

Web-based Authentication Technique for Systems without database Server

BARMPOUTIS J. ANGELOS
Informatics Department, School of Science
Aristotle University of Thessaloniki
angelbar@csd.auth.gr

Abstract: - Server based authentication techniques are widely used by many software companies in order access to a software product to be controlled. One database server, which answers queries from a software product about password verification, is required. If the product has users from all over the world, there must be more than one server available, for example one for each continent. That is, staff required, branches required, foreign offices required and of course funds are required. This is untenable for small software companies and it is very risky for bigger companies. In this paper a web-based authentication technique for software products without a database server is presented, which could be used by small companies for their products, because it offers a quick and chip world wide authentication web-based system (Figure 2). [1]

Key-Words: - Authentication, web-based, web services, server, database, access, e-commerce, username, Psifiak

1 Introduction

It is known that a very common authentication technique is the unique registry code for a specific username. To be more precise, every user sets a username and then a unique registry code is required for the completion of the registration procedure. This is an algorithmic technique and no database is needed. (Figure 1a)

On the other hand, a common authentication technique is the opening of a user account. According to this technique there is a database, and every user has a username and a password. There isn't any algorithm for password generation, but a database is needed. (Figure 1b)

In this paper a web-based authentication technique for software products without a database server is presented, which is a combination of the above techniques. It will be shown that the structure of this technique is based to a few web-placed files, which are controlled intermittently by the system administrator. These files are encoded and contain database records and variables, which are analyzed on (2). The software product decodes these files in order to verify the username-PIN* combination of a user, who wants to have an access. (Figure 1c)

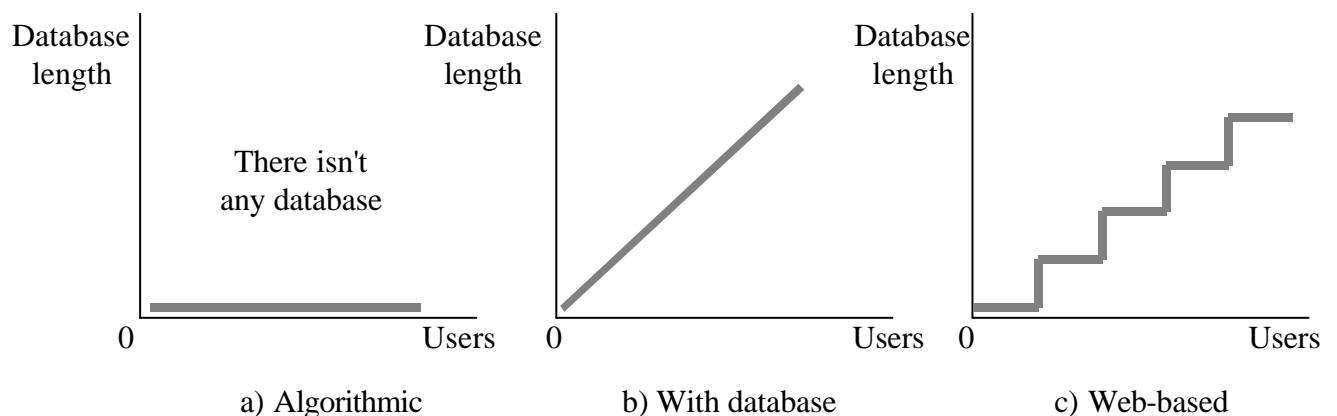


Fig.1: Database length / Users diagrams

2 Topic Description & Analysis

According to this web-based technique, there is a PIN generator algorithm, which uses one of the web-placed files to generate a number with few digits for each username string of characters. This algorithm remains stable, but the

* PIN: Password Identity Number

related input web-file is changed intermittently. That means that correspondence between username strings and PIN number is changed, when the related input web-file is also changed. While the correspondence between username strings and PIN number remains stable, software product uses the generator algorithm for access verification.

$$\text{PIN} \leftarrow \text{Generator}(\text{username string}, \text{variables from web-file})$$

If the software product is a free web service or a trial version of a software system, usually there is a web license form, which is filled by a new user. After the substantiation of this form by the user, an e-mail is sent to him with the PIN number, which is the output of the PIN Generation algorithm. Then he can use his username with this number, in order to have access to this product. After the substantiation of this form by this user, an e-mail also is sent to the system administrator with the data of the registry form. So, everyone can opens a new account and then he can use the username-PIN combination in order to have an access to the software product. This is a real-time procedure.

There is a verification algorithm that is used by the product in order to allow (or not) the access to the product for each username-PIN combination. The algorithm is consisted of six steps:

- Step 1:** A user gives his *username-PIN* combination. Set **FLAG=false**.
- Step 2:** Set this username as input to the Generator algorithm and generate a *temporary PIN*.
- Step 3:** If *user PIN = temporary PIN* then set **FLAG=true** and go to step 6. Else go to step 4.
- Step 4:** Search a web-placed database file, for a record with the *username-PIN* combination.
- Step 5:** If *username-PIN* was found then set **FLAG=true**.
- Step 6:** Result = **FLAG**.

According to the previous algorithm, there is a web-placed database file, which contains the *username-PIN* records. Every user can update his personal data of his account, but this isn't a real-time procedure. Updated data are send to the administrator with the e-mail protocol. The administrator updates this file intermittently. He uses a mail collector and a simple database table control, so as to add the new form's data that he received. So, according to this technique, every user has a personal account. Account opening and entering are real-time procedures. The whole authentication system diagram is depicted on Figure 2. [2]

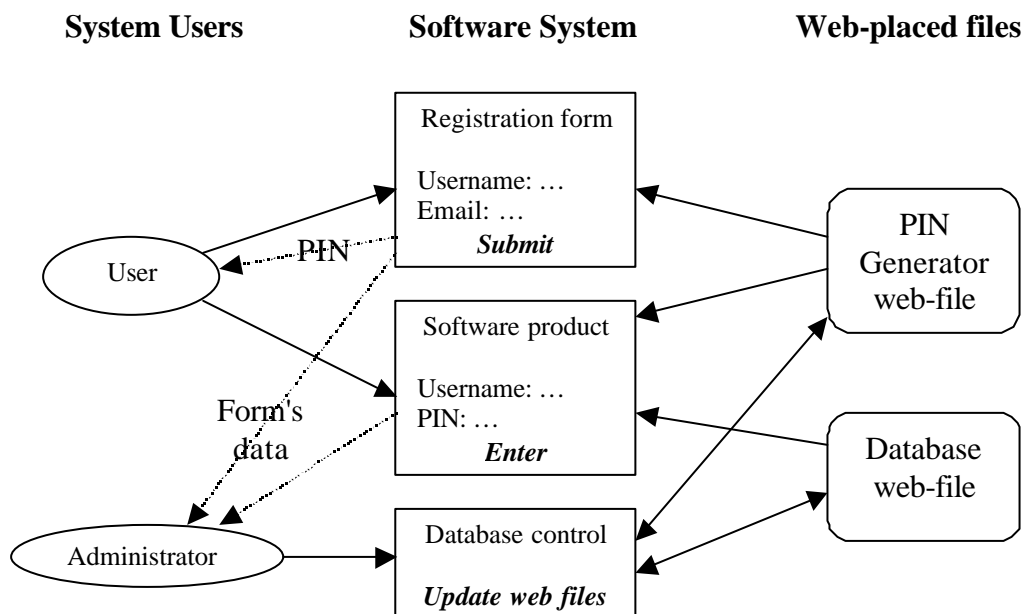


Fig. 2: Web-based authentication system diagram

To sum up, let's see how does this technique work. For example there is a free music catalog software. First of all, a new user sets a username and he fills the registration form. In a few seconds he receives an e-mail with a PIN number, which is the output of the PIN generation algorithm. Then, when he wants to enter to this software, he uses his username-PIN combination. However his username-PIN combination isn't stored in the database yet. In a few days, administrator will update the database web-files, he is the only person that can update the database.

3 Advantages of this technique

According to this technique every user has a personal account and a database server is not required. Users can open a new account every time, because of the PIN-Generator algorithm. This algorithm sets an initial password to the new account. This algorithm remains stable, but the related input web-file is changed intermittently. That means that correspondence between username strings and PIN number is changed, when the related input web-file is also changed. So, this technique is safer than a simple algorithmic technique because we can "change" the generator algorithm. Finally, every user can update his personal data of his account, because we use the e-mail protocol to transfer the updated data to the administrator of the system. There is only one disadvantage, which is the fact that the update procedure isn't a real-time procedure, because there isn't any database server.

Features	Algorithmic	Database server	Web-based
User accounts	No	Yes	Yes
Database Server	No	Yes	No
PIN-Generator	Yes	No	Yes
Web required	No	Yes	Yes

Table 1: Features of algorithmic, database server and web-based techniques

4 Conclusion

This web-based authentication technique for software systems does not require a database server. Just only an e-mail account is required and a few space on the web (5 Megabytes), which are free services nowadays. That is, this technique offers a simple and a safe way for user entrance controlling. It is an ideal entrance authentication system, which could be successfully used by e-commerce, e-learning, advertising, competitions and other web services with users from all over the world. It could be also used on personal web sites, in order access to this site to be controlled.

This technique is implemented and it was successfully used by the *Psifiak-Digital Circuit Designer and Simulator** application. The implementation was written in Java and is consisted of the following three applications: a) Registration form, b) Software product and c) Database control. The required web-files were placed on a web page account of Aristotle University of Thessaloniki and was also opened an e-mail account. Users from different places around the world used successfully this application and there wasn't any problem about the entrance authentication system. Psifiak application was developed by Angelos Barmpoutis and it is free available to the public, at the URL: <http://www.psifiak.8m> [5]

References:

- [1] **Andrew S. Tanenbaum**, *Computer Networks*, 3rd Edition, Prentice-Hall Inc, 1996
- [2] **Raghu Ramakrishnan, Johannes Gehrke**, *Database Management Systems*, The McGraw-Hill Companies Inc, 1998
- [3] **Stallings W.**, *Network and Internetwork Security*, Engelwood Cliffs, Prentice-Hall, 1995b
- [4] **Merkle R.C.**, *Fast Software Encryption Functions*, Advances in Cryptology-CRYPTO '90 Proceedings, New York, Springer-Verlag, 1991
- [5] **Van Der Linden P.**, *Just Java*, Engelwood Cliffs, Prentice-Hall, 1996

* Informatics Department of Aristotle University of Thessaloniki uses Psifiak-Digital Circuit Designer and Simulator, for academic purpose, during Digital Circuit Design and Digital Electronics courses.