International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 7: July 2015, pp 37-40. www.aetsjournal.com ISSN (Online) : 2394-6237

Protocol Based Security Analysis Of Two-Way Authentication Using Handheld Devices

A. Sheik Mohammed , T.Siva Chidambaram , R.Ponnambalanathan , A.Malathi

Abstract— Protocol based user authentication protocol named DUOS which leverages a user's cell phone and internet to thwart password stealing, phishing, pharming, social engineering, etc,. Our implementation provides a high level security for the online attacks and authenticates the user in a reliable manner. Thereby the system can be used to reduce the total execution time and improve the performance than existing web authentication and communication model.Protocol based verification and authentication for two different mediums (Duos) which leverages a user's cell phone and short message service to thwart password stealing and password reuse attacks. Duos only require each participating website possesses a unique phone number, and involves a telecommunication service provider in registration and recovery phases. Through Duos, users only need to remember a long-term password for login on all websites. After evaluating the Duos prototype, we believe Duos is efficient and affordable compared with the conventional web authentication mechanisms.

Keywords— Protocol based verification and authentication for two different mediums (Duos) Telecommunication Service Provider (TSP),Web Service Definition Language(WSDL),Long-Term Password(LTPWD), International Mobile Equipment Identity(IMEI).

I. INTRODUCTION

The Security issues and privacy threats through malware are continuously increasing both in quantity and quality aspects. Over the past few decades, text password has been adopted as the primary mean of user authentication for websites. People select their username and text passwords when registering accounts on a website. Here, the traditional login/password authentication was insecure for most security critical applicationlike online banking or logins to personal accounts. In order to log into the website successfully, users must recall the selected passwords. Generally, password-based user authentication can resist brute force and dictionary attacks if users select strong passwords to provide sufficient entropy. However, password-based user authentication has a major problem that humans are not experts in memorizing text strings. Thus, most users would choose easy-to-remember passwords (i.e., weak passwords) even if they know the passwords might be unsafe. Another crucial problem is that users tend to reuse passwords across various websites. Therefore there will be a chance for insecurity across various websites.In order to rectify this insecurity issue Protocol based verification and authentication for two different mediums (Duos) provides a maximum protection level by making aseparate process for verification and authentication in two different mediums instead of a single authentication factor. This is because the chance of malware to gain control over the two mediums (i.e., PC and Mobile device) simultaneously is considered to be very low.

A. Sheik Mohammed , T.Siva Chidambaram , R.Ponnambalanathan , UG Scholars, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.

A.Malathi is Assistant Professor, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.

II. SYSTEM ANALYSIS

A. EXISTING WORK

Password has been one of the major credential for security process. Text Passwords and Graphical Passwords are the most simple and convenient user authentication on websites. A user having number of accounts using same password, which when compromised suffers from Domino effect.Some of the authentication processes that are commonly used now-a-days for login based approaches are as follows:

Password Based Authentication

In recent years, one of the most widely used authentication method is a password-based authentication method. In this method, users are required to create a secure and memorable password when they create one. Taking account of these two important requirements a mnemonic phrase-based password has been proposed. However it is easy to crack a password if the users adapt famous phrase-based password.

Four Factor Authentications

In the four factor authentication method user identity is a combination of user name, password, biometric and fourth factor as the location of the user. The location of the user gives preference to the sensitive areas requires privacy preservation like military applications.

Smart Card Based Authentication

Smart card is like a credit card in size and appearance. It contains secure crypt processor and file system. It communicates with external devices like ATMs, card reader, etc,. This card can be used as contact and contactless cards. It provides both identity and authentication. But this scheme also prone to man-in-the-browser attacks.

Three Factor Authentications

Some researches focus on TFA rather than password-based authentication to provide more reliable user authentication. Figure 2 depicts the TFA that consist of three major factors of authentication which includes verification by something a user knows (such as a password), something the user has (such as

a smart card or a security token), and something the user is (such as biometrics).

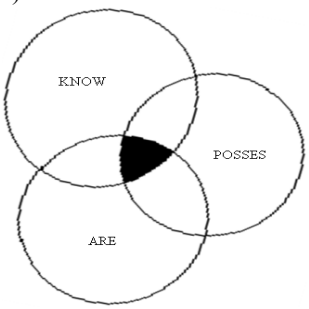

Fig 2:Three Factor Authentication

There are also some limitations using these methods. Increasing chances for Forget the Password with different websites. Reusing passwords causes a domino effect. Hackers Applying Random-Key Function/Method for Hacking the user password.

B.PROPOSED WORK

The main Objective of Duos is free users from having to remember or type any passwords into conventional computers for authentication. Unlike generic user authentication, Duos involves a new component, the Smart Phone, which is used to generate Context Token using SOAP protocol and a new communication channel, Context generation, which is used to transmit authentication Context to SOAP where verification takes place where LTP & STP has been sent to mobile application. Authentication and Verification will be processed only in protocol it provides more challenging job to Hackers.

.

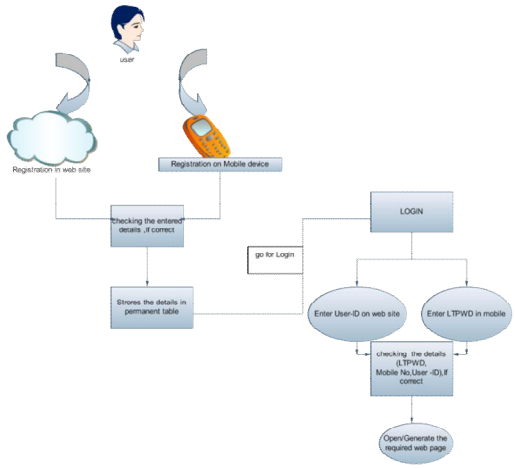

Figure 1: Architecture Diagram

The main advantages of the system are Anti-malware, Phishing Protection, Secure Registration and Recovery, Password Reuse Prevention and Weak Password Avoidance, Cell phone Protection, Password generated at client side will give more security for authentication.

The algorithms and protocols used are

Triple DES(Data Encryption Standard)

SOAP – Implementation

TRIPLE DES(Data Encryption Standard)

Triple DES is based on the DES (Data Encryption Standard) algorithm.It also has the advantage of proven reliability and a longer key length that eliminates many of the attacks that can be used to reduce the amount of time it takes to break DES. It takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL then breaks the user-provided key into three sub keys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it is repeated three times, hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key.

1. Triple DES runs three times slower than DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process.

2. SOAP (Simple Object Access protocol)

SOAP, originally an acronym for Simple Object Access protocol, is a protocol specification for exchanging structured information in the implementation of web services in computer networks. It uses XML Information Set for its message format, and relies on other application layer protocols, most notably Hypertext Transfer Protocol (HTTP) orSimple Mail Transfer Protocol (SMTP), for message negotiation and transmission.

SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework for web services. This XML-based protocol consists of three parts:

An envelope, which defines the message structure and how to process it. A set of encoding rules for expressing instances of application-defined data types. A convention for representing procedure calls and responses.

SOAP has three major characteristics:

- extensibility (security and WS-routing are among the extensions under development)
- neutrality (SOAP can operate over any transport protocol such as HTTP, SMTP, TCP, UDP, or JMS)
- independence (SOAP allows for any programming model)

SOAP is versatile enough to allow for the use of different transport protocols. The standard stacks use HTTP as a transport protocol, but other protocols such as SMTP can also

be used. SOAP can also be used over JMS and Message Queues.

III. IMPLEMENTATION

MODULE DESCRIPTION

A modular design reduces complexity, facilitates changes and results in easier implementation by encouraging parallel development of different part of system. Software with effective modularity is easier to develop because function may be compartmentalized and interfaces are simplified. Software architecture embodies modularity i.e. software is divided into separately named and addressable components called modules that are integrated to satisfy problem requirements. The Duos prototype is dealing with the following modules which gives the clear cut description,

- Website Registration
- Mobile Registration
- Authorization
- Password Generation
- Authentication
- Salvage Phase
- Application Maintenance

WEBSITE REGISTRATION

Online customers must have access to a computer and a method of payment. In proposed system, the user interactions are login, registration, communication, online payments and transaction. User details are handled in backend common database. In computer security, a login or logon is the process by which individual access to a computer system is controlled by identifying and authenticating the user referring to credentials presented by the user. A user can log in to a system to obtain access and can then log out or log off when the access is no longer needed. To log out is to close off one's access to a computer system after having previously logged in.

The steps in User Registration are

- Open a particular website from where to get the web services.
- New user has to register their personal details by entering into the new user mode.
- Now it will open the Registration Form. User has to fill up everything and submit.
- It will be stored on the Temporary table in server's database.

MOBILE REGISTRATION

In this phase, install Duos application in user's Android mobile. When registration process starts, it will generate a signup page. The user has to fill up the registration form by giving user's details.

The main security for the system is one time password authentication. Triple DES algorithm is used for one time password encryption.

OTP Decryption

The One time password decryption process done in android application using same Triple DES algorithm and same key of encryption.

AUTHORIZATION

The server will generate Mobile and E-mail verification codes (OTP-One Time Passwords).

These verification codes (OTPs) will be sent to the corresponding Mobile (through SMS) and Mail-ID.

After getting these verification codes (OTPs), user should enter these codes in another webpage when registration which is called as OTP verification.

Waiting for Accessing page will be in processing mode.

PASSWORD GENERATION

Now, the mobile device will generate a Long Term PWD for further successful logins.

This Long Term PWD is used for secured mobile web authentication.

This will be stored in an encrypted form in server database.

AUTHENTICATION

In this phase, user has to give the user-ID in Login webpage and user has to give Long-term PWD in their mobile device also. In the meanwhile another webpage called Loading will be opened. From these two logins on website and mobile device it will verify the details such as User-ID, Long-Term PWD and mobile number. After this verification, the corresponding required webpage will be opened for access.

SALVAGE PHASE

This phase is taken places when two cases are occurred. First, if the user misses the mobile, which means that, if that particular mobile number cannot be used for the mean while, he cannot access through the old mobile number. Second, if the user forgets the Long-Term PWD, he cannot access the mobile device.

Different web pages will be opened, for both the above cases .By selecting and giving the necessary information that user currently have, in the particular webpages, user can get his/her details related to their account back successfully. This is done successively by using Long-Term PWD which is stored in the encrypted form in server's database.

APPLICATION MAINTENANCE

Final module of the work as application maintenance. That is, to maintain the application with more and more security. Such as PIN code evaluation and Duos verification. In this application user use Mail Services. In this mail services user perform two operations. Such a read a mail from server and compose mail.

IV. CONCLUSION

The secured web authentication has been done successfully by using two types of registration which are named as registration on website and on the mobile device. the scalability and

efficiency for secured web authentication using a personal device has been found out to be very essential. the long term pwd has been generated for secured web authentication which means that secured and successful logins. the otps will be generated to eliminate the problems of pwd reuse and weak pwds. the long term pwd will be stored in encrypted form for security purpose.

REFERENCES

[1] A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks Hung-Min Sun, Yao-HsinChen, andYue-HsunLin 2012

[2] Oprea, D. Balfanz, G. Durfee, and D. K. Smetters. "Securing a remote terminal application with a mobile trusted device". In Proc.of the ACSAC, 2004.

[3] S. Garriss, R. Cáceres, S. Berger, R. Sailer, L. van Doorn, and X. Zhang, "Trustworthy and personalized computing on public kiosks, "in Proc. 6th Int. Conf. Mobile Systems, Applications Services, 2008, pp. 199–210, ACM.

[4] R.Sharp, A.Madhavapeddy, R. Want, and T. Pering."Enhancing web browsing security on public terminals using mobile composition". In Proceeding of the MobiSys, 2008.

[5] M.Wu, S.Garfinkel, and R. Miller, "Secure web authentication with mobile phones," in DIMACS Workshop Usable Privacy SecuritySoftware,Citeseer, 2004.

[6] R.Biddle, S.Chiasson, and P.vanOorschot, "session magnifier a simple approach to secure and convenient kiosk browsing" in ACM Computing Surveys, Carleton Univ., 2010.

[7] Towards Secure Design Choices for Implementing Graphical Passwords Julie Thorpe P.C.vanOorschotSchool of Computer Science, Carleton University {jthorpe,paulv} @scs. carleton.ca

[8] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell, "Stronger password authentication using browser extensions," in SSYM'05: Proc. 14th Conf. USENIX Security Symp., Berkeley, CA,2005, pp. 2–2, USENIX Association.

[9] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks, "in CCS '02: Proc. 9th ACM Conf. Computer Communications Security, New York, 2002, pp. 161–170, ACM.

[10] Dinei Florencio and Cormac Herley, "A Large-Scale Study of Web Password Habits",(Proc. WWW 2007, Banff, BC)