Three-Factor Authentication for Electronic Locker

Prof . Reeta Shaktivel M. E, Vikrant Patil, Dipesh Patil, Shailesh Naik , Prathamesh Panjari.
Department of Electronics and telecommunication
K.C. College of Engineering,
University of Mumbai,

Abstract—As part of the security within distributed systems, various services and resources need protection from unauthorized use. Remote authentication is the most commonly used method to determine the identity of a remote client. This paper investigates a systematic approach for authenticating clients by three factors, namely password, smart-card and biometrics. A generic and secure framework is proposed to upgrade two-factor authentication to three-factor authentication. The conversion not only significantly improves the information assurance at low-cost but also protects client privacy in distributed systems. In addition, our framework retains several practice-friendly properties of the underlying two-factor authentication, which we believe is of independent interest.

I. INTRODUCTION

AUTHENTICATION is a process of verifying the identity of the user.

Three-factor authentication means using any independent three of these authentication methods (passport + PIN) to increase the assurance that the bearer has been authorized to access secure systems. The owner of secure data or the operator of such secure systems is implementing three-factor authentication for laptops first because of the inherent security risks in mobile computers, to make it more difficult for unauthorized persons to use a “found” laptop to access secure data or systems. With mobile phones or smart phones, the quality of the problem does not change: A lost or left phone shall not be activated to enable the finder for unauthorized access to secure data or system. Multi-factor authentication hence means three or more of the authentication factor required for being authenticated .Three-factor authentication means that instead of using only one type of authentication factor, such as only things a user knows (login IDs, passwords, secret images, shared secrets, solicited personal information, etc), a second factor, something the user has or something the user is, must be supplied in order to authenticate.
IN a distributed system, various resources are distributed in the form of network services provided and managed by servers. Remote authentication is the most commonly used method to determine the identity of a remote client. In general, there are three authentication factors:

1) Something the client has: smart-card;

2) Something the client knows: password

3) Something the client has and knows: Mobile and OTP

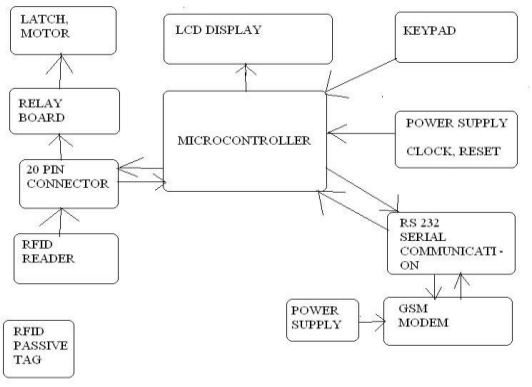
Most early authentication mechanisms are solely based on password. While such protocols are relatively easy to implement, passwords (and human generated passwords in particular) have many vulnerabilities.
As an example, human generated and memorable passwords are usually short strings of characters and (sometimes) poorly selected. By exploiting these vulnerabilities, simple dictionary attacks can crack passwords in a short time. Due to these concerns, hardware authentication tokens are introduced to strengthen the security in user authentication, and smart-card-based password authentication has become one of the most common authentication mechanisms.
Smart-card-based password authentication provides two-factor authentication, namely a successful login requires the client to have a valid smart-card and a correct password. While it provides stronger security guarantees than password authentication, it could also fail if both authentication factors are compromised (e.g., an attacker has successfully obtained the password and the data in the smart-card). In this case, a third authentication factor can alleviate the problem and further improve the system’s assurance. Another authentication mechanism is one time password. The system generates a random number each time the RFID chip is detected and this no is then sent to the Authenticated user to ensure that the person trying to access the locker is authenticated .Thus improving the security of the system.

II .RELATED WORK

Several authentication protocols have been proposed to integrate biometric authentication with password authentication and/or smart-card authentication. Lee et al.

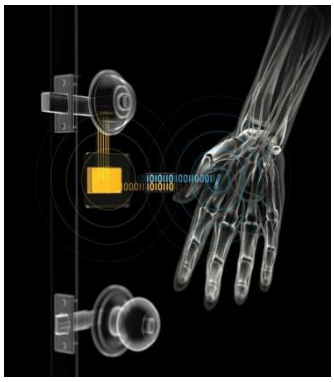
[5] designed an authentication system which does not need a password table to authenticate registered users. Instead, smart-card and fingerprint are required in the authentication. However, due to the analysis given in [6], Lee et al.'s scheme is insecure under conspiring attack. Lin and Lai [7] showed that Lee et al.'s scheme is vulnerable to masquerade attack namely, a legitimate user (i.e., a user who has registered on the system) is able to make a successful login on behalf of other users. An improved authentication protocol was given by Lin and Lai to fix that flaw. The new protocol, however, has several other security vulnerabilities. First, Lin-Lai's scheme only provides client authentication rather than mutual authentication, which makes it susceptible to the server spoofing attack [8].
Second, the password changing phase in Lin-Lai's scheme is not secure as the smart-card cannot check the correctness of old passwords [9]. Third, Lin-Lai's scheme is insecure under impersonation attacks due to the analysis given by Yoon and Yoo [10], who also proposed a new scheme. However, the new scheme is broken and improved by Lee and Kwon [11]. In [12], Kim et al. proposed two ID-based password authentication schemes where users are authenticated by smartcards, passwords and
fingerprints. However, Scott [13] showed that a passive eavesdropper (without access to any smart card, password or fingerprint) can successfully login to the server on behalf of any claiming identity after passively eavesdropping only one legitimate login. Bhargav-Spantzel et al. proposed a privacy preserving multi-factor authentication protocol with biometrics [14]. The authentication server in their protocol does not have the biometric information of registered clients. However, the biometric authentication is implemented using zero knowledge proofs [15], which requires the server to maintain a database to store all users' commitments and uses costly modular exponentiations in the finite group.

III. SYSTEM ARCHITECT



The microcontroller AT89S51 consist of four ports from 0 1 2 3. Port 0 is connected to LCD display which will provide us the inner processor going in a bag. At port 1 we have connected 8 switches which act as keypad. At port 2 GSM module is connected. At port 3 we have connected RFID reader of 125 khz.
versatile 8-bit CPU with In-System Programmable Flash on a monolithic chip, the Atmel AT89S51 is a powerful microcontroller which provides a highly-flexible and cost-effective solution to many embedded control applications.

RFID CHIP:



This is a glass, cylindrical RFID tag; it's very similar to those implanted into pets or human for identification purposes. Each tag comes with a unique 32-bit ID code and is not reprogrammable. The carrier frequency of this tag is 125 kHz, so it works great with our 125 KHz RFID readers.

We tested this RFID tag with one of our ID-12 readers and measured a maximum read distance of about 10mm.

Working **:**

The project consists of microcontroller (89S51) which has GSM modem ,RFID device,8 switches which works as a keypad, DC motor ,relay board and a LCD display
The rfid tag is used to recognize the biochip or rfid card. It forwards the 12 digit number to the microcontroller through serial port .
Then the microcontroller displays a message on LCD and asks to enter the pin . The pin is frstly stored in the microcontroller . If the entered pin is correct the microntroller sends a random number through SMS with the help of GSM modem
Then the user enters the received random number,and if its correct then the motor works and opens the locker
The motor is connected to contacts which are open by default.when the three factors are performed correctly the relay is magnetized which inturn closes the contacts and motor runs.
The relay can be used for other applications too such as for vehicle , turning COMPUTER ON or triggering any computer software,opening door etc.

IV. CONCLUSION

Preserving security and privacy is a challenging issue in distributed system. This project makes a step forward in solving this issue by proposing a generic framework for services and resources from unauthorized used. Our frame work not only demonstrate how to obtain secure three factor authentication three factor authentication to protect from two factor authentication but also address several prominent issues of biometric authentication in distributed system (eg. Client privacy and error tolerance).The analysis shows that the framework satisfies all security requirements on three factor authentication and has several other practice friendly properties (eg. Key aggrement , forward security and mutual authentication).The future work is to fully identify the practical threats on three factor authentication and develop concrete three factor authentication protocols with better performance.

V. REFERENCES

[1] D.V. Klein, "Foiling the Cracker: A Survey of, and Improvements to, Password Security," Proc. Second USENIX Workshop Security, 1990.

[2] A.K.Jain,R.Bolle,andS.Pankanti,Eds.,"Biometrics:Personal Identification in Networked Society," Norwell, MA: Kluwer, 1999.

[3] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition," New York: Springer-Verlag, 2003.

[4] Ed. Dawson, J. Lopez, J. A. Montenegro, and E. Okamoto, "BAAI: Biometric Authentication and Authorization Infrastructure,"Proc. IEEE Intern. Conference on Information Technology: Research and Education (ITRE'03), pp. 274-278, 2004.

[5] J.K. Lee, S.R. Ryu, and K.Y. Yoo, "Fingerprint-Based Remote User Authentication Scheme Using Smart Cards," Electron. Lett., vol. 38, no. 12, pp. 554-555, Jun. 2002.