Politechnika Warszawska
Instytut Telekomunikacji

Ewolucja zabezpieczeń w sieciach TCP/IP

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

NETSEC'99 - Katowice, 20-21 maja 1999

Plan prezentacji

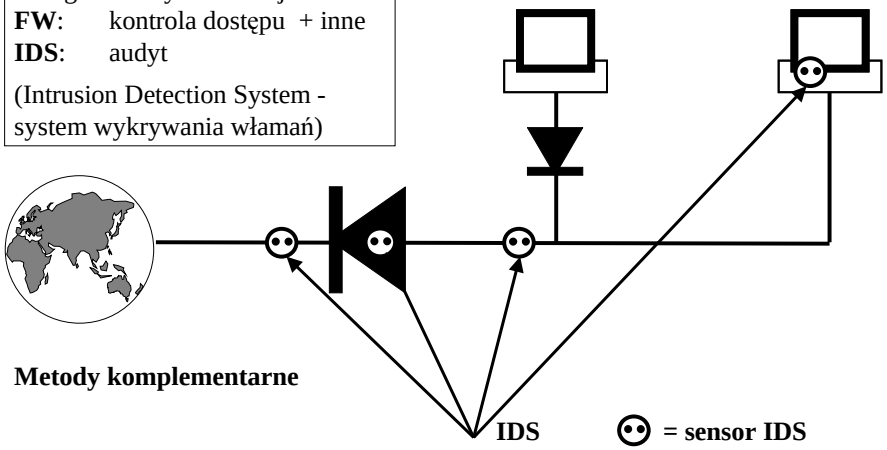
- Ewolucja zabezpieczeń:
  - **ewolucja systemów zabezpieczeń** (zastosowanie, klasyfikacja, działanie, wady i zalety)
    - ściany przeciwogniowe
    - systemy wykrywania włamań
    - współpraca systemów
  - **ewolucja protokołów zabezpieczeń i rozszerzeń aplikacji** (zastosowanie, cechy)
    - warstwa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

Ewolucja systemów zabezpieczeń

Zastosowanie

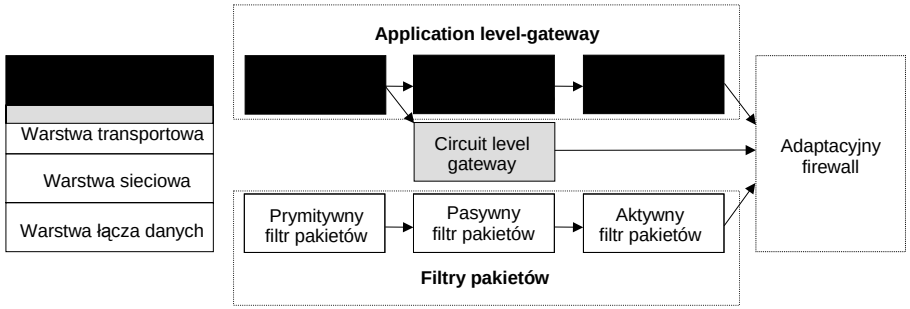
Usługi ochrony informacji:
FW: kontrola dostępu + inne
IDS: audyt

(Intrusion Detection System - system wykrywania włamań)



Ściany przeciwogniowe (firewalls)

Klasyfikacja. Działanie.



Ściany przeciwogniowe (firewalls)

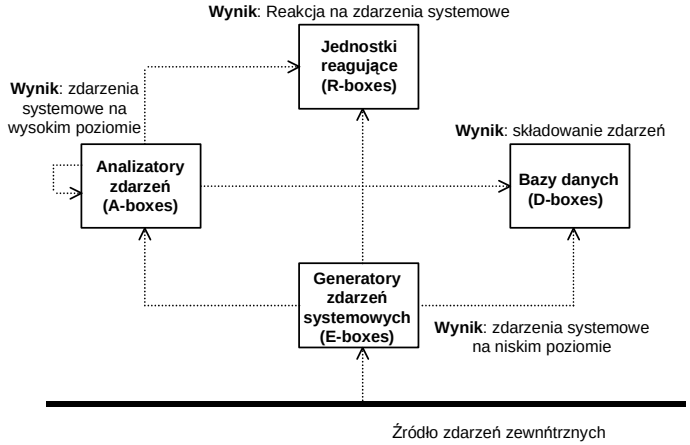
Zalety i wady

	Filtr pakietów	Application level gateway	Circuit level gateway	Adaptacyjny firewall
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 application level gateway	• 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 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)

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

Systemy wykrywania włamań (IDS)

Działanie IDS na bazie architektury Common Intrusion Detection Framework

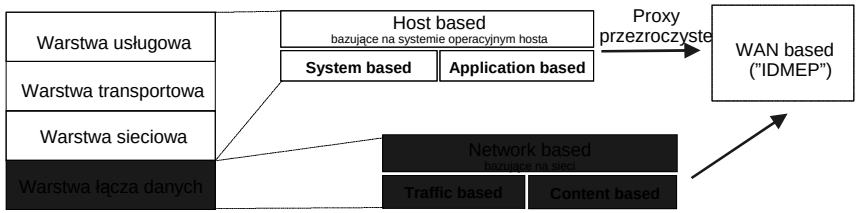


Systemy wykrywania włamań (IDS)

Klasyfikacja

Podział ze względu na umiejscowienie **E-box**:

Źródło zdarzeę 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)

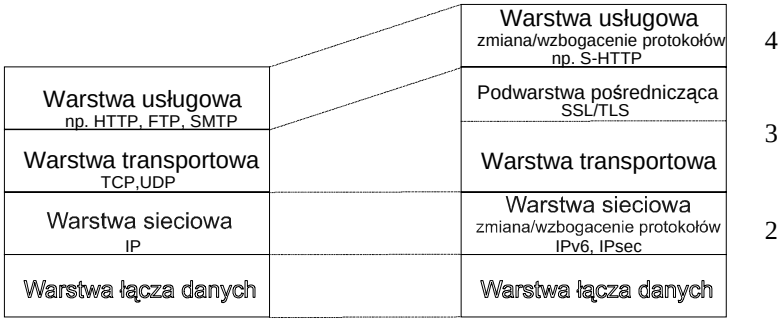
Zalety i wady

	IDS bazujący na systemie operacyjnym hosta	IDS bazujący na sieci		IDS wykrywający anomalie	IDS wykrywający nadużycia
zalety	• 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
		Traffic based	**Content based**		
		• generuje małą ilość logów • nie ingeruje w prywatność sesji	• wykrywa więcej ataków niż traffic based (analizuje zawartość)		
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 typu odmowa usługi, modyfikacja • strata pakietów przy większym obciążeniu sieci		• potencjalnie duża ilość fałszywych ataków - trudny dobór odpowiednich parametrów pracy • możliwość "szkolenia" systemu przez atakującego	• może wykrywać **tylko** znane ataki

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



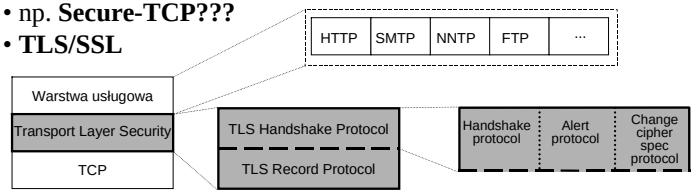
Ewolucja w poszczególnych warstwach

2

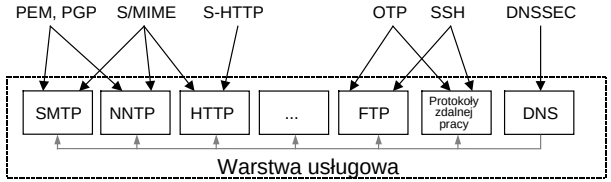
- **IPv6/IPsec** - Authentication Header, Encapsulating Security Payload, Internet Key Exchange

3

- np. **Secure-TCP???**
- **TLS/SSL**



4



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:**
  - ujednolicenie 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