Bezpieczny serwer WWW

Grzegorz Wójcik
Instytut Automatyki i Informatyki Stosowanej
Politechniki Warszawskiej
e-mail: *G.Wojcik@ia.pw.edu.pl*

Podstawowe zagrożenia

1. Uzyskanie przez osoby niepowołane dostępu do prywatnych lub poufnych danych przechowywanych na serwerach WWW.
2. Przechwycenie tajnych informacji, które są przesyłane do serwera.
3. Wydobycie przez kogoś wiadomości na temat serwera, na którym działa WWW; wiedzy, która pozwoliłaby mu na wdarcie się do systemu.
4. Błędy w oprogramowaniu, które umożliwiłyby komuś z zewnątrz zniszczenie danych zawartych na serwerze.

Wybór serwera

- komputer i system operacyjny
- serwer WWW
- pozostałe oprogramowanie

Konfiguracja serwera

- ograniczenie usług sieciowych
- ograniczenie dostępu dla użytkowników
- niewielkie prawa dla serwera WWW

  `conf/httpd.conf:`

  ```
  User www
  Group www
  ```

- `chroot` ??

  `chroot /public/www /usr/local/http/httpd`

Potencjalnie groźne opcje serwera

- automatic directory listings
- symbolic link following
- Server Side Includes
- users home pages

Skrypty CGI

1. Skrypt CGI nie powinien udostępniać informacji, które mogłyby pozwolić innym na wdarcie się do systemu.
2. Skrypty CGI nie mogą dawać użytkownikowi możliwości wykonywania komend systemowych innych niż dokładnie określone przez cele działania skryptu.

Autoryzacja

- dostępu
- użytkownika
- serwera

Pliki konfiguracyjne:

- `conf/access.conf`
- `.htaccess`

Ograniczenie dostępu (nazwa + hasło)

```
<Directory /public/www/data/secret>
AuthUserFile /usr/local/http/conf/.htpasswd
AuthGroupFile /usr/local/http/conf/.htgroup
AuthName Top Secret
AuthType Basic

<Limit GET>
require group adm
</Limit>
</Directory>
```

Ograniczenie dostępu (domena)

```
<Directory /public/www/data/secret>
<Limit GET>
order allow, deny
allow from .ia.pw.edu.pl
deny from all
</Limit>
</Directory>
```


Secure HTTP

Eterprise Integration Technologies i NCSA

- rozszerzenie protokołu HTTP
- zastosowane mechanizmy ochrony bazują na RSA
- istnieje możliwość negocjacji pomiędzy serwerem a przeglądarką rodzaju zabezpieczeń
- protokół zapewnia nie tylko szyfrowanie, ale i możliwość elektronicznego „podpisania” przesyłanych danych

Secure Sockets Layer

Netscape Communications

- dodatkowa warstwa odpowiedzialna za szyfrowanie pomiędzy warstwą transportową (przesyłanie danych), a warstwą aplikacji (WWW, ftp, telnet)
- zastosowane mechanizmy ochrony bazują na RSA
- klucze o długości 40 bitów (cały świat) i 128 bitów (tylko USA)
- szeroka popularność