Monitorowanie dostępu do baz danych

Marcin Tunia

Plan prezentacji

- Obszary zastosowania baz danych
- Dlaczego chronimy bazy danych?
- Metody ochrony BD
- Kontrola dostępu
- Usługa niezaprzeczalności
  - Założenia
  - Zastosowania
  - Propozycja rozwiązania
- Podsumowanie
- Dyskusja

Gdzie stosujemy bazy danych?

onet.pl INTERIA.PL WP.PL YAHOO!

facebook

grono.net

PGE

merlin.pl

FBI

Dlaczego chronimy bazy danych?

- Zawierają informacje poufne

- Ochrona przed modyfikacją
- Ustawa o ochronie danych osobowych
  - (Dz.U. 1997 Nr 133 poz. 883 *USTAWA* z dnia 29 sierpnia 1997 r.)
- Tajemnica firmowa

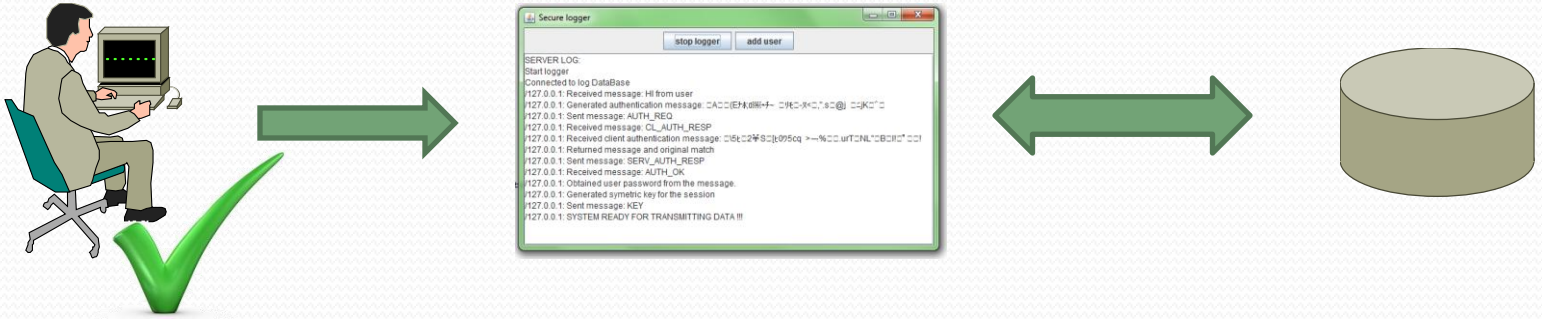
Przykład:

- Rejestracja pacjentów online

- Zyski zagrożone przez:
  - Czasowy brak dostępności
  - Utratę poufności
  - Nieuprawniona modyfikacja
- Podobna analiza dla:
  - Dane finansowe
  - Przewaga konkurencyjna firmy
  - Jedno hasło do różnych systemów

Dlaczego kontrolujemy dostęp do BD?

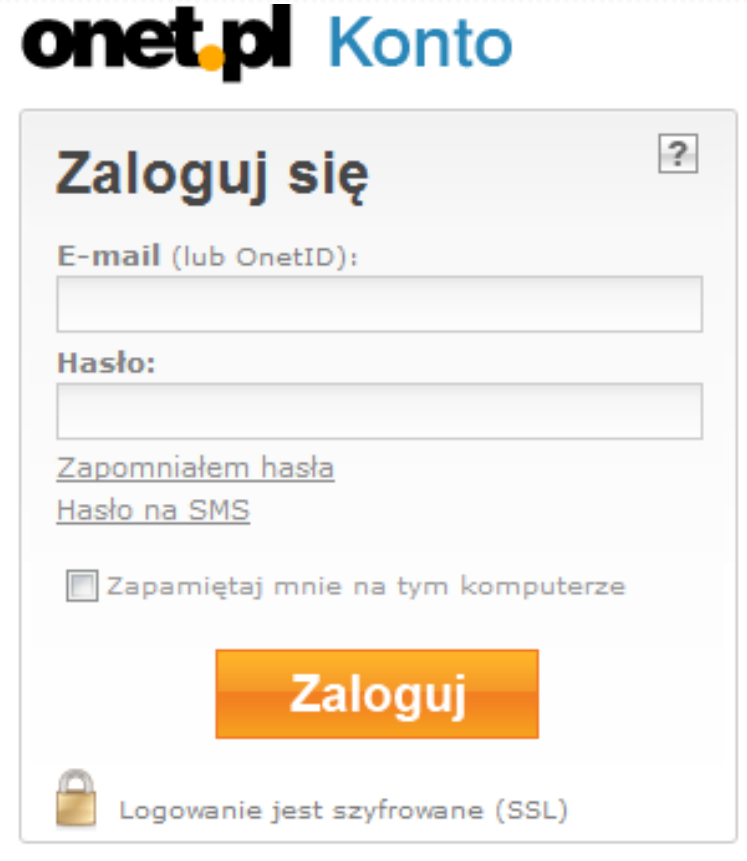
- Zmanipulowana aplikacja:

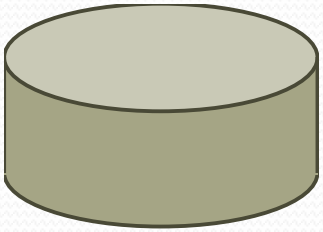


- Nieuprawniony dostęp
- Nadużycia w dostępie

SQL Injection

Złośliwy kod





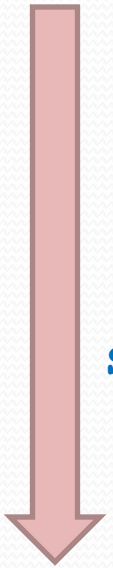
Zapytanie do bazy

SQL Injection

```
$q = mysql_query("SELECT * FROM users WHERE user = '$user'");
```

```
$user = Marcin
```

```
SELECT * FROM users WHERE user = 'Marcin'
```



```
$user = x';DROP TABLE users;
 SELECT * FROM data WHERE name LIKE '%
```

```
SELECT * FROM users WHERE user = 'x';
DROP TABLE users; SELECT * FROM data WHERE name LIKE '%'
```

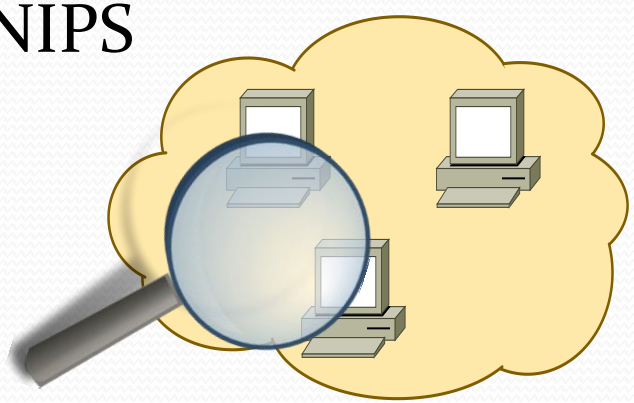
Zapytania parametryzowane

- Zmienne nie są używane bezpośrednio
- Dołączanie zmiennych w czasie wykonania
  - W ramach API
  - Przez obsługę w aplikacji (cytowanie)

```
$query = $sql -> prepare("select * from users where name = ?");
 $query -> execute($user_name);
```

Mechanizmy bezpieczeństwa

- Systemy NIPS



- Systemy HIPS

- Skanery podatności
- Szyfrowanie baz danych
- Uprawnienia użytkowników

NIPS vs. HIPS

Network-based IPS

- Własne zasoby sprzętowe
- Single point of failure
- Perspektywa sieciowa
- Wykrywa ataki sieciowe
- Analiza/wykrywanie/ raportowanie
- Odrzucanie złośliwego ruchu

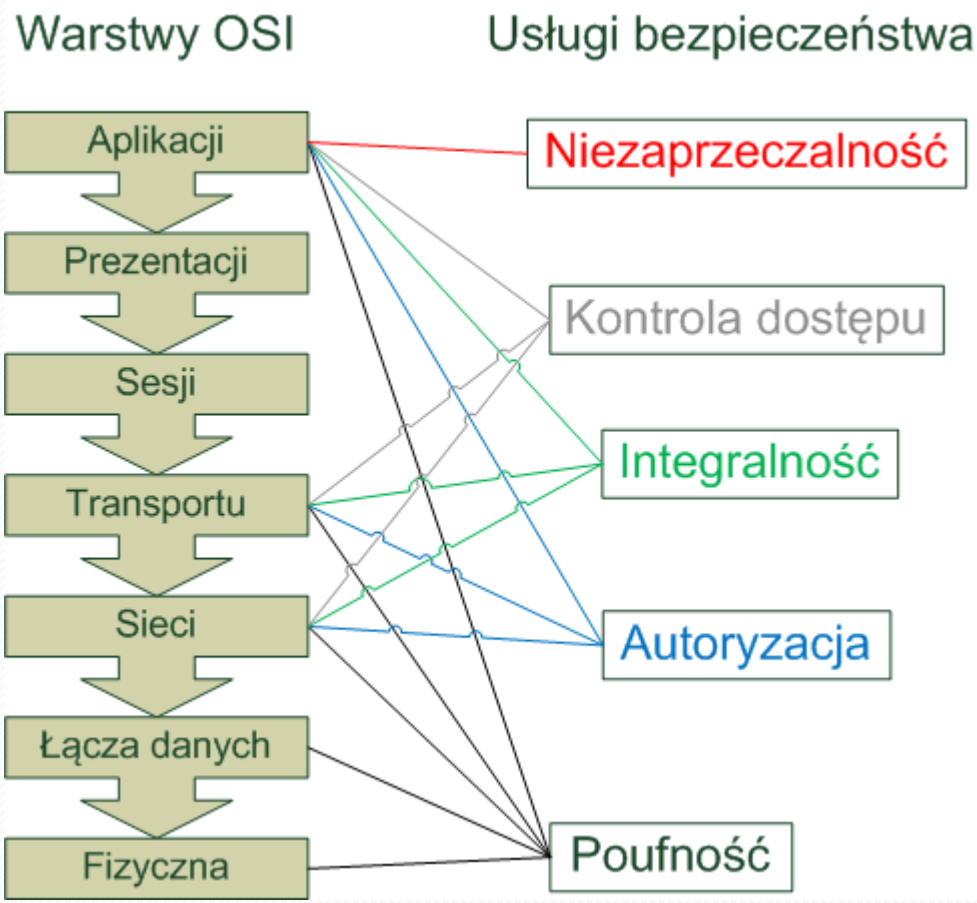
Host-based IPS

- Dane szyfrowane i nieszyfrowane
- Perspektywa hosta
- Współdzielone zasoby z hostem
- Nie wymaga ciągłych aktualizacji

Kontrola dostępu i monitorowanie

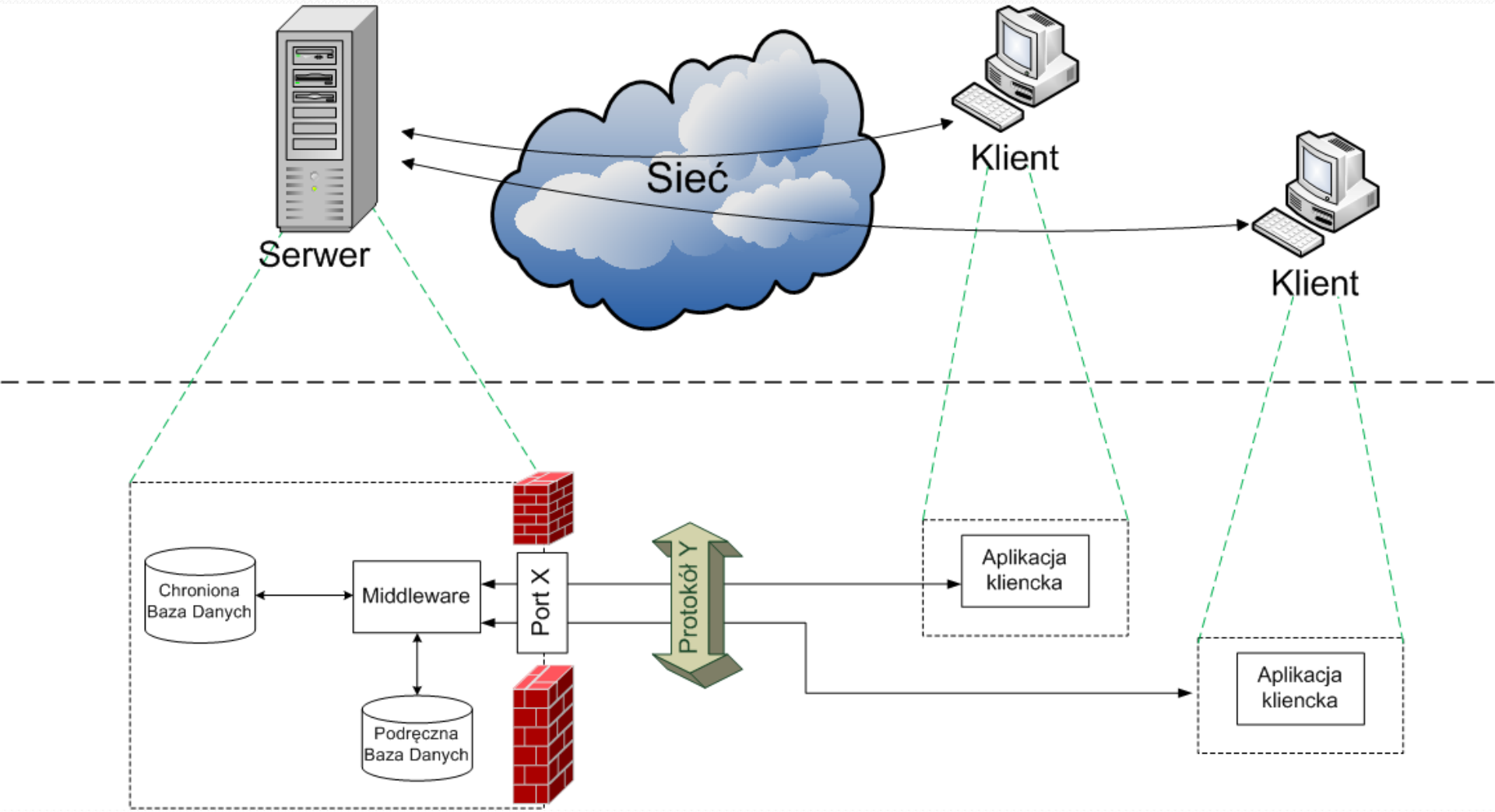
- Zasada „least priviledges”
- Wykrywanie odstępstw
- Pogorszenie wydajności?
- Logowanie dostępu do BD
  - Próby uwierzytelnienia (udane i nieudane)
  - Operacje SQL na bazie danych
  - Bezpieczne składowanie wyników
  - Backup
  - Księgowanie lokalne/zdalne

Usługa niezaprzeczalności

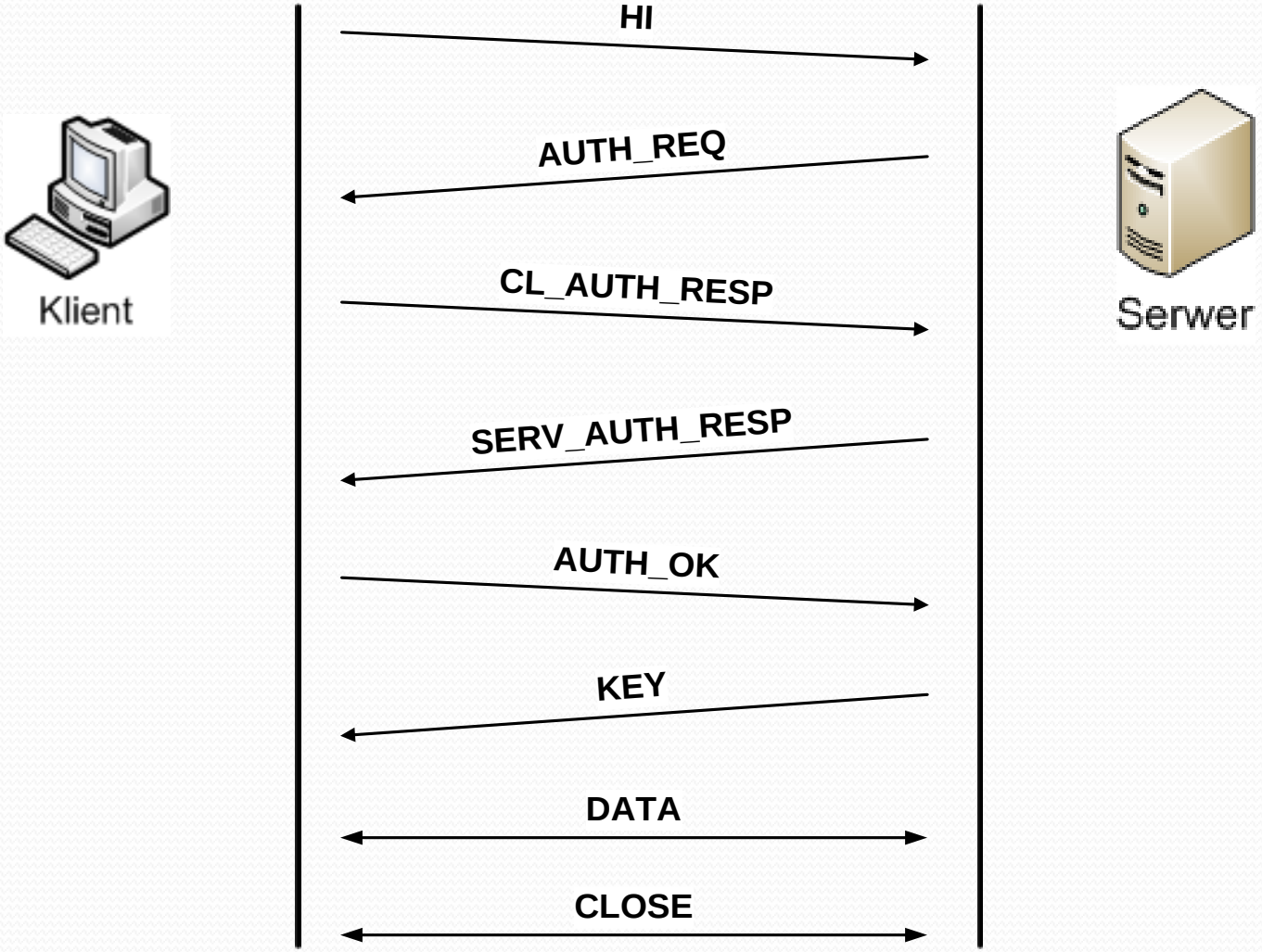


- ✓ **Zapis przebiegu sesji z bazą danych**
- ✓ **Zastosowanie warstwy pośredniczącej**
- ✓ **Przezroczystość**
- ✓ **Skalowalność**
- ✓ **Bezpieczeństwo transmisji**
- ✓ **Bezpieczeństwo baz danych**

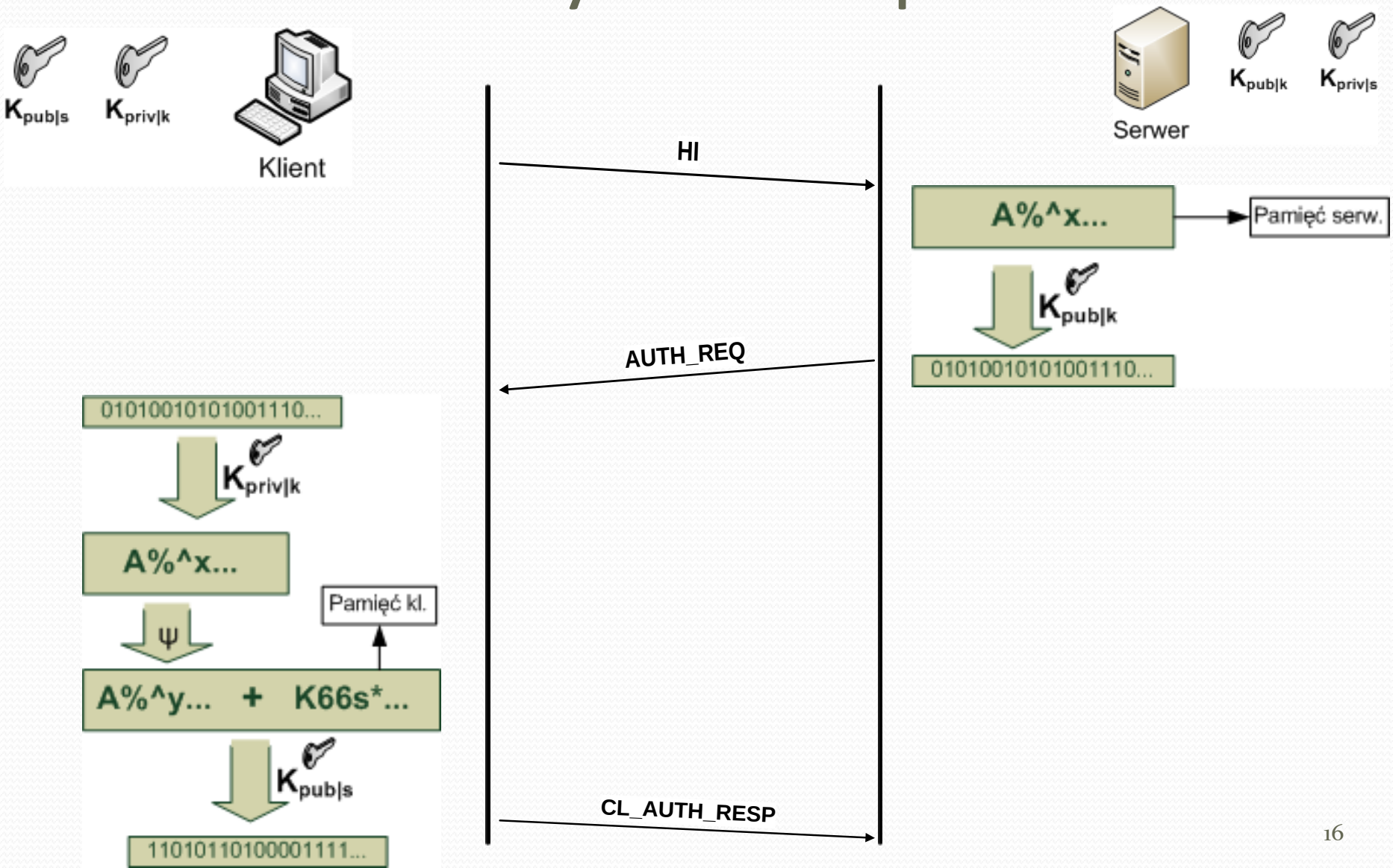
Ogólna architektura rozwiązania



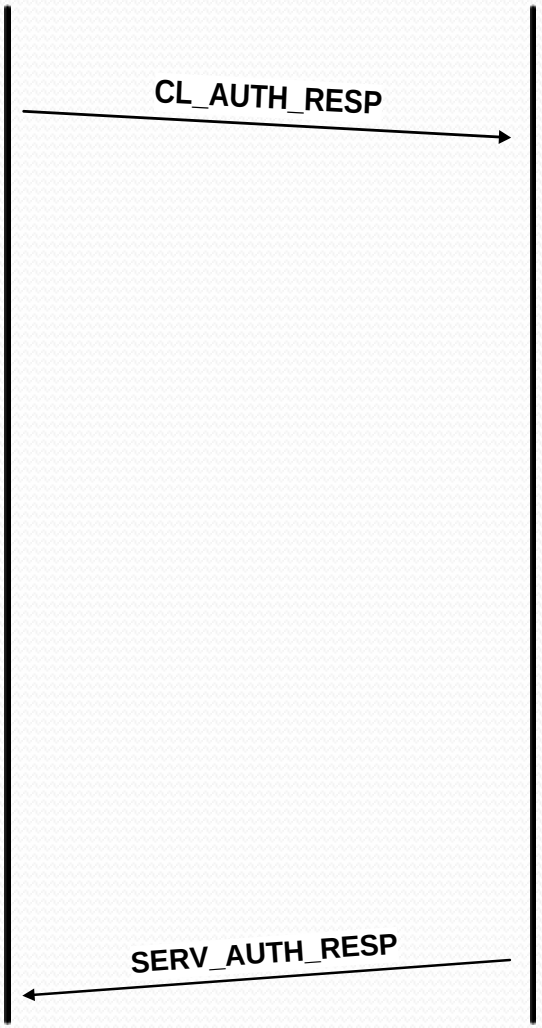
Architektura systemu - protokół

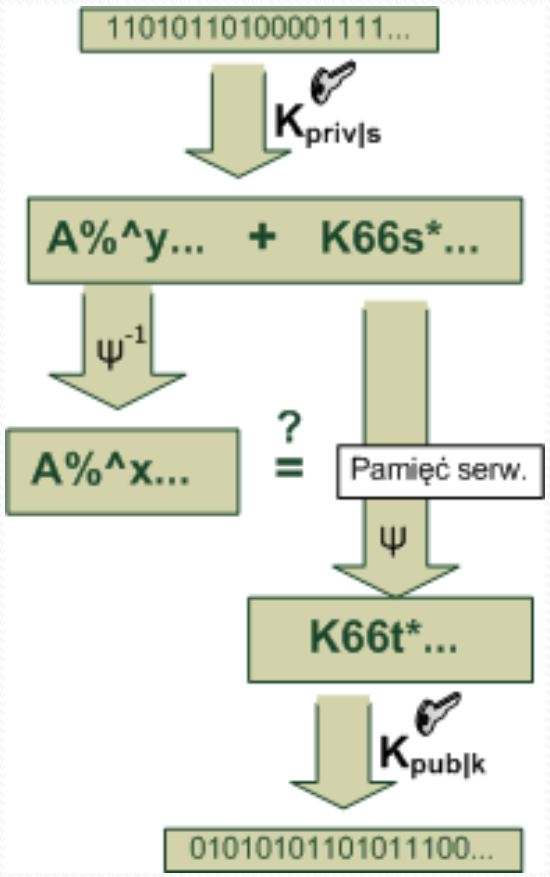


Architektura systemu - protokół

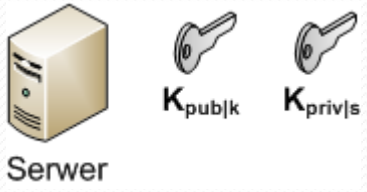


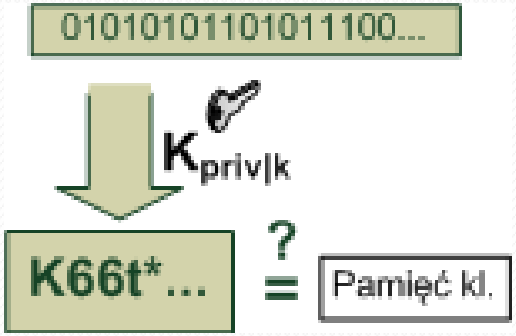
Architektura systemu – protokół…

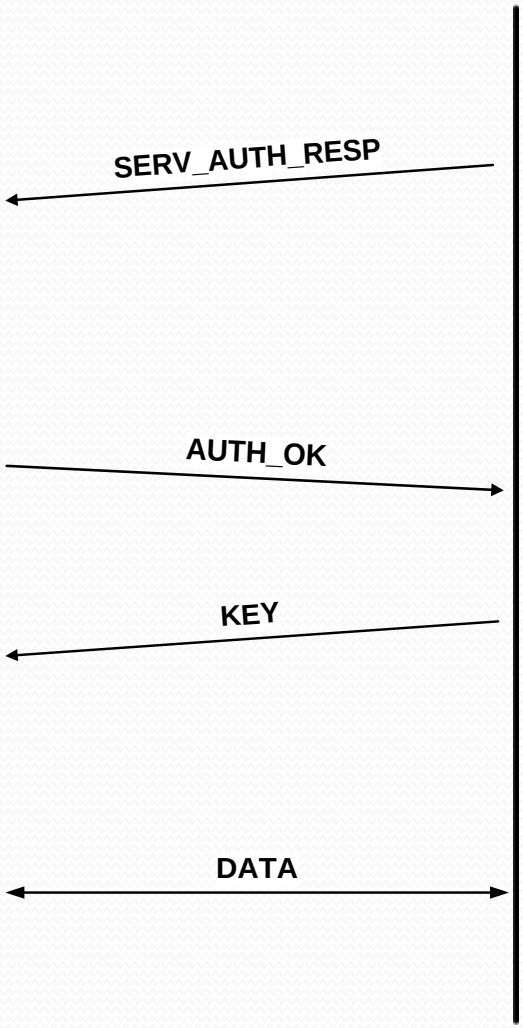




Architektura systemu – protokół…





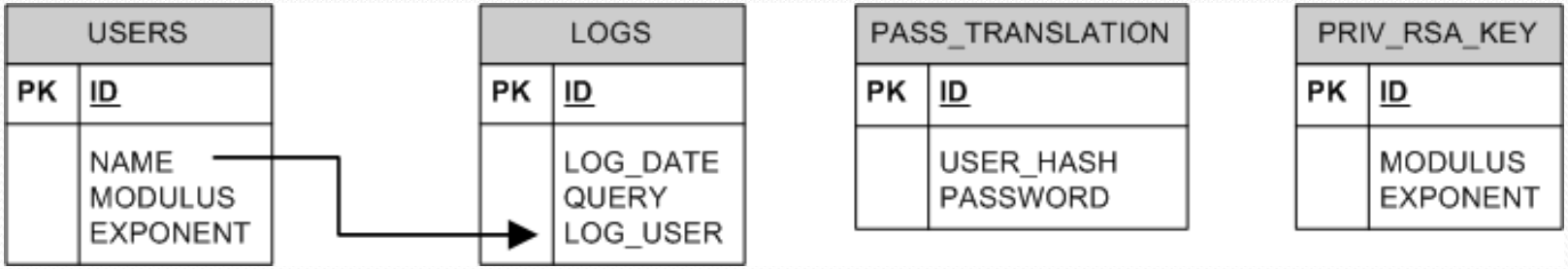


Losowy klucz symetryczny

10101010101011101...

10101010101011101...

Architektura systemu – baza danych



LOGS

EDIT	ID	LOG_DATE	QUERY	LOG_USER
	1	2010-03-14 14:09:59:563 CET	test_action	user
	2	2010-03-14 14:13:05:975 CET	akcja 1	user
	3	2010-03-14 14:19:14:872 CET	akcja 2	user

row(s) 1 - 3 of 3

USERS

EDIT	ID	NAME	MODULUS	EXPONENT
	1	user	168828087120614942304800925462707947084034247963	65537

row(s) 1 - 1 of 1

PRIV_RSA_KEY

EDIT	ID	MODULUS	EXPONENT
	1	27475458068073573641025327843	17067973332123990687732

PASS_TRANSLATION

EDIT	ID	USER_HASH	PASSWORD
	1	[B@7ced01	super_passwd
	2	[B@1feca64	hi5
	3	[B@1e9cb75	bardzo-dluuugie-haslo
	4	[B@1e9cb75	bbbbb
	5	[B@17f1ba3	blablablablablablabla
	6	[B@1ac1fe4	kabanosy
	21	^æ"[illegible]#¦÷w├¥ oł(([illegible]#y[illegible]	super_password

row(s) 1 - 7 of 7

Odporność na ataki

- *Atak powtórzeniowy* (stempel czasowy)
- *Sniffing* (szyfrowanie symetryczne i PKI)
- *Niekontrolowany dostęp do BD* (translacja haseł)
- *Odczyt nazwy użytkownika i hasła z podręcznej BD* (substytucja i hash)
- *Nieautoryzowany dostęp* (PKI i hasło)
- *Man in the middle* (PKI i szyfr symetryczny)
- *DoS* (maksymalna ilość nieudanych logowań)

Odniesienie do dobrych praktyk*

- Logowanie dostępu do BD
  - Próby uwierzytelnienia (udane i nieudane)
  - Operacje SQL na bazie danych
  - Bezpieczne składowanie wyników
  - Backup
  - Księgowanie lokalne/zdalne

* według www.securitum.pl – „Bezpieczeństwo baz danych – weryfikacja”

Odniesienie do dobrych praktyk*

- Szyfrowanie
  - Zabezpieczony proces uwierzytelniania
  - Szyfrowanie danych pomiędzy klientem i serwerem
  - Wymuszanie szyfrowania
  - Dane w bazie danych w formie zaszyfrowanej

* według www.securitum.pl – „Bezpieczeństwo baz danych – weryfikacja”

Odniesienie do dobrych praktyk*

- Warstwa aplikacji
  - Czy aplikacja korzysta z jednego użytkownika BD?
  - Zapytania parametryzowane

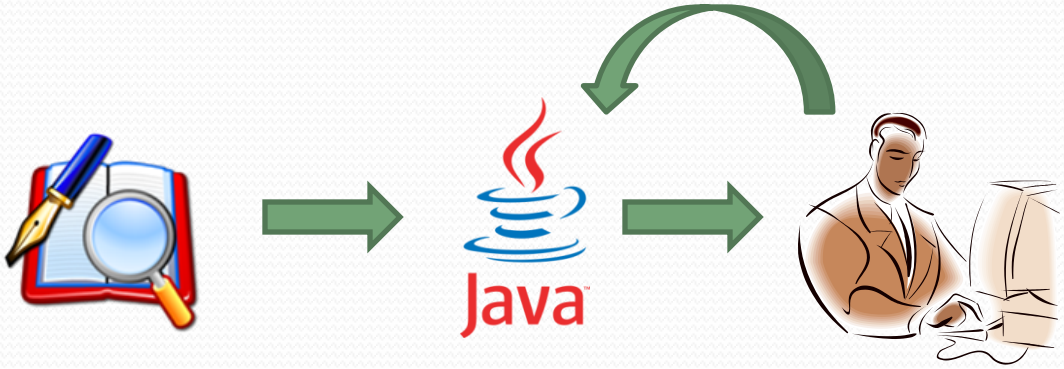
```
PreparedStatement prep = conn.prepareStatement("SELECT * FROM USERS WHERE USERNAME=? AND PASSWORD=?");
prep.setString(1, username);
prep.setString(2, password);
prep.executeQuery();
```

  - Czy po stronie klienta są przechowywane dane dostępowe do BD?

* według www.securitum.pl – „Bezpieczeństwo baz danych – weryfikacja”

Podsumowanie

- Aplikacja „oddzielona” od chronionej bazy danych
- Zapewnienie bezpieczeństwa end-to-end
- Implementacja w języku Java
- Podział na fazy:
  - Projektowanie
  - Implementacja
  - Testy



- Praktyczne zastosowanie w kontroli dostępu do danych

Dziękuję za uwagę

Zapraszam do dyskusji ;)