# „Bezpieczne” protokoły

*Materiały pomocnicze do wykładu*

**Bezpieczeństwo systemów informatycznych**

Bezpieczne protokoły



## „Bezpieczne” protokoły

- IPSec (*Secure IP*)
- L2TP (*Layer 2 Tunneling Protocol*)
- PPTP (*Point-to-Point Tunneling Protocol*)
- SSL (*Secure Socket Layer*)
- TLS (*Transport Layer Security*)
- SHTTP (*Secure HyperText Transfer Protocol*)
- SSH (*Secure Shell*)



## IPSec

- poufność
- integralność
- uwierzytelnienie
- przezroczystość



## Składniki IPSec

- Protokoły bezpieczeństwa
  - uwierzytelniający (*Authentication Header* - AH)
  - zabezpieczenia zawartości pakietu (*Encapsulating Security Payload* - ESP).
- Połączenia bezpieczeństwa (*Security Assaciations*)
- Zarządzanie kluczami (*Internet Key Management* - IKE)
- Algorytmy uzgadniania parametrów (ISAKMP, Photuris), szyfrowania, kompresji danych (IPCOMP).



## IPSec - połączenia bezpieczeństwa

- Security Parameter Index (SPI)
- Adres IP przeznaczenia (DA)
- Protokół bezpieczeństwa (AH lub ESP)

## Co określa *SA*?

- Informacje definiujące algorytm szyfrowania
- Informacje definiujące algorytm uwierzytelniania
- Informacje definiujące algorytm integralności
- Klucze szyfrujące i kodujące wykorzystywane w AH i ESP
- Okres ważności kluczy
- Okres ważności tunelu

Zbigniew Suski BSI – protokoły 6

## Bazy połączeń

- Baza polityki bezpieczeństwa *(Security Policy Database)*
- Baza połączeń bezpieczeństwa *(Security Association Database)*

Zbigniew Suski BSI – protokoły 7

## Tryb transportowy

| | | | |
|---|---|---|---|
| Nagłówek IP | Nagłówek AH | Dane | |
| Nagłówek IP | Nagłówek ESP | Dane | |
| Nagłówek IP | Nagłówek ESP | Nagłówek AH | Dane |
| Nagłówek IP | Nagłówek AH | Nagłówek ESP | Dane |

Zbigniew Suski BSI – protokoły 8

## Tryb tunelowy

| | | | | |
|---|---|---|---|---|
| Nagłówek IP2 | Nagłówek AH | Nagłówek IP1 | Dane | |
| Nagłówek IP2 | Nagłówek AH2 | Nagłówek IP1 | Nagłówek AH1 | Dane |
| Nagłówek IP2 | Nagłówek ESP2 | Nagłówek IP1 | Nagłówek ESP1 | Dane |
| Nagłówek IP2 | Nagłówek AH | Nagłówek IP1 | Nagłówek ESP | Dane |
| Nagłówek IP2 | Nagłówek ESP | Nagłówek IP1 | Nagłówek AH | Dane |

Zbigniew Suski BSI – protokoły 9

## IPSec - negocjacje i wymiana kluczy

- Algorytmy szyfrujące
- Algorytmy uwierzytelnienia
- Algorytmy kompresji
- Kombinacje w/w w poszczególnych kanałach SA
- Parametry szczegółowe algorytmów i kluczy kryptograficznych

Zbigniew Suski BSI – protokoły 10

## IPSec – wybrane protokoły negocjacji i dystrybucji

- ISAKMP (*Internet Security Associattion and Key Management Protocol*)
- OAKLEY
- IKE (*Internet Key Exchange*)
- PHOTURIS
- SKIP

Zbigniew Suski BSI – protokoły 11

## Nagłówek protokołu uwierzytelniającego AH

- Next *Header* - typ zawartości pakietu za nagłówkiem AH.
- *Payload Len* - długość nagłówka AH
- *Security Parameters Index* (SPI) – element identyfikatora SA
- *Sequence Number* – licznik pakietów
- *Authentication Data* - wartość uwierzytelniająca *(Integrity Check VaJue* - ICV)



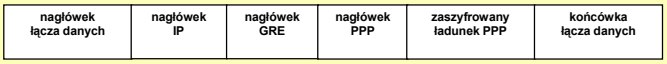
## L2TP i PPTP

- Baza: protokół PPP (warstwa 2 – łącza danych)
  - uwierzytelnianie
  - kompresja
  - kapsułkowanie TCP → IP → PPP
  - PPP LCP (*Link Control Protocol*)
  - PPP NCP (*Network Control Protocol*)
- Port docelowy połączenia sterującego PPTP: 1723
- Po utworzeniu ładunku PPP powrót do wyższych warstw



## Struktura pakietów

- PPTP




- L2TP

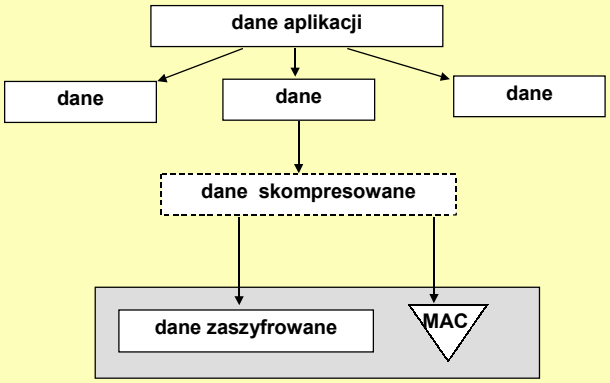



## SSL (*Secure Socket Layer*)

- *SSL Record Protocol,*
- *SSL Handshake Protocol*
- *SSL Change Cipher Spec Protocol*
- *SSL Alert Protocol*

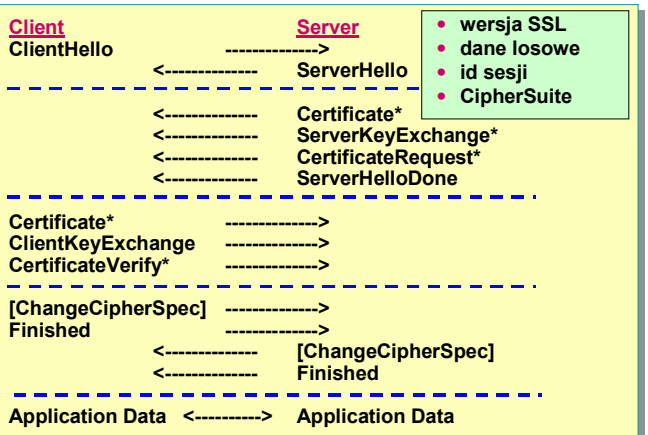


## *SSL Record Protocol*






## SSL *Handshake Protocol*



## TLS (*Transport Layer Security*)

- **Interoperacyjność**
- **Łatwość rozszerzenia**

**RFC 2246** ***Transport Layer Security*** **(TLS) v 1.0.**

**RFC 2817** ***Upgrading to TLS Within HTTP/1.1***

**RFC 2818** ***HTTP Over TLS***

**RFC 2487** ***SMTP Service Extension for Secure SMTP over TLS***



## Protokół HTTP

***Request = Request-Line***
****(( general-header***
***| request-header***
***| entity-header ) CRLF)***
***CRLF***
***[ message-body ]***

***Response = Status-***
****(( general-header***
***| response-header***
***| entity-header ) CRLF)***
***CRLF***
***[ message-body ]***



## Protokół HTTP i SHTTP

Request-Line = Method SP Request-URI SP HTTP-Version CRLF
Np.: **GET http://www.w3.org/pub/WWW/TheProject.html HTTP/1.1**

Status-Line = HTTP-Version SP Status-Code SP Reason-Phrase CRLF
Np.: **HTTP/1.1 200 OK**

Przykłady kodów:
Status-Code =
**"100" ; Continue**
**| "200" ; OK**
**| "202" ; Accepted**
**| "400" ; Bad Request**
**| "403" ; Forbidden**
**| "404" ; Not Found**

**Linia żądania:**
**Secure * Secure-HTTP/1.4**
**Odpowiedź serwera:**
**Secure-HTTP/1.4 200 OK**



## SHTTP – nagłówki (*Secure HyperText Transfer Protocol*)

- **SHTTP-Privacy-Domain**
  **określa standard zapisu zabezpieczanej wiadomości**
- **SHTTP-Certificate-Type**
  **określa akceptowane formaty certyfikatów**
- **SHTTP-Key-Exchange-Algorithm**
  **określa algorytm używamy do wymiany kluczy**
- **SHTTP-Signature-Algorithms**
  **określa algorytm podpisu cyfrowego**
- **SHTTP-Message-Digest-Algorithms**
  **określa algorytm funkcji skrótu**
- **SHTTP-Symmetric-Content-Algorithms**
  **określa algorytm symetrycznego szyfru pól danych**
- **SHTTP-Symmetric-Header-Algorithms**
  **określa symetryczny algorytm szyfrowania nagłówków**
- **SHTTP-Privacy-Enhancements**
  **określa zabezpieczenia związane z wiadomością**



## SSH (*Secure Shell*)

- ***Transport layer protocol*** **[SSH-TRANS]**
- ***User authentication protocol*** **[SSH-USERAUTH]**
- ***Connection protocol*** **[SSH-CONN]**

**Struktura pakietu SSH-TRANS**

- ***packet_length***
- ***padding_length***
- ***payload***
- ***random padding***
- ***mac (message authentication code)***



## SSH – TRANS inicjowanie negocjacji

- ***code (SSH_MSG_KEXINIT)***
- ***kex_algorithms***
- ***server_host_key_algorithms***
- ***encryption_algorithms_client_to_server***
- ***encryption_algorithms_server_to_client***
- ***mac_algorithms_client_to_server***
- ***mac_algorithms_server_to_client***
- ***compression_algorithms_client_to_server***
- ***compression_algorithms_server_to_client***
- ***languages_client_to_server***
- ***languages_server_to_client***
- ***first_kex_packet_follows***

## SSH - USERAUTH

**Żądanie autentykacji:**

- *code (SSH_MSG_USERAUTH_REQUEST)*
- *user name*
- *service name*
- *authentication method name*

**reszta pakietu zależy od zaproponowanej metody autentykacji**



## SSH - USERAUTH

**Odpowiedź na żądanie autentykacji:**

**negatywna:**
- *code (SSH_MSG_USERAUTH_FAILURE)*
- *authentications that can continue*
- *partial success*

**pozytywna:**
- *code (SSH_MSG_USERAUTH_SUCCESS)*

**Banner dla klienta:**
- *code (SSH_MSG_USERAUTH_BANNER)*
- *message*
- *language tag*



## SSH – USERAUTH metoda *publickey*

- *code (SSH_MSG_USERAUTH_REQUEST)*
- *user name*
- *service*
- *"publickey"*
- *public key algorithm name*
- *public key blob – tutaj może być certyfikat*
- *signature*



## SSH – USERAUTH metoda *hostbased*

- *code (SSH_MSG_USERAUTH_REQUEST)*
- *user name*
- *service*
- *"hostbased"*
- *public key algorithm for host key*
- *public host key and certificates for client host*
- *client host name*
- *client user name on the remote host*
- *signature*



## SSH – USERAUTH metoda *password*

- *code (SSH_MSG_USERAUTH_REQUEST)*
- *user name*
- *service*
- *"password"*
- *plaintext password*



## SSH-CONN otwarcie kanału

- *code (SSH_MSG_CHANNEL_OPEN)*
- *channel type*
- *sender channel identifier*
- *initial window size*
- *maximum packet size*
- *channel type specific data follows*