Politechnika Warszawska
Instytut Telekomunikacji

IT.FORUM SECURE 2001

Systemy wykrywania włamań w praktyce

Piotr Kijewski, Krzysztof Szczypiorski
E-mail: {P.Kijewski, K.Szczypiorski}@tele.pw.edu.pl
Secure 2001 – Warszawa, 7-8 listopada 2001

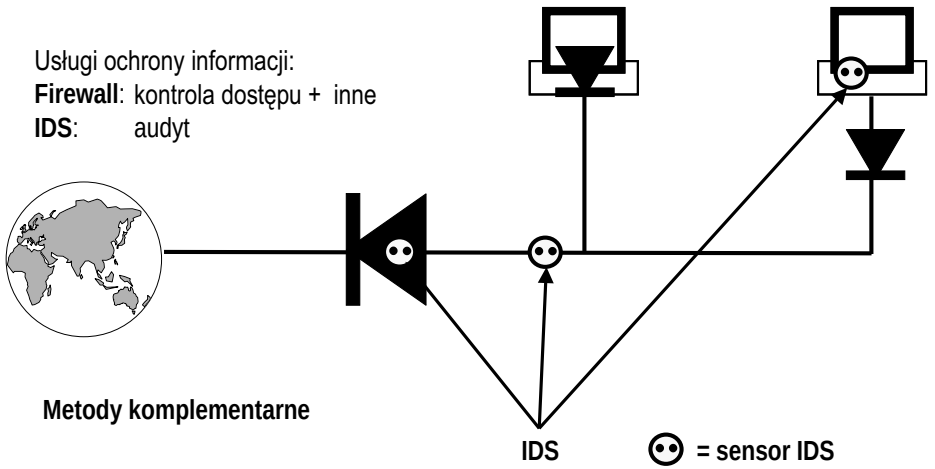
Główne cele prezentacji

- Przedstawienie ograniczeń występujących w rzeczywistych systemach wykrywania włamań
- Uświadomienie użytkownikom tych systemów, że automatyczne (bezmyślne) stosowanie tego typu zabezpieczeń nie ma żadnego sensu
- Wskazanie potencjalnych kierunków rozwoju systemów wykrywania włamań

Plan prezentacji

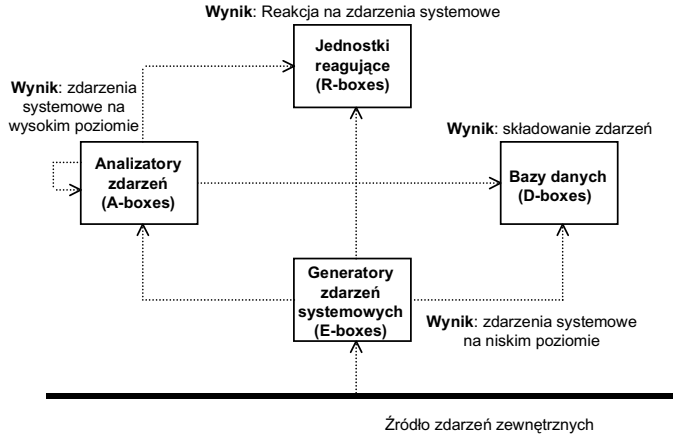
- Rola ***systemów wykrywania włamań*** (=***systemów IDS – Intrusion Detection System***)
- Działanie idealnego systemu IDS
- Cztery fundamentalne pytania związane z działaniem systemów IDS
- W podsumowaniu: najważniejsze wnioski dla twórców/administratorów

Umiejscowienie systemu IDS w sieci



Jak działa idealny system IDS?

Common Intrusion Detection Framework



Cztery fundamentalne pytania,

na które odpowiemy przez pryzmat działania systemu idealnego

Pyt. 1. Co to jest zdarzenie wyglądające na włamanie?

Pyt. 2. Jak rozpoznać zdarzenie wyglądające na włamanie?

Pyt. 3. O czym powinien informować system IDS?

Pyt. 4. Jak należy reagować na te informacje?

Pyt. 1. Co to jest zdarzenie wyglądające na włamanie?

- **Zdarzenie wyglądające na włamanie** może być **nadużyciem** lub **anomalią**
- **Nadużycie** – zachowanie rozpoznane jako znany, skatalogowany atak na system teleinformatyczny
- **Anomalia** - wszelkie zachowania niezgodne z przyjętymi zasadami np.:
  - większe wykorzystanie mocy obliczeniowej
  - użycie przez użytkownika niestandardowej sekwencji komend
  - wykorzystanie przez aplikację nietypowego dla niej wywołania systemowego lub ich sekwencji)

Pyt. 2. Jak rozpoznać zdarzenie wyglądające na włamanie?

- **Wykrywanie nadużyć -** posiadanie wiedzy w postaci bazy danych o typowych atakach, typowych sekwencjach pojawiających się w okolicznościach ataku, **ale**
  - źródło ataku może być rozproszone (różne adresy)
  - atak może być rozciągnięty w czasie
  - niespójność semantyczna
  - nieznajomość semantyki (np. wpływ szyfrowania)

Pyt. 2. Jak rozpoznać zdarzenie wyglądające na włamanie?

- **Wykrywanie anomalii -** brak jednoznacznego modelu zachowania systemu teleinformatycznego
- Zdefiniowanie anomalii wymaga określenia:
  - **parametrów oraz progów**, które odróżniają zachowanie typowe od uznawanego za anomalię
- Np. prymitywny system wykrywania włamań:
  - parametr: ilość nieudanych prób zalogowania się do systemu w ciągu określonego czasu
  - próg: 3 próby w ciągu godziny
  - wykrycie 3 nieudanych logowań w ciągu 1 minuty – anomalia - jak interpretować tę anomalię?

Pyt. 3. O czym powinien informować system IDS?

- Czy system IDS powinien informować **o wszystkich** zdarzeniach, które są uznane za anomalię lub nadużycie?
- **Fałszywe alarmy** – paradoks:
  - częstotliwość: 1/1.000.000 – wierność testu: 99,99% - wiarygodność wyniku potwierdzającego ~1%
  - przy większej częstotliwości 1/1.000 – wiarygodność tylko ~91%

Pyt. 3. O czym system IDS powinien informować?

- Wnioski dla twórców/administratorów systemów IDS nie są jednoznaczne:
  - zestaw reguł **wykrywających nadużycia** powinien być bardzo precyzyjny, ale przesadna dokładność może doprowadzić do tego, że działania pozostaną nie wykryte
  - brak ogólnych wyznaczników do **wykrywania anomalii** - różne cechy modeli zachowania systemu teleinformatycznego – różne parametry, progi i zależności między nimi

Pyt. 4. Jak należy reagować na informacje o włamaniu?

- bajka Ezopa o pastuchu, wilkach i owcach
- skutki fałszywych alarmów
- utopia systemu automatycznego
- kluczowa rola wykształconego personelu obsługującego system IDS
- działania wspomagające

Wnioski

- Systemy IDS w obecnej formie są ułomne - praktyczne zastosowanie ich jako narzędzi samodzielnych jest wątpliwe
- Kłopotliwe wykrywanie/definiowanie anomalii
- Niejednoznaczność semantyczna
- Pułapka fałszywych alarmów
- Automatyzacja a czynnik ludzki
- Czy warto stosować IDS czy nie?

Pytania?

Piotr Kijewski, Krzysztof Szczypiorski

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