Bezpieczeństwo systemów komputerowych

Podstawowe problemy bezpieczeństwa sieci komputerowych

Marcin Peczarski

Instytut Informatyki Uniwersytetu Warszawskiego

29 listopada 2011

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

Aspekt historyczny

- Większość aktualnie stosowanych technologii sieciowych ma swoje początki w latach 70.
- Problemy bezpieczeńtwa nie były wtedy rozważane.
- Celem wprowadzanych później modyfikacji było na ogół usprawnienie działania.
- Modyfikacje musiały zachować kompatybilność, co nie sprzyja podnoszeniu poziomu bezpieczeństwa.
- Problemy bezpieczeństwa powinno się rozważać dla każdej warstwy protokołów sieciowych już na etapie ich projektowania.

Warstwa fizyczna

- Problemy bezpieczeństwa mogą być związane z topologią sieci:
  - magistrala,
  - pierścień,
  - gwiazda.
- Problemy bezpieczeństwa mogą być związane z rodzajem medium:
  - fale radiowe,
  - skrętka nieekranowana,
  - skrętka ekranowana,
  - kabel koncentryczny,
  - światłowód.

Warstwa łącza, warstwa dostępu do medium

- Problemy bezpieczeństwa związane z najpopularniejszą obecnie technologią sieciową Ethernet:
  - ruch niejawnie rozgłoszeniowy, współdzielenie medium (topologia logiczna);
  - komunikacja jawnie rozgłoszeniowa (adresy rozgłoszeniowe i grupowe);
  - możliwość pracy sterownika sieciowego w trybie diagnostycznym (ang. *promiscuous*);
  - integralność transmitowanych ramek zapewniana przez prostą sumę kontrolną (CRC).
- Most (ang. *bridge*), przełącznik (ang. *switch*):
  - umożliwia selektywną propagację danych;
  - prosta metoda filtracji;
  - mogą implementować protokół drzewa rozpinającego, np. wg IEEE 802.1D.

Warstwa sieciowa

- Problemy bezpieczeństwa w najpowszechniej używanym protokole IP:
  - adresacja oparta na zaufaniu,
  - semantyka bezpołączeniowa,
  - zawodna transmisja pakietów (datagramów),
  - algorytm trasowania oparty na lokalnie podejmowanych decyzjach,
  - fragmentacja podatna na oszustwa,
  - rozgłaszanie,
  - odwzorowanie adresów za pomocą ARP,
  - możliwość kapsułkowania pakietów.

Adresacja

- Nie ma gwarancji, że pakiet został wysłany z adresu wpisanego w polu adres źródłowy (ang. *source address*).
- Lokalną kontrolę adresu źródłowego w systemie operacyjnym można łatwo ominąć.
- Nie wszyscy dostawcy usług dostępowych stosują filtry blokujące pakiety z nieprawidłowym adresem źródłowym.
- Nie można polegać na poprawności adresu źródłowego odebranego pakietu.
- Atak może polegać na sfałszowaniu adresu źródłowego (ang. *IP spoofing*).

Trasowanie

- Przeciążony ruter może odrzucać nadchodzące pakiety.
- Za retransmisję odpowiadają protokoły warstw wyższych.
- Jeśli ruter zostanie zalany bardzo dużą masą pakietów (nieistotne czy prawidłowych), to ewentualne przeciążenie doprowadzi do zablokowania transmisji pakietów należących do aktywnych sesji innych użytkowników.
- Przeciążenie rutera implikuje zagrożenia dostępności danych transmitowanych w pakietach kierowanych do niego.
- Potencjalny atak zdalny skierowany przeciwko innym stacjom sieciowym może wykorzystywać chwilową niedostępność pakietów z oryginalnego źródła celem podszycia się pod źródłowy komputer.

Fragmentacja

- Każdy fragment jest również datagramem i może teoretycznie mieć rozmiar do 64 kB.
- Spreparowane fragmenty przekraczające w sumie 64 kB mogą powodować błędy scalania.
- Manipulacje wartościami pola przesunięcie fragmentu (ang. *fragment offset*) mogą powodować błędy scalania.
- Często filtry przetwarzają właściwie (np. odrzucają) tylko pierwszy fragment pakietu:
  - w praktyce informacje niezbędne do przeprowadzenia filtracji znajdują się tylko w pierwszym fragmencie;
  - to wystarcza do wykluczenia poprawnego scalenia niepożądanego datagramu w węźle odbiorcy;
  - mimowolnie przepuszczane są kolejne fragmenty należące do ruchu sklasyfikowanego jako niepożądany.
- RFC 1858 opisuje dwie metody ataku wykorzystujące:
  - bardzo krótkie fragmenty (ang. *tiny fragment attack*),
  - nakładające się fragmenty (ang. *overlapping fragment attack*).

Rozgłaszanie

- IP i wiele innych protokołów oferuje mechanizmy rozgłaszania.
- Ukierunkowane rozgłaszanie może być wykorzystane do przeprowadzenia ataku na dostępność informacji DoS (ang. *Denial of Service*).
- Stanowi to najistotniejsze zagrożenie związane z mechanizmem rozgłaszania.
- Wiele ruterów posiada funkcję blokowania ruchu rozgłoszeniowego.

Odwzorowanie adresów

- Odwzorowaniem adresów IP na adresy MAC (np. Ethernet) zajmuje się ARP (Address Resolution Protocol).
- ARP stosuje rozgłaszanie zapytań i zbiera odpowiedzi bez zapewnienia poufności i autentyczności.
- Dla poprawy efektywności protokół wykorzystuje pamięć podręczną do chwilowego składowania informacji pozyskanych z docierających zapytań i odpowiedzi ARP.
- Stacja w sieci lokalnej może wysyłać fałszywe zapytania lub odpowiedzi ARP.
- Nieuczciwa stacja może kierować nieadresowane do niej pakiety w swoim kierunku (ang. *ARP spoofing*).
- Agresor może:
  - modyfikować strumienie danych;
  - podszywać się pod wybrane komputery.

Warstwa transportowa

- W rodzinie protokołów internetowych występują 2 protokoły transportowe:
  - TCP (Transmission Control Protocol) – protokół strumieniowy, połączeniowy;
  - UDP (User Datagram Protocol) – protokół pakietowy, bezpołączeniowy.
- Zestawienie połączenia w TCP wymaga wykonania 3-etapowej procedury nawiązania połączenia (ang. *3-way handshake*):
  - segmenty SYN, SYN+ACK, ACK;
  - ustalenie początkowych numerów sekwencyjnych, rozpoczynających numerowanie oktetów strumieni danych dla obu kierunków połączenia;
  - każde połączenie może rozpocząć numerację oktetów danych od arbitralnej wartości;
  - jeśli początkowy numer sekwencyjny ma wartość N, to pierwszy transmitowany oktet ma numer $N + 1$;
  - początkowy numer sekwencyjny jest ustalany oddzielnie dla każdego kierunku transmisji.

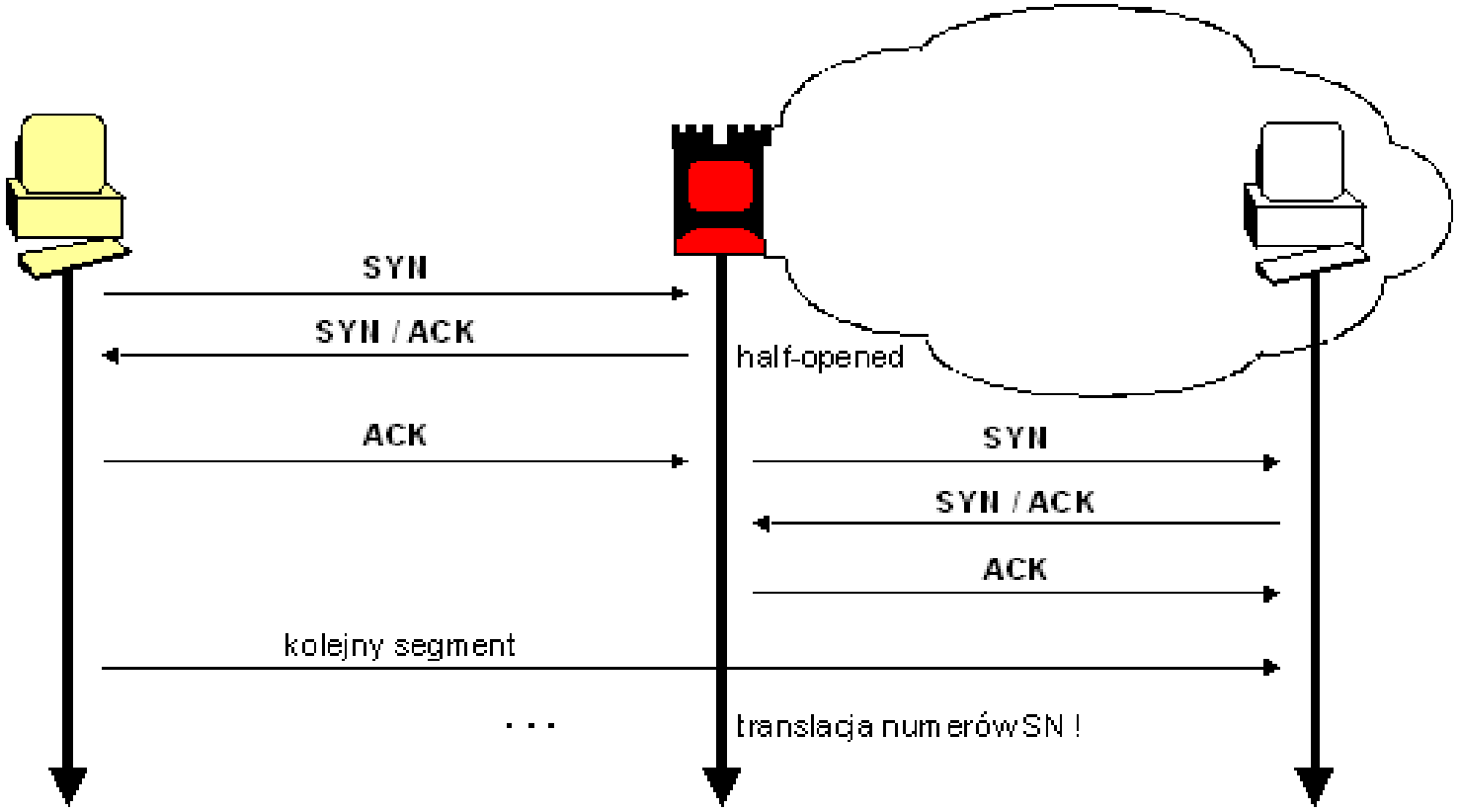
Atak zalewający nowonawiązywanymi połączeniami TCP

- Dla każdego nawiązanego połączenia system przydziela pewne zasoby, w szczególności pamięć.
- Zasoby zwalniane są po zamknięciu połączenia.
- Jeśli zamknięcie nie następuje, zasoby pozostają zajęte, mimo że mogły w ogóle nie być wykorzystane.
- Odpowiednio duża liczba zestawionych połączeń może doprowadzić do przydzielenia im całej dostępnej pamięci, nie pozostawiając żadnych dostępnych zasobów do pracy systemu i powodując załamanie jego pracy.

Atak zalewający ofiarę segmentami SYN (ang. *SYN flood*)

- Agresor wysyła na adres ofiary dużą liczbę segmentów SYN adresowanych z dowolnych (nieistniejących) adresów IP.
- Nieświadoma tego ofiara odpowiada segmentami SYN+ACK i rozpoczyna bezowocne oczekiwanie na segmenty ACK.
- Instancja protokołu TCP po stronie ofiary jest w stanie na wpół otwartym (ang. *half-opened*).
- W praktyce system operacyjny przydziela zasoby dla nowozestawianego połączenia już po pojawieniu się pierwszego segmentu SYN, jeszcze zanim 3-etapowa procedura nawiązywania zostanie zakończona.
- Duża liczba na wpół nawiązanych połączeń może wyczerpać zasoby systemu operacyjnego ofiary i zablokować system.
- Taki atak jest trudno wykryć, bowiem typowe implementacje TCP nie raportują wyższym warstwom OSI (systemowi operacyjnemu) żadnych zdarzeń związanych z połączeniem, które nie jest jeszcze w pełni nawiązane.

Obrona przed atakiem SYN flood – SYN defender



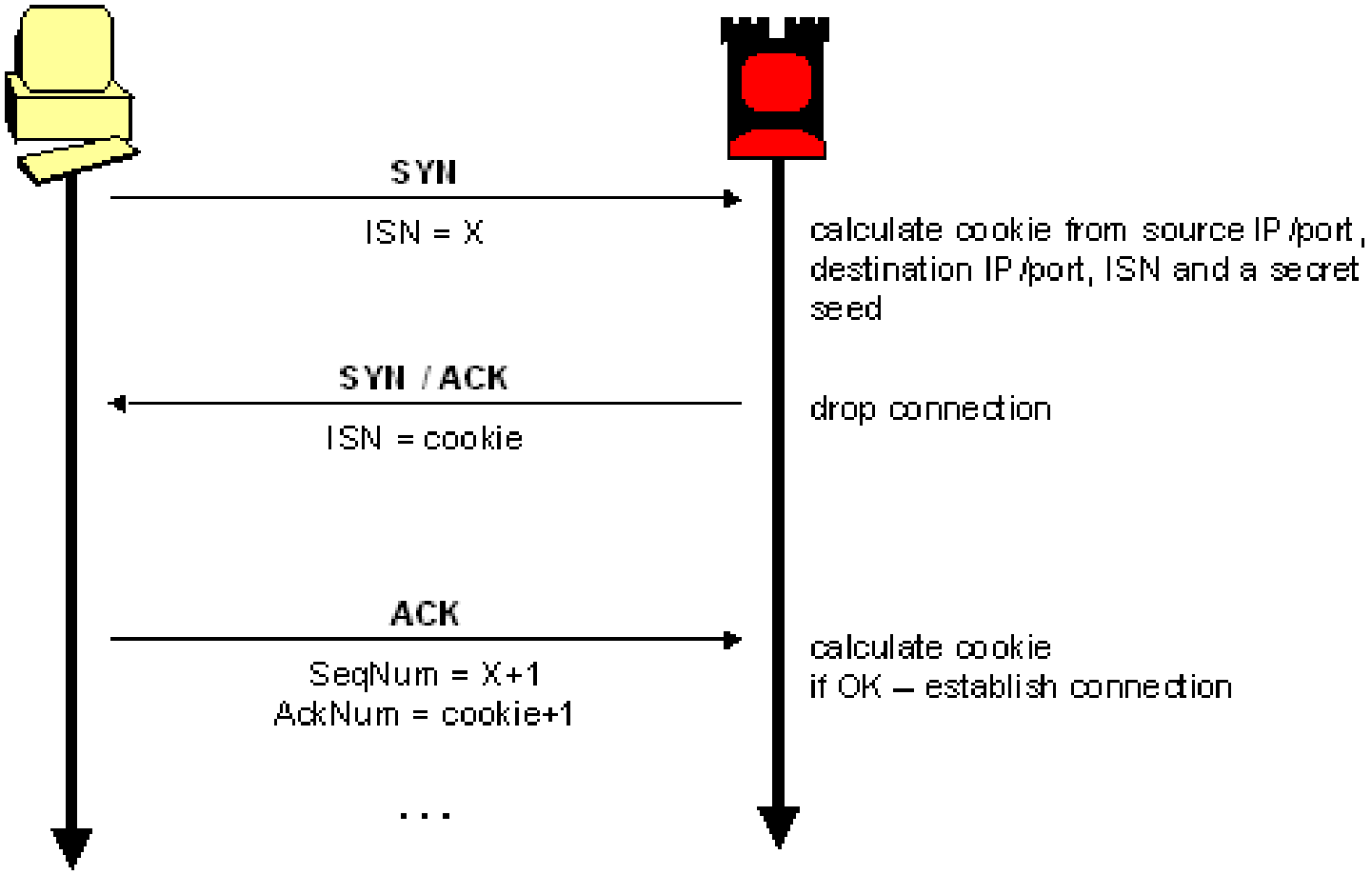
Obrona przed atakiem SYN flood – SYN defender, cd.

- Pomiędzy agresora i ofiarę wprowadza się wyspecjalizowanego obrońcę, który przejmuje wszystkie segmenty SYN skierowane do ochranianego systemu i propaguje połączenia dopiero, gdy wykluczy atak, czyli gdy dotrze trzeci segment nawiązania połączenia.
- Jeśli SYN defender rozpozna atak (nie doczeka się na trzeci segment), zapomina o parametrach połączenia, a system ochraniany nawet nie dowie się o ataku.
- Jeśli SYN defender wykluczy atak, to wówczas samodzielnie zestawia nowe połączenie z systemem ochranianym, które posłuży to retransmitowania segmentów odebranych od nadawcy.

Obrona przed atakiem SYN flood – SYN defender, cd.

- Oczywiście to nowe połączenie nie będzie miało identycznych parametrów, np. początkowy numer sekwencyjny wybrany przez ochranianego będzie z pewnością inny, niż uprzednio zaproponowany otwierającemu połączenie przez obrońcę.
- Propagowane segmenty muszą być poddane konwersji parametrów (nagłówka) przy przejściu przez węzeł obrońcy.
- Istotą ochrony przed atakiem jest przeniesienie punktu obrony z ofiary na zewnętrzny system, który przygotowany na okoliczność ewentualnego ataku nie pozwoli na przeciążenie siebie poprzez zużycie wszystkich zasobów.
- Ilość zasobów potrzebna obrońcy na obsługę połączeń jest tu minimalna, a system ofiary obsługuje wyłącznie połączenia, które nie są elementem ataku SYN flood.

Obrona przed atakiem SYN flood – SYN cookies



Obrona przed atakiem SYN flood – SYN cookies, cd.

- SYN cookies umożliwia realizację obrony w systemie potencjalnej ofiary.
- System broniący się nie musi rezerwować zasobów dla połączenia w momencie odebrania segmentu SYN.
- Zamiast tego system ten generuje specjalną wartość, przekazywaną nadawcy segmentu SYN i tak spreparowaną, aby po otrzymaniu w przyszłości trzeciego segmentu (ACK) rozpoznać, że jest to kontynuacja wcześniej rozpoczętego nawiązywania połączenia.
- Zasoby są rezerwowane dopiero po otrzymaniu segmentu ACK.

Obrona przed atakiem SYN flood – SYN cookies, cd.

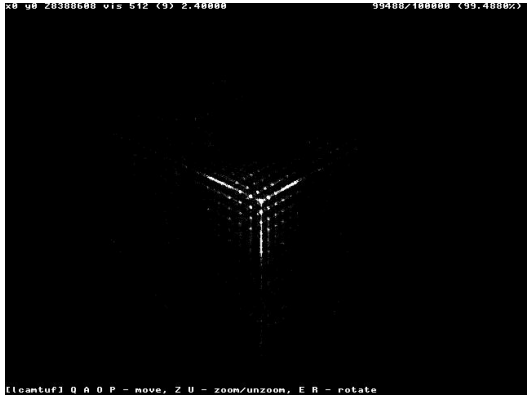
- Aby rozpoznać poprawność późniejszego segmentu ACK, broniący po odebraniu segmentu SYN generuje ciasteczko (ang. *cookie*) zawierające:
  - 5-bitowy znacznik czasowy,
  - 3-bitowy znacznik maksymalnej długości segmentu,
  - 24-bitowy skrót kryptograficzny adresów i numerów portów końców połączenia oraz znacznika czasowego.
- Ciasteczko jest wysyłane jako początkowy numer sekwencyjny w segmencie SYN+ACK.
- Ciasteczko powróci (zwiększone o jeden) w polu potwierdzenia w segmencie ACK, umożliwiając detekcję poprawności procedury zestawiania połączenia.
- Mechanizm SYN cookies posiada niestety pewne ograniczenia, nie można korzystać z niektórych użytecznych rozszerzeń specyfikacji TCP, np. large window.

Problem wyboru początkowego numeru sekwencyjnego

- Możliwe jest zdalne wymuszenie połączenia i przechwycenie komunikacji nawet bez odbioru segmentu SYN+ACK.
- Wymaga to odgadnięcia numeru sekwencyjnego zawartego w tym segmencie.
- Co prawda początkowe numery sekwencyjne są wybierane pseudolosowo, ale na ogół z rozkładem dalekim od losowego.
- Wg sugestii z RFC 793 licznik numerów sekwencyjnych powinien być zwiększany co 4 μs.
- Starsze jądra, np. wywodzące się z BSD 4.2, zwiększają licznik o stałą wartość co 1 s i przy każdym nowym połączeniu.
- W RFC 1948 opisano modyfikację generowania numerów sekwencyjnych w TCP.

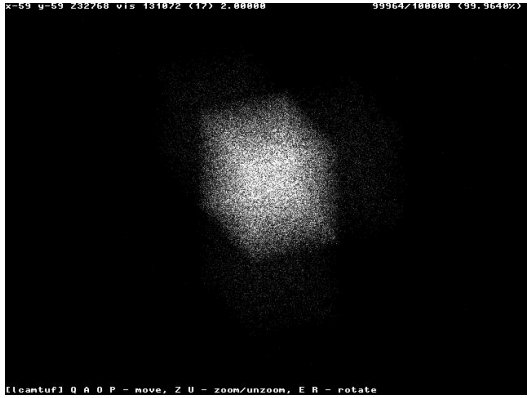
Wykresy fazowe

- Umożliwia ocenę losowości wyboru numeru sekwencyjnego.
- $x_t = s_t - s_{t-1}$, $y_t = s_{t-1} - s_{t-2}$, $z_t = s_{t-2} - s_{t-3}$.

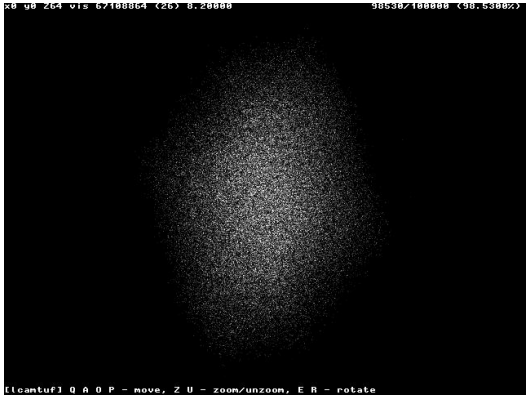


Windows 98 SE

Windows NT4 SP3



Windows 2000

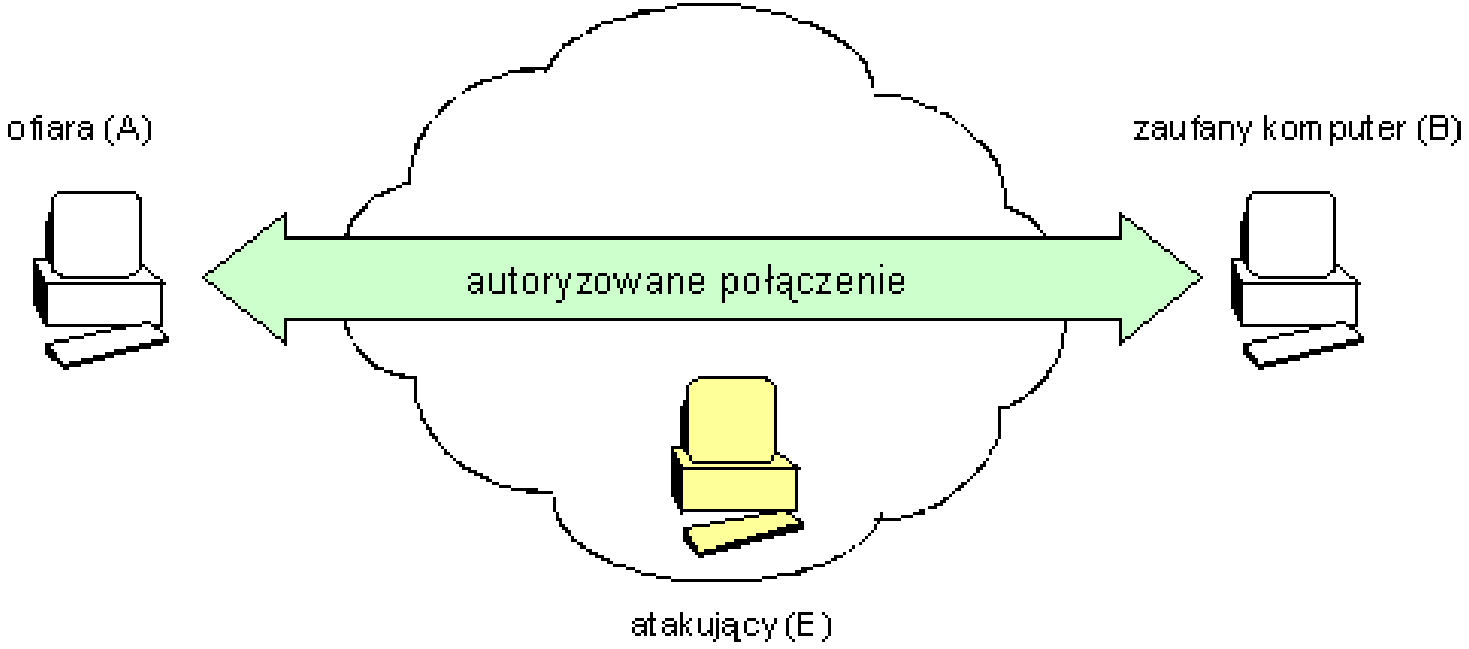


Linux 2.2

Źródło: Michał Zalewski, *http://lcamtuf.coredump.cx/oldtcp/tcpseq.html*

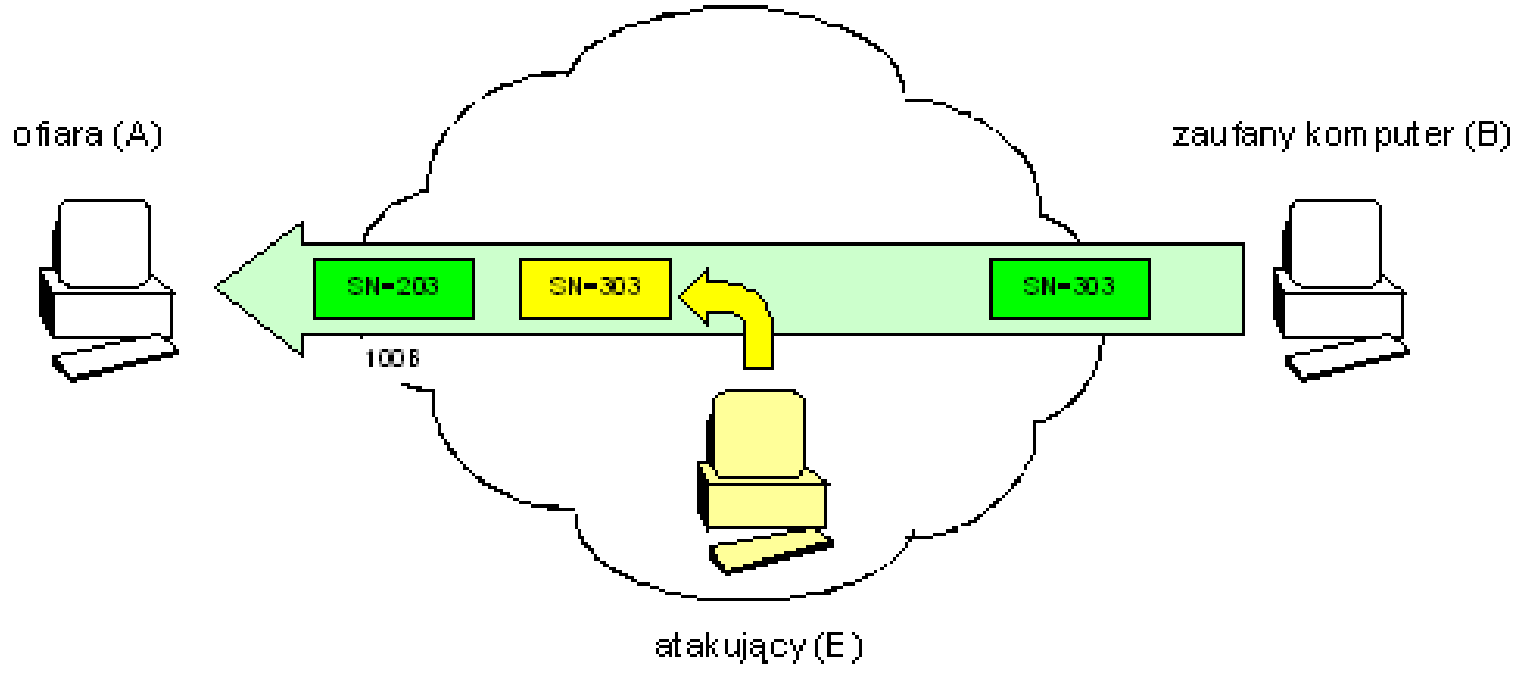
TCP session hijacking

- Celem ataku jest nieuprawnione wstrzelenie segmentów protokołu transportowego w strumień wymieniany w autoryzowanym (poprawnie zestawionym) połączeniu między ofiarą ataku a systemem, któremu ofiara ufa.



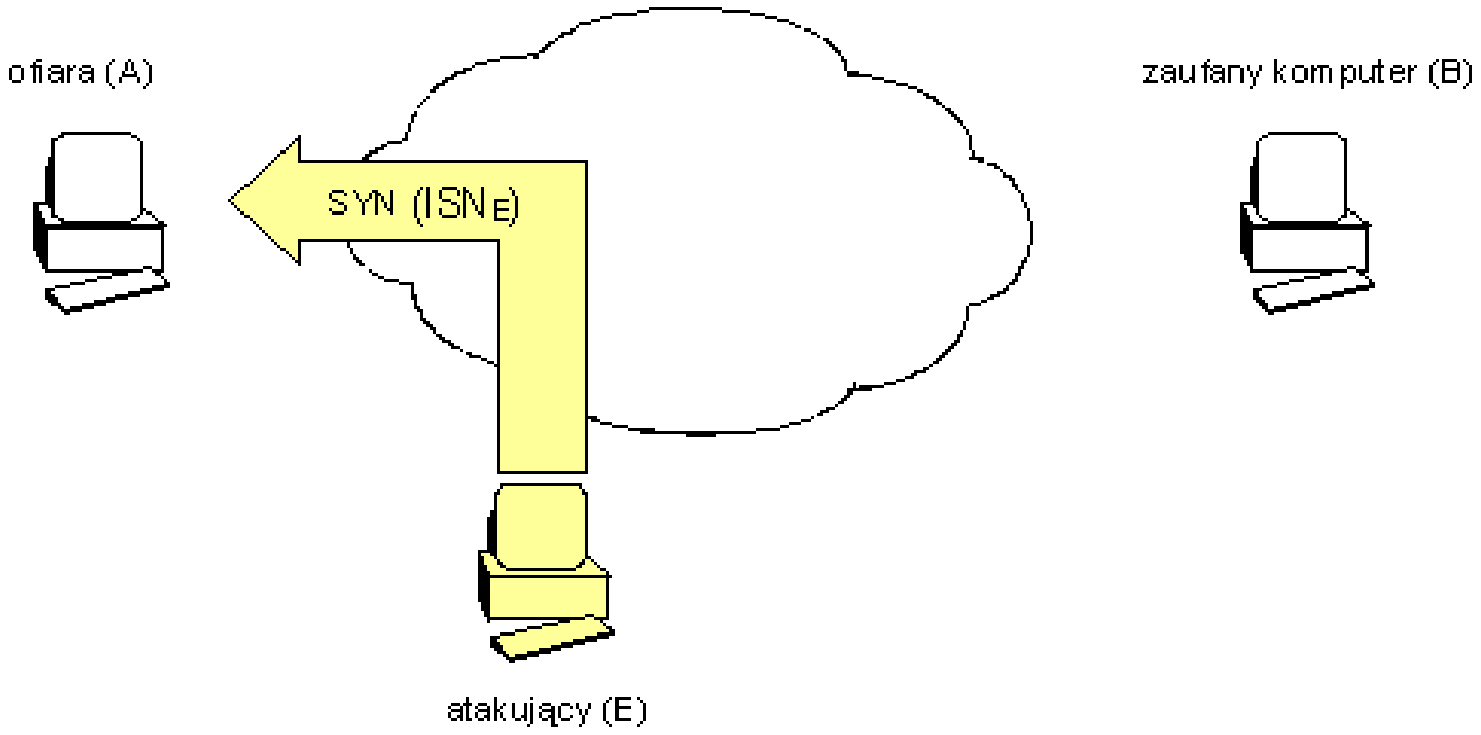
TCP session hijacking, cd.

- Agresor, mając wgląd w dotychczasową zawartość strumienia w kierunku od systemu zaufanego do ofiary (ang. *sniffing*), może spreparować poprawny i oczekiwany przez ofiarę segment, który podsunie jako rzekomo autentyczny segment wysłany przez zaufany system.



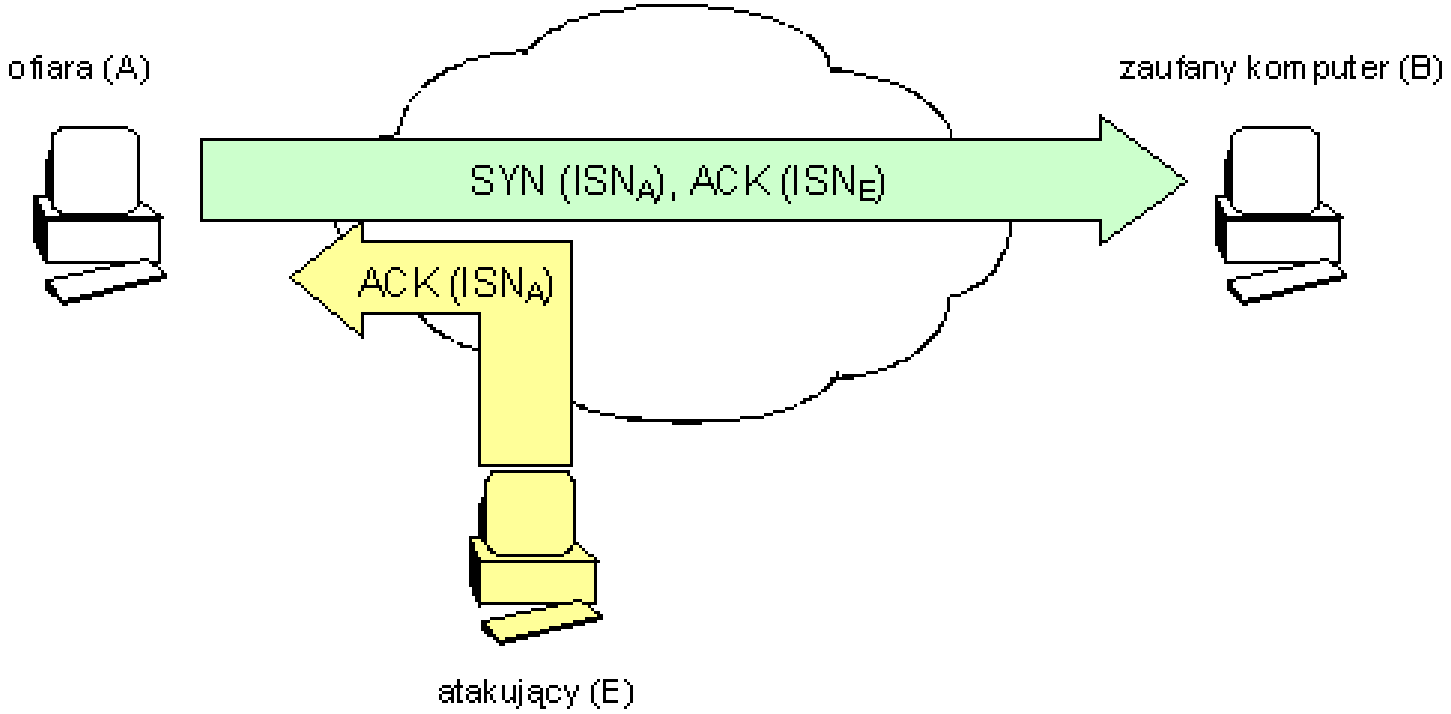
TCP spoofing

- Celem ataku jest nieuprawnione zestawienie połączenia z systemem A (ofiarą ataku) w imieniu systemu B, któremu ofiara ufa.
- Agresor E nie ma wglądu w komunikację między A i B, co czyni atak znacznie trudniejszym niż session hijacking.
- Atak wymaga sfałszowania adresu źródłowego.



TCP spoofing, cd.

- Atak wymaga dodatkowo poprawnego przewidzenia początkowego numeru sekwencyjnego ISN_A, który zaproponuje A w segmencie SYN+ACK.
- Atak wymaga zablokowania poprawnej komunikacji z B, co może wymagać przeprowadzenia ataku DoS przeciw B, aby B nie mógł zakończyć (zresetować) niechcianego połączenia.



TCP spoofing, cd.

- Najtrudniejszym krokiem ataku jest wysłanie poprawnego segmentu ACK zawierającego potwierdzenie początkowego numeru sekwencyjnego ISNA wybranego przez A.
- Ze względu na brak możliwości podglądu przez E komunikacji z A do prawdziwego B, wymaga to przewidzenia wartości ISNA przez E.
- Jest to prawdopodobne przy wygenerowaniu relatywnie niedużej liczby segmentów ACK, jeśli system A nie posiada poprawnego generatora początkowych numerów sekwencyjnych.
- Właściwą wartość ISNA można wytypować np. przez uprzednie nawiązanie autoryzowanego połączenia na inny port (pozyskanie wcześniejszego numeru ISNA).
- Wówczas jest szansa, że jeden z wygenerowanych przez E segmentów będzie przenosił poprawną wartość potwierdzenia i zostanie przez A uznany za oczekiwany.

Warstwa aplikacji

- Brak mechanizmów ochrony poufności oraz integralności w najpopularniejszych protokołach: TELNET, FTP, SMTP, POP, IMAP.
- Mało wiarygodne, trywialne mechanizmy uwierzytelniania.

Identyfikacja usługi na podstawie numeru portu

- Nie można polegać na identyfikacji usługi na podstawie numeru portu źródłowego lub docelowego.
- Lokalny numer portu klienta jest niemal zawsze wybierany przypadkowo przez system operacyjny (choć klient może go wybrać sam).
- W systemach uniksowych występują tzw. porty systemowe (uprzywilejowane) – o numerach mniejszych od 1024.
- Z portów systemowych mogą korzystać tylko procesy posiadające uprawnienia administratora.
- Teoretycznie można domniemywać, że proces uruchomiony na porcie systemowym należy do zaufanych i bezpiecznych.
- Jednak w praktyce nie ma oczywiście pewnego sposobu zdalnej weryfikacji prawdziwości tego domniemania.
- Restrykcja wykorzystania portów systemowych tylko przez administratora jest wyłącznie konwencją:
  - nie należy do specyfikacji protokołu,
  - nie dotyczy systemów innych niż uniksowe,
  - poleganie na niej absolutnie nie jest bezpieczne.

System nazw dziedzinowych

- Jedną z najpopularniejszych usług narzędziowych jest DNS (Domain Name System).
- DNS to rozproszona baza danych odwzorowań nazwa domenowa – adres sieciowy.
- Baza DNS ma strukturę drzewiastą, poddrzewa odpowiadają poszczególnym domenom niższego poziomu (poddomenom).
- Zarządzanie poddrzewami może być delegowane innym serwerom DNS.
- Aktualizacje bazy DNS mogą obejmować pojedyncze rekordy (ang. *RR – resource records*), jak i całe poddrzewa.
- Za pomocą DNS można pytać o pojedyncze odwzorowania, jak i realizować pozyskanie pełnej kopii fragmentu obszaru nazw, tzw. transfer stref (ang. *zone transfer*), np. w celu aktualizacji serwerów zapasowych.
- DNS dostępny jest poprzez oba protokoły transportowe:
  - UDP – pojedyncze zapytania,
  - TCP – transfer stref.

System nazw dziedzinowych, cd.

- Z punktu widzenia bezpieczeństwa istotne jest, że niektóre zapisy RR dostarczają informacji użytecznych dla agresora, np. HINFO może zawierać informacje o systemie operacyjnym, WKS (well-known-services). Pola te są obecnie na szczęście rzadko stosowane.
- Baza DNS składa się z dwóch oddzielnych drzew:
  - odwzorowanie nazw na adresy (zapytania proste),
  - odwzorowanie adresów na nazwy (zapytania odwrotne).
- Nie ma wymuszonej relacji między drzewami – każde z nich jest w praktyce utrzymywane niezależnie.
- Przy czym drzewo odwzorowań odwrotnych jest aktualizowane rzadziej niż drzewo odwzorowań prostych, a do tego w ogóle jest utrzymywane w gorszym stanie.
- Istnienie odwzorowań w obu kierunkach można wykorzystać do weryfikacji poprawności tłumaczenia nazwy – oba odwzorowania przechowywane są zwykle na różnych maszynach.

Problemy bezpieczeństwa DNS

- Udostępnianie użytecznych informacji agresorom.
- Brak uwierzytelniania w protokole zapytań DNS i transferu stref, co umożliwia fałszowanie danych (ang. *pharming*).
- Możliwość podszywania się pod autoryzowne nazwy uniemożliwia uwierzytelnianie przez nazwę.
- Możliwość „zatruwania” fałszywymi odpowiedziami lokalnej pamięci podręcznej usługi DNS jeszcze zanim wyśle ona zapytanie o odwzorowanie.

Bezpieczny system nazw dziedzinowych

- W 1999 zaproponowano rozszerzenie DNS o mechanizmy kryptograficznego uwierzytelniania i kontroli integralności [RFC 4033, 4035, 4470].
- Zaproponowano dodanie rekordów SIG zawierających podpisy cyfrowe zbiorów rekordów informacyjnych (RRset).
- Rolę certyfikatu pełni klucz publiczny umieszczony w samym zbiorze.
- Klucz jest przechowywany w rekordzie nowego typu DNSkey.
- Usługa DNSsec również może służyć przechowywaniu samych kluczy publicznych dla innych celów, np. infrastruktury klucza publicznego PKI.
- Niestety wdrożenie DNSsec wciąż napotyka trudności.
- Przykładowym problemem jest m.in. kwestia pełnego lub częściowego podpisywana zbiorów dla dużych domen, takich jak *com*.

Inne usługi narzędziowe

- Inne popularne usługi narzędziowe BOOTP i DHCP również udostępniają informacje o infrastrukturze sieciowej i to często bardzo bogate informacje, praktycznie bez uwierzytelniania.
- Na szczęście dostępne są one na ogół tylko w obrębie sieci lokalnej, zatem mogą być wykorzystane tylko przez agresorów, którzy wdarli się już do atakowanej podsieci.
- Istotny jest jednak problem bezpiecznej wymiany danych pomiędzy serwerami DHCP a DNS, a ta z kolei może przechodzić przez kilka podsieci.

Typowe ataki na infrastrukturę sieciową

- Information recovery – nieuprawnione uzyskanie danych.
- Host impersonation – podszycie się pod inny system w sieci.
- Temper with delivery mechanisms – manipulacja mechanizmami dostarczania pakietów.

Typowe ataki na infrastrukturę sieciową, cd.

- Network sniffing – jest to pasywny podgląd medium transmisyjnego, np. w celu przechwycenia interesujących ramek (ang. *packet snooping*).
- Network scanning – jest to wykorzystanie specyfiki implementacji protokołów do sondowania (ang. *enumeration*) urządzeń aktywnych w sieci, aktywnych usług, konkretnych wersji systemu operacyjnego i poszczególnych aplikacji.
- Powolne skanowanie, aby nie wzbudzać alarmu – filtry sieciowe potrafią wykrywać próby skanowania.

Typowe ataki na infrastrukturę sieciową, cd.

- TCP session hijacking – przejmowanie połączeń poprzez „wstrzelenie” odpowiednio dobranych pakietów – wymaga dostępu do uprzednio legalnie zestawionego połączenia TCP.
- TCP spoofing – podszywanie bazujące na oszukaniu mechanizmu generowania początkowych numerów sekwencyjnych.
- UDP spoofing – prostsze od TCP w realizacji (ze względu na brak mechanizmu szeregowania i potwierdzania ramek w protokole UDP), użyteczne podczas atakowania usług i protokołów bazujących na UDP, np. DNS.

Typowe ataki na infrastrukturę sieciową, cd.

- ARP spoofing/poisoning – zdalna modyfikacja wpisów w tablicach ARP systemów operacyjnych oraz przełączników.
- DNS cache poisoning (pharming, birthday attack) – modyfikacja wpisów domen w dynamicznej pamięci podręcznej DNS.
- ICMP redirect – zmiana trasowania dla wybranych adresów sieciowych.
- Ataki na urządzenia sieciowe za pomocą protokołu SNMP.

Typowe ataki na infrastrukturę sieciową, cd.

- DoS – Denial of Service – odmowa usługi – atak, którego ostatecznym celem jest unieruchomienie poszczególnych usług, całego systemu lub całej sieci komputerowej:
  - SYN flood,
  - ping of death,
  - land,
  - UDP flood, UDP bomb atack, UDP storm,
  - email bombing, zip bombing.
- DDoS – Distributed Denial of Service – agresor nie przeprowadza ataku bezpośrednio, lecz doprowadza do skomasowanego natarcia, wykorzystując inne systemy, które uczestniczą w ataku mimowolnie, gdyż zostały wcześniej opanowane przez agresora:
  - smurf, fraglle,
  - tfn (tribal/tribe flood network), trinoo/trin00, trinio, trinity v3,
  - stacheldraht.

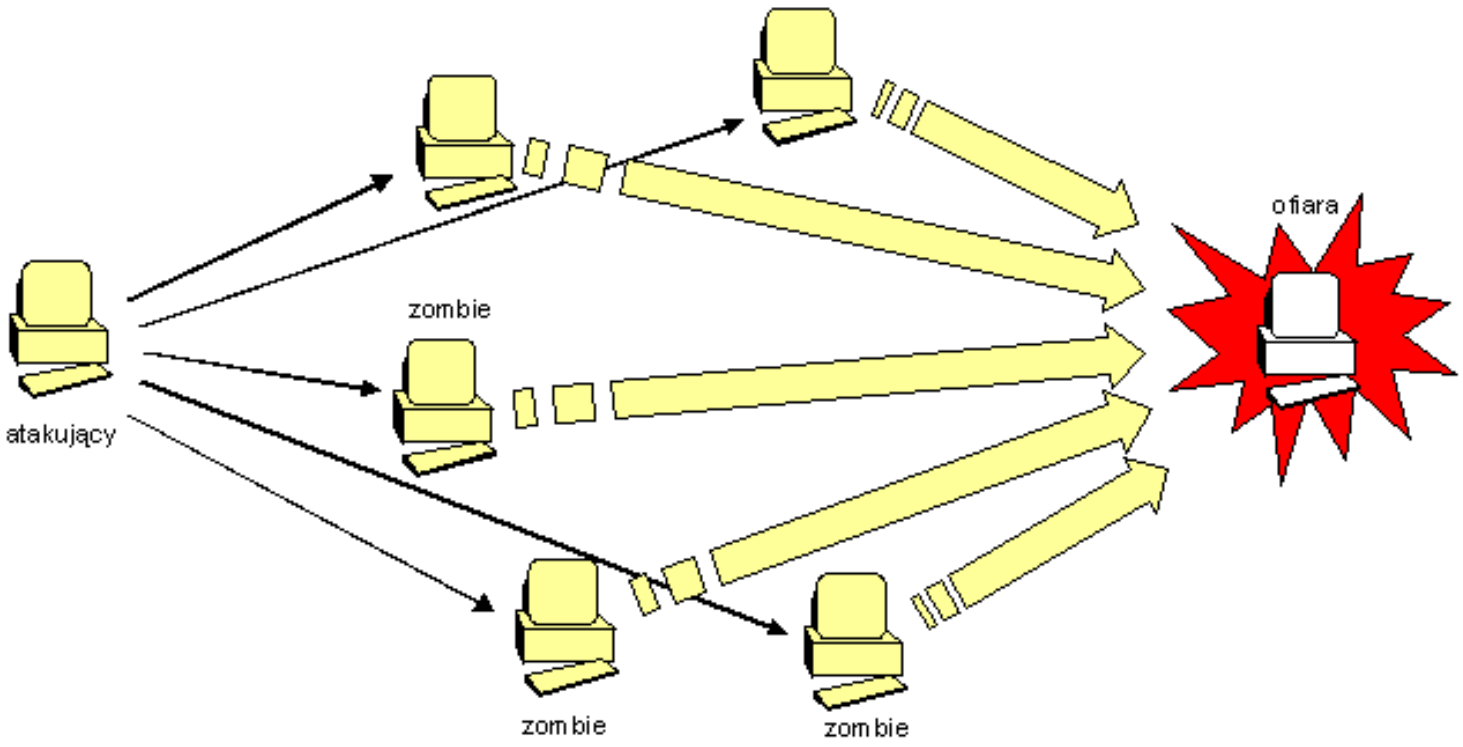
Skanowanie portów

- Za pomocą pofragmentowanych pakietów:
  - skaner dzieli nagłówek TCP na wiele fragmentów IP;
  - niektóre filtry sieciowe przepuszczają takie pakiety, ponieważ nie widząc całego nagłówka, nie mogą dopasować reguły filtracji;
  - niektóre filtry kolejkują fragmenty, ale to nie zawsze jest pożądane ze względów wydajnościowych.
- Za pomocą segmentów SYN:
  - skaner wysyła segement ze znacznikiem SYN w nagłówku;
  - odpowiedź segmentem SYN+ACK oznacza, że port jest otwarty;
  - odpowiedź segmentem RST oznacza, że port jest zamknięty;
  - takie zdarzenie zwykle nie jest zapisywane do dziennika, bo nie doszło do otwarcia połączenia.
- Za pomocą segmentów FIN:
  - otwarty port ignoruje taki segment nie należący do żadnego połączenia;
  - zamknięty port odpowiada segmentem RST;
  - segmenty nie należące do połączenia mogą być odrzucane na zaporze sieciowej.

Skanowanie portów, cd.

- Bounce Scan:
  - ukrywanie skanera bywa kluczowe dla atakującego;
  - atakujący znajduje system, który wykonuje skanowanie w jego imieniu;
  - jako pośrednika (ang. *proxy*) można wykorzystać serwer FTP, który umożliwia otwarcie połączenia do przesyłania danych.
- Za pomocą UDP:
  - skaner wysyła pusty datagram;
  - otwarty port odpowiada komunikatem błędu lub ignoruje go;
  - zamknięty port odpowiada komunikatem ICMP lub milczy.
- Za pomocą ICMP:
  - nie umożliwia skanowania portów;
  - umożliwia szybkie określenie aktywnych węzłów w sieci.
- Uzyskiwanie „odcisku palca” systemu operacyjnego:
  - systemy jednakowo odpowiadają na poprawne dane;
  - systemy różnie odpowiadają na błędne dane.

DDoS



Ping of death

- Atak ten przeprowadza się poprzez wygenerowanie pofragmentowanych pakietów ICMP przekraczających w sumie 64 kB.
- W niektórych implementacjach powoduje błąd przepełnienia bufora, prowadzący do zawieszenia systemu.
- Podobnie działa teardrop.

Land

- Agresor 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 niektórych implementacjach może to doprowadzić do zawieszenia systemu.

UDP flood

- Agresor zalewa sieć pakietami UDP przesyłanymi pomiędzy dwoma komputerami.
- Korzysta z usług:
  - echo, port 7 [RFC 862],
  - daytime, port 13 [RFC 867],
  - quote of the day, port 17 [RFC 865],
  - chargen, port 19 [RFC 864].

Email bombing, zip bombing

- Wysyłanie wiadomości o dużych rozmiarach zapychających skrzynkę odbiorczą.
- Wysyłanie małych załączników rozpakowujących się do bardzo dużych plików (np. powtórzona miliardy razy ta sama litera) – może blokować system przy sprawdzaniu programem antywirusowym, który musi rozpakować załącznik.

Smurf

- Określany też jako amplification attack.
- Jest to atak DDoS.
- Polega na wygenerowaniu dużej ilości pakietów rozgłoszeniowych (ang. *directed broadcast*) ICMP echo (ping) z adresem źródłowym IP ofiary ataku.
- Ofiara zostanie zalana odpowiedziami ping.
- Atak jest skuteczny jedynie, jeśli ruter brzegowy sieci ofiary przepuszcza ping w ukierunkowanym rozgłoszeniu, a system operacyjny stacji odpowiada na taki ping.

Fraglle

- Określany też jako amplification attack.
- Posiada identyczny schemat postępowania jak smurf.
- Wykorzystuje usługę echo UDP.

DoS guard

- DoS guard jest nazwą osobnego narzędzia lub modułu większej aplikacji zabezpieczającej, realizującego ochronę przed atakami DoS.
- Funkcje DoS guard posiada większość ścian ogniowych, a także wiele systemów operacyjnych ruterów, np. TCPintercept w CiscoIOS lub Finesse (PiX).
- Niektóre z dostępnych narzędzi są nawet dość zaawansowane, np. SYN defender w Checkpoint Firewall-1 lub SYN cookies w PiX-ach.

Kryptograficzne zabezpieczanie komunikacji

- SSH
- SSL/TLS
- IPsec