e-ISSN: 2349-9745
p-ISSN: 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

A NOVEL DYNAMIC AND SECURE AUTHENTICATION SYSTEM USING ACCELEROMETER SENSOR

PRABHU KAVIN B[1], Dr S UMA[2] , DONBYNTALANG DEWKHAID[3], KARTHIKEYAN M[4]
[1] *PG Scholar, PG CSE Department, Hindusthan Institute of Technology, Coimbatore, Tamil Nadu, India*
[2] *Head of the Department, PG CSE Department, Hindusthan Institute of Technology, Coimbatore, Tamil Nadu, India*
[3] *PG Scholar, PG CSE Department, Hindusthan Institute of Technology, Coimbatore, Tamil Nadu, India*
[4] *PG Scholar, PG CSE Department, Hindusthan Institute of Technology, Coimbatore, Tamil Nadu, India*

Abstract— Android is a software stack for mobile devices that includes an operating system, middleware and key applications. Android is a software platform and operating system for mobile devices based on the Linux operating system and developed by Google and the Open Handset Alliance. It allows developers to write managed code in a Java-like language that utilizes Google-developed Java libraries, but does not support programs developed in native code. The unveiling of the Android platform on 5 November 2007 was announced with the founding of the Open Handset Alliance, a consortium of 34 hardware, software and telecom companies devoted to advancing open standards for mobile devices. When released in 2008, most of the Android platform will be made available under the Apache free-software and open-source license. Open Android allows to access core mobile device functionality through standard API calls. All applications are equal Android does not differentiate between the phone's basic and third-party applications even the dialer or home screen can be replaced .Breaking down boundaries Combine information from the web with data on the phone such as contacts or geographic location to create new user experiences. Fast and easy development. The SDK contains what need to build and run Android applications, including a true device emulator and advanced debugging tools.

I. INTRODUCTION

Password-based authentication schemes are the most widely used techniques for remote user authentication. Many static ID-based remote user authentication schemes both with and without smart cards have been proposed. Most of the schemes do not allow the users to choose and change their passwords, and maintain a verifier table to verify the validity of the user login. In this paper we present a dynamic ID-based remote user authentication scheme using smart cards. Our scheme allows the users to choose and change their passwords freely, and do not maintain any verifier table. The scheme is secure against ID-theft, and can resist the reply attacks, forgery attacks, guessing attacks, insider attacks and stolen verifier attacks[1]Modern distributed applications are embedding an increasing degree of dynamism, from dynamic supply-chain management, enterprise federations, and virtual collaborations to dynamic resource acquisitions and service interactions across organizations. Such dynamism leads to new challenges in security and dependability[6].

Collaborating services in a system with a Service-Oriented Architecture (SOA) may belong to different security realms but often need to be engaged dynamically at runtime. If their security realms do not have a direct cross-realm authentication relationship, it is technically difficult to enable any secure collaboration between the services. A potential solution to this would be to locate intermediate realms at runtime, which serve as an authentication path between the two separate realms. However, the process of generating an authentication path for two distributed services can be highly complicated. It

could involve a large number of extra operations for credential conversion and require a long chain of invocations to intermediate services[11].

Addressing to this problem by designing and implementing a new cross-realm authentication protocol for dynamic service interactions, based on the notion of service-oriented multiparty business sessions. Our protocol requires neither credential conversion nor establishment of any authentication path between the participating services in a business session. The correctness of the protocol is formally analyzed and proven, and an empirical study is performed using two production-quality Grid systems, Globus 4 and CROWN[3].

The experimental results indicate that the proposed protocol and its implementation have a sound level of scalability and impose only a limited degree of performance overhead, which is for example comparable with those security-related overheads in Globus[4]. The secure authentication and transaction is one of the important parts in networking security. Because of the security flaws of some existing schemes, this paper proposes a secure authentication and transaction protocol based on digital certificates and dynamic password.

The protocol not only can realize the mutual authentication of the client and server, but also can achieve secure authentication and secure transaction by combing digital certificates and dynamic password. Analysis shows that the protocol can effectively resist many attacks and improve the security of the system[9]. Group key agreement protocol allows all the members to agree upon a common session key, which may be used for later secure communication among all the participants. Since TGDH (tree based Diffie-Hellman) has been proposed by Yongdae Kim, Adrian Perrig, and Gene Tsudik, there are several group key agreement protocols proposed to improve the security and performance of TGDH.

First propose authenticated two-party and three-party key agreement protocols based on bilinear pairing. Then, using authenticated two party or three party key agreement protocols to compute the key of a node which has two or three child nodes, we propose a novel tree-based authenticated group key agreement protocol. Our protocol provides implicit key authentication, which TGDH cannot provide. Through substituting ternary tree for binary and substituting bilinear pairing and ellipse curve DH for DH, our protocol is more efficient both in term of computation and communication than TGDH[14].

II. LITERATURE SURVEY

Password-based authentication schemes are the most widely used techniques for remote user authentication. Many static ID-based remote user authentication schemes both with and without smart cards have been proposed. Most of the schemes do not allow the users to choose and change their passwords, and maintain a verifier table to verify the validity of the user login. In this paper we present a dynamic ID-based remote user authentication scheme using smart cards. Our scheme allows the users to choose and change their passwords freely, and do not maintain any verifier table.

The scheme is secure against ID-theft, and can resist the reply attacks, forgery attacks, guessing attacks, insider attacks and stolen verifier attacks[1]Modern distributed applications are embedding an increasing degree of dynamism, from dynamic supply-chain management, enterprise federations, and virtual collaborations to dynamic resource acquisitions and service interactions across organizations. Such dynamism leads to new challenges in security and dependability[6].

Collaborating services in a system with a Service-Oriented Architecture (SOA) may belong to different security realms but often need to be engaged dynamically at runtime. If their security realms do not have a direct cross-realm authentication relationship, it is technically difficult to enable any secure collaboration between the services. A potential solution to this would be to locate intermediate

realms at runtime, which serve as an authentication path between the two separate realms. However, the process of generating an authentication path for two distributed services can be highly complicated. It could involve a large number of extra operations for credential conversion and require a long chain of invocations to intermediate services[11].

Addressing to this problem by designing and implementing a new cross-realm authentication protocol for dynamic service interactions, based on the notion of service-oriented multiparty business sessions. Our protocol requires neither credential conversion nor establishment of any authentication path between the participating services in a business session. The correctness of the protocol is formally analyzed and proven, and an empirical study is performed using two production-quality Grid systems, Globus 4 and CROWN[3].

The experimental results indicate that the proposed protocol and its implementation have a sound level of scalability and impose only a limited degree of performance overhead, which is for example comparable with those security-related overheads in Globus[4]. The secure authentication and transaction is one of the important parts in networking security. Because of the security flaws of some existing schemes, this paper proposes a secure authentication and transaction protocol based on digital certificates and dynamic password.

The protocol not only can realize the mutual authentication of the client and server, but also can achieve secure authentication and secure transaction by combing digital certificates and dynamic password. Analysis shows that the protocol can effectively resist many attacks and improve the security of the system[9]. Group key agreement protocol allows all the members to agree upon a common session key, which may be used for later secure communication among all the participants. Since TGDH (tree based Diffie-Hellman) has been proposed by Yongdae Kim, Adrian Perrig, and Gene Tsudik, there are several group key agreement protocols proposed to improve the security and performance of TGDH.

First propose authenticated two-party and three-party key agreement protocols based on bilinear pairing. Then, using authenticated two party or three party key agreement protocols to compute the key of a node which has two or three child nodes, we propose a novel tree-based authenticated group key agreement protocol. Our protocol provides implicit key authentication, which TGDH cannot provide. Through substituting ternary tree for binary and substituting bilinear pairing and ellipse curve DH for DH, our protocol is more efficient both in term of computation and communication than TGDH[14].

III. EXISTING WORK

One form of attack on networked computing systems is eavesdropping on network connections to obtain authentication information such as the login IDs and passwords of legitimate users. Once this information is captured, it can be used at a later time to gain access to the system.

The exploit is the code developed by hackers to attack a specific vulnerability of the target system or application. This analysis was done with data collected from the database of exploits found in the Milw0rm web site .The scheme is secure against ID-theft, and can resist the reply attacks, forgery attacks, guessing attacks, insider attacks and stolen verifier attacks

3.1.1 Limitations of the Existing System

The limitations of the existing system are,

- ✶ Less security
- ✶ Easy way for attacker, guessing password.
- ✶ Does not consider the system file

- It has lot of security issues.
- Confidential data will be lost.
- Hackers can easily access the system.

IV. PROPOSED WORK

The main objectives of this work are,

- Authentication alert system to quick transmission of message to preconfigured contacts to intimate the victims.
- To provide maximum assistance to protect our profile to access from others.
- To incorporate the technology and make more versatile applications of defense& war fields

This proposed methodology is the automatic system which will provide the solution to protect profile by changing password spontaneously.

4.1 MODULE DESCRIPTION

- Application Design And Configuration Module
- Registration And Login Module
- Alert Setting Module
- Alert Action Module

4.1.1 Application Design and Configuration Module

In this system, it will choose to assign to design application and configure it with online database(Sql server). In most cases, every Android application runs in its own Linux process. This process is created for the application when some of its code needs to be run, and will remain running until it is no longer needed and the system needs to reclaim its memory for use by other applications.

An important and unusual feature of Android is that an application process's lifetime is not directly controlled by the application itself. Instead, it is determined by the system through a combination of the parts of the application that the system knows are running, how important these things are to the user, and how much overall memory is available in the system.

It is important that application developers understand how different application components (in particular Activity, Service, and IntentReceiver) impact the lifetime of the application's process. Not using these components correctly can result in the system killing the application's process while it is doing important work.

A common example of a process life-cycle bug is an IntentReceiver that starts a thread when it receives an Intent in its onReceiveIntent() method, and then returns from the function. Once it returns, the system considers that IntentReceiver to be no longer active, and thus its hosting process no longer needed (unless other application components are active in it). Thus, it may kill the process at any time to reclaim memory, terminating the spawned thread that is running in it. The solution to this problem is to start a Service from the IntentReceiver, so the system knows that there is still active work being done in the process. application is to register user with name , password , mail id and mobile number

4.1.2 Registration And Login Module

Once registration done ,user provided with UID and password for future use in this application.Login with UID and password to set alert system contact numbers to receive sms when user need password.In this application accerlometer sensor .To developed an application that takes the input of contact details to store in sql server.In this module user can set accerlometer sensors sense speed to get password from android application to login application

4.1.3 Alert Setting Module

The attacker visits the website as a normal user aiming to compromise the webserver process or exploit vulnerabilities to bypass authentication. At that point, the attacker issues a set of privileged (e.g., admin-level) DB queries to retrieve sensitive information.

Attacker will log and process both legitimate web requests and database queries in the session traffic, but there are no mappings among them. DoubleGuard separates the traffic by sessions. If it is a user session, then the requests and queries should all belong to normal users and match structurally. Using the mapping model that we created during the training phase, DoubleGuard can capture the unmatched cases.

4.1.4 Alert Action Module

The designed system will establish the mappings between HTTP requests and database queries, clearly defining which requests should trigger which queries. For an SQL injection attack to be successful, it must change the structure (or the semantics) of the query, which our approach can readily detect. First of all, according to our mapping model, DB queries will not have any matching web requests during this type of attack. On the other hand, as this traffic will not go through any containers, it will be captured as it appears to differ from the legitimate traffic that goes through the containers. DoubleGuard is designed to mitigate DDoS attacks. These attacks can occur in the server architecture without the back-end database.

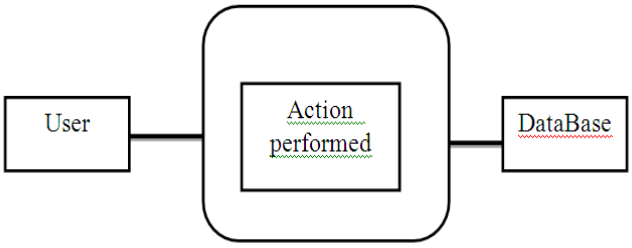

Fig.2. 2.1 System Architecture For Application

V. CONCLUSION

This project presents authentication alert system with SMS to the user defined mobile numbers. The GSM alert based algorithm is designed and implemented with LPC2148 MCU in embedded system domain. The proposed authentication alert system can generate information automatically and sends an alert SMS regarding password. Experimental work has been carried out carefully. The result shows that higher sensitivity and accuracy is indeed achieved using this project. Online database is interfaced to store the mobile numbers permanently. This made the project more userfriendly and reliable. The proposed method is verified to be highly beneficial for the authentication system.

REFERENCES

1.Azim.T, Jaffar.M.A, Mirza M.A. "Automatic Fatigue Detection of Drivers through Pupil Detection and Yawning Analysis." In: Proc. Fourth International Conf. on Innovative Computing, Information and Control, 2009,pp. 441-445.
2.Chen.Y et al. "Yawning Detection for Monitoring Driver Fatigue Based on Two Cameras." In: Proc. 12th International IEEE Conf. on Intelligent Transportation Systems, St.Louis, MO, USA, 2009, pp.12-17.ISSN (Print) : 2320
3.Fan.X, Yin.B, Fun.Y. "Yawning Detection For Monitoring Driver Fatigue." In: Proc.Sixth International Conf. on Machine Learning and Cybernetics, Hong Kong, 2007, pp. 664-668.
4.GPS: Theory and Practice, B. Hofmann-Wellenhof et al., Springer Verlag, 1992, ISBN GSM Networks: Protocols, Terminology and Implementation by Gunnar Heine.
5. GSM Switching, Services, and Protocols by Joerg Eberspaecher.
6.GSM System Engineering (Artech House Mobile Communications Series) by Asha K. Mehrotra.

