Credential Proactive Protection Guard: A Proactive Password Checking Tool

MONIKA PATHAK
Department of Computer Science
Multani Mal Modi College, Patiala
Patiala, Punjab, India
monika_mca@yahoo.co.in

SUKHDEV SINGH
Department of Computer Science
Multani Mal Modi College, Patiala
Patiala, Punjab, India
tomrdev@gmail.com

Abstract

Over the internet, user profiling is one of the key activity in which user is asked to provide personal as well as professional information. The user is not aware about the misuse of profiling. It has been observed that user choose password from his/her profile unintentionally which create serious problem. The password has been taken from small domain which enables hackers to crack credentials by trying different fields of the user profile. To overcome this problem, proactive password checker is required which enforces password policies and prevents users from choosing easily guessable passwords. In this paper, we have introduced proactive password checking tool (Credential Proactive Protection Guard) based on user profiling which automatically check whether the given credential is safe or not and find the relationship between user profile and credentials. The focus of the current study is to check the level of association between different fields of user profile with credentials. The detailed technique, mechanism and tool of the proposed proactive password checker is also discussed in detail.

Keywords: User profiling, Authentication, Safe Credentials, Proactive Password Checking, Naive Pattern Matching, Social Engineering.

I. INTRODUCTION

Proactive password checking has been a common means to enforce password policies and prevent users from choosing easily guessable passwords. In authentication process, when a user chooses a password, a proactive checker will determine whether his/her password choice is acceptable or not. A good proactive password checker also provides possible options for secure passwords as in the case of Gmail registration process. In general, human chosen passwords are insecure because these passwords chosen from small knowledge domain due to which these passwords are easily guessable. The hackers can easily crack the passwords by trying all possible strings from that local domain. The other alternative to crack passwords is "dictionary attacks. A dictionary attack [1] tries to defeat an authentication mechanism by finding each word in a dictionary as a password and trying to crack the required password. Dictionary attacks are often successful because many users and businesses use ordinary words as passwords. The root cause of above problem is the choice of password from user profile where user profile includes personal as well as professional informational. When a user select password from his/her profile then the password can be easily guessed by exploring information of the profile. The second factor is Social Engineering which refers to psychological manipulation of user in order to gain confidential or personal information so that private resources can be accessed. It can be done through formal/informal interaction with the user. In such case, if the credentials of your private resource like internet banking account, email account etc. is from your profile, then credentials are highly insecure. It is again recommended your credentials should not be from your profile.

Proactive password checking enforces password policies and prevents users from choosing easily guessable passwords. Proactive password checking method provides an automatic tool which check whether the given credential is safe or not and find the relationship between user profile and credentials. In this paper, we have discussed about the threats of user profile and credentials. The user profiling [2] is a most frequent activity over the internet by which user has asked to provide personal information. Proactive password checking technique is introduced to solve these problems. It is used to determine whether the password choice is acceptable or not. Different techniques [3, 10, 11, 12], mechanism and tools of proactive password checking are also discussed in this paper. The main concern is to check the level of association between different fields of user profile with credentials. For example, let us consider a user create password based on personal information like birth city, pet

name, surname or combination of these. It is severe problem because hackers can easily guess user's password based on personal information. The present study is focused on safe web based profiling and safe credentials. The concept of proactive password checking plays an important role to overcome this problem. This paper is focused on issues related to safe profiling and proactive password checking tool based on profiling.

II. WEB BASED AUTHENTICATION USING PROACTIVE PASSWORD CHECKING

Web Authentication is a system designed to identify the correct user by providing login interface. The login interface asks the user to enter correct Id and password. Id and password are also known as credentials. Web based authentication system [4] is a three tier architecture that is client, application server and database server. The following diagram shows web based authentication process.

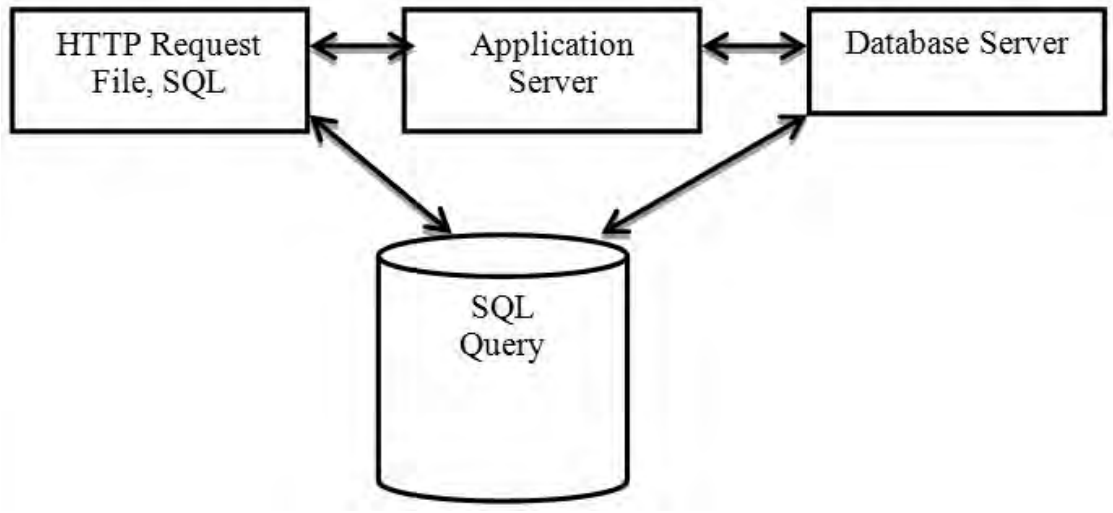


Fig.-1 Web based Authentication Process

In three tier authentication system, a client makes request for logging page (API for authentication), then application server provides the requested resources by communicating database server. In API for authentication, client is asked to enter credentials which are further passed to application server. According to the script, application server verifies the credentials with database and responds accordingly. In general, the proactive password checker [5] is introduced in first level i.e. client side. It acts as an interface between user or client and API for authentication. The job of proactive password checker is to provide facility to create safe credentials. In the current study, proactive password checker is placed somewhere in between client and database server, so that it can communicate with database as well. The proposed tool named as credentials protection guard is placed in between of client side and server side so that it can receive credentials from client and process the information with the help of database server. It is used at the time of generation of credentials of a particular login account. The following diagram demonstrate role of credentials protection guard:

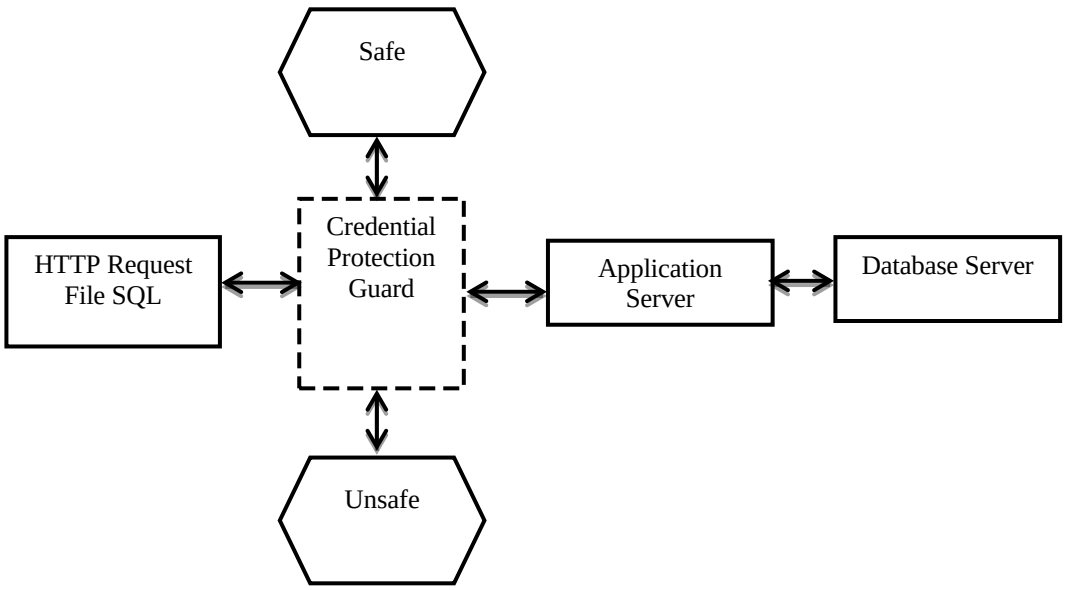


Fig-2 Role of Credentials Protection Guard

III. IMPLEMENTATION OF CREDENTIALS PROTECTION GUARD

The literature review serves as the base of present study. In literature, it has been found that most of the proactive password checkers are based on dictionary attacks and no proactive password checker has been found based on profiling. The following mechanism has been implemented in ASP (Active Server Pages) and MS-Access.

The mechanism allows a security system to check the security level of credentials created by new user. This would protect the misuse of user personal information.

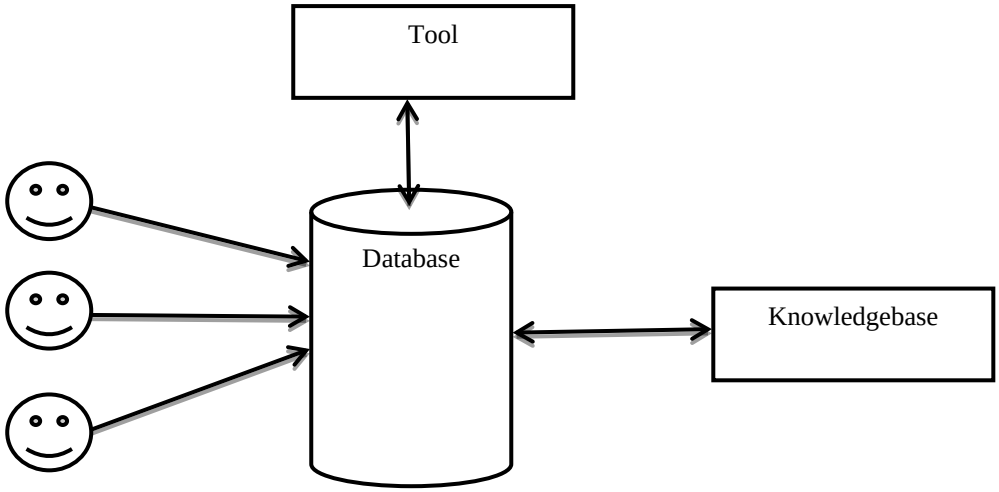


Fig.-3 General Mechanism of Credential Protection Guard

The above diagram (Fig.1) describes that different user's profile with credentials is stored into database. Pattern matching tools can be further applied to produce the desired knowledge. The co-relation technique has been applied to find the necessary relationship between the personal data and the password. This knowledge helps to determine how user profile is associated with the credentials and how security is enhanced with safe credentials.

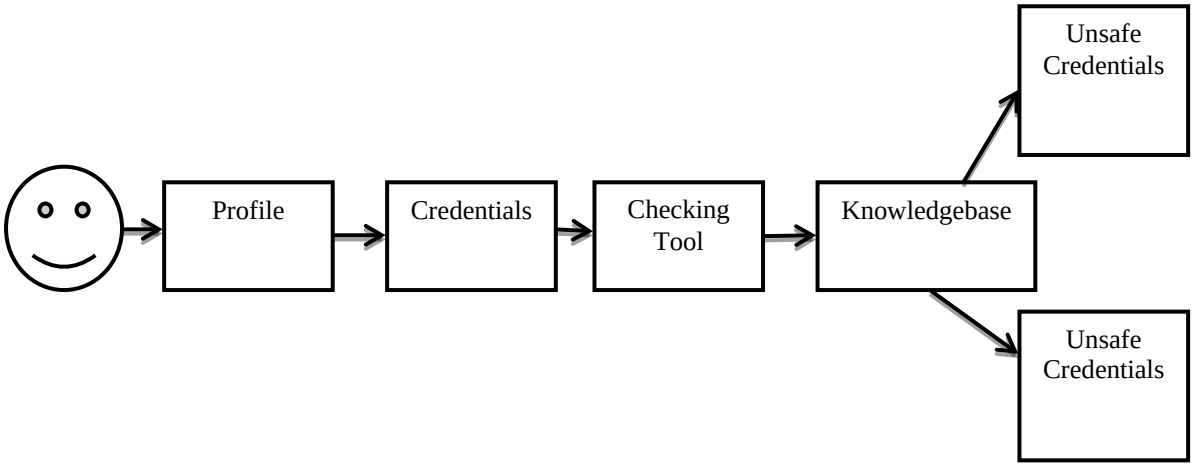


Fig.-4 Association of User Profile with Credentials

Fig.2 describes that a single entered his profile using some web based interface and then create/use credentials. In next step data is stored into a database, which is further fetched by matching tools. The pattern matching technique has been applied to find the necessary relationship between the personal data and the password. This knowledge helps to determine how user profile is associated with the credentials and how security is enhanced with safe credentials. If there is a strong relation between user profile and credentials then it will be considered as unsafe credentials. This research is based on theme "More secure are the credentials, safer is the business".

The techniques used in implementation are shown in the following diagram:

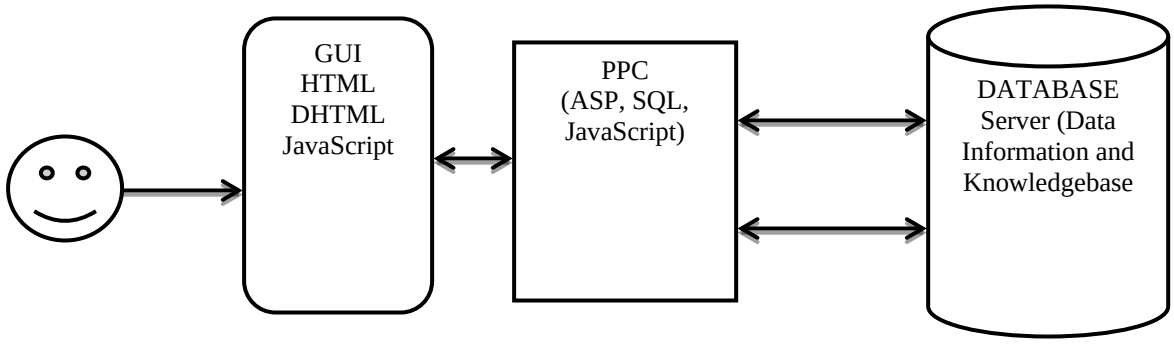


Fig.-5 Different Techniques Used in Implementation

ASP: ASP is an active server pages technology [6] used on server side for computational purpose. The VBScript is used in ASP pages. The proposed tool is credential protection guard which is a web based application developed in ASP. The whole business logic is implemented. Interactive interfaces are developed with the use of CSS, DHTML and JAVA Script. It is also used for interaction with database server i.e. MS-Access.

MS-Access: The Microsoft access is a database package [7] shaped with MS-Office. The database server is used to store information of user (user profile information) and credential information (Id and Password).The different tables has been created to store the information and required relationship has been established.

Naive Pattern Matching Algorithm: Pattern matching is used to compare two or more strings and find out the correlation between them. In literature, there are n number of techniques are reported. For the present study, we consider Naive Algorithm [8] as described below.

Naive pattern matching algorithm

i=1

while i <= n-m+1 do begin//represent phase

j=1

while (j<=m) and (pat[j]=text[i]) do begin//represent steps

j=j+1

i=i+1

end

if j<=m then i=i-j+2

else Print("found at Location", i-j+1)

end

Proactive Credential Policy: Proactive credential policy is the main theme of the research. The present research is based on user profiling and its association with credentials. The process of implementation of proactive credential policy is shown in the diagram below:

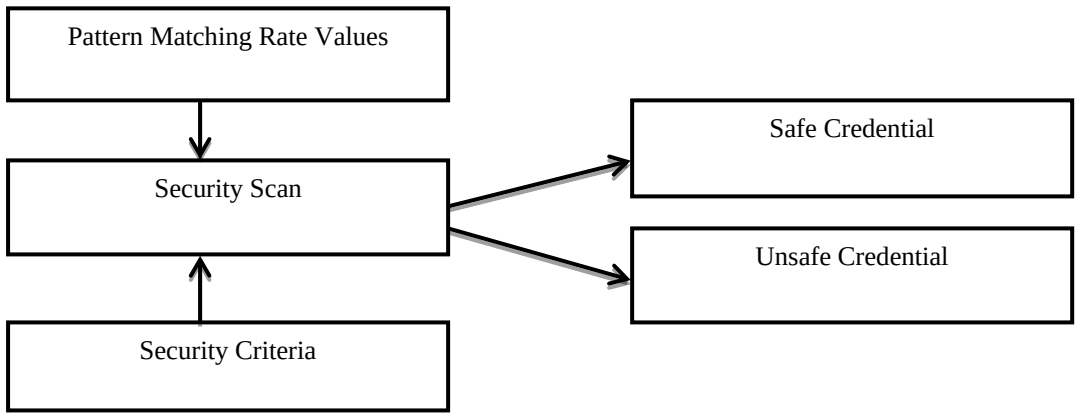


Fig.-6 Different Techniques Used in Implementation

As shown in above diagram, the user profile is compared with credentials and this process is known as security scan. The naive algorithm is used for security scan and level of pattern matching is represented with different

rates as shown in table 1. The selection criteria define certain rules which actually evaluate credentials with reference to profile and security rates/levels. Finally credentials are classified as safe and unsafe.

The concept of security criteria plays key rule in the whole process where security criteria define different levels of security based on correlation between credential and user profile. There are five levels of security named as R1, R2, R3, R4 and R5. Where R1 represents highest level of security and R5 represents highest level of insecurity. The following table shows different levels of security.

Table1: Security Levels

Rate	Condition (%)	Remarks
R1	70-100	Highly secure
R2	60-69	Secure
R3	50-59	Weak
R4	40-49	Insecure
R5	25-39	Highly insecure

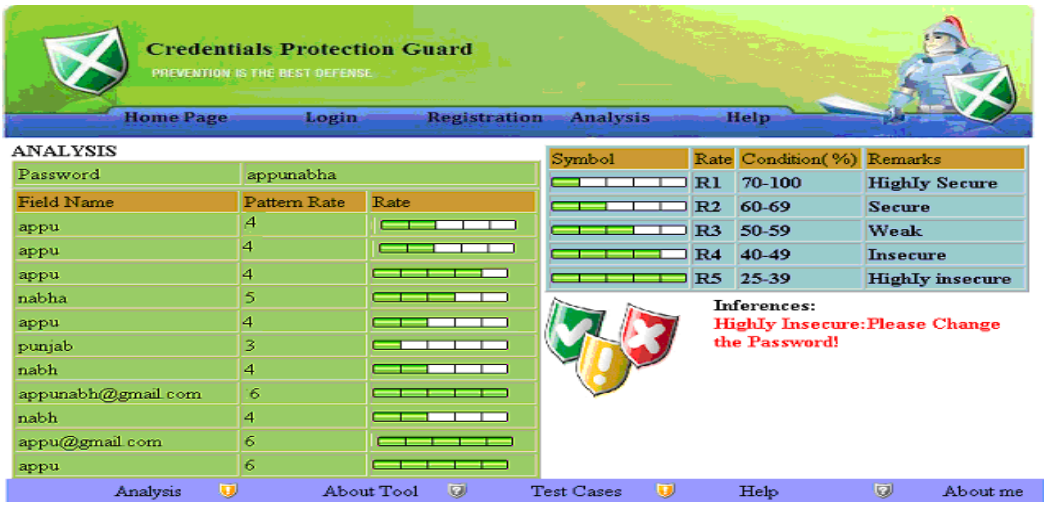
Security rule is based on security levels (Table 1). R1 defines highest level of security and R5 define lowest level of security. These rules can vary acceding to the security mechanism of the organization and sensitivity of the system and information. Further we use the concept of Security Criteria which defines different combination of security level, which may be considered for decision-making.

The following table shows the different conditions for security criteria as:

Table 2: Security Criteria

Inference	Condition1	Condition2
Highly secure	R5>=1	R4>=2
Secure	R4>2	R3>=3
Weak	R3>=1	----
Secure	R5=0	R4=0
Highly Secure	R2=0 & R3=0 &R4=0	---

Security rules are used to define the security level. These rules are not fixed in nature; they can vary according to the situation. Following screen of tool demonstrate of the rules used:

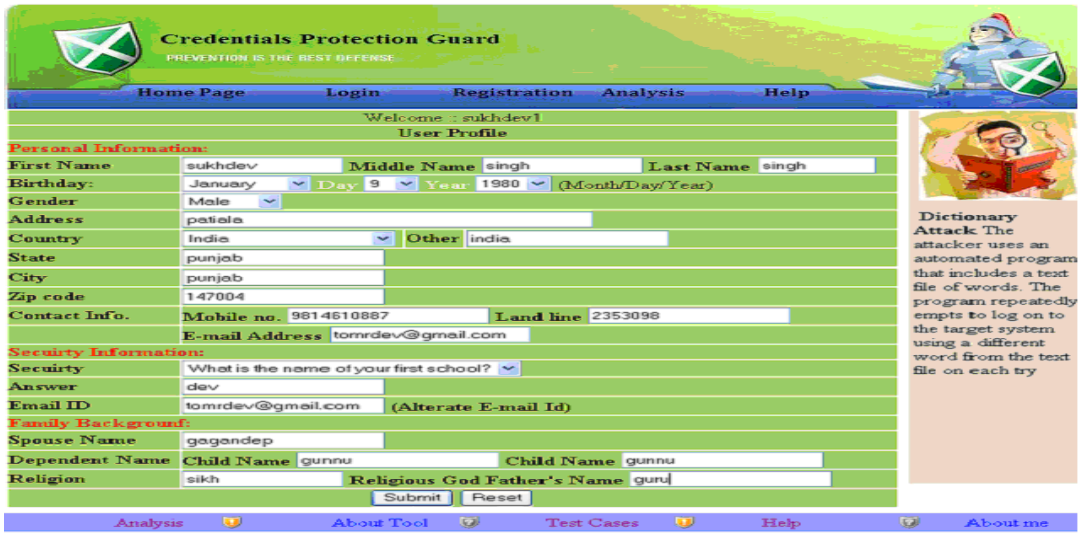


The above diagram shows graphical user interface which is developed in ASP. It shows analysis of security rules by representing different rates.

IV. DATA COLLECTION AND ANALSIS

The data has been collected through web users by providing web based GUI. The user is asked to enter profile information which is stored into database. After this, user is allowed to create credentials. While creating credentials, proactive password checker is activated for safe credentials. Standard Structured Query (SQL) language [9] is used to interact with database server. The entire interface has been developed with server side script i.e. active server pages (ASP).

The following web form is used for retrieving user information:



Data Analysis is used to find out stability of the software. Data from more than 50 users have been collected for analysis. Data analysis reveals that credentials of approx. 30 users have strong relationship with their profile.

V. CONCLUSION

Proactive password checking has been a common means to enforce password policies and prevent users from choosing easily guessable passwords. When a user chooses a password, a proactive checker will determine whether his/her password choice is acceptable or not. We proposed new user profile based proactive password checking tool "Credential Protection Guard". The data analysis shows that the tool is successfully find out the relationship between credential and user profile so that it can classify safe and unsafe password.

VI. FUTURE SCOPE

Present research work can be useful in many situations like Prevent weak password selection: Present research work prevents the selection of weak password, which can be helpful for new users to decide secure password. Integration with Anti-hacking System: It can be integrating with anti-hacking system so that user cannot provide personal information from which password guessing can be carried out. Safe Profiling: User profiling is required at different situations, current study can be used to make safe profiling process can be integrated with this method. So that user may not provide sensitive information. Integration with Fraud detection tool: Present research work can be integrated with Fraud detection tool. The study can be used to find retaliation ship between two or more independent variables. Profile Comparing: Current study can be used to compare two or more profiles and patterns. Compatibility of Profiles: The present research work can be used for finding compatibility of two or more profiles using pattern matching component.

Present work may be improved if we use advance comparison techniques like Ontology matching and advanced data structure.

VII. REFERENCES

[1] F Bergadano, "High dictionary compression for proactive password checking", ACM trans. on info and system security Vol.1, No.1, Nov. 1998.
[2] J.Bonneau," The science of guessing: analyzing an anonymized corpus of 70 million passwords", in IEEE Symposium on Security and Privacy, pages 538-552,2012.
[3] Marchany, R. , Tront J, "E-commerce Security Issues", in the proceedings of 35th Annual Hawaii International Conference on System Sciences , Page-193,IEEE,2002.William Stallings, "Cryptography and network Security", 3rd edition, Prentice Hall,2003
[4] J. Bonneau, S. Preibusch, "The password thicket: technical and market failures in human authentication on the web", In Workshop on the Economics of Information Security, 2010.
[5] F Bergadano, "High dictionary compression for proactive password checking", ACM trans. on info and system security Vol.1, No.1, Nov. 1998.
[6] Introduction to Active Server Pages, http://www.w3schools.com/asp/
[7] Gerard S. Cook, Ellen Monk, Joseph Brady, "Problem-Solving Cases in Microsoft Access and Excel Annual", 2011.
[8] DVKlein.Foiling, "The Cracker: A Survey of, and Improvements to Unix Password Security" , in proceedings of the USENIX
[9] Security Workshop. Portland, Oregon: USENIX Association, summer 1990.
[10] Gregory Speegle, Michael Donahoo, "SQL: Practical Guide for Developers", 2005.
[11] Burton Bloom. Space/time trade-offs in hash coding with allowable errors, CACM, 13(7): 422-426, July 1979
[12] T. Raleigh and R. Underwood, ''CRACK: A Distributed Password Advisor,'' USENIX UNIX. Security, Workshop Proceedings, August 1988.
[13] Yanhong Cui, Renkuan Guo, "Education Technology and Training" in the proceedings of International Workshop on Geoscience and Remote Sensing, 2008.