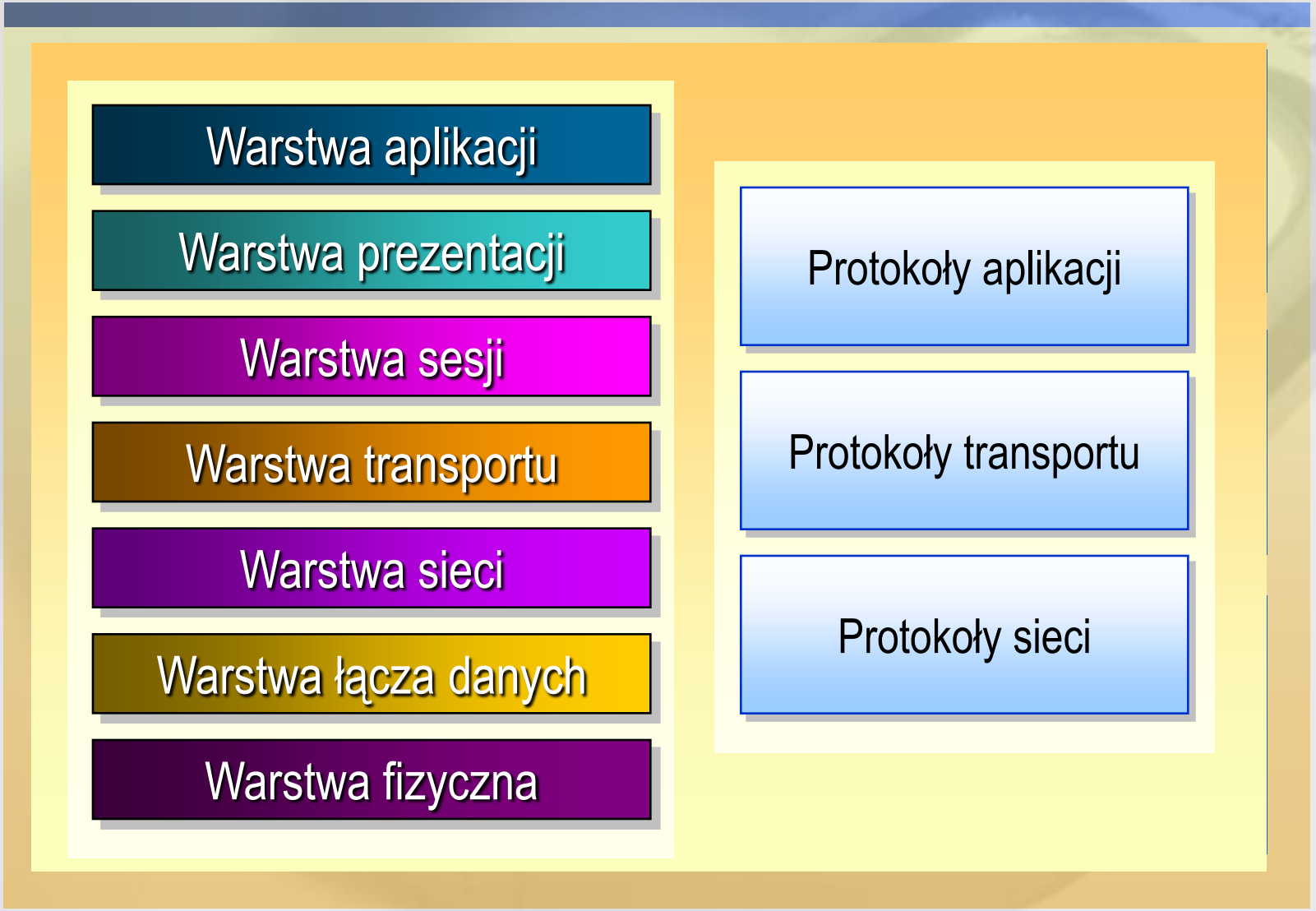
Sieć

Marcin Szeliga
marcin@wss.pl

Agenda

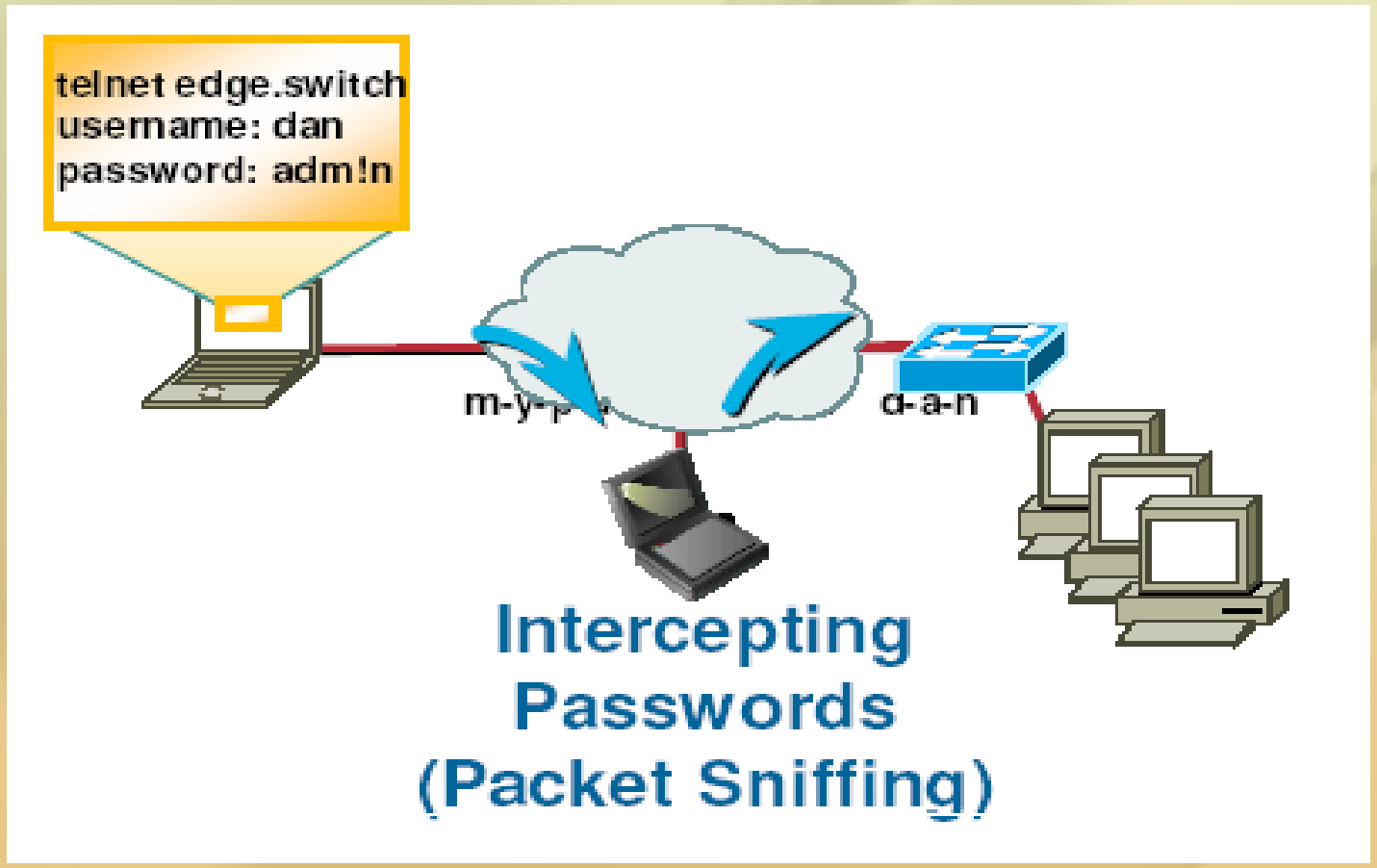
- **Wprowadzenie**
  - Model OSI
  - Zagrożenia
- **Kontrola dostępu**
  - Standard 802.1x (protokół EAP i usługa RADIUS)
- **Zabezpieczenia**
  - IPSec
  - SSL/TLS
  - SSH
  - Zapory
- **Sieci bezprzewodowe**

Wprowadzenie – Model OSI



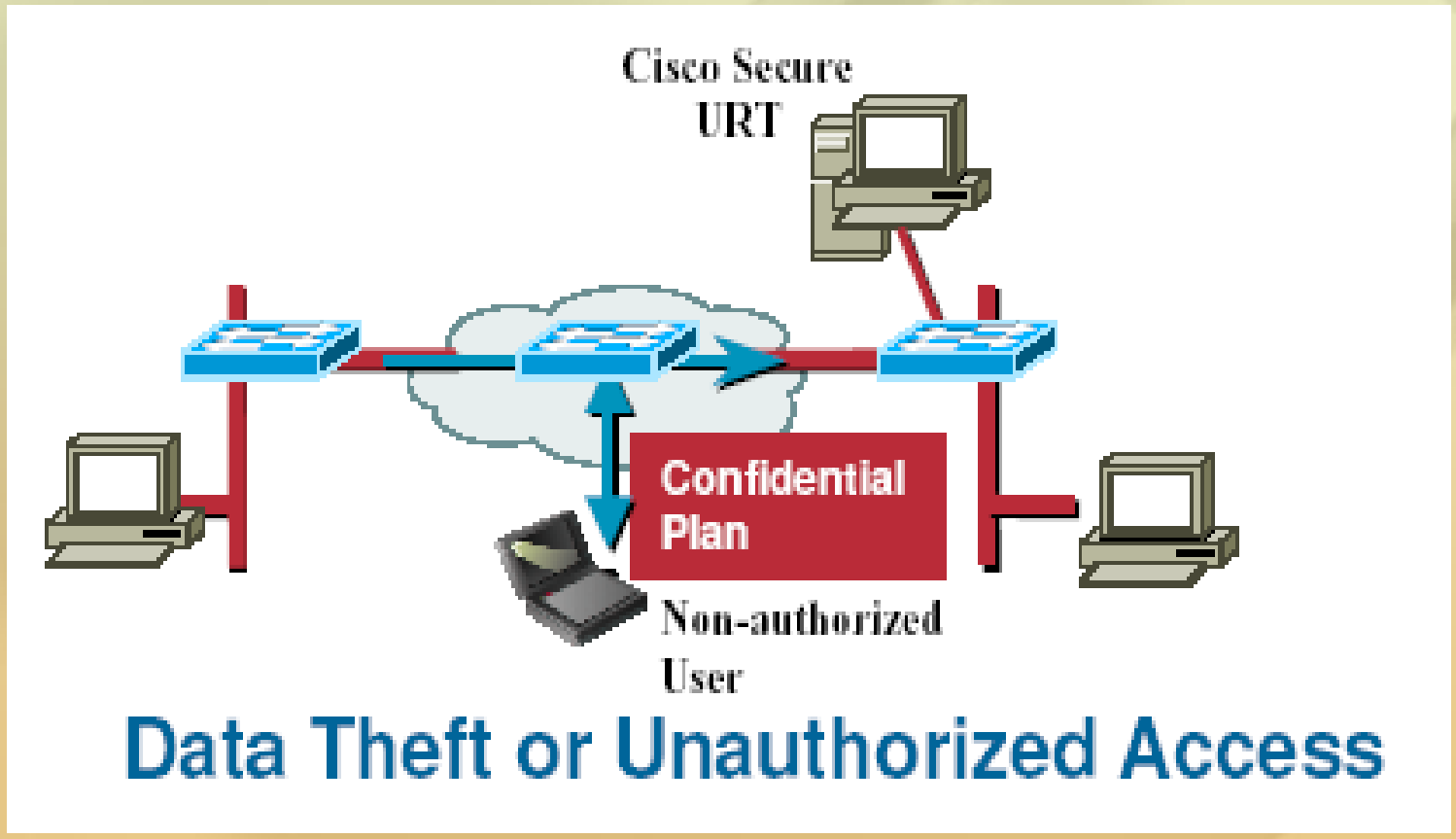
Wprowadzenie – Zagrożenia

- Podsłuchiwanie (Sniffing)



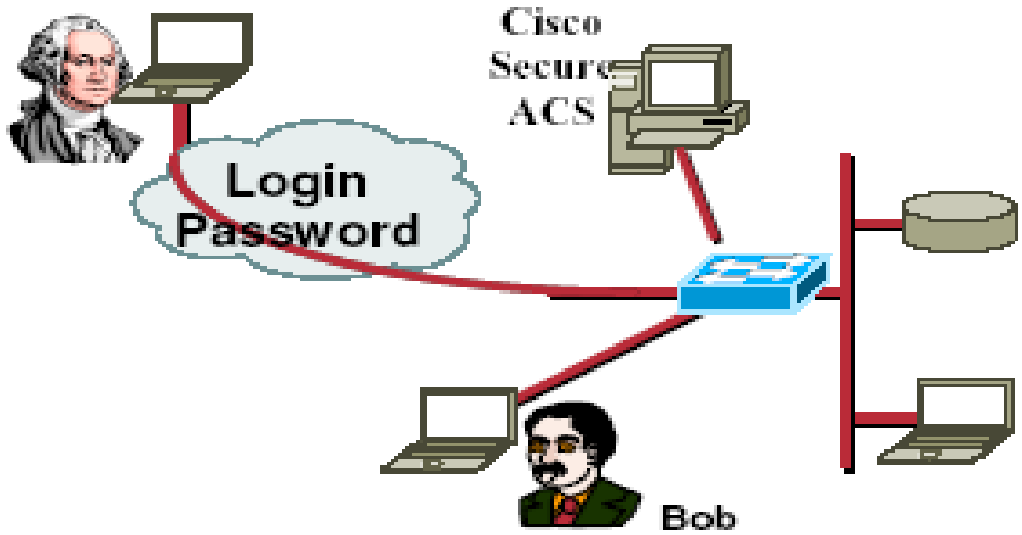
Wprowadzenie – Zagrożenia

- Kradzież danych



Wprowadzenie – Zagrożenia

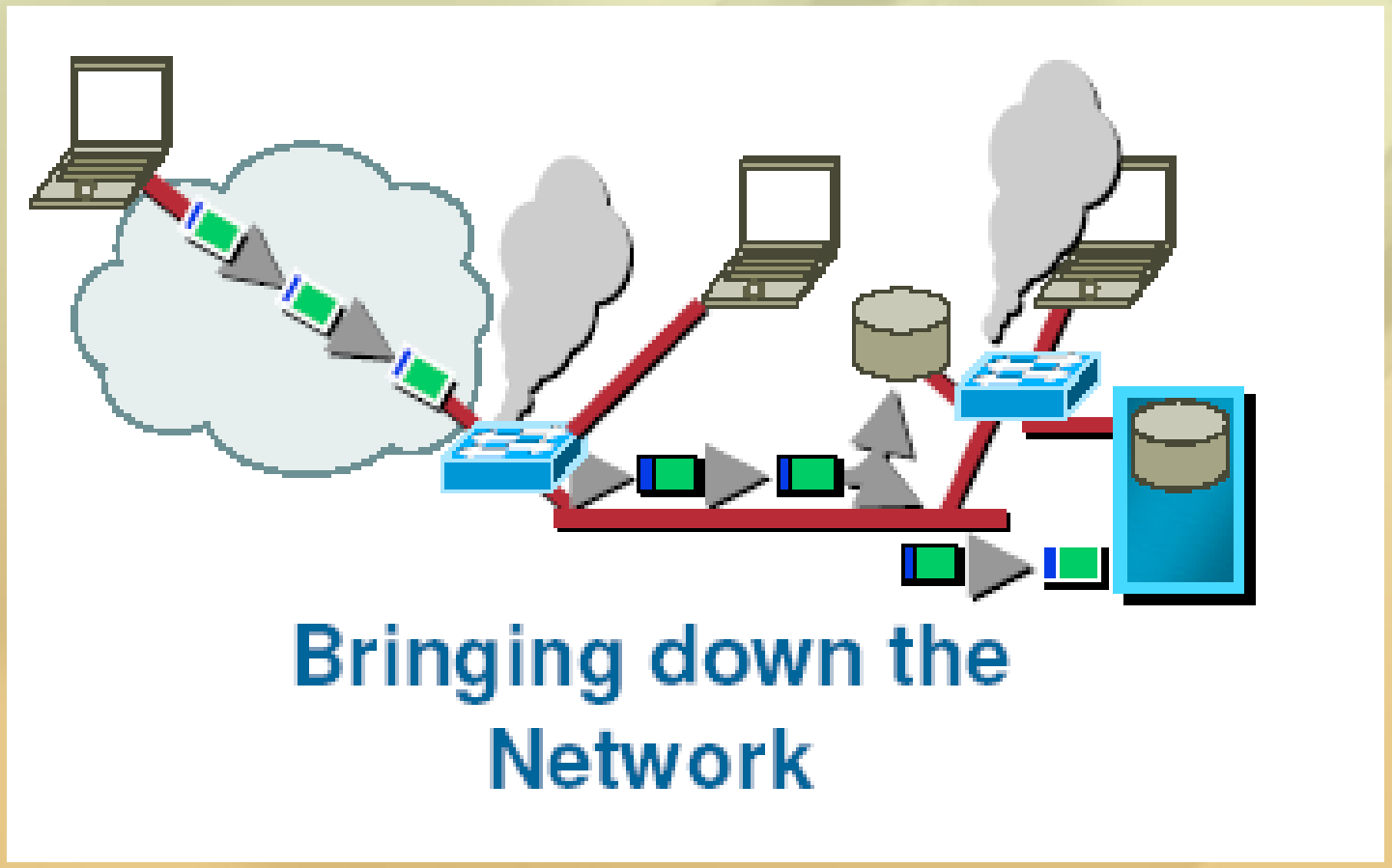
- Podszywanie się (kradzież tożsamości)



Impersonation
(Identity Spoofing)

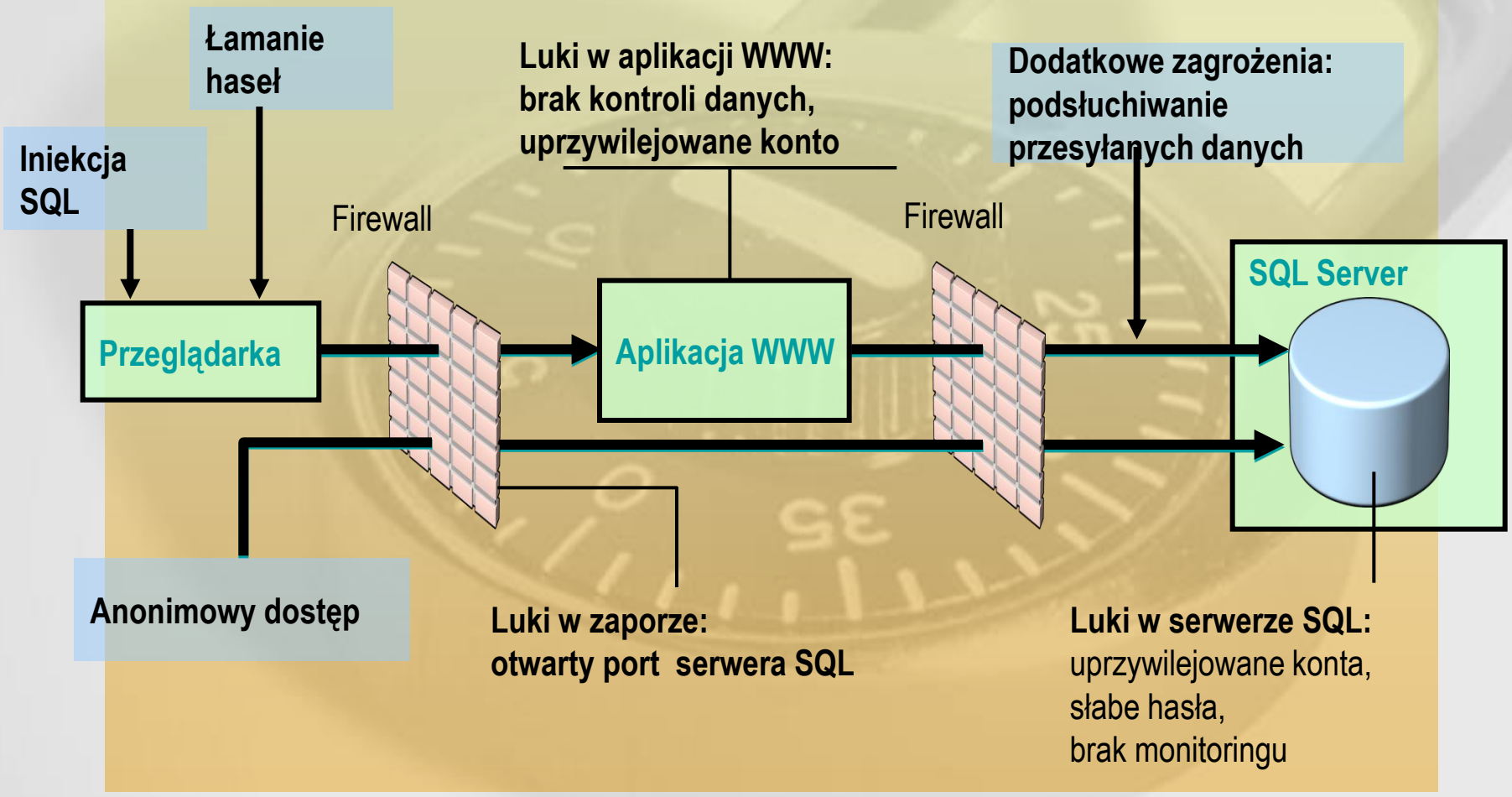
Wprowadzenie – Zagrożenia

- Atak DOS (odmowy obsługi)



Wprowadzenie – Zagrożenia

- Atak na aplikacje



Wprowadzenie – Zagrożenia

- Protokoły poszczególnych warstw modelu OSI „ufają sobie”
- Zbyt prosty, anonimowy dostęp do medium
- Usługi ułatwiające korzystanie z sieci, np. DHCP, nie zawierają mechanizmów zabezpieczeń

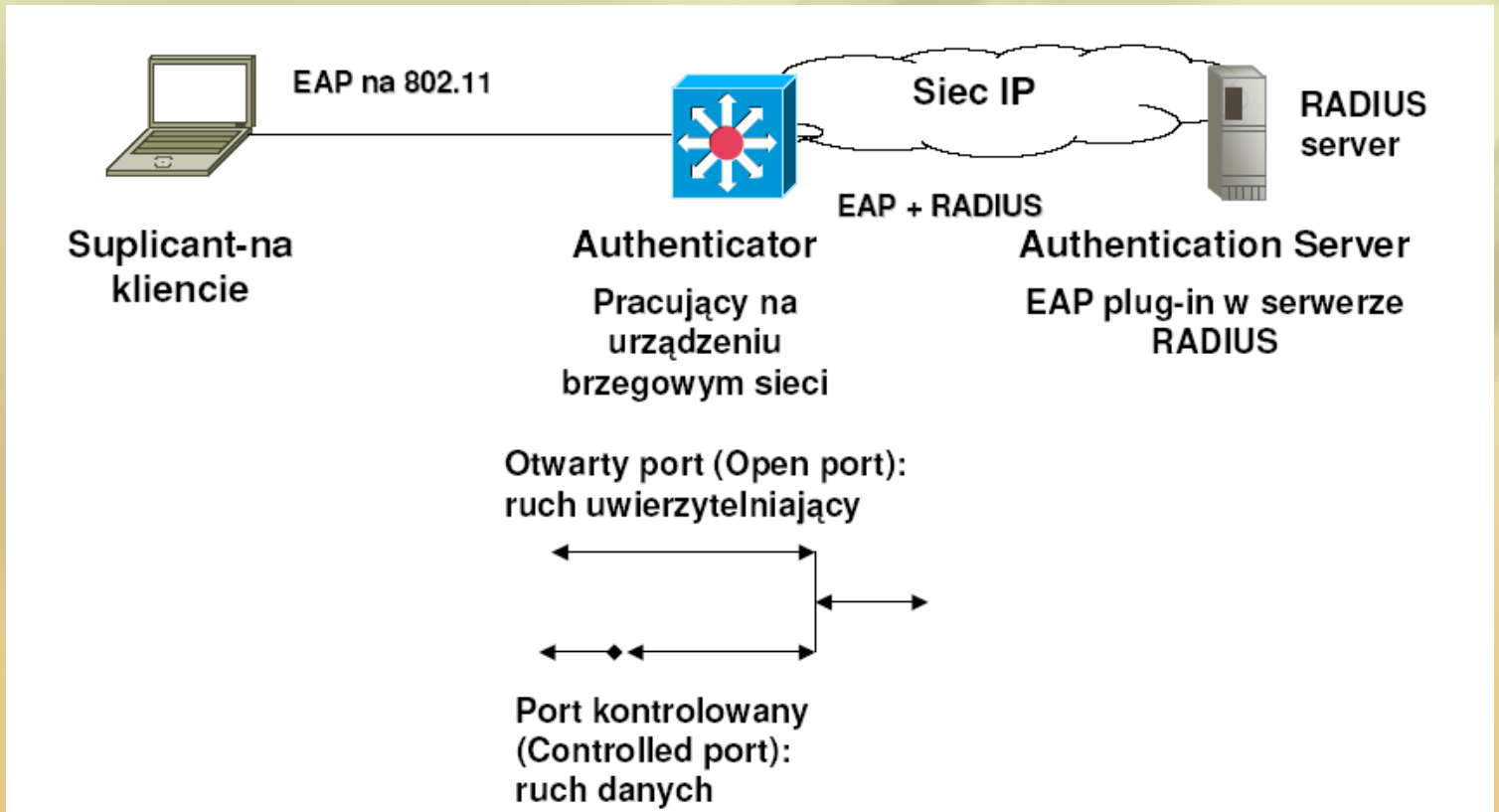
Warstwa sieci zamiast eliminować, dodaje dodatkowe zagrożenia

Kontrola dostępu - Standard 802.1x

- Standard IEEE kontroli dostępu do sieci przewodowych i bezprzewodowych
- Działa w warstwie fizycznej, a więc w sposób niewidoczny dla protokołów sieciowych i aplikacji
- Umożliwia:
  - Uwierzytelnienie urządzeń połączonych do portów sieci LAN (przełączników i punktów dostępowych)
  - ustanowienie połączenia punkt-punkt
- Blokuje anonimowy i nieautoryzowany dostęp do medium

Kontrola dostępu - Standard 802.1x

- **Zasada działania**



Kontrola dostępu - Standard 802.1x

- Wymagania i podział ról:
  - Klient (suplikant) musi posiadać kod 802.1x (sterownik, serwis)
  - Autentykator (przełącznik lub punkt ostępowy) działa jako pośrednik serwera RADIUS
  - Serwer RADIUS musi wspierać protokół EAP

Kontrola dostępu - EAP

- Extensible Authentication Protocol
- Zdefiniowany w dokumencie RFC 3748
- Definiuje format wiadomości, nie protokół ich przesyłania
- Przystosowany do przenoszenia dowolnych danych uwierzytelniających
- Najczęściej używane są trzy rodzaje uwierzytelniania
  - EAP-MD5
  - EAP-PSK
  - EAP-TLS

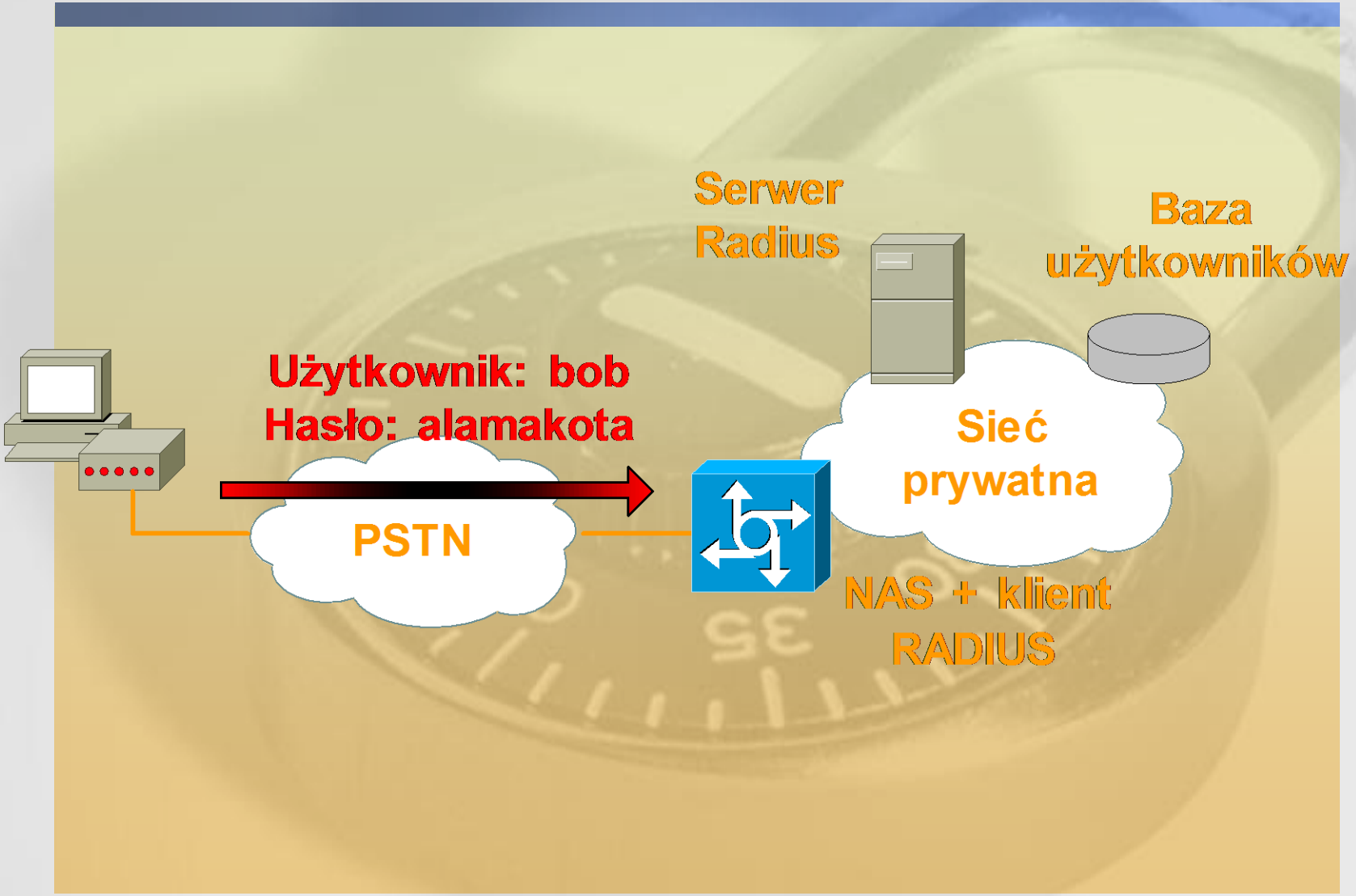
Kontrola dostępu - EAP

- EAP-MD5:
  - Najprostsza z metod
  - Uwierzytelnianie typu wyzwanie - odpowiedź
  - Brak szyfrowania kanału
- EAP-PSK:
  - Zdefiniowana w dokumencie RFC 4764
  - Uwierzytelniania na podstawie współdzielonego sekretu PSK (ang. Pre-Shared Key)
  - Wzajemne uwierzytelnianie i ochrona kanału
- EAP-TLS:
  - Uwierzytelnianie na podstawie certyfikatu
  - Wzajemne uwierzytelnianie i ochrona kanału

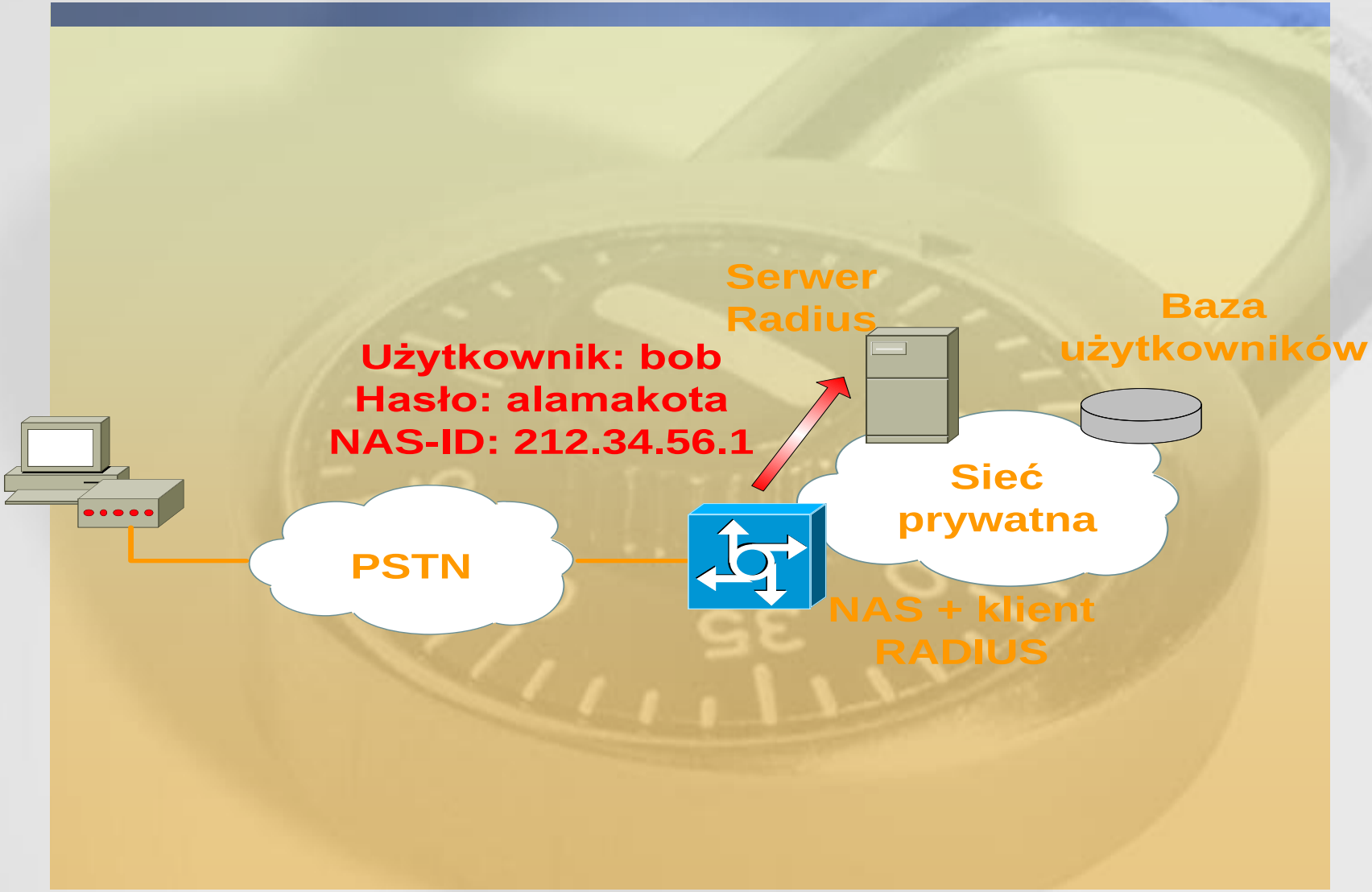
Kontrola dostępu - RADIUS

- Remote Authentication Dial In User Service
- Zdefiniowany w dokumentach:
  - RFC 2058 (usługa)
  - RFC 2138 (mechanizmy uwierzytelniania)
  - RFC 2139 (mechanizmy rozliczania)
- Protokół komunikacji między urządzeniem sieciowym a serwerem uwierzytelniającym i autoryzującym dostęp do sieci
- Transportuje dane uwierzytelniające i konfigurujące
- Transport dla EAP

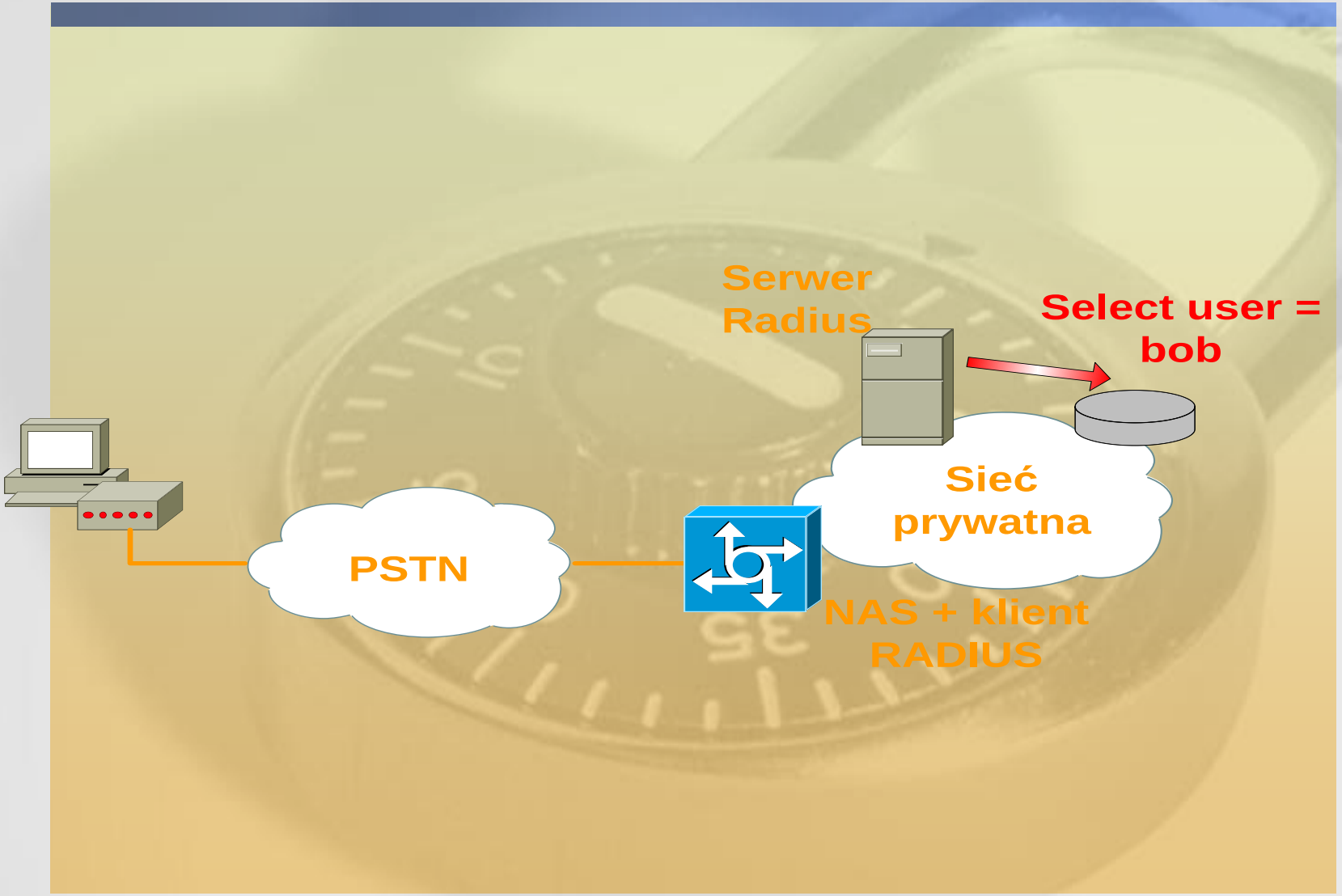
Kontrola dostępu – uwierzytelnianie przez serwer RADIUS



Kontrola dostępu – uwierzytelnianie przez serwer RADIUS



Kontrola dostępu – uwierzytelnianie przez serwer RADIUS

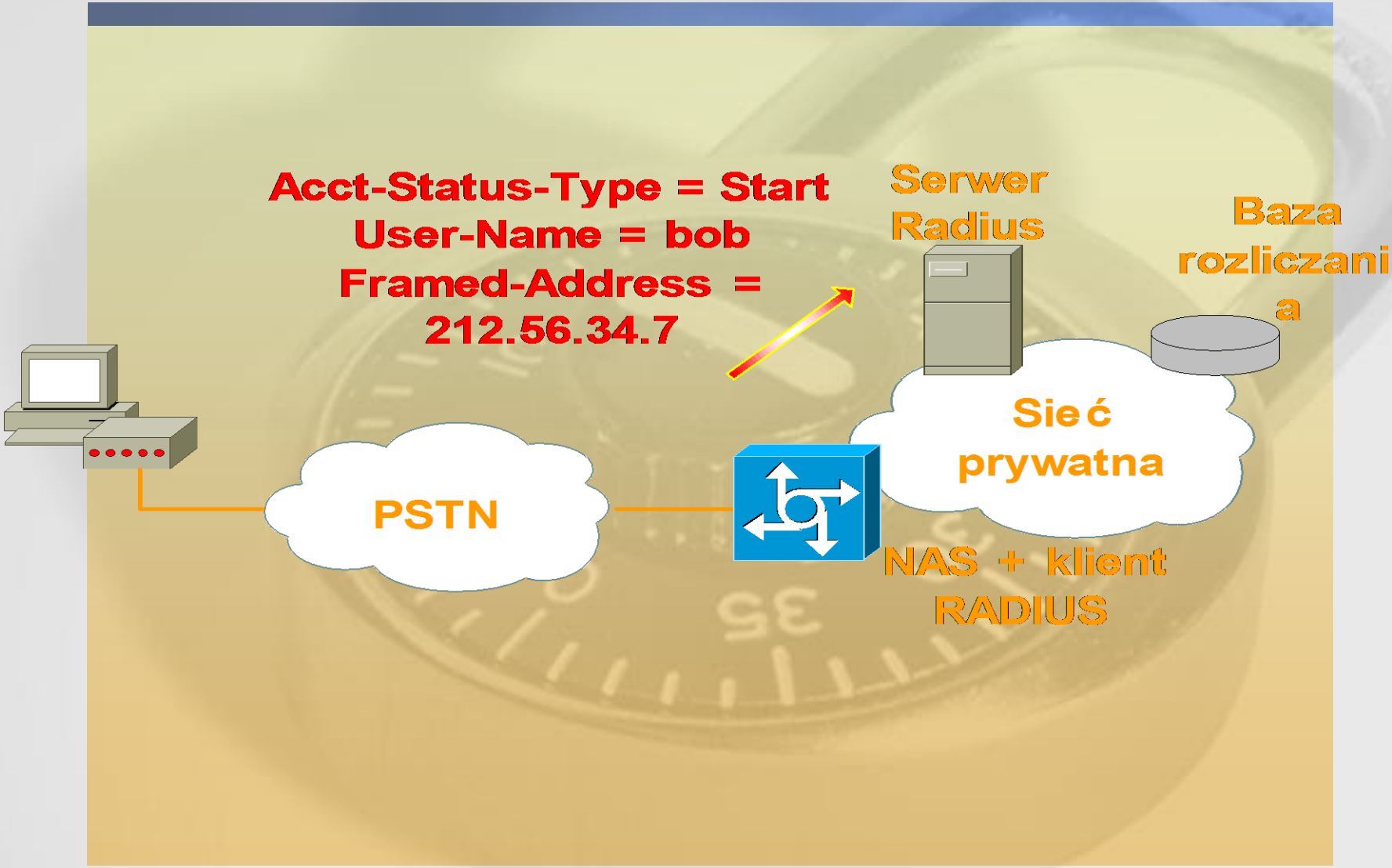


Kontrola dostępu – uwierzytelnianie przez serwer RADIUS

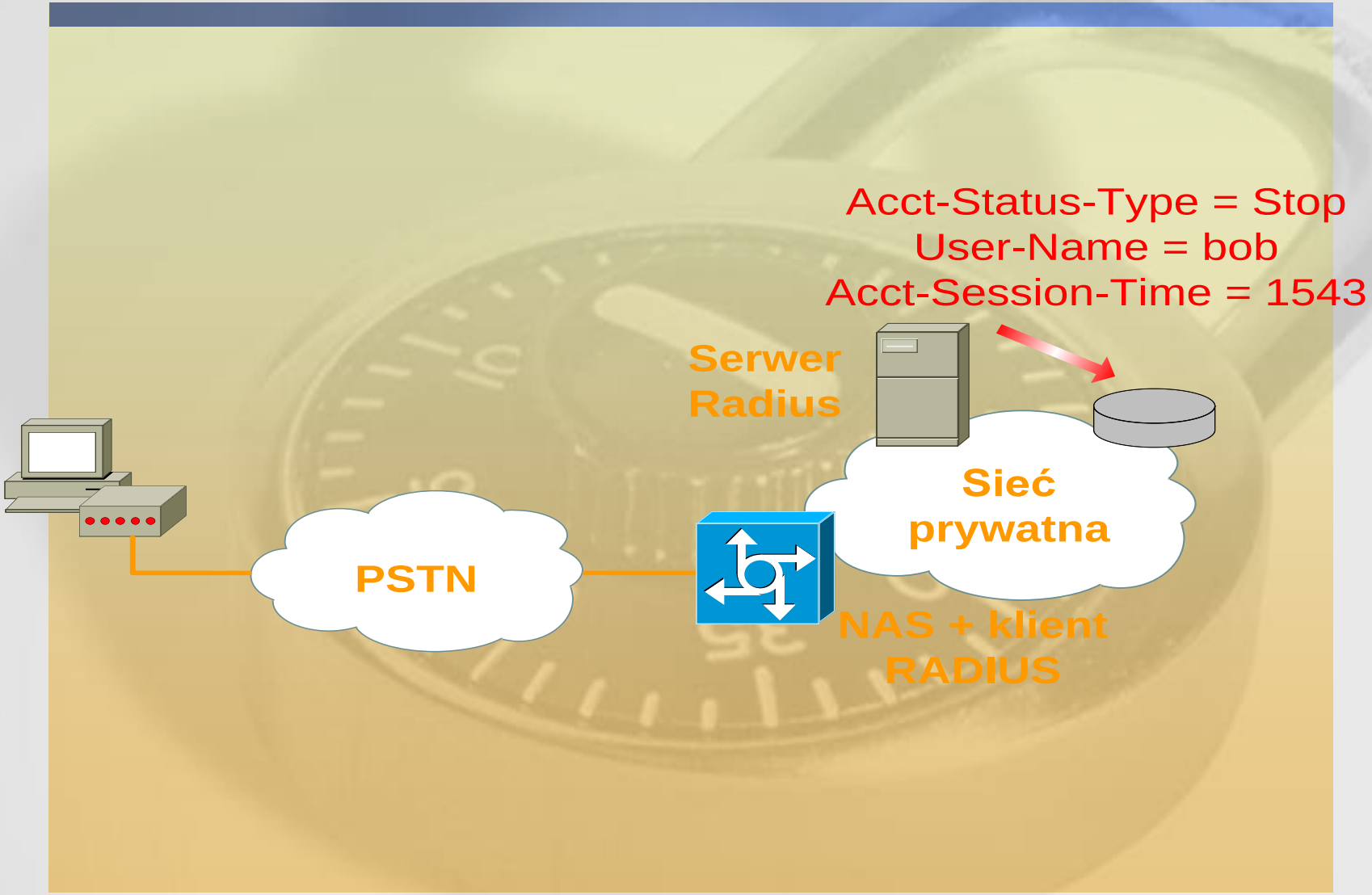
Kontrola dostępu – uwierzytelnianie przez serwer RADIUS

Kontrola dostępu – rozliczanie przez serwer RADIUS

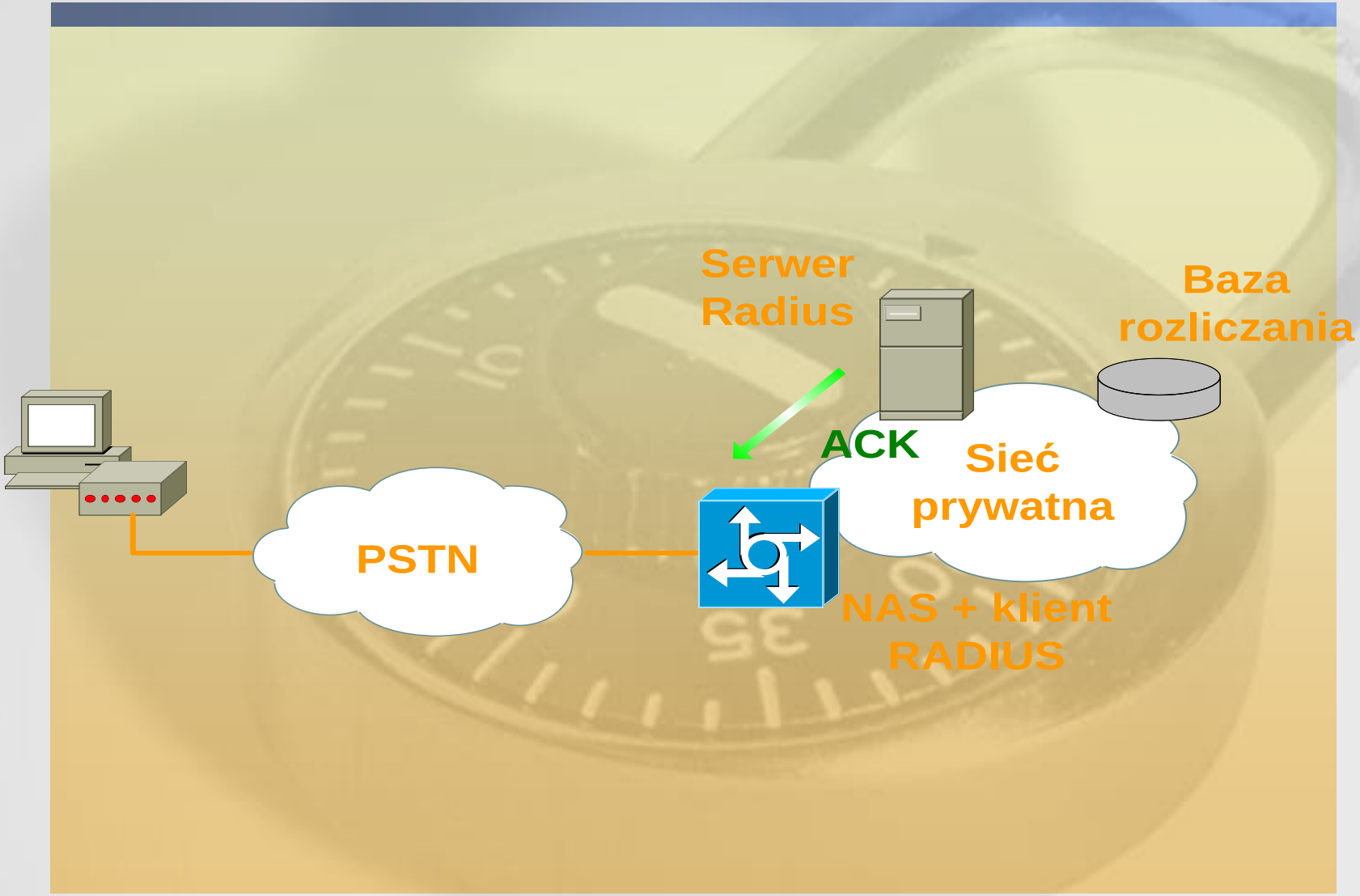
Kontrola dostępu – rozliczanie przez serwer RADIUS



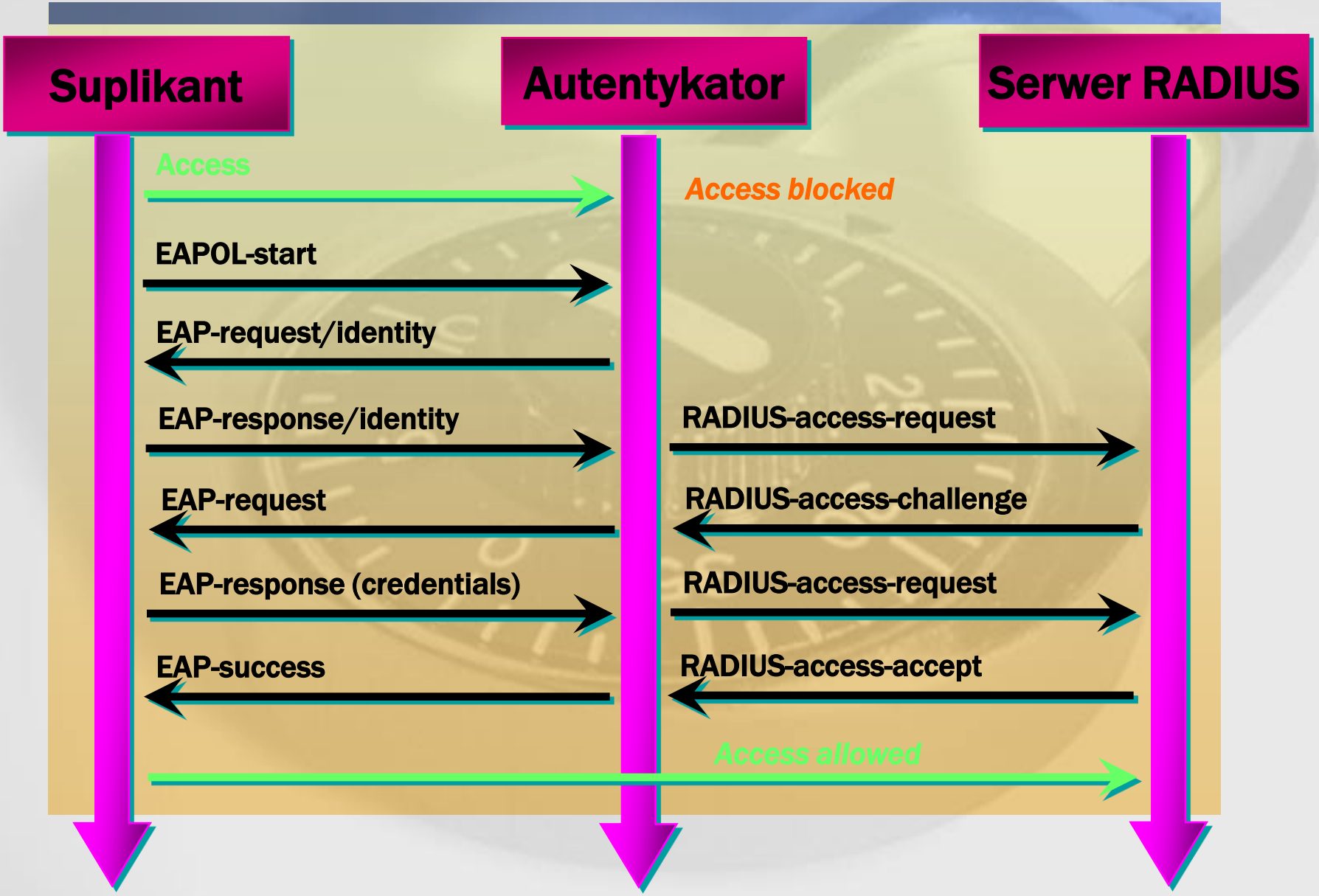
Kontrola dostępu – rozliczanie przez serwer RADIUS



Kontrola dostępu – rozliczanie przez serwer RADIUS



Kontrola dostępu - Standard 802.1x

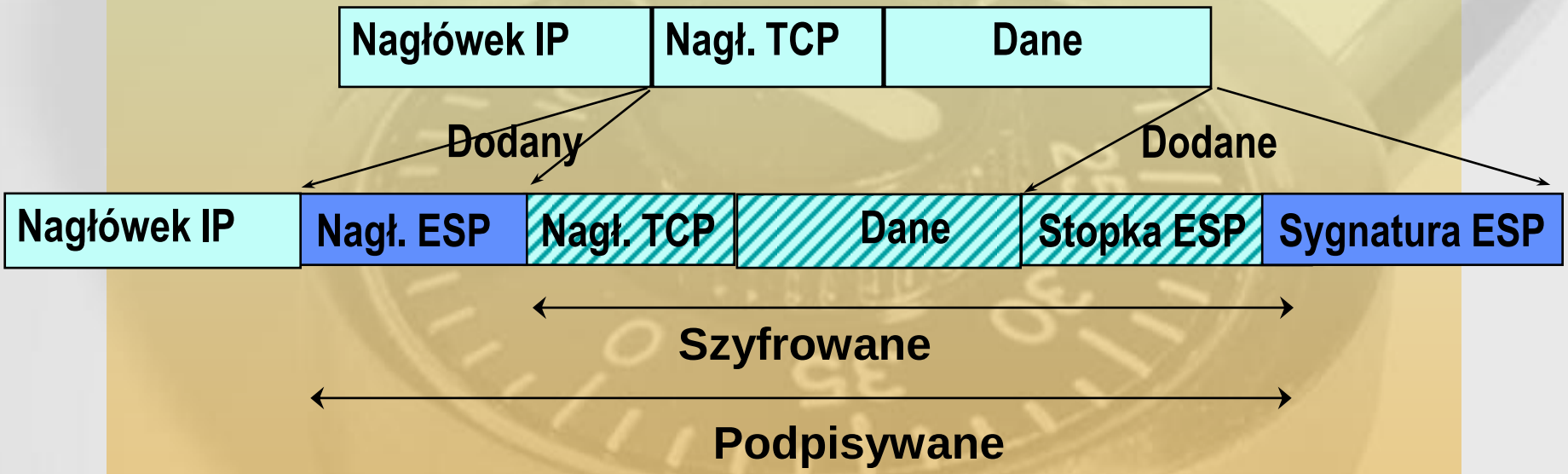


Zabezpieczenia - IPSec

- Protokół ESP (Encapsulated Security Payload)
  - Szyfrowany i ewentualnie podpisywany każdy pakiet
  - Pakiety są najpierw szyfrowane
  - Podpisywane jest nagłówek IPSec i dane
  - Protokół IP 50
- Dwa tryby:
  - Transportu
  - Tunelowania

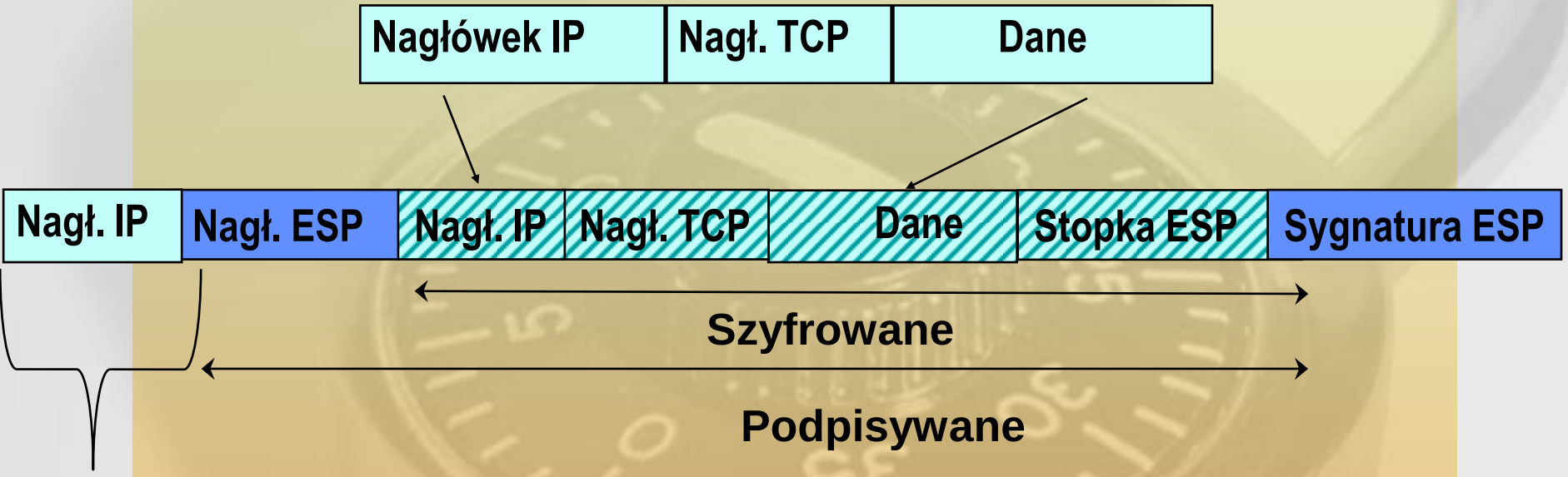
Zabezpieczenia – IPSec

- Protokół ESP w trybie transportu
  - Narzut od 22 do 36 bajtów



Zabezpieczenia – IPSec

- Protokół ESP w trybie tunelowania



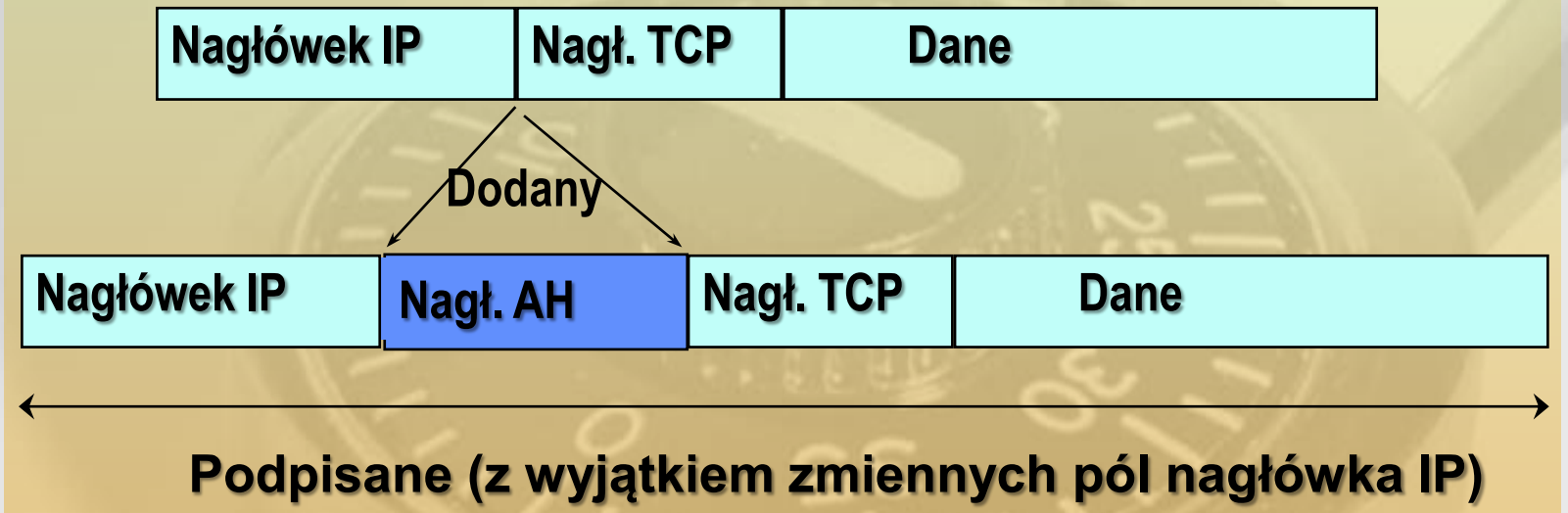
Nowy nagłówek IP ze zmienionymi adresami nadawcy i odbiorcy

Zabezpieczenia - IPSec

- Protokół AH (Authentication Header)
  - Podpisywany jest cały pakiet IP
  - Zmienne pola w nagłówku IP najpierw są zerowane
  - Jeżeli stosowany jest też protokół ESP, dane są najpierw szyfrowane
  - Protokół IP 51
- Dwa tryby:
  - Transportu
  - Tunelowania

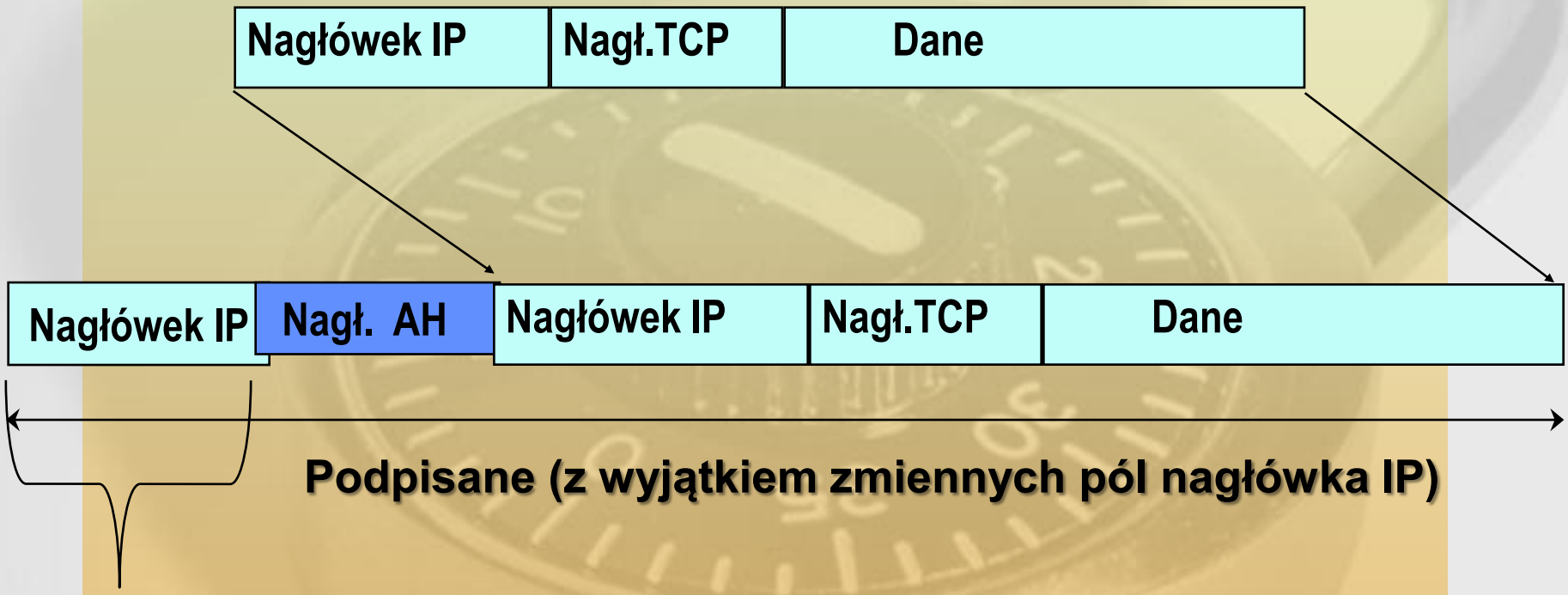
Zabezpieczenia - IPSec

- Protokół AH w trybie transportu
  - Narzut 24 bajtów



Zabezpieczenia - IPSec

- Protokół AH w trybie tunelowania



Zabezpieczenia - IPSec

- Protokół IKE (Internet Key Exchange)
- Faza 1:
  - Nawiązanie bezpiecznego kanału (ISAKMP SA)
  - Potwierdzenie tożsamości komputera
- Faza 2:
  - Nawiązanie bezpiecznego kanału pomiędzy źródłowym i docelowym komputerem (IPSec SA)
- Dwa tryby:
  - Główny
  - Szybki

Zabezpieczenia - IPSec

- Tryb główny (Main) ma na celu:
  - Nawiązanie bezpiecznego, dwukierunkowego połączenia
  - Uzgodnienie mechanizmów zabezpieczeń (np. protokołu IPSec)
- Trzy kroki:
  - Negocjacja SA
  - Wymiana wyzwania (protokół Diffiego-Hellmana)
  - Uwierzytelnienie

Zabezpieczenia - IPSec

- Tryb główny ze współdzielonym sekretem

inicjator

Odpowiadający

Header, SA Proposals →

← Header, Selected SA Proposal

Header, D-H Key Exchange, $Nonce_i$ →

← Header, D-H Key Exchange, $Nonce_i$,

ZASZYFROWANE

Header, Id_i, $Hash_i$ →

← Header, Id_r, $Hash_r$

Zabezpieczenia - IPSec

- Tryb główny z użyciem certyfikatów

inicjator

Odpowiadający

Header, SA Proposals →

← Header, Selected SA Proposal

Header, D-H Key Exchange, $Nonce_i$ →

← Header, D-H Key Exchange, $Nonce_i$, Certificate Request

ZASZYFROWANE

Header, Id_i, $Certificate_i$, $Signature_i$, Certificate Request →

← Header, Idr, Certificater, Signaturer

Zabezpieczenia - IPSec

- Tryb główny z użyciem protokołu Kerberos

inicjator

Odpowiadający

Header, SA Proposals →

← Header, Selected SA Proposal

Header, D-H Key Exchange,
$Nonce_i$, $Kerberos\ Token_i$ →

← Header, D-H Key Exchange,
$Nonce_i$, $Kerberos\ Token_i$

ZASZYFROWANE

Header, Id_i,
$Hash_i$ →

← Header, Id_r,
$Hash_r$

Zabezpieczenia - IPSec

- Tryb szybki

Inicjator

Odpowiadający

ZASZYFROWANE

Header, IPSec
Proposed SA →

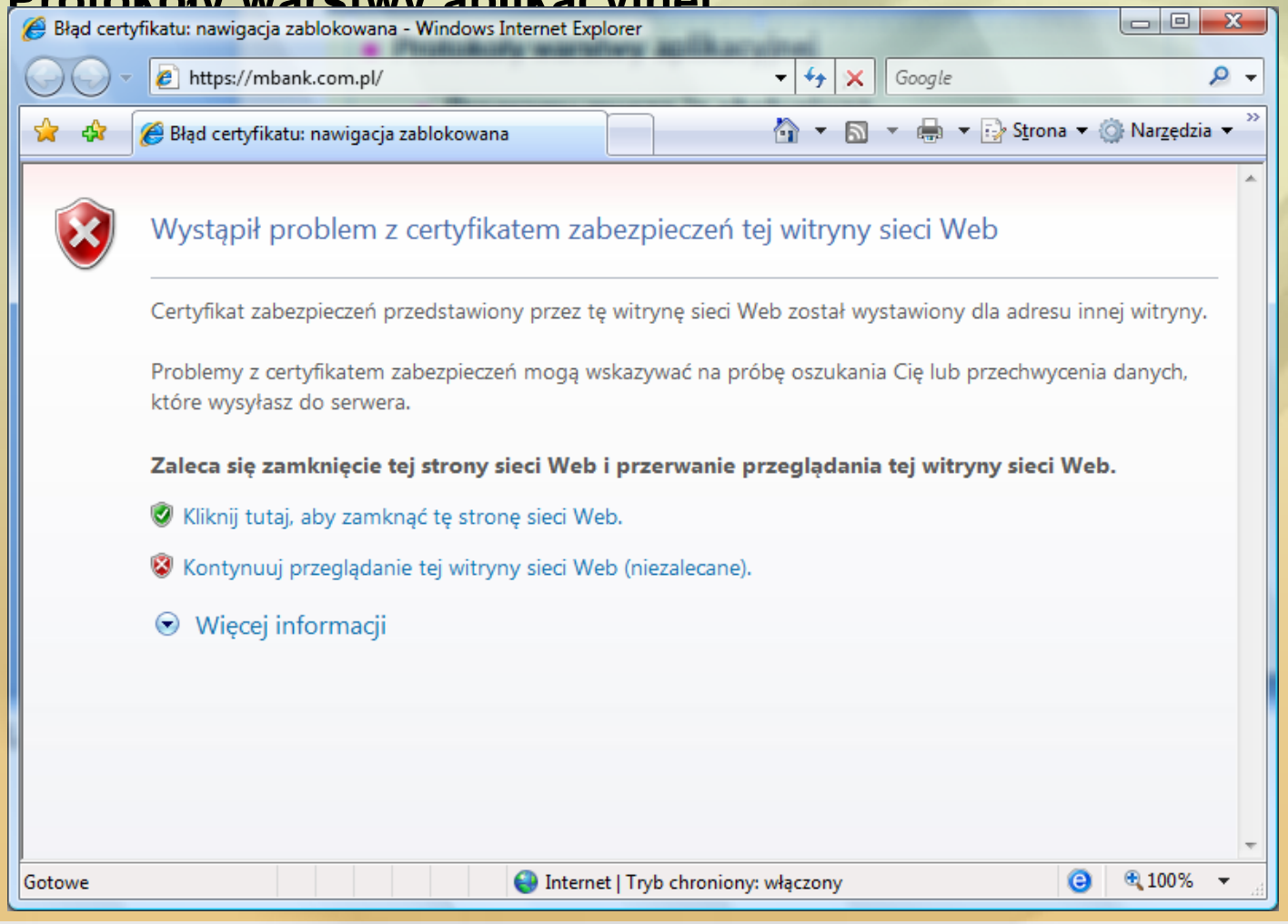
← Header, IPSec
Selected SA

Header, Hash →

← Header, Connected
Notification

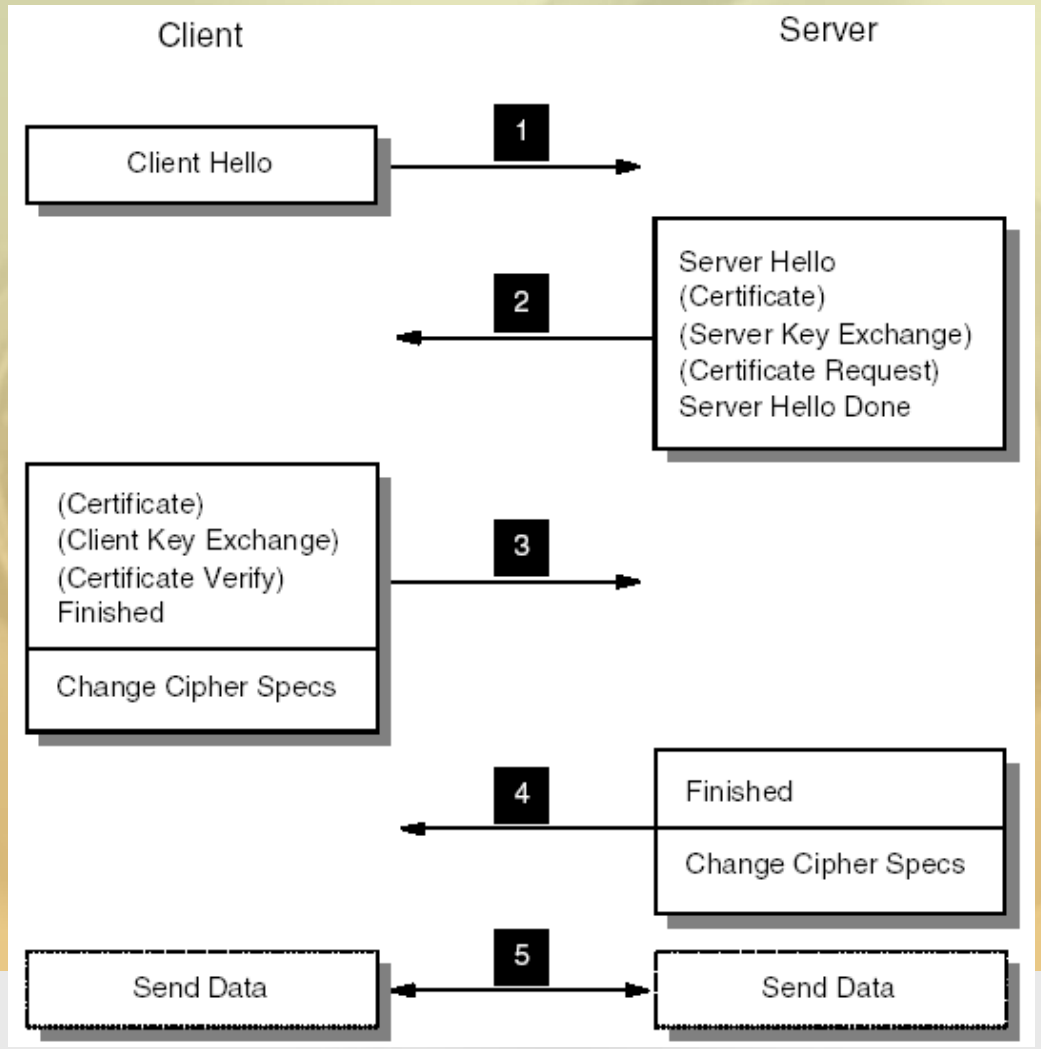
Zabezpieczenia – SSL/TLS

- Protokoły warstwy aplikacyjnej



Zabezpieczenia – SSL/TLS

- **Zestawienie bezpiecznego połączenia**

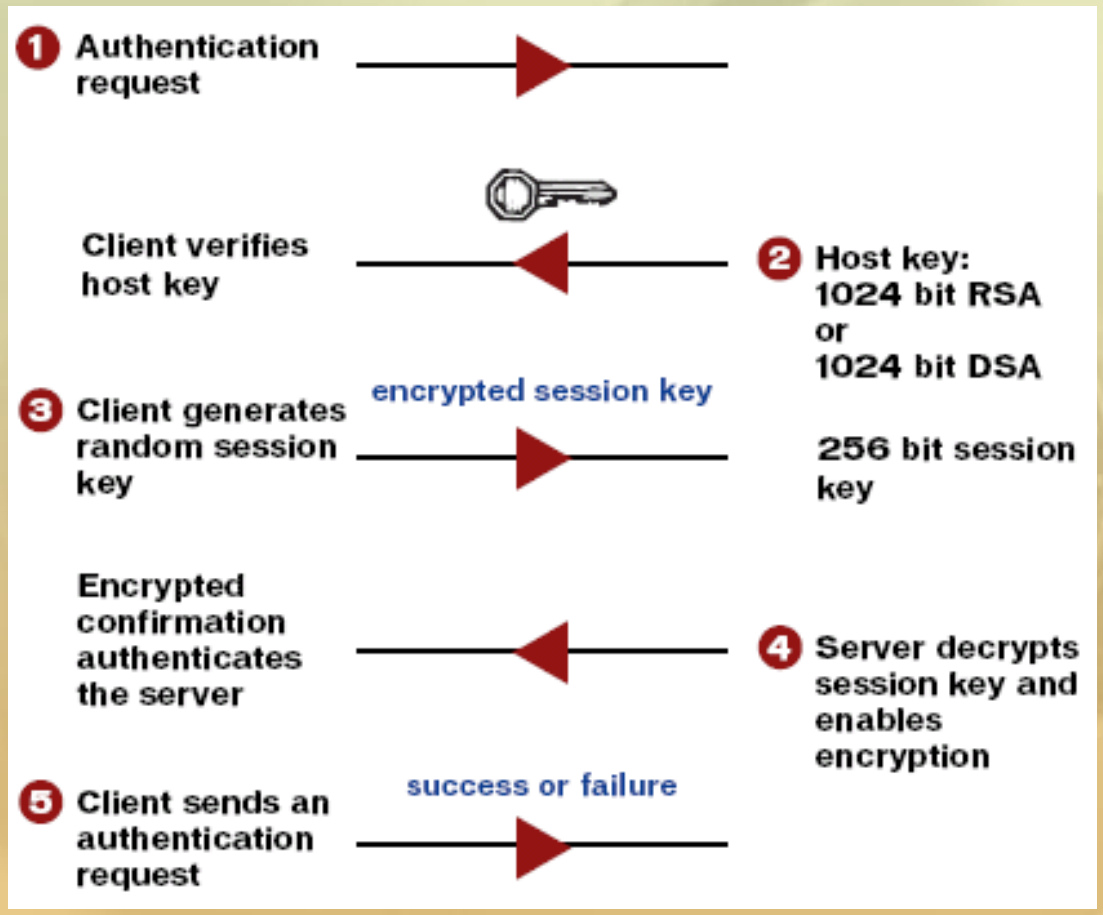


Zabezpieczenia - SSH

- SSH (Secure Shell):
  - Opracowany w celu realizacji bezpiecznego połączenia terminala znakowego:
  - Alternatywa dla usługi Telnet.
- Dodatkowo umożliwia:
  - Przesyłanie plików (usługa SCP / SFTP),
  - Tunelowanie połączenia dowolnej aplikacji lokalnej do zdanego serwera,

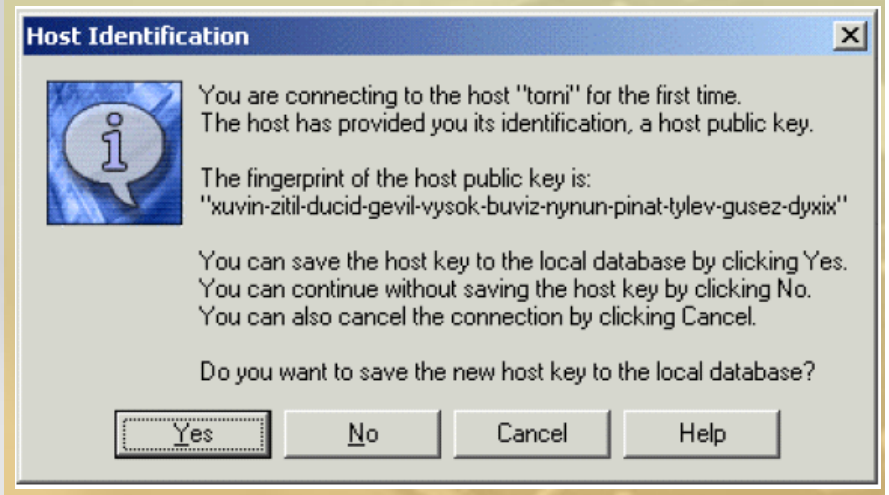
Zabezpieczenia - SSH

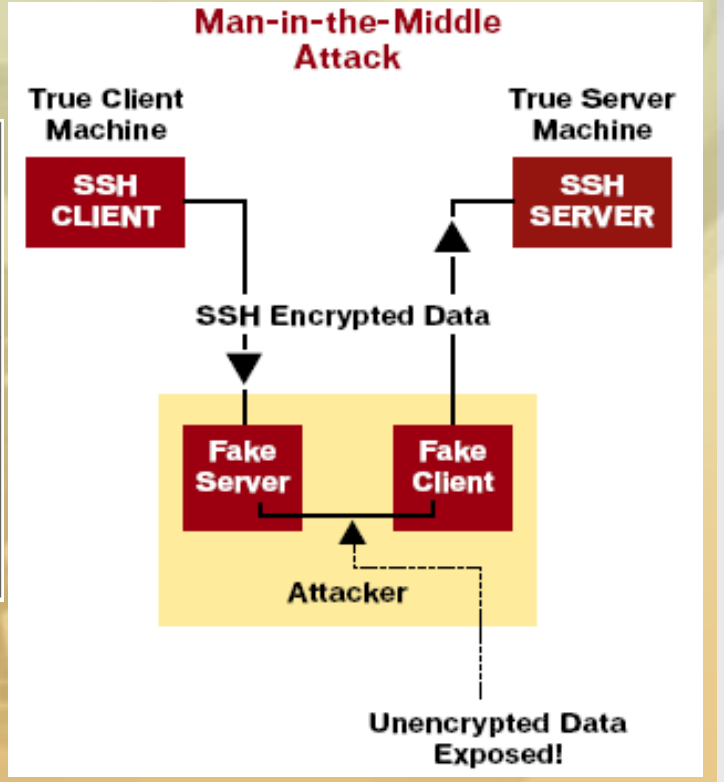
- Zestawienie bezpiecznego tunelu



Zabezpieczenia - SSH

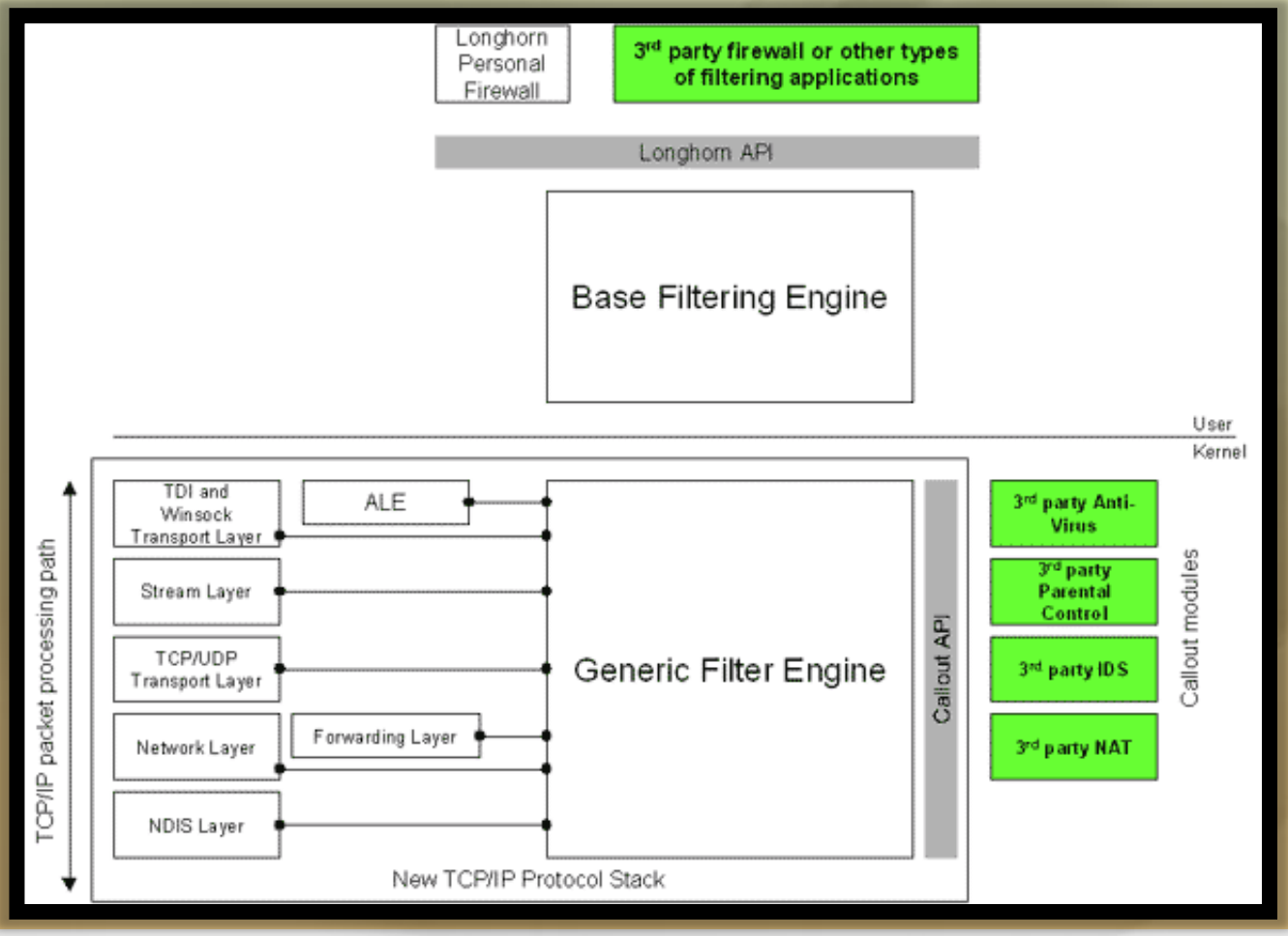
- Wymiana kluczy publicznych i atak typu Man-in-the-middle





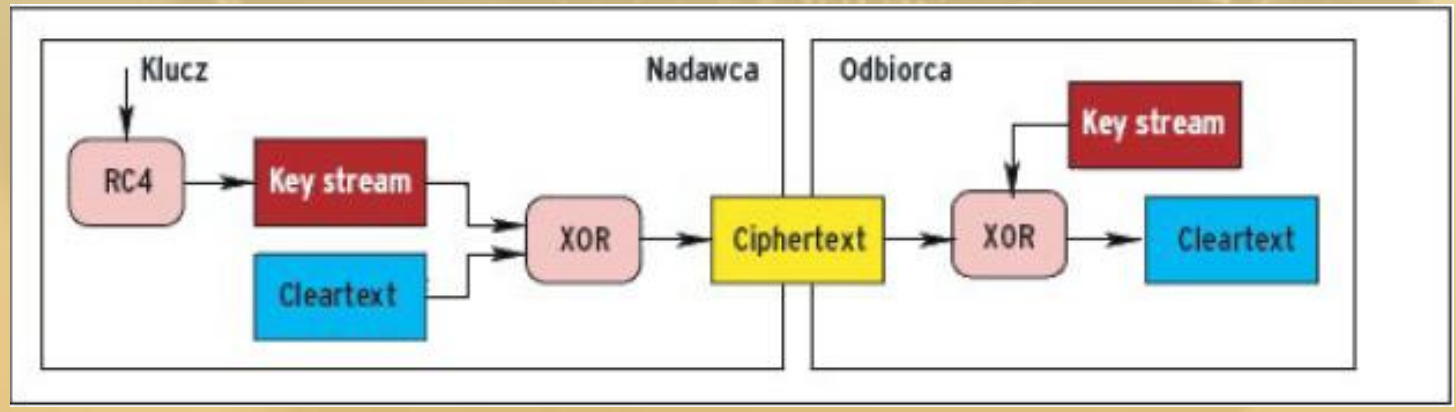
Zabezpieczenia - Zapory

- Zapora systemu Windows



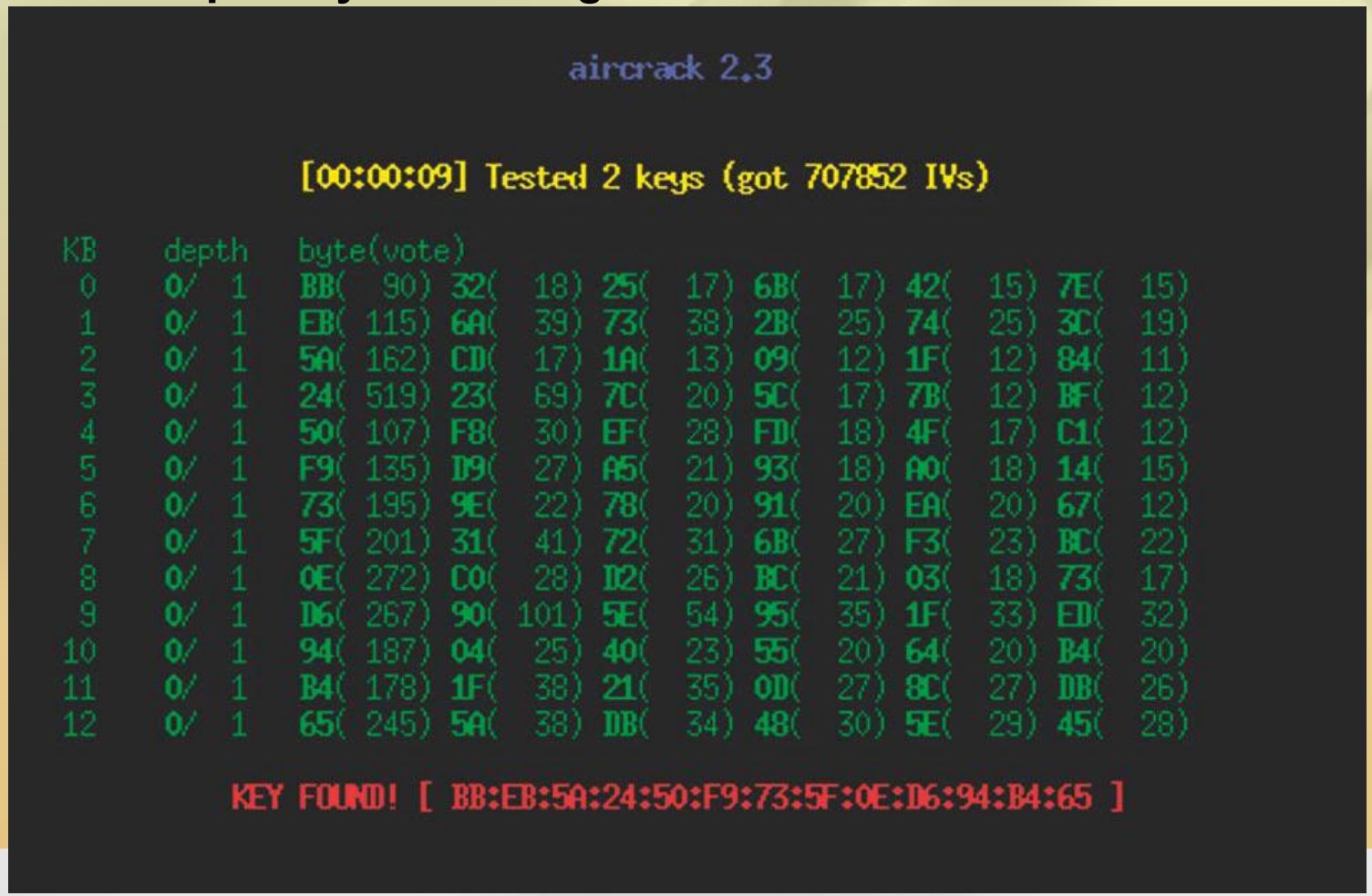
Sieci bezprzewodowe

- **Szyfrowanie WEP (Wired Equivalent Privacy):**
  - Wyliczana jest suma kontrolna c oryginalnego pakietu P
  - Suma dołączana jest do danych pakietu
  - Karta sieciowa generuje 24 bitowy wektor inicjalizujący (IV) który razem ze kluczem WEP (K) jest używany do zaszyfrowania danych pakietu algorytmem RC4



Sieci bezprzewodowe

- Słabe punkty technologii WEP:



Sieci bezprzewodowe

- WPA (Wi-Fi Protected Access):
  - Uwierzytelnianie przez serwer RADIUS albo na podstawie współdzielonego sekretu (tryb PSK)
  - Automatyczne zarządzanie kluczami – domyślnie są one zmieniania co godzinę za pomocą protokołu TKIP
- WPA2 (standard IEEE 802.11i):
  - Algorytm CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)

Sieci bezprzewodowe

- **Porównanie standardów**

Nazwa standardu	WEP	WPA	WPA2 / 802.11i
Protokół szyfrowania	RC4	RC4	CCMP
Długość klucza w bitach	40 lub 104	40 lub 104	128
Protokół wymiany kluczy	BRAK	TKIP	CCMP
Rozmiar wektora IV w bitach	24	48	48