Politechnika Warszawska
Wydział Elektroniki i Technik Informacyjnych
Instytut Telekomunikacji

Zagadnienia bezpieczeństwa w Internecie

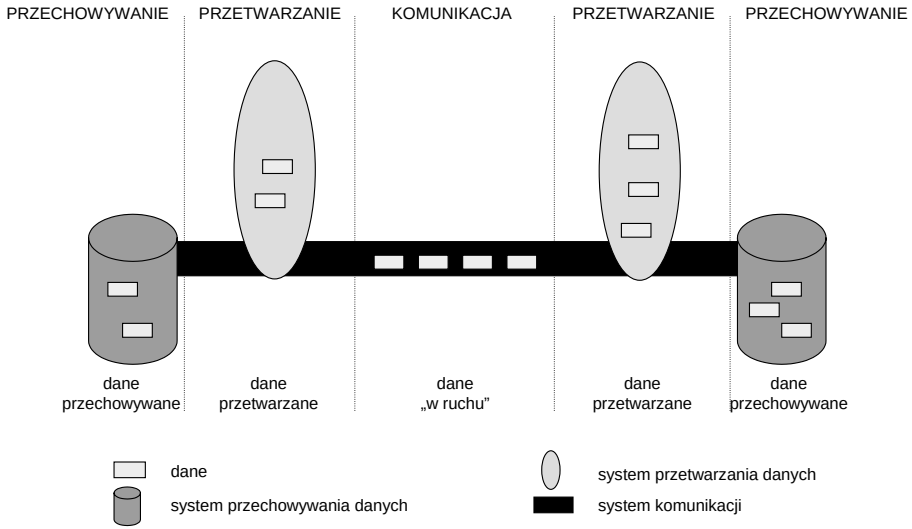
Piotr Kijewski, Krzysztof Szczypiorski
e-mail:{P.Kijewski, K.Szczypiorski}@tele.pw.edu.pl

Konferencja FORUM 2001
„Bezpieczne komunikowanie się w gospodarce cyfrowej”
Warszawa 18 maja 2001

Plan prezentacji

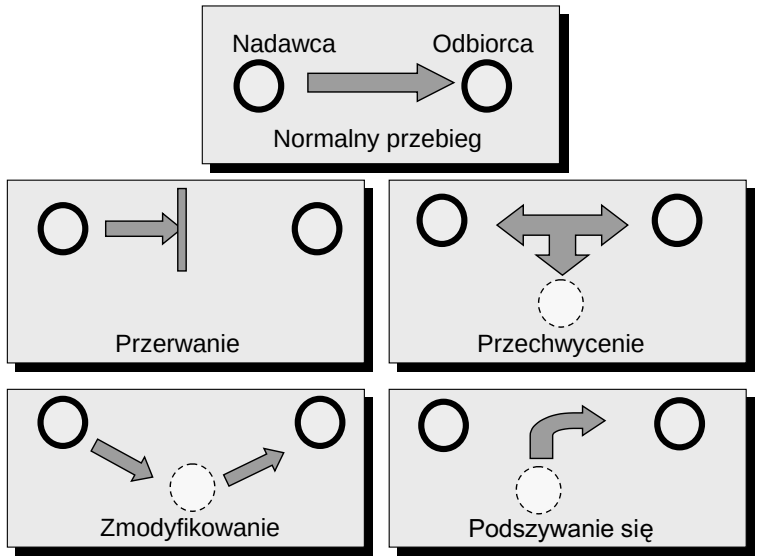
- Ataki na sieci TCP/IP
- Ewolucja zabezpieczeń:
  - **ewolucja systemów zabezpieczeń**
  - **ewolucja protokołów zabezpieczeń i rozszerzeń aplikacji**
- Podsumowanie: inne trendy

Zależności funkcjonalne pomiędzy elementami sieci



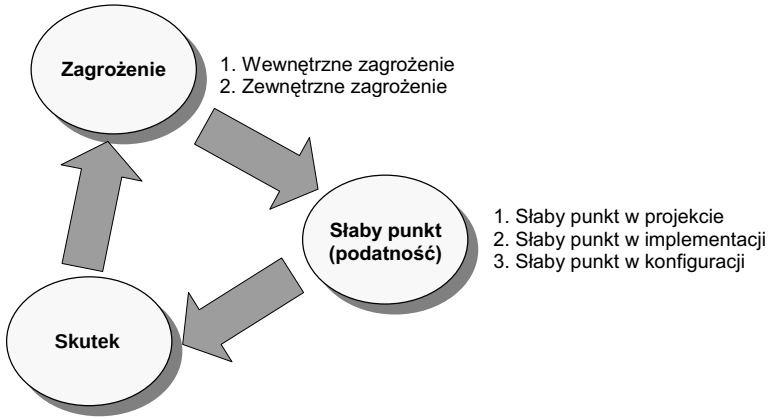
Klasyfikacja ataków

według zachodzącego procesu



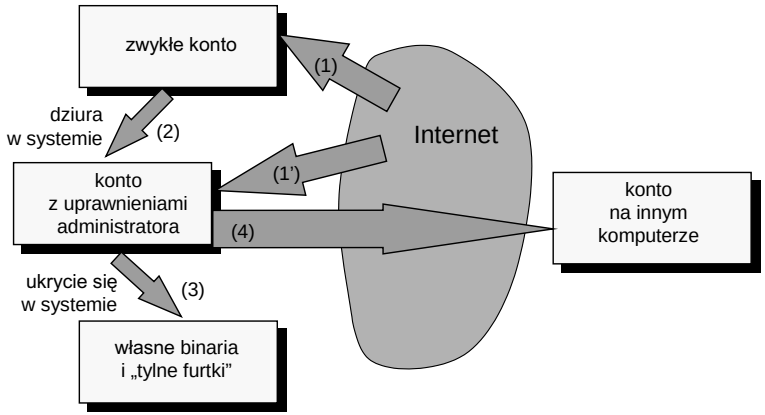
Klasyfikacja ataków

oparta na cyklicznej relacji pomiędzy zagrożeniem, słabym punktem oraz skutkiem



Schemat działań hackera

„Skakanie z wyspy na wyspę”

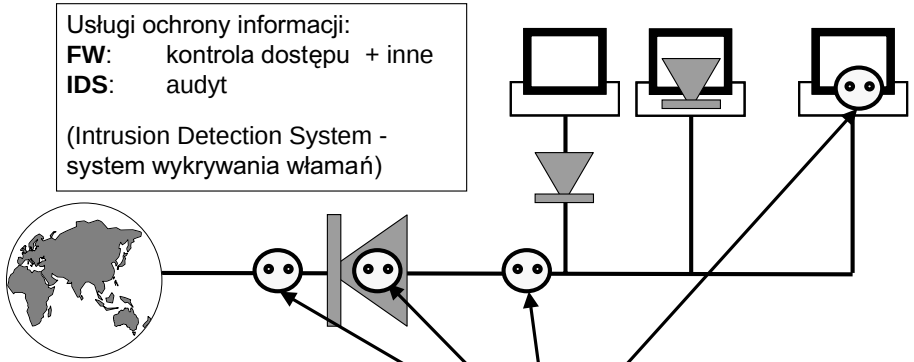


Ewolucja systemów zabezpieczeń

Zastosowanie

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

(Intrusion Detection System - system wykrywania włamań)

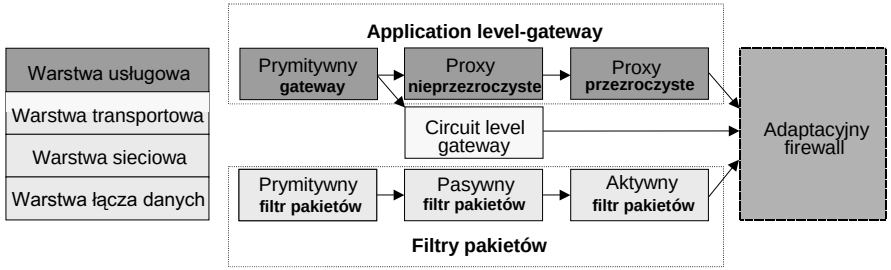


Metody komplementarne

IDS **= sensor IDS**

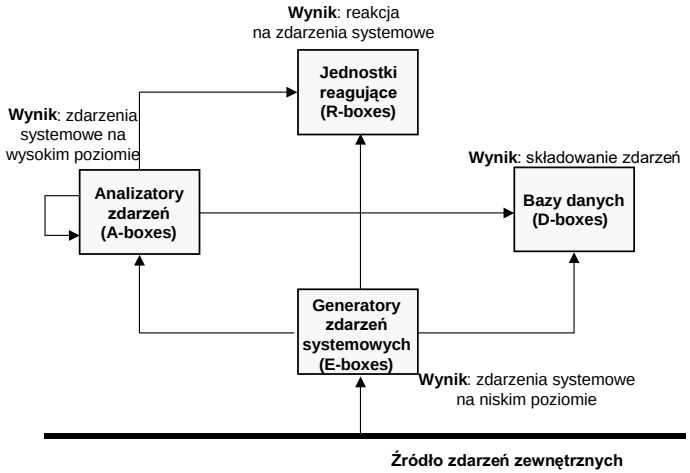
Ściany przeciwogniowe (firewalls)

Klasyfikacja. Działanie.



Systemy wykrywania włamań (IDS)

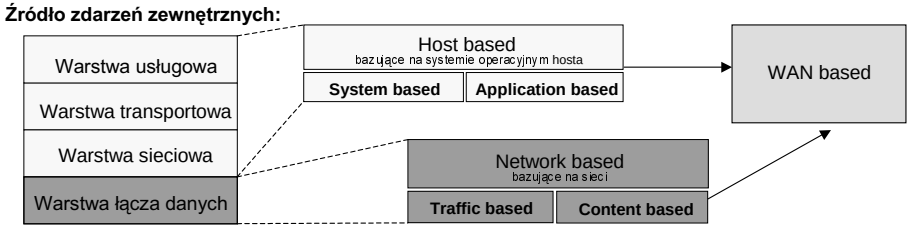
Działanie IDS na bazie architektury Common Intrusion Detection Framework



Systemy wykrywania włamań (IDS)

Klasyfikacja

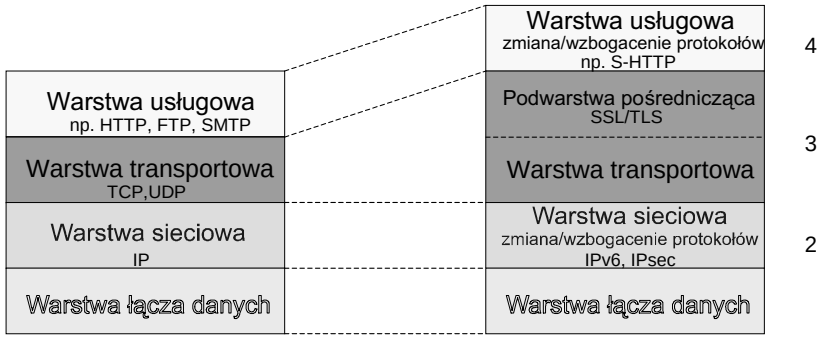
Podział ze względu na umiejscowienie **E-box**:



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)

Ewolucja protokołów zabezpieczeń

Ewolucja poszczególnych warstw modelu sieci TCP/IP



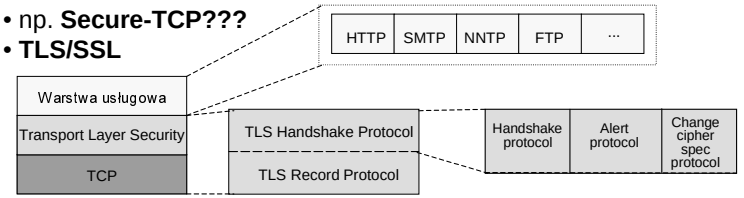
Ewolucja w poszczególnych warstwach

2

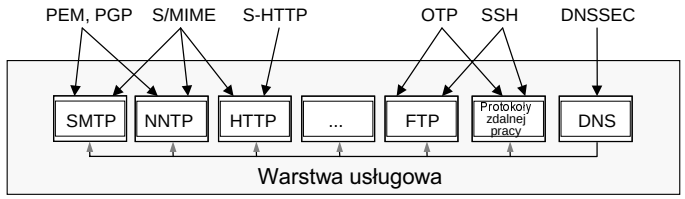
- **IPv6/IPsec** - Authentication Header, Encapsulating Security Payload, Internet Key Exchange

3

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



4



Podsumowanie

- **zabezpieczenia podążają dwiema drogami:**
  - **specjalistyczne systemy ochrony informacji**
    - status ścian przeciwogniowych wydaje się być stabilny
      - ewentualnie migracja w stronę rozproszonych ścian przeciwogniowych
    - 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:**
  - upowszechnienie systemów certyfikacji klucza publicznego
  - nowa generacja protokołów zarządzania
  - rozwój komunikacji grupowej

KONIEC

Pytania?