Podstawowe problemy bezpieczeństwa sieci komputerowych

Zagadnienia

1. Bezpieczeństwo podstawowych protokołów sieciowych
2. Klasyfikacja ataków na środowiska sieciowe
3. Podstawowe metody obrony
4. Narzędzia podnoszące poziom bezpieczeństwa sieci
5. Bezpieczeństwo sieci bezprzewodowych

Bezpieczeństwo modelu OSI i TCP/IP

Bezpieczeństwo aplikacji (usług) sieciowych

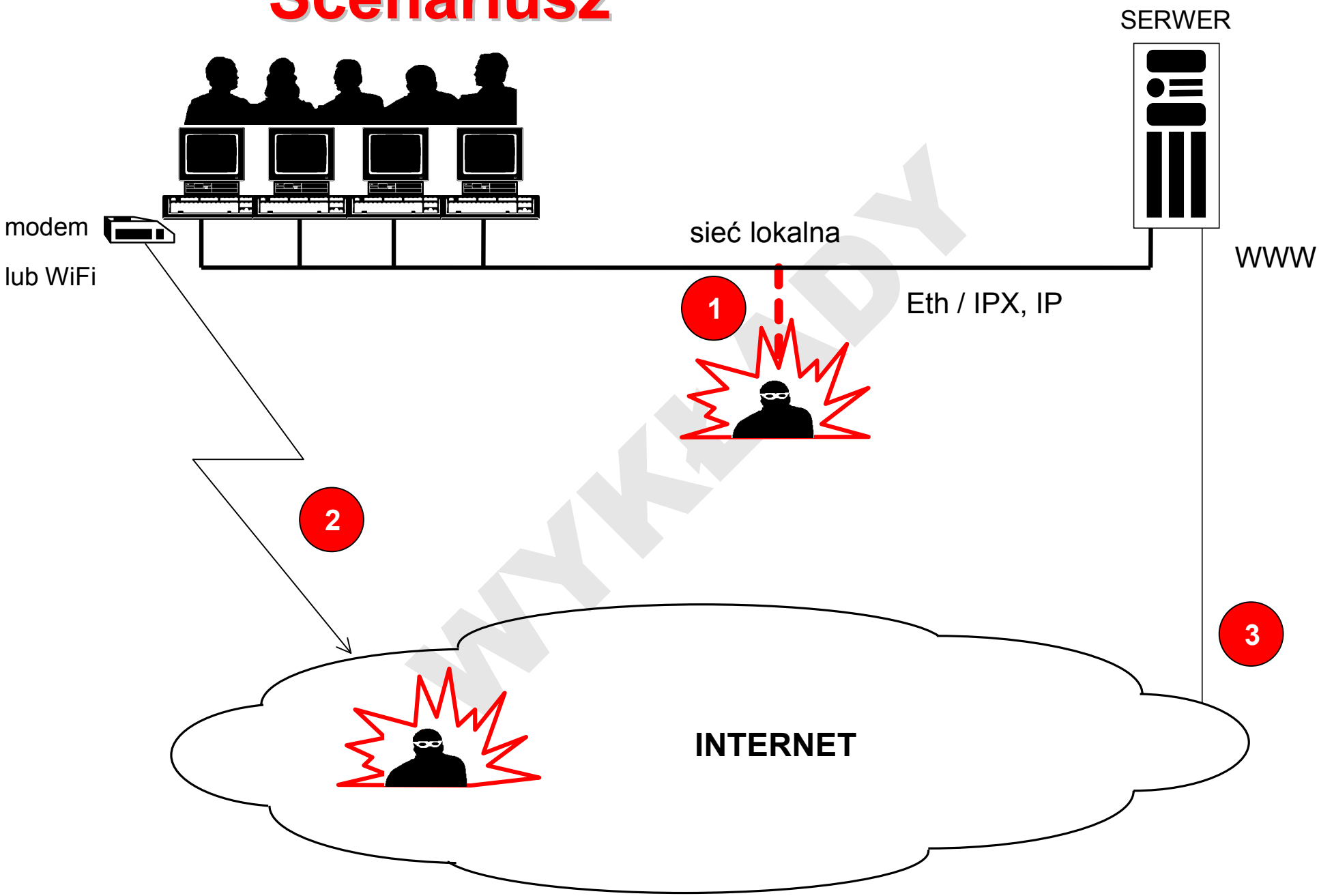
na ogół nie może opierać się
na zaufaniu do warstw niższych

ze względu na

brak mechanizmów
bezpieczeństwa
w niższych warstwach

TCP/IP	ISO/OSI
APPLICATION	APPLICATION
	PRESENTATION
	SESSION
HOST-HOST	TRANSPORT
INTERNET	NETWORK
NETWORK ACCESS	DATA LINK
	PHYSICAL

Scenariusz



Zagrożenia

1. **Podsłuch w segmencie lokalnym**
2. **Niedozwolony dostęp spoza segmentu lokalnego (włamanie)**
3.

Konsekwencje

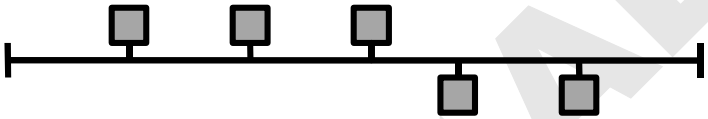
1. **Uzyskanie dostępu do konta w systemie / bazie danych**
   - naruszenie poufności / integralności / dostępności przechowywanych danych
   - rekonfiguracja systemu, sieci
2. **Pozyskanie / modyfikacja transmitowanych danych**

Przyczyny

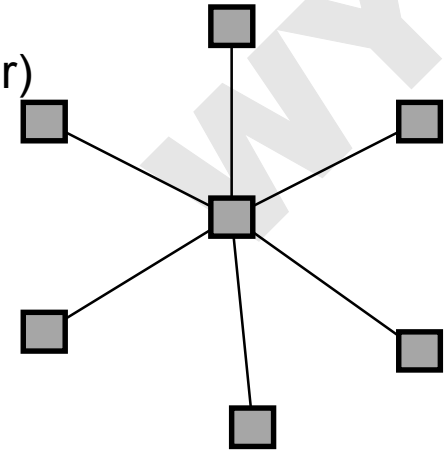
Warstwa fizyczna

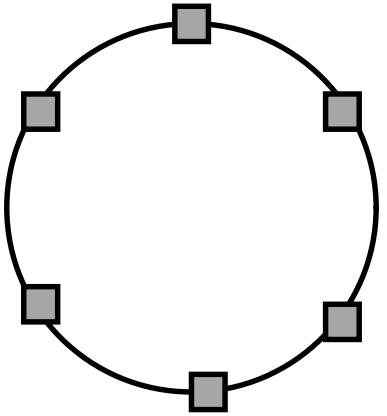
Topologie sieci

magistrala (bus)



gwiazda (star)





pierścień (ring)

Przyczyny

Warstwa łącza danych

Architektura sieci Ethernet

- ruch rozgłoszeniowy, współdzielenie medium (topologia logiczna)
- adresy rozgłoszeniowe i grupowe
- tryb *promiscuous* pracy karty sieciowej
- liniowe sumy kontrolne (CRC)

Urządzenia sieciowe

- mosty i przełączniki – mostowanie transparentne (TB) i źródłowe (SR)
- automatyka obsługi dowolnych stacji i współpracy z innymi mostami STP

Przyczyny

Warstwa sieciowa

- datagramy IP – semantyka bezpołączeniowa i zawodna transmisja
- wsparcie dla adresacji: ARP, RARP
- routing dynamiczny
- kapsułkowanie (kopertowanie) pakietów

Warstwa transportowa

- mechanizmy sterowania przepływem

Warstwa aplikacyjna

- popularne protokoły (telnet, ftp, POP, IMAP) przesyłają dane jawnie
- mało wiarygodne mechanizmy uwierzytelniania

Warstwa sieciowa

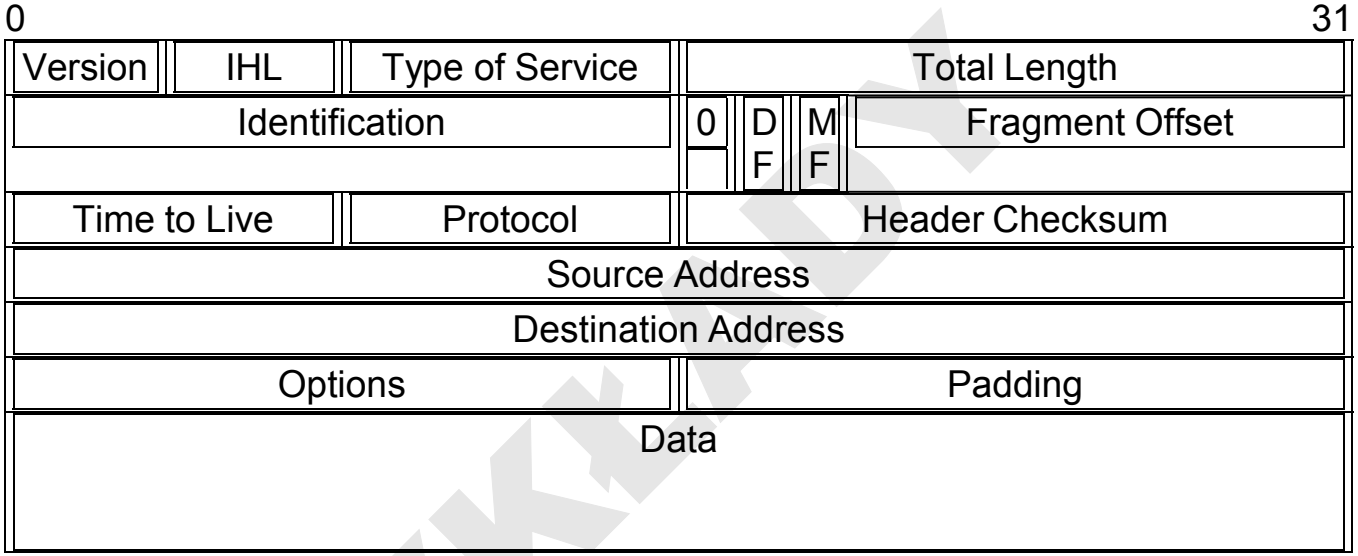
Protokół IP (*Internet Protocol*)

Semantyka bezpołączeniowa:

- brak gwarancji dostarczenia datagramu do odbiorcy
- brak gwarancji zachowania kolejności dostarczania datagramów
- brak kontroli duplikacji datagramu
- jedynie kontrola integralności datagramu (suma kontrolna)

Warstwa sieciowa

PDU protokołu IP v.4 (RFC-791)



IHL = IP Header Length – w jednostkach 32-bitowych (IHL $\geqslant$ 5)

Warstwa sieciowa

Adresacja IP

- nie ma gwarancji, że pakiet został wysłany z adresu wpisanego w polu *Source Address*
- wiele systemów kontroluje to pole w momencie wysyłania datagramu
- niektórzy dostawcy blokują pakiety z nieprawidłowym adresem źródłowym
- mimo tego nie można polegać na poprawności adresu źródłowego odebranego pakietu
- chyba że mamy do czynienia ze ściśle określonymi i kontrolowanymi okolicznościami

Uwierzytelnianie poprzez wartość pola adresu źródłowego

- wiele protokołów posiada wbudowane takie mechanizmy
- atak może polegać sfałszowaniu adresu źródłowego (*IP spoofing*)
- uwierzytelnianie należy pozostawić warstwom wyższym

Warstwa sieciowa

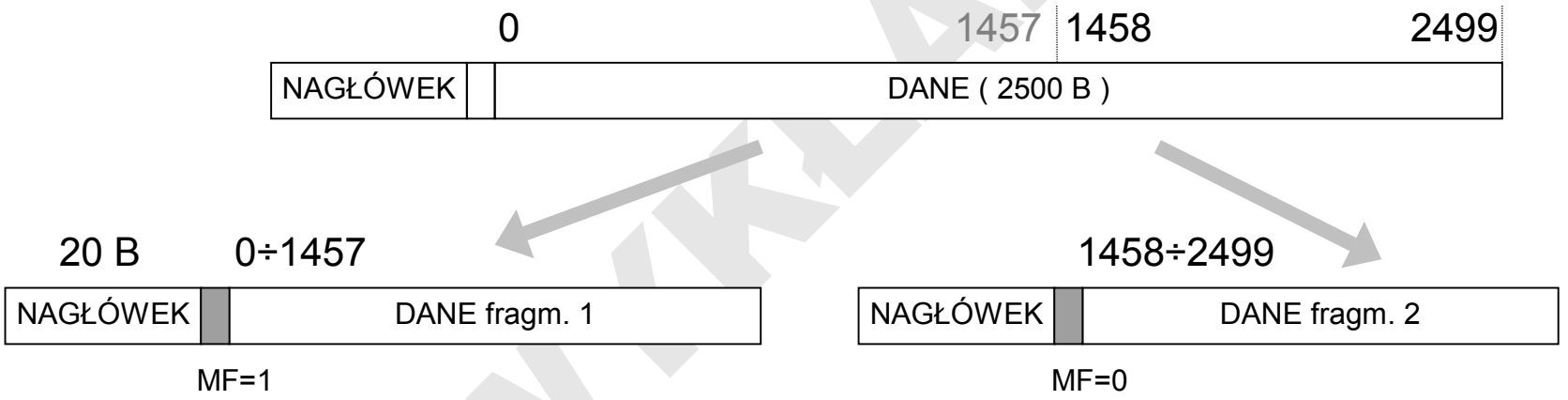
Routing IP

- przeciążony router może odrzucać nadchodzące pakiety
- za retransmisję odpowiadać muszą protokoły warstw wyższych
- jeśli router zostanie „zalany” bardzo dużą masą pakietów (nieistotne czy prawidłowych), to ewentualne przeciążenie doprowadzi do zablokowania komunikacji (pakietów należących do aktywnych sesji – asocjacji IP)
- atak może wykorzystywać chwilową niedostępność pakietów z oryginalnego źródła celem podszycia się pod źródłowy komputer

Warstwa sieciowa

Fragmentacja datagramów IP

- decyduje o niej wartość MTU (*Maximum Transfer Unit*)
- rozmiar fragmentu jest wielokrotnością 8 oktetów (→*Fragment Offset*)



- scalanie fragmentów odbywa się na węźle odbiorcy

Warstwa sieciowa

Fragmentacja datagramów IP

- niektóre stacje IP, w tym zabezpieczenia (filtry pakietów), mogą zachowywać się niepoprawnie atakowane przez niewłaściwie pofragmentowane pakiety [Ziemba, RFC 1858] – *teardrop attack*
- często filtry przetwarzają właściwie (np. odrzucają) tylko pierwszy fragment pakietu
- wartości pola *Fragment Offset* też mogą być wykorzystywane do wywołania błędów scalania w stacji protokołu IP węzła odbiorcy

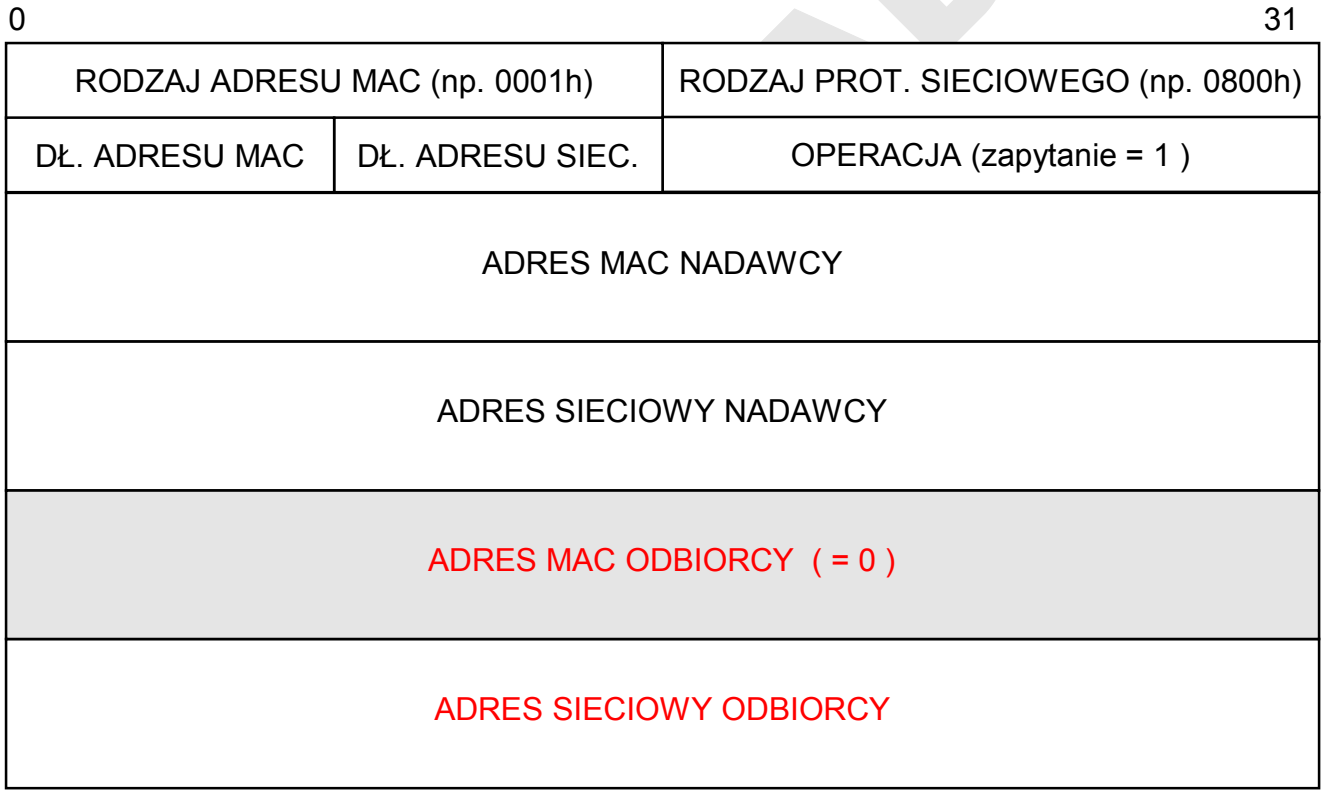
Pakiety rozgłoszeniowe

- ukierunkowane rozgłoszenie może być wykorzystywane do przeprowadzenia ataku typu *DoS*
- wiele routerów posiada funkcję blokowania ruchu rozgłoszeniowego

Warstwa sieciowa

Odwzorowanie adresów

Protokół ARP (*Address Resolution Protocol*)



Warstwa sieciowa

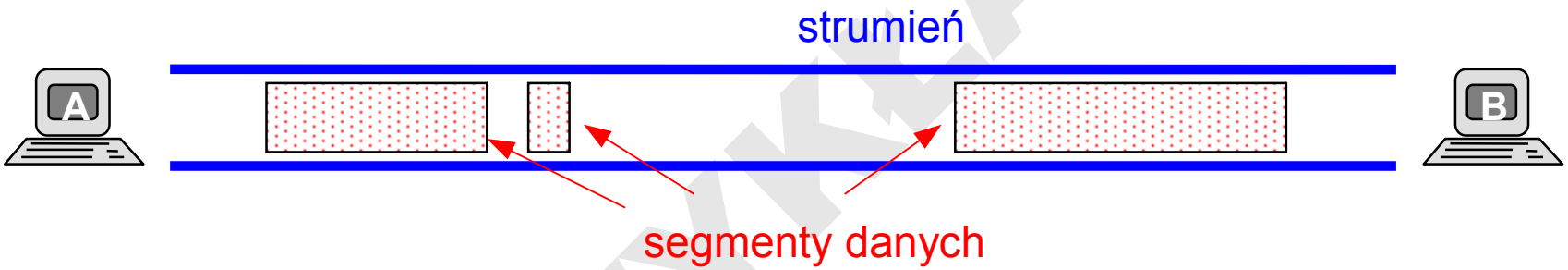
Protokół ARP

- stacja w sieci lokalnej może wysyłać fałszywe zapytania lub odpowiedzi ARP
- kierując w efekcie inne pakiety w swoim kierunku (*ARP spoofing*)
- dzięki czemu napastnik może:
  - modyfikować strumienie danych
  - podszywać się pod wybrane komputery
- można skonfigurować lokalne statyczne mapowanie ARP
- wyłączając przy tym automatyczną obsługę zapytań i odpowiedzi ARP (!)
- o ile to możliwe

Warstwa transportowa

Protokół TCP (*Transmission Control Protocol*)

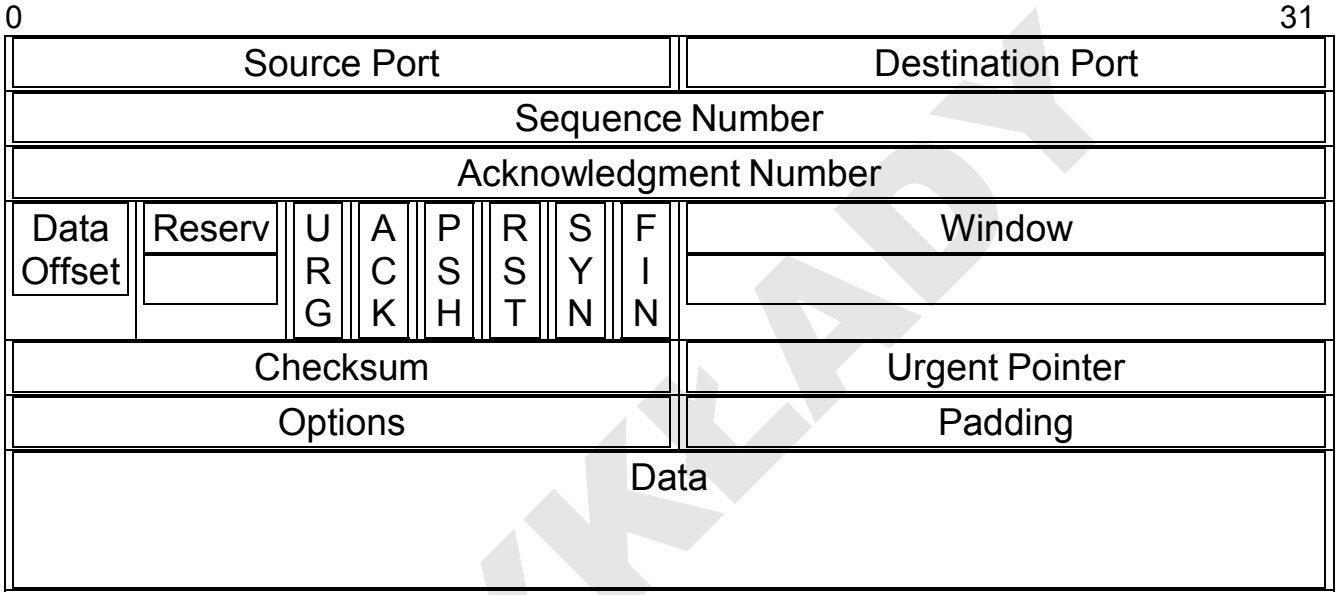
- protokół strumieniowy zorientowany połączeniowo:



Asocjacja $\langle \text{TCP}, \text{IP}_A, \text{port}_A, \text{IP}_B, \text{port}_B \rangle$ reprezentuje połączenie

Warstwa transportowa

PDU protokołu TCP (RFC-793)



URG: Urgent Pointer field significant

ACK: Acknowledgment field significant

PSH: Push Function

RST: Reset the connection

SYN: Synchronize sequence numbers
(pole Sequence Number zawiera Initial Sequence Number)

FIN: No more data from sender

Urgent Pointer – dla URG=1 oznacza miejsce gdzie kończą się dane pilne (offset oktetu o numerze Sequence Number)

Warstwa transportowa

SN = Numer sekwencyjny w nagłówku segmentu określa numer pierwszego oktetu danych przesyłanych w tym segmencie

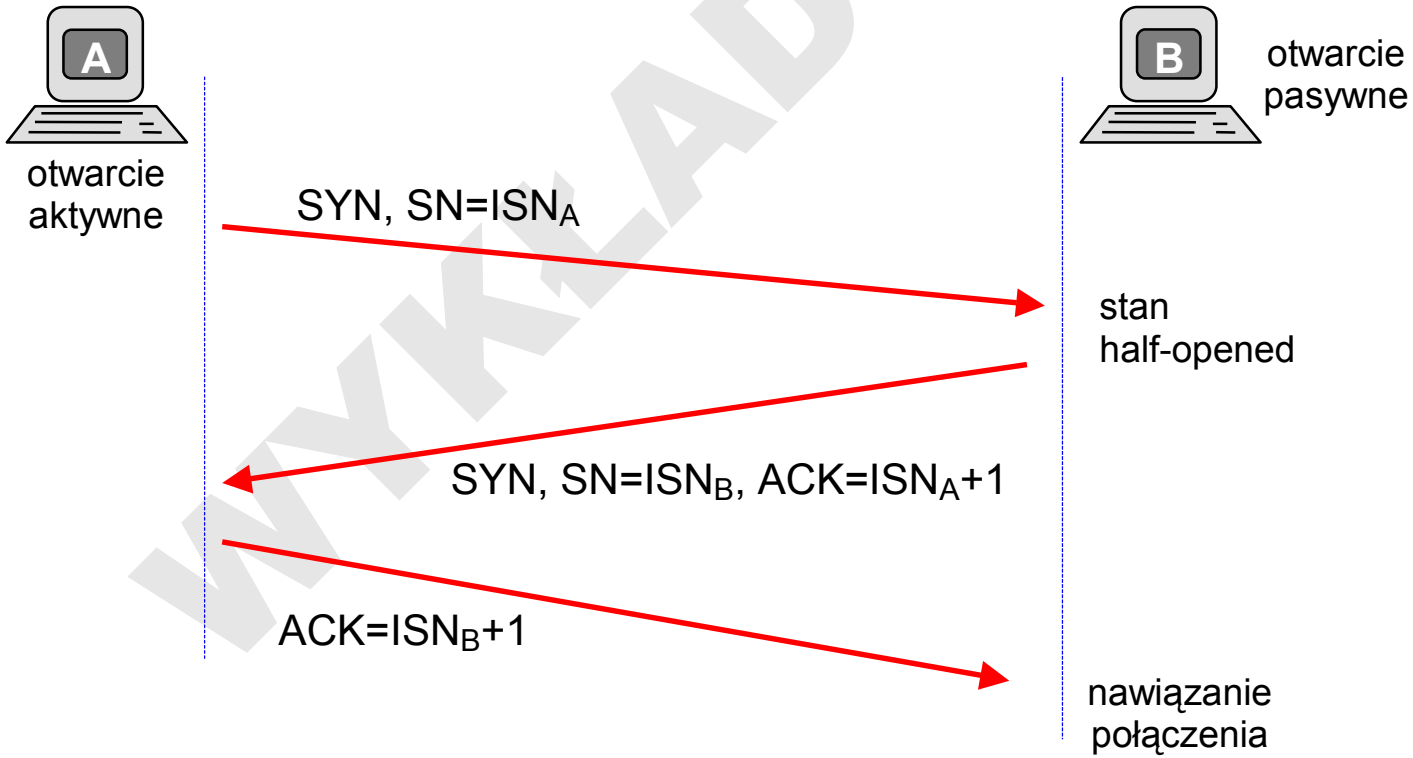
ACK = Numer potwierdzenia – numer sekwencyjny następnego oktetu danych po ostatnim pomyślnie odebranym (numer oczekiwanego oktetu)

ISN = Inicjalny numer sekwencyjny (*Initial Sequence Number*) – początkowy numer sekwencyjny danych przesyłanych w danym połączeniu, ustalany w procesie nawiązania połączenia (w segmencie SYN). Każde połączenie może rozpocząć numerację oktetów danych od arbitralnej wartości (jeśli ISN=0, to pierwszy oktet w całym połączeniu ma numer ISN+1=1). Inicjalny numer sekwencyjny jest ustalany oddzielnie dla obu stron połączenia (w ogólności $ISN_A \neq ISN_B$)

Warstwa transportowa

Nawiązanie połączenia TCP

3-way handshake:



Warstwa transportowa

Nawiązanie połączenia TCP

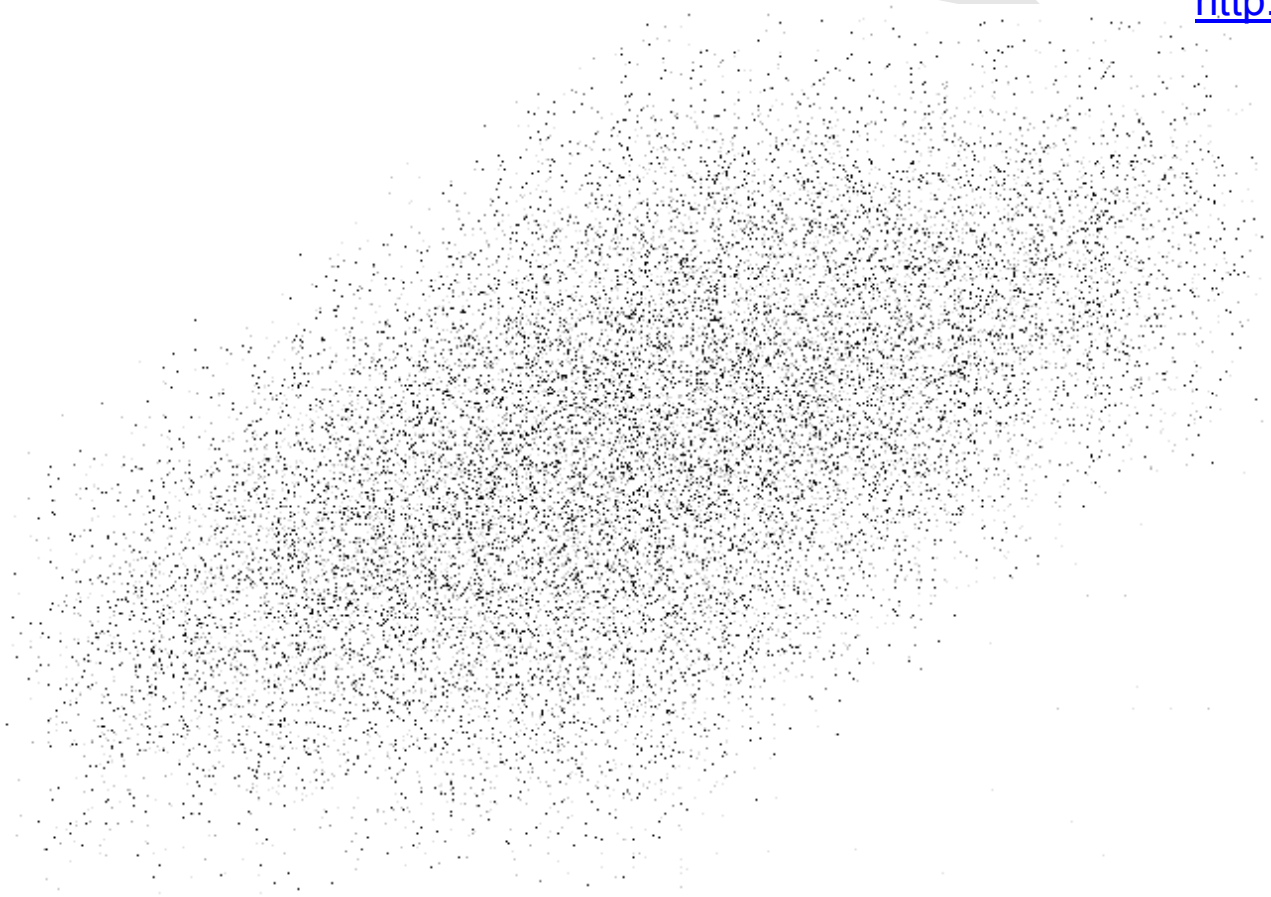
- ataki wykorzystujące zestawione częściowo połączenie (*half-open*) do przechwycenia asocjacji
- na szczęście numery ISN są wybierane pseudolosowo
- na ogół z rozkładem bardzo dalekim od losowego
  - wg sugestii z RFC 793 – licznik ISN jest inkrementowany co 4 μs
  - starsze jądra wywodzące się z BSD (4.2) dokonują inkrementacji o wartość stałą co 1 sek i przy każdym nowym połączeniu
- więc łatwo przewidzieć dla nowych połączeń

Warstwa transportowa

wykres fazowy generatora ISN w systemach:

FreeBDS 4.6, Solaris 7, HPUX 11, OS/400, MacOS X, Netware [Zalewski]

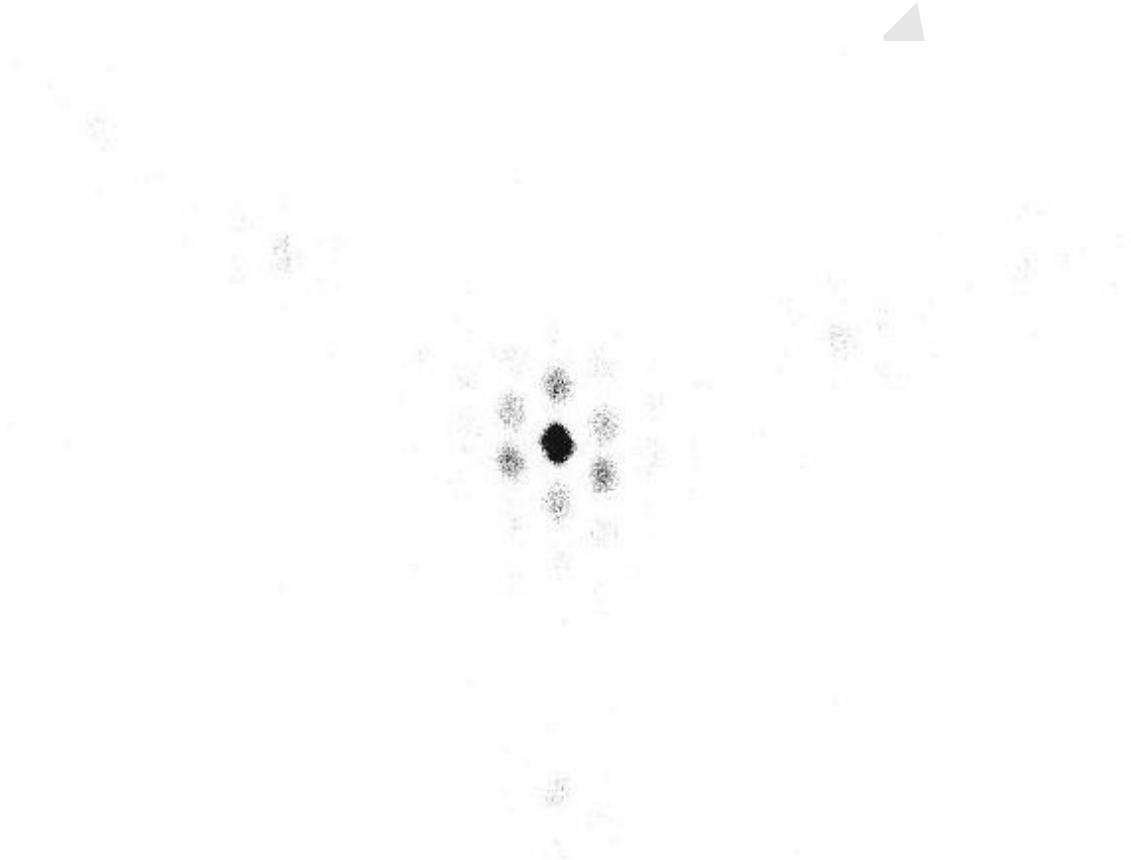
http://alon.wox.org/tcpseq/



to jest prawidłowy generator zgodny z RFC 1948 (sugerowane wykorzystanie MD5)

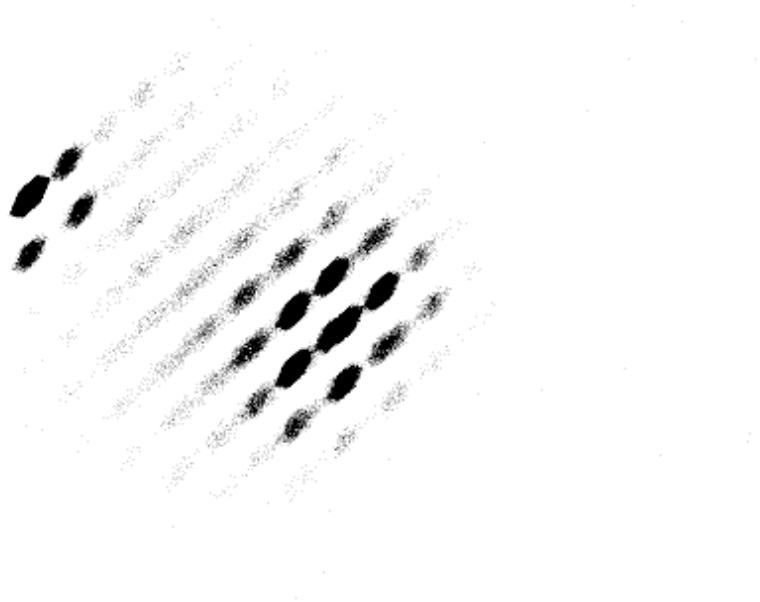
Warstwa transportowa

wykres fazowy generatora ISN w systemie IRIX 6.5.15 (insecure mode)



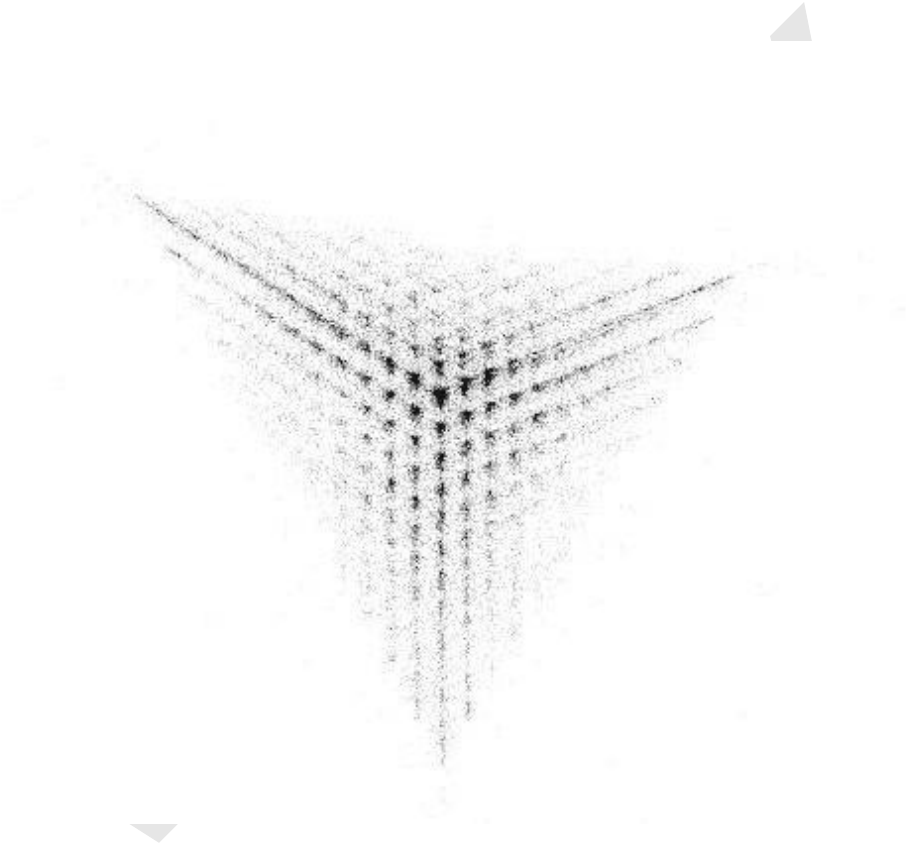
Warstwa transportowa

wykres fazowy generatora ISN w systemie IRIX 6.5.15 (secure mode)



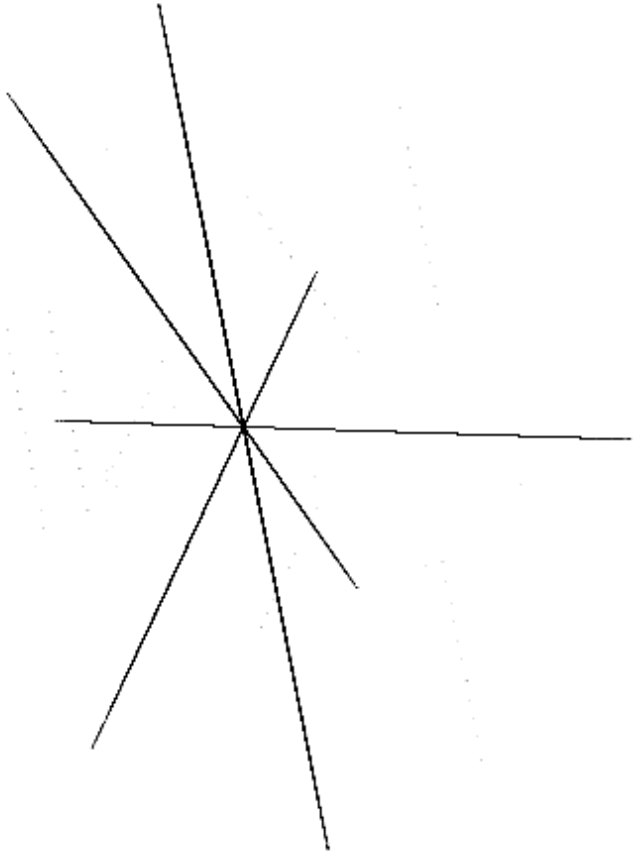
Warstwa transportowa

wykres fazowy generatora ISN w systemie Cisco IOS 12.0 (unpatched)



Warstwa transportowa

wykres fazowy generatora ISN w systemie OpenVMS V7.2

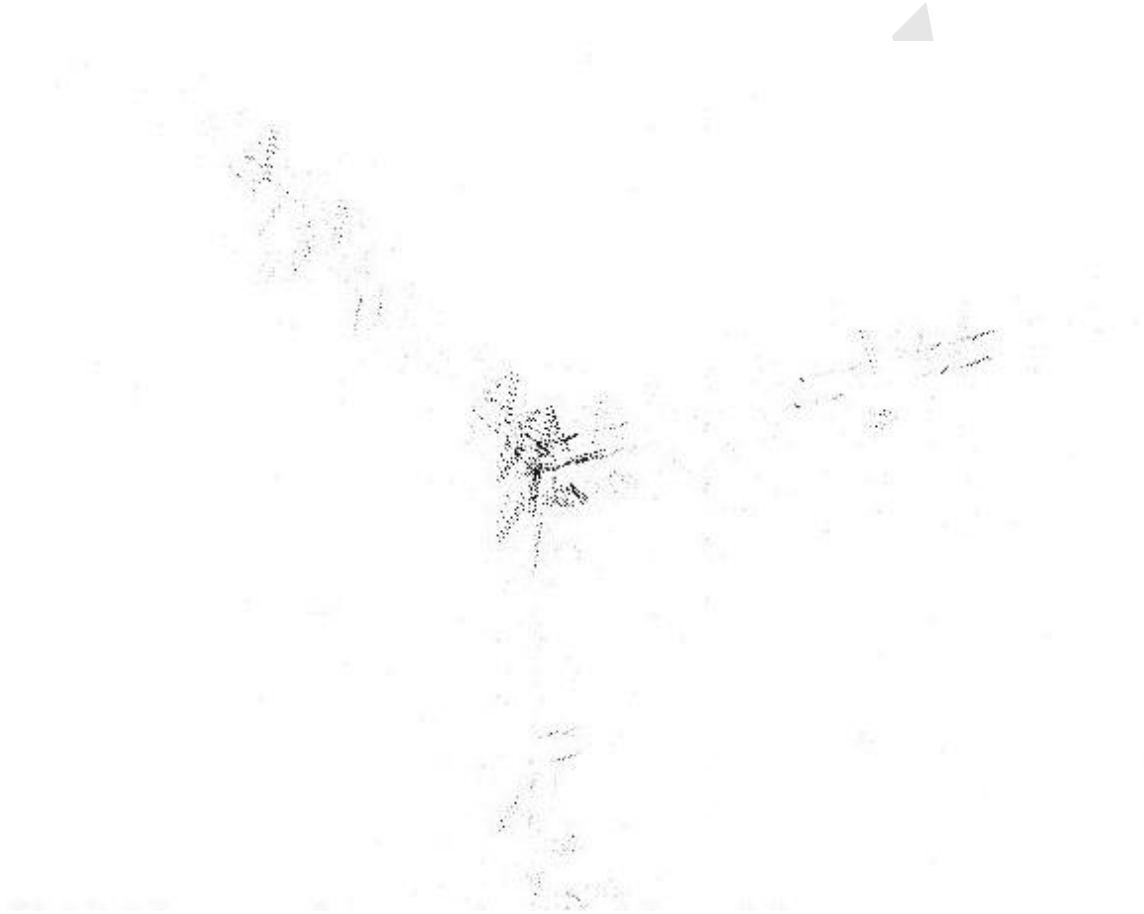


Warstwa transportowa

wykres fazowy generatora ISN w systemie NextSTEP

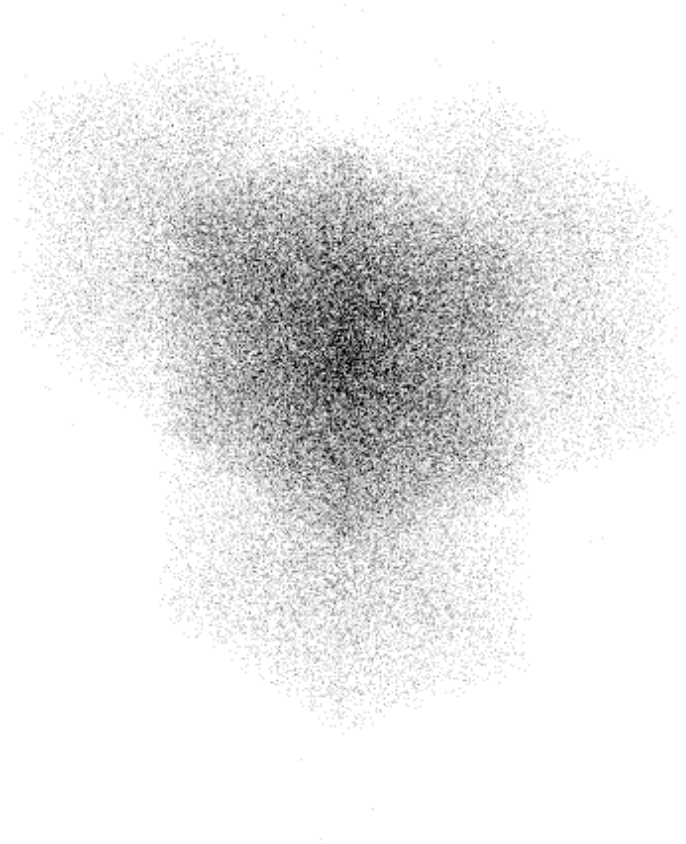
Warstwa transportowa

wykres fazowy generatora ISN w systemie Windows NT4 SP3



Warstwa transportowa

wykres fazowy generatora ISN w systemach Windows 2000 SP2 i Windows XP



Warstwa transportowa

Nawiązanie połączenia TCP

- ataki wykorzystujące stan *half-open* do zalewania odbiorcy segmentami SYN
- duża liczba na wpół nawiązanych połączeń blokuje stację protokołu TCP
- co więcej, zwykle TCP nie raportuje wyższym warstwom (systemowi operacyjnemu) żadnych zdarzeń związanych z połączeniem, które nie jest jeszcze w pełni nawiązane

Warstwa aplikacyjna

Identyfikacja usług

Numer portu

- lokalny numer potu klienta jest niemal zawsze wybierany przypadkowo przez system operacyjny (choć klient może go wybrać sam)
- Unix – tzw. porty uprzywilejowane (systemowe) < 1024
- systemy zdalne polegają na zaufaniu do asocjacji obejmujących te porty
- porty uprzywilejowane może otwierać tylko root
- restrykcja ta jest wyłącznie konwencją – nie należy do specyfikacji protokołów usług
- nie dotyczy systemów innych niż Unix – poleganie na niej nie jest bezpieczne

Warstwa aplikacyjna

Usługi narzędziowe infrastruktury sieciowej

DNS (*Domain Name Service*)

- rozproszona baza danych odwzorowań nazwa ↔ adres
- struktura drzewiasta, poddrzewa mogą być delegowane (np. poddomeny)
- UDP – proste zapytania, TCP – transfer stref DNS (*zone transfer*)
- niektóre zapisy RR (*resource records*) dostarczają informacji użytecznych dla włamywaczy, np. HINFO, WKS, na szczęście rzadko dziś stosowane

Warstwa aplikacyjna

DNS – drzewa mapowań

- dwa oddzielne drzewa – dla mapowania nazw na adresy i adresów na nazwy (zapytania odwrotne – *inverse queries*)
- nie ma wymuszonej relacji między drzewami,
- drzewo mapowań odwrotnych zwykle nie jest równie często aktualizowane
- i ogólnie jest utrzymywane w gorszym stanie
- stanowi to potencjalne ułatwienie w przejęciu kontroli nad częściami drzewa mapowań odwrotnych i, w efekcie, podszywaniu się pod autoryzowane nazwy

Warstwa aplikacyjna

DNS – podstawowe problemy

- udostępnianie informacji użytecznych atakującym
- brak uwierzytelniania w protokole zapytań DNS i transferu stref umożliwia fałszowanie danych (*pharming*)
- podszywanie się pod autoryzowne nazwy kompromituje system uwierzytelniania przez nazwę – możliwa obrona przez dodatkową weryfikację w drzewie mapowań nazw i wykrycie fałszerstwa
- chociaż istnieje przecież możliwość „zatruwania” fałszywymi odpowiedziami cache DNS stacji uwierzytelniającej jeszcze zanim wyśle ona zapytanie o mapowanie – wówczas fałszerstwo nie wyjdzie na jaw

Warstwa aplikacyjna

Usługi narzędziowe infrastruktury sieciowej

BOOTP i DHCP

- udostępniają bogate informacje o infrastrukturze sieciowej
- praktycznie bez uwierzytelniania
- na szczęście na ogół tylko w obrębie sieci lokalnej
- problem bezpiecznej wymiany danych pomiędzy serwerami DHCP a DNS

Ataki

Powszechne techniki ataków na infrastrukturę sieciową wykorzystują głównie niedoskonałości protokołów oraz technologii sieciowych w celu:

- uzyskania danych (*information recovery*)
- podszycie się pod inne systemy w sieci (*host impersonation*)
- manipulacji mechanizmami dostarczania pakietów (*temper with delivery mechanisms*)

Techniki ataków

Sniffing/scanning

- *network sniffing* – pasywny podgląd medium transmisyjnego, np. w celu przechwycenia interesujących ramek (*packet snooping*)
- *network scanning* – wykorzystanie specyfiki implementacji protokołów do sondowania (*enumeracji*) urządzeń aktywnych w sieci, aktywnych usług, konkretnych wersji systemu operacyjnego i poszczególnych aplikacji (program *nmap*)

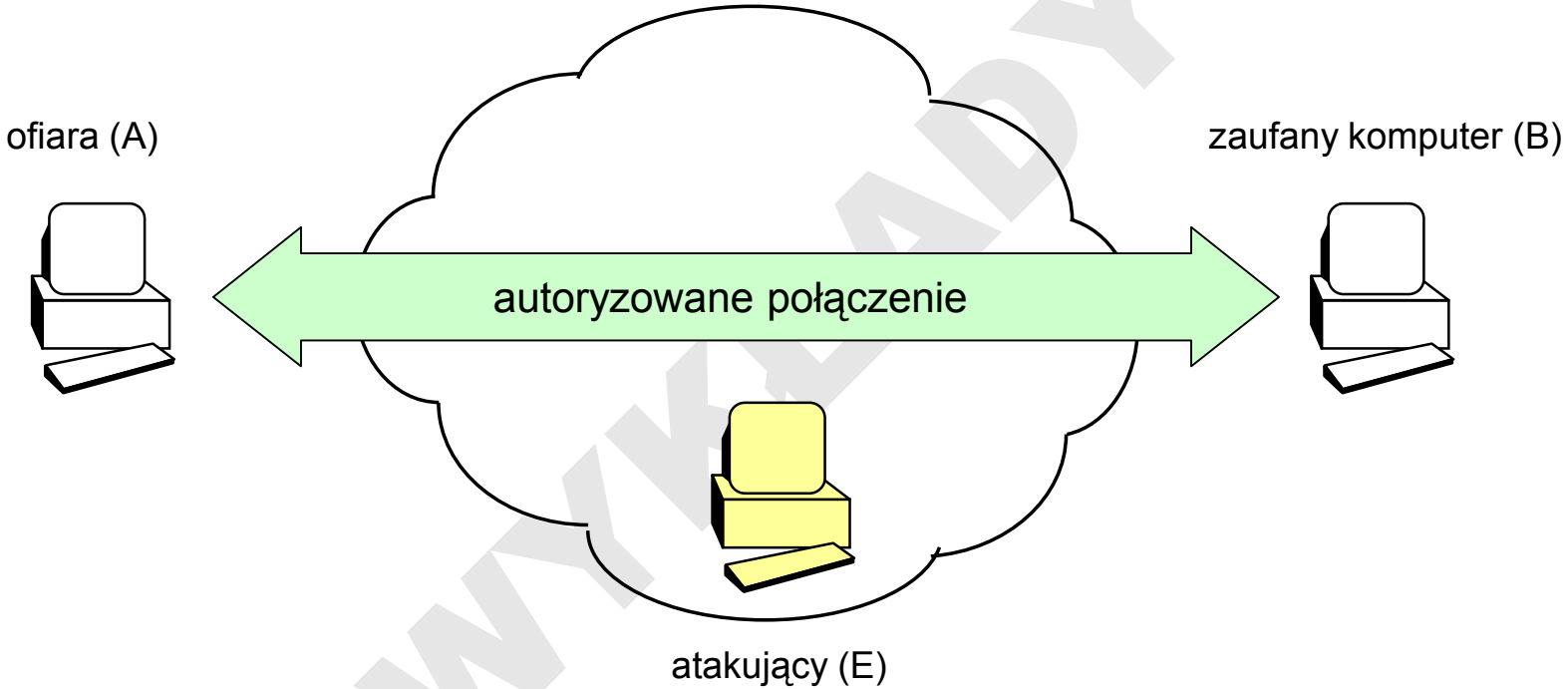
Techniki ataków

Spoofing

- *session hijacking* – przejmowanie połączeń poprzez „wstrzelenie” odpowiednio dobranych pakietów – wymaga dostępu do uprzednio legalnie zestawionego połączenia TCP
- *TCP spoofing* – podszywanie bazujące na oszukaniu mechanizmu *three way handshake*: generowania numerów ISN w rożnych systemach, wykorzystanie ataku w celu oszukania mechanizmów autoryzacji usług r* (autoryzacja przy użyciu funkcji rusersok())
- *UDP spoofing* – prostsze od TCP w realizacji (ze względu na brak mechanizmu szeregowania i potwierdzeń ramek w protokole UDP), użyteczne podczas atakowania usług i protokołów bazujących na UDP np. DNS.

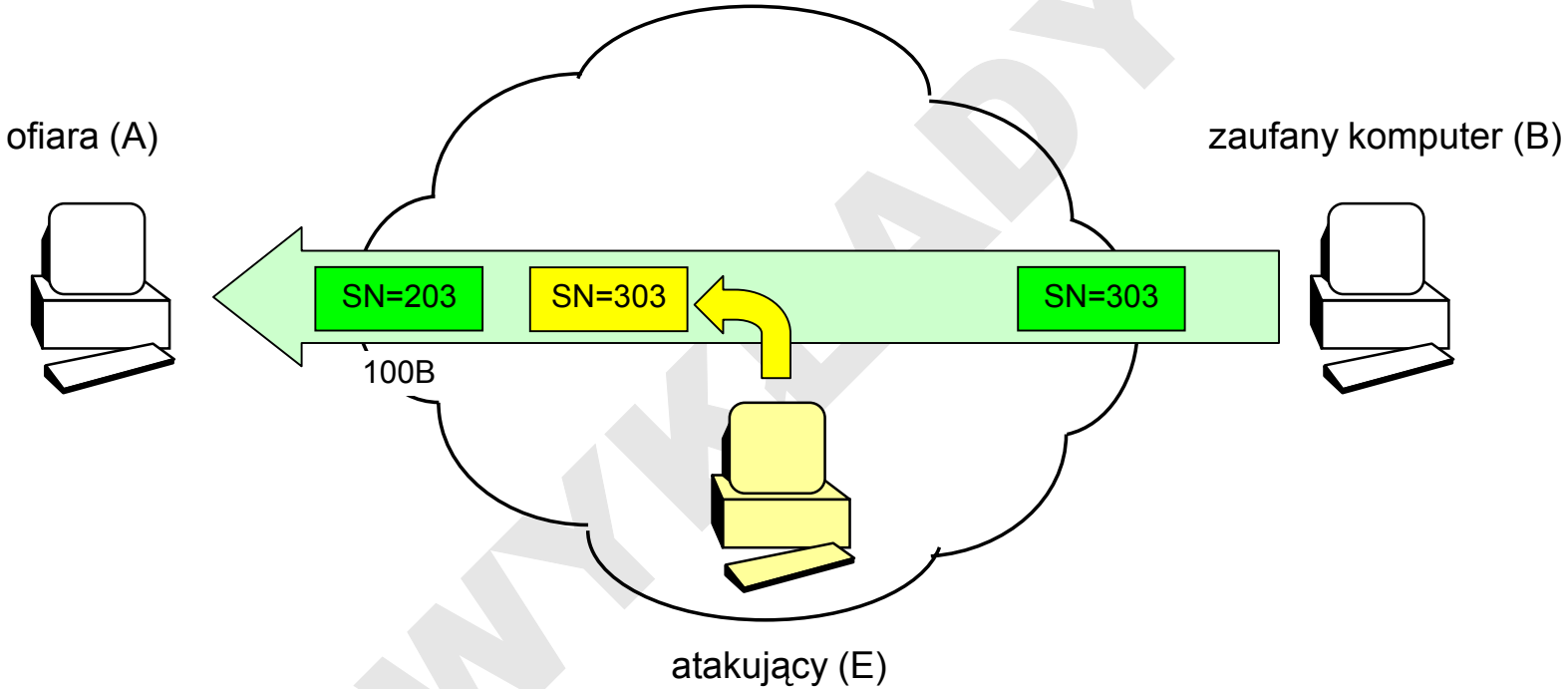
Techniki ataków

Schemat ataku session hijacking (1):



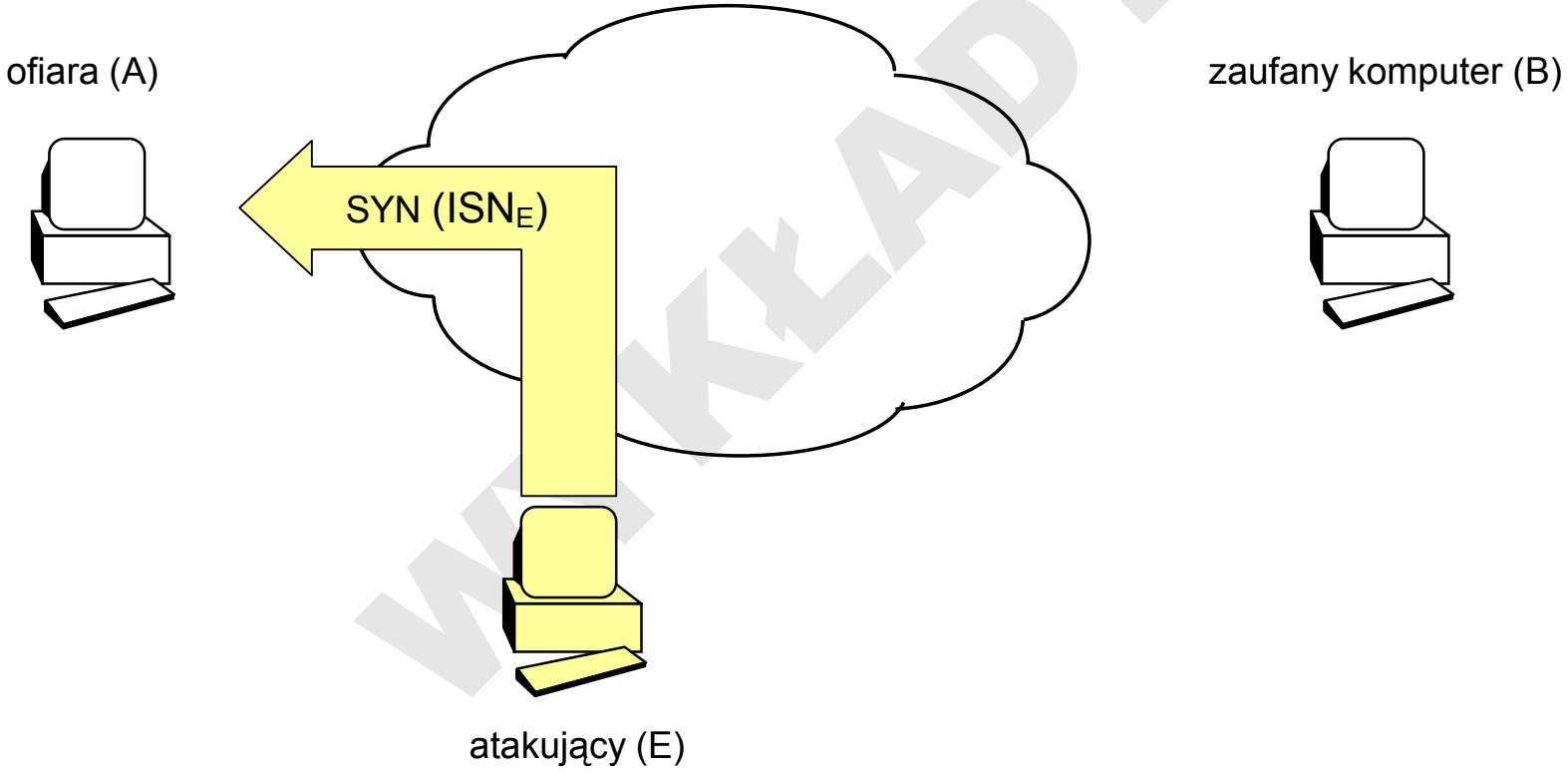
Techniki ataków

Schemat ataku session hijacking (2):



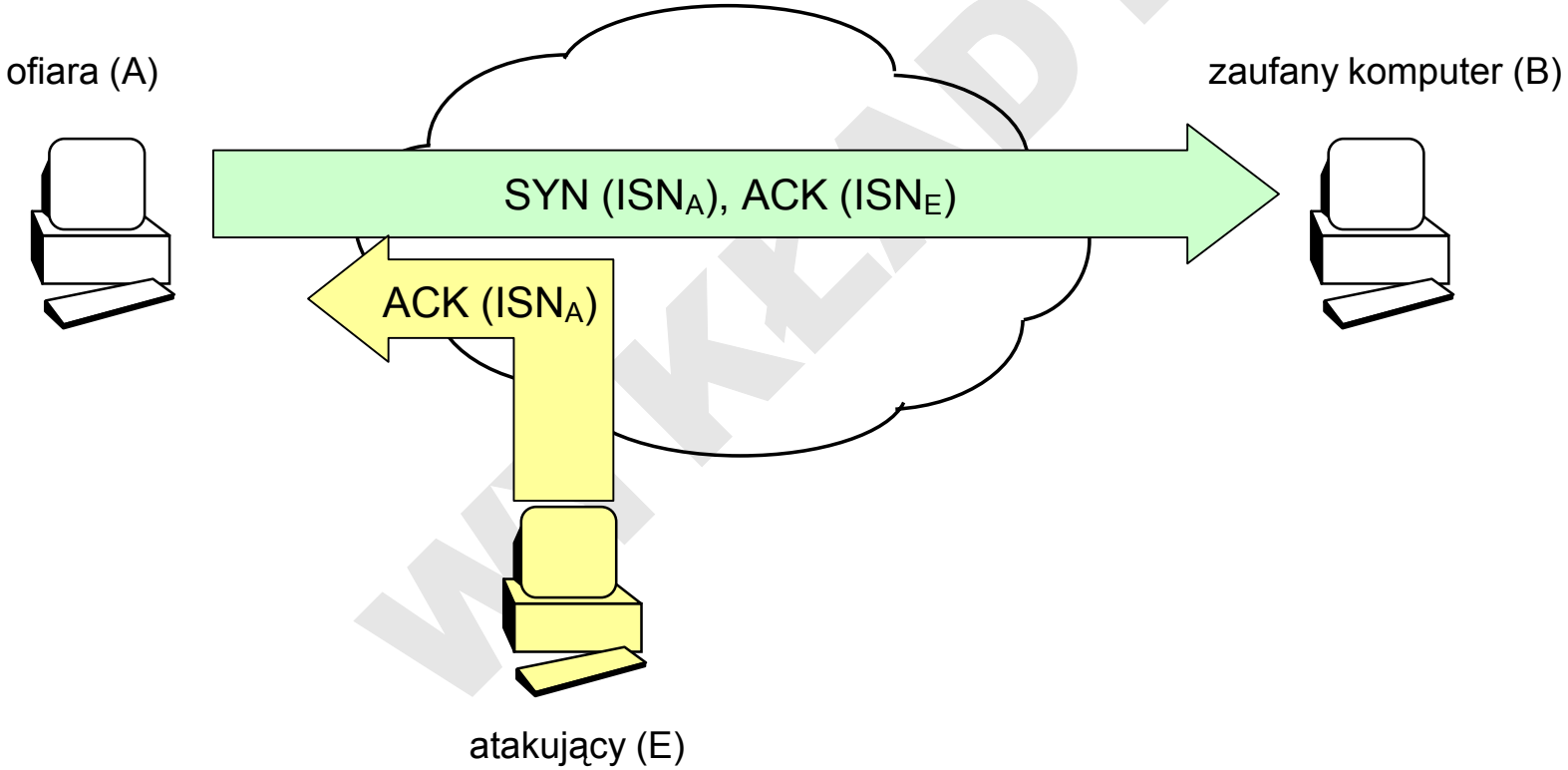
Techniki ataków

Schemat ataku TCP Spoofing (1):



Techniki ataków

Schemat ataku TCP Spoofing (2):



Techniki ataków

Elementy ataku TCP Spoofing:

- wyznaczenie właściwego ISN_A – np. poprzez uprzednie nawiązanie autoryzowanego połączenia na inny port (pozyskanie wcześniejszego numeru ISN'_A)
- celowe uniemożliwienie przetwarzania segmentu SYN (ISN_A), ACK (ISN_E)
- obserwacje:
  - atakujący nie musi mieć dostępu do segmentów autoryzowanego połączenia (*sniffing*)
  - jeśli ma – może podejrzeć numer sekwencyjny (nie musi zgadywać)
  - i podpiąć się na dowolnym etapie już zestawionego połączenia

Pytanie:

- dlaczego akurat usługi r* są szczególnie upodobanym celem ataków?

Techniki ataków

Poisoning

- *ARP spoofing/poisoning* – wykorzystuje zasady działania protokołu ARP, umożliwiając zdalną modyfikację wpisów w tablicach ARP systemów operacyjnych oraz przełączników, a przez to przepełnianie tablic ARP
- *DNS cache poisoning* (*pharming*, także znany jako *birthday attack*) – umożliwia modyfikację wpisów domen w dynamicznym *cache* DNS, co jest niezwykle dużym zagrożeniem w połączeniu z atakami pasywnymi
- *ICMP redirect* – wykorzystanie funkcji *ICMP* do zmiany trasy routingu dla wybranych adresów sieciowych
- ataki na urządzenia sieciowe przy pomocy protokołu SNMP

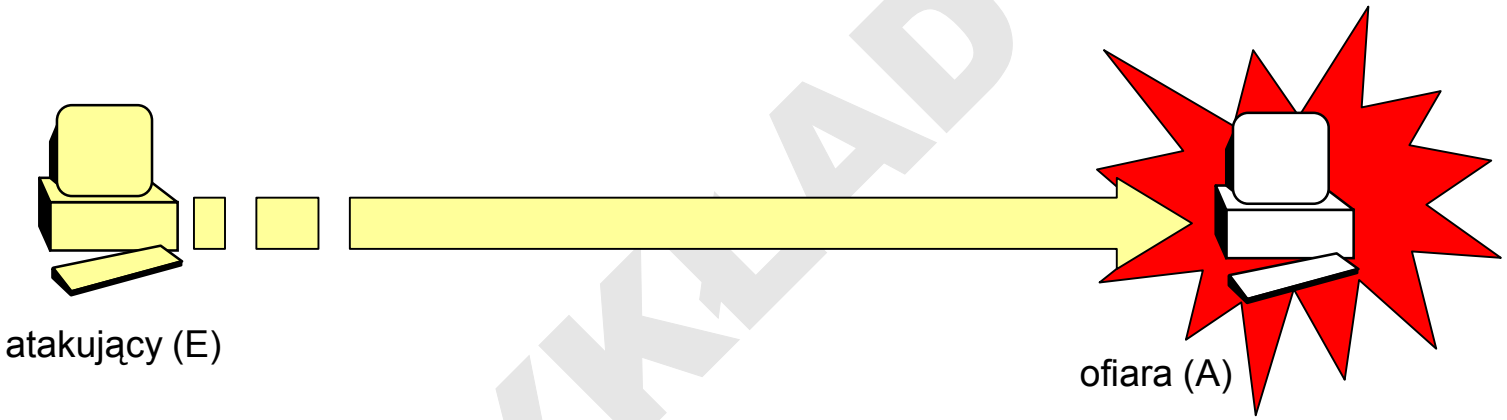
Techniki ataków

Denial of Service (DoS)

- przykłady najpopularniejszych ataków:
  - SYN flood
  - smurf, fraglle
  - land
  - tribal flood (trin00, trinio, trinity v3)
  - subseven, stacheldracht
  - UDP storms (teardrop, bonk)
  - ICMP destination unreachable
  - ...
- wyższe warstwy:
  - e-mail bombing, ...

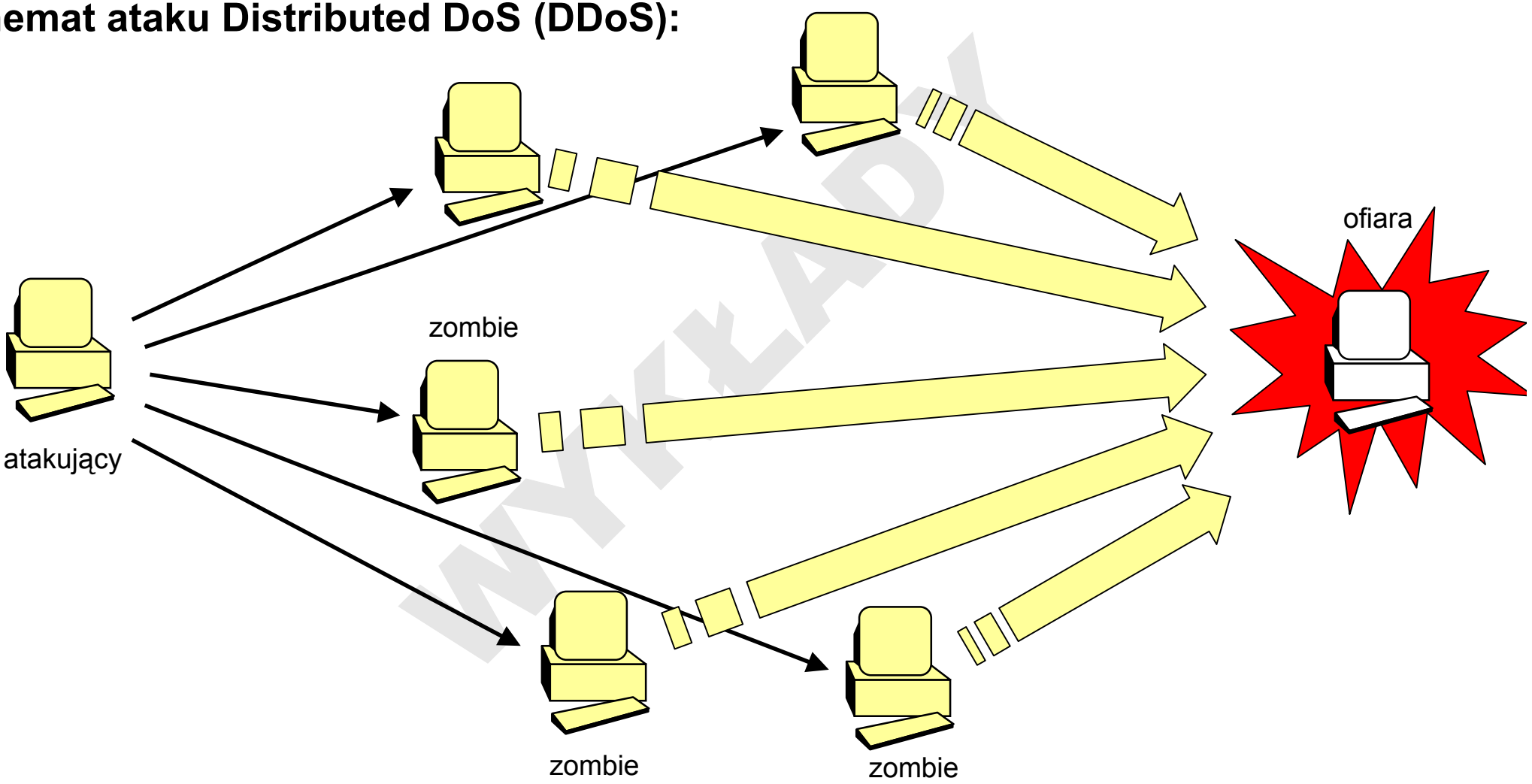
Techniki ataków

Schemat ataku Denial of Service (DoS):



Techniki ataków

Schemat ataku Distributed DoS (DDoS):



Techniki ataków

SYN flood

- atakujący (E) wysyła na adres ofiary (A) dużą liczbę segmentów SYN protokołu TCP adresowanych z dowolnych (nieistniejących) adresów IP
- A odpowiada segmentami SYN/ACK i rozpoczyna oczekiwanie na segmenty ACK (TCP half open)
- w trakcie oczekiwania wyczerpują się zasoby stacji protokołu TCP

w 1997 r. atak SYN flood na WebCom wyłączył z użycia ponad 3000 witryn WWW

Techniki ataków

Ping of Death

- generowanie pofragmentowanych pakietów ICMP przekraczających w sumie 64kB
- scalanie może w niektórych implementacjach powodować błędy prowadzące do zawieszenia stacji IP

Techniki ataków

Smurf attack

- wygenerowanie dużej ilości rozgłoszeniowych (*directed broadcast*) pakietów ICMP echo – ping z adresem IP ofiary ataku jako źródłowym
- ofiara zostanie zalana odpowiedziami ping
- jeśli router przepuszcza ping w ukierunkowanym rozgłoszeniu
- a system operacyjny stacji odpowiada na taki ping

Fraglle attack

- identycznie wykorzystuje usługę echo na UDP

Techniki ataków

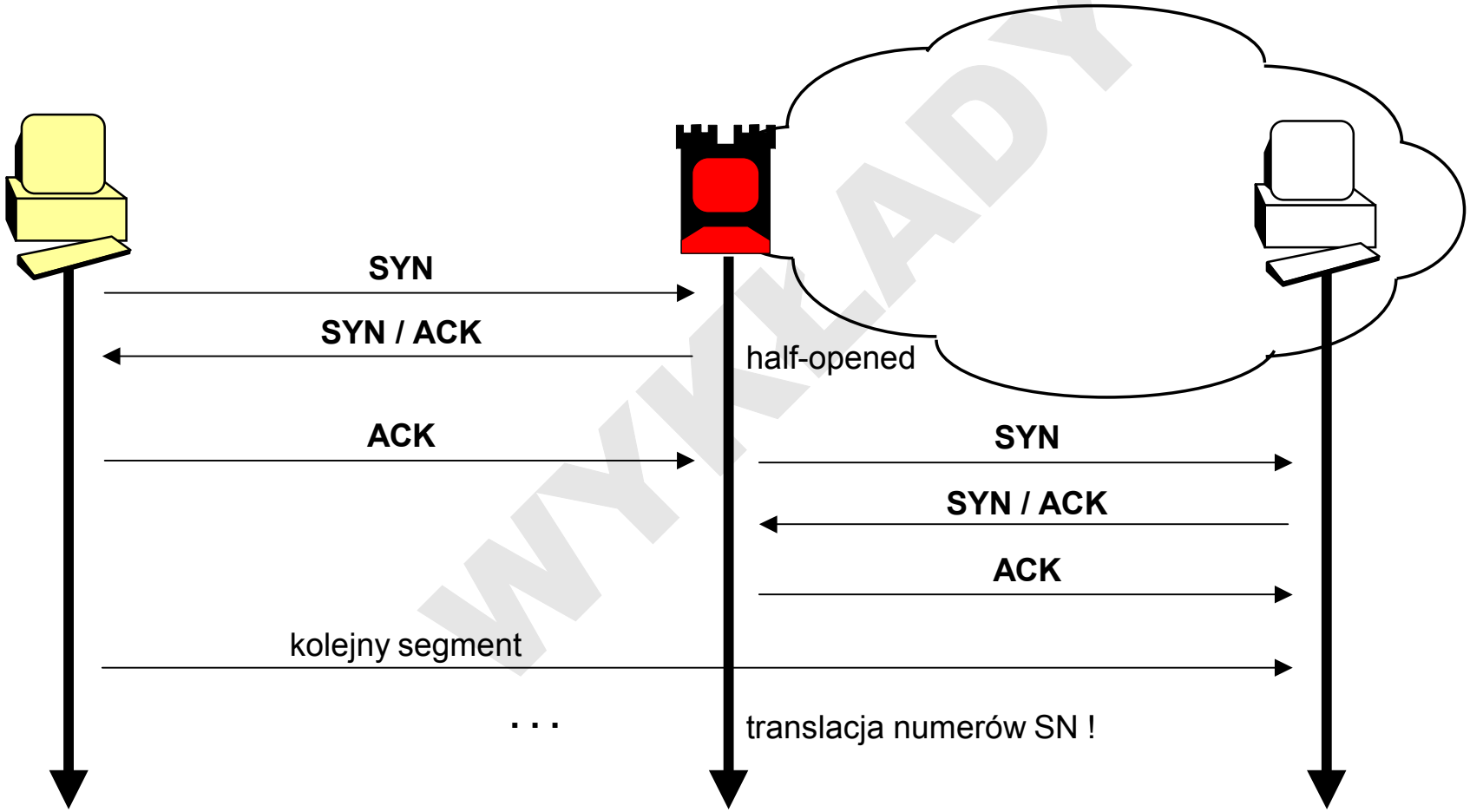
Land attack

- atakujący wysyła segment SYN na adres ofiary podając jej własny adres jako źródłowy
- i nadając ten sam numer portu źródłowego i docelowego
- stacja TCP ofiary nigdy nie zestawi połączenia zapętlając się w nieskończoność
- w niektórych implementacjach może to prowadzić do jej zawieszenia

Metody obrony

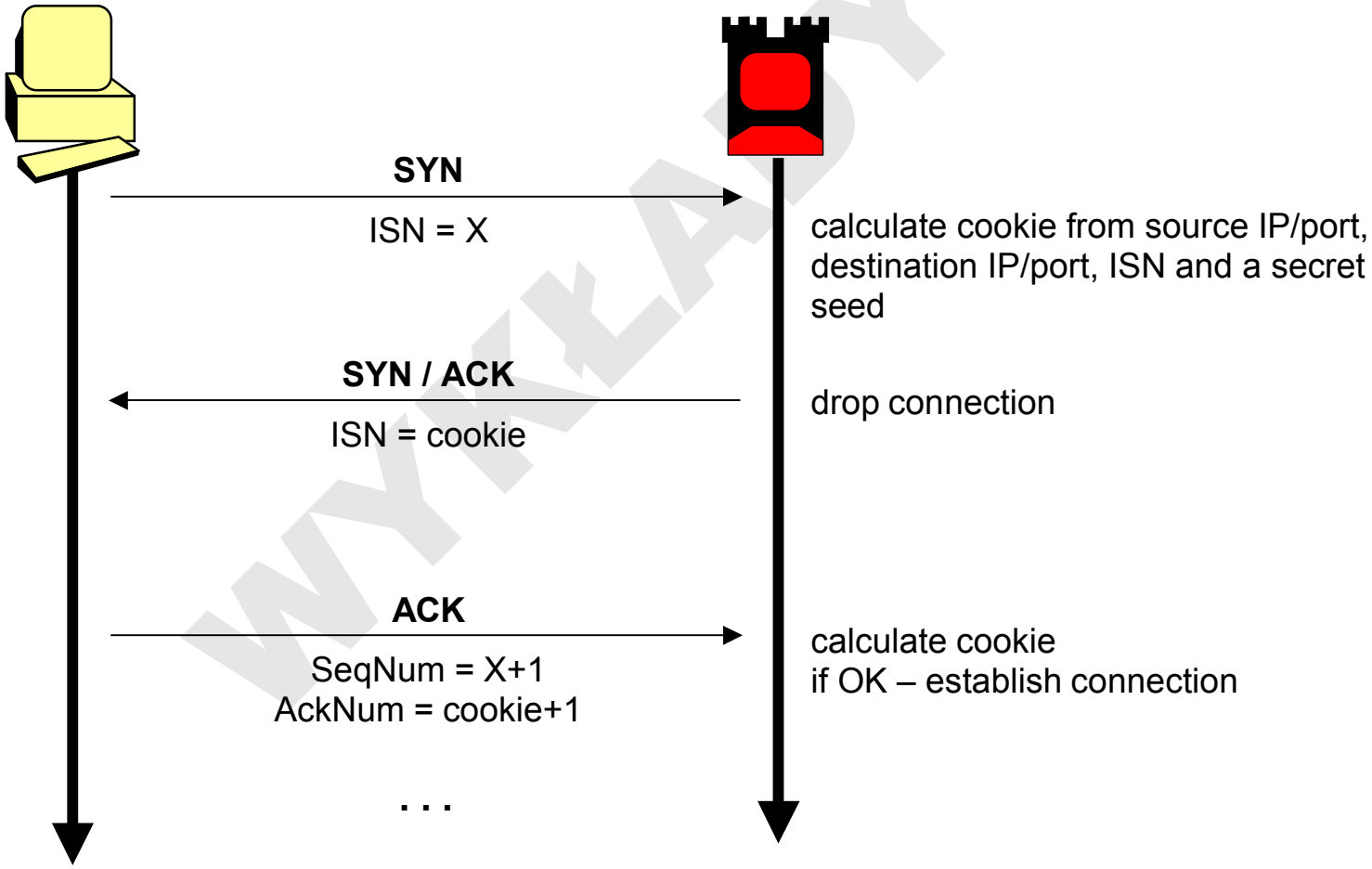
nie ma uniwersalnych metod obrony przez atakami DoS

Obrona przed atakiem SYN flood – SYN Defender



Metody obrony

Obrona przed atakiem SYN flood – SYN cookies



Metody obrony

Ograniczenia SYN cookies

- nie można korzystać niektórych rozszerzeń specyfikacji protokołu IP,

  np. Large Window

http://cr.yp.to/syncookies.html

Metody obrony

Eliminacja możliwości zdobycia hasła użytkownika:

- wyrafinowane systemy uwierzytelniania (hasła jednorazowe, karty identyfikacyjne)
- szyfrowanie komunikacji (układy sprzętowe, pakiety programowe)
- konsekwentna polityka ochrony haseł

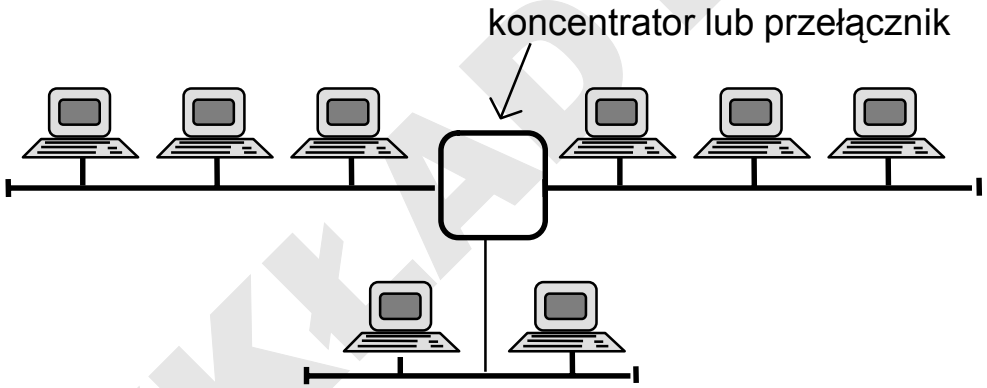
Utrudnianie podsłuchu:

- system okablowania strukturalnego
- mikrosegmentacja sieci, separacja ruchu sieciowego (VLAN)
- szyfrowanie komunikacji

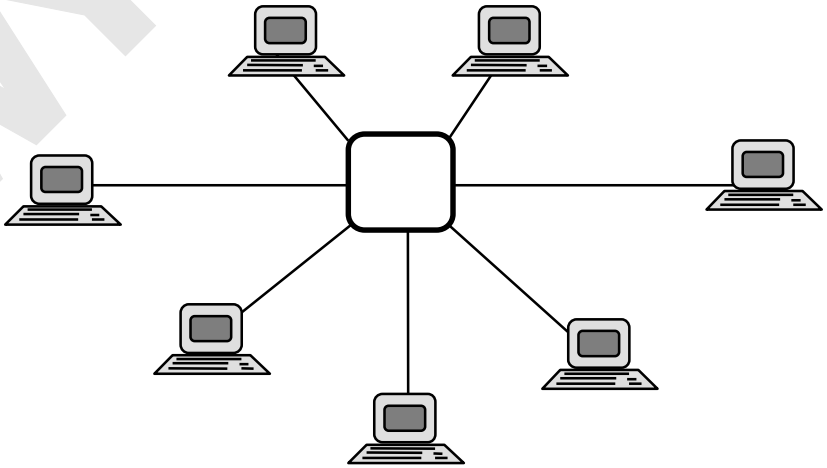
Mikrosegmentacja

SIEĆ JEDNOSEGMENTOWA

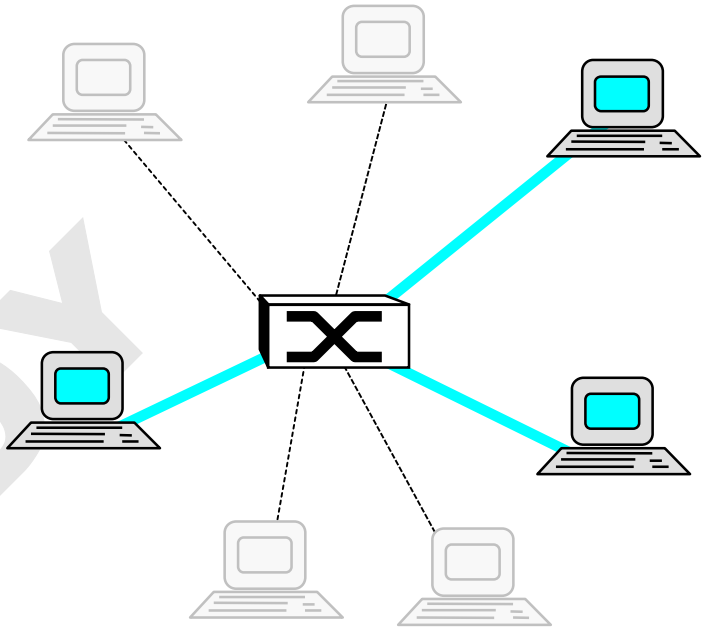
SEGMENTACJA SIECI



MIKROSEGMENTACJA SIECI



Sieci wirtualne



Typy realizacji sieci wirtualnych:

wirtualizacja na poziomie warstwy 1 OSI:

1. wirtualne segmenty – grupowanie portów

wirtualizacja na poziomie warstwy 2 OSI:

2. lista adresów MAC – grupowanie adresów (i portów)
3. wirtualne podsieci – grupowanie różnych protokołów sieciowych w oddzielne podsieci

wirtualizacja na poziomie warstwy 3 OSI:

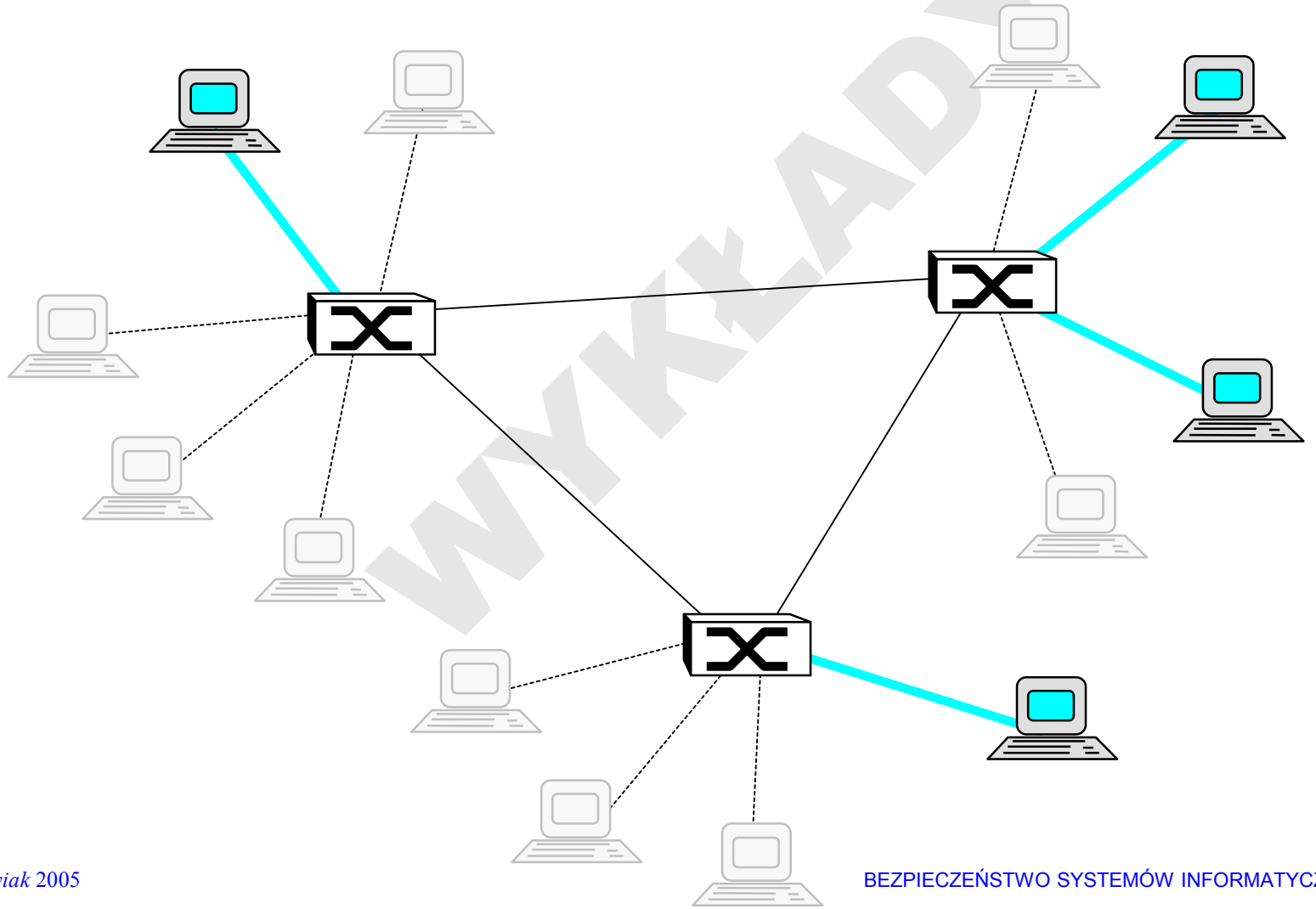
4. lista adresów sieciowych
5. reguły logiczne

   (selekcja wielokryterialna, analiza nagłówków protokołów wyższych warstw)

Sieci wirtualne

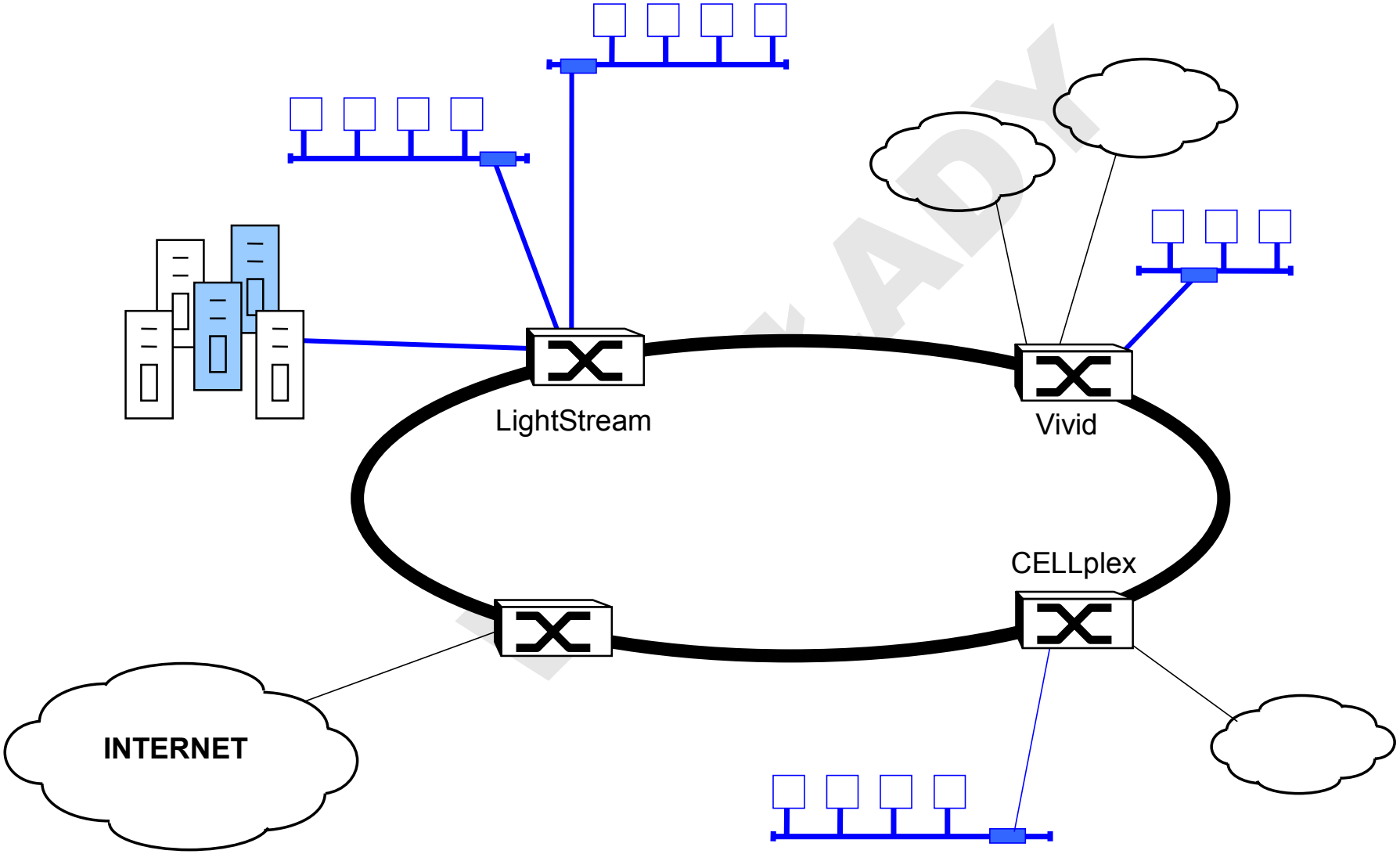
Sieci wirtualne realizowane poprzez wiele przełączników – std. 802.1Q:

problem globalnego określenia przynależności ramki do określonej sieci wirtualnej



Sieci wirtualne

Sieci wirtualne w technologii ATM



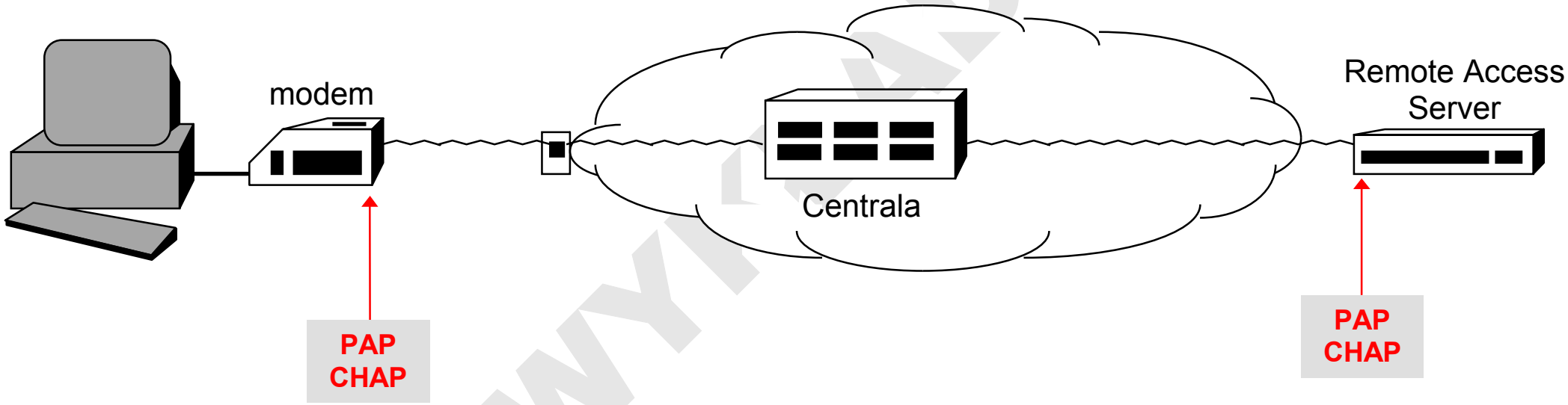
Metody obrony (c.d.)

Blokada niepowołanego dostępu do segmentu lokalnego:

- kontrola dostępu zdalnego (filtracja ruchu z zewnątrz do sieci lokalnej i przeciwnie)
- ukrycie wewnętrznych adresów sieci lokalnej (NAT)
- zabezpieczenie serwera (w tym: dezaktywacja i mapowanie usług, usługi proxy)
- szyfrowanie komunikacji

Zdalny dostęp

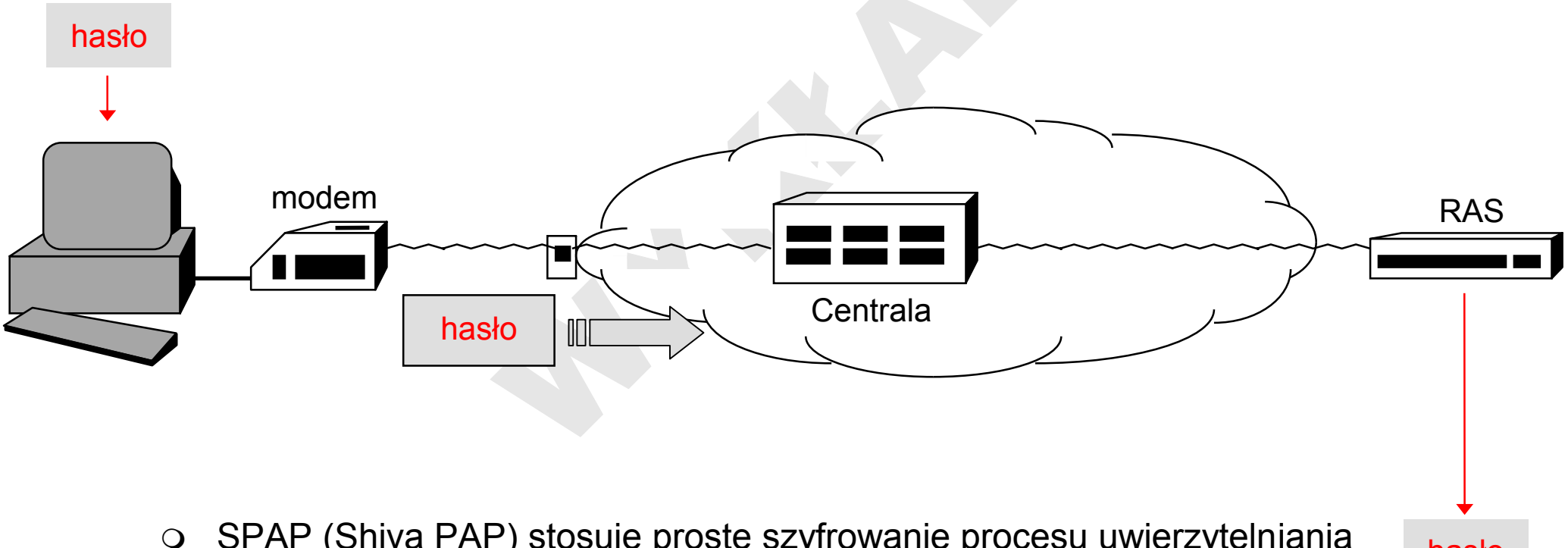
Schemat uwierzytelniania przy zdalnym dostępie



Zdalny dostęp

PAP (*PPP Authentication Protocol*) RFC1334

- RAS pyta o ID użytkownika, a następnie o hasło i decyduje o dopuszczeniu do sieci
- nazwa użytkownika i hasło są przesyłane tekstem jawnym !

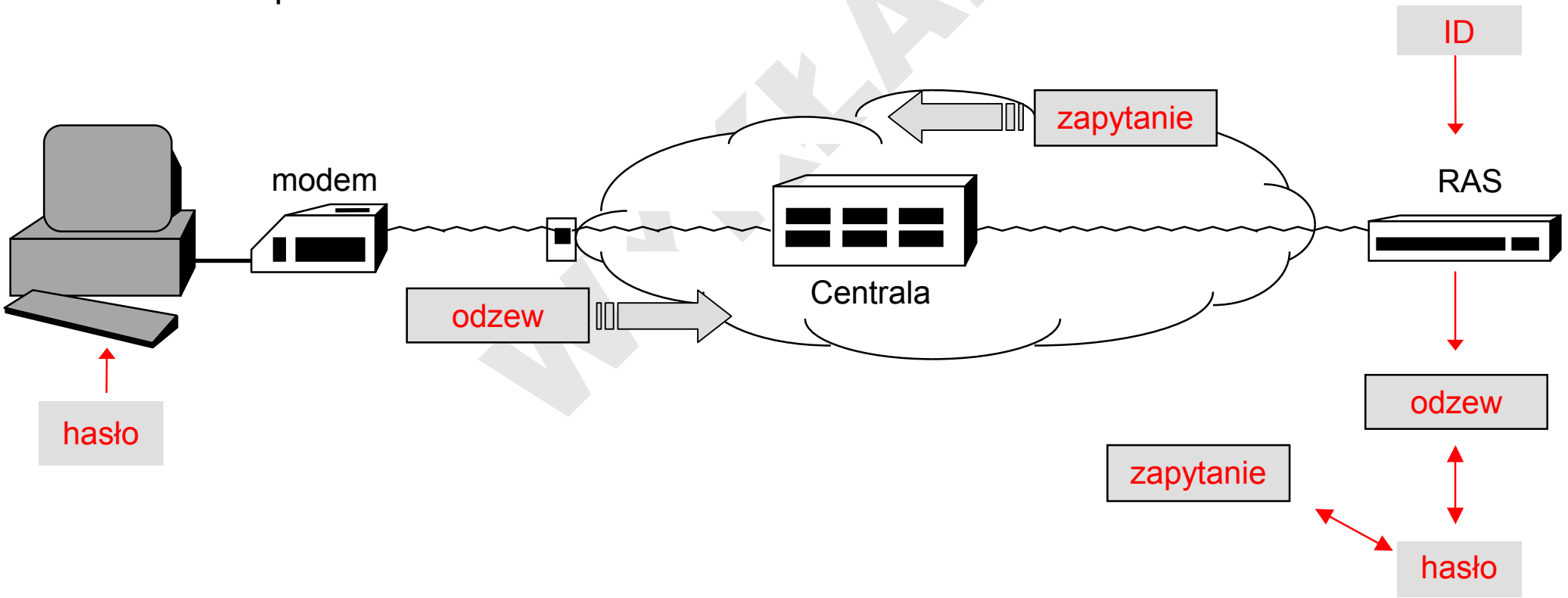


- SPAP (Shiva PAP) stosuje proste szyfrowanie procesu uwierzytelniania

Zdalny dostęp

CHAP (*Challenge Handshake Authentication Protocol*) RFC1994

- RAS pyta o ID użytkownika, a następnie przesyła unikalne „zapytanie”
- klient koduje zapytanie hasłem (MD5) i odsyła jako „odzew” decydujący o dopuszczeniu do sieci



Zdalny dostęp

EAP (*PPP Extensible Authentication Protocol*) RFC2284

- RAS wysyła jedno lub więcej zapytań do uwierzytelnianego podmiotu
- każdorazowo specyfikuje typ żądania (np. żądanie hasła lub skrótu MD5)
- możliwość korzystania z wielu protokołów uwierzytelniania
- bez potrzeby uprzedniego ich negocjowania

Zdalny dostęp

Dodatkowe mechanizmy kontroli połączeń komutowanych

Dial-back

- RAS ustala tożsamość klienta (np. za pomocą PAP, CHAP) i jego numer telefonu
- następnie RAS zrywa połączenie i zestawia je dzwoniąc na numer klienta

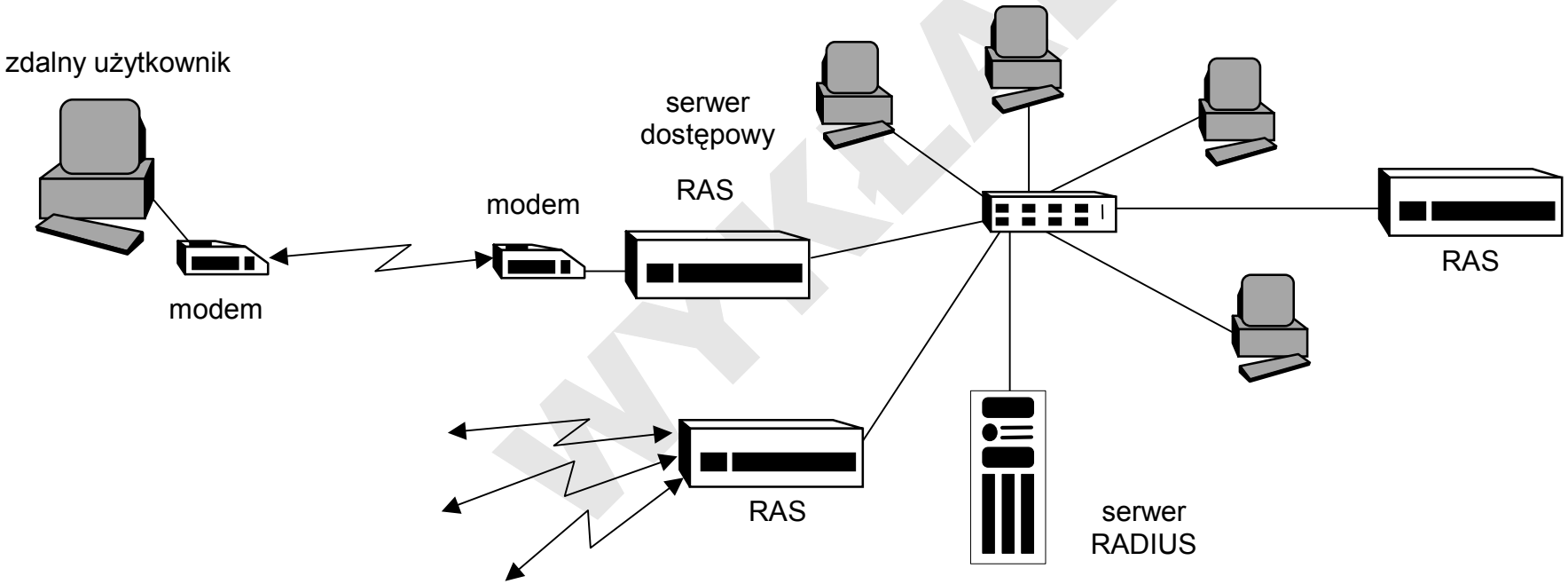
Caller ID (ISDN) / CLIP (PSTN, GSM)

- sieć podaje numer telefonu, z którego nawiązywane jest połączenie
- RAS decyduje o dopuszczeniu do sieci na podstawie tej informacji

Zdalny dostęp

Protokół RADIUS (*Remote Access Dial-In User Service*) – RFC2138

- AAA = Authentication + Authorization + Accounting
- serwer RADIUS – centrum uwierzytelniania i kontroli dostępu



Podobne protokoły – TACACS (*Terminal Access Control – Access Control System*), XTACACS, TACACS+

Uwierzytelnianie stanowisk

Standard IEEE 802.1x

- ochrona infrastruktury sieciowej przed nieautoryzowanym dostępem
- poprzez centralne uwierzytelnianie stacji sieciowych
- np. przełącznik wymusza uwierzytelnienie nowo wpiętej / uruchomionej stacji
- protokoły RADIUS, TACACS+, ...

Bezpieczny system nazw

DNSsec

- w 1999 zaproponowano rozszerzenie DNS o mechanizmy kryptograficznego uwierzytelniania i kontroli integralności (RFC 2535)
- poprzez dodanie rekordów SIG zawierających podpisy cyfrowe
- podpisujące zbiory rekordów informacyjnych (RRset)
- rolę certyfikacji pełni umieszczenie klucza publicznego w samym zbiorze – rekordy DNSkey
- DNSsec również może służyć przechowywaniu samych kluczy publicznych dla innych celów, np. PKI
- niestety wdrożenie DNSsec wciąż napotyka trudności (np. kwestia pełnego lub częściowego podpisywana zbiorów dla dużych domen, jak .com)

Narzędzia

Filtracja dostępu do usług sieciowych połączeń

tcp_wrapper

- filtracja dostępu do usług
- przekierowanie dostępu na *proxy-services*
- umożliwia realizację *dual homed gateway*

sockd i socks library

- pakiet filtracji dostępu do usług na podstawie adresów źródłowych
- rejestr *audit*
- *proxy* dla FTP i finger

kernel_wrap

- wrapper dla RPC wykorzystywanego przez takie demony jak portmap, ypserv, ypbind, mountd, pwauthd itp.

Narzędzia

Ochrona przed DoS

DoS guard

- funkcje DoS guard posiada większość zapór sieciowych (również osobistych)
- także wiele systemów operacyjnych routerów,
  np. TCPintercept w CiscoIOS lub Finesse (PiX)
- niektóre są nawet zaawansowane,
  np. SYN defender w Checkpoint Firewall-1
  lub SYN cookies w PiX-ach

Narzędzia

Kryptograficzne zabezpieczenie komunikacji

SSH – Secure Shell

- protokół szyfrowanej transmisji dla emulacji wirtualnego terminala i nie tylko
- usługa TCP port 22
- zastępuje telnet, rlogin, rsh, rexec, rcp, ftp
- umożliwia tunelowanie ruchu (VPN – tryb *port forwarding*)
- *de facto* standard (specyfikacje ver.1, ver.2)
- wiele implementacji, w tym darmowych dla większości Unixów (Open SSH)
- dla MS Windows, MacOS dostępnych wielu klientów

Narzędzia

SSH – wykorzystywane algorytmy krytpograficzne

SSH1	SSH2
DES	Arcfour
3DES	3DES (domyślny)
IDEA (domyślny)	Twofish
Blowfish	Blowfish
RC4 128b	RC4 128b
RSA	DSA
	CAST 128
	D-H key exchange

Implementacje mogą domyślnie używać inne algorytmy niż wskazane w specyfikacji protokołu (np. OpenSSH)

Narzędzia

SSH1

- różnorodne metody uwierzytelniania:
  - tradycyjne – hasłem konta systemu zdalnego
  - kryptograficzne – zapytanie odzew z kluczem publicznym i prywatnym RSA
  - .rhosts / .shosts (z uwierzytelnieniem kryptograficznym komputerów)
  - Kerberos, S/Key, AFS (Andrew File System)
- istnieją implementacje wykorzystujące tokeny elektroniczne
- oraz zintegrowane z filtrami TCPwrapper
- luki bezpieczeństwa: np. pluskwa w SSH v. 1.2.0 umożliwiająca pozyskanie klucza prywatnego hosta

Narzędzia

SSH2

- znacząco zmodyfikowany standard: nowe funkcje (sFTP, wsparcie dla TLS)
- nie jest w pełni kompatybilny z SSH1
- zawiera usprawnienia bezpieczeństwa, wydajności i przenośności
- oprogramowanie w mniejszym stopniu wymaga (i korzysta z) uprawnień administratora – istotne ze względu na możliwość ataków na aplikację (np. przepełnienie bufora)
- ograniczone metody uwierzytelniania – tylko metoda tradycyjna i kryptograficzna
- istnieją wtyczki GSSAPI (do Kerberosa v.5)

Narzędzia

Zagrożenia

- konieczna ochrona newralgicznych składników konfiguracji, takich jak klucze prywatne uwierzytelniania (katalogi domowe użytkowników – szcz. eksportowane przez NFS)

Narzędzia

Kryptograficzne zabezpieczenie komunikacji

NetCrypto (McAfee)

- szyfrowany kanał TCP/IP między poszczególnymi stacjami
- Windows, MacIntosh System7, Solaris, HP-UX, AIX, IRIX
- DES, 3DES, Blowfish, PC1, DH

Sieci bezprzewodowe

Standard IEEE 802.11 (Wi-Fi)

Autoryzacja WEP (*Wired Equivalency Privacy*)

- opcjonalnie kryptograficzna z kluczem symetrycznym (często 40b!)
- nie zawsze – często konfiguracja „dla turystów” (*war driving*) – bez kryptografii i z pełnym wsparciem DHCP
- wiele słabości i błędów projektowych – duża podatność na ataki (łącznie z prostą kryptoanalizą na podstawie analizy statystycznej, podszycia, manipulacje, oszukiwanie punktów dostępowych itd.):
  - wszyscy użytkownicy współdzielą ten sam klucz statyczny
  - prymitywny szyfr strumieniowy oparty na RC4
  - wektor inicjujący (IV) ma 24b – częste kolizje w punktach o większej przepustwości
  - integralność – liniowa suma kontrolna CRC-32

Sieci bezprzewodowe

Standard IEEE 802.11 (Wi-Fi)

Klucze WEP

- standard: 60b = 40b klucz + 24b IV
- klucz 128b (Lucent, 1998r.) – w zasadzie powszechnie dostępna opcja
- klucze 152b (Agere), 256b (US Robotics) – coraz częściej dostępne

Wektor inicjujący IV

- w praktyce nie jest niepowtarzalny
- dołączany jawnie do kryptogramu

Sieci bezprzewodowe

Standard IEEE 802.11 (Wi-Fi)

Ataki na WEP

- bierny atak kryptograficzny *FMS attack* (2001) – wystarcza tylko jeden bajt tekstu jawnego i kilka milionów pakietów i mamy klucz RC4 użyty w WEP
- winna jest metoda kapsułkowania pakietów 802.11 w 802.2
- narzędzia crackerskie – *AirSnort*, *WEPcrack*

Sieci bezprzewodowe

WPA (*Wi-Fi Protected Access*)

- tymczasowy zastępca WEP
- **EAP** (*Extensible Authentication Protocol*)
  - rozbudowany protokół dwustronnego uwierzytelniania z przyszłego standardu 802.11i
  - współpracuje z protokołami typu RADIUS lub innymi autorskimi protokołami zdalnego uwierzytelniania (np. LEAP firmy CISCO)
- **TKIP** (*Temporal Key Integrity Protocol*)
  - RC4 ze zmiennymi IV i dynamiczną (częstą) zmianą kluczy
- suma kontrolna MIC jest również uzyskiwana kryptograficznie
- mimo tego może lepszym wyborem są wyższe warstwy OSI

Sieci bezprzewodowe

Standard IEEE 802.11i

- zatwierdzony w poł. 2004 r.
- wymaga nowego sprzętu
- silne mechanizmy kryptograficzne:
  - TKIP (*Temporal Key Integrity Protocol*)
  - EAP (*Extensible Authentication Protocol*)
  - AES-CCMP (*Counter-mode cipher block Chaining Message Authentication Protocol*)
  - WRAP (*Wireless Robust Authentication Protocol*)

Sieci GSM

Technologie GSM:

- Global System for Mobile communication (GSM900)
- Digital Cellular System (DCS1800)
- Personal Communication System (PCS1900)

Nietypowość problemów bezpieczeństwa (dot. też PDA):

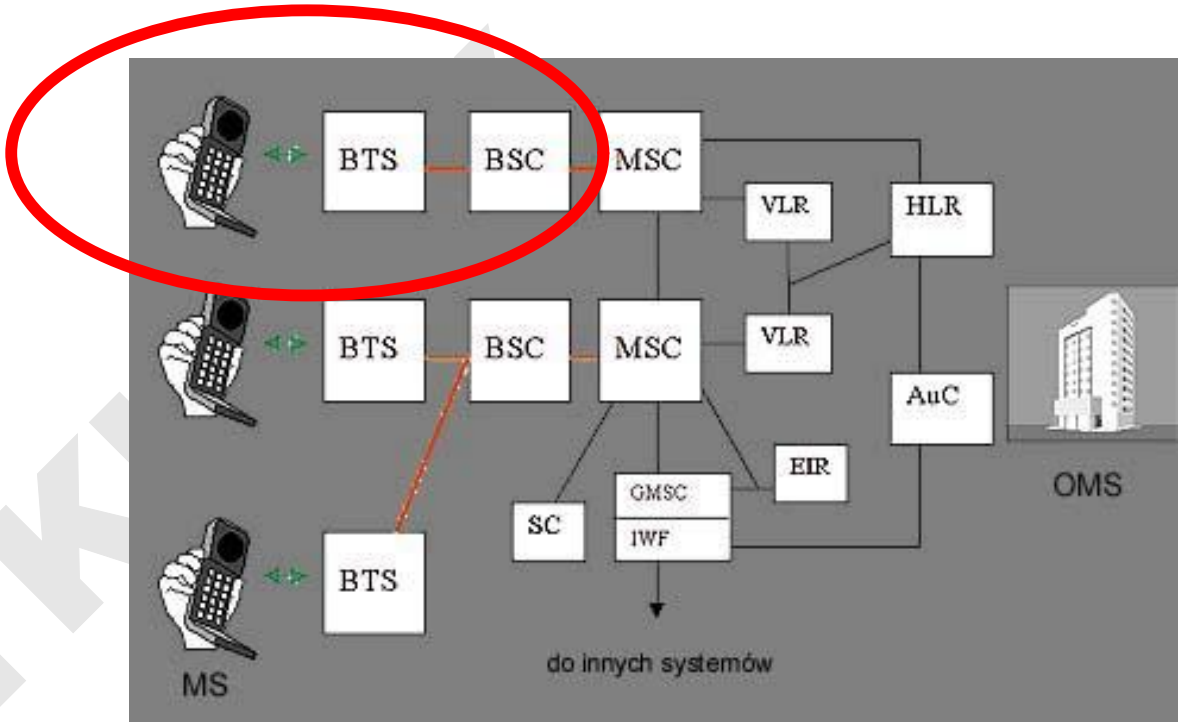
- słabsze procesory
- małe wyświetlacze
- brak klasycznej klawiatury

} wymagane nowe podejście do uwierzytelniania, kontroli dostępu, zachowania poufności

Sieci GSM

Schemat sieci:

- komórki
- stacje ruchome – telefony
  MS (*Mobile Station*)
- stacje bazowe
  BTS (*Base Transceiver Station*)
  (ew. przekaźniki)
- kontrolery
  BSC (*Base Station Controller*)
- i reszta sieci ...



Sieci GSM

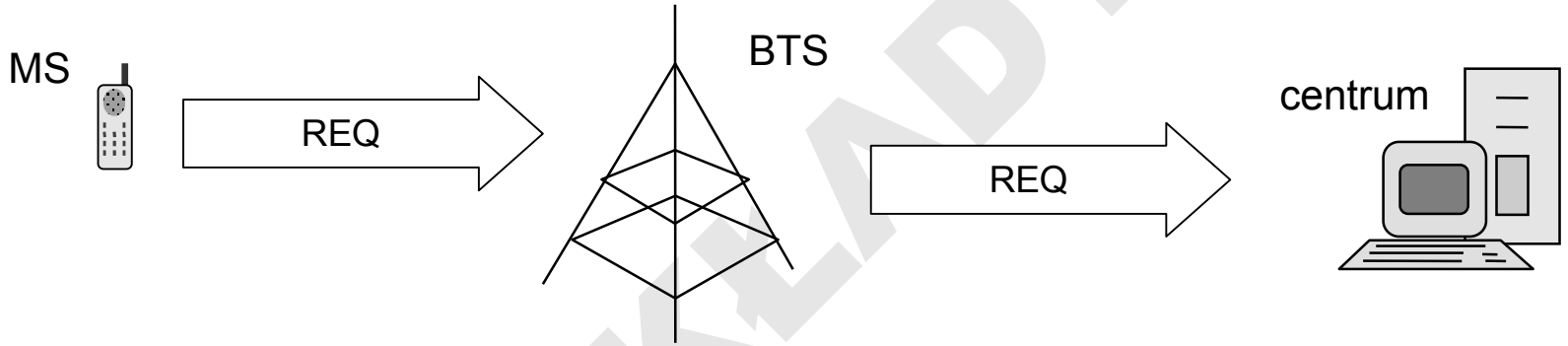
Transmisja:

- głos konwertowany do postaci cyfrowej, kompresowany, szyfrowany algorytmem symetrycznym A5 i przesyłany w pakietach 114b
- na karcie SIM zapisany jest unikalny numer seryjny i 64b tajny klucz K_{SIM}(fizycznie chroniony przed odczytem z zewnątrz) pamiętany również w bazie danych operatora
- są w niej również zaimplementowane dwa algorytmy kryptograficzne A3 i A8 (oba jednocześnie nazywane też COMP128)
- numer seryjny, IMSI (*International Mobile Subscriber Identity*), jest rzeczywistym identyfikatorem telefonu w sieci – jest on tłumaczony przez operatora na postać łatwą do posługiwania się użytkownikom

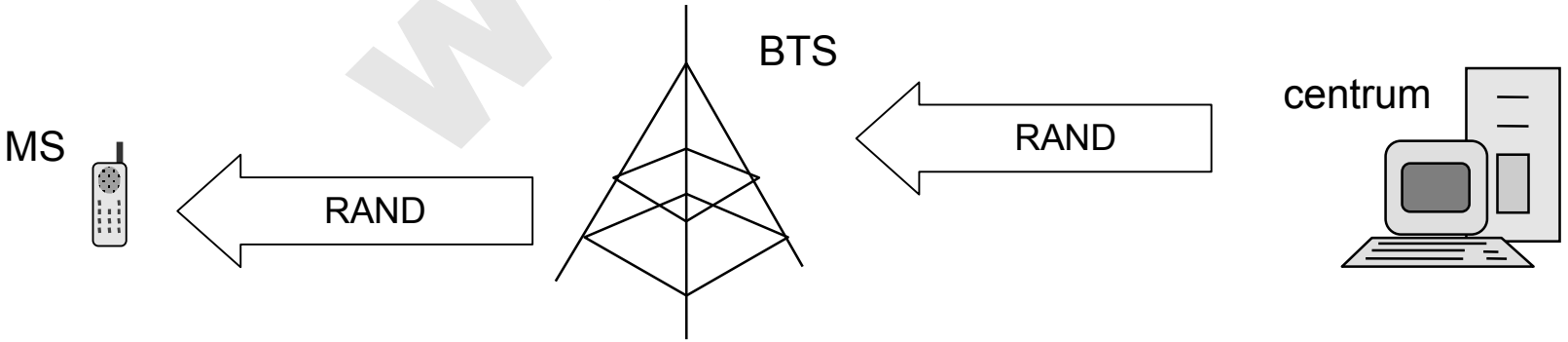
Sieci GSM

Uwierzytelnianie (1):

- metodą zapytanie-odzew



- komputer centralny generuje losową liczbę RAND

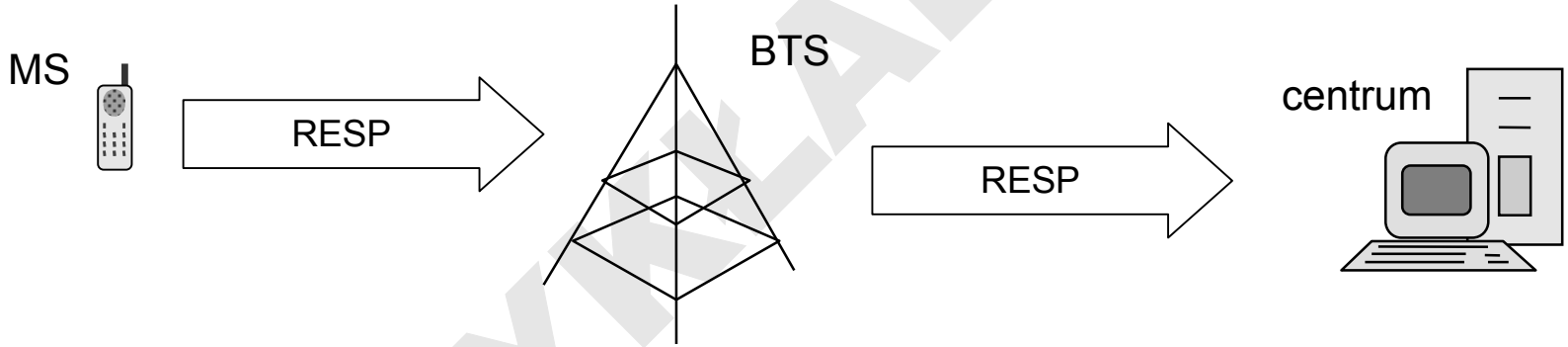


Sieci GSM

Uwierzytelnianie (2):

- karta SIM generuje odpowiedź RESP = A8 [K_{SIM}, RAND]

  (oczywiście podobnie robi serwer systemu uwierzytelniania operatora)



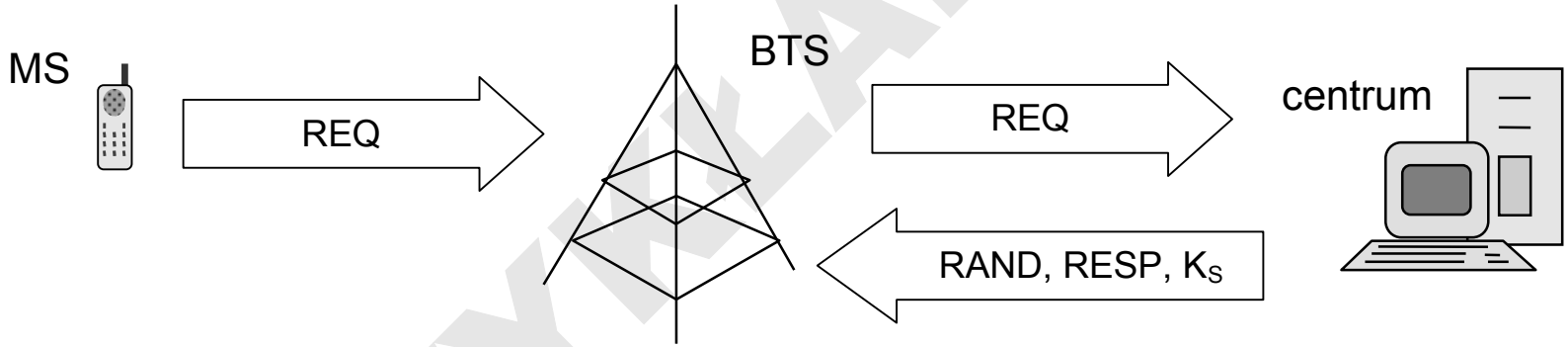
- jednocześnie karta SIM i komputer centralny wylicza 64b klucz sesji

  K_S = A3 [K_{SIM}, RAND]

Sieci GSM

Uwierzytelnianie (roaming):

- lokalna BTS prosi rodzimego operatora zestaw trójek ⟨RAND, RESP, K_S⟩
  (RESP = A8 [K_{SIM}, RAND], K_S = A3 [K_{SIM}, RAND])



- komputer centralny generuje i przesyła od razu kilka zestawów
- sam klucz K_{SIM} nie jest przesyłany!

Sieci GSM

Poufność:

- cała transmisja miedzy MS a BTS szyfrowana będzie prostym szyfrem strumieniowym $A5_{K_s}$ zaimplementowanym w telefonie (z uwagi na wydajność)
- szyfrowanie i deszyfrowanie w algorytmie A5 polega na prostym XOR z rejestrem (IV zależny od K_S)
- w telefonach implementowane są 2 wersje A5:
  - A5/1 – wcześniejsza i silniejsza , opracowana na potrzeby pierwotnej specyfikacji GSM
  - A5/2 – osłabiona (obawy eksportowe)
- telefon może był przełączany z A5/1 na A5/2

Sieci GSM

Słabości

- uwierzytelnianiu podlega tylko telefon, stacja bazowa nie
- pakiety danych nie są podpisywane kryptograficznie
- pakiety nie mają bezpiecznych numerów sekwencyjnych, co umożliwia atak przez ponowne wysyłanie przechwyconych pakietów (*replaying*)
- szyfrowany jest tylko przekaz radiowy – ruch w sieci stacjonarnej (zwykle w światłowodach) nie jest szyfrowany

Sieci GSM

Słabości

- kryptoanalitycy zgadzają się, że A5 jest szyfrem słabym, chociaż jak dotąd nie jest powszechnie znana żadna praktyczna metoda ataku
- w 2000 r. Shamir i Biryukov przeprowadzili udany atak na A5/1 metodą z wybranym tekstem jawnym – małe znaczenie praktyczne
- od 2003 znana też jest metoda ataku na A5/2 – nie są znane jej praktyczne zastosowania

Sieci GSM

Słabości

IMSI catcher

- urządzenie diagnostyczne, służące do symulowania stacji bazowej przy testowaniu telefonów komórkowych.
- używany przez włamywacza może udawać stację bazową dla wszystkich telefonów w promieniu 300 metrów, a przed inną stacją bazową może udawać telefon (*man-in-the-middle*)
- pozwala obejść (wyłączyć) szyfrowanie i dokonać pasywnego podsłuchiwania

Sieci GSM

Inne aspekty

Usługi lokalizacyjne

- telefony komórkowe dostarczają dodatkowej informacji – umożliwiają zlokalizowanie użytkownika.
- najprościej wyznaczyć można komórkę, w której zasięgu przebywa telefon
- rodzice mogą skorzystać z usługi pozwalającej lokalizować dzieci przy użyciu telefonu komórkowego
- systemy tego typu mogą mieć również zastosowanie w analizie zachowania konsumentów

Silent SMS

- pozwala one na odpytywanie telefonu („ping”) w sposób niezauważalny dla użytkownika, by sprawdzić czy jest on włączony

Sieci UMTS

- UMTS jest znacznie ulepszony w porównaniu do GSM
- algorytm szyfrujący KASUMI, klucz 128b
- stacja bazowa też jest uwierzytelniania (IMSI catcher bezużyteczny)
- pakiety danych wyposażone w kryptograficzne sumy kontrolne i kryptograficznie zabezpieczone numery sekwencyjne
- deszyfrowanie nie odbywa się zawsze w stacji bazowej, ale w tzw. kontrolerach sieci radiowej (RNC – *Radio Network Controllers*) – pozwala to łączyć stacje bazowe w bardziej bezpieczny sposób