

Advanced Security Option oraz inne metody szyfrowania w Oracle 9i

1

Prezentujący: Marcin Przepiórowski

- **Omównienie Advanced Security Option**
 - **Szyfrowanie**
 - **Zewnętrzne metody autentyfikacji**
- **Szyfrowanie za pomocą narzędzi OpenSource:**
 - **Stunnel**
 - **SSH**

Zagrożenia w sieci:

- **Kradzież danych**
- **Modyfikacja transakcji**
- **Fałszowanie tożsamości**
- **Nadmierna ilość haseł**

Szyfrowanie ruchu i kontrola spójności

- **Algorytmy szyfrowania**
 - **DES**
 - **3DES**
 - **RSA RC4**
- **Kontrola spójności**
 - **MD5**
 - **SHA-1**

Szyfrowanie ruchu i kontrola spójności

- **Wybór klucza**
 - Każda sesja negocjuje swój klucz
 - Zastosowanie algorytmu *Diffie-Hellman-a*
- **Negocjowanie algorytmów**
 - Różne możliwości stosowania algorytmów szyfrowania
 - Wybór algorytmów z listy dostępnych

Zastosowanie SSL-a w Oracle 9i

- **SSL – sposób działania**
- **Certyfikaty – Centrum Autoryzacji, podpisywanie żądań certyfikatów**
- **Oracle Wallet Manager – przechowywanie kluczy prywatnych i certyfikatów**

Autentifikacja zewnętrzna

- **Kerberos**
- **Radius**
- **CyberSafe**
- **DCE**

Szyfrowanie za pomocą innych narzędzi

- **Szyfrowanie za pomocą STUNNEL**
 - Konfiguracja po stronie klienta i serwera
 - Możliwości kontroli połączeń
- **Szyfrowanie za pomocą SSH**
 - konfiguracja