Piotr KIJEWSKI, Krzysztof SZCZYPIORSKI**

Bezpieczeństwo w sieciach TCP/IP[1)]

Klasyczne protokoły rodziny **TCP/IP** nie zapewniają podstawowych usług ochrony informacji, takich jak kontrola dostępu, poufność, integralność czy uwierzytelnienie. Podczas prac nad ich udoskonalaniem powstały dwie grupy zabezpieczeń:

- **systemy ochrony informacji –** specjalistyczne mechanizmy analizujące działanie protokołów wymiany danych (np. systemy wykrywania włamań),
- nowe **protokoły zabezpieczeń i rozszerzenia aplikacji** (np. *Transport Layer Security* – **TLS**).

Celem artykułu jest przedstawienie metodyki ataków na sieci TCP/IP, w tym na sieć **Internet** oraz usystematyzowanego przeglądu stosowanych w tych sieciach zabezpieczeń przez prezentację logicznej ewolucji poszczególnych klas metod zabezpieczeń, ze szczególnym zaznaczeniem kierunków ich rozwoju.

W kolejnych trzech częściach artykułu przedstawiono uogólnione spojrzenie na te ataki oraz wspomniane wyżej dwie grupy metod zabezpieczeń. Następnie przedstawiono inne istotne, zdaniem autorów, zagadnienia związane z kształtowaniem się metod ochrony informacji w sieciach TCP/IP. W podsumowaniu przedstawiono najważniejsze wnioski wynikające z opracowania.

W niniejszym artykule przez **model sieci** będzie rozumiany **czterowarstwowy model sieci TCP/IP**. Niestety, znane z literatury angielskiej odpowiedniki niektórych mechanizmów zabezpieczeń (np. *circuit level gateway*) nie mają czytelnych i jednoznacznych polskich określeń. Używając pojęcia **sieci TCP/IP,** mamy na myśli wszystkie sieci wykorzystujące stos protokołów TCP/IP, a więc oprócz Internetu, jego mniej lub bardziej lokalne odmiany, takie jak np. intranet i ekstranet.

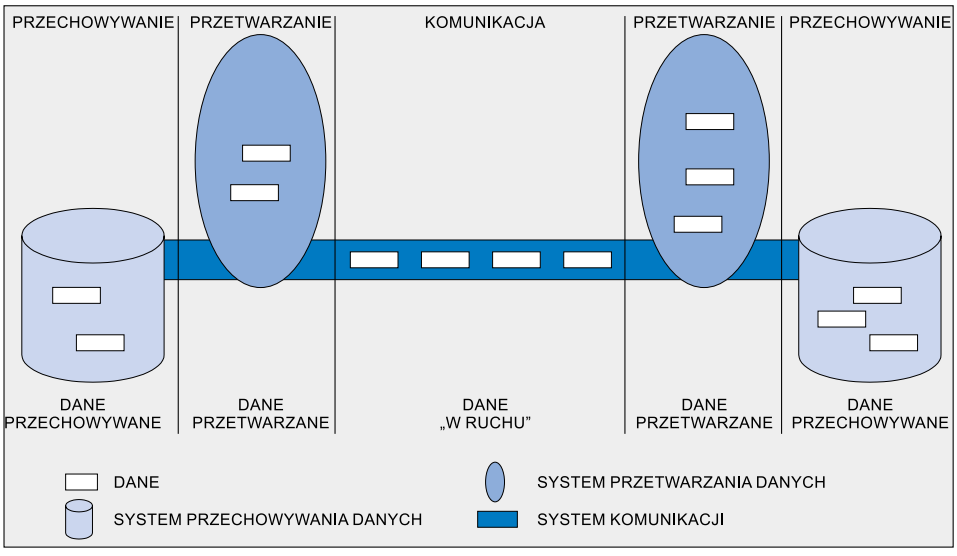
ATAKI NA SIECI TCP/IP

Architekturę sieci TCP/IP można opisać za pomocą relacji pomiędzy trzema podstawowymi elementami funkcjonalnymi (rys. 1):

- **systemem komunikacji** wykorzystującym protokoły komunikacyjne w celu przekazywania danych (tzw. danych w „ruchu") pomiędzy urządzeniami sieciowymi lub maszynami,
- **systemem przetwarzania danych** przeprowadzającym operacje na danych (tzw. danych przetwarzanych),
- **systemem przechowywania danych** składującym te dane (tzw. przechowywane dane).

Te elementy funkcjonalne są składowymi komputerów sieciowych (np. serwerów internetowych), ruterów i innych urządzeń.

Historycznie najwcześniej zainteresowano się ochroną informacji w samodzielnie działających komputerach, a dokładnie w systemach przechowywania danych, takich jak bazy danych czy systemy plików. W momencie szerszego zainteresowania sieciami telekomunikacyjnymi spostrzeżono, że istotna jest ochrona danych przekazywanych pomiędzy maszynami. W końcu dostrzeżono rolę właściwego, od strony bezpieczeństwa, przetwarzania danych za pomocą aplikacji.



Rys 1. Zależności funkcjonalne pomiędzy podstawowymi elementami sieci

Żeby lepiej zidentyfikować kwestie związane z bezpieczeństwem podstawowych elementów sieci (traktowanych dalej jako zasoby), wprowadzono trzy pojęcia: **zagrożenie**, **słaby punkt (podatność)** i **skutek**. Wykorzystując te pojęcia można wprowadzić taksonomię ilustrującą ideę ataków na zasoby sieci Internet.

Źródłem **zagrożeń** są osoby, obiekty lub zdarzenia, które mogą naruszyć bezpieczeństwo danego zasobu. Przez zagrożenie wewnętrzne rozumie się zagrożenia wynikające z posiadania władzy nad częścią lub całością zasobu, przez zagrożenia zewnętrzne – pozostałe.

Słabymi punktami (podatnościami) zasobu określa się newralgiczne, ze względu na bezpieczeństwo, obszary i fragmenty zasobu. Słaby punkt, nazywany nieformalnie „dziurą", stanowi niekontrolowaną drogę do zasobu i może zostać wykryty, a następnie wykorzystany przez osobę, obiekt lub zdarzenie – czyli przez źródło zagrożenia. Celem wprowadzania zabezpieczeń jest wyeliminowanie tych słabych punktów. Słabe punkty można znaleźć w projekcie, w implementacji lub w konfiguracji zasobów.

*** Instytut Telekomunikacji Politechniki Warszawskiej, e-mail: P.Kijewski@tele.pw.edu.pl, K.Szczypiorski@tele.pw.edu.pl**

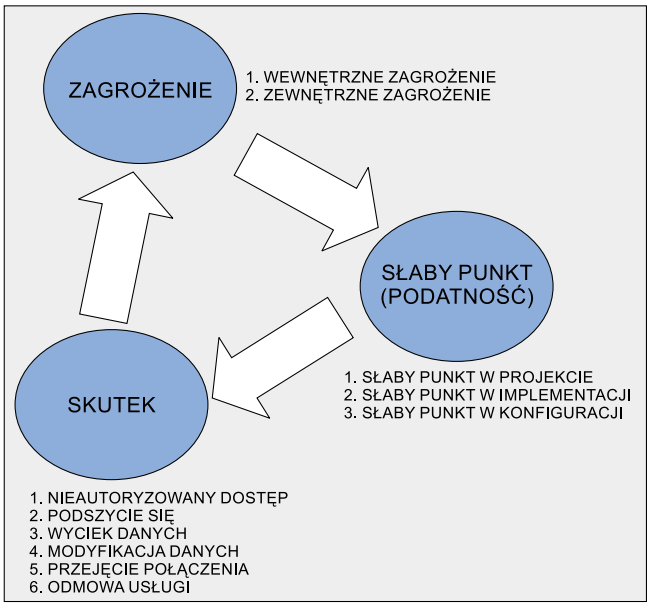
[1)] Artykuł jest uaktualnioną i rozszerzoną wersją referatu *Kierunki rozwoju zabezpieczeń w sieciach TCP/IP* wygłoszonego na Krajowym Sympozjum Telekomunikacji KST'99

Bezpośredni wynik pogwałcenia integralności zasobu – wykorzystania słabego punktu – określa się mianem **skutku**. Typowe skutki przeprowadzonego ataku to:

- nieautoryzowany dostęp – wykorzystanie zasobu przez nieuprawnione podmioty,
- podszycie się – spreparowanie danych wskazujących na innego nadawcę,
- wyciek (przechwycenie) danych,
- modyfikacja danych,
- przejęcie połączenia sieciowego,
- odmowa usługi – uniemożliwienie skorzystania z usługi lub degradacja parametrów jej obsługi.

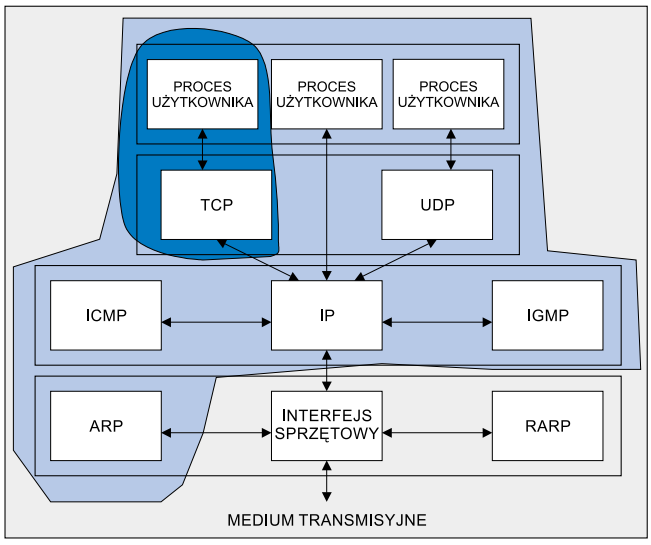
Z punktu widzenia bezpieczeństwa każdemu z wyróżnionych elementów (zasobów) może być przypisany inny mechanizm zabezpieczeń.

Na rys. 2 przedstawiono cykliczną relację pomiędzy zagrożeniem, słabym punktem a skutkiem. Zagrożenie wykorzystuje słaby punkt, aby osiągnąć pewien cel (skutek). Skutek może przerodzić się w nowe potencjalne źródło zagrożenia. Na skuteczne wykorzystanie słabego punktu może wpłynąć kilka zagrożeń, podobnie jak skutek może być osiągnięty przez odkrycie (eksplorację) kilku słabych punktów.

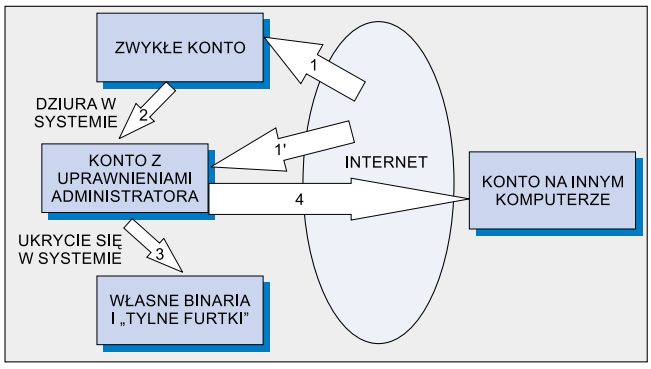


Rys. 2. Taksonomia ataków oparta na cyklicznej relacji pomiędzy zagrożeniem, słabym punktem oraz skutkiem

Stos protokołów TCP/IP, ze względu na niezbyt wyraźne zaznaczenie granic pomiędzy niższymi warstwami, a także dużą swobodę we wprowadzaniu nowych aplikacji, cechuje się szczególną podatnością na propagację błędów. Postępująca przeważnie od najniższych warstw propagacja polega na destabilizacji lub osłabieniu wiarygodności protokołów warstw wyższych. Przykładowo (rys. 3) słabe punkty protokołu **ARP** (*Address Resolution Protocol* – warstwa fizyczna) implikują niestabilne zachowanie się protokołów ze wszystkich wyższych warstw, a słabe punkty TCP – niestabilność aplikacji, takich jak np. **HTTP** (*HyperText Transfer Protocol*), telnet, **FTP** (*File Transfer Protocol*). Stosunkowo rzadko mamy do czynienia z propagacją błędów od warstw najwyższych do najniższych, za przykład może posłużyć wpływ protokołu **SNMP** (*Simple Network Management Protocol* – warstwa aplikacji) na konfigurację węzłów. Oprócz pionowej propagacji błędów niekiedy mamy do czynienia z propagacją poziomą – w obrębie jednej warstwy, np. podszycie się na poziomie **DNS** (*Domain Name System*) będzie implikować nierzetelną pracę aplikacji wykorzystujących tę usługę.



Rys. 3. Propagacja błędów w stosie protokołów TCP/IP. Oznaczenia: ARP – *Address Resolution Protocol*, ICMP – *Internet Control Message Protocol*, *IGMP – Internet Group Management Protocol*, IP – *Internet Protocol*, RARP – *Reverse Address Resolution Protocol*, TCP – *Transmission Control Protocol*, UDP – *User Datagram Protocol*



Rys. 4. Schemat typowego włamania

Rys. 4 obrazuje schemat typowego włamania do urządzenia sieciowego. Atakujący uzyskuje dostęp do systemu operacyjnego (1) na poziomie zwykłego użytkownika wykorzystując słabe punkty usług. Uzyskanie dostępu może być poprzedzone zbieraniem (tzw. skanowaniem) informacji o dostępnych usługach, wersjach aplikacji, wersji systemu operacyjnego, strukturze sieci i użytkownikach. W kolejnym etapie (2) atakujący wykorzystuje słaby punkt w aplikacji uruchomionej w systemie operacyjnym umożliwiający uzyskanie nieograniczonych praw administratora systemu. Następnie (3) może „ukryć się w systemie" przez modyfikację systemu operacyjnego (np. standardowego oprogramowania systemowego) i logów systemowych. Tak opanowany system może posłużyć jako „baza wypadowa" do następnego ataku (4). Faza (1) i (2) może być pominięta, jeśli w trakcie zdalnego skanowania celu atakujący znajdzie słaby punkt umożliwiający bezpośrednie uzyskanie praw administratora (1'). Przechodzenie włamywaczy tą drogą z jednej maszyny na drugą jest czasami nazywane „skakaniem z wyspy na wyspę" (*island hopping*).

EWOLUCJA SYSTEMÓW OCHRONY INFORMACJI

Obecnie zostaną omówione dwa charakterystyczne dla sieci TCP/IP systemy ochrony informacji: **ściany przeciwogniowe (*firewalls*)** i **systemy wykrywania włamań**. Dla każdego z sys-

temów przedstawiono klasyfikację, ewolucję oraz zalety i wady obecnie spotykanych rozwiązań.

Zastosowanie obydwu klas jest komplementarne. Zadaniem ścian przeciwogniowych jest kontrolowanie dostępu do podsieci lub pojedynczej stacji. Jest to zatem rola ukierunkowana na zewnątrz. Systemy wykrywania intruzów analizują ruch wewnątrz podsieci i pracę umieszczonych w niej systemów operacyjnych, operują na informacjach, które mają dostęp do tej podsieci. Jest to więc rola „introwertyczna", czyli wewnętrzna.

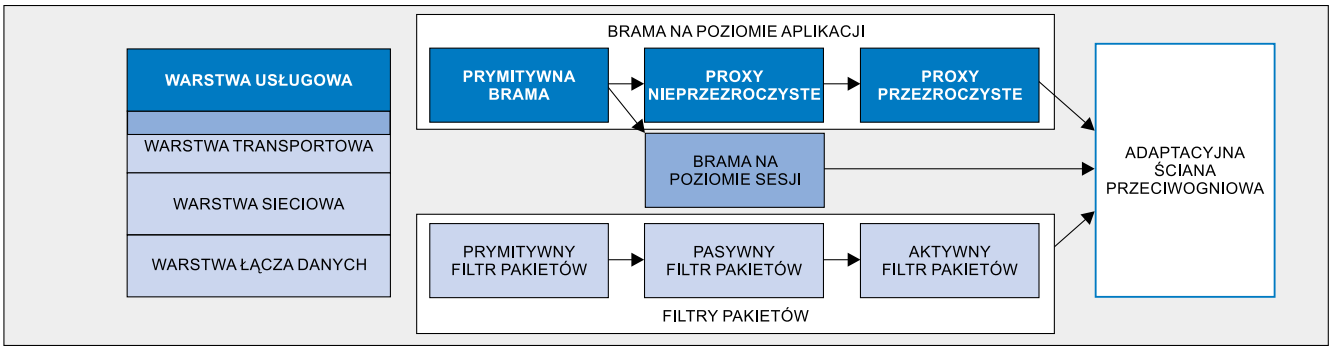
Ściany przeciwogniowe (*firewalls*)

Zadania i klasyfikacja

Ściany przeciwogniowe należą do pierwszej generacji systemów zabezpieczeń dla sieci TCP/IP. Ich pojawienie się było odpowiedzią na zagrożenia wynikające z faktu, że w sieciach TCP/IP każdy węzeł może skomunikować się z dowolnym innym węzłem. *Firewall* realizuje usługę kontroli dostępu do wybranej warstwy sieci przez **filtrowanie lub pośredniczenie w przekazywaniu (funkcja *proxy*)** jednostek danych.

Ze względu na umiejscowienie w warstwach sieci (a zatem na technikę działania) wyróżnia się trzy kategorie ścian przeciwogniowych (rys. 5):

- **filtry pakietów** (warstwy: łącza danych, sieciowa, transportowa),
- **bramy na poziomie sesji – *circuit level gateway*** (na granicy warstwy transportowej i usługowej – „odpowiednik" warstwy sesji w **OSI RM**),
- **bramy na poziomie aplikacji – *application level gateway*** (warstwą usługowa).



Rys. 5. Ewolucja i podział systemów typu *firewall*

W kolejnych trzech podpunktach omówiono poszczególne typy ścian przeciwogniowych.

Filtry pakietów

Pierwsze **prymitywne filtry pakietów** opierają swoje działanie na analizie adresów źródła i przeznaczenia na poziomie protokołu IP oraz na poziomie warstwy niższej (np. *Medium Access Control* – **MAC** w sieciach **LAN**). Na podstawie reguł określonych dla adresów, filtr decyduje o tym, czy „przeglądany" pakiet ma być przekazany do odpowiedniego węzła czy też usunięty. **Pasywne filtry pakietów** (*static filters*) dodatkowo analizują nagłówek protokołu warstwy transportowej – rozróżniają typ protokołu (**TCP**, **UDP**) oraz poszczególne flagi (tylko TCP). W przypadku protokołu bezpołączeniowego, jakim jest UDP, filtr pakietu nie ma możliwości wywnioskowania kontekstu wysłania datagramu; w TCP (protokole połączeniowym) informacje o stanie połączenia są reprezentowane na sześciu flagach[2]. Powyższego ograniczenia nie mają **aktywne filtry pakietów** (*stateful, active* lub *dynamic filters*) zachowujące kontekst sesji pomiędzy aplikacjami przez utworzenie „wirtualnego połączenia" także dla UDP.

Bramy na poziomie aplikacji (*application level gateways*)

Pierwszą odmianą bram na poziomie aplikacji jest **prymitywna brama,** która jako dedykowana maszyna w sieci lokalnej pośredniczy w komunikacji z siecią zewnętrzną. Zwyczajowo brama tej klasy jest nazywana **bastion hostem**. Bez jej pośrednictwa nie jest możliwa wymiana danych pomiędzy aplikacją uruchomioną w sieci lokalnej a aplikacją rezydującą w sieci zewnętrznej. Praca z pierwszymi bastion hostami polegała na uruchomieniu na nich zdalnej sesji, a następnie na połączeniu się z docelową maszyną. Podstawową wadę tego rozwiązania – bezpośredni dostęp do kont na bramie – usuwają ***proxy* nieprzezroczyste**. Są one związane z konkretnym protokołem aplikacyjnym – zatem każdy z nich wymaga zaimplementowania innej wersji mechanizmu. Aplikacje oraz użytkownicy muszą być poinformowani o obecności *proxy* (brak przezroczystości) – utrudnia to zarówno zarządzanie siecią, jak i pracę w niej. Najnowsza generacja bram na poziomie aplikacji jest pozbawiona tej uciążliwej cechy i nosi nazwę ***proxy* przezroczyste** (*transparent proxy*). W tym przypadku ściana przeciwogniowa „przechwytuje" połączenie i automatycznie kieruje je na *proxy*.

Bramy na poziomie sesji

Firewalle typu brama na poziomie sesji (*circuit level gateways*) pełnią rolę uogólnionych (ale nie do końca inteligentnych) *proxy* – nie są związane z konkretnym protokołem aplikacji. Dzięki temu transport danych przez *bastion hosta* staje się o wiele prostszy, z punktu widzenia administrowania siecią. Po odpowiednim dostosowaniu oprogramowania (np. po właściwej kompilacji klienta) bramy te są zawsze przezroczyste dla użytkownika[3].

Adaptacyjna ściana przeciwogniowa

Adaptacyjna ściana przeciwogniowa (*adaptive* lub *cut-through firewall*) jest hybrydą trzech poprzednich odmian – jej działanie polega na równoległym zastosowaniu wszystkich możliwych metod obsługi danego ruchu (odpowiednie pośredniczenie bądź filtrowanie). Np. początkowe połączenie klienta z serwerem zostaje przeanalizowane na poziomie aplikacji przez *proxy* przezroczyste, a następnie po podjęciu decyzji na temat jego charakteru kolejne porcje danych są przetwarzane przez aktywny filtr pakietów.

[2] Niektórych usług bazujących na TCP nie można w ten sposób bezpiecznie filtrować (np. aktywnego ftp)

[3] Obecnie wiekszość oprogramowania nie wymaga ingerencji

Tabela 1. Zalety i wady obecnie dostępnych systemów typu firewall

	Filtr pakietów	Brama na poziomie aplikacji	Bramy na poziomie sesji	Adaptacyjna ściana przeciwogniowa
Zalety	• szybkość w działaniu – znikomy wpływ na obciążenie węzła i spadek przepływności • elastyczność	• brak bezpośrednich połączeń • przezroczystość • możliwość uwierzytelnienia • analiza zawartości informacyjnej – wydanych poleceń itp., • rozbudowane możliwości logowania	• brak bezpośrednich połączeń • przezroczystość • możliwość uwierzytelnienia • szybszy od bramy na poziomie aplikacji	• zalety pozostałych trzech klas
Wady	• brak możliwości uwierzytelnienia • nie rozumie protokołu warstwy aplikacji • bezpośrednia komunikacja z siecią chronioną • elastyczność • trudna konfiguracja	• wolniejszy od filtrów pakietów i od bram na poziomie sesji (circuit level gateway) • brak wsparcia dla nowszych protokołów (do czasu napisania odpowiednich modułów)	• wolniejszy od filtrów pakietów·nie rozumie protokołu warstwy aplikacji	• nadmiar elastyczności (możliwe ustawienie słabszego trybu zabezpieczenia)

Zalety i wady

Tabela 1 zawiera zestawienie zalet i wad obecnie spotykanych systemów typu firewall.

Przyszłość *firewalli*

Ewolucja systemów *firewall* wydaje się zakończona. Zauważalne na rynku trendy dotyczą przede wszystkim udoskonalenia implementacji (specjalizowane układy cyfrowe), dedykowania ściany przeciwogniowej jednej maszynie, a nie całej podsieci (na co pozwalają współczesne komutatory), zwiększenia funkcjonalności (np. ochrona antywirusowa – *VirusWall*).

Często ściany przeciwogniowe umożliwiają konfigurowanie wirtualnych sieci prywatnych (**VPN** – *Virtual Private Network*) przez tworzenie szyfrowanych kanałów, np. na bazie IPsec albo indywidualnych rozwiązań producentów. Oprócz tego często firewalle są wyposażone w użyteczną, m. in. w zastosowaniach intranetowych, funkcję translacji adresów z wewnętrznych na internetowe (**NAT** – *Network Address Translation*).

Systemy wykrywania włamań

Zadania. Klasyfikacja

Systemy wykrywania włamań (*Intrusion Detection Systems* – **IDS**), mimo że pojawiły się w szczątkowej formie przed firewallami, należą do drugiej generacji systemów zabezpieczeń przeznaczonych dla sieci TCP/IP. Przez **włamanie** jest rozumiana sekwencja zdarzeń zagrażających bezpieczeństwu sieci. Zadaniem IDS jest odnotowanie faktu włamania, a także odpowiednia na nie reakcja[4)].

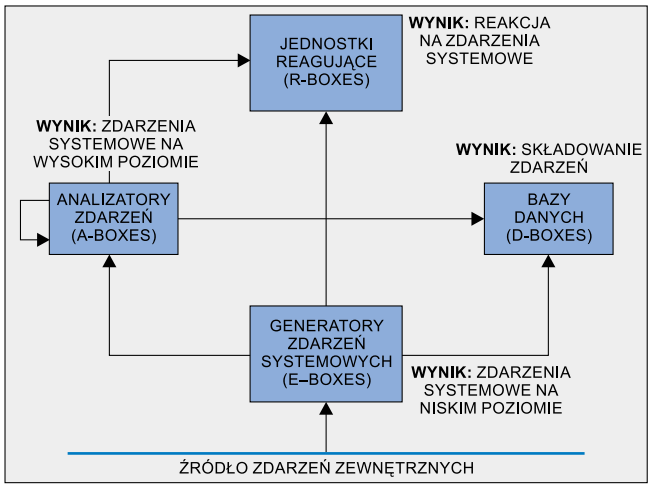
Przedstawiona w tym artykule klasyfikacja IDS jest oparta na architekturze **CIDF** (*Common Intrusion Detection Framework* – wspólna architektura wykrywania włamań [5]) i uwzględnia funkcjonalność systemów. Według CIDF w systemach wykrywania włamań można wyróżnić cztery komponenty (rys. 6):

- **E-boxes** (*Event generators*) – generatory zdarzeń systemowych – analizujące zewnętrzne zdarzenia,
- **A-boxes** (*event Analyzers*) – analizatory zdarzeń systemowych,
- **D-boxes** (*event Databases*) – bazy danych,
- **R-boxes** (*Response units*) – jednostki reagujące.

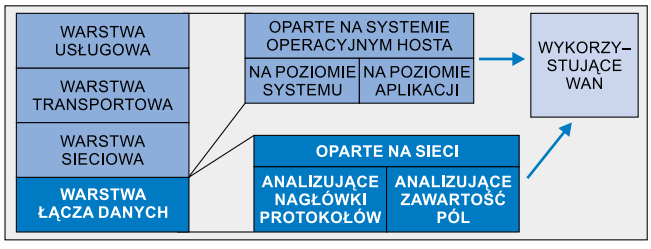
Ze względu na źródło zdarzenia zewnętrznego (a zatem i umiejscowienia *E-box*) systemy wykrywania włamań dzieli się na dwie grupy (rys.7):

- **oparte na systemie operacyjnym hosta** (*host based*), które analizują informacje w pozostałych warstwach zaimplementowanych w węźle – działają na poziomie systemu operacyjnego (*system based*) lub uruchamianych w nim aplikacji (*application based*),
- **oparte na sieci** (*network based*), które pobierają informacje z warstwy łącza danych przez podsłuch kanału transmisyjnego, w tym przypadku są analizowane: nagłówki protokołów (*traffic based*) lub zawartość pola danych (*content based*).

W odróżnieniu od ścian przeciwogniowych, które od początku swojego istnienia operowały na strumieniach danych w czasie rzeczywistym, pierwsze IDS były systemami *off-line*.



Rys. 6. Wspólna architektura wykrywania włamań (por. [6])



Rys. 7. Ewolucja i podział systemów IDS ze względu na źródło zdarzenia zewnętrznego

[4)] Reakcja może polegać np. na powiadomieniu administratora sieci, przez wysłanie krótkiej informacji tekstowej (SMS) na telefon komórkowy albo na odcięciu podejrzanego połączenia; w tym artykule przyjęto, że reakcja należy do funkcji IDS (inaczej niż w [1])

Ze względu na sposób analizy danych (*A-boxes*) wyróżnia się systemy wykrywające **anomalie** (*anomaly detection*) i **nadużycia** (*misuse detection*). W systemie IDS przyjmuje się pewien model standardowego zachowania użytkowników sieci. Wszelkie zachowania niezgodne z przyjętymi zasadami są uznawane za anomalie (np. większe wykorzystanie mocy obliczeniowej, użycie przez użytkownika niestandardowej sekwencji komend). Natomiast nadużycie jest rodzajem zachowania, które IDS rozpoznaje jako konkretny atak na system.

Jednostki reagujące (*R-boxes*) w najnowszych systemach IDS mają zdolność podejmowania decyzji służących złagodzeniu skutków włamania, mogą też „przekierowywać" intruza na specjalną maszynę-pułapkę. Stare systemy jedynie logowały rozpoznane zdarzenia i informowały o tym administratora.

Bazy danych (*D-boxes*) zawierają: znane wzorce ataków (zwane niekiedy sygnaturami), profile zachowań użytkowników i systemu, ścieżki śladów (logi wygenerowane przez pozostałe komponenty systemu).

Zalety i wady IDS

Tabela 2 zawiera zestawienie zalet i wad obecnie spotykanych systemów IDS.

Wady związane z niewystarczającą ilością informacji dotyczących perspektywy działania wybranego typu IDS (np. opartego na systemie operacyjnym hosta) można wyeliminować przez rozproszenie funkcjonalności systemu IDS, np. przez zastosowanie autonomicznych agentów rezydujących w węzłach sieciowych. Nastąpi wtedy korelacja wiadomości odbieranych ze wszystkich warstw sieci.

Wydaje się dość skomplikowane analizowanie przez system IDS zaszyfrowanego strumienia danych. W takim przypadku dla wszystkich relacji zaufania w sieci IDS musiałby stać się zaufaną trzecią stroną, bądź też wszystkie systemy ochrony informacji (np. **TLS** – patrz dalej) powinny mieć wsparcie dla systemu IDS – przekazywać dane niezbędne do jego pracy po uprzednim ich odszyfrowaniu.

Współpraca systemów wykrywania włamań ze ścianami przeciwogniowymi

Trzecia generacja systemów zabezpieczeń będzie łączyć w sobie funkcje systemów wykrywania włamań i ścian przeciwogniowych. Integracja wpłynie na większą ich elastyczność przy reagowaniu na anomalie czy też nadużycia, a także zmniejszy redundancje informacji przechowywanych w bazach danych.

Tabela 2. Zalety i wady systemów IDS

	IDS oparty na systemie operacyjnym hosta*	IDS oparty na sieci		IDS wykrywający anomalie	IDS wykrywający nadużycia
Zalety	• obserwuje i interpretuje zdarzenia w kontekście znanego systemu operacyjnego albo aplikacji	• łatwo monitoruje całe podsieci • obserwuje i interpretuje zdarzenia na najniższej warstwie sieci		• może wykrywać nieznane ataki	• może wykrywać znane ataki i ich warianty
		Analizujące nagłówki protokołów (*traffic based*)	**Analizujące zawartość pól danych (*content based*)**		
		• generuje małą liczbę logów • nie ingeruje w prywatność sesji	• wykrywa więcej ataków niż analizujący nagłówki protokołów (*traffic based*)		
Wady	• nie obserwuje warstw niższych • trudno monitoruje całe podsieci • (potencjalnie) generuje dużo logów	• trudno określić, co się dzieje na docelowej stacji • podatne na takie ataki, jak odmowa usługi, modyfikacja • strata pakietów przy większym obciążeniu sieci		• potencjalnie duża liczba fałszywych ataków – trudny dobór odpowiednich parametrów pracy • możliwość „szkolenia" systemu przez atakującego	• może wykrywać tylko znane ataki
		Analizujące nagłówki protokołów (*traffic based*)	**Analizujące zawartość pól danych (content based)**		
		• wykrywa mniej ataków niż analizujący zawartość pól danych (*content based*)	• nie potrafi analizować zaszyfrowanych danych • (potencjalnie) generuje dużo logów		

* działający na poziomie systemu operacyjnego (*system based*) i uruchamianych w nim aplikacji (*application based*)

Przyszłość systemów IDS

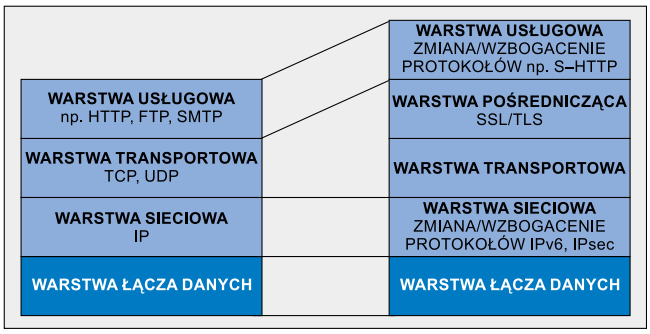
W przyszłości jest planowane rozszerzenie pola zastosowania IDS do sieci rozległych (np. Internet) oraz wyeliminowanie obecnych ograniczeń (tabela 2). W tym celu prowadzi się prace w grupie roboczej **IDWG** (*Intrusion Detection Exchange Format*) **IETF** oraz w ramach **CIDF** standaryzujące wymianę informacji na temat wykrytych przypadków włamań pomiędzy różnymi systemami oraz komponentami IDS[5)].

[5)] Por. rys. 7 – IDS wykorzystujący WAN sieć (*WAN based*) oparty na sieci rozległej

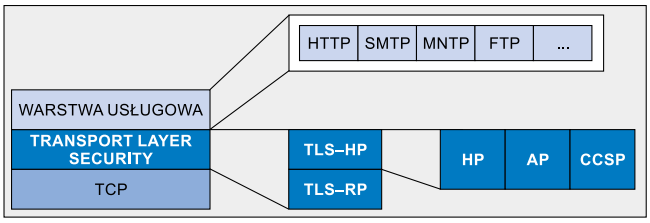
EWOLUCJA PROTOKOŁÓW ZABEZPIECZEŃ I ROZSZERZEŃ APLIKACJI

Ewolucję protokołów zabezpieczeń i rozszerzeń aplikacji widać na przykładzie zmiany warstw modelu sieci (rys. 8). Dla poszczególnych protokołów i aplikacji są zauważalne dwa podstawowe kierunki:

- **rozbudowanie (wzbogacenie)** tego, co jest – potraktowanie bezpieczeństwa jako opcji,



Rys. 8. Ewolucja poszczególnych warstw sieci TCP/IP



Rys. 9. Protokół TLS: schemat, umiejscowienie w modelu sieci TCP/IP. Oznaczenia: HTTP – *HyperText Transfer Protocol*, SMTP – *Simple Mail Transfer Protocol*, NNTP – *Network News Transfer Protocol*, FTP – *File Transfer Protocol*

● **zmiana** tego, co jest – potraktowanie zabezpieczeń jako niezbędnej składowej.

Za pierwszym trendem przemawia przede wszystkim elastyczność, brak konfliktów natury prawnej, cena, za drugim – pełna i bezwarunkowa realizacja usług ochrony informacji. Warto dodać, że zabezpieczenia w poszczególnych warstwach powinny być realizowane niezależnie.

W dziedzinie używanych algorytmów kryptograficznych jest zauważalny wzrost zainteresowania systemem uzgodnienia klucza *Diffie-Hellman* (**DH** – [2]), rozszerzonym o uwierzytelnienie za pomocą podpisów cyfrowych **DSS** (*Digital Signature Standard* – [3]), kosztem spadku popularności systemu **RSA** (*Rivest Shamir Adleman* – [13]). Wynika to z problemów związanych z patentami – na algorytm DH patent już wygasł. Coraz większą rolę zaczynają odgrywać systemy kryptograficzne oparte na krzywych eliptycznych [4].

W kolejnych trzech podrozdziałach przedstawiono ewolucję poszczególnych warstw sieci, z wyłączeniem warstwy łącza danych, która wykracza poza zakres tego opracowania.

Warstwa sieciowa

Protokół IP wersja 4 (IPv4) – serce komunikacyjne sieci TCP/IP – nie zawiera w sobie żadnych usług ochrony informacji. Ataki typu odmowa usługi, podsłuch (przechwycenie) danych, modyfikacja danych, podszycie się są dość rozpowszechnione.

Następna wersja protokołu **IPv6** (IP wersja szósta [8]) zawiera wsparcie dla usług ochrony informacji. Proponowane dwa mechanizmy bezpieczeństwa to: *IP Authentication Header* (**AH**) – nagłówek uwierzytelniający, zapewniający integralność i uwierzytelnienie [9], *IP Encapsulating Security Payload* (**ESP**) – bezpieczna koperta, zapewniająca zawsze poufność i zależnie od użytego algorytmu oraz trybu także integralność i uwierzytelnienie [10]. Wspomniane mechanizmy zostały także zaadaptowane dla IPv4 – tak rozszerzony protokół nosi nazwę **IPsec**. Dystrybucja klucza, połączona z uwierzytelnieniem, jest realizowana za pomocą protokołu **IKE –** *Internet Key Exchange* [11].

Warstwa transportowa

W warstwie transportowej zwiększa się bezpieczeństwo przez **dodanie podwarstwy – TLS**[6] (*Transport Layer Security* [7]) – pośredniczącej w wymianie danych z aplikacjami (rys. 9). Zapewnia to bezpieczną warstwę gniazd transportowych (co koresponduje z poprzednią nazwą systemu: **SSL** – *Secure Socket Layer*). Warstwa TLS składa się z dwóch podwarstw: podwarstwy zarządzania bezpieczeństwem połączenia (usługi tej warstwy realizuje protokół – *TLS-HPC Handshake Protocol*[7]) oraz podwarstwy tworzącej jednostki protokołu TLS-RP (*TLS Record Protocol*) zgodnie z wynegocjowanym kontekstem (algorytmy szyfrujące, kompresja da nych). Przy nawiązywaniu połączenia za pomocą protokołu TLS jest uzgadniany – przy użyciu algorytmów klucza publicznego – klucz sesyjny. Dane szyfrowane tym kluczem chronią informacje przed podsłuchem. Dodatkowo istnieje możliwość uwierzytelnienia klienta bądź serwera. Protokół TLS w obecnej formie (wersja 1.0) ma kilka ograniczeń: wymaga niezawodnego protokołu transportowego (TCP), nie ma wsparcia dla *proxy*, wymaga zastosowania kosztownych obliczeniowo algorytmów klucza publicznego. Trwają pracę nad zintegrowaniem protokołu TLS z innymi („starymi") systemami kryptograficznymi, takimi jak np. Kerberos.

Należy spodziewać się, że coraz więcej usług w sieciach TCP/IP będzie miało wsparcie dla TLS (obecnie są to m. in. protokoły: HTTP, SMTP, NNTP, FTP, TELNET, IMAP4, IRC, POP3). Wprowadzenie warstwy TLS (a przedtem SSL) położyło kres nieudanym pod względem elastyczności próbom bezpośredniej ingerencji w protokoły warstwy transportowej – TCP i UDP (zapomniane już koncepcje typu *Secure TCP*).

Warstwa usługowa

Zabezpieczenie warstwy usługowej jest równie bogate, jak liczba występujących w niej aplikacji. Najsilniej dają się zaobserwować wspomniane wcześniej dwa równoległe trendy:

- wzbogacenie starego protokołu,
- zaproponowanie nowego protokołu z zabezpieczeniami.

Coraz częściej wykorzystuje się także wsparcie na poziomie warstwy transportowej (**TLS/SSL**).

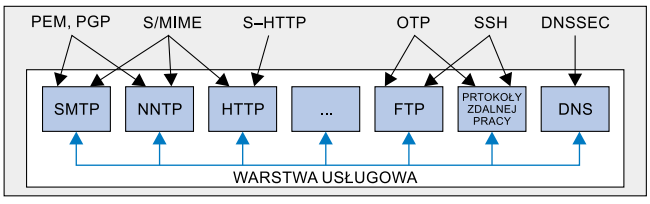
Elementem wspólnym dla bezpieczeństwa większości usług jest ich powiązanie z systemem nazywania domen **DNS** (*Domain Name System*). System ten definiuje relacje pomiędzy adresami warstwy IP (w IPv4 32-bitowe) a hierarchicznymi nazwami sieci, podsieci i maszyn. System DNS jest podatny na atak podszycia się, stąd też zaproponowane rozszerzenie [12] – nazywane czasem **DNSSEC** – uzupełnia system o usługę uwierzytelnienia przez zastosowanie dodatkowego pola z podpisem cyfrowym potwierdzającym wiadomość. Dodatkowo na poziomie DNS może być realizowana dystrybucja klucza – także na potrzeby innych usług (również transportowych).

Rys. 10 ilustruje zależności pomiędzy wybranymi mechanizmami zabezpieczeń a usługami w sieciach TCP/IP:

[6] Jest to zarówno nazwa podwarstwy, jak i protokołu który realizuje jej usługi

[7] W podwarstwie tej występują trzy protokoły: HP – *Handshake Protocol* (uzgodnienie), AP – *Alert Protocol* (obsługa błędów), CCSP – *Change Cipher Spec Protocol* (zmiana kryptosystemów)

- **PGP** (*Pretty Good Privacy*) i **PEM** (*Privacy Enhancement for Internet Electronic Mail*) – systemy ochrony wiadomości wymienianych za pomocą poczty elektronicznej, a także grup dyskusyjnych News,
- **S/MIME** (*Secure/Multipurpose Internet Mail Extensions*) – rozszerzenie o usługi ochrony informacji systemu przekazywania obiektów multimedialnych przez pocztę elektroniczną, grupy dyskusyjne i protokół HTTP,
- **S-HTTP** (*Secure HTTP*) – zmiana protokołu HTTP,
- **OTP** (*One Time Password*) – system haseł jednorazowych (dynamicznych),



Rys. 10. Zależność pomiędzy wybranymi mechanizmami zabezpieczeń a usługami w sieciach TCP/IP. Oznaczenia wyjaśniono na rys. 9 i w tekście

- **SSH** (*Secure Shell*) – system zabezpieczeń aplikacji (klient-serwer) działający podobnie do protokołu TLS.

W odróżnieniu od innych warstw bezpieczeństwo warstwy usługowej jest niejednolite. Przypuszcza się, że określenie wspólnej platformy zarządzania (w tym systemu certyfikacji kluczy publicznych) dla zabezpieczeń umożliwi uporządkowanie protokołów rozszerzających bezpieczeństwo aplikacji.

INNE ISTOTNE ZAGADNIENIA

Oprócz trendów wspomnianych w poprzednich rozdziałach wydają się istotne z punktu widzenia rozwoju zabezpieczeń trzy poniższe zagadnienia:

- **rozwój komunikacji grupowej typu *multicast*** – jako zmiana unicastowej optyki postrzegania ochrony informacji,
- **nowa generacja protokołów zarządzania** (**SNMPv3** – *Simple Network Management Protocol version 3*), która zapewni bezpieczne sterowanie zasobami sieci TCP/IP, bowiem SNMPv2 oraz jego mutacje nie zyskały popularności,
- **ujednolicenie systemów certyfikacji klucza publicznego** (na razie proponowane jest **X. 509**) ewentualnie wprowadzenie procedur metacertyfikacji (jeden węzeł potwierdza certyfikaty wydane w różnych systemach).

Stworzenie infrastruktury klucza publicznego (**PKI –** *Public Key Infrastructure*) ułatwiłoby zarządzanie ochroną informacji w sieciach TCP/IP przez obsługę jednolitej platformy do realizacji usług bezpieczeństwa. W dalszej perspektywie na podstawie PKI będą tworzone nowe usługi, takie jak: cyfrowi notariusze, anonimowe głosowanie, systemy potwierdzonej dostawy.

***

Przedstawione w artykule uogólnione spojrzenie na ataki na sieci TCP/IP opiera się na cyklicznej relacji pomiędzy zagrożeniem, słabym punktem i skutkiem. Eliminacja wszystkich słabych punktów jest w zasadzie niemożliwa – celem wprowadzania zabezpieczeń jest kontrola nad najpowszechniejszymi zagrożeniami.

Omówione w artykule kierunki rozwoju zabezpieczeń przebiegają dwiema równoległymi drogami. Tworzone są specjalistyczne systemy ochrony informacji oraz nowe protokoły zabezpieczeń i rozszerzeń aplikacji. Rozwój jednej grupy metod nie zahamuje ewolucji drugiej (np. *firewalle* nie zostaną wyparte przez IPv6).

Status ścian przeciwogniowych wydaje się być stabilny, natomiast systemy wykrywania intruzów czeka migracja w stronę sieci WAN. Zwiększenie ich funkcjonalności polega na skoordynowaniu pracy na poziomie sieci i aplikacji oraz analizowaniu danych pochodzących z różnych źródeł. Wspomniane systemy są ściśle związane z aplikacjami – w szczególności zastosowanie kryptografii w warstwie usług może komplikować ich działanie.

W przypadku ewolucji stosu protokołów największe nadzieje pokłada się w TLS (*Transport Layer Security*), zdecydowanie mniejsze w IPv6/IPsec. Zabezpieczenie komunikacji pomiędzy aplikacjami już teraz opiera się głównie na TLS, treść na poziomie usług jest chroniona właściwie tylko w poczcie elektronicznej.

Ujednolicenie systemów certyfikacji klucza publicznego – stworzenie infrastruktury klucza publicznego – powinno ułatwić zarządzanie bezpieczeństwem w sieciach TCP/IP.

Warto zauważyć, że tworzenie zabezpieczeń w sieciach TCP/IP jest pierwotne względem innych środowisk sieciowych. Przykładem tego mogą być systemy wykrywania intruzów, które w zmodyfikowanej formie mogą tworzyć (coraz popularniejsze wśród operatorów sieci telekomunikacyjnych) systemy zarządzania nadużyciami (*fraud management systems*).

LITERATURA

[1] Balasubraminiyan J., Garcia-Fernandez J., Isacoff D., Spafford E., Zamboni D.: *An Architecture for Intrusion Detection using Autonomous Agents*. COAST Technical Report 98/05, June 1998

[2] Diffie W., Hellman M. E.: *New Directions in Cryptography*. IEEE Transactions on Information Theory, V. IT-22, n. 6, June 1977

[3] NIST FIPS PUB 186 – *Digital Signature Standard*. National Institute of Standards and Technology, U. S. Department of Commerce, May 18, 1994

[4] Menezes A., van Oorschot P., Vanstone S.: *Handbook of Applied Cryptography*. CRC Press, October 1996

[5] Porras P., Schnackenberg D., Staniford-Chen S. i in.: *The Common Intrusion Detection Framework Architecture,* 1997

[6] Ptacek T., Newsham T.: *Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection.* Secure Networks Inc., January 1998

[7] Dierks T., Allen C.: *The TLS – Protocol Version 1.0.* RFC 2246, January 1999

[8] Kent S., Atkinson R.: *Security Architecture for the Internet Protocol*. RFC 2401, November 1998

[9] Kent S., Atkinson R.: *IP Authentication Header*. RFC 2402, November 1998

[10] Kent S., Atkinson R.: *IP Encapsulating Security Payload*. RFC 2406, November 1998

[11] Harkins D., Carrel D.: *The Internet Key Exchange (IKE)*. RFC 2409, November 1998

[12] Eastlake D.: *Domain Name System Security Extensions*. RFC 2535, March 1999

[13] Rivest R., Shamir A., Adleman L. M.: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM, v. 21, n. 2, February 1978

Artykuł recenzowany