Specific Problems of User Identification Methods Implementation in Web-applications

Oldřich Horák

***Abstract*—**This article describes problems of user identification methods implementation in web-applications. The implementation costs are accentuated as the condition of these methods comparison. At the beginning, some specific issues of user identification are discussed due to features of front-end applications and application protocols used in background connection. The identification method implementation costs are meant as a part of the TCO, and the term of "Addition Implementation Costs" is defined closely. Some tips and techniques are accentuated to use for undesirable multi-user issue detection and avoidance in the relation to the user policy and conditions of the given application. The usability is discussed across common web-application in comparison to special application such as public administration systems or geographic information systems.

***Keywords*—**GeoWeb, Identification methods, Implementation costs, Information system, User identification, Web-application

I. Introduction

THE usability of information systems depends on many features. One of these features is a user-friendly environment with a simple user interface. In present, modern systems use thin clients realized as web page or web-site presented via browser, and the robust system backend running on powerful server hardware. This configuration forms the "web-application" as a common information system design.

Most of the information systems need a basic user access control subsystem at least. The access control subsystem can be designed for different security levels. It depends on the target application purpose and security measurements suitable for the owner of the information system.

The information system designed as the web-application deals with specific environment of the worldwide web rules and conditions. In general, the web is unsecured. Many issues and threats can encounter the information system in the form of the web-application. Designers are responsible for sufficient solution of such situations.

Some systems providing the user interface in the form of web-applications deal with the undesirable multi-user issue. Social networks or so-called browser games are sensitive to this problem. The only one user account per person is expected to use in these systems, and the ability to detect such rule violation is very important. No certain way to solve this task is used to use in general, but features of some identification methods are usable to support such solution.

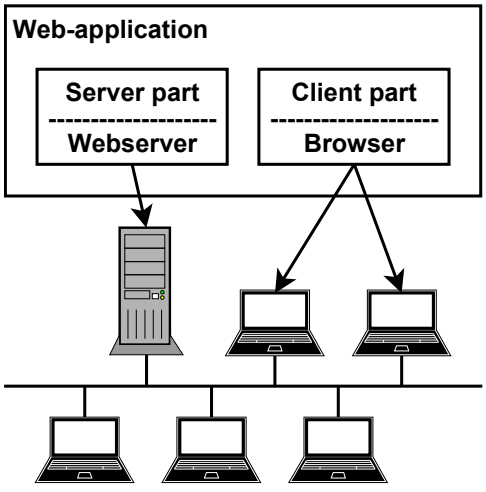
Each one solution depends on the security demands of the information provided by the system. Some systems need to distinguish the separate identities of their users, the user's accounts uniqueness is important for others. In general, each one needs to assign an access rights to provided information by the user or user-group identity. In the web environment, the process of user identification is more difficult.

II. Web-application Architecture

A web-application consists of two basic part overall. As a network application it has a server part and one or more client parts (client/server architecture). "*If we look at the client-server model in detail, we see that two processes are involved, one on the client machine and one on the server machine.* [1]"

The server part is commonly found as a running service of a dedicated network server. The client part can be found on workstations as an application used to browse through the worldwide web service (web-browser), see Fig. 1.

Some types of web-application are based on frameworks providing component integration. Such components can be distributed and/or heterogeneous. Their services often act as a separate network application with their own client-to-server communication. [2]



Manuscript received October 17, 2010. This work was supported in part by the Grant Agency of the Czech Republic under Grant project no. 402/09/0219, and in part by the Student Grant Agency of University of Pardubice.

Oldřich Horák is with the Institute of System Engineering and Informatics, Faculty of Economics and Administration, University of Pardubice, Czech Republic (e-mail: oldrich.horak@upce.cz).

Fig. 1 Web-application Architecture

Client-to-server connection is realized by unsecured (HTTP) or secured (HTTPS) protocol going over transport protocol (TCP). The common data format transmitted between server and client part is hypertext. Server part also provides other file types transmission including graphics and multimedia.

Other file type transports from client part to server is unhandy and only way to realize it is the interactive upload service provided by form HTML element. By this reason, any file transport from client to server is problematic, and it requires user's effort. [3]

The capabilities of modern web-design techniques can be used for better presentation of the web content (i.e. Web 2.0 [4], etc.), but the client-to-server data transmission still remain limited.

Another way to transport more data from client to server is provided by integrated components in the form of embedded objects. But, such solutions lead to more security problems based on bad knowledge of the 3rd-party components internal design. [2]

A specific attention must be focused on the application security. Fig. 2 illustrates various possible attacks on the web-application. The points of the possible vulnerability also are demonstrated, so it can be seen where they happen.

III. Identification Methods Overview

The usage of user identification is various, but two main purposes are commonly used. The first one is used for monitoring of individual user's activity, usually without user's knowledge about the monitoring. Other one is used for authentication. In this case user's cooperation with the system can be necessary, and user's identification can be cognizant.

A special purpose is the capability of disclosing false user accounts created by robots or viruses. The importance of this task increases nowadays. Such accounts are often used to illegal activities, i.e. social engineering.

Children and adolescents use the social networks most frequently, and the communication using Internet is their nature [5, 6]. Members of this social group are most endangered by some illegal activities in the Internet. The false identity created in the social network environment could be misused to some criminal acts. "*For example, there are many cases where people take advantage of these social media to involve in activities that lead to crime cases.* [7]" The right user identification can prevent this kind of acts.

Three groups of identification method exist. First, user can be identified by some unique knowledge. Typical case is using of a password. Next group includes methods based on ownership of some unique item, typically a token or a thing. The methods of the third group are based on some specific feature (mainly body feature) of given user as some unique biometrics parameters.

A. Knowledge Oriented Methods

These methods are based on user knowledge of given fact, i.e. username and the corresponding password. For user

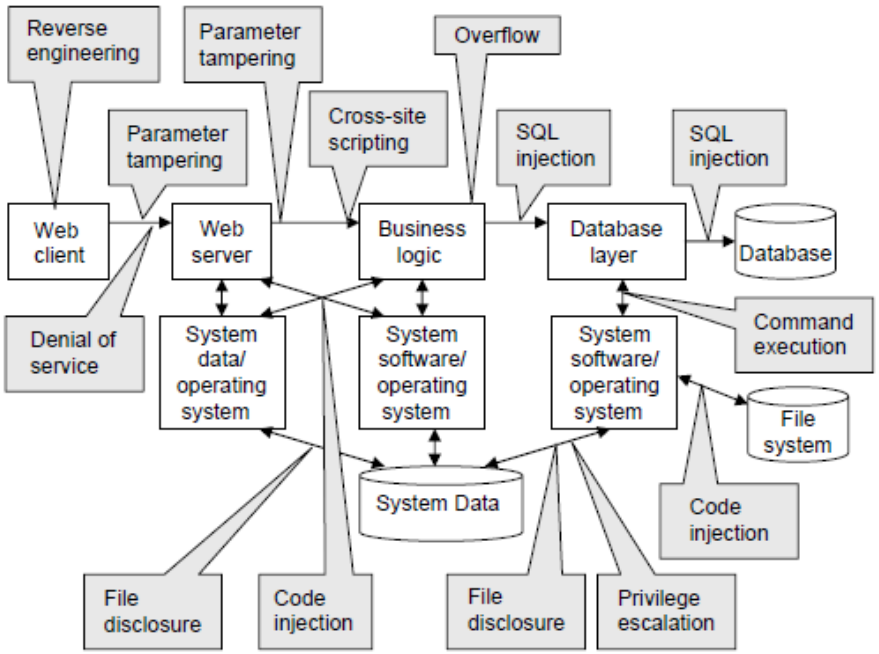


Fig. 2 Points of Vulnerability for a Web-application [3]

identification by this method a unique username is required. But, the username and password can be accidentally disclosed, and the security of the identification fails.

Some form of shared or pre-shared password or pass-phrase without the username can't be used for sufficient user identification, because more users could use the shared password to be accepted by a system. Such form of identification can be used for access into shared environment, i.e. a course of e-learning system, where is sufficient to distinguish between given groups of users only.

B. Ownership Oriented Methods

All the methods based on ownership of some item are inappropriate for secure user identification, when the owned item can be passed to other user or can be stolen. The improper user can be identified in this case, because of ownership of foreign identification item. Additional measures must be realized to avoid this situation.

C. Biometrics Methods

Specific parameters of human body or user's specific behavior can be used for user identification. Many biometrics methods depend on special techniques or complicated equipment is needed for such body or behavior features extraction. However, some methods can be realized using common computer accessories or peripheral.

IV. Identification Methods Usability

The usability of identification method depends on several basic conditions or features of the target system. Each method requires other type of features extraction, and each system requires other form of feature transmission across its infrastructure.

A. Network System Specific Conditions

The common feature of the network architecture designed systems is user remote access. An identification feature transport across the network can be slightly difficult there.

First, the amount of the information used for the identification can be bigger in many cases. A transport capability problem originates by this reason. The second problem springs from security issue, because to keep the identification feature safe is necessary. Third, the question of technological capability to gain the information by the client part from the user can be fundamental at several methods.

A qualified decision about whether to extract basic features from identification information by server or by client part must be done. It depends on used transport technology and on network application type.

The next problem originates from technical requirements. Some methods require sophisticated reading equipment that can be more expensive than others. It makes some methods unusable for network environment because each one client has to have its own expensive reader. It's the disadvantage of some ownership-oriented and biometrics methods especially, so these can be used only by systems where the client count is limited.

B. Web-application Specific Conditions

The influence of conditions described above is stronger when using web-application environment. The transport is very limited by the protocol specification that is why only a small amount of data can be transmitted from the client to server part. The need of a quick identification is evident, so the transport speed has to be sufficient.

The basic application protocol used to hypertext transport (HTTP) is unsecured that is why it is not well usable for identification features transmission. The secured form (HTTPS) provides secured sockets layer (SSL) capability to encapsulate that transport into an encrypted stream, see Fig. 3. It increases the communication security and enables to keep the secret data safe. But, the encapsulation consumes some system and connection resources, such as computing time or transfer capacity.

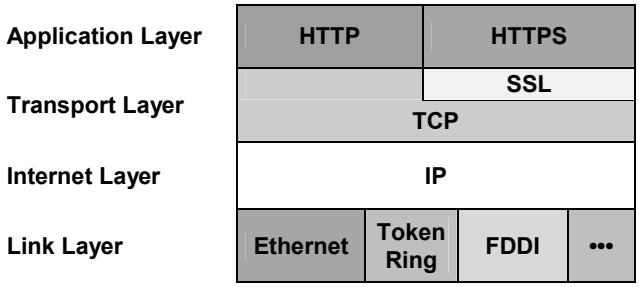


Fig. 3 HTTP and HTTPS in TCP/IP stack

Other security issue is connected with processing of the identification data obtaining or feature extraction. Basic technologies providing a scripting capability of the server or client part aren't designed to be usable securely. The main problem rising from the insufficient security of scripting is on the client side.

The client part of the web-application is in general realized by web-browsers. Scripting support is limited to a few scripting languages only (JavaScript, VBScript) with many incompatibility issues between browsers. Along with them none security questions are solved, because the source code of the web page and other resources linked in are viewable and can be inspect by the browser additions as a plain text. Some compiled additions (i.e. Java-applets) can be decompiled easily by free utilities, so the security is out of the question. [8]

C. Identification Usage Specific Conditions

More conditions lead from the usage of user identification. If the identification is used for statistical monitoring of user behavior, the system needs to distinguish between users, but the knowledge of their identity is not necessary. The access control management system usually needs the user identity knowledge.

In the web-application environment the tracking cookie

method can be used for the individual user identification. This cookie-based user identification requires the web server's and web-application access log analyzes. "*For tracking the users' behavior the log files are extended with cookies and some other fields as well. Cookies are the most common way of client side data storing, ...* [9]"

V. Examples of Web-application

The common web-application characteristics are described above. Special features and task solutions are needed by application focused on private or secret information processing and providing. Following examples are introduced for the demonstration and better explanation of the web-applications diversity and variety:

A. Public Administration Systems

This group of information systems includes various types of applications used to provide public or private citizen or property data. A part of information can be provided as public data (some registrars, business identification data, etc.). The access to other part of information needs to be regulated by some rules (private or sensitive data, criminal record, penal register, etc.).

The grant of the access to provided data is based on either user identity or user's membership to a group. The user's behavior monitoring can be used for a better usability of the web-application. The system can predicate the next step of the user's way across the web site, and offer direct links to related data. Some system can provide direct or indirect web-application personalization.

B. Remote Health Records Systems and Databases

Patient health records are very private data, so the security measures are really very important. Management of such records is processed by centralized systems nowadays. The remote access is the common way to read and/or write patient health records. Health care professionals in medical centers or hospitals to be able to provide the medical care and diagnostics quickly and effectively use such systems. [10]

The remote access across the worldwide connection requires implementation of the best user identification method, and the reliability of the chosen method must be high. The costs of implementation play the second role in this case, because the security is most important.

C. Web-based Games

The web-based games (also web-games, online-games, and browser-games) are web-applications providing ability of multiplayer network game, where the clients interface is realized by the web browser. These games often have the background of some social network infrastructure with many elements creating a virtual world or virtual space. Some games have features of war and/or economic simulators including many social and economic relations among players, rather among player's virtual profiles. The range of player's ages can be various. [11, 12]

The main problem related to user identification in these applications is multi-account issue. The owning of more than one account by one player is mostly strictly prohibited, because it leads to undesirable advantage for the owner of more than one user profile account. Providers of these games spend many resources on the security measures against multi-account owners. The appropriate user identification methods can help them to avoid these issues.

D. Geographic Information Systems

The geographic information systems often provide the information with web-based interface as GeoWeb sites. The management of user access uses the same principles as described in previous paragraph. But, the GeoWeb often displays data from different servers with different access rules. The access management needs to be solved not only for the entire web-application, but for the individual layers of the map service.

VI. Motivation for GeoWeb User Identification

As it was described above, the GeoWeb sites can use data from more backend systems and servers, with various types of security level and access rules. It is the motivation for user identification. The GeoWeb site has to distinguish individual users or users group to allow or deny access to some specific map-layers or geo-information. It is important on systems used for tasks as *Emergency action plan*, *Evacuation plan and procedure during floods*, or *Critical infrastructure and key resources*.

A. Geographic Information Systems Architecture

If the GIS provide a GeoWeb interface, it has the form of the typical client/server application with the three basic layers:

Data layer can be provided by the given server, but some data can be dynamically loaded or linked from another server or public services across the local network or Internet.

Application layer has to process the user requests and provide appropriate responses. This task is typically divided to be processed partly by server and by client side of the system.

Presentation layer is the user interface used to collect the request and to visualize the response. [13]

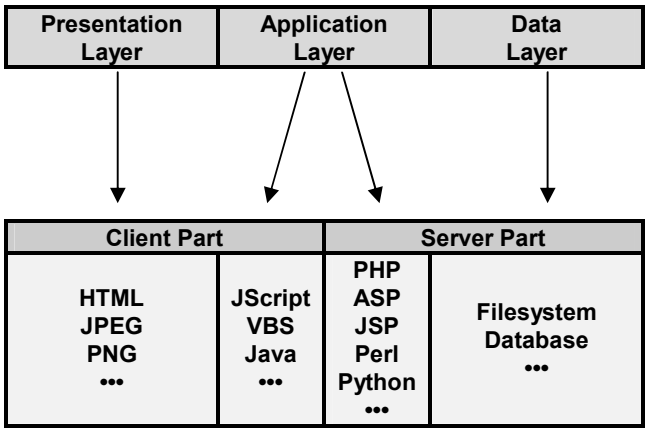


Fig. 4 Web-application Implementation

For a better web-application implementation overview see Fig. 4. Client part is realized by web-browser. There the hypertext and images are presented to the user. A dynamic functionality at the client side is provided by client-side scripting tools and languages, i.e. JavaScript, Visual Basic Script, Java Applets, etc. These procedures fall under the application logic. Rest of the application layer is processed server-side, and provided by common web-server enhanced by scripting capabilities of PHP, ASP, JSP, or other programming languages and techniques. The server part provides the data layer functionality using simple filesystem and storage, or more sophisticated solution based on some intelligent database services. The object-oriented databases with many objects' characteristics and relations are often used nowadays.

B. Geographic Information Systems User Groups

The GIS provided as web-application have some user groups with various relations to the presented data. Each one user group needs a different access to have granted. Because the GIS application can be able to analyze some information on demand, the user access has to be solved not only as the "data access", but the solution has to be able to manage access to run these analyzes. There are these user groups:

High-end users – some specialists with access to run a high time or system resources consumption tasks, i.e. spatial analyses, etc.

Regular end-users – employees or regular customers, etc., with access to only several functions or data.

Casual end-users – citizens or common guests of the web-application with access to only some analyses results or public data. [14]

VII. User Identification Method Costs

Costs of the user identification method can be defined from two main points of view. First, we can express the costs of the solution implementation. It means all the resources spent on the changes extending the application to be able to provide the given user identification method.

Second, we can evaluate the costs of the solution processing and providing. So it means the resources consumed in relation with the user identification method service running. The general cost value is expressed by some combination of these two viewpoints.

If we need to add the user identification functionality to web-application, the costs of this addition will be the matter of the user identification method choice. For this purpose the costs of addition needs to be evaluated. The cardinal evaluation is more difficult and can be used to express the absolute financial costs. In many cases the ordinal evaluation is sufficient. It provides only the pseudo-values usable for the methods implementation costs comparison. These additional system upgrade costs can be expressed as a total of these values:

σ – server side addition implementation costs
κ – client side addition implementation costs
τ – data transmission addition implementation costs

Each one of these values consists of three parts. First, there are hardware costs. It means the value of the hardware components that are added to given system part (server, client or transmission circuit) for the user identification process needing. Most of the methods do not need additional server side hardware, but some client side hardware can be necessary.

Second part of the value represents the software costs, that is the value of additional software needed to user identification feature of the system. The maintenance of the software is included in this value. For details see Fig. 5:

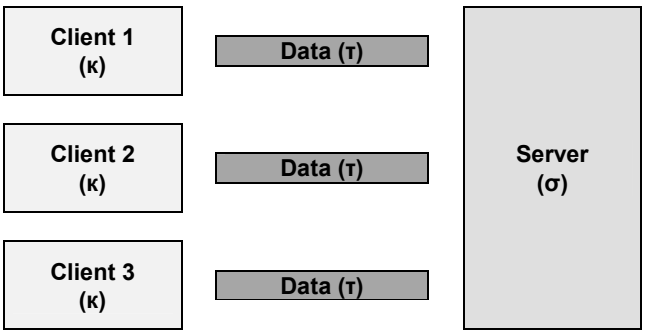


Fig. 5 Identification Method Implementation Costs

Last value depends on the computing time when system processes the user identification. The costs of this time can be most important in some critical applications.

A. Server Side Costs

σ_{HW} – server side hardware costs are low or none for most user identification methods.

σ_{SW} – server side software costs are very dependent on type of method; if the data processes the server side, there is only one instance of the server software, but more data needs to be transmitted from clients.

σ_{I} – server side identification costs depends on the identification process.

B. Client Side Costs

κ_{HW} – client side hardware costs are low or none for some methods, but for others can be very high.

κ_{SW} – client side software costs depends on the element processing collected data; if this process is provided by server part, no more client software addition needed, and this costs go to zero, but the client side data processing increases the costs with each one new client requesting to add some software instance in most cases licensed and expensive.

κ_{I} – client side identification costs depends on the used method and the way of processing.

C. Data Transmission Costs

τ_{HW} – data transmission hardware costs are none or very low, if the Internet is used as the transmission media; the system designer can not modify the infrastructure, excluding of usage in private network environment.

τ_{SW} – data transmission software costs explanation is similar to above described τ_{HW}.

τ_{I} – data transmission identification costs depend on the amount of data the system transmits from client to server side; if there are used some method with identification processing located in the server part, the amount of data to transmit can be high.

The generic evaluation of implementation costs can be expressed by equation (1) where the value ***TIC*** means *Total Implementation Costs*:

$$TIC = N_{\sigma} \cdot \sigma + N_{\kappa} \cdot \kappa + N_{\tau} \cdot \tau \tag{1}$$

The parameters ***N*** mean number of servers, clients and transmission links. So, if N_{σ} is equal to 3, it means there are three servers to implement the identification method addition. The N_{κ} is the number of clients to be enhanced by the identification addition. Most of the systems are single-server. It means the value of N_{σ} is one. If the hardware costs needed to be evaluated, the expression (2) will be used. Similarly for the software costs (3) and per identification costs (4):

$$TIC_{HW} = N_{\sigma} \cdot \sigma_{HW} + N_{\kappa} \cdot \kappa_{HW} + N_{\tau} \cdot \tau_{HW} \tag{2}$$

$$TIC_{SW} = N_{\sigma} \cdot \sigma_{SW} + N_{\kappa} \cdot \kappa_{SW} + N_{\tau} \cdot \tau_{SW} \tag{3}$$

$$TIC_{I} = N_{\sigma} \cdot \sigma_{I} + N_{\kappa} \cdot \kappa_{I} + N_{\tau} \cdot \tau_{I} \tag{4}$$

We can use a matrix expression for the better form of evaluation. The unit costs matrix ***UC*** includes the nine values of the basic coefficient (5). The number of servers, clients, and transmission links to be adapted is expressed by the vector N in equation (6):

$$UC = \begin{pmatrix} \sigma_{HW} & \kappa_{HW} & \tau_{HW} \\ \sigma_{SW} & \kappa_{SW} & \tau_{SW} \\ \sigma_{I} & \kappa_{I} & \tau_{I} \end{pmatrix} \tag{5}$$

$$N = \begin{pmatrix} N_{\sigma} & N_{\kappa} & N_{\tau} \end{pmatrix} \tag{6}$$

The values of ***TIC*** component (7) will be evaluated by expression (8):

$$TIC = \begin{pmatrix} TIC_{HW} & TIC_{SW} & TIC_{I} \end{pmatrix} \tag{7}$$

$$TIC = N \cdot UC^{T} \tag{8}$$

All the matrix expressions can be used for the better view of evaluation of the user identification methods implementation costs in future work.

VIII. Identification Method Costs Comparison

The comparison by the costs is one of the important parts of the decision what user identification method use. In this point is necessary to say that the weight of this criterion may be very different in dependency on the web-application usage. For the example of comparison see Table I. Some identification method implementation costs are compared by pseudo-values **none**, **low** and **high**, because the real costs are not evaluable directly in general case.

TABLE I
User Identification Method Costs Comparison Example

Method	Server side			Client side			Data transmisson		
	σ_{HW}	σ_{SW}	σ_{I}	κ_{HW}	κ_{SW}	κ_{I}	τ_{HW}	τ_{SW}	τ_{I}
Password	none	low	low	none	none	none	none	none	low
ID Card	none	low	low	high	low	low	none	none	low
Fingerprint	none	high	high	high	high	low	none	none	high
Hand metrics	none	low	high	high	high	low	none	none	low
Speaker recognition	none	high	high	low	low	high	none	none	high

If we set a weight for these criteria, the result will be expressed as the sum of pseudo-costs (1), (2) to (4). The client side hardware and software costs have to be multiplicated by the count of clients. All the per-identification costs must be multiplicated by expected identification processes in the calculated period.

This example displays the password method as the low costs way. There are none client side and data transmission costs. The value of κ_{HW} is important for web-application, because of many clients in such system expected. Other method with none client side hardware costs is speaker recognition. Each one new personal computer includes sound interface with or without microphone (if none, it is cheap to buy it) today. It is sufficient hardware for speaker recognition processing. But, if the client side processing of the audio signal is needed, the client side software will be expensive. If the audio signal is transmitter to be processed server sides, more costs for the transmission will be expected.

The use of pseudo-values is not available in the case of general ***TIC*** evaluation, because there are not defined how many values “low” in total reach the value meant as “high”.

But, if we defined the weights of “low” and “high” in some units, the matrix evaluation would be usable very simply and correctly. The better way for this evaluation to be used is to express the coefficients in money. The approximate values are

sufficient in the order evaluation.

IX. Identification Method Reliability Problem

The reliability of some identification methods is the important problem of the general use. There are two weak points in the identification task processing. First, some methods enable the matter of identification to be stolen. It means the access can be granted to person who identifies him/herself by stolen password or token. The system evaluates it as the right identification in error. Second, some methods can not recognize the identification features with the success always. It leads to situation, when the right identification is evaluated as wrong and the access is not granted. Several biometrics methods have this problem. Repeated identification process can solve the issue in several cases. Some examples of identification methods weaknesses are introduced below in the Table II.

TABLE II
User Identification Method Weakness Example

Method	Weaknesses
Password	Can be forgotten or disclosed
ID Card	Can be stolen or unreadable
ID Token	Can be stolen
Fingerprint	Can be unreadable if injured
Eye identification	Can be unreadable in specific condition
Hand metrics	Can be inaccurate
Keyboard dynamics	Can be inaccurate or imitated
Speaker recognition	Can be inaccurate in specific condition

More identification methods can be combined to avoid the reliability inconvenience. It increases the user identification method implementation costs. These costs evaluation is rather difficult, and expects more specific values to be set. The identification method reliability has to be included in the criteria of methods comparison. Other way is to compare the more methods combination (with sufficient reliability) as the one option.

The weight of the reliability problem also depends on the purpose of the user identification. If the identification do not serve for granting of access, but for statistics or monitoring only, the decreased reliability can be covered by some statistic errors.

X. Conclusion and Future Work

The usability of user identification in the web-application environment is the complex problem. The common task of user identification by information system is limited by the specific conditions and rules of the web environment and communication across the Internet.

The special focus of GeoWeb applications leads to more specific rules and needing given by various tasks of such systems. More users and user groups access levels and the security reasons of the provided information make the solution more difficult.

The decision what identification method select for concrete usage depends on the costs of that solution. At the other hand the usability of identification method depends on more characteristics such reliability and success ability. This problem can be eliminated by use of combination of two or more methods, but it may lead to more additional costs.

The future work is to elaborate more precisely the evaluation and comparison of identification methods. Inclusion of the reliability in described evaluation model is necessary, because the costs can not be the only criterion for the decision.

Some identification methods need to be tested in this specific environment with the focus given to the client side implementation. The server side can be modified or upgraded easily, but the thousands of user's browsers used as client sides, can not be modified above the options of the web and hypertext standards.

Acknowledgment

This work was supported in part by the Grant Agency of the Czech Republic under Grant project no. 402/09/0219, and in part by the Student Grant Agency of University of Pardubice.

References

[1] A. S. Tanenbaum, *Computer networks*. 4th edition. Upper Saddle River, Pearson Education, 2003, p. 4.

[2] R. A. Wasniowski, " Component integration for web based applications," in *Proceedings of the 4th WSEAS international Conference on Software Engineering, Parallel & Distributed Systems*, pp 1-5, 2005.

[3] A. S. Tanenbaum, *Computer networks*. 4th edition. Upper Saddle River, Pearson Education, 2003, ch. 7.3.1.

[4] N. Vlahovic, "Web 2.0 and its Impact on Information Extraction Practices" in *Proceedings of the International Conference on Applied Computer Science*, pp. 574-579, 2010.

[5] M. Žumárová, M. Černá, and V. Maněna, "Young Generation and their Internet Communication" in *Proceedings of the International Conference on Applied Computer Science*, pp. 313-316, 2010.

[6] L. Stašová, G. Slaninová, and M. Žumárová, "Internet social networks in the contemporary adolescents lives" in *Proceedings of the International Conference on Applied Computer Science*, pp. 279-284, 2010.

[7] S. Z. Z. Abidin et al., "Socio-Informatics: Identifying Influential Factors in Digital Elements," in *Latest Trends on Computers (Volume I), Proceedings of the 14th WSEAS International Conference on COMPUTERS*, vol. I, pp. 397-402, 2010.

[8] A. K. Talukder and M. Chaitanya; *Architecting secure software systems.* Taylor & Francis Group, LLC, 2009, ch. 8.

[9] R. Ivancsy and S. Juhasz, "Analysis of Web User Identification Methods," in *World Academy of Science, Engineering and Technology*, vol. 34, pp. 338-345, 2007,
Available: http://www.waset.org/journals/waset/v34/v34-59.pdf

[10] G. Triantafyllou et al., "A Web based Telemedicine Portal for centralized access to Patient Health Records," in *Proceedings of the 5th WSEAS International Conference on Multimedia, Internet and Video-Technologies*, pp. 186-191, 2005.

[11] H. Chang, "A study of Multimedia Systems based Knowledge Community for a type of Web Game," in *Proceedings of the 9th WSEAS International Conference on Multimedia Systems & Signal Processing*, pp. 85-90, 2009.

[12] C. Lee and S. Han, "Development of the Scale for Diagnosing Online Game Addiction," in *Proceedings of the 3rd WSEAS/IASME International Conference on Educational Technologies*, pp. 362-397, 2007.

[13] J. Komarkova, O. Visek, and M. Novak, "Heuristic Evaluation of Usability of GeoWeb Sites," Lecture Notes in Computer Science, vol. 4857, pp. 264-278, 2007.

[14] J. Komarkova et al., "Usability of GeoWeb Sites: Case Study of Czech Regional Authorities Web Sites," Lecture Notes in Computer Science, vol. 4439, pp. 411-423, 2007.

Oldřich Horák was born in Vrchlabí, Czech Republic in 1973. His educational background: the bachelor degree (Bc.) in Applied Informatics (2004), the master degree (Ing.) in Information Management (2006), both at Faculty of Informatics and Management, Univerzity of Hradec Králové, Czech Republic; he is a student of doctoral study programme in Systems Engineering and Informatics, Informatics in Public Administration at Faculty of Economics and Public Administration, University of Pardubice, Czech Republic.

He worked in informatics and accounting department of house of correction "Husův domov" in Dvůr Králové nad Labem, Czech Republic (1993-1997), and as a secondary school teacher of computer networks, programming, and accounting at SPS in Dvůr Králové nad Labem, Czech Republic (1997-2004). Now he is a lecturer at Institute of System Engineering and Informatics, Faculty of Economics and Public Administration, University of Pardubice, Czech Republic.