Piotr Kijewski, Krzysztof Szczypiorski
Instytut Telekomunikacji
Politechnika Warszawska, Warszawa
E-mail: {P.Kijewski,K.Szczypiorski}@tele.pw.edu.pl

# Kierunki rozwoju zabezpieczeń w sieciach TCP/IP

**STRESZCZENIE**

W artykule przedstawiono ewolucję zabezpieczeń w sieciach TCP/IP, uwzględniając dwie równolegle rozwijające się klasy metod: systemy ochrony informacji oraz protokoły zabezpieczeń i rozszerzenia aplikacji. Omówiono stan obecny i przyszłość ścian przeciwogniowych (firewalls) oraz systemów wykrywania intruzów. Zaprezentowano metody ochrony informacji stosowane w poszczególnych warstwach sieci TCP/IP (w tym IPv6/IPsec, TLS/SSL, rozszerzenia aplikacji).

Piotr Kijewski, Krzysztof Szczypiorski
Institute of Telecommunications
Warsaw University of Technology, Warsaw
E-mail: {P.Kijewski,K.Szczypiorski}@tele.pw.edu.pl

# Evolution of Information Security in TCP/IP Networks

**ABSTRACT**

The paper describes the evolution of information security in TCP/IP networks, taking into account two parallel lines of development: information security systems and security protocols, as well as security extensions to existing protocols and applications. The current state and future of firewalls and intrusion detection systems is outlined. Security mechanisms adopted in the different layers of the TCP/IP protocol stack are also presented (including IPv6/IPsec, TLS/SSL, application extensions).

Piotr Kijewski, Krzysztof Szczypiorski
Instytut Telekomunikacji
Politechnika Warszawska, Warszawa
E-mail: {P.Kijewski,K.Szczypiorski}@tele.pw.edu.pl

# Kierunki rozwoju zabezpieczeń w sieciach TCP/IP

W artykule przedstawiono ewolucję zabezpieczeń w sieciach TCP/IP, uwzględniając dwie równolegle rozwijające się klasy metod: systemy ochrony informacji oraz protokoły zabezpieczeń i rozszerzenia aplikacji. Omówiono stan obecny i przyszłość ścian przeciwogniowych (firewalls) oraz systemów wykrywania intruzów. Zaprezentowano metody ochrony informacji stosowane w poszczególnych warstwach sieci TCP/IP (w tym IPv6/IPsec, TLS/SSL, rozszerzenia aplikacji).

## 1. Wprowadzenie

Klasyczne protokoły rodziny TCP/IP - tworzone podobno z myślą o odporności na atak nuklearny - nie zapewniają podstawowych usług ochrony informacji takich jak kontrola dostępu, poufność, integralność, czy uwierzytelnienie. Podczas prac nad udoskonalaniem ich 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).

Celem artykułu jest przedstawienie logicznej ewolucji poszczególnych klas metod zabezpieczeń, ze szczególnym zaznaczeniem kierunków ich rozwoju.

W kolejnych dwóch częściach artykułu przedstawiono wspomniane wyżej dwie grupy metod zabezpieczeń (systemy ochrony informacji – rozdz. 2 – oraz protokoły zabezpieczeń rozszerzenia aplikacji - rozdz. 3). Następnie przedstawiono inne istotne zdaniem autorów zagadnienia związane z kształtowaniem się metod ochrony informacji w sieciach TCP/IP (rozdz. 4). W podsumowaniu przedstawiono najważniejsze wnioski płynące z opracowania (rozdz. 5).

W niniejszej pracy przez **model sieci** będzie rozumiany **czterowarstwowy model sieci TCP/IP**. Postanowiono także pozostać przy angielskich odpowiednikach niektórych mechanizmów zabezpieczeń (np. circuit level gateway), gdyż polskie w większości przypadków nie istnieją, a jeśli istnieją są nieczytelne.

## 2. Ewolucja systemów ochrony informacji

W niniejszym rozdziale zostaną omówione dwa charakterystyczne dla sieci TCP/IP systemy ochrony informacji: **ściany przeciwogniowe (firewalls)** i **systemy wykrywania włamań**.

Dla każdego z systemów przedstawiono klasyfikację, ewolucję oraz zalety i wady obecnie spotykanych rozwiązań.

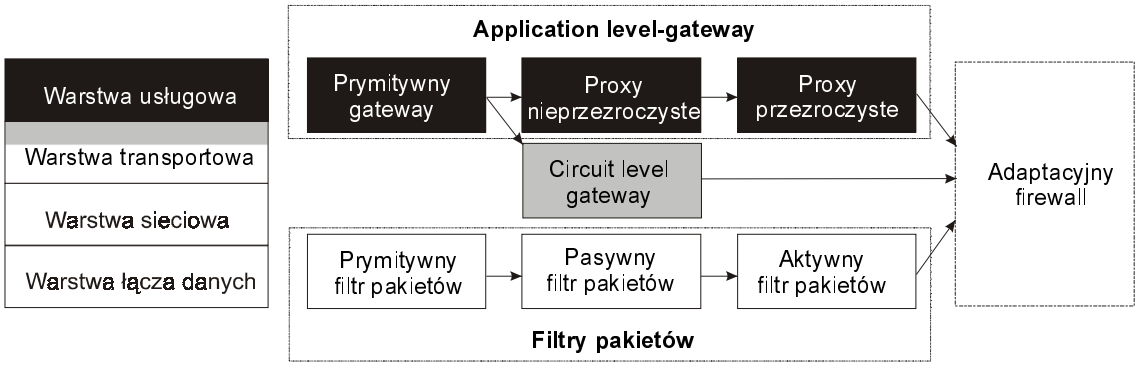
Zastosowanie obydwu klas jest komplementarne. Zadaniem ścian przeciwogniowych jest kontrolowanie dostępu do podsieci lub pojedynczej stacji. Jest to zatem rola ukierunkowana na zewnątrz. Systemy wykrywania intruzów analizują ruch wewnątrz podsieci i pracę systemów

operacyjnych umieszczonych w niej, operują na informacjach, które mają dostęp do tej podsieci. Jest to więc rola "introwertyczna".

## 2.1 Ściany przeciwogniowe (firewalls)

### 2.1.1 Zadania. Klasyfikacja

Ściany przeciwogniowe (firewalls) należą do pierwszej generacji systemów zabezpieczeń dla sieci TCP/IP. Pojawienie się firewalli jest odpowiedzią na zagrożenia wynikające z faktu, że w sieciach TCP/IP każdy węzeł może skomunikować się z dowolnym innym[1]. Firewall realizuje usługę kontroli dostępu do wybranej warstwy sieci poprzez **filtrowanie lub pośredniczenie w przekazywaniu** jednostek danych[2].




**Rysunek 1 Ewolucja i podział systemów typu firewall**

Ze względu na umiejscowienie w warstwach sieci (a co za tym idzie na technikę działania) wyróżnia się trzy kategorię firewalli (Rysunek 1):

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

W kolejnych trzech podpunktach omówiono poszczególne typy ścian przeciwogniowych.

### 2.1.2 Filtry pakietów

Pierwsze **prymitywne filtry pakietów** opierają swoje działanie na adresach źródła i przeznaczenia na poziomie protokołu IP oraz na poziomie warstwy niższej (np. Medium Access Control - MAC w sieciach LAN). Na podstawie określonych dla adresów reguł, 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[3]. Powyższego ograniczenia nie posiadają **aktywne filtry pakietów** (stateful, active lub dynamic filters) zachowujące kontekst sesji pomiędzy aplikacjami poprzez utworzenie "wirtualnego połączenia" także dla UDP.

---

[1] podobnie jak dowolni abonenci sieci telefonicznej PSTN
[2] kontynuując analogię - ścianę przeciwogniową można porównać do pośredniczącego w połączeniach sekretariatu
[3] niektórych usług bazujących na TCP nie można w ten sposób bezpiecznie filtrować (np. aktywnego ftp)

### 2.1.3 Application level gateways

Pierwszą odmianą firewalla typu application level gateway jest **prymitywny gateway,** który jako dedykowana maszyna w sieci lokalnej pośredniczy w komunikacji z siecią zewnętrzną. Zwyczajowo tej klasy bramka jest nazywana **bastion hostem**.

Bez pośrednictwa bastion hosta 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 gatewayu - usuwają **proxy**[4] **nieprzezroczyste**. Proxy nieprzezroczyste są 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 firewalli typu application level gateway 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.

### 2.1.4 Circuit-level gateways

Firewalle typu circuit level gateways pełnią rolę uogólnionych (ale nie do końca inteligentnych) proxy - nie są związane z konkretnym protokołem aplikacji. Dzięki temu transport danych poprzez bastion hosta staje się z punktu widzenia administrowania siecią o wiele prostszy. Po odpowiednim dostosowaniu oprogramowania (np. po właściwej kompilacji klienta) circuit level gateways zawsze są przezroczyste dla użytkownika[5].

### 2.1.5 Adaptacyjny firewall

**Adaptacyjny firewall** (adaptive lub cut-through firewall) jest hybrydą trzech poprzednich odmian – jego działanie polega na równoległym zastosowaniu wszystkich możliwych metod do 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.

### 2.1.6 Zalety i wady

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

**Tabela 1 Zalety i wady obecnie dostępnych systemów typu firewall**

| | Filtr pakietów | Application level gateway | Circuit level gateway | Adaptacyjny firewall |
|---|---|---|---|---|
| zalety | • szybkość w działaniu – znikomy wpływ na obciążenie węzła i spadek przepływności<br>• elastyczność | • brak bezpośrednich połączeń<br>• przezroczystość<br>• możliwość uwierzytelnienia<br>• analiza zawartości informacyjnej – wydanych poleceń itp.,<br>• rozbudowane możliwości logowania | • brak bezpośrednich połączeń<br>• przezroczystość<br>• możliwość uwierzytelnienia<br>• szybszy od application level gateway | • zalety pozostałych trzech klas |
| wady | • brak możliwości uwierzytelnienia<br>• nie rozumie protokołu warstwy aplikacji<br>• bezpośrednia komunikacja z siecią chronioną<br>• elastyczność<br>• trudna konfiguracja | • wolniejszy od filtrów pakietów i od circuit level gateway<br>• brak wsparcia dla nowszych protokołów (do czasu napisania odpowiednich modułów) | • wolniejszy od filtrów pakietów<br>• nie rozumie protokołu warstwy aplikacji | • nadmiar elastyczności (możliwe ustawienie słabszego trybu zabezpieczenia) |

[4] system pośredniczący

[5] obecnie większość oprogramowania nie wymaga ingerencji

### 2.1.7 Przyszłość firewalli

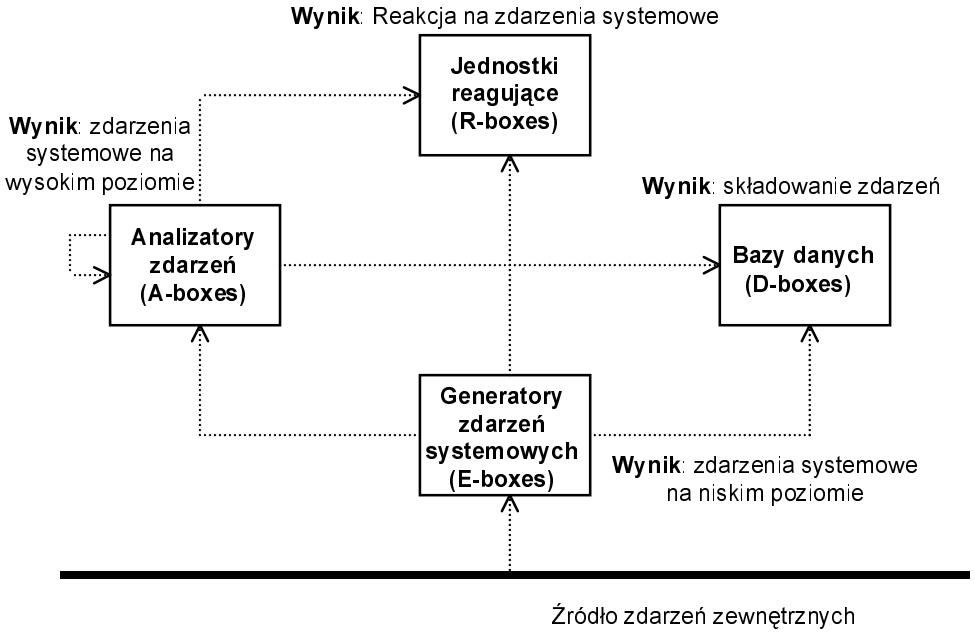
Ewolucja systemów firewall wydaje się być zakończona. Zauważalne na rynku trendy dotyczą przede wszystkim udoskonalenia implementacji (specjalizowane układy cyfrowe), dedykowania ściany przeciwogniowej jednej maszynie, a nie całej podsieci (na co pozwalają współczesne switche), zwiększenia funkcjonalności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

Coraz częściej ściany przeciwogniowe zezwalają na konfigurowanie wirtualnych sieci prywatnych (VPN – Virtual Private Network) poprzez 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).

## 2.2 Systemy wykrywania włamań

### 2.2.1 Zadania. Klasyfikacja

**Systemy wykrywania włamań** (intrusion detection systems - **IDS**), mimo że pojawiły się w szczątkowej formie przed firewallami, należą do drugiej generacji systemów zabezpieczeń dla sieci TCP/IP. Poprzez **włamanie** rozumiana jest sekwencja zdarzeń zagrażających bezpieczeństwu sieci. Zadaniem IDS jest odnotowanie faktu włamania, a także odpowiednia na nie reakcja[6].



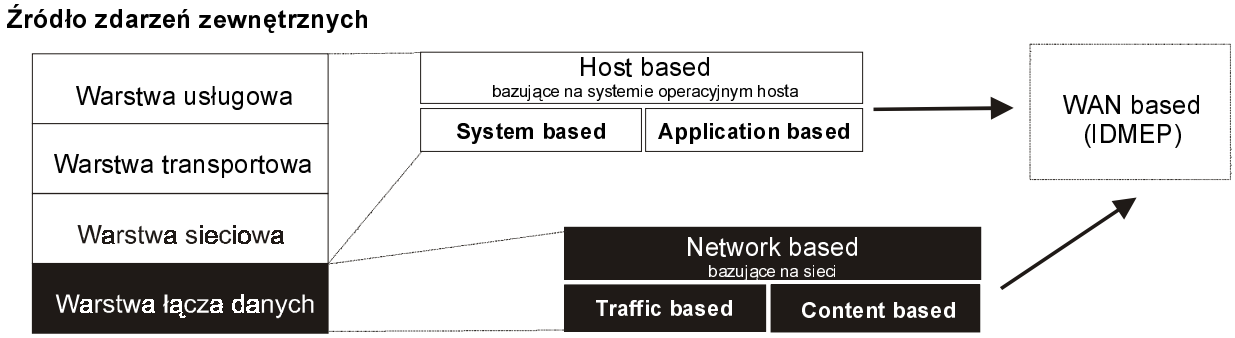

**Rysunek 2 Architektura Common Intrusion Detection Framework (por. [Ptacek98])**

Przedstawiona w tej pracy klasyfikacja IDS oparta jest na architekturze CIDF (Common Intrusion Detection Framework - [Porras97]) i uwzględnia funkcjonalność systemów. Według CIDF w systemach wykrywania włamań można wyróżnić cztery komponenty (Rysunek 2):

---

[6] reakcja może polegać np. na powiadomieniu administratora poprzez wysłanie krótkiej informacji tekstowej (SMS) na telefon komórkowy albo na odcięciu podejrzanego połączenia; w tej pracy traktujemy, że reakcja należy do funkcji IDS (inaczej niż w [Balasu1998])

- E-boxes (**e**vent generators) - generatory zdarzeń systemowych - analizujące zewnętrzne zdarzenia,
- A-boxes (event **a**nalyzers) - analizatory zdarzeń systemowych,
- D-boxes (event **d**atabases) - bazy danych,
- R-boxes (**r**esponse units) - jednostki reagujące.




**Rysunek 3 Ewolucja i podział systemów IDS ze względu na źródło zdarzenia zewnętrznego**

Ze względu na źródło zdarzenia zewnętrznego (a zatem i umiejscowienia E-box) systemy wykrywania włamań dzieli się na dwie grupy (Rysunek 3):

- **bazujące na systemie operacyjnym hosta** (host based), które analizuję informacje w pozostałych warstwach zaimplementowanych w węźle - działają na poziomie systemu operacyjnego (system based) lub uruchamianych w nim aplikacji (application based),
- **bazujące na sieci** (network based), które pobierają informacje z warstwy łącza danych poprzez podsłuch kanału transmisyjnego, w tym wypadku analizowane są: 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.

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[7]. Natomiast nadużycie jest rodzajem zachowania, które IDS rozpoznaje jako konkretny atak na system.

Jednostki reagujące (R-boxes) w najnowszych systemach IDS posiadają zdolność podejmowania decyzji mających na celu złagodzenie skutków włamania, mogą też "przekierowywać" intruza na specjalną maszynę-pułapkę. Stare systemy jedynie logowały rozpoznane zdarzenia i informowały o tym administratora (por. przypis 6).

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

### 2.2.2 Zalety i wady IDS

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

[7] np. większe wykorzystanie mocy obliczeniowej, użycie przez użytkownika niestandardowego sekwencji komend

**Tabela 2 Zalety i wady systemów IDS**

| | IDS bazujący na systemie operacyjnym hosta[8] | IDS bazujący na sieci | | IDS wykrywający anomalie | IDS wykrywający nadużycia |
|---|---|---|---|---|---|
| **zalety** | • obserwuje i interpretuje zdarzenia w kontekście znanego systemu operacyjnego albo aplikacji | • łatwo monitoruje całe podsieci<br>• obserwuje i interpretuje zdarzenia na najniższej warstwie sieci | | • może wykrywać nieznane ataki | • może wykrywać znane ataki i ich warianty |
| | | **Traffic based** | **Content based** | | |
| | | • generuje małą ilość logów<br>• nie ingeruje w prywatność sesji | • wykrywa więcej ataków niż traffic based (analizuje zawartość) | | |
| **wady** | • nie obserwuje warstw niższych<br>• trudno monitoruje całe podsieci<br>• (potencjalnie) generuje dużo logów | • trudno określić co się dzieje na docelowej stacji<br>• podatne na takie ataki typu odmowa usługi, modyfikacja<br>• strata pakietów przy większym obciążeniu sieci | | • potencjalnie duża ilość fałszywych ataków - trudny dobór odpowiednich parametrów pracy<br>• możliwość "szkolenia" systemu przez atakującego | • może wykrywać **tylko** znane ataki |
| | | **Traffic based** | **Content based** | | |
| | | • wykrywa mniej ataków niż content based | • nie potrafi analizować zaszyfrowanych danych<br>• (potencjalnie) generuje dużo logów | | |

### 2.2.3 Przyszłość systemów IDS

W przyszłości planowane jest rozszerzenie pola zastosowania IDS do sieci rozległych (np. Internet) oraz wyeliminowanie obecnych ograniczeń (por. Tabela 2). W tym celu rozwijany jest protokół IDMEP - Intrusion Detection Message Exchange Protocol - standaryzujący wymianę informacji na temat wykrytych przypadków włamań pomiędzy różnymi systemami oraz komponentami IDS[9].

Wady związane z niewystarczającą ilością informacji pochodzących z perspektywy działania wybranego typu IDS (np. bazującego na systemie operacyjnym hosta) można rozwiązać poprzez rozproszenie funkcjonalności systemu IDS np. poprzez zastosowanie autonomicznych agentów rezydujących w węźle sieciowych. Nastąpi wtedy korelacja wiadomości odbieranych ze wszystkich warstw sieci.

Dość skomplikowana wydaje się analizowanie przez 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 - por. 3.2) powinny mieć wsparcie dla IDS - przekazywać niezbędne do jego pracy dane po uprzednim odszyfrowaniu.

### 2.3 Współpraca systemów wykrywania włamań ze ścianami przeciwogniowymi

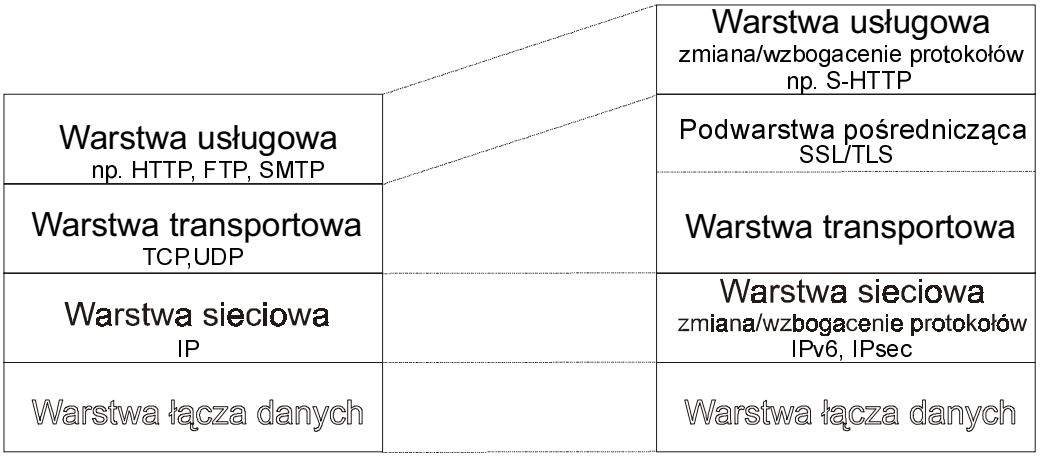
Według autorów trzecia generacja produktów zabezpieczeń będzie łączyć w sobie funkcje systemów wykrywania włamań i ścian przeciwogniowych. Integracja wpłynie na większą elastyczność przy reagowaniu na anomalie czy też nadużycia, a także zmniejszy redundancje informacji przechowywanych w bazach danych.

## 3. Ewolucja protokołów zabezpieczeń i rozszerzeń aplikacji

Ewolucję protokołów zabezpieczeń i rozszerzeń aplikacji widać na przykładzie zmiany warstw modelu sieci (Rysunek 4). Dla poszczególnych protokołów i aplikacji są zauważalne dwa podstawowe kierunki:

- **rozbudowanie (wzbogacenie)** tego co jest – potraktowania bezpieczeństwa jako opcji,
- **zmiana** tego co jest – potraktowania zabezpieczeń jako niezbędnej składowej.

[8] system based i application based
[9] por. Rysunek 3 - WAN based - IDS bazujący na sieci rozległej




**Rysunek 4 Ewolucja poszczególnych warstw sieci TCP/IP**

Za pierwszym trendem przemawia przede wszystkim elastyczność, brak konfliktów natury prawnej[10], cena[11]. 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 zauważalny jest wzrost zainteresowania systemem uzgodnienia klucza Diffie-Hellman (DH – [Diffie77]) rozszerzonym o uwierzytelnienie za pomocą podpisów cyfrowych DSS (Digital Signature Standard – [FIPS186]), kosztem spadku popularności systemu RSA (Rivest Shamir Adleman – [Rivest78]). Wynika to z problemów związanych z patentami[12]. Coraz większą rolę zaczynają odgrywać systemy kryptograficzne oparte na krzywych eliptycznych [Menezes96].

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

### 3.1 Warstwa sieciowa

Protokół IP wersja 4 – serce komunikacyjne sieci TCP/IP – nie zawiera w sobie żadnych usług ochrony informacji[13]. Ataki typu odmowa usługi, podsłuch informacji, nieautoryzowana modyfikacja informacji, podszycie się są dość rozpowszechnione.

Następna wersja protokołu IPv6 (IP wersja szósta [RFC2401]) zawiera wsparcie dla usług ochrony informacji. Proponowane dwa mechanizmy bezpieczeństwa to: **IP Authentication Header** (AH) - nagłówek uwierzytelniający - zapewniający integralność i uwierzytelnienie [RFC2402], **IP Encapsulating Security Payload** (ESP) - bezpieczna koperta - zapewniająca zawsze poufność i zależnie od użytego algorytmu i trybu także integralność i uwierzytelnienie [RFC2406]. 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 [RFC2409].

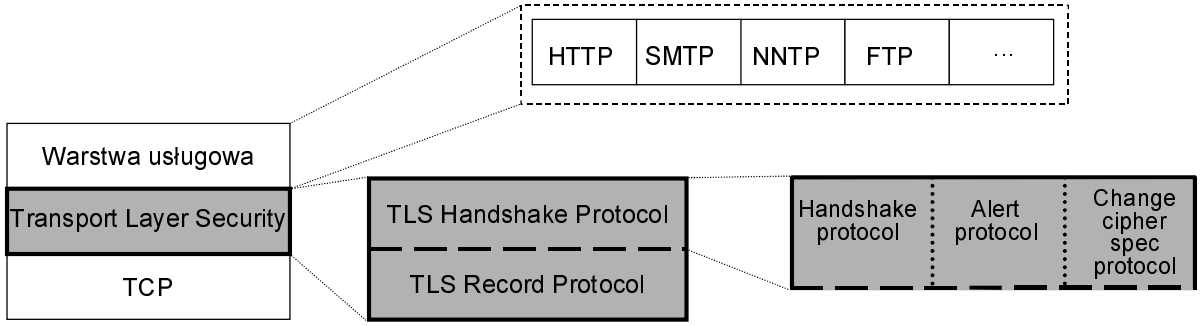
---

[10] ograniczenia w używaniu kryptografii w niektórych państwach (np. Francja, Rosja)
[11] nie trzeba zmieniać od razu całego oprogramowania i sprzętu
[12] na DH patent już wygasł
[13] był projektowany w latach 70.

### 3.2 Warstwa transportowa

W warstwie transportowej zwiększa się bezpieczeństwo poprzez **dodanie podwarstwy – TLS - Transport Layer Security** [RFC2246] - pośredniczącej w wymianie danych z aplikacjami (Rysunek 5). Zapewnia to bezpieczną warstwę gniazd transportowych (co koresponduje z poprzednią nazwą systemu: SSL - Secure Socket Layer). TLS składa się z dwóch warstw: warstwy zarządzania bezpieczeństwem połączenia (TLS Handshake Protocol[14]) oraz warstwy tworzącej jednostki protokołu TLS (TLS Record Protocol) zgodnie z wynegocjowanym kontekstem (algorytmy szyfrujące, kompresja danych). Przy nawiązywaniu połączenia za pomocą TLS uzgadniany jest przy użyciu algorytmów klucza publicznego klucz sesyjny. Dane szyfrowane tym kluczem chronią informacje przed podsłuchem. Dodatkowo istnieje możliwość uwierzytelnienia klienta bądź serwera. TLS w obecnej formie (wersja 1.0) posiada kilka ograniczeń: wymaga niezawodnego protokołu transportowego (TCP), nie ma wsparcia dla proxy, wymaga zastosowania kosztownych obliczeniowo algorytmów klucza publicznego. Trwają pracę nad zintegrowaniem TLS z innymi (”starymi”) systemami kryptograficznymi takimi jak np. Kerberos.

Należy się spodziewać, że coraz więcej usług w sieciach TCP/IP będzie miało wsparcie dla TLS[15]. Wprowadzenie 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).




**Rysunek 5 Protokół TLS: schemat, umiejscowienie w modelu sieci TCP/IP**

### 3.3 Warstwa usługowa

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

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

Także coraz częściej wykorzystuje się 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. DNS jest podatny na atak podszycia się - stąd też zaproponowane rozszerzenie [RFC2535] – nazywane czasem DNSSEC[16] - uzupełnia system o usługę uwierzytelnienia poprzez zastosowanie

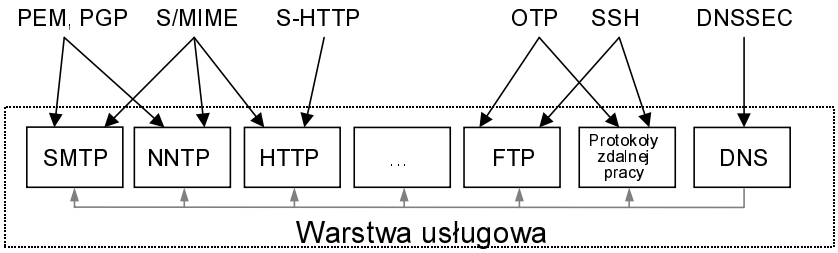
---

[14] w podwarstwie występują trzy protokoły: Handshake protocol (uzgodnienie), Alert protocol (obsługa błedów), Change ciper spec protocol (zmiana kryptosystemów)

[15] obecnie są to m.in.: HTTP, SMTP, NNTP, FTP, TELNET, IMAP4, IRC, POP3

[16] od nazwy grupy IETF

dodatkowego pola z podpisem cyfrowym potwierdzającym wiadomość. Dodatkowo na poziomie DNS może być realizowana dystrybucja klucza – także na potrzeby innych usług.




**Rysunek 6 Zależność pomiędzy wybranymi mechanizmami zabezpieczeń a usługami w sieciach TCP/IP**

Rysunek 6 ilustruje zależności pomiędzy **wybranymi** mechanizmami zabezpieczeń a usługami w sieciach TCP/IP:

- 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 poprzez pocztę elektroniczną, grupy dyskusyjne i protokół HTTP,
- S-HTTP (Secure HTTP) – zmiana protokołu HTTP,
- OTP (One Time Password) – system haseł jednorazowych (dynamicznych),
- SSH (Secure Shell) – system zabezpieczeń aplikacji (klient-serwer) działający podobnie do TLS.

W odróżnieniu do innych warstw bezpieczeństwo warstwy usługowej jest niejednolite. Przypuszczamy, że określenie wspólnej platformy zarządzania (w tym systemu certyfikacji kluczy publicznych) dla zabezpieczeń pozwoli na uporządkowanie protokołów rozszerzających bezpieczeństwo aplikacji.

## 4. Inne istotne zagadnienia

Oprócz wspomnianych w poprzednich rozdziałach trendów wydaje się nam, że trzy poniższe zagadnienia są istotne z punktu widzenia rozwoju zabezpieczeń:

- **rozwój komunikacji grupowej** (multicast) – jako zmiana unicastowej optyki postrzegania ochrony informacji,
- **nowa generacja protokołów zabezpieczeń** (SNMPv3 – Simple Network Management Protocol version 3) – która zezwoli[17] na bezpieczne sterowania zasobami sieci TCP/IP,
- **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 bazie PKI będą tworzone nowe usługi takie jak: cyfrowi notariusze, anonimowe głosowanie, systemy potwierdzonej dostawy.

[17] SNMPv2 oraz jego mutacje nie zyskały popularności

## 5. Podsumowanie

Przedstawione w pracy 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 funkcjonalności poprzez skoordynowanie pracy na poziomie sieci i aplikacji oraz analizowane danych 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


[Balasu1998] J. Balasubraminiyan, J. Garcia-Fernandez, D. Isacoff, E. Spafford, D. Zamboni - *An Architecture for Intrusion Detection using Autonomous Agents* - COAST Technical Report 98/05 - June 1998

[Diffie77] W. Diffie, M. E. Hellman - *New Directions in Cryptography* - IEEE Transactions on Information Theory, V. IT-22, n. 6, June 1977

[FIPS186] NIST FIPS PUB 186 - *Digital Signature Standard* - National Institute of Standards and Technology, U.S. Department of Commerce, May 18, 1994.

[Menezes96] A.Menezes, P. van Oorschot, S.Vanstone - *Handbook of Applied Cryptography* - CRC Press, October 1996

[Porras97] P. Porras, D. Schnackenberg, S. Staniford-Chen i in. - *The Common Intrusion Detection Framework Architecture* - 1997

[Ptacek98] T. Ptacek, T. Newsham - *Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection* - Secure Networks Inc., January 1998

[RFC2246] T. Dierks, C. Allen - *The TLS - Protocol Version 1.0* - RFC 2246, January 1999

[RFC2401] S. Kent, R. Atkinson - *Security Architecture for the Internet Protocol*, RFC 2401, November 1998

[RFC2402] S. Kent, R. Atkinson - *IP Authentication Header*, RFC 2402, November 1998

[RFC2406] S. Kent, R. Atkinson - *IP Encapsulating Security Payload*, RFC 2406, November 1998

[RFC2409] D. Harkins, D. Carrel - *The Internet Key Exchange (IKE)*, RFC 2409, November 1998

[RFC2535] D. Eastlake - *Domain Name System Security Extensions* - Eastlake - RFC 2535, March 1999

[Rivest78] R. Rivest, A. Shamir, L. M. Adleman - *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* - Communications of the ACM, v. 21, n. 2, February 1978