Protokoły Internetu , ochrona danych i uwierzytelnianie w Internecie

Jacek Wieczorek

PWr 2012

- HTTP / HTTPS
- POP3 / IMAP, SMTP
- FTP
- Telnet I SSH
- Inne …
- Ochrona danych
- Uwierzytelnienie

HTTP / HTTPS

- Hypertext Transfer Protocol
- Określa formę żądań klienta i odpowiedzi serwera
- Bezstanowy
- Http – port 80, Https – port 443
- Header + Body
- GET, POST, PUT, DELETE, HEAD, OPTIONS, TRACE, CONNECT

POP3 / IMAP, SMTP

- Post Office Protocol version 3
- Pobieranie poczty ze zdalnego serwera do komputera lokalnego
- Internet Message Access Protocol – zaawansowany “następca” POP3
- Simple Mail Transfer Protocol (port 25)

FTP

- File Transfer Protocole
- Komunikacja typu klient-serwer
- Wykorzystanie TCP
- Protokół 8-bitowy
- Tryb aktywny – port 21 dla poleceń, 20 do przesyłu
- Tryb pasywny – 21 dla poleceń, > 1024 – transfer danych

Telnet

- Standard protokołu do komunikacji w sieciach komputerowych
- Tylko terminale alfanumeryczne
- Nieszyfrowany

SSH

- Secure Shell
- Następca Telnet
- Zaszyfrowany transfer danych
- SSH – wspólna nazwa dla całej rodziny

Inne …

- IRC,
- XMPP
- DNS
- Wiele, wiele innych …

Ochrona danych

- Stosowanie certyfikatów
- Szyfrowanie danych
  - Algorytmy symetryczne : DES, 3DES
  - Algorytmy asymetryczne : RSA
- Podpis cyfrowy
- Eliminacja błędów ludzkich

Uwierzytelnienie

- Weryfikacja tożsamośći osoby, usługi lub urządzenia
- Login I hasło, tokeny, kody pin
- Uwierzytelnianie biometryczne
- Uwierzytelnienie dwuetapowe

Uwierzytelnienie

- Public key
- Kerberos
- Http Digest access authentication
- Http Basic access authentication
- Http + Html form based authentication

Linki

Google, RFC, Wikipedia