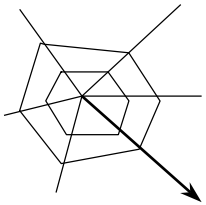
SECURE '98

Bezpieczeństwo WWW



Krzysztof Szczypiorski, Piotr Kijewski
Instytut Telekomunikacji Politechniki Warszawskiej
e-mail: {K.Szczypiorski,P.Kijewski}@tele.pw.edu.pl

Secure'98 - Zegrze, 2-3 kwietnia 1998

Plan prezentacji

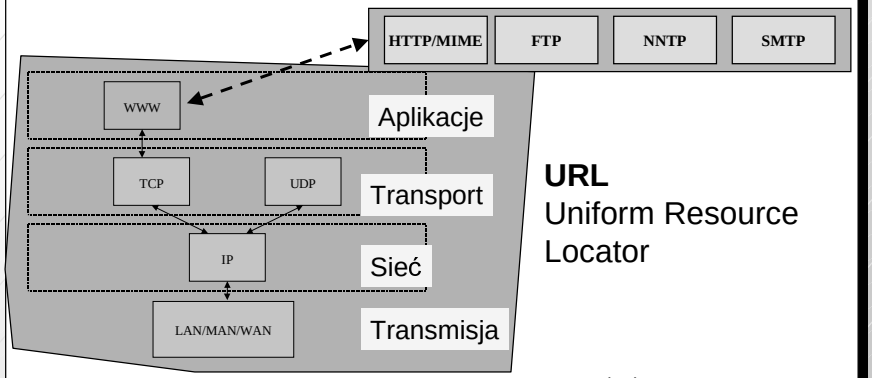
- Wprowadzenie
  - czym jest WWW?
  - związek z protokołami rodziny TCP/IP, URL
- Architektura WWW
  - MIME, HTTP, wymiana pomiędzy klientem a serwerem
  - architektura usługowa
- Zagrożenia
- Bezpieczeństwo
  - transportu (S-HTTP, SSL, PCT)
  - po stronie serwera (konfiguracja, umiejscowienie serwera)
  - po stronie klienta (Java, JavaScript, ActiveX)

Czym jest WWW?

- **WWW, W3 - World Wide Web - World Wide Wait**
- reakcja na frustracje związane:
  - z ograniczeniami Internetu
  - i z jego niekontrolowanym rozwojem (liczba dokumentów i ich rozmieszczenie)
- w przeszłości każdy protokół (FTP, Gopher, NNTP, WAIS, Telnet, SMTP) wymagał:
  - innego oprogramowania do obsługi (klienta)
  - różnił się reprezentacją przechowywanych plików
  - wymagał zaangażowania ludzi
- pomysł - unifikacja poprzez WWW (nowy protokół HTTP)
- najważniejsze fakty z 9. letniej historii

1989 Tim Bernes-Lee z grupą fizyków z European Laboratory for Particle Physics (CERN) proponuje stworzenie nowego systemu
1990 powstaje nazwa WWW dla pierwszej implementacji na maszynach NeXT; HTTP i HTML
1990 grudzień - pierwsze wersję oprogramowania dostępne poza CERN
1992 styczeń - pierwsza tekstowa przeglądarka z CERN rozumiejąca HTML 2.0

WWW a protokoły TCP/IP; URL



URL
Uniform Resource Locator

nazwa maszyny ścieżka

`http://www.tele.pw.edu.pl:8000/www/przyklad.html`

protokół numer portu

MIME

Multipurpose Internet Mail Extensions

- typ pliku rozpoznawany po końcówce
- x dla eksperymentalnych typów MIME

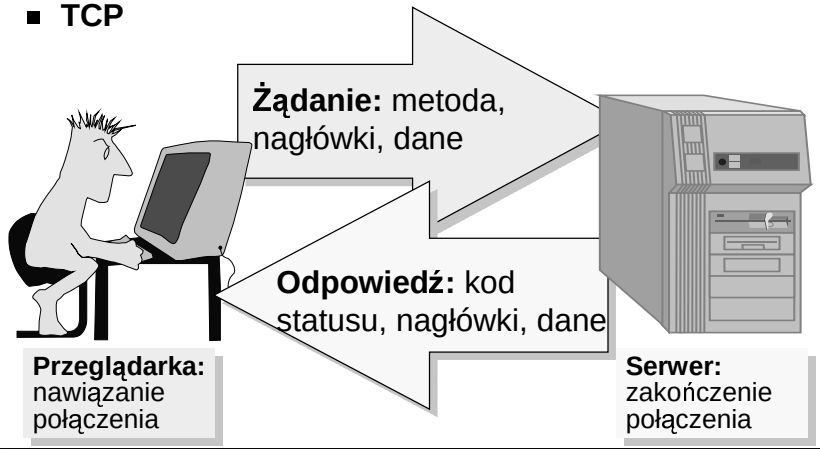
```
application/msword            message/news
application/news-message-id   message/rfc822
application/postscript
application/x-tex             multipart/alternative
application/zip               multipart/mixed

audio/basic                   text/html
audio/x-wav                   text/plain

image/gif                     video/mpeg
image/jpeg                    video/x-msvideo
```


Idea działania HTTP

- **HyperText Transfer Protocol** - wersja 1.0
- **TCP**



HTTP - żądania klienta

Żądanie: metoda

GET	pobierz zawartość danego dok.
HEAD	pobierz info. o nagłówku danego dok.
POST	potraktuj dokument tak jak skrypt - wyślij do niego dane
PUT	*zamień zawartość danego dokumentu*
DELETE	*skasuj dany dokument*

From	adres e-mail użytkownika
User-Agent	info. o przeglądarce
Accept	wspierane typy MIME
Accept-Encoding	wspierany typ kompresji
Referer	ostatnio wyświetlany URL
Authorization	kontrola dostępu
Charge-To	opłaty
If-Modified-Since	„tylko jeśli modyfikacja po”
Pragma	instrukcje wewn. serwera
Content-Length	długość danych w bajtach

Żądanie: nagłówki

HTTP - odpowiedź serwera cz.1/2

2xx	**sukces**
200	OK
202	Accepted
204	No response
3xx	**przekierowanie**
4xx	**błąd po stronie klienta**
400	Bad Request
403	Forbidden
404	Not Found
5xx	**bląd po stronie serwera**
500	Internal Error
501	Not Implemented

Odpowiedź: kod statusu

Przykłady

HTTP - odpowiedź serwera cz.2/2

Odpowiedź: nagłówki

Server	info. o serwerze
Date	aktualna data (czas GMT)
Last-Modified	ostatnia modyfikacja dokumentu
Expires	data ważności
URI	adres przekierowania
MIME-Version	wersja MIME
Content-Length	długość danych
Content-Type	typ danych
Content-Encoding	metoda kompresji
Content-Language	język dokumentu
Content-Transfer-Encoding	metoda kodowania (np. 7-bitowe, binarne)
WWW-Authenticate	kontrola dostępu
Message-Id	identyfikator wiadomości (tylko News)
Cost	koszt
Link	URL „ojca” dokumentu
Title	tytuł
Allowed	żadania żądającego użytk. mogą zostać wykonane
Public	żądania dowolnego użytk. mogą zostać wykonane

Przykład wymiany HTTP

```
>telnet www.tele.pw.edu.pl http
Trying 148.81.65.117
Connected to bach.tele.pw.edu.pl.
Escape character is '^]'.
GET /www/example.txt HTTP/1.0
From: lamer@any.site.pl
Accept: text/plain
Accept: text/html

HTTP/1.0 200 OK
Date: Monday, 2-Apr-98 12:34:56 GMT
Server: WebServer/1.0
MIME-version: 1.0
Last-modified: Sunday, 1-Apr-98 11:11:11 GMT
Content-length: 12

Udalo sie!

Connection closed by foreign host.
>
```

Przeglądarka:
1. nawiązanie połączenia

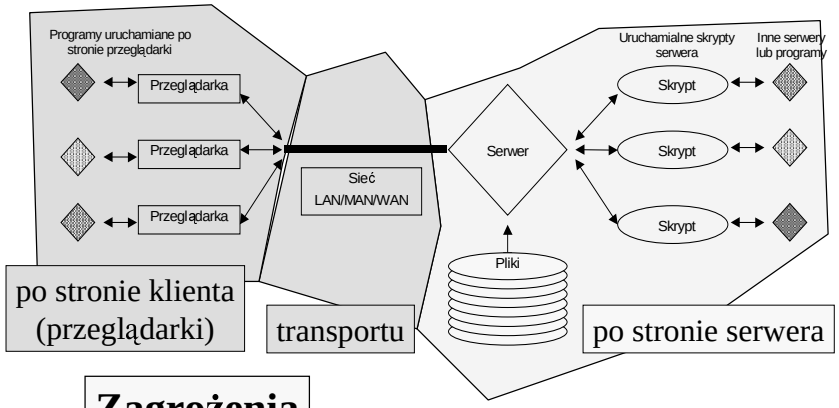
2. żądanie

Serwer:
3. odpowiedź

4. zakończenie połączenia

WWW - architektura usługowa. Zagrożenia

Obszary zabezpieczeń



Zagrożenia

S-HTTP/1.3 (Secure HTTP)

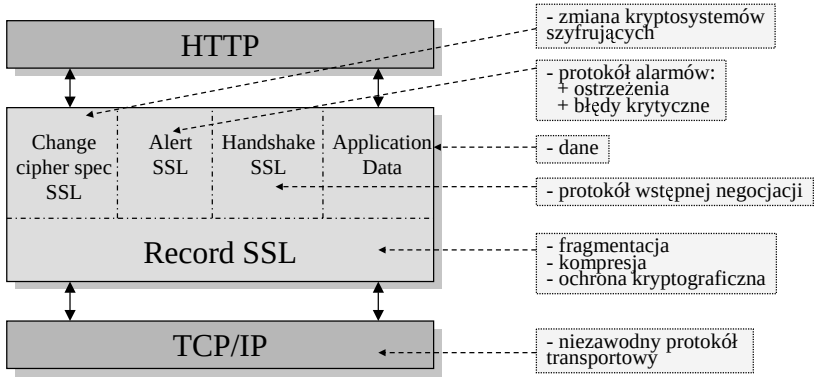
- 1995 - Enterprise Integration Technologies Corp. - E. Rescorola i A.Schiffman
- rozszerzenie HTTP
- shttp:// - ten sam port TCP co http://
- szyfrowanie, integralność (MAC), podpis cyfrowy
- żądanie: `Secure * Secure-HTTP/1.3`
- jedyna linia statusu: `Secure-HTTP/1.3 200 OK.`
- dwa typy nagłówków:
  - nagłówki ogólne - definiują zastosowane mech. ochrony informacji - nie chronione
  - nagłówki HTTP - chronione poprzez enkapsulację

SSL

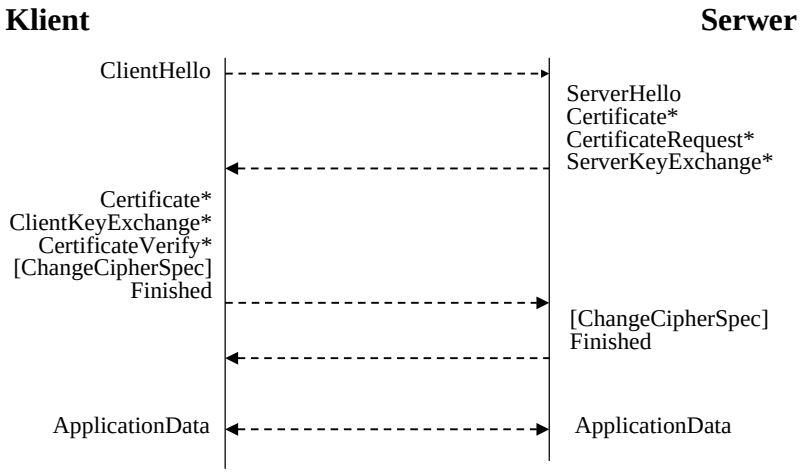
- Secure Sockets Layer - wersja 3.0
- Netscape Communications
- na popularność składa się:
  - proste tworzenie aplikacji, łatwość w użyciu
  - bezpieczeństwo (nie chroni jednak przed analizą ruchu)
  - biblioteki (public domain SSL - SSLeay, SSLava - Java)
- https:// - port TCP 443
- poufność, integralność, uwierzytelnienie
- ulepszenie wersji 2.0
- przyszłość: Transport Layer Security 1.0 draft IETF z 12.11.97 (ważny do 12.05.98)

`http://www.ietf.org/internet-drafts/draft-ietf-tls-protocol-05.txt`

SSL 3.0 - architektura



SSL 3.0 - Handshake SSL



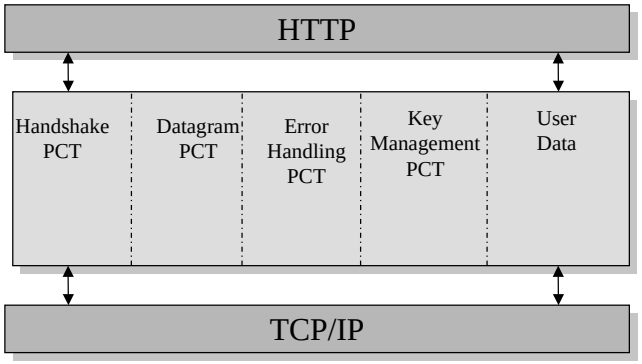
Najważniejsze problemy związane z SSL

wg. Paula Kochera

1. Obciążenie obliczeniowe klienta i serwera.
2. Dodatkowy ruch w sieci (handshake).
3. Trudna migracja w stronę systemu symetrycznego.
4. Nie współpracuję dobrze z istniejącymi tokenami kryptograficznymi (Kerberos).
5. Zarządzanie kluczami kosztowne (często wymaga hardware'u).
6. Wymaga urzędu ds. certyfikacji z określoną polityką.
7. Zaszyfrowane informacje nie dają się kompresować (modemy).
8. Międzynarodowe restrykcje na algorytmy kryptograficzne.

PCT v2.0

- Private Communication Technology
- 1995 - Microsoft - wersja 1.0
- mutacja SSL 2.0

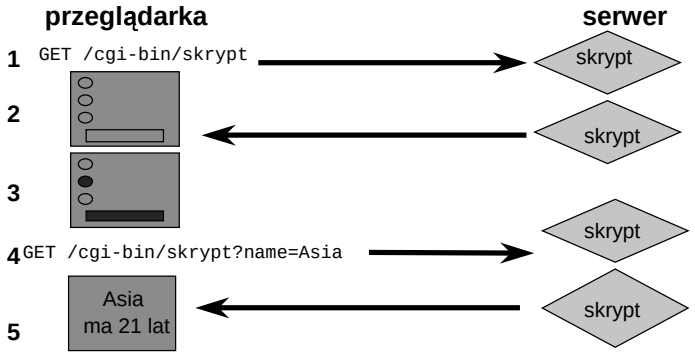


Bezpieczeństwo po stronie serwera

- „bezpieczna maszyna”
  - usunięcie zbędnych usług i użytkowników,
  - rozszerzone logowanie, aktualne łaty
- bezpieczny serwer HTTP
  - wybór bezpiecznego serwera (producent, produkt, wersja)
  - konfiguracja:
    - wyłączenie automatycznego listowania katalogów
    - wyłączenie Symbolic Link Following
    - katalogi użytkowników - szczególne restrykcje na symlinki i skrypty
    - skrypty: serwer uruchomiony z prawami „nobody”
    - anonimowe FTP bez możliwości zapisu
    - ograniczenie praw na plikach konfiguracyjnych
    - uruchomienie w środowisku chroot
    - zablokowanie odczytu plików access-log i error-log
    - kontrola dostępu na poziomie serwera
- bezpieczne skrypty
- anonimowość

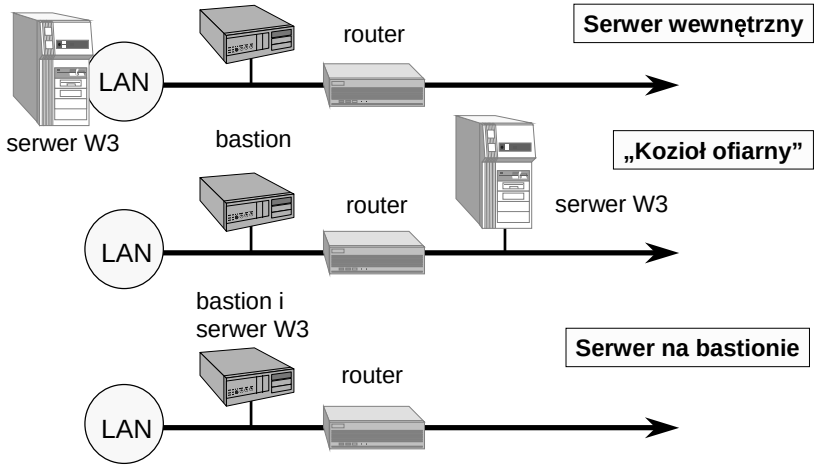
Bezpieczne CGI

Common Gateway Interface

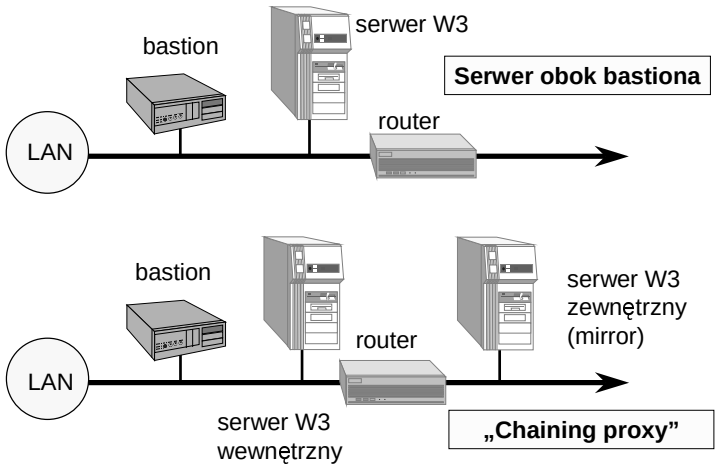


- wybór języka (Perl vs. C/C++)
- czego należy unikać pisząc programy?
- jak weryfikować „ściągnięte” skrypty?

Serwer WWW a firewalle cz.1/2



Serwer WWW a firewalle cz.2/2



Bezpieczeństwo po stronie przeglądarki

- prywatność żądań klienta
- problemy z:
  - Java (Sun)
  - JavaScript (Netscape)
  - ActiveX (Microsoft)
- inne błędy w implementacjach przeglądarek:
  - Microsoft Internet Explorer
  - Netscape Navigator

KONIEC

Czy mają Państwo pytania?

Krzysztof Szczypiorski, Piotr Kijewski
Instytut Telekomunikacji Politechniki Warszawskiej
e-mail: {K.Szczypiorski,P.Kijewski}@tele.pw.edu.pl