KOMUNIKACJA DANYCH I BEZPIECZEŃSTWO INFORMACJI

Czasami atakujący może po prostu podejść do komputera docelowego. Jednak w większości przypadków atakujący muszą używać sieci do osiągnięcia swoich celów. Niektóre ataki wymierzone są nawet w sieci, próbując ograniczyć lokalne sieci , a nawet globalny Internet. W niniejszej części przedstawiono przegląd sieci, aby pomóc czytelnikom, gdy natkną się oni na koncepcje sieciowe w innych miejscach lub w innych kontekstach. Obejmujemy ograniczoną liczbę koncepcji sieciowych. W szczególności koncentruje się na aspektach sieci, które są najbardziej istotne dla bezpieczeństwa. Przed rozpoczęciem czytelnicy powinni zwrócić uwagę na trzy ważne elementy terminologii, które przenikają tą część

1. Bardzo często używa się terminu oktet, który jest bajtem-zbiorem ośmiu bitów. Networking wyrósł z elektrotechniki, gdzie oktet jest preferowanym terminem; jest również szeroko stosowany w międzynarodowej społeczności technicznej.

2. Drugi termin to host. Każde urządzenie podłączone do globalnego Internetu nazywa się hostem. Obejmuje to wszystko, od dużych hostów serwerów po komputery klienckie, osobiści asystenci cyfrowi, telefony komórkowe, dostępne przez Internet.

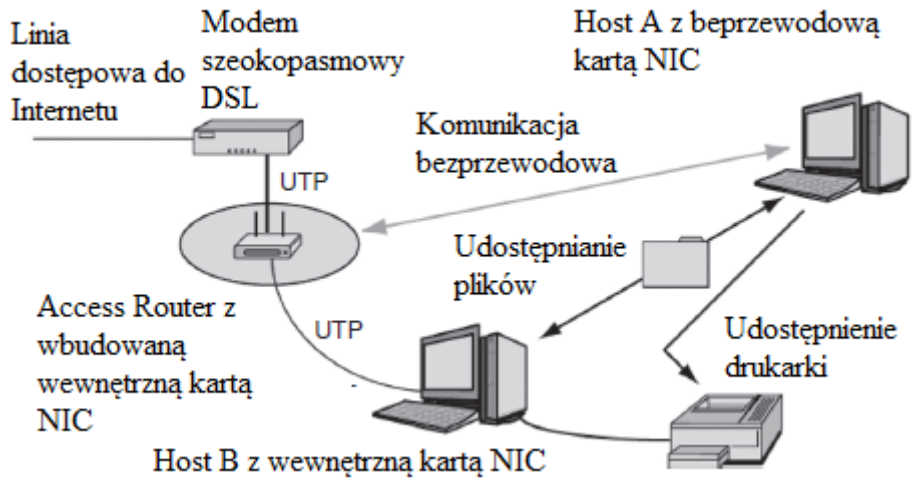
3. Rozróżniamy pojęcia internet i Internet; ten ostatni odnosi się do globalnego Internetu. Jednak internetowy pisany małymi literami jest albo warstwą internetową w architekturze TCP, albo zbiorem sieci, które nie są globalnym Internetem

PRÓBKOWANIE SIECI

Ta sekcja przedstawia krótko serię coraz bardziej złożonych sieci, dając czytelnikowi ogólny przegląd tego, jak sieci wyglądają w realnym świecie.

PROSTA SIEĆ DOMOWA.

Poniższy rysunek pokazuje prostą domową sieć komputerową. Dom ma dwa komputery osobiste. Sieć umożliwia dwóm komputerom współdzielenie plików i rodzinnej pojedynczej drukarki laserowej. Sieć łączy również dwa komputery z Internetem.



Dostęp do routera : Sercem tej sieci jest jej router dostępowy. To małe urządzenie wykonuje wiele funkcji, a przede wszystkim te pięć:

1. Działa jako przełącznik. Kiedy jeden komputer w domu wysyła komunikaty (zwane pakietami) do innych hostów, przełącznik przesyła pakiety między nimi.

2. Router dostępu to bezprzewodowy punkt dostępowy (WAP), który umożliwia łączenie się z komputerami bezprzewodowymi. Host A łączy się bezprzewodowo z routerem dostępu.

3. Router łączy sieć z inną siecią - w tym przypadku łączy wewnętrzną sieć z globalnym Internetem.

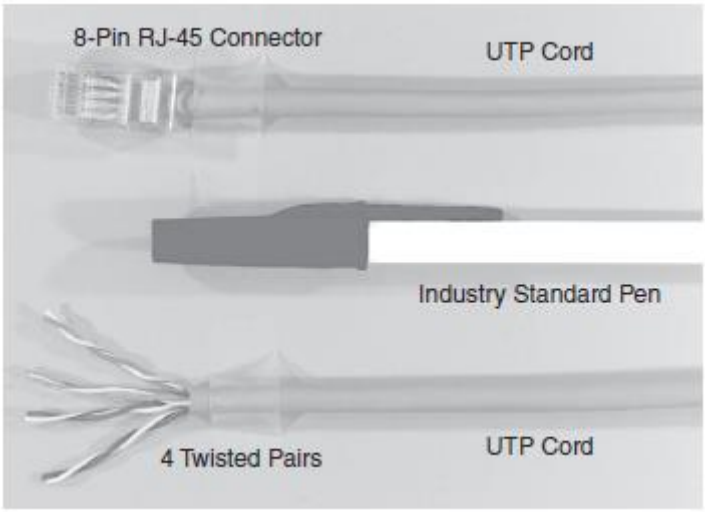
4. Aby korzystać z Internetu, każdy komputer wymaga adresu protokołu internetowego (IP). Zobaczymy później, że IP jest głównym protokołem, który reguluje komunikację przez Internet. Router dostępu ma wbudowany serwer DHCP (Dynamic Host Configuration Protocol), który nadaje każdemu komputerowi domowemu adres IP.

5. Router zapewnia translację adresów sieciowych (NAT), która ukrywa wewnętrzne adresy IP przed potencjalnymi napastnikami. Większość routerów ma również zaporę ogniową dla zwiększenia bezpieczeństwa. WAP są łatwo wykorzystywane, jeśli nie są skonfigurowane z odpowiednim uwierzytelnieniem bezpieczeństwa. Sygnały bezprzewodowe mogą być przesyłane na odległość do 243 metrów lub więcej za pomocą specjalnego sprzętu. Bez ciągłego monitorowania w celu pokonania ataków intruz może połączyć się z punktem dostępu bez wiedzy użytkownika i przechwycić wszystkie przekazywanie ruchu. Korzystanie z NAT jest niezbędne do zapewnienia bezpieczeństwa sieci domowej. Użytkownicy powinni zawsze włączać tę funkcję, aby uniemożliwić bezpośredni dostęp hostów do publicznego Internetu, w którym dominują bezpośrednie skany i ataki

komputery osobiste : Każdy z dwóch komputerów potrzebuje obwodów do komunikacji w sieci. Tradycyjnie, ten zespół obwodów był w postaci płytki drukowanej, więc zespół był nazywany komputerową kartą interfejsu sieciowego (NIC). W większości dzisiejszych komputerów zespół obwodów jest wbudowany w komputer; nie ma oddzielnej płytki drukowanej. Jednak obwody nadal nazywa się NIC komputera. W tej małej sieci dwa komputery udostępniają swoje pliki. Biorąc pod uwagę możliwości dostępu bezprzewodowego w sieci, hakerzy na poczekaniu mogą również czytać udostępnione pliki. Udostępnianie plików bez silnego zabezpieczenia bezprzewodowego jest niebezpieczne. Ważne jest skonfigurowanie zabezpieczeń Wi-Fi Protected Access (WPA lub WPA2) lub 802.11i w trybie klucza wstępnego (PSK) zarówno na routerze dostępu / punkcie dostępowym, jak i na każdym z komputerów klienckich. Ważne jest, aby skonfigurować komputery pod kątem bezpieczeństwa. Chociaż NAT sam w sobie jest silny, a większość routerów zapewnia również zapory ogniowe z kontrolą stanu, niektóre ataki będą nieuchronnie przedostawać się do sieci wewnętrznej. Hosty muszą mieć silne zapory ogniowe, programy antywirusowe i programy antyszpiegowskie; i muszą być aktualizowane automatycznie po wydaniu poprawek zabezpieczeń przez dostawcę systemu operacyjnego i przez dostawców programów aplikacji.

Okablowanie UTP

Na powyższym rysunku host B łączy się z routerem dostępu za pomocą okablowania miedzianego zwanego kablem UTP, kabla Ethernet (IEEE 802.3), lub powszechnie Cat5 (Cat5 oznacza okablowanie kategorii 5, zdefiniowane w standardzie ANSI / TIA / EIA-568-A) . Wykorzystuje okablowanie czteroparowej nieekranowanej skrętki (UTP) w płaszczu kabla. Jak pokazuje rysunek

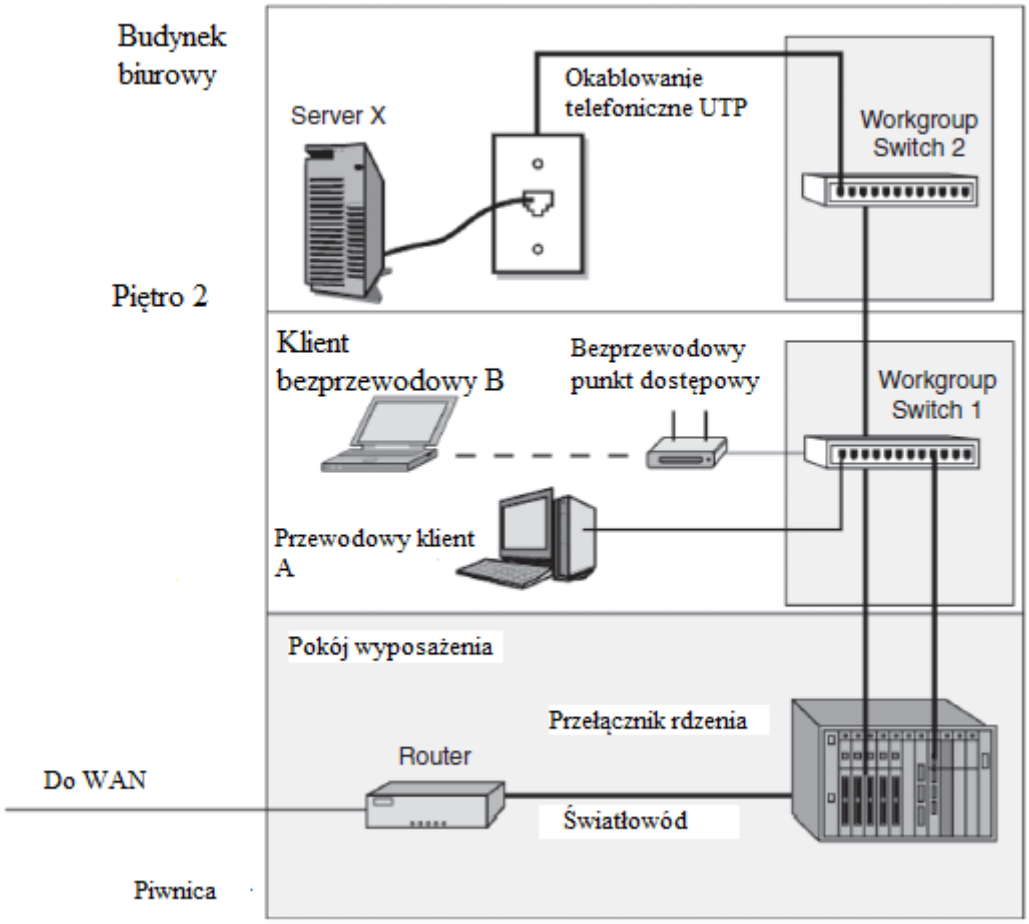


przewód UTP zawiera osiem miedzianych przewodów zorganizowanych jako cztery pary. Dwa druty każdej pary są skręcone wokół siebie. Złącza RJ-45 na końcach przewodu UTP wyglądają jak złącza telefoniczne RJ-11, ale są nieco szersze. (RJ oznacza Zarejestrowany Jack i pierwotnie odnosił się do kodów zamówień Bell System, jest teraz określany przez Radę Administracyjną ds. Załącznika Terminalu, ACTA.)

Linia dostępu do Internetu : Sieć domowa wymaga linii dostępu do Internetu, aby połączyć dom z Internetem. Na pierwszym rysunku ta linia dostępu jest linią szybkiego dostępu do cyfrowej linii abonenckiej (DSL), a domowa łączy się z tą linią dostępową za pośrednictwem niewielkiego pudełka nazywanego modemem DSL. (Modem DSL łączy się z routerem dostępowym za pośrednictwem UTP przewód, łączy się z gniazdem ściennym zwykłym kablem telefonicznym). Inny dostęp do Internetu technologie obejmują wolne modemy telefoniczne, szybkie modemy kablowe, połączenia geosynchroniczne, a nawet systemy dostępu bezprzewodowego. Większość z tych technologii jest zwana szerokopasmowymi liniami dostępowymi. Ogólnie rzecz biorąc, łącze szerokopasmowe oznacza po prostu bardzo szybko, chociaż w transmisji radiowej opisuje szeroki zakres częstotliwości.

BUDOWANIE SIECI LAN

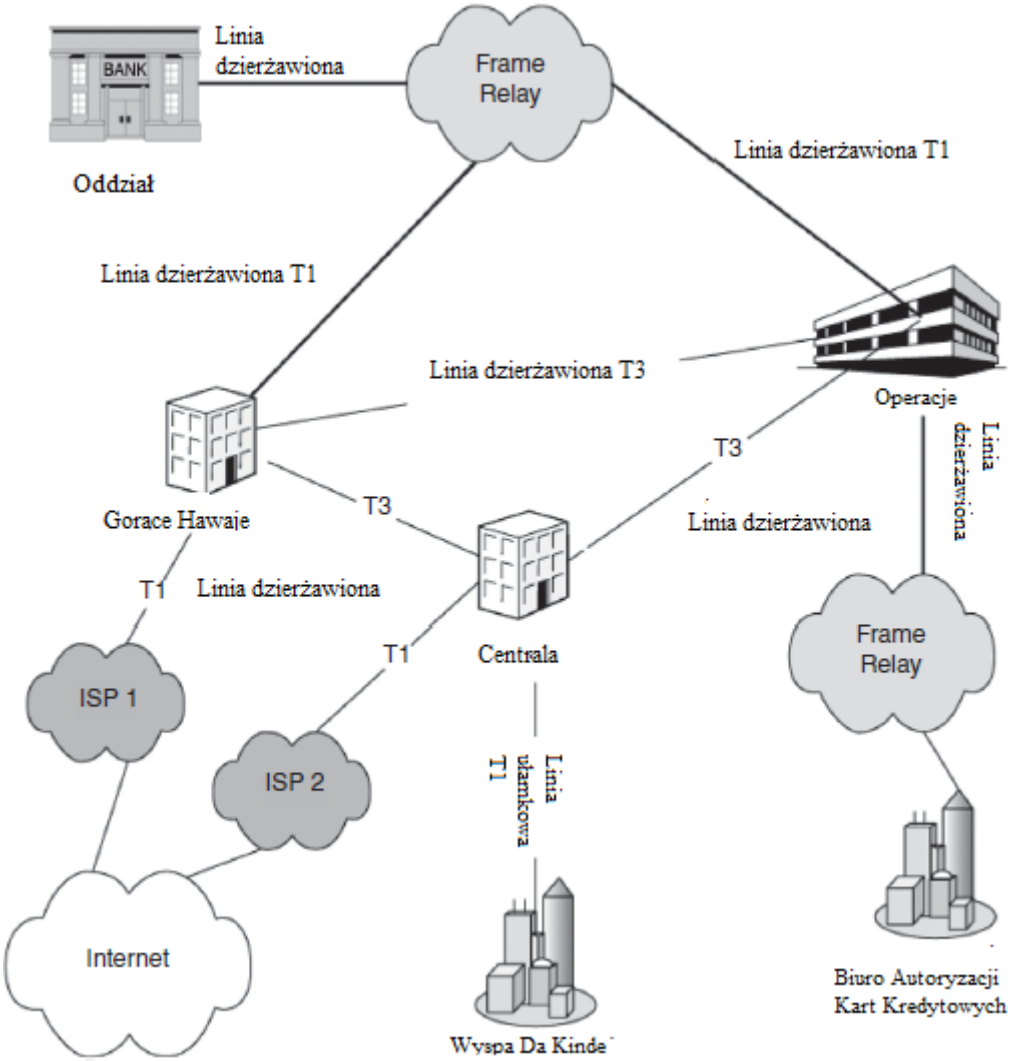
Sieć domowa pokazana na pierwszym rysunku jest siecią lokalną (LAN). Sieć LAN działa w siedzibie klienta - nieruchomości należącej do użytkownika sieci LAN. (Ze względów historycznych lokale są zawsze pisane w liczbie mnogiej.) W przypadku sieci domowej lokal składa się z domu lub mieszkania użytkownika. Ilustracja pokazuje znacznie większą sieć LAN



Tutaj lokal składa się z korporacyjnego wielopiętrowego budynku biurowego. Na każdym piętrze komputery łączą się z przełącznikiem grupy roboczej piętra za pomocą przewodu UTP lub bezprzewodowego punktu dostępowego. Przełącznik grupy roboczej na każdym piętrze łączy się z przełącznikiem rdzeniowym w pomieszczeniu wyposażenia piwnicy. Router w piwnicy łączy budynek sieci LAN ze światem zewnętrznym. Załóżmy, że klient A na piętrze 1 wysyła pakiet do serwera X na piętrze 2. Klient A wysyła pakiet do przełącznika Grupa robocza 1 na pierwszym piętrze. Przełącznik grupy roboczej wysyła pakiet do wyłącznika rdzenia w piwnicy. Przełącznik rdzenia wysyła następnie pakiet do przełącznika grupy roboczej 2, który przekazuje pakiet do serwera X. UTP jest łatwy do podsłuchu, umożliwiając atakującym odczytanie wszystkich pakietów przepływających przez przewód. Szafy telekomunikacyjne powinny być zawsze zamknięte, a kable powinny być poprowadzone przez cienkie metalowe przewody kablowe tam, gdzie to możliwe. UTP generuje również słabe sygnały radiowe, gdy przepływa przez niego ruch. Możliwe jest odczytywanie tych sygnałów z pewnej odległości za pomocą wysoce specjalistycznego sprzętu. Nowsze specyfikacje - Cat5e i Cat6 - zostały opracowane w celu zmniejszenia zakłóceń, a kable można zabezpeiczyć za pomocą ekranu, ale nawet wtedy możliwe jest podsłuchiwanie. Podsłuch poprzez stukanie kabla UTP nie jest trudny po uzyskaniu fizycznego dostępu; jednak zazwyczaj istnieją o wiele łatwiejsze sposoby uzyskania dostępu do sieci i znacznie bardziej pożądanych celów. Podsłuch na przewodzie ujawniłby każdy ruch przechodzący, ale podsłuch na routerze lub przełączniku ujawniłby ruch uliczny na wielu przewodach. Fizyczne bezpieczeństwo jest ważnym aspektem bezpieczeństwa sieci i musi być odpowiednio rozwiązane, ale większość ataków opiera się dziś na więcej wirtualnych lukach.

FIRMOWE SIECI ROZLEGŁE (WAN)

Chociaż sieci lokalne działają w siedzibie firmy, sieci rozległe (WAN) łączą geograficznie oddzielne witryny - zwykle w ramach jednej korporacji. Korporacje nie mają uprawnień regulacyjnych niezbędnych do prowadzenia przewodów w obszarach publicznych. W przypadku usługi WAN firmy muszą korzystać z firm zwanych operatorami, którzy mają te prawa pierwszeństwa. Rysunek pokazuje, że większość firm korzysta z WAN wielu operatorów.

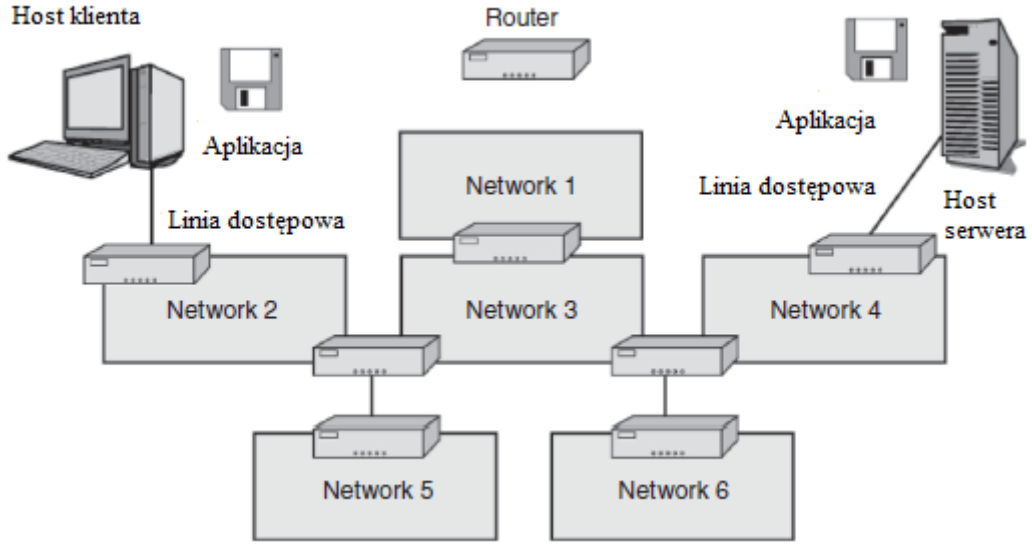


Na rysunku niektóre witryny w tej firmie są połączone liniami dzierżawionymi typu punkt-punkt od firmy telekomunikacyjnej. Firmy również subskrybują usługi sieci komutowanej, które przesyłają ruch między kilkoma witrynami. Ekspozycja pokazuje, że te przełączane usługi sieciowe korzystają z technologii Frame Relay. Firma korzysta z dwóch oddzielnych sieci Frame Relay - jednej do łączenia własnych witryn i drugiej w celu połączenia z inną firmą. Technologia przenoszenia jest zwykle uważana za bezpieczniejszą przez specjalistów od bezpieczeństwa ze względu na jej zamknięty charakter. W przeciwieństwie do Internetu, który pozwala każdemu się z nim połączyć, tylko firmy komercyjne mogą łączyć się z sieciami WAN operatora, co utrudnia dostęp osobom atakującym. Dostęp atakującego nie jest jednak niemożliwy. Na przykład, jeśli atakujący włamie się do komputera będącego własnością dostawcy (lub nawet przez klienta), to naruszenie może umożliwić dostęp. Ponadto sam dosatwca wie, w jaki sposób kieruje ruchem w swojej sieci. To powinno powstrzymać napastników, nawet jeśli w jakiś sposób uzyska dostęp do sieci. Jednak takie bezpieczeństwo przez zaciemnienie jest uważane przez specjalistów ds. bezpieczeństwa za kiepską praktykę, ponieważ atakujący mogą włamać się do komputerów przenośnych, aby uzyskać dostęp do informacji o routingu. Chociaż technologia nośnej

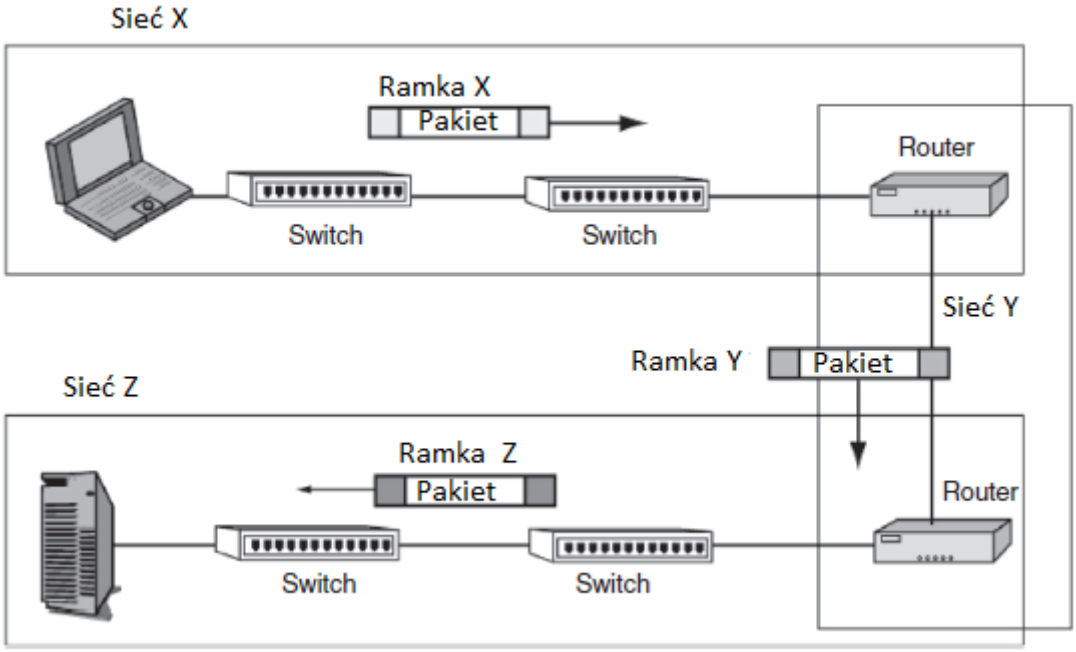
jest bezpieczniejsza, jest również niezwykle kosztowna. Wraz z rozwojem wirtualnych sieci prywatnych (VPN) firmy mogą łączyć geograficznie różne grupy komputerów praktycznie za pośrednictwem wspólnego Internetu. Zapewnia to znaczną część korzyści bezpieczeństwa sieci WAN, a jednocześnie radykalnie obniża koszty wdrożenia.

INTERNET

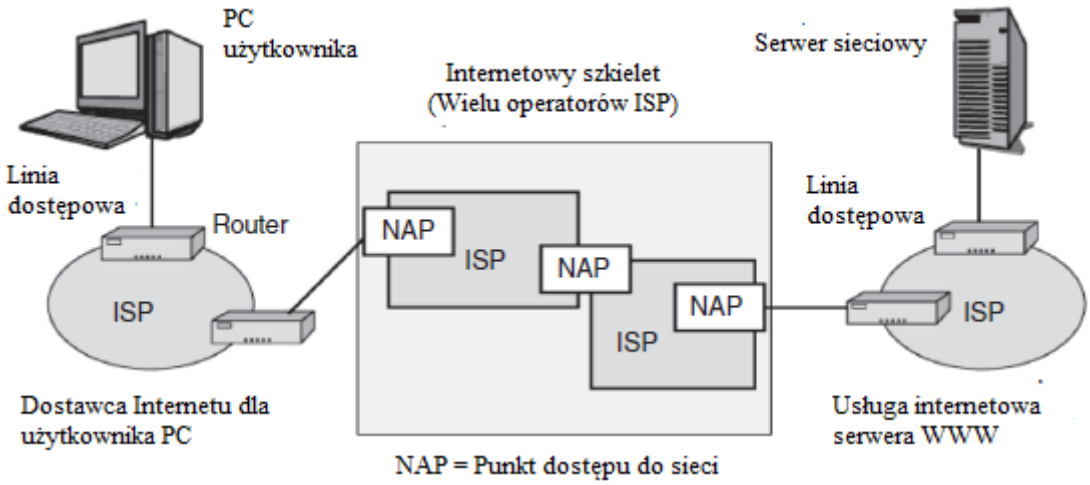
Pod koniec lat 70. na świecie było wiele sieci LAN i WAN. Wiele z WAN było sieciami non-profit, które łączyły uniwersytety i instytucje badawcze. Niestety komputery w jednej sieci nie mogły komunikować się z komputerami w innych sieciach. Aby rozwiązać ten problem, Agencja Zaawansowanych Projektów Badawczych ds. Obrony (DARPA) stworzył ARPANET w 1969 roku, źródło dzisiejszego Internetu, oparte na pionierskim konceptualnym projekcie tego, co J. C. R. Licklider nazwał Intergalactic Computer Network w artykule z 1963 roku. Z definicji internet łączy ze sobą poszczególne sieci. Później sieci komercyjne mogły dołączyć do późniejszych wersji ARPANET i stały się internetem, który znamy dzisiaj. Ilustracja poniższa pokazuje, że urządzenia zwane routerami łączą poszczególne sieci.



Początkowo urządzenia te nazywane były bramami. Termin bramy został użyty zamiast "routera" w niektórych wczesnych standardach, ale większość dostawców przyjęła teraz nazwa "router". Istnieją dwa wyjątki, z których pierwszy to Microsoft, który wciąż ma tendencję do wywoływania routerów "bramek". Drugim jest router bezpośrednio dostępny dla sieci, oraz w ten sposób pierwszy przeskok podczas wychodzenia z sieci jest często nazywany bramą domyślną. Każdy komputer w dowolnej sieci w Internecie może wysyłać wiadomości do dowolnego komputera w dowolnej innej sieci w Internecie. Wiadomości przesyłane z komputera do komputera przez Internet są nazywane pakietami. Rysunek pokazuje, że pakiet przemieszcza się z hosta źródłowego do hosta docelowego.



Po drodze jest on kierowany przez różne sieci aż do przybycia do miejsca docelowego. Globalny Internet wykorzystuje zestaw protokołów komunikacyjnych, znanych jako protokół transmisji / protokół internetowy (TCP / IP). Ponadto wiele firm buduje oddzielne wewnętrzne sieci TCP / IP do własnej komunikacji. Te wewnętrzne sieci nazywane są intranetami, aby odróżnić je od Internetu. Początkowo bezpieczeństwo w sieciach wewnętrznych było stosunkowo niewielkie, ponieważ zakładano, że zewnętrzni napastnicy będą mieli trudności z dostaniem się do firmowych intranetów. Jeśli jednak haker przejmie wewnętrzny komputer podłączony do intranetu, bezpieczeństwo stanie się poważnym problemem. W związku z tym większość firm stopniowo wzmacnia bezpieczeństwo swoich intranetów. Rysunek pokazuje, że poszczególne domy i korporacje łączą się z Internetem za pośrednictwem operatorów zwanych dostawcami usług internetowych (ISP).



Internet ma wielu dostawców usług internetowych, ale wszyscy łączą się w centrach, które zazwyczaj nazywają się punktami dostępu do sieci (NAP). Połączenia te umożliwiają globalną komunikację dla wszystkich podłączonych hostów. Większość dostawców usług internetowych to komercyjne organizacje działające dla zysku w celu zapewnienia dostępu do Internetu dla użytkowników domowych. Nie ma centralnej kontroli dostępu do Internetu; istnieją jednak centralne agencje do

kontrolowania systemów nazw domen (DNS) zwanych rejestratorami. Kiedy Internet powstał pod koniec lat siedemdziesiątych XX wieku, podjęto świadomą decyzję o promowaniu otwartości i nie dodawaniu ciężarów bezpieczeństwa. W wyniku braku technologii bezpieczeństwa i otwartego dostępu do niemal każdego, zabezpieczenie Internetu to koszmar. Firmy, które przesyłają poufne informacje przez Internet, muszą rozważyć ochronę kryptograficzną.

APLIKACJE

Mimo że wewnętrzne funkcjonowanie Internetu polega na sieciach, większość użytkowników zdaje sobie sprawę tylko z powszechnie używanych aplikacji działających na sieciach. Znane aplikacje osobiste to między innymi World Wide Web, poczta e-mail i wiadomości błyskawiczne. Korporacje używają niektórych z tych aplikacji, ale korzystają również z wielu aplikacji biznesowych, takich jak księgowość, płace, rozliczenia i zarządzanie zapasami. Aplikacje biznesowe często są aplikacjami do przetwarzania transakcji, które charakteryzują się dużą ilością prostych powtarzalnych transakcji. Natężenie ruchu generowane przez przetwarzanie transakcji i inne aplikacje biznesowe zwykle znacznie przewyższają ruch osobistych aplikacji w firmie. Wszystkie programy zawierają błędy, w tym luki w zabezpieczeniach. Istnieje wiele aplikacji, a śledzenie luk w aplikacjach i ciągłe łatanie wielu aplikacji jest ogromnym zadaniem, które zbyt łatwo można odłożyć lub zakończyć tylko częściowo. Ponadto każda aplikacja musi być skonfigurowana z opcjami zapewniającymi wysokie bezpieczeństwo, a ochrona musi być zarządzana w każdej aplikacji (np. antywirus i blokowanie spamu w wiadomościach e-mail).

PROTOKÓŁ SIECIE I ZBEZPIECZENIA

Produkty różnych dostawców sieci muszą współpracować (współdziałać). Jest to możliwe tylko wtedy, gdy istnieją silne standardy komunikacyjne, które regulują sposób interakcji sprzętu i oprogramowania. Dzięki takim standardom dwa lub więcej programów może skutecznie współpracować. Normy wiążą się z trzema problemami bezpieczeństwa. Jednym jest sam standard. Na przykład Standard TCP omówiony w dalszej części jest trudny do zaatakowania, ponieważ atakujący nie może wysłać fałszywej wiadomości, chyba że jest w stanie odgadnąć numer sekwencji następnej wiadomości. Zwykle jest to bardzo trudne. Jednakże, jeśli atakujący wyśle komunikat RST (reset), który kończy połączenie, ochrona ta zostaje znacznie zmniejszona. W rzeczywistości dość łatwo jest wysyłać wiadomości RST, które są blisko otwartej znajomości. Drugi problem to bezpieczeństwo wbudowane w standard. Większość standardów została stworzona bez zabezpieczeń, a zabezpieczenia zostały dodane tylko w późniejszych wersjach, czasami w sposób niezręczny . Na przykład IP, który jest głównym protokołem dostarczania pakietów przez Internet, początkowo nie miał żadnych zabezpieczeń. Standardy bezpieczeństwa IP (IPsec, wymawiane eye-pea-sek) zostały stworzone, aby rozwiązać ten problem, ale IPsec jest uciążliwy i nie jest powszechnie stosowany. Inną wadą bezpieczeństwa we wczesnych wersjach IP, w tym w szeroko stosowanym IPv4, jest ograniczenie przestrzeni adresowej spowodowane 32-bitowym polem adresu w pakiecie IPv4 (co daje przestrzeń adresową około 4 × 10⁹); rozwiązanie problemu wyczerpania adresów IPv4 rozwiązuje migracja do IPv6, 128-bitowe adresy (przestrzeń adresowa około 3 × 10³⁸). Kolejną kwestią jest bezpieczeństwo wdrażania standardów w produktach dostawców. Większość ataków, których celem są słabości standardów, atakuje produkty dostawców, które mają luki w zabezpieczeniach, niezwiązane z protokołami, które implementują

STANDARDY

Bezpieczeństwo sieci i sieci zależy od standardów. Normy zezwalały na globalne połączenia międzysieciowe, w przeciwieństwie do wczesnych lat tworzenia sieci, gdy produkty zastrzeżone dominowały w świecie komputerów, a wzajemne połączenia były trudne lub niemożliwe.

WARSTWY RDZENIA

Standardy są skomplikowane, a kiedy ludzie radzą sobie ze złożonymi problemami, zazwyczaj dzielą te problemy na mniejsze części i mają różnych specjalistów pracujących nad różnymi częściami. Poniżej pokazano, że normy są podzielone na trzy podstawowe warstwy, które łącznie mają funkcjonalność niezbędną do umożliwienia programowi aplikacji w jednej sieci w Internecie współdziałania z innym programem w innym komputer w innej sieci.

Super Warstwa :	**Opis**
Aplikacja	:Komunikacja między programami aplikacji na różnych hostach podłączonych do różnych sieci w siecI
Internetworking	:Przesyłanie pakietów w routowanym Internecie. Pakiety zawierają komunikaty warstwy aplikacji.
Pojedyncza sieć	:Transmisja pakietów w sieci jednokomutowanej

W warstwie podstawowej aplikacji obie aplikacje muszą być w stanie efektywnie współpracować. Na przykład, dostęp do aplikacji w World Wide Web, dwa programy aplikacji to przeglądarka na komputerze klienckim i program serwera WWW na serwerze WWW. Standardowe interakcje w sieci WWW to protokół HTTP (Hypertext Transfer Protocol). Zarówno aplikacje przeglądarki, jak i serwera WWW muszą wysyłać wiadomości zgodne ze standardem HTTP. Warstwa środkowa jest warstwą rdzeniową Internetu. Standardy na tej warstwie określają sposób dostarczania pakietów w routowanym Internecie. Jednym z głównych standardów internetowej warstwy podstawowej jest Internet Protocol (IP). Zobaczymy później inne standardy pracy w Internecie. Najniższą warstwą rdzenia jest warstwa rdzenia o pojedynczej sieci. Standardy na tej warstwie regulują transmisję pakietów przez przełączniki i linie transmisyjne w sieci z jednym komutatorem (LAN lub WAN).

ARCHITEKTURA STANDARDÓW WARSTWOWYCH

Normy są tworzone przez agencje normalizacyjne. Te agencje normalizacyjne najpierw tworzą szczegółowe plany tworzenia warstw dla tworzenia standardów. Te konkretne plany warstw są nazywane architekturami warstwowych standardów. Następnie agencje normalizacyjne tworzą standardy na poszczególnych warstwach. Poniżej pokazano dwie popularne architektury warstw i łączy te architektury standardów z trzema warstwami rdzeni, które widzieliśmy wcześniej. Internet Engineering Task Force (IETF) to agencja standardów dla Internetu. Jego architektura standardów nazywa się TCP / IP - nazwa pochodzi od dwóch najważniejszych standardów, TCP i IP. TCP / IP ma cztery warstwy.

Super Warstwa :	**Aplikacja**
TCP/IP :	Aplikacja
OSI :	Aplikacja, Prezentacja, Sesja
Hybrydowe TCP/IP - OSI :	Aplikacja

Super Warstwa:	Internet
TCP/IP :	Transport, Internet
OSI :	Transport, Sieć

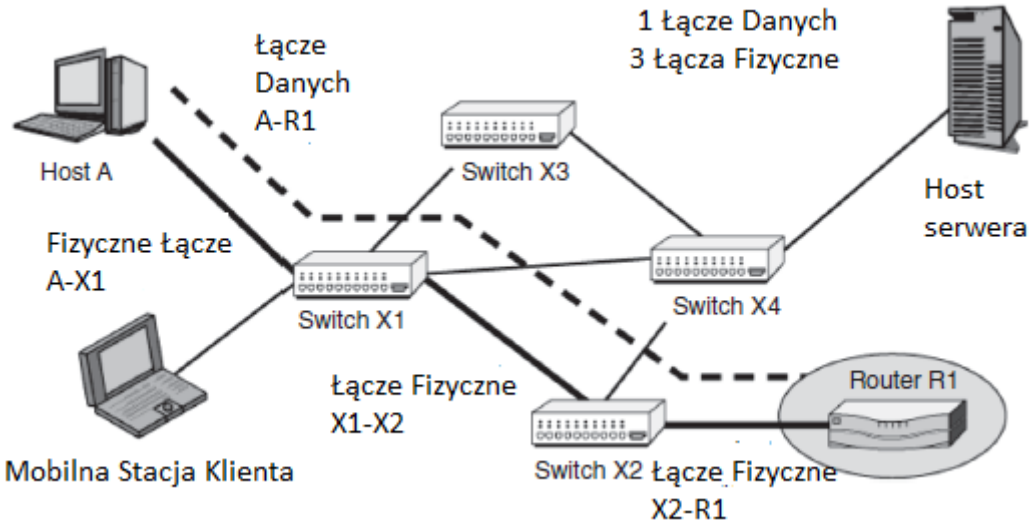
Hybrydowe TCP/IP - OSI :	Transport , Internet

Super Warstwa:	Sieć
TCP/IP :	Dostęp do podsieci
OSI :	Łącze danych, FizycZna
Hybrydowe TCP/IP - OSI :	Łącze danych, Fizyczna

Dolna warstwa, warstwa dostępu do podsieci, odpowiada warstwie rdzenia z pojedynczą siecią. Z kolei warstwa wierzchnia to warstwa aplikacji, która odpowiada warstwie rdzenia aplikacji. Dwie środkowe warstwy - warstwa internetowa i transportowa - odpowiadają internetowej warstwie rdzeniowej. TCP / IP koncentruje się głównie na pracy w Internecie. Podział tej warstwy rdzeniowej na dwie warstwy TCP / IP pozwala na większy podział pracy w opracowywaniu standardów. Inna architektura standardów pokazana na rysunku to OSI, która jest rzadko opisywana przez swoją pełną nazwę - Model odniesienia otwartych połączeń między systemami. OSI jest zarządzane przez dwie agencje normalizacyjne. Jednym z nich jest ISO, Międzynarodowa Organizacja Normalizacyjna. Drugą jest ITU-T, Międzynarodowa Unia Telekomunikacyjna - Sektor Norm Telekomunikacyjnych. (Oficjalne nazwy i oficjalne akronimy nie pasują do siebie, ponieważ pochodzą z różnych języków). Tabela pokazuje, że OSI dzieli trzy warstwy rdzenia na siedem warstw. Pojedyncze sieci OSI stosują standardy na dwóch warstwach - warstwy fizyczne i łącza danych. Przewaga rynkowa OSI jest tak silna na warstwach fizycznych i łącza danych, że IETF rzadko opracowuje standardy na tych warstwach. Wskazanie dostępu do podsieci w strukturze TCP / IP zasadniczo oznacza tutaj stosowanie standardów OSI. Żadna z tych dwóch architektur standardów nie dominuje. Co prawie wszystkie firmy używają dziś jest to hybrydowa architektura standardów TCP / IP-OSI, którą ilustruje rysunek. Ta hybrydowa architektura wykorzystuje standardy OSI w warstwie fizycznej i łącza danych oraz w standardach TCP / IP w warstwie internetowej i transportowej. Korporacje stosują również standardy z innych architektur standardów w Internecie i warstwach transportowych, ale dominują standardy TCP / IP. Na poziomie warstwy aplikacji sytuacja jest złożona. Stosowane są zarówno standardy OSI, jak i TCP / IP, często w połączeniu. W rzeczywistości, standardy OSI często odnoszą się do standardów TCP / IP i odwrotnie. Chociaż OSI i TCP / IP są często postrzegane jako rywale, w rzeczywistości tak nie jest. Kilka innych agencji normalizacyjnych tworzy również standardy warstwy aplikacji, co jeszcze bardziej komplikuje obraz.

STANDARDY POJEDYNCZEJ SIECI

Jak już wspomniano, standardy OSI dominują w dwóch warstwach jednej sieci - fizycznej i łącza danych. Rysunek pokazuje, w jaki sposób powiązane są warstwy fizyczne i łącza danych.



Warstwa łącza danych: Ścieżka, którą ramka przechodzi przez pojedynczą sieć nazywana jest łączem danych ramki. Na rysunku powyższym łącze danych przebiega między hostem A i routerem R1. To łącze danych przechodzi przez Przełącznik X1 i Przełącznik X2. Komputer źródłowy przesyła ramkę do pierwszego przełącznika, który przesyła ramkę dalej do następnego przełącznika wzdłuż łącza danych, które przekazuje dalej ramkę. Ostatni przełącznik wzdłuż łącza danych przekazuje ramkę do komputera docelowego (lub routera, jeśli pakiet w ramce jest przeznaczony dla komputera w innej sieci).

Warstwa fizyczna : Normy warstwy fizycznej regulują fizyczne połączenia między kolejnymi urządzeniami wzdłuż łącza danych. Na powyższym rysunku te fizyczne połączenia to A-X1, X1-X2 i X2-R1. Wcześniej widzieliśmy popularne medium transmisyjne, nieekranowany skrętka w kablach Cat5. UTP dominuje w połączeniach pomiędzy komputerami a przełącznikami grup roboczych. Sygnały UTP zazwyczaj obejmują zmiany napięcia. Na przykład, wysokie napięcie może wskazywać 1, podczas gdy niskie napięcie może wskazywać 0. (Rzeczywiste wzorce napięciowe są zwykle znacznie bardziej złożone.) W przypadku dłuższych odległości i bardzo dużych prędkości, innym popularnym medium transmisyjnym jest światłowód, który wysyła sygnały świetlne przez cienkie szklane rurki. Sygnały światłowodowe są rzeczywiście bardzo proste. W cyklu zegara światło jest włączane dla 1 lub wyłączone dla 0. Przewody UTP działają jak anteny radiowe, gdy przenoszą sygnały. Niektóre sygnały zawsze promieniują, pozwalając ludziom przechwytywać sygnały transmisji, umieszczając urządzenia w pobliżu (ale nie dotykając) kabla. Zrozumienie i interpretacja emisji elektromagnetycznych z urządzeń komputerowych nazywa się van Eck phreaking (znany również pod nazwą kodową "TEMPEST" przez NSA) po tym, jak holenderski naukowiec Wim van Eck opublikował w 1985 r. artykuł pokazujący, jak monitorować i odtwarzać wyciekające sygnały z terminali katodowych (CRT). W przeciwieństwie do tego światłowód wymaga fizycznego gwintowania w kable światłowodowym. Fizyczne podsłuchiwanie można również wykonać za pomocą UTP, ale często są znacznie łatwiejsze metody przechwytywania lub kradzieży ruchu, niż próby fizycznego dotknięcia przewodów. Transmisja bezprzewodowa wykorzystuje fale radiowe. Pozwala to na wyświetlanie urządzeń mobilnych w sposób, jaki nigdy wcześniej nie był możliwy. Transmisja bezprzewodowa jest używana zarówno do transmisji LAN, jak i WAN. Sygnały radiowe rozprzestrzeniają się szeroko, nawet gdy są używane anteny antenowe. W związku z tym, bardzo łatwo jest podsłuchiwać w transmisjach radiowych i robić inne psoty. Sygnały radiowe muszą być silnie zaszyfrowane, a strony muszą być silnie uwierzytelnione, aby zapobiec wysyłaniu przez oszustów transmisji radiowej. Sygnalizacja radiowa jest bardzo złożona. Większość sygnalizacji radiowych wykorzystuje transmisję z rozsiewem widmowym, w której informacje są przesyłane w szerokim zakresie częstotliwości. Rozpiętość transmisji widmowej służy do

poprawy niezawodności propagacji. Transmisja radiowa ma wiele problemów z propagacją, takich jak zakłócenia z innych źródeł. Wiele problemów występują tylko przy określonych częstotliwościach. Rozprzestrzeniając sygnał na szerokie spektrum częstotliwości i robiąc to w sposób redundantny, sygnał będzie nadal zrozumiały, nawet jeśli występują poważne problemy na niektórych częstotliwościach. Prabakaran Kalkakar podsumował korzyści płynące z komunikacji w zakresie widma rozproszonego następująco: Systemy z widmem rozproszonym zapewniają projektantom wyraźne korzyści ... [H] Jest to dziewięć korzyści, których projektanci mogą się spodziewać w przypadku korzystania z systemu bezprzewodowego opartego na widmie rozproszonym.

1. Zmniejszone interferencje przesłuchu: w systemach z widmem rozproszonym, interferencja przesłuchów jest znacznie osłabiona ze względu na wzmocnienie przetwarzania systemu widma rozproszonego, jak opisano wcześniej

2. Lepsza jakość głosu / integralność danych i mniej szumu statycznego

3. Obniżona podatność na wielościeżkowe zanikanie

4. Bezpieczeństwo wewnętrzne: W systemie z widmem rozproszonym sekwencja PN [pseudolosowa] jest używana do modulowania sygnału w dziedzinie czasu (systemy sekwencji bezpośrednich) lub wyboru częstotliwości nośnej (systemy przeskoków częstotliwości). Ze względu na pseudolosowy charakter sekwencji PN, sygnał w powietrzu został "randomizowany". Tylko odbiornik mający dokładnie taką samą sekwencję pseudolosową i synchroniczne taktowanie mogą rozproszyć i odzyskać oryginalny sygnał. W związku z tym system widma rozproszonego zapewnia bezpieczeństwo sygnału, które nie jest dostępne dla konwencjonalnych analogowych systemów bezprzewodowych.

5. Współistnienie: system widma rozproszonego jest mniej podatny na zakłócenia niż inne nierozproszone systemy widmowe. Ponadto, przy prawidłowym projektowaniu sekwencji pseudolosowych, wiele systemów widma rozproszonego może współistnieć bez powodowania poważnych zakłóceń w innych systemach. To dodatkowo zwiększa pojemność systemu dla widma rozproszonego systemy lub urządzenia.

6. Dłuższe odległości robocze

7. Trudne do wykrycia: sygnały o rozproszonym spektrum są znacznie szersze niż konwencjonalna transmisja wąskopasmowa (rzędu 20-254 razy w stosunku do szerokości pasma transmisji wąskopasmowych). Ponieważ pasmo komunikacyjne jest rozproszone, może być transmitowane z małą mocą, nie będąc szkodliwie przez szumy tła

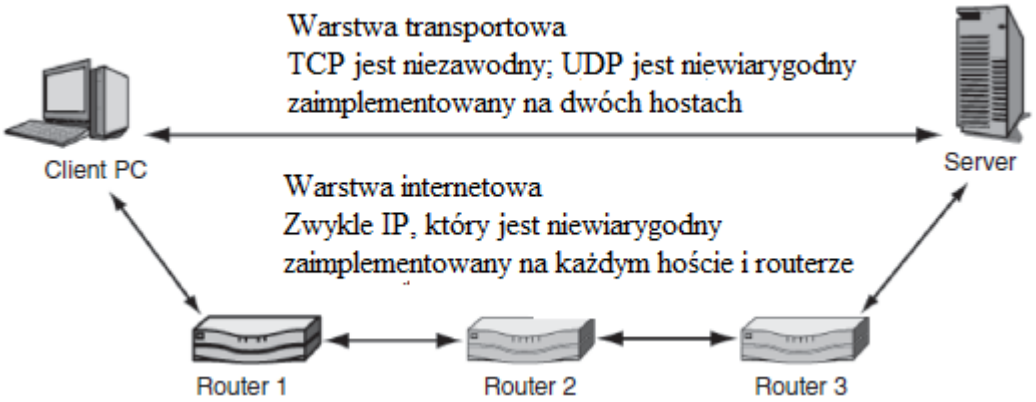
8. Trudne do przechwycenia lub demodulacji: podstawą techniki rozprzestrzeniania jest kod stosowany do rozprzestrzeniania sygnału

9. Trudniej zablokować: Najważniejszą cechą widma rozproszonego jest jego zdolność do odrzucania zakłóceń

Wojsko wykorzystuje transmisję z rozsiewem częstotliwości (FHSS) do celów bezpieczeństwa. Wojskowa transmisja z rozsiewem widmowym działa w taki sposób, że utrudnione są transmisje przechwytujące. Cywilna transmisja o widmie rozproszonym ma natomiast na celu ułatwienie łączenia, a zatem zapewnia stosunkowo niewielkie bezpieczeństwo. Przełączniki spędzają prawie cały czas na przekierowaniu ramek. Jednakże, przełączniki spędzają część czasu na wymianie pakietów informacji nadzorujących ze sobą, aby sieć działała sprawnie. Na przykład w sieci Ethernet (IEEE 802.3), która dominuje standardy LAN, jeśli między przełącznikami są pętle, sieć będzie działać nieprawidłowo. Jeśli przełącznik wykryje pętlę, wysyła pakiety nadzorcze do innych przełączników. Przełączniki w sieci

komunikują się, dopóki nie określą najbardziej odpowiedniej ścieżki i nie będą blokować innych portów, aby zapobiec wewnętrznej pętli. Proces ten jest zarządzany przez protokół drzewa opinającego (STP, część IEEE 802.1) lub nowszy protokół Rapid Spanning Tree (RSTP, zdefiniowany w IEEE 802.1w i obecnie część IEEE 802.1D-2004). Atakujący mogą tworzyć ataki DoS (Denial-of-Service) na przełączniki w sieci podszywając się pod przełącznik i wysyłając zalew fałszywych wiadomości do prawdziwych przełączników sieci, wskazując na obecność pętli. Przełączniki mogą spędzać tak wiele czasu na reorganizacji sieci, że nie będą w stanie obsłużyć legalnego ruchu. Może także atakować kilka innych protokołów nadzorczych, aby przełączniki były niedostępne do przetwarzania normalnych pakietów. Standard 802.1AE został zaprojektowany w celu ograniczenia przełączania między przełącznikami komunikacja z uwierzytelnionymi przełącznikami.

Normy dotyczące Internetu: Jak wspomniano wcześniej, IETF podzielił rdzeń sieci internetowej na dwie warstwy - warstwę internetową i transportową. Rysunek pokazuje, w jaki sposób te dwie warstwy są ze sobą powiązane.

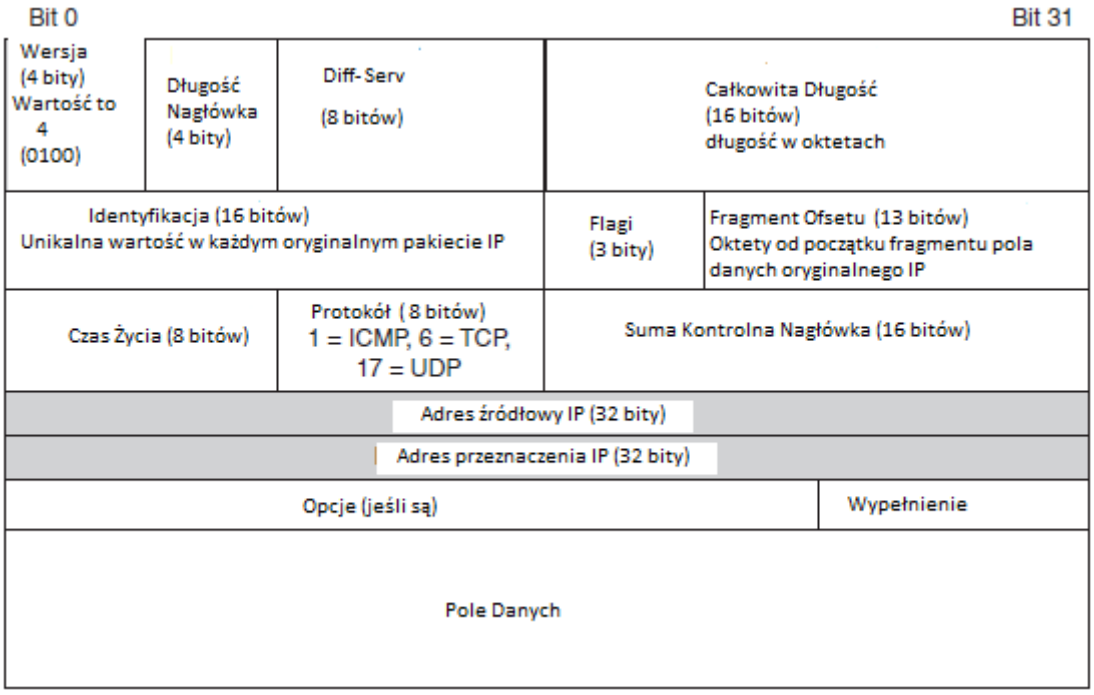


Warstwa internetowa przekazuje pakiety, przeskakując chmielem, pomiędzy routerami, aż pakiet dotrze do hosta docelowego. Podstawowym standardem w warstwie internetowej jest Internet Protokół (IP). Projektanci TCP / IP zdali sobie sprawę, że nie są w stanie przewidzieć, jakie usługi zapewnią pojedyncze sieci łączące routery. Protokół IP został wykonany w prosty sposób, aby uzyskać minimalną funkcjonalność w pojedynczych sieciach po drodze. Nie ma gwarancji, że pakiety w ogóle dotrą lub, jeśli się pojawią, że dotrą do celu. Aby zrekompensować ograniczenia IP, dodano warstwę transportową. Główny standard przeznaczony dla tej warstwy, TCP (Transmission Control Protocol), został utworzony jako protokół o wysokiej zdolności, który naprawiałby wszelkie błędy popełniane po drodze, zapewniał porządkowanie pakietów, powolną transmisję, gdy sieć była przeciążona, oraz zrobić kilka innych rzeczy. W przypadku aplikacji, które nie wymagały takiego poziomu niezawodności, utworzono prostszy standard - User Datagram Protocol (UDP).

PROTOKÓŁ INTERNETOWY

Protokół internetowy (IP) robi dwie główne rzeczy. Po pierwsze, określa sposób organizacji pakietów. Po drugie, określa sposób, w jaki routery przesuwają pakiety do hosta docelowego. (Analogicznie, standardy warstwy łącza danych decydują o tym, jak zorganizowane są ramki zawierające pakiety i jak przełączniki po drodze przesuwają ramkę przez sieć z jednym komutatorem).

Pakiet IP w wersji 4 : Główną wersją protokołu internetowego jest wersja 4 (IPv4). (Nie było wersji 0, 1, 2 ani 3.) Ta wersja była w użyciu od czasu jej definicji w 1981 roku i będzie nadal używana przez wiele lat, chociaż IPv6 ma to zastąpić. Ilustracja przedstawia organizację pakietu IPv4.



Pakiet to długi strumień 1 i 0. Nagłówek IP zwykle jest wyświetlany w kilku wierszach, z 32 bitami w każdym rzędzie. Pierwszy wiersz zawiera bity od 0 do 31; następny wiersz pokazuje bity od 32 do 63 i tak dalej. Nagłówek jest podzielony na mniejsze jednostki zwane polami. Pola są definiowane przez ich bit pozycja w pakiecie. Na przykład pierwsze cztery bity zawierają pole numeru wersji. Są to bity od 0 do 3. W IPv4 to pole zawiera 0100, czyli 4 w binarnym. Pole długości nagłówka zawiera następne cztery bity (bity od 3 do 7).

Pierwszy rząd : Jak już wspomniano, pierwsze pole (bity od 0 do 3) jest polem numeru wersji. W IPv4 wartość wynosi 0100 (4). W nowszej wersji protokołu IP, wersja 6 (IPv6), wartość wynosi 0110. Kolejne pole to pole długości nagłówka. Daje to długość nagłówków w jednostkach 32-bitowych. Jak pokazuje rysunek 5.12, nagłówek bez opcji ma pięć linii 32-bitowych, więc to pole będzie miało wartość 0101 (5 w binarnym). Korzystanie z opcji jest w praktyce rzadkością. W rzeczywistości opcje mają tendencję do wskazywania na ataki. Dlatego wartość większa niż 5 w polu długości nagłówka wskazuje, że nagłówek pakietu ma opcje i dlatego jest podejrzany. Pole 1-oktetowe dif-serv (usługi różnicowe) zostało utworzone, aby umożliwić różnym usługom (priorytet itp.) Ten pakiet. Jednak to pole zwykle nie jest używane. Pole całkowitej długości podaje długość całego pakietu IP w oktetach (bajtach). Biorąc pod uwagę 16-bitową długość tego pola, maksymalna liczba oktetów w pakiecie IP wynosi 65 536 (216). Większość pakietów IP jest jednak znacznie mniejsza. Długość pola danych to całkowita długość pomniejszona o długość nagłówka w oktetach.

Drugi rząd : Jeśli pakiet IP jest zbyt długi dla pojedynczej sieci po drodze, router wysyłający pakiet do tej sieci podzieli jego zawartość na kilka mniejszych pakietów. Do złożenia na docelowym hoście, wszystkie pakiety fragmentów otrzymują tę samą wartość pola identyfikacyjnego, co w oryginalnym pakiecie. Oktety danych w oryginalnych pakietach są ponumerowane i liczba pierwszych danych oktet w pakiecie otrzymuje wartość odsunięcia fragmentu (13 bitów). Istnieją trzy pola flag (pola 1-bitowe). Jeden z nich, więcej fragmentów, ma wartość 1 we wszystkich oprócz ostatniego pakietu, w którym jest tworzony 0. Informacje w tych trzech polach pozwalają docelowemu hostowi uporządkować pakiety i wiedzieć, kiedy pakiety nie mogą przybyć. Fragmentacja IP przez routery jest zwykle rzadka, a napastnicy mogą używać fragmentacji do ukrywania informacji o ataku. Nawet jeśli pierwszy fragment fragmentu zostanie upuszczony przez zaporę ogniową, inne pakiety, które nie mają

informacji o sygnaturze w pierwszym nagłówku, mogą przejść. Dlatego fragmentacja IP jest podejrzana.

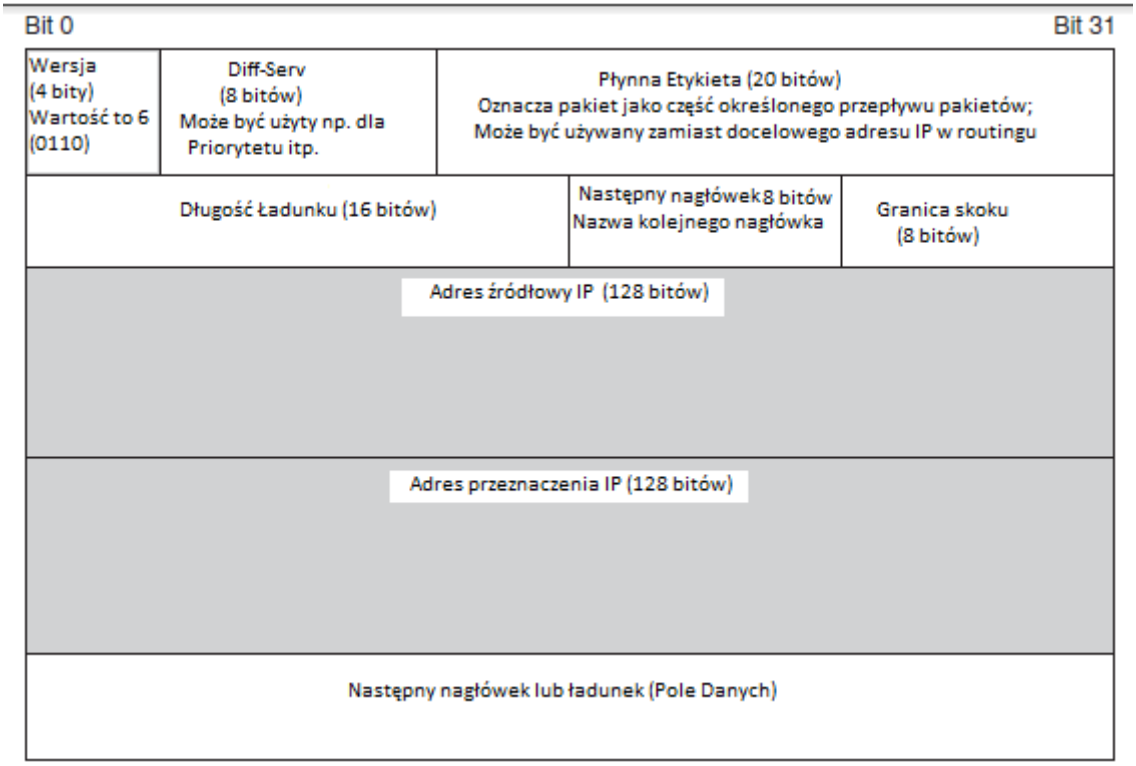
Trzeci rząd: Trzecia linia rozpoczyna się od złowieszczo brzmiącego czas życia (TTL), który ma wartość z zakresu od 0 do 255. Host wysyłający ustawia wartość początkową (64 lub 128 w większości systemów operacyjnych). Każdy router po drodze zmniejsza wartość o 1. Jeśli router zmniejszy wartość do 0, odrzuca pakiet. Ten proces został stworzony w celu zapobiegania nieopłaconym pakietom krążenia bez końca w Internecie. Aby zidentyfikować hosty, intruz użyje protokołu ICMP (Internet Control Message Protocol) do pingowania wielu adresów IP. Odpowiedź informuje atakującego, że host istnieje z tym adresem IP. Ponadto, odgadując początkową wartość TTL i patrząc na wartość TTL w nadchodzącym pakiecie, osoba atakująca może odgadnąć, ile haków routera oddziela host atakującego od hosta ofiary. Wysyłanie wielu pingów na różne adresy IP może pomóc atakującemu mapować routery w docelowej sieci. Często administratorzy wyłączają ruch ICMP poza wewnętrznymi sieciami, aby uniemożliwić mapowanie aktywnych hostów wewnętrznych osobom, które nie są autoryzowanymi użytkownikami. Pole danych pakietu IP może zawierać segment komunikatu TCP, wiadomość AUDPdatagram lub coś innego, na przykład komunikaty ICMP. Wartość 1 w tym polu wskazuje, że pole danych jest komunikatem ICMP. Z kolei 6 wskazuje segment TCP, a 17 wskazuje, że pole danych zawiera nagłówek UDP. Pole sumy kontrolnej nagłówka zawiera wartość umieszczoną tam przez nadawcę. Liczba ta jest określana na podstawie obliczeń na podstawie wartości innych pól. Odbierający proces internetowy zmienia obliczenia. Jeśli te dwie liczby są różne, musiała wystąpić usterka. Jeśli tak, router lub host docelowy odbierający pakiet po prostu odrzuci pakiet. Nie ma retransmisji, więc IP nie jest z natury wiarygodne; jednak jedną z funkcji TCP jest monitorowanie numerów sekwencji i inicjowanie retransmisji brakujących pakietów.

Źródłowy i docelowy adres IP: Kiedy wysyłasz list, koperta ma adres i adres zwrotny. Analogiczne adresy w nagłówkach IP są źródłowymi i docelowymi adresami IP. Zwróć uwagę, że adresy IP mają długość 32 bitów. W przypadku odczytu przez człowieka te 32 bity są podzielone na cztery 8-bitowe segmenty, a bity każdego segmentu są przekształcane na liczbę dziesiętną z przedziału od 0 do 255. Cztery numery segmentów są następnie rozdzielane kropkami. Przykładem jest 128.171.17.13. Zauważ, że ta kropkowana notacja dziesiętna jest pamięcią i zapisem dla gorszych bytów biologicznych (ludzi). Komputery i routery pracują bezpośrednio z 32-bitowymi adresami IP. Wiele form filtrowania firewall opiera się na adresach IP. Ponadto wielu napastników podszywa się pod źródłowy adres IP swojego pakietu (tj. Zamienia prawdziwy adres IP na fałszywy Adres IP).

WERSJA IP 6

Chociaż wersja IP 4 jest szeroko stosowana, jej 32-bitowy rozmiar adresu IP powoduje problemy: Może adresować tylko 4 294 967 296 ~ 10⁹) urządzeń. Ten względnie mały rozmiar ogranicza liczbę możliwych adresów IP. Ponadto, gdy adresy IP były dystrybuowane, większość adresów została przypisana do Stanów Zjednoczonych, ponieważ Internet został tam wynaleziony. W rzeczywistości niektóre amerykańskie uniwersytety otrzymały więcej adresów IP niż Chiny. Aby rozwiązać problemy związane z 32-bitowym rozmiarem adresu IP, została utworzona nowa wersja protokołu internetowego. To jest wersja IP 6 (IPv6). (Została zdefiniowana wersja 5, ale nigdy nie była używana.) Rysunek pokazuje organizację pakietów IPv6.Jednak ta zdolność nie jest szeroko stosowana. Istnieje pole limitu przeskoku, które obsługuje tę samą funkcję co pole czasu życia (TTL) w IPv4. Z kolei długość ładunku podaje długość pola danych w oktetach. Główną innowacją w IPv6 jest następne pole nagłówka. Po pierwszym nagłówku może być wiele nagłówków pokazanych. Na przykład zabezpieczenia IPsec są zaimplementowane z nagłówkiem bezpieczeństwa. Chociaż opcje są nietypowe w IPv4, protokół IPv6 w znacznym stopniu wykorzystuje dodatkowe nagłówki. Następne

pole nagłówka mówi, czym jest następny nagłówek. Każdy dodatkowy nagłówek ma następne pole nagłówka, które identyfikuje następny nagłówek lub mówi, że nie ma następnego nagłówka.



Jedną z oczywistych zmian jest to, że adresy IP są znacznie większe - 128 bitów. Każdy adres IP wymaga czterech linii 32-bitowych do zapisu i jest równy ~ 1038. Zapewni to adresy IP, dzięki którym niemal każde urządzenie będzie hostem w Internecie - w tym tosterami i kawiarkami. Aby dać nam poczucie skali tej ogromnej liczby, wystarczy zająć się każdą pojedynczą cząsteczką wody w sześcianie ponad 2 km po bokach. Innym popularnym opisem różnicy w wielkości przestrzeni adresowej IPv4 i IPv6 jest to, że jeśli przestrzeń adresowa IPv4 była reprezentowana jako kwadrat około 4 cm na boku, równoważny obszar dla przestrzeni adresowej IPv6 pokryłby układ słoneczny na zewnątrz Plutona orbita. Pole numeru wersji ma długość 4 bitów, a jego wartość to 6 (0110). Istnieje również pole dif-serv i pole etykiety przepływu o długości 20 bitów. Te pola pozwalają na przypisanie pakietu do kategorii pakietów o podobnych potrzebach. Wszystkie pakiety w tej kategorii będą miały przypisaną tę samą etykietę przepływu i będą traktowane w ten sam sposób przez routery. Jednak ta zdolność nie jest szeroko stosowana. Istnieje pole limitu przeskoku, które obsługuje tę samą funkcję co pole czasu życia (TTL) w IPv4. Z kolei długość ładunku podaje długość pola danych w oktetach. Główną innowacją w IPv6 jest następne pole nagłówka. Po pierwszym nagłówku może być wiele nagłówków pokazanych. Na przykład zabezpieczenia IPsec są zaimplementowane z nagłówkiem bezpieczeństwa. Chociaż opcje są nietypowe w IPv4, protokół IPv6 w znacznym stopniu wykorzystuje dodatkowe nagłówki. Następne pole nagłówka mówi, czym jest następny nagłówek. Każdy dodatkowy nagłówek ma następne pole nagłówka, które identyfikuje następny nagłówek lub mówi, że nie ma następnego nagłówka.

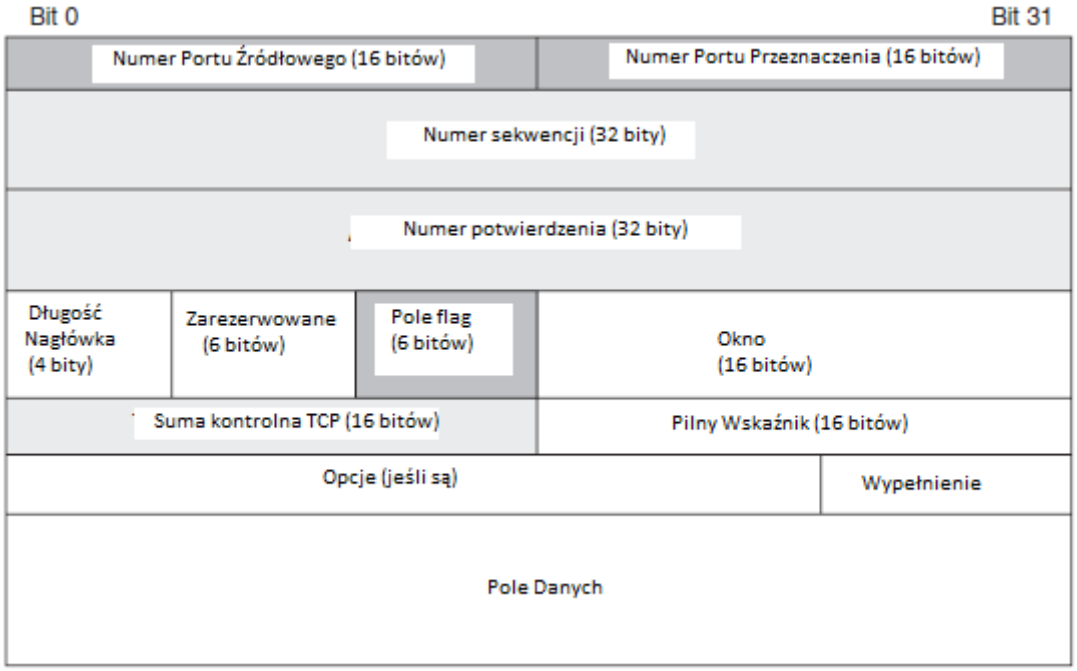
IPsec

IP, które zostało utworzone we wczesnych latach 80-tych, początkowo nie miało żadnego bezpieczeństwa. Wreszcie w latach 90. Internet Engineering Task Force opracował ogólny sposób zabezpieczenia transmisji IP. To było zabezpieczenie IP, które normalnie jest właśnie wywoływane IPsec. Funkcje IPsec chronią pakiet lub większość pakietów i wysyłają chroniony pakiet do innego pakietu. IPsec to ogólne rozwiązanie bezpieczeństwa, ponieważ wszystko w polu danych chronionego

pakietu jest bezpiecznie szyfrowane, w tym informacje o transporcie i warstwie aplikacji. Obejmuje to komunikat transportowy i komunikat aplikacji zawarty w komunikacie transportowym. Pierwotnie opracowany dla IPv6, został również rozszerzony na IPv4, stając się całkowicie ogólnym rozwiązaniem.

TRANSMISSION CONTROL PROTOCOL (TCP)

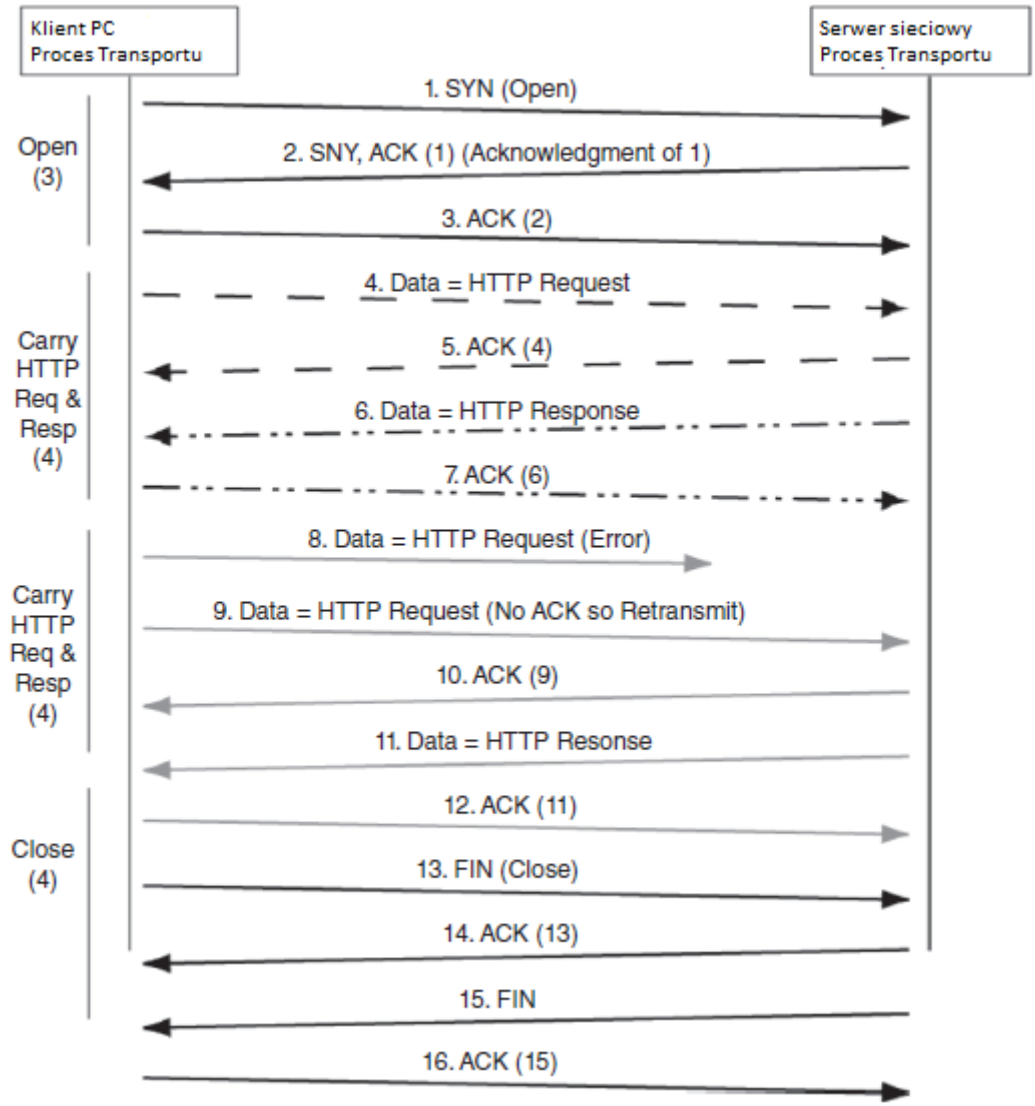
Jak wspomniano wcześniej, protokół TCP (Transmission Control Protocol) jest jednym z dwóch możliwych protokołów TCP / IP w warstwie transportowej. Rysunek pokazuje komunikat TCP, który nazywa się segmentem TCP



Protokół zorientowany na połączenie i niezawodność : Protokoły są albo bezpołączeniowe, albo zorientowane na połączenie.

* Protokoły zorientowane na połączenie są jak rozmowy telefoniczne. Kiedy dzwonisz do kogoś, na początku rozmowy jest co najmniej milcząca zgoda, że jesteś w stanie mówić. Wyraźne wskaźniki, takie jak "Zaczekaj, proszę." I "Czy mogę oddzwonić?" wskazują na niechęć do kontynuowania w tej chwili. Ponadto istnieje przynajmniej milcząca zgoda, że skończysz rozmowę na końcu rozmowy; po prostu zawieszenie uważa się za nieuprzejme. "Do widzenia" lub "Zadzwonię do ciebie później" są przykładami sygnałów końcowych.

* Protokoły bezpołączeniowe z kolei są jak e-maile. Gdy wysyłasz wiadomość, nie ma wcześniejszej zgody, a po wysłaniu wiadomości nie ma wbudowanego przepisu na odpowiedź (chyba że jesteś jedną z osób, które prosi o powiadomienie, gdy odbiornik odczytuje wiadomość). Na rysunku pokazano przykładowe połączenie TCP.



Trzy wiadomości są wysyłane, aby otworzyć połączenie. Autor wysyła segment TCP SYN, aby wskazać, że chce otworzyć sesję TCP. Drugi proces transportu odsyła segment TCP SYN / ACK, który potwierdza komunikat otwarcia połączenia i wskazuje, że chce otworzyć połączenie. Autor wysyła następnie segment ACK, aby wskazać odbiór segmentu SYN / ACK. Atakujący mogą korzystać z otworów połączeń TCP w celu wykonania ataków typu "odmowa usługi", które uniemożliwiają serwerowi zareagowanie na legalny ruch. Atakujący wysyła segment SYN, aby otworzyć połączenie z serwerem ofiary. Serwer ofiary odpowiada komunikatem SYN / ACK. Serwer ofiary rezerwuje również zasoby dla połączenia. Atakujący nigdy nie odpowiada ACK, więc nazywa się to atakiem SYN na wpół otwarty. Jeśli atakujący zaleje serwer segmentami SYN, serwer ofiary zarezerwuje tyle zasobów, że będzie przeciążony i nie będzie w stanie obsłużyć uzasadnionych prób otwarcia połączenia. Serwer może nawet ulec awarii. Kończąc rozmowę, zwykle przyjmuje cztery wiadomości. Jedna ze stron przesyła segment FIN, potwierdzony przez drugą stronę. Następnie druga strona wysyła FIN segment, który potwierdza druga strona. Po tym jak pierwsza strona wyśle oryginalny segment FIN, nie wyśle żadnych nowych informacji, ale wyśle potwierdzenia dla segmentów wysłanych przez drugą stronę. Istnieje inny sposób zakończenia sesji lub nawet odrzucenia pierwszej. W dowolnym momencie każda ze stron może wysłać wiadomość RST (reset). Komunikat RST kończy nagle rozmowę. Nie ma nawet potwierdzenia. To jest jak rozmowa w rozmowie telefonicznej. Atakujący często poprzedzają atak, próbując zidentyfikować adresy IP prowadzenie hostów - podobnie jak złodzieje mieszkający w sąsiedztwie. Jednym ze

sposobów jest wysłanie segmentów TCP SYN do hostów. Jeśli hosty odrzucają segment SYN, często odsyłają komunikat RST. Jak wspomniano wcześniej, segmenty TCP są przenoszone w polach danych pakietów IP. Źródłowy adres IP w pakiecie dostarczającym segment TCP RST będzie pochodził od hosta wewnętrznego. Za każdym razem, gdy atakujący otrzymuje segment RST, sprawdza on istnienie działającego hosta pod adresem IP tego pakietu. Zapory ogniowe często powstrzymują segmenty RST przed opuszczaniem witryny, aby uniemożliwić im dotarcie do atakującego.

Niezawodność : Oprócz tego, że są one bezpołączeniowe lub zorientowane na połączenie, protokoły są niezawodne lub nierzetelne. Nieprawidłowy protokół nie wykrywa i nie koryguje błędów. Niektóre niewiarygodne protokoły nawet nie sprawdzają błędów. Inne sprawdzają dla błędów, ale po prostu odrzucają wiadomość, jeśli stwierdzi, że zawiera błąd. TCP jest niezawodnym protokołem. Naprawia błędy. Pole sumy kontrolnej TCP jest obliczane na podstawie wartości z innych pól. Nadawca umieszcza wynik swoich obliczeń w polu sumy kontrolnej. Odbiornik zmienia obliczenia i porównuje je z przesyłaną wartością. Jeśli proces otrzymywania warstwy transportowej stwierdzi, że komunikat jest poprawny (wartości są takie same), wysyła komunikat potwierdzenia. Jeśli jednak odbiornik wykryje błąd w odbieranym segmencie TCP (wartości są różne), odrzuca segment i nie robi nic innego. W jaki sposób odbiornik wie, że w komunikacie jest błąd? Nadawca oblicza wartość na podstawie innych bitów w segmencie TCP (nie tylko w nagłówku). Odbiornik zmienia obliczenia. Jeśli te dwie wartości są zgodne, odbiornik wysyła potwierdzenie. Jeśli nie pasują, odbiornik po prostu upuszcza segment i nie wysyła potwierdzenia. Jeśli segment dotrze poprawnie, oryginalny nadawca otrzyma potwierdzenie. Jeśli jednak segment nigdy nie dotrze lub zostanie odrzucony z powodu uszkodzenia, nie ma odpowiedzi ,że wysłano. Jeśli oryginalny nadawca nie otrzyma potwierdzenia w określonym czasie, wyśle ponownie oryginalny segment. Będzie nawet używał oryginalnego numeru kolejnego.

Pola flag :Pole flagi to ogólna nazwa dla 1-bitowego pola, które jest logiczne (prawda lub fałsz). Aby powiedzieć, że pole flagi jest ustawione, oznacza to, że jego wartość wynosi 1. Aby powiedzieć, że pole flagi nie jest ustawione, oznacza to, że jego wartość wynosi 0. Nagłówek TCP zawiera pewną liczbę pól flagi. Jednym z nich jest SYN. Aby zażądać otwarcia połączenia, nadawca ustawia bit SYN. Drugi wysyła segment SYN / ACK, w którym ustawiane są oba bity SYN i ACK. Inne powszechnie używane flagi to FIN, RST, URG i PSH. Flaga URG wskazuje na obecność pilnych danych, które należy obsłużyć przed wcześniejszymi oktetami danych. Pilne pole wskaźnika wskazuje lokalizację pilnych danych. Jeśli wiadomość aplikacji jest duża, protokół TCP dzieli komunikat aplikacji na wiele segmentów TCP i wysyłać segmenty pojedynczo. Aby pomóc procesowi odbierania TCP, proces transportu wysyłającego może ustawić bit PSH (push) w ostatnim segmencie wiadomości aplikacji. Dzięki temu proces transportu odbierającego natychmiast przenosi dane do aplikacji bez buforowania i opóźnień.

Oktety i kolejny numer : Wartość pola numeru sekwencyjnego pozwala odbiorcy na umieszczanie przychodzących segmentów TCP w kolejności, nawet jeśli pakiety niosące je przychodzą nieuporządkowane (w tym, gdy segment jest ponownie transmitowany). Numery sekwencji są również używane w potwierdzeniach, choć pośrednio. W transmisji TCP liczy się każdy wysłany oktet od pierwszego. Liczenie oktetów służy do wybierania numeru kolejnego każdego segmentu.

*W pierwszym segmencie losowy numer początkowej sekwencji (ISN) umieszczany jest w polu numeru kolejnego.

* Jeśli segment zawiera dane, numer pierwszego oktetu zawarty w danych jest używany jako numer kolejny segmentu.

* W przypadku czysto nadzorczego komunikatu, który nie zawiera żadnych danych, takich jak segment ACK, SYN, SYN / ACK, FIN lub RST, numer sekwencji jest zwiększany o 1 w stosunku do poprzedniego komunikatu.

Jednym z niebezpiecznych ataków jest przechwytywanie sesji TCP, w której atakujący przejmuje rolę jednej strony. Dzięki temu porywacz może czytać wiadomości i wysyłać fałszywe wiadomości na drugą stronę. Aby przeprowadzić przechwycenie sesji, atakujący musi być w stanie przewidzieć numery sekwencji, ponieważ jeśli segment przybędzie z niewłaściwym numerem sekwencji, odbiorca go odrzuci. Przejęcie sesji TCP może zakończyć się powodzeniem tylko wtedy, gdy początkowy numer sekwencji jest przewidywalny. Niewiele systemów operacyjnych wybiera dziś początkowe numery sekwencji w przewidywalnym terminie, ale przewidywalne numery sekwencji były powszechne we wcześniejszych systemach operacyjnych, z których niektóre są nadal w użyciu.

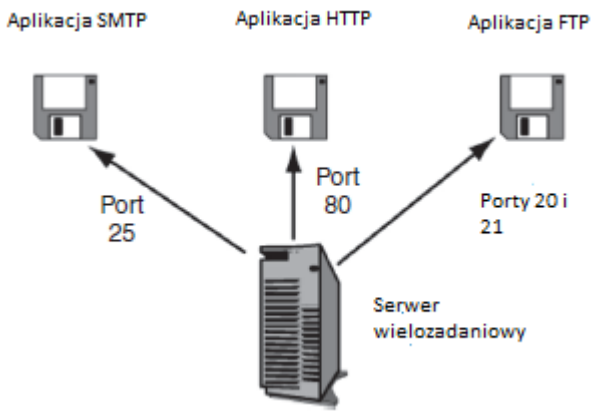
Numery potwierdzeń : Kiedy odbiornik wysyła potwierdzenie, ustawia bit ACK. Wprowadza również wartość w polu potwierdzenia numeru, aby wskazać, który segment jest potwierdzany. Ten proces jest potrzebny, ponieważ nadawca wysyła wiele segmentów i dlatego, że potwierdzenia mogą być opóźnione. Możesz pomyśleć, że numerem potwierdzenia jest numer sekwencji potwierdzanego segmentu. W tym przypadku jest to numer ostatniego oktetu w polu danych plus 1. Innymi słowy, numer potwierdzenia podaje numer oktetu pierwszego oktetu w następnym segmencie do wysłania. Wydaje się to nieco dziwne, ale czyni pewne obliczenia łatwiejszym dla odbiorcy.

Pole okna : Kontrola przepływu ogranicza szybkość, z jaką strona wysyła segmenty TCP. Pole okna TCP pozwala ograniczyć liczbę oktetów, które druga strona może wysłać przed otrzymaniem kolejnego potwierdzenia. W potwierdzeniach ustawiony jest bit ACK, a pola potwierdzenia i wielkości okna są wypełniane.

Opcje : Podobnie jak nagłówek IPv4, nagłówek TCP może mieć opcje. Jednak, mimo że opcje IP są rzadkie i powodują podejrzenia, protokół TCP w dużym stopniu wykorzystuje opcje. Jedną z powszechnych opcji, często przesyłanych z początkowym segmentem SYN lub SYN / ACK, jest opcja maksymalnego rozmiaru segmentu (MSS). Daje to drugiej stronie ograniczenie maksymalnej wielkości pól danych segmentu TCP (nie dotyczy rozmiarów segmentów jako całości). Obecność opcji TCP nie jest więc sama w sobie podejrzana.

Numery portów : Przeglądaliśmy teraz większość pól w nagłówku TCP. Dwa pierwsze pola zasługują na szczególną uwagę.

Numery portów na serwerach : Pola numeru portu oznaczają różne rzeczy dla klientów i serwerów. Dla serwera reprezentuje konkretną aplikację uruchomioną na tym serwerze, jak pokazuje rysunek

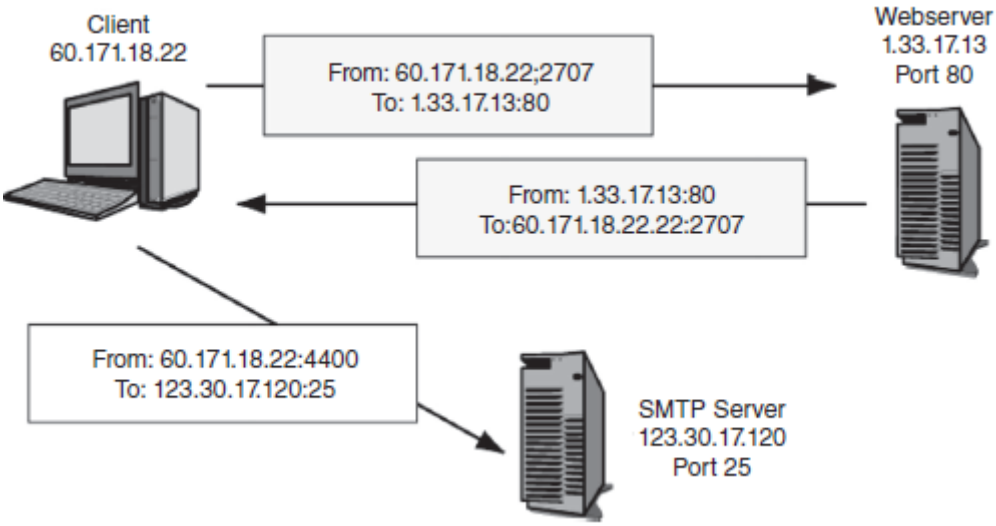


Serwery są wielozadaniowymi komputerami, co oznacza, że mogą uruchamiać wiele aplikacji jednocześnie. Każda aplikacja jest określona przez inny numer portu. Na przykład na serwerze aplikacja sieci Web może działać na porcie TCP 80. Przychodzące segmenty TCP, które mają 80 jako docelowy numer portu, są przekazywane do aplikacji serwera WWW. W rzeczywistości port TCP 80 jest dobrze

znanym portem dla programów serwera WWW, co oznacza, że jest to zwykły numer portu dla aplikacji. Mimo że serwerom sieci Web można nadać inne numery portów TCP, uniemożliwia to użytkownikom nawiązywanie połączeń, chyba że znają lub mogą odgadnąć niestandardowy numer portu TCP. Zakres portów TCP od 0 do 1023 jest zarezerwowany dla dobrze znanych numerów portów głównych aplikacji, takich jak HTTP i poczta e-mail. Na przykład, programy serwera pocztowego Simple Mail Transfer Protocol (SMTP) zwykle są uruchamiane na porcie TCP 25, a protokół FTP wymaga dwóch dobrze znanych numerów portów - port TCP 21 dla kontroli nadzorczej i portu TCP 20 dla rzeczywistego transferu plików.

Numery portów na klientach : Hosty klientów używają inaczej numerów portów TCP. Za każdym razem, gdy klient łączy się z aplikacją na serwerze, generuje losowy, efemeryczny numer portu, którego używa tylko dla tego połączenia. Na komputerach z systemem Windows efemeryczne numery portów TCP mieszczą się w zakresie od 1024 do 4999. Zakres numerów portu Microsoft dla efemerycznych numerów portów może różnić się od oficjalnego zakresu IETF o wartości 5000-65534. Używanie niestandardowych, efemerycznych numerów portów przez system Windows i niektóre inne systemy operacyjne powoduje problemy z filtrowaniem firewall.

Gniazda : Rysunek pokazuje, że celem pracy w sieci jest dostarczanie komunikatów aplikacji z jednej aplikacji na jednym komputerze do innej aplikacji na innej maszynie.



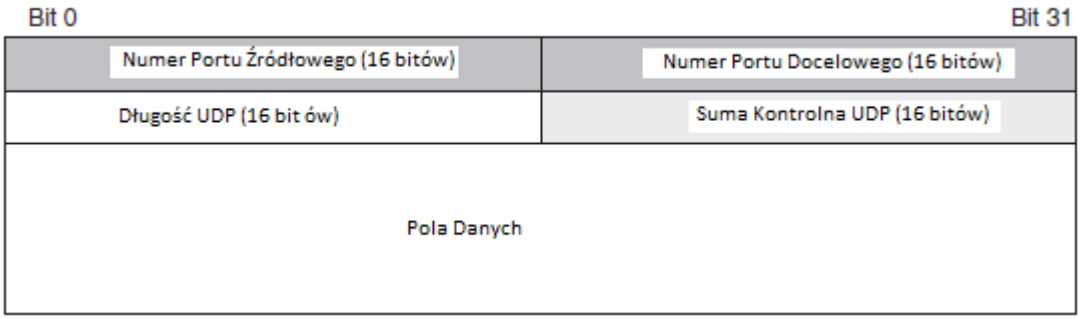
Na każdym komputerze znajduje się numer portu TCP, który określa aplikację (lub połączenie) i adres IP w celu określenia komputera. Gniazdo to połączenie adresu IP i numeru portu TCP. Jest zapisany jako adres IP, dwukropek i numer portu TCP. Typowe gniazdo to coś takiego jak 128.171.17.13:80. Atakujący często robią podszywanie pod gniazdo - zarówno podszywanie się pod adres IP, jak i podszywanie się pod port. W przypadku przejęcia sesji TCP, jeśli atakujący chce przejąć tożsamość klienta, musi znać zarówno adres IP klienta, jak i tymczasowy numer portu. Oczywiście te pola są przesyłane w przejrzysty sposób (bez szyfrowania) w protokole TCP, więc osoba atakująca z snifferem przechwytującym i odczytującym ruch przepływający między klientem a serwerem może łatwo uzyskać te informacje.

Zabezpieczenia TCP : Podobnie jak IP, protokół TCP został utworzony bez zabezpieczeń. Mimo że protokół IPsec zapewnił bezpieczeństwo IP, IETF nie stworzył w porównywalny sposób bezpiecznego protokołu TCP. Jednym z powodów tego jest zdolność IPsec do transparentnego zabezpieczenia całego ruchu warstwy transportowej, bez modyfikacji protokołów warstwy transportowej. IETF uczynił z IPsec centralny element zabezpieczeń i jedną metodę obsługi zabezpieczeń na wyższych poziomach.

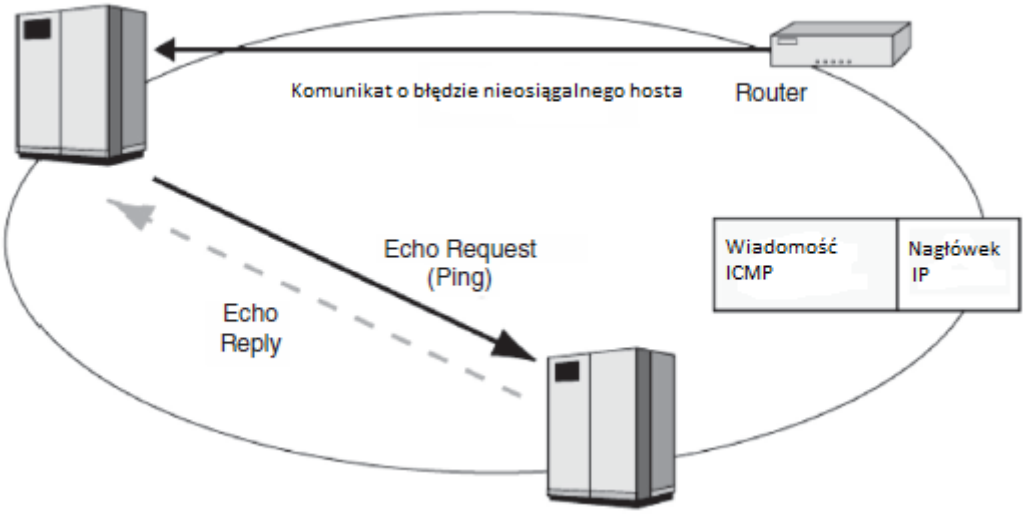
Komunikacja partnerów, którzy chcą zabezpieczeń TCP, powinna implementować IPsec. Jednak niewiele sesji TCP jest chronionych przez IPsec. W związku z tym niektóre pary użytkowników stosują opcję w protokole TCP, która dodaje podpis elektroniczny do każdej sesji TCP. Ta sygnatura potwierdza tożsamość nadawcy. Ta opcja, opisana w dokumencie RFC 2385, wymaga od obu stron podania tajnej wartości. Ta opcja jest niezręczna, ponieważ nie zapewnia automatycznego udostępniania kluczy i nie zapewnia szyfrowania ani innych zabezpieczeń. Ta opcja jest używana przede wszystkim w protokole Border Gateway Protocol (BGP). BGP służy do wymiany informacji o routingu między systemami administracyjnymi - powiedzmy system korporacyjny i dostawca usług internetowych. BGP zawsze korzysta z połączeń jeden-do-jednego, strony komunikacyjne zazwyczaj dobrze się znają, a obie strony mają długoterminowe relacje, co sprawia, że wymiana kluczy jest mniej uciążliwa i ryzykowna. Jednak poza BGP opcja podpisu elektronicznego RFC 2385 wydaje się nie być wykorzystywana znacząco. Nawet w BGP jest powszechnie uważany za bardzo słabe zabezpieczenie.

USER DATAGRAM PROTOCOL

Jak wspomniano wcześniej, TCP jest protokołem, który nadrabia ograniczenia IP. TCP dodaje korektę błędów, sekwencjonowanie pakietów IP, kontrolę przepływu i inne funkcje, których nie omawialiśmy. Nie wszystkie aplikacje wymagają niezawodnej usługi oferowanej przez TCP. Na przykład, w Voice over IP (VOIP), nie ma czasu na czekanie na retransmisję utraconych lub uszkodzonych pakietów niosących głos. Z kolei protokół Simple Network Management Protocol (SNMP), który jest używany do komunikacji zarządzania siecią, wysyła tak wiele komunikatów tam i z powrotem, że dodatkowy ruch pakietów otwierania połączenia, potwierdzeń i innych segmentów nadzorczych TCP może spowodować przeciążenie sieci. , VoIP, SNMP i wiele innych aplikacji nie używa TCP w warstwie transportowej. Zamiast tego korzystają z User DatagramProtocol (UDP). Ten protokół jest bezpołączeniowy i niewiarygodny. Każda wiadomość UDP (nazywana datagramem UDP) jest wysyłana samodzielnie. Nie ma żadnych otworów, zamknięć ani potwierdzeń. W związku z prostotą działania UDP, organizacja datagramów UDP jest również bardzo prosty, jak pokazuje rysunek

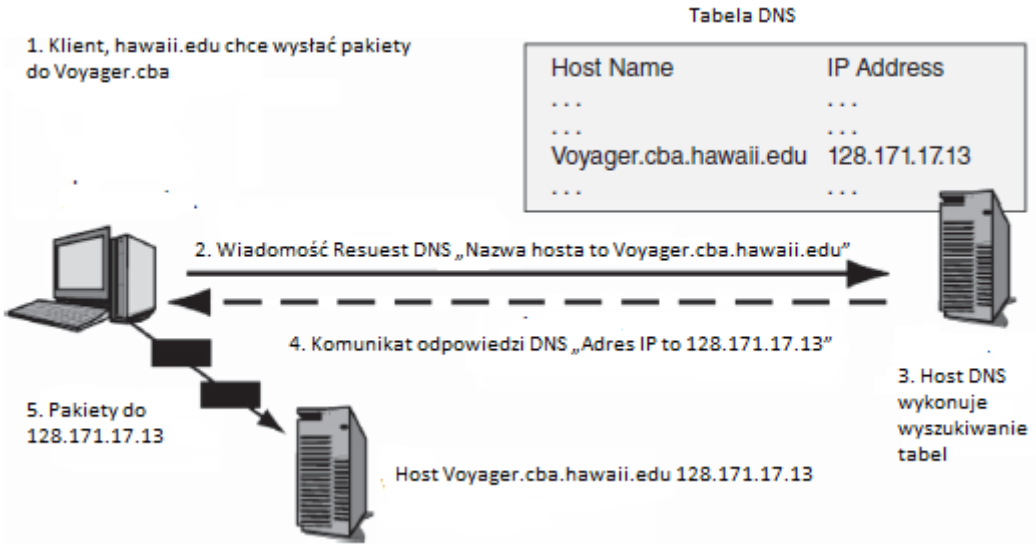


Nie ma numerów sekwencji, numerów potwierdzeń, pól flag ani większości innych pól znalezionych w TCP. Istnieją numery portów źródłowych i docelowych, długość nagłówka UDP, aby umożliwić datagramy UDP o zmiennej długości oraz sumę kontrolną UDP. Jeśli odbiornik wykryje błąd za pomocą sumy kontrolnej, po prostu odrzuca wiadomość. Nie ma retransmisji. Fakt, że zarówno TCP, jak i UDP używają numerów portów, oznacza, że ilekroć powinieneś odnosić się do numerów portów dla dobrze znanych aplikacji, musisz również sprawdzić, czy numery portów są numerami portów TCP lub UDP. Z tego powodu dobrze znanym numerem portu dla serwerów sieciowych jest port TCP 80. Numery sekwencji TCP bardzo utrudniają przechwytywanie sesji TCP. Odbiornik odrzuci komunikaty o błędnych numerach sekwencji, nawet jeśli gniazda źródłowe i docelowe są poprawne. UDP nie ma tej ochrony, co czyni UDP nieco bardziej niebezpiecznym protokołem niż TCP. Podobnie jak TCP, UDP nie ma wrodzonych zabezpieczeń. Firmy, które chcą zabezpieczyć swoją komunikację UDP, muszą używać IPsec.



Komunikaty ICMP są dostarczane w polach danych pakietów IP. Najbardziej znaną parą typów komunikatów ICMP jest komunikat echa ICMP i komunikat odpowiedzi echa. Załóżmy, że host wysyła komunikat echa ICMP na adres IP. Jeśli host jest aktywny pod tym adresem, może odesłać komunikat odpowiedzi echa ICMP. Ten proces jest często nazywany pingowaniem, ponieważ najpopularniejszy program do wysyłania komunikatu echa ICMP nazywa się Ping. Komunikat echa jest bardzo ważnym narzędziem do zarządzania siecią. Jeśli menedżer sieci podejrzewa, że wystąpił problem, wyszuka szeroki zakres adresów hostów, aby sprawdzić, które z nich są osiągalne. Wzór odpowiedzi może ujawnić, gdzie występują problemy w sieci. Atakujący uwielbiają również pingować szeroki zakres adresów IP hosta. Może to dać im listę hostów dostępnych do ataków. Innym popularnym narzędziem do zarządzania i ataku sieci jest traceroute (lub tracert na komputerach z systemem Windows). Traceroute jest podobny do ping, ale traceroute wymienia również routery leżące między hostem wysyłającym a hostem, który jest celem polecenia traceroute. Umożliwia to intruzowi mapowanie sieci. Graniczne zapory ogniowe często zrzucają wiadomości z odpowiedziami echa, pozostawiając firmę na zewnątrz. Wiele komunikatów ICMP to komunikaty o błędach. Na przykład, jeśli router nie może dostarczyć pakietu, może wysłać komunikat o błędzie ICMP do hosta źródłowego. Ten komunikat o błędzie zawiera możliwie najwięcej informacji o typie błędu, który wystąpił. Jeśli atakujący nie może pingować docelowych hostów, ponieważ zapora ich zatrzymuje, atakujący często wysyłają pakiety IP, które są zniekształcone, a więc zostaną odrzucone. Błąd wiadomości ICMP jest dostarczany w pakiecie IP, a źródłowy adres IP w tym pakiecie ujawni adres IP routera wysyłającego. Analizując komunikaty o błędach, osoba atakująca może dowiedzieć się, w jaki sposób routery są zorganizowane w sieci. Ta informacja może być bardzo przydatna dla atakujących.

System nazw domen (DNS) : Aby wysłać pakiet do innego hosta, host źródłowy musi umieścić adres IP hosta docelowego w polu adresu docelowego pakietów. Często jednak użytkownik po prostu wpisuje nazwę hosta docelowego, na przykład cnn.com. Niestety, nazwy hostów to tylko pseudonimy. Jeśli użytkownik wpisze nazwę hosta, to komputer musi nauczyć się odpowiedniego adresu IP. Jak pokazuje rysunek, host, który chce wysłać pakiet do hosta docelowego, wysyła wiadomość z żądaniem systemu DNS (DNS) do serwera DNS.



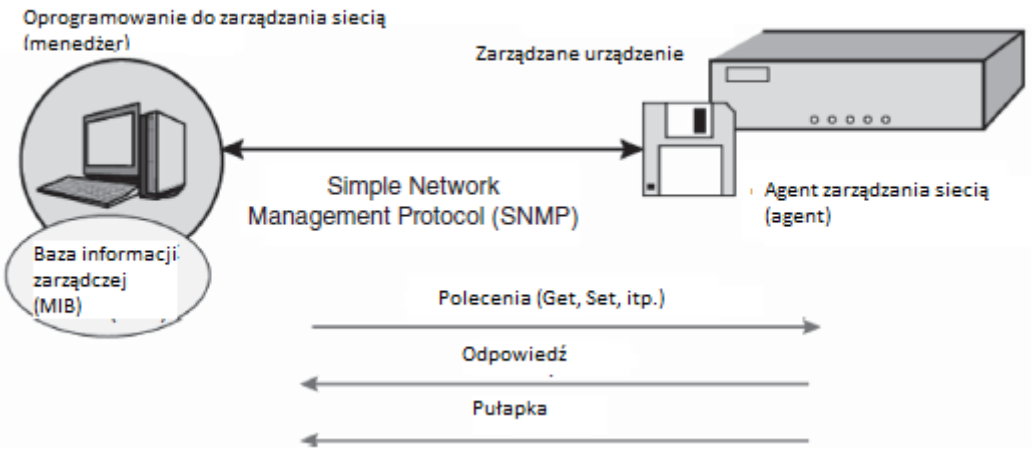
Ta wiadomość zawiera nazwę hosta docelowego. Komunikat odpowiedzi DNS odsyła adres IP hosta docelowego. Aby dać analogię, jeśli znasz czyjeś imię, musisz sprawdzić swój numer telefonu w książce telefonicznej, jeśli chcesz do niego zadzwonić. W DNS, ludzka nazwa odpowiada nazwie hosta, numer telefonu odpowiada adresowi IP, a serwer DNS odpowiada katalogowi telefonicznemu. System DNS ma kluczowe znaczenie dla działania Internetu. Niestety, DNS jest podatny na kilka ataków. Na przykład w zatruwaniu pamięci podręcznej DNS atakujący zamienia adres IP nazwy hosta na inny adres IP. Po zatruciu pamięci podręcznej prawowity użytkownik, który kontaktuje się z serwerem DNS w celu wyszukania nazwy hosta, otrzyma fałszywy adres IP, wysyłając użytkownika na wybraną przez atakującego witrynę. Ataki typu "service-service" również są zbyt łatwe do wykonania. RFC 3833 zawiera listę problemów związanych z bezpieczeństwem DNS. Kilka prób wzmocnienia bezpieczeństwa DNS zostało opracowanych pod ogólną nazwą DNSSEC (Domain Name System Security Extensions), w szczególności RFC 2535.3. Jednak okazało się, że zarówno oryginalne specyfikacje DNSSEC, jak i nowsze specyfikacje DNSSEC bis (RFC 4033-40354) okazały się być niewystarczający. Opracowanie standardu bezpieczeństwa, który jest wystarczająco kompatybilny wstecz w celu wdrożenia na skalę internetową, okazało się niezwykle trudne. Jeśli serwer DNS nie zna nazwy hosta, kontaktuje się z innym serwerem DNS. System DNS zawiera wiele serwerów DNS zorganizowanych w hierarchii. Na szczycie hierarchii znajduje się 13 serwerów głównych DNS. Poniżej są to serwery DNS dla najwyższego poziomu domeny, takie jak .com, .edu, .ie, .uk, .nl i .ca Każda z domen najwyższego poziomu ma dwa lub więcej serwerów DNS najwyższego poziomu dla swojej domeny. Nazwy domen drugiego poziomu są nadawane organizacjom (np. Hawaii.edu i Microsoft.com) .Organizacje są wymagane, aby utrzymywać serwery DNS dla komputerów w swojej domenie. Gdyby napastnicy mogli zniszczyć 13 serwerów głównych, mogliby sparaliżować Internet. Powszechny paraliż nie nastąpiłby natychmiast, ale za kilka dni Internet zacząłby poważnie przestać działać.

Protokół dynamicznej konfiguracji hosta (DHCP) : Hosty serwerów otrzymują statyczne (stałe) adresy IP. Komputery klienckie otrzymują dynamiczne (tymczasowe) adresy IP za każdym razem, gdy korzystają z Internetu. Standard protokołu DHCP (Dynamic Host Configuration Protocol), który widzieliśmy umożliwia to. Serwer DHCP ma bazę danych dostępnych adresów IP. Gdy klient żąda adresu IP, serwer DHCP wybiera jeden z bazy danych i wysyła go do klienta. Następnym razem, gdy klient korzysta z Internetu, serwer DHCP może nadać mu inny adres IP. Fakt, że klienci mogą otrzymywać różne adresy IP za każdym razem, gdy dostają się do Internetu, powoduje problemy w aplikacjach peer-to-peer (P2P). Aby znaleźć adres IP drugiej strony, należy użyć serwera obecności lub innego mechanizmu. Brak akceptowanych standardów obecności (w tym bezpieczeństwo obecności)

jest poważnym problemem, ponieważ aplikacje P2P są szeroko rozpowszechnione. W rzeczywistości większość kwestii związanych z zabezpieczeniami na serwerach obecności P2P jest wykorzystywana w aplikacjach pirackich P2P, mając na względzie unikanie odkryć przez uprawnione organy

Dynamiczne protokoły routingu : W jaki sposób routery w Internecie dowiadują się, co zrobić z pakietami adresowanymi do różnych adresów IP? Często rozmawiają ze sobą, wymieniając informacje o organizacji Internetu. Te wymiany muszą często występować, ponieważ struktura Internetu zmienia się często wraz z dodawaniem lub upuszczaniem routerów. Protokoły wymiany informacji organizacji są nazywane dynamicznymi protokołami routingu. Istnieje wiele dynamicznych protokołów routingu, w tym protokół RIP (Routing Information Protocol), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP) i zastrzeżony protokół Cisco Systems Enhanced Interior Gateway Routing Protocol (EIGRP). Każdy jest używany w różnych okolicznościach. Te protokoły mają bardzo różne funkcje zabezpieczeń, a różne wersje każdego protokołu mają różne poziomy funkcjonalności. Osoba atakująca, która potrafi podszyć się pod router, może wysyłać fałszywe komunikaty protokołu dynamicznego routingu do innych routerów. Te fałszywe wiadomości mogą spowodować, że routery nie dostarczą swoich pakietów. Atakujący może nawet spowodować, że pakiety przejdą przez komputer atakującego (nazywany atakiem człowiek-w-środku lub MIMA) w celu odczytania ich zawartości. Protokoły wymienione na liście mają bardzo różne funkcje bezpieczeństwa i różne wersje każdego protokołu mają różne poziomy bezpieczeństwa

Prosty protokół zarządzania siecią (SNMP) : Sieci często mają wiele elementów - routery, przełączniki i komputery hosta. Zarządzanie dziesiątkami, setkami lub tysiącami urządzeń może być prawie niemożliwe. Aby ułatwić zarządzanie, IETF opracował prosty protokół zarządzania siecią (SNMP). Jak pokazuje Ilustracja 5.21, program zarządzający może wysyłać komunikaty SNMP do zarządzanych urządzeń w celu ustalenia ich warunki.



Program zarządzający może nawet wysyłać wiadomości konfiguracyjne, które mogą zmienić sposób działania urządzeń zdalnych. Dzięki temu menedżer może zdalnie rozwiązywać wiele problemów.

STANDARDY APLIKACJI

Większość aplikacji ma własne standardy warstwy aplikacji. W rzeczywistości, biorąc pod uwagę dużą liczbę aplikacji na świecie, istnieją dosłownie setki standardów warstwy aplikacji. W miarę, jak korporacje radzą sobie lepiej w walce z atakami na niższych warstwach, napastnicy zaczęli skupiać swoją uwagę na słabych punktach aplikacji. Jeśli atakujący może przejąć aplikację działającą z wysokimi

uprawnieniami, uzyskuje te uprawnienia. Wiele aplikacji działa z najwyższymi uprawnieniami, a napastnicy, którzy je naruszają, są właścicielami skrzynki.

HTTP i HTML : Wiele aplikacji ma dwa rodzaje standardów. Standard transportu przenosi komunikaty warstwy aplikacji pomiędzy aplikacjami na różnych komputerach; w przypadku sieci WWW jest to protokół HTTP (Hypertext Transfer Protocol). Drugi to standard dla struktury dokumentu. Podstawowym standardem struktury dokumentu dla WWW jest Hypertext Markup Language (HTML). Netscape, który stworzył pierwszą szeroko używaną przeglądarkę, również stworzył standard bezpieczeństwa do ochrony komunikacji HTTP. To była Secure Sockets Layer (SSL). Później grupa inżynierów internetowych przejęła protokół SSL i zmieniła nazwę standardu na Transport Layer Security (TLS).

E-mail : Popularnymi standardami przesyłania wiadomości e-mail są: prosty protokół przesyłania poczty (SMTP), protokół POP (Post Office Protocol) i protokół IMAP (Internet Message Access Protocol) do pobierania wiadomości e-mail do klienta ze skrzynki pocztowej na serwerze. Popularne standardy dokumentów i dokumentów obejmują RFC 2822 (dla wiadomości pełnotekstowych), HTML i Multipurpose Internet Mail Extensions (MIME). S / MIME (Secure MIME) dodaje klucz publiczny szyfrowanie do MIME i jest zdefiniowane w dokumentach RFC 2634, 3850 i 3851. Oczywistym problemem z zabezpieczeniami w wiadomościach e-mail jest filtrowanie zawartości. Wirusy, spam, wiadomości phishingowe i inne niepożądane treści powinny zostać odfiltrowane, zanim dotrą do użytkowników i mogą wyrządzić szkodę. (Aby uzyskać więcej informacji na temat spamu i innych ataków typu low-technology, kolejnym problemem bezpieczeństwa w wiadomościach e-mail jest zabezpieczenie wiadomości przesyłanych od klienta wysyłającego na serwer pocztowy nadawcy, na serwer pocztowy odbiorcy oraz na klienta odbierającego. dla części lub wszystkich przepływów komunikatów, w tym między innymi SSL / TLS i S / MIME Niestety, IETF nie był w stanie uzgodnić standardu bezpieczeństwa, gdy używana jest poczta internetowa, która używa HTTP i HTML do komunikacji e-mailowej, następnie protokół SSL / TLS może działać między nadawcą a serwerem pocztowym nadawcy oraz między serwerem poczty odbiorcy a odbiorcą. Przesyłanie między serwerami poczty e-mail to kolejna kwestia. Oczywiście nadawcy mogą wysyłać zaszyfrowane wiadomości bezpośrednio do odbiorców. Zapobiega to jednak filtrowaniu w zaporach. Użytkownicy powinni szczególnie uważać na używanie poczty internetowej za pośrednictwem połączeń bezprzewodowych.

Telnet, FTP i SSH : Dwie najwcześniejsze aplikacje w Internecie to File Transfer Protocol (FTP) i Telnet. FTP zapewnia masowe przesyłanie plików między hostami. Telnet pozwala użytkownikowi uruchomić powłokę poleceń (interfejs użytkownika) na innym komputerze. Żaden z tych standardów nie ma żadnego bezpieczeństwa. Szczególną troską jest to, aby podczas logowania wysyłać hasła w sposób przejrzysty (bez szyfrowania). Nowszy standard Secure SHell (SSH) może być używany zamiast FTP i Telnetu, zapewniając jednocześnie wysokie bezpieczeństwo poprzez szyfrowanie całego przesyłanego ruchu między hostami.

Inne standardy aplikacji : Istnieje wiele innych aplikacji, a tym samym standardów aplikacji. Należą do nich między innymi Voice over IP, aplikacje peer-to-peer, usługi zorientowane na usługi (SOA) i aplikacje serwisowe Web. Większość aplikacji ma poważne problemy z bezpieczeństwem. Bezpieczeństwo aplikacji stało się być może najbardziej złożonym aspektem bezpieczeństwa sieci