Image Based Registration and Authentication System

Srinath Akula, Veerabhadram Devisetty

Department of Computer Science
St cloud State University, St. Cloud, MN 56301
aksr0201@stcloudstate.edu, deve0301@stcloudstate.edu

Abstract
Security-sensitive environments protect their resources against unauthorized access by enforcing access control mechanisms. Text based passwords are not secure enough for such applications. User authentication can be improved by using both text passwords and structured images. Our image based registration and authentication system is called IBRAS. The system developed displays an image or set of images to the user, who would then select one to identify them. The system uses such image based passwords and integrates image registration and notification interfaces. Image registration enables users to have their favorite image. The paper will describe our experience and future work.

Introduction
Authentication plays an important role in protecting resources against unauthorized use. Many authentication processes exist from simple password based authentication system to costly and computation intensive Biometric authentication systems. But still the most widely used authentication system is based on the use of text passwords [2] [4]. Text based passwords are not secure enough for many applications that enforce security by access control mechanisms. Authentication based on text based passwords has major drawbacks. More sophisticated authentication process is costly and may need additional equipment or hardware. To overcome such drawbacks we developed a system for verification of personal identity using Java. In this project we have investigated how the security of user authentication can be improved by using both text passwords and structured images. Our registration and authentication algorithm is called IBRAS.

The purpose of this paper is to present the authentication process IBRAS which is simple enough, cost effective and does not need any additional hardware. This IBRAS can be used in educational institutions as well as corporate world with ease. The paper is organized in to many sections. Firstly we present the authentication problem and different authentication processes. The next section explains the advantages and disadvantages of existing authentication systems. Then we present our solution authentication system.

Authentication
Authentication is a function where a user presents some credentials to the system. If the system recognizes this set of credentials or the credentials match a given set on the system, then the user is said to be authorized otherwise the user is not

authorized [7]. Authentication is needed to let the system perform some tasks for the user. The user needs to be authorized to request services from the system. Before a user can be authenticated to the system, he has to be registered with the system for the first time. This step is called registration. So, for a new user, he has to get registered with a system and then authenticated before he can request services.

In a basic authentication process, a user presents some credentials like user ID and some more information to prove that the user is the true owner of the user ID. This process is simple and easy to implement. An example of this type of authentication process is the use of user ID and password.

A complicated process involves a user ID, password and a key value generated with time and which changes constantly at fixed intervals. A user is authenticated only if all three values are right. This is better and more secure than the basic authentication process as the user has to be there physically to use the changing key. An example of this process is use of smart cards [6].

The third authentication process uses biometrics. Biometrics can measure finger prints, retinal scan, facial image scan and many more. In this case, a user always has these credentials on him. User has to present physically for authentication.

The most widely used authentication process uses user ID and a password. Our authentication system can be classified under the simple authentication process which is more secure and powerful than the password based system.

Comparison of Passwords, Biometrics and IBRA systems

The pros and cons of existing and proposed system are discussed in the following sections.

Password based authentication system

This is a simple system where a user presents a user ID and a password to the system. If the user ID and password match with the one stored on the system, then the user is authenticated. A user may have many accounts on many computers. He has to remember many passwords. Research on human cognitive ability has generated a lot of knowledge on what an individual can remember [1]. For example, domain names are used instead of IP addresses and telephone numbers are broken in to chunks for an individual to remember easily. It is also proved that individuals can remember images more easily than the text. The general tendency is that an individual may not remember text passwords easily and he may write it down. This can lead to stealing password to gain unauthorized access to a system. Since passwords cannot be very long, they are easy to break using brute force attacks like attempting different passwords (online attack) or by offline attack on the password hash file. There are many other ways to break passwords like packet sniffing, by accidental discovery. Network traffic is easy to capture and analyze using the tools available in the web. Network protocol analyzers, such as Ethereal

Packet Sniffer and tcpdump can be used to accumulate both incoming and outgoing network data including text based passwords.

Biometric based authentication system

Biometrics, the application of statistical analysis to identify individuals through their biological or physiological characteristics, is emerging as a key aspect in new security systems. Using biometrics, it is possible to avoid pitfalls encountered with traditional security systems where users are required to keep information, such as passwords, safe [3]. Biometric authentication systems may be very safe and secure and reliable but these systems are costly and need additional hardware and software support. These systems are difficult to change and maintain. Deploying such systems for internet may be very complex and not suitable.

Image Based Registration and Authentication System (IBRAS**)**

IBRAS is a simple authentication system, which uses images as passwords [5], [8]. The user submits user ID and an image as credentials to the system. If the image matches with the one stored in the system, the user is authenticated. Images are easy to remember. It is not easy to guess images. Performing brute force attacks on such systems is very difficult. A first time user has to register him with the system by providing all his details. The interface guides the user in a step-by-step fashion. No major change is to be made to the existing password based systems to incorporate the use of images. The system remains simple as the password based one. The images are not stored in the system. Only the hashed values are stored. The user carries the image with him. This system is easy for Internet applications also.

IBRAS was designed as an experimental security tool, which can be used in classroom for demonstrating basic security mechanisms or as an access control system in any of the applications needing authorization.

Implementation

The system has a very user friendly graphical user interface GUI. The main window has options for a new user or an existing user. A user has to register before he can log into the system. A user is registered using his first name, middle name, last name, user name and an image. All the fields except middle name are required fields. Once the user selects the image, it is displayed on the window for the user to verify his image. The image is user's choice. He can bring his own image in a storage device.

The system does not store the images. The images are read byte wise and hashed using a secure hashing function SHA-1. Images are large files. But SHA-1 algorithm produces a 20 byte output which is very secure and requires less memory.

This system was implemented in Java. Java is platform independent, portable and most suitable for Internet applications. Figure 1 gives the class interaction diagram for IBRAS.

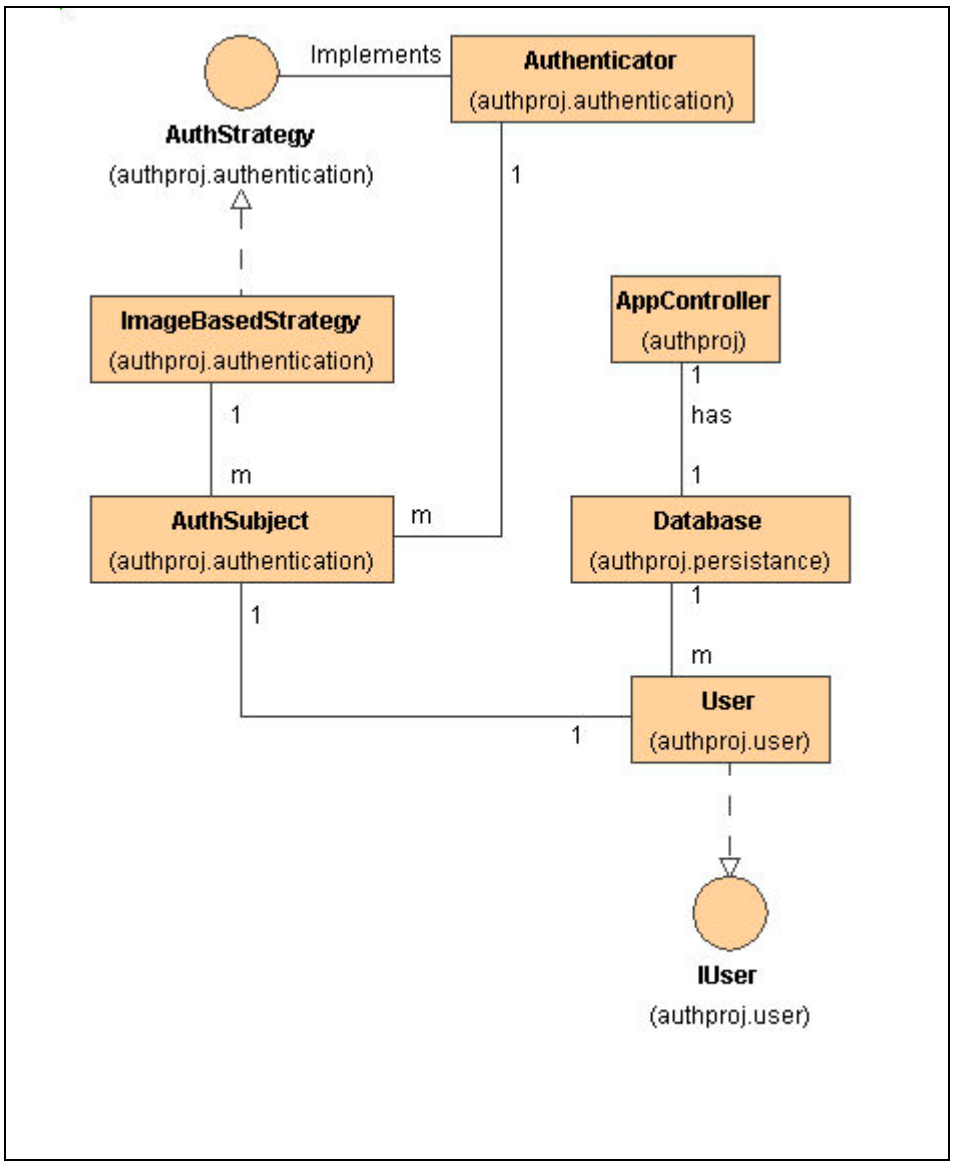

Figure 1: Class diagram on the IBRAS

As per the above Class diagram Authenticator is the Class which has the responsibility of implementing an Authentication Strategy to authenticate any Subject. The Subject is the Object created with the information, combination of the unique UserId and The Image which the User provides to get authenticated. Appcontroller is the Class which is responsible for maintaining a persistent data base, which has the relational table of User details including the message digest of the Image with which the user got registered.

Here we have user some hierarchies for further enhancement of the system without affecting the design. Like later there can be diff hierarchies of user in the system and each of them might have diff levels of information. Or even we can authenticate different levels of users of the system using different authentication strategies. The GUI will be connected to the AppController and will generate events depending upon the user inputs on the database.

Summary and Future Enhancements

In this paper we proposed integrating text based passwords with images to strengthen the security of systems. The process was enhanced by using a hash function for authentication. Also, we briefly discussed how the proposed authentication system could help enhance existing popular systems. This design can be further improved to enhance security. The current system is not built with complete Object Oriented design. Our next step is to rebuild the system using OO methodology using the popular required design patterns. The IBRAS tool can be very well developed to perform role based access control. The database can be maintained as relational database by connecting the system to the database using JDBC connectivity. Our future work would focus on improving the database by providing the persistent storage. Our present system is developed as a stand-alone application. It can be deployed on the Internet easily. It can be integrated with simple biometric systems to enhance the security of the system. The system can be enhanced to make them suitable for small devices like cell phones and PDA's.

References

[1] G.A. Miller, "The Magical Number Seven, Plus or Minus Two: Some limits on our Capacity for processing Information", The Psychological Review, vol. 63, pp. 81-97, 1956.

[2] Art Conklin, Glenn Dietrich, Diane Walz, "Password-Based Authentication: A System Perspective", Proceedings of the 37th Hawaii International Conference on System Sciences – 2004.

[3] Ross A.J. Everitt, Peter W. McOwan, "Java-Based Internet Biometric Authentication System", IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 1166-1172.

[4] Takada Tetsuji, Koike Hideki, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images".

[5] Dhamija Rachna, Perrig Adrian, "Déjà Vu: A User Study Using Images for Authentication", 9th Usenix Security Symposium, August 2000.

[6] Hyun-Sung Kim, Sung-Woon Lee, Kee-Young Yoo, "ID-based password authentication scheme using smart cards and fingerprints", ACM SIGOPS Operating Systems Review, Volume 37, Issue 4 (October 2003), Pages: 32 – 41.

[7] Michael Burrows, Martin Abadi, Roger Needham, "A logic of authentication", ACM Transactions on Computer Systems (TOCS)**,** Volume 8, Issue 1 (February 1990), Pages: 18 – 36.

[8] Trevor Pering, Murali Sundar, John Light, Roy Want, "Photographic Authentication through Untrusted Terminals", IEEE Pervasive Computing , January 2003, pp. 30-36.