

# Kierunki rozwoju zabezpieczeń w sieciach TCP/IP

Piotr Kijewski, Krzysztof Szczypiorski  
e-mail: {P.Kijewski, K.Szczypiorski}@tele.pw.edu.pl

KST'99 - Bydgoszcz, 8-10 wrzesień 1999

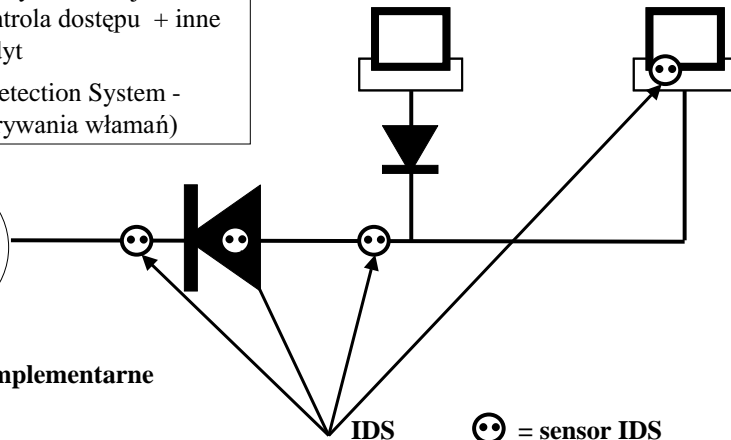
## Plan prezentacji

- Ewolucja zabezpieczeń:
  - ewolucja systemów zabezpieczeń (zastosowanie, klasyfikacja, działanie, wady i zalety)
    - ściany przeciwogniowe
    - systemy wykrywania włamań
    - współpraca systemów
  - ewolucja protokołów zabezpieczeń i rozszerzeń aplikacji (zastosowanie, cechy)
    - warstwa sieciowa
    - warstwa transportowa
    - warstwa usługowa
- w podsumowaniu: inne trendy

## Ewolucja systemów zabezpieczeń

Zastosowanie

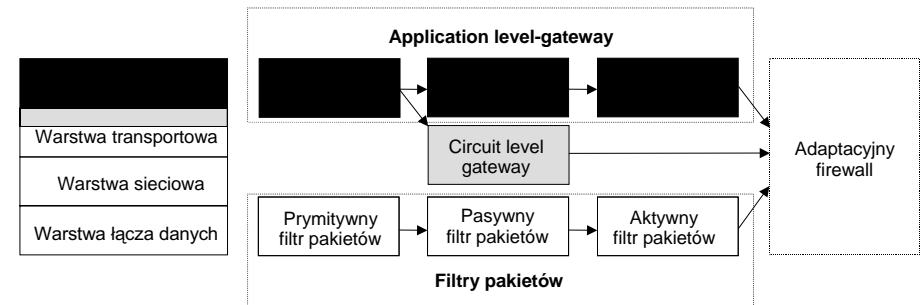
Usługi ochrony informacji:  
**FW:** kontrola dostępu + inne  
**IDS:** audyt  
 (Intrusion Detection System - system wykrywania włamań)



Metody komplementarne

## Ściany przeciwogniowe (firewalls)

Klasyfikacja. Działanie.



# Ściany przeciwogniowe (firewalls)

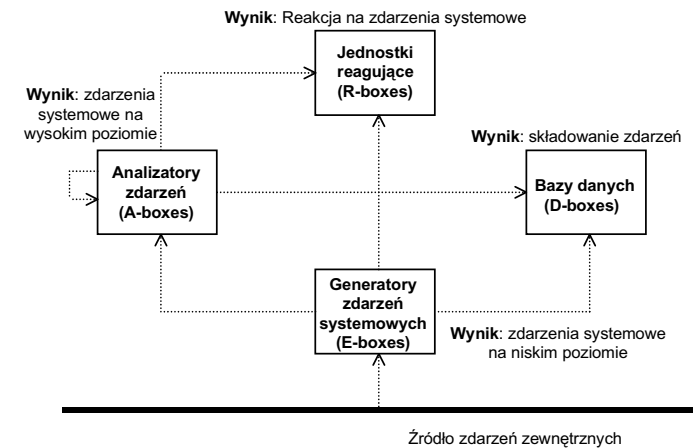
Zalety i wady

	Filtr pakietów	Application level gateway	Circuit level gateway	Adaptacyjny firewall
zalety	<ul style="list-style-type: none"> <li>szybkość w działaniu – znikomy wpływ na obciążenie węzła i spadek przepływności</li> <li>elastyczność</li> </ul>	<ul style="list-style-type: none"> <li>brak bezpośrednich połączeń</li> <li>przezroczystość</li> <li>możliwość uwierzytelnienia</li> <li>analiza zawartości informacyjnej – wydanych poleceń itp.</li> <li>rozbudowane możliwości logowania</li> </ul>	<ul style="list-style-type: none"> <li>brak bezpośrednich połączeń</li> <li>przezroczystość</li> <li>możliwość uwierzytelnienia</li> <li>szybszy od application level gateway</li> </ul>	<ul style="list-style-type: none"> <li>zalety pozostałych trzech klas</li> </ul>
wady	<ul style="list-style-type: none"> <li>brak możliwości uwierzytelnienia</li> <li>nie rozumie protokołu warstwy aplikacji</li> <li>bezpośrednia komunikacja z siecią chronioną</li> <li>elastyczność</li> <li>trudna konfiguracja</li> </ul>	<ul style="list-style-type: none"> <li>wolniejszy od filtrów pakietów i od circuit level gateway</li> <li>brak wsparcia dla nowszych protokołów (do czasu napisania odpowiednich modułów)</li> </ul>	<ul style="list-style-type: none"> <li>wolniejszy od filtrów pakietów</li> <li>nie rozumie protokołu warstwy aplikacji</li> </ul>	<ul style="list-style-type: none"> <li>nadmiar elastyczności (możliwe ustawienie słabszego trybu zabezpieczenia)</li> </ul>

Perspektywy rozwoju? (rozbudowa wsparcia dla VPN, NAT; VirusWall)

# Systemy wykrywania włamań (IDS)

Działanie IDS na bazie architektury Common Intrusion Detection Framework

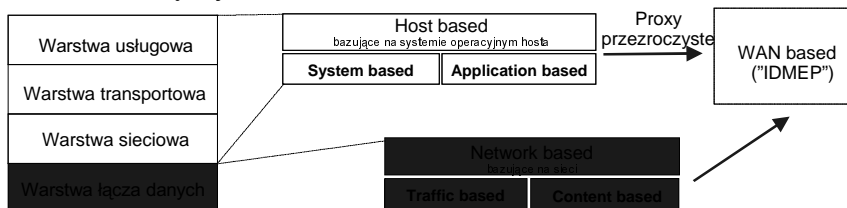


# Systemy wykrywania włamań (IDS)

Klasyfikacja

Podział ze względu na umiejscowienie E-box:

Źródło zdarzeń zewnętrznych:



Podział ze względu na sposób analizy danych (A-box):

- IDS wykrywające **anomalie** (czyli zachowania niezgodne z przyjętymi zasadami)
- IDS wykrywające **nadużycia** (czyli konkretny **atak** na system)

# Systemy wykrywania włamań (IDS)

Zalety i wady

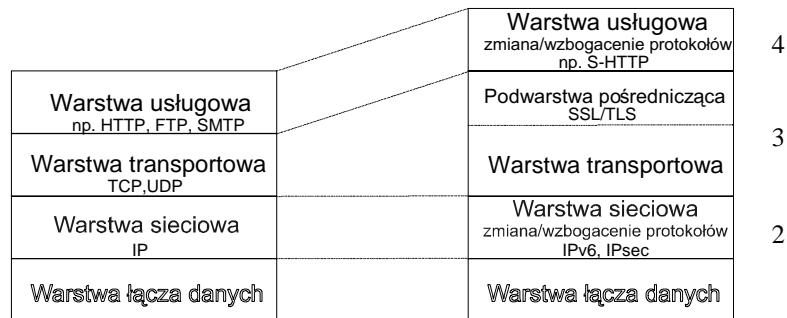
	IDS bazujący na systemie operacyjnym hosta	IDS bazujący na sieci	IDS wykrywający anomalie	IDS wykrywający nadużycia				
zalety	<ul style="list-style-type: none"> <li>obserwuje i interpretuje zdarzenia w kontekście znanego systemu operacyjnego albo aplikacji</li> </ul>	<ul style="list-style-type: none"> <li>łatwo monitoruje całe podsieci</li> <li>obserwuje i interpretuje zdarzenia na najniższej warstwie sieci</li> </ul> <table border="1"> <tr> <th>Traffic based</th> <th>Content based</th> </tr> <tr> <td> <ul style="list-style-type: none"> <li>generuje małą ilość logów</li> <li>nie ingeruje w prywatność sesji</li> </ul> </td> <td> <ul style="list-style-type: none"> <li>wykrywa więcej ataków niż traffic based (analizuje zawartość)</li> </ul> </td> </tr> </table>	Traffic based	Content based	<ul style="list-style-type: none"> <li>generuje małą ilość logów</li> <li>nie ingeruje w prywatność sesji</li> </ul>	<ul style="list-style-type: none"> <li>wykrywa więcej ataków niż traffic based (analizuje zawartość)</li> </ul>	<ul style="list-style-type: none"> <li>może wykrywać nieznane ataki</li> </ul>	<ul style="list-style-type: none"> <li>może wykrywać znane ataki i ich warianty</li> </ul>
Traffic based	Content based							
<ul style="list-style-type: none"> <li>generuje małą ilość logów</li> <li>nie ingeruje w prywatność sesji</li> </ul>	<ul style="list-style-type: none"> <li>wykrywa więcej ataków niż traffic based (analizuje zawartość)</li> </ul>							
wady	<ul style="list-style-type: none"> <li>nie obserwuje warstw niższych</li> <li>trudno monitoruje całe podsieci</li> <li>(potencjalnie) generuje dużo logów</li> </ul>	<ul style="list-style-type: none"> <li>trudno określić co się dzieje na docelowej stacji</li> <li>podatne na takie ataki typu odmowa usługi, modyfikacja</li> <li>strata pakietów przy większym obciążeniu sieci</li> </ul>	<ul style="list-style-type: none"> <li>potencjalnie duża ilość fałszywych ataków - trudny dobór odpowiednich parametrów pracy</li> <li>możliwość "szkolenia" systemu przez atakującego</li> </ul>	<ul style="list-style-type: none"> <li>może wykrywać <b>tylko</b> znane ataki</li> </ul>				

Perspektywy rozwoju ("IDMEP\*", problemy z zaszyfrowanym strumieniem danych)  
Współpraca ze ścianami przeciwogniowymi.

\*IDMEP = Intrusion Detection Message Exchange Protocol

# Ewolucja protokołów zabezpieczeń

Ewolucja poszczególnych warstw modelu sieci TCP/IP

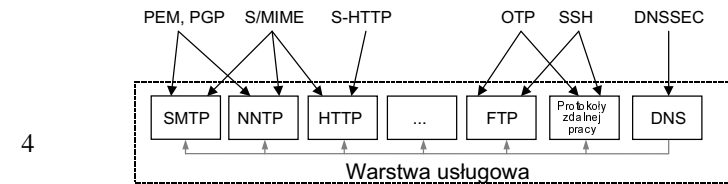
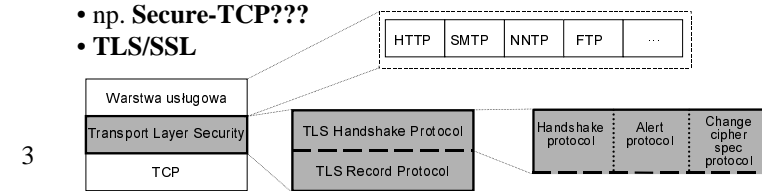


# Ewolucja w poszczególnych warstwach

2 • IPv6/IPsec - Authentication Header, Encapsulating Security Payload, Internet Key Exchange

• np. Secure-TCP???

• TLS/SSL



## Podsumowanie

- **zabezpieczenia podążają dwiema drogami:**
  - **specjalistyczne systemy ochrony informacji**
    - status ścian przeciwogniowych wydaje się być stabilny
    - systemy wykrywania włamań czeka:
      - migracja w stronę sieci WAN
      - zwiększenie funkcjonalności poprzez skoordynowanie pracy na poziomie sieci i aplikacji
      - analizowane danych z różnych źródeł
  - **nowe protokoły zabezpieczeń i rozszerzenia aplikacji**
    - TLS, w mniejszym stopniu IPv6/IPsec
  - **żadna z dróg nie wyeliminuje drugiej (FW vs. IPv6)**
- **inne trendy:**
  - ujednoczenie systemów certyfikacji klucza publicznego
  - nowa generacja protokołów zarządzania
  - rozwój komunikacji grupowej
- **zabezpieczeniach w sieciach TCP/IP a zabezpieczenia w innych sieciach telekomunikacyjnych:**
  - rozwiązania pierwotne
  - np. IDS vs. Fraud Management System (system zarządzania nadużyciami)

# KONIEC

Czy mają Państwo pytania?



# Literatura

- **IDS:**
  - 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
  - P. Porras, D. Schnackenberg, S. Staniford-Chen i in. - *The Common Intrusion Detection Framework Architecture* - 1997
  - T. Ptacek, T. Newsham - *Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection* - Secure Networks Inc., January 1998
- **TLS 1.0** - RFC 2246
- **IPv6/IPsec** - RFC 2401, 2402, 2406, 2409
- **bezpieczny DNS** - RFC 2535
- **PGP** - RFC 1991
- **PEM** - RFC 1421-1424
- **SNMPv3** - RFC 2264
- **S/MIME** - RFC 2311-2312
- **SSH** - <http://www.ietf.org/html.charters/secsh-charter.html>
- **S-HTTP** - <http://www.ietf.org/html.charters/wts-charter.html>
- **OTP** - RFC 2289, 2243-2244