88 UDP
- Jest bazą danych dotyczącą tożsamości i haseł
- Służy do wydawania biletów będących przepustkami do usług

Algorytm uwierzytelnienia

WERSJA 1

1. Klient na swojej maszynie wprowadza login i hasło (szyfrowane za pomocą jednokierunkowej funkcji skrótu)
2. Klient > AS. Prośba o umożliwienie komunikacji z TGS (wywołanie do AS, prośba nie jest szyfrowana, zawiera ID, identyfikator TGS, timestamp)
3. AS sprawdza czy dany użytkownik jest w bazie. Następnie tworzy skrót zapisanego hasła
4. AS > Klient. (TGT i Odpowiedz). Odpowiedz zaszyfrowana, przy użyciu klucza utworzonego z hasła klienta, Odpowiedź zawiera: ID TGS, Klucz sesji klient TGS, timestamp, czas ważności biletu. TGT zaszyfrowane jest kluczem wspólnym dla AS i TGS. Klient nie odszyfruje TGT, posłuży to do Identyfikacji przy następnej próbie połączenia. TGT zawiera: ID klienta, adres klienta, ID TGS, Klucz sesji klient TGS, timestamp, czas ważności biletu. TGT pozwala uniknąć każdorazowej identyfikacji klienta

5. Klient > TGS. (Prośba o przepustkę do serwera usług + TGT). Prośba zaszyfrowana kluczem sesji AS. Zawiera: ID serwera usług, uwierzytelnienie klienta ID + IP + timestamp
6. TGS > Klient. (Ticket + klucz sesji) Klucz sesji zaszyfrowany przy użyciu klucza sesji współdzielonego przez klienta i TGS. Ticket zaszyfrowany kluczem współdzielonym przez TGS i serwer usług. Zawiera: ID klienta, adres klienta, okres ważnośc ,Klucz sesji klientserwer usług.
7. Klient > serwer usług (Ticket + uwierzytelnienie) Uwierzytelnienie zaszyfrowane jest kluczem sesji współdzielonym przez klienta i serwer usług. Zawiera ID klienta i timestamp. Serwer deszyfruje Ticket i uzyskuje klucz sesji klient serwer usług. Następnie przy wykorzystaniu klucza sesji deszyfruje otrzymane uwierzytelnienie i przesyła wiadomość do klienta.
8. Serwer usług > Klient (wiadomosc) Wiadomosc zawiera timestamp otrzymany od klienta powiększony o 1. Całość zaszyfrowana jest kluczem sesji klient serwer usług.
9. Klient deszyfruje wiadomość i sprawdza czy timestamp jest prawidłowy. Jeśli tak klient uznaje serwer usług jako zaufany i rozpoczyna transmisję. Serwer przesyła odpowiedzi na żądania. ŻĄDANIE<>ODPOWIEDŹ

WERSJA 2

1. Klient na swojej maszynie wprowadza login i hasło
2. Hasło jest zabezpieczane przy użyciu jednokierunkowej funkcji skrótu

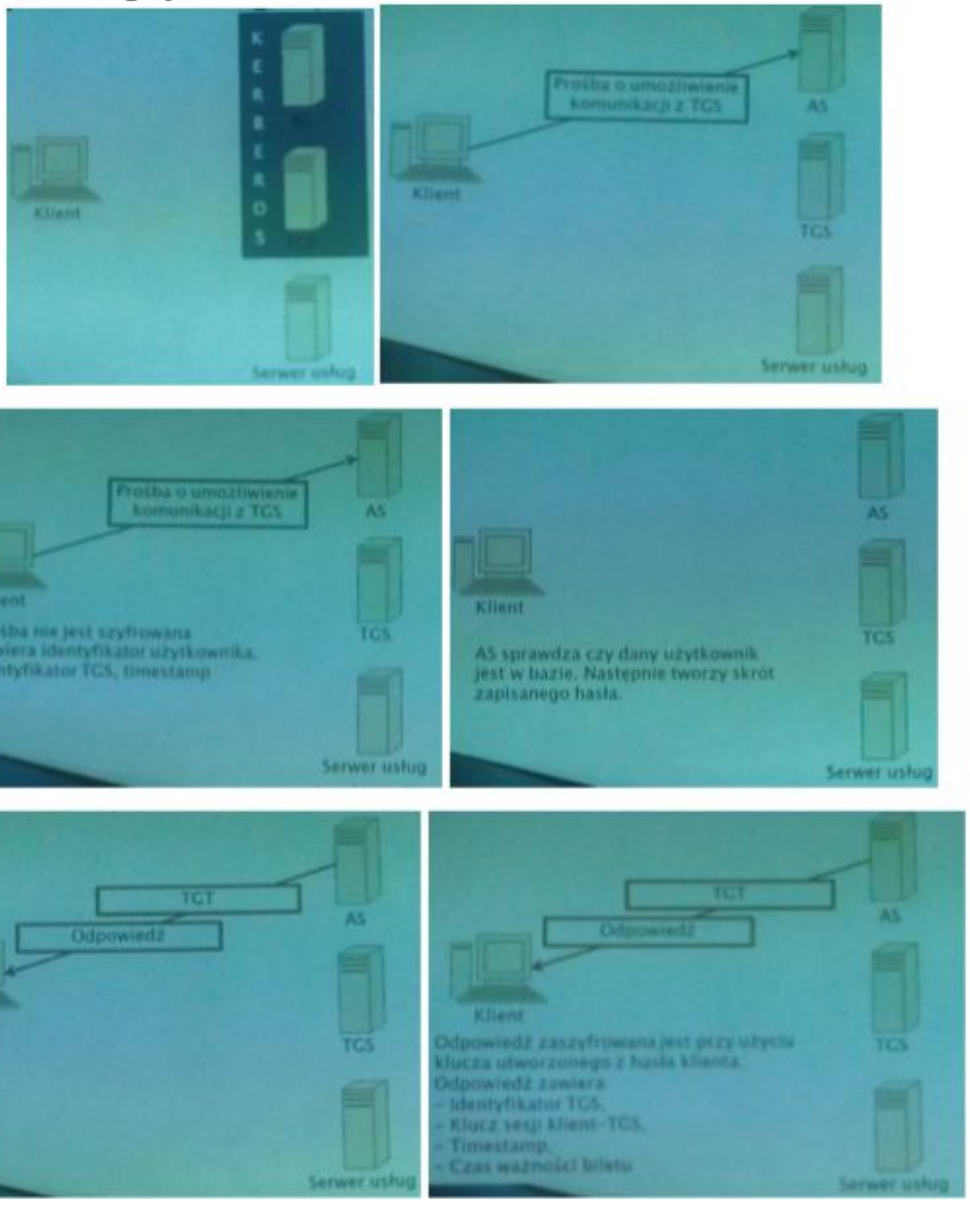
AS + TGS = KERBEROS

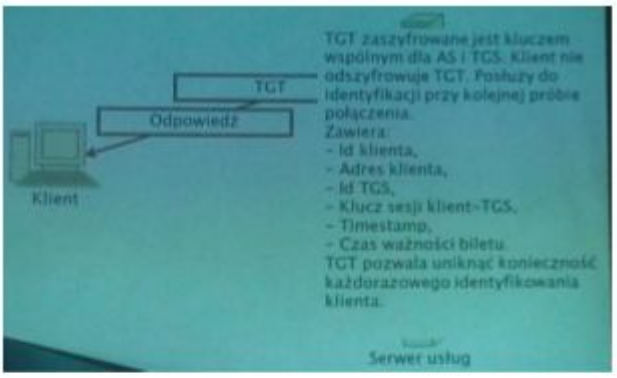
- Klient à AS prośba o umożliwienie komunikacji z TGS. Prośba nieszyfrowana, wysyłana jawnym tekstem. Zawiera identyfikator użytkownika, Identyfikator TGS, timestamp (znakowanie czasem)
- AS sprawdza czy użytkownik jest w bazie, następnie tworzy skrót zapisanego hasła
- AS à Klient odpowiedź (1 pakiet) i TGT (2 pakiet) – ticket granting ticket. Odpowiedź zaszyfrowana przy użyciu klucza utworzonego z hasła klienta. Odpowiedź zawiera identyfikator TGS, klucz sesji klient-TGS, timestamp i czas ważności biletu.
- TGT zaszyfrowane jest kluczem wspólnym dla AS i TGS. Klient nie odszyfrowuje TGT. Posłuży do identyfikacji przy kolejnej próbie połączenia. Zawiera: id klienta, adres klienta, id TGS, klucz sesji klient-TGS, timestamp, czas ważności biletu. TGT pozwala uniknąć konieczność każdorazowego identyfikowania klienta
- Klient à TGS: Przesyłane prośba o przepustkę do serwera usług i TGT.
- Prośba o przepustkę zaszyfrowana kluczem sesji (AS). Prośba zawiera identyfikator serwera usług, uwierzytelnienie klienta (identyfikator+IP+timestamp).
- TGT à Klient. Przesyłane klucz sesji i Ticket.
- Klucz sesji zaszyfrowany przy użyciu klucza sesji współdzielonego przez klienta i TGS. Ticket zaszyfrowany kluczem współdzielonym przez TGS i serwer usług. Zawiera id klienta, adres klienta, okres ważności, klucz sesji klient-serwer usług
- Klient à serwer usług. Przesyłany ticket i uwierzytelnienie.
- Uwierzytelnienie zaszyfrowane jest kluczem sesji współdzielonym przez klienta i serwer usług. Zawiera identyfikator klienta i timestamp. Serwer deszyfruje ticket i uzyskuje klucz sesji klient-serwer usług.
- Następnie przy wykorzystaniu klucza sesji deszyfruje otrzymane uwierzytelnienie i przesyła wiadomość do klienta.

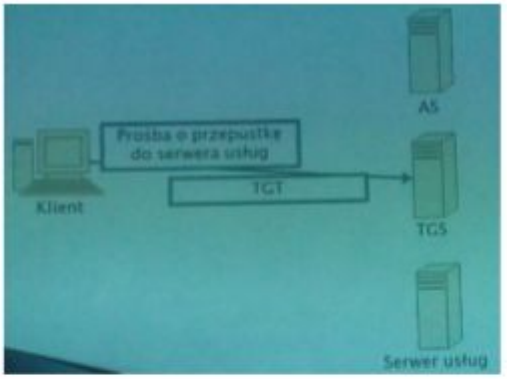
- Klient deszyfruje wiadomość i sprawdza czy timestamp jest prawidłowy. Jeśli tak, to klient uznaje serwer za zaufany i rozpoczyna transmisję żądań. Serwer przesyła odpowiedzi na żądania
- Normalna komunikacja klient – serwer usług, żądania i odpowiedzi

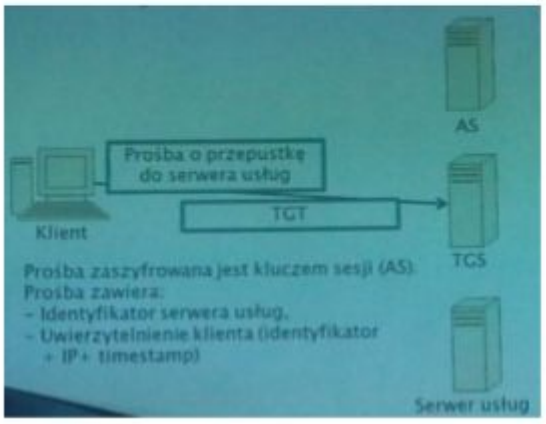
WERSJA 3

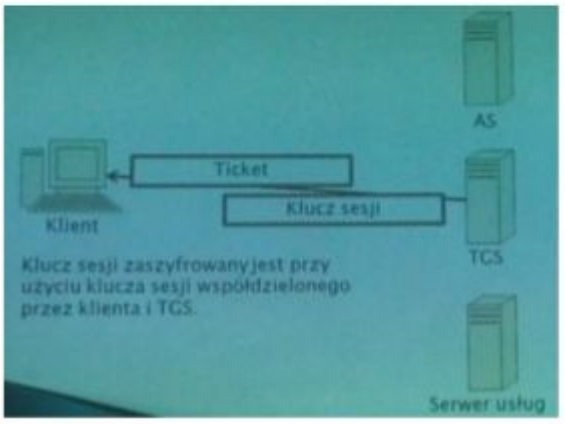
Uwierzytelnianie – algorytm

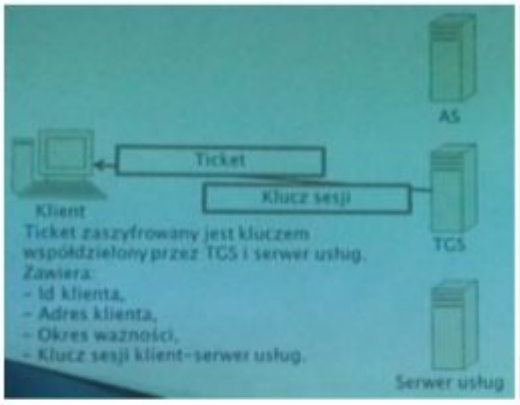


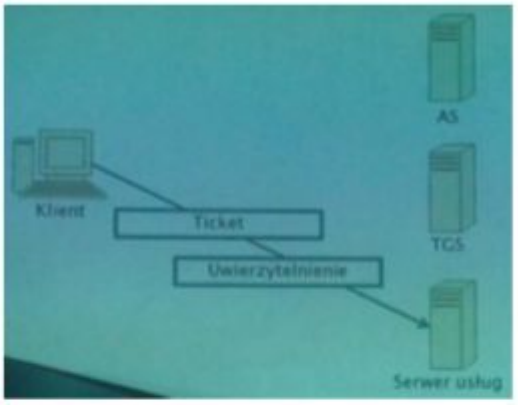

TGT
Odpowiedź
Klient
TGT zaszyfrowane jest kluczem wspólnym dla AS i TGS. Klient nie odszyfrowuje TGT. Posłuży do identyfikacji przy kolejnej próbie połączenia.
Zawiera:
- Id klienta,
- Adres klienta,
- Id TGS,
- Klucz sesji klient-TGS,
- Timestamp,
- Czas ważności biletu.
TGT pozwala uniknąć konieczność każdorazowego identyfikowania klienta.
Serwer usług

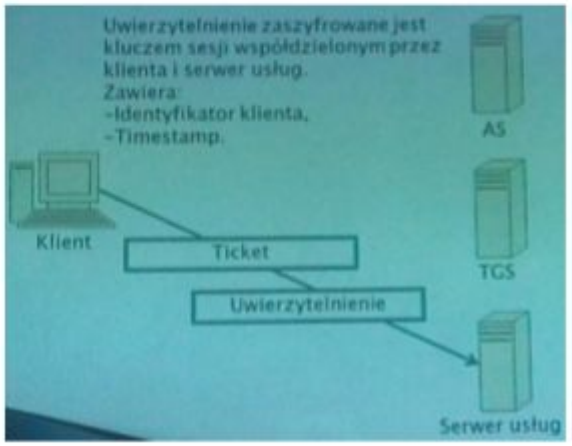

AS
Prośba o przepustkę do serwera usług
TGT
Klient
TGS
Serwer usług

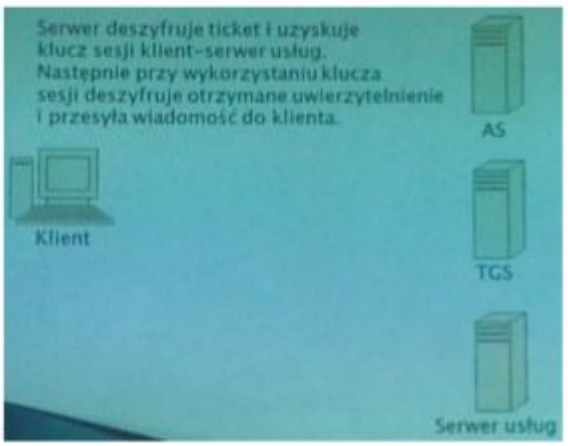

AS
Prośba o przepustkę do serwera usług
TGT
Klient
TGS
Prośba zaszyfrowana jest kluczem sesji (AS).
Prośba zawiera:
- Identyfikator serwera usług,
- Uwierzytelnienie klienta (identyfikator + IP + timestamp)
Serwer usług

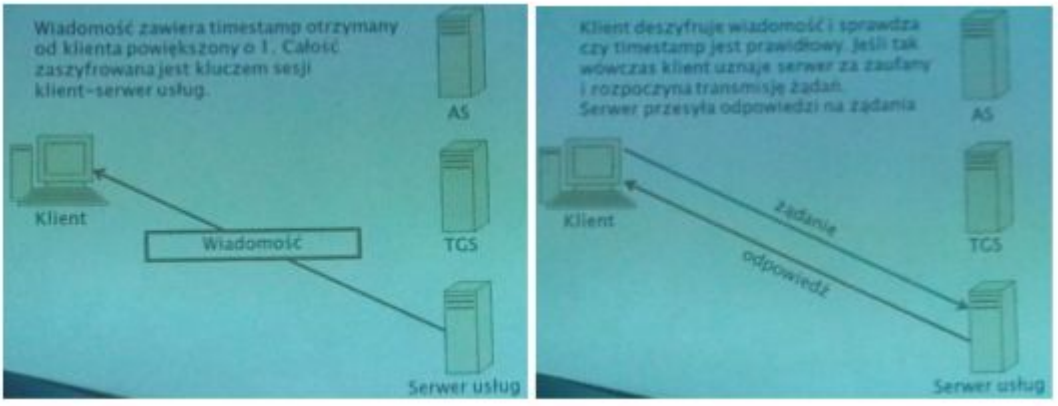

AS
Ticket
Klucz sesji
Klient
TGS
Klucz sesji zaszyfrowany jest przy użyciu klucza sesji współdzielonego przez klienta i TGS.
Serwer usług


AS
Ticket
Klucz sesji
Klient
TGS
Ticket zaszyfrowany jest kluczem współdzielonym przez TGS i serwer usług.
Zawiera:
- Id klienta,
- Adres klienta,
- Okres ważności,
- Klucz sesji klient-serwer usług.
Serwer usług


AS
Klient
Ticket
Uwierzytelnienie
TGS
Serwer usług


Uwierzytelnienie zaszyfrowane jest kluczem sesji współdzielonym przez klienta i serwer usług.
Zawiera:
-Identyfikator klienta,
-Timestamp.
AS
Klient
Ticket
Uwierzytelnienie
TGS
Serwer usług


Serwer deszyfruje ticket i uzyskuje klucz sesji klient-serwer usług.
Następnie przy wykorzystaniu klucza sesji deszyfruje otrzymane uwierzytelnienie i przesyła wiadomość do klienta.
AS
Klient
TGS
Serwer usług



Bezpieczeństwo sieci bezprzewodowych.

Wi-Fi

- Zestaw standardów stworzonych do budowy bezprzewodowych sieci komputerowych
- **Wi-Fi to nie Wireless Fidelity (niektórzy tak twierdzą)**

802.11

- Grupa standardów definiujących warstwę fizyczną i podwarstwę MAC sieci WLAN
- Utworzone i zarządzane przez IEEE.
- Pierwszy standard w 1997 r.
- Half-duplex
- Brak koncesjonowania częstotliwości – ograniczenie mocy, np. w Polsce 100 mW dla 2.4 GHz
- Mechanizm dostępu do medium – CSMA/CA
- RTS/CTS

802.11 – pasmo ISM

- Industrial, Scientific, Medical
- Pasmo nielicencjonowane
- Dla sieci bezprzewodowych
- Pasmo 2,4 GHz oraz 5 GHz

802.11 – pasmo ISM 2,4 GHz

- 14 kanałów
- Odstęp 5 MHz (z wyjątkiem kanału 14)
- Szerokość kanału 20 MHz (zazwyczaj)
- Problem wzajemnego zakłócania
- Stosowanie kanałów o pełnej separacji – 3 sieci dla kanału 20 MHz i jedna dla kanału 40 MHz
- Dostępność kanałów: Polska 1-13, USA 1-11, Japonia 1-14

802.11 – pasmo ISM 5 GHz

- 19 kanałów
- Mniejszy zasięg niż 2,4 GHz
- Brak wzajemnej interferencji

Zalety i wady sieci bezprzewodowych

- Stosunkowo mały zasięg
- Połączenia na dalekie odległości mogą okazać się niestabilne, gdy odbierany sygnał z punktu dostępowego jest zbyt słaby
- Prędkość transmisji danych w przypadku wykorzystania standardu Wi-FI nie dorównuje rozwiązaniom kablowym
- Mniej bezpieczne od sieci kablowych, przez co konieczne jest stosowanie dodatkowych zabezpieczeń, które dodatkowo zmniejszają prędkość przesyłu
- Czasami (szczególnie w miastach) przesył może być wzajemnie zakłócany przez dużą liczbę urządzeń działających na tych samych kanałach
- Prędkość transmisji zależy od odległości między urządzeniami komunikującymi się
- Bardzo podatne na zakłócenia

AccessPoint (AP) – punkt dostępu, urządzenie zapewniające bezprzewodowy dostęp do sieci

Tryby działania karty sieciowej

- managed/active – przyjmowanie pakietów adresowanych bezpośrednio do karty
- monitor – przyjmowanie wszystkich pakietów, niezależnie od tego, do kogo były adresowane, oraz w jakiej sieci lokalnej był adresat

Rodzaje sieci bezprzewodowych

- sieć niezabezpieczona
- sieć niezabezpieczona z wyłączonym nadawaniem SSID
- sieć pozornie niezabezpieczona – filtrowanie adresów MAC (whitelist / blacklist)
- sieć jawnie zabezpieczona kluczem szyfrującym (z tzw. kłódką)
- ** dodatkowo możliwe są zabezpieczenia firewallem

WEP

- Wired Equivalent Privacy
- Szyfr strumieniowy RC4 + suma kontrolna CRC-32
- Dwa warianty WEP-40 i WEP-104
- Klucze WEP: 10/26 cyfr heksadecymalnych (np. 3e414a457b)
- //Skrajnie niebezpieczny – lepiej żeby nikt już nie stosował – złamanie w kilkadziesiąt sekund/kilka minut
- WEP-40: 24 bit – IV (initiation vector), 40 bit – hasło w zapisie heksadecymalnym
- Klucz IV przesyłany jawnie celem umożliwienia odszyfrowania danych
- 24-bitowa przestrzeń dla wektora jest niewystarczająca by zapewnić jego unikalność – co 5000 pakietów wektor IV powtarza się
- Wykorzystując pakiety z tymi samymi IV możemy rozszyfrować hasło („related key”)

WPA/WPA2 (Personal)

- Skrót of WiFi Protected Access
- WPA – wprowadzony w pośpiechu standard zabezpieczeń kompatybilny z urządzeniami obsługującymi WEP
- WPA2 – ukończony standard wymagający do działania nowych urządzeń

- Samo podsłuchiwanie transmisji (przechwytywanie pakietów) nie pozwala na jej odszyfrowanie
- Ze względu na zmienny w czasie klucz szyfrujący posiadanie przechwyconej transmisji, lecz bez handshake, nie pozwoli na jej rozszyfrowanie
- Naprawienie problemu z kolizją IV
- Lepsze zabezpieczenie integralności pakietów
- Zaawansowane mechanizmy uwierzytelniania
- Podatność na ataki siłowe off-line, w przypadku zastosowania uwierzytelniania z wykorzystaniem PSK (czyli WPA-Personal) także przy użyciu tęczowych tablic (rainbow tables)
- Podatność na siłowy atak on-line, na protokół WPS, pozwalający uzyskać PSK (Access Pointy z przyciskiem parowania i funkcją łączenia przez PIN)
- Podatności kryptograficzne w TKIP
- Dziurawe oprogramowanie Access Pointów

WPA/WPA2 – atak BRUTEFORCE

- Do przeprowadzenia wymagany jest 4-way handshake
- Przestrzeń dopuszczalnych wartości PSK: 8-63 znaki ASCII – sprawdzenie wszystkich kombinacji jest póki co niewykonalne
- W praktyce stosuje się ataki słownikowe
- Alternatywnie: użycie tablic tęczowych wykorzystujących zjawisko kolizji w funkcjach haszujących

https://drive.google.com/open?id=1pO5sP4JRUx7gsDg_uoxIWyVhINrZe13Q

EGZAMINY KTÓRE KIEDYŚ BYŁY?? I BYŁY W FOLDERZE *Egzamin, nie sprawdzane!!!!!!!!!!!!!!!*

https://docs.google.com/document/d/1qd0fNPfr45U4IN0vTcTAidE7X0ea9xem3aAPiLqB8Xo/edit?usp=sharing
https://docs.google.com/document/d/1qd0fNPfr45U4IN0vTcTAidE7X0ea9xem3aAPiLqB8Xo/edit?usp=sharing
https://docs.google.com/document/d/1qd0fNPfr45U4IN0vTcTAidE7X0ea9xem3aAPiLqB8Xo/edit?usp=sharing
https://docs.google.com/document/d/1qd0fNPfr45U4IN0vTcTAidE7X0ea9xem3aAPiLqB8Xo/edit?usp=sharing
https://docs.google.com/document/d/1qd0fNPfr45U4IN0vTcTAidE7X0ea9xem3aAPiLqB8Xo/edit?usp=sharing

Pytanka z poprzedniego roku:
1 termin
1. IPSec + jego protokoły i usługi
2. Klasyczne algorytmy szyfrowania, wymienić i opisać 4
3. NAT opisz, wypisz zastosowanie dla IPv4 i IPv6. Opisz typy 1:1 itp
4. Bezpieczeństwo sieci bezprzewodowych, standardy. Który najlepszy.
5. Kerberos opisz jak wyglada komunikacja.

2 termin
1) VPN - wszystko o nim + rodzaje (Personal i Enterprise) - opisać
2) NAT (to co było na 1 terminie)
3) Wymyśl przykładowy scenariusz ataku na warstwę transportową (wybrać jeden z protokołów np. TCP -> zalewanie SYNami tablicę na serwerze)
4) Ochrona sieci bezprzewodowej (nie tylko WEP, WPA, WPA2, ale także inne trzeba podać np. filtrowanie pakietów etc.)

inne notatki:
https://drive.google.com/drive/folders/1naFkeON-T49I5edJfeIK3O3TIs1giT3k?fbclid=IwAR1ItFquEYTFDZverlVmwyDYozluJr-RxXnDnEd95kz1jYBOj1rADBQURFQ