Vetrov A.N., Vetrov N.A., Kotova E.E.
RF, Saint-Petersburg city
“The international banking institute”
“The Saint-Petersburg state electrotechnical university "LETI"”

THE FEATURES OF SUPPORT OF THE INFORMATION SAFETY AT THE LEVEL OF APPLICATIONS IN THE ENVIRONMENT OF WWW WITH THE USE OF PHP

At the creating of the Web-applications it is often neglected by the providing of security. The information security covers a very wide range of problems and compels to watch for the latest achievements in this area. The system of security needs to be constantly supported, it can not simply be added to the project after, as it is completed and introduced. The providing of protection of the application in the environment “WWW” is the multi-aspect problem, which begins from the carrier,- a Web-server,- it is the literate providing of the mechanisms of patches and updates (both at the level of the environment of application, and at the level of the operating system), the strengthening of the server (instead of the service “Telnet” it is highly desirable to use its secure alternatives, for example “OpenSSH”,- it is potentially reduced the intensity of use of “FTP” and “Telnet” and etc.), the constant monitoring of the condition of server (the analysis of the technical log files of server and environment) and the information-awareness (the constant awareness as the basis of protection).

The questions of protection also include directly: the delimiting and analyzing of the rights of access to the directories “ServerRoot”, the prohibiting on the changing of the parameters of server and the protecting of the files of server:

```
# do not allow the access to the files outside of “DocumentRoot”
<Directory/>
AllowOwerride None
Options None
Order deny, allow
Deny from all
</Directory>
# allow the access to the files in “DocumentRoot”
<Directory “/usr/local/apache/htdocs”>
AllowOwerride None
Options Indexes FollowSymlinks
Order allow, deny
Allow from all
</Directory>
# the providing to the each group of applications the own environment
UserDir disabled
UserDir enabled alice bob
UserDir public_html
<Directory “/home/public_html”>
AllowOverride None
Options Includes NOEXEC SymbLinksIfOwnerMatch
Order allow, deny
Allow from all
</Directory>
UserDir disabled root
```

The control of the inclusions on the side of server “SSI” (the own restrictions for the each application, for example,- “Apache” has the parameter “IncludeNOEXEC”, which allows “SSL”, but forbids the users to run from them the programs or scenarios of “CGI”).

The allowing on the execution of the scenarios “CGI” only from the certain location (can be forbidden the execution of “CGI”, allowing at the same time to execute the scenarios “PHP”).

(it was submitted to “IBI” on the int. conf. “APE and NTT (SR)” of “IHEAS”, the 11th-13th of March 2004 y.)

The placement of the analyzer "PHP" outside the hierarchy of directories of the Web-server (it is excluded the possibility of parasitic abuse by the analyzer).

The identification and authentication of the user with the help of "PHP" (realized by the classical principle "request-response"). Although the realization of identification by means of "PHP" is somewhat more difficult, but the positive results are worth the made efforts.

To the key advantages of this way of authentication should be attributed: it cannot be canceled (the user can "unregister", what is achievable in the merging with "Apache",- the so-called controlled rollback of the transaction on the any stage of registration); at it also can be entered the term of validity (it is provided the resource-saving and the automation of monitoring of the account records,- the registration automatically becomes invalidated on the expiration of the certain interval of time); it can be adjusted (limit only the level of skill and imagination, and also the developer completely controls by the process of authentication); in the basis of authentication is provided the connection of databases (it is possible to conduct the full accounting of actions of the users and to use any data); it is the transactional-iterative with the various levels (the technological solutions for the each separate object, and also the high degree of flexibility and reliability); besides to the authentication it is provided the capability of registration (the high degree of automation of the control of the account records and the analysis of behavior of the user, which is given the capability to register); it is fully supported the program "CGI" (the universal capabilities of interface exchange between the applications): the possibility of realization of the checking and accounting of IP-addresses (although this sometimes does not have the proper effect); the use of cryptography (the encryption of data and the creation of checksums or digests for the recovery of information); the use of encryption (the use and realization of the algorithms, providing the work with the open and closed keys, and also the creation and exchange of certificates); the using of the hash-functions (often used for the storing of passwords and the identifying of some fragments of the data); the application of the mechanism "suEXEC" in "Apache" (the setting of the certain limits on the period of time of the execution of application); the providing of security of the scenarios of "PHP" (the minimization of risk at the startup); the reliability of applications, the storage and forwarding of confidential information (the protection of software from the involuntary use from the outside); the analysis of data of the user (the excluding of possibility of the transmission of dubious information and the undesirable control constructions in the composition of input data).

At the creating of the applications for "WWW" it is often neglected by the providing of security,- this is explained due to the fact, that the security is difficult to measure quantitively, and for the ordinary visitors of the resource (site) it remains invisible. For the literate users the gaps in the system of security are easily founded out, and at the same time the consequences can be the most unpredictable, as a rule, the catastrophic consequences.

Do You whether trust the confidential information to those, who are not in a condition to provide it confidentiality?

(it was submitted to "IBI" on the int. conf. "APE and NTT (SR)" of "IHEAS", the 11th-13th of March 2004 y.)