AN Efficiently Detect and Filter False Data Injected Using Quantum Cryptography in Wireless Sensor Networks

*B.Pratheepa, #M.Praveen Umar
*PG Scholar Dept of CSE
#M.E., MBA AP/CSE
King College of Technology, Namakkal

Abstract –
Security is the key term which revolves around every user's Confidentiality and Privacy on web. It is mainly achieved through passwords and conventional login systems.The literature survey clearly shows that the existing systems results in severe issues due to poor remembrance, reusability, weak passwords, hacking. This turns out to be a great problem for users having number of accounts either using same or distinct passwords for each. Considering the current mechanisms, authenticating users via passwords is not a comprehensive solution.In this paper, we design a human verifiable authentication protocol named Duoswhich combines user's handheld device and message service to thwart password stealing or reuse. The goal of this protocol is to prevent users from typing their memorized passwords into kiosks.. Users only need to remember a Long-Term Password (LTPWD) for login on all websites. We believe this to be efficient and affordable compared with the conventional web authentication mechanisms.

Index Terms- Domino Effect, Human verifiable, Long Term Password, Password Stealing attacks.

I. INTRODUCTION

The existing systems which includes Password as a main credential for a secure authentication has led to various serious problems. Text passwords and Graphical passwords are the simple and convenient user authentication on websites. However, these passwords are prone to different threats and vulnerability which includes dictionary attacks, phishing attacks, password stealing and reuse attacks, malware etc. A user having number of accounts using same password, which when compromised suffers from Domino effect.Protecting a user's password on kiosks is infeasible when key loggers and or backdoors are already installed on it PWD-Reuse and Weak-PWD are the most important loopholes where the users get trapped in the net of hackers. Users need to memorize credentials such as username, passwords.1.5% of Yahoo users forget their passwords each month[1]. Since the users could not remember passwords, despite knowing the hackers play a dangerous role, they keep weak passwords due to poor memory. Another important threat is users inputting the secured credentials in the Untrusted Kiosks. Survey shows 2149, out of a total of 50.1k users forget passwords [2]. The survey data indicates that on the order of 0.4% of the population falls victim to a phishing attack a year. Up to now, researchers have investigated a variety of technology to reduce the negative influence of human factors in the user authentication procedure. Since humans are more adept in remembering graphical passwords than text passwords, many graphical password schemes were designed to address human's password recall problem. Using password management tools is an alternative. These tools automatically generate strong passwords for each website, which ad-dresses password reuse and password recall problems.Earlier existing protocols such as Tripartite , Bipartite etc fail to support the authentication systems in case of different devices. Securely demonstrating identities between two handheld devices are often omitted by theoretical protocol designers. Let's consider that two people meet in person and desire to build a secure channel using their handheld devices. They may employ existing authentication protocols that utilize passwords [1]–[4], long secret keys [5], or public key [6] as the proofs of identity. However, most of the above methods are impractical or insecure for this situation.

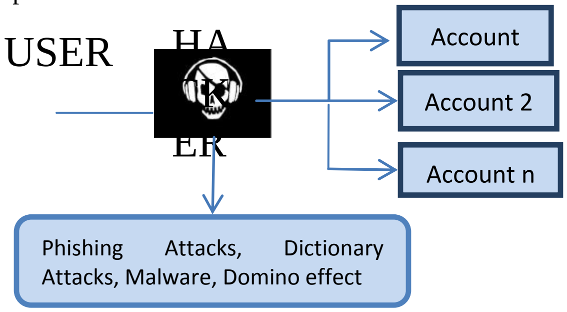

USER
HA
CK
ER
Account
Account 2
Account n
Phishing Attacks, Dictionary Attacks, Malware, Domino effect

Fig 1.System showing the threats

The **proposed protocol Duos** combines the usage of a handheld device and a message service for a secure authentication over the channel. It uses the SOAP, HTTP protocols and web services to create a request-response chain between the channels. Unlike the existing systems leading to threats, our proposed concept overcomes these threats considerably. The generation of **Long term passwords and short term passwords** in our proposed system overcomes the disadvantage of domino effect and other threats. Users can memorize only the long term password in our proposed concept. Users need not input the secured credentials in the web. In our proposed concept , long term passwords gets generated in the mobile phone only. In our opinion, it is difficult to thwart password reuse attacks from any scheme where the usershaveto remember something. We also state that the main causeof stealing password attacks is when users type passwords tountrusted public computers. Therefore, the main concept of the proposed concept 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, thecell phone, which is used to generate long term and short term passwords for at most security.

II. EXISTING SYSTEM

Text Passwords and Graphical Passwords are the most simple and convenient user authentication on websites. However, these passwords are prone to different threats and vulnerability which includes dictionary attacks, phishing attacks, password stealing and reuse attacks, malware etc. A user having number of accounts using same password, which when compromised, suffers from Domino effect.

The existing system surveyed by many authors has resulted in various threats considerably. Users cannot memorize the password for each account. The existing system results in inputting the credentials in untrusted kiosks. The below given diagram clearly shows the bad effects being faced by each user.

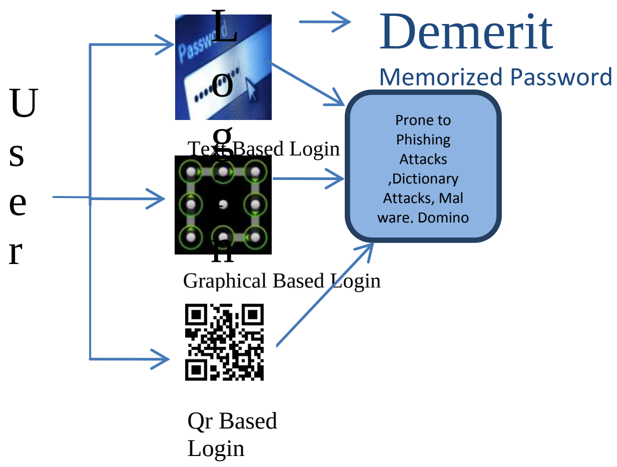


Fig 2 Existing System Architecture

A. *Related Work*

QR code (abbreviated from Quick Response Code) is the trademark for a type of matrix barcode (or two-dimensional barcode) first designed for the automotive industry in Japan.

Fig 3. OR Code

arcode is an optically machine-readable label that is attached to an item and that records information related to that item. A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed using Reed–Solomon error correction until the image can be appropriately interpreted; data is then extracted from patterns present in both horizontal and vertical components of the image.[2]

In this existing system we are using the bipartite and tripartite protocol for encryption purpose. The main disadvantage of this existing system we need the same device (e.g. phone to phone or mobile to mobile)to do the operation. Writing code in QR code is difficult and lengthy process.

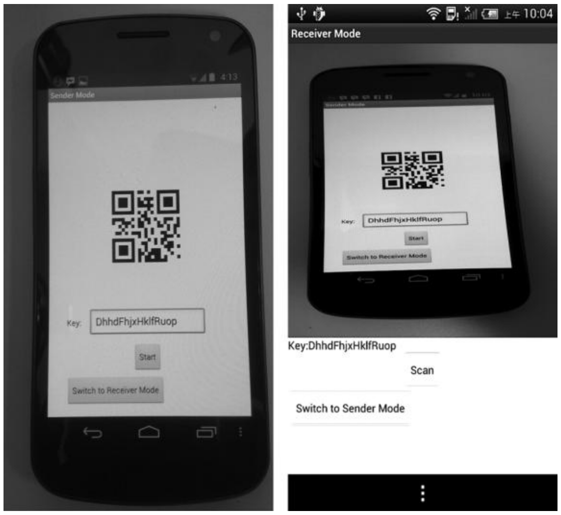


Fig4. Implementation screen shot. Left: sender's screen. Right: receiver's screen.

III. PROPOSED SYSTEM

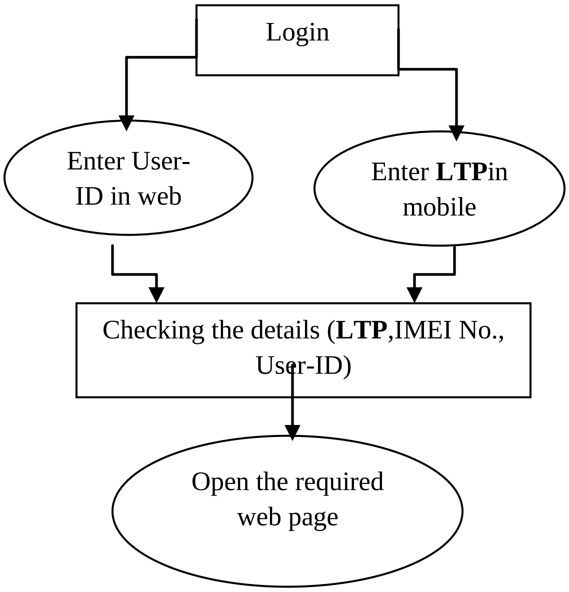
The main Objective of Duos is free users from having to remember or type any passwords into conventional computers for authentication. Unlike generic user authentication, Duos involves a new component, the Smart Phone, which is used to generate Context Token using SOAP protocol and a new communication channel, Context generation, which is used to transmit authentication Context to SOAP where verification takes place where Long Term Password (LTP)&Short Term Password (STP)has been sent to mobile application. Authentication and Verification will be processed only in protocol it provides more challenging job to Hackers. Our Proposed System Comprise of 3 Modules: Sign up Process, Sign In Process, Recovery Process.

A. *Sign Up Process*

In Sign Up process, the user needs a Web Application and an Mobile Application. Both in Web Application and Mobile Application, the User needs to enter and submit all the required details simultaneously. Now a verification process will be carried out in order to check whether the entered details are correct. Once the verification is successful then the entered details are stored onto the Database and a Long Term Password (LTP) is generated in the Smartphone.

B. *Sign In Process*

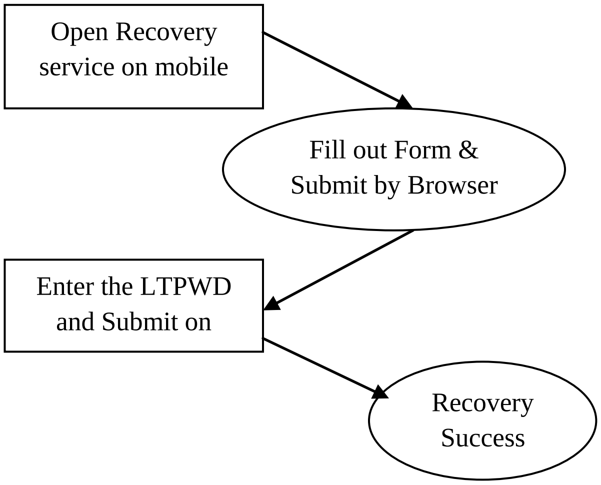
In Sign In Process, the user needs to enter the User- ID which he has earlier given in the Sign Up process. In the SmartPhone, the User needs to enter the Long Term Password (LTP)that was generated during Sign Up process. A verification process is carried out using **Context Generation** in order to check wheather the entered details and the details stored in the database match with one another. Once the Verification is successful then a **Short Term Password (STP) is generated to the Mobile Application** and as the result the required Web Page will be Logged IN.


Login
Enter User-ID in web
Enter LTPin mobile
Checking the details (LTP,IMEI No., User-ID)
Open the required web page

- **LTPWD** – long Term Password
- **IMEI** - International Mobile Equipment Identity

C. *Recovery Process*

In the Recover Process, when the Mobile Phone has been stolen then the User needs tolodge a complaint where these details are stored on to the Equipment Identity Register (EIR) which contains the backlist of all stolen devices. Then the User needs to buy a new Smartphone and open the Recovery Service and fills in the necessary detailson mobile and browser. The user needs to enter theLong Term Password (LTP) on the Mobile. Once submitted then again the verification and Authentication process is carried out. Once it is successful then the required Web Page will be Logged IN.


Open Recovery service on mobile
Fill out Form & Submit by Browser
Enter the LTPWD and Submit on
Recovery Success

IV. CONCLUSION

In our paper , we presented a concept called DUOS which overcomes all the attacks and proves to be an element of at most security. User's negative influence of forgetting passwords, keeping weak passwords, inputting credentials in untrusted kiosks etc can be compromised by our new concept. The major threat of hacking can be controlled considerably. This paper throws light on remembering only long term password. This proves to be a better concept when compared to the conventional existing systems.

REFERENCES

[1] Chien-Ming Chen, King-Hang Wang, Tsu-Yang Wu, Jeng-Shyang Pan, and Hung-Min Sun"A Scalable Transitive Human Verifiable Human Authentication Protocol For Mobile Devices" in IEEE Transactions On Information Forensics And Security, VOL. 8, NO. 8, AUGUST 2013.

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

[3] Shirley Gaw, Edward W.Felten "Password Management Strategies for Online Accounts" in Symposium On Usable Privacy and Security (SOUPS) 2006, July 12-14, 2006.

[4] P.C. van Oorschot, Amirali Salehi-Abari, Julie Thorpe "Purely Automated Attacks on PassPoints-Style Graphical Passwords" in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 3, SEPTEMBER 2010.

[5] Scott Garriss, Ramón Cáceres ,Stefan BergerReiner Sailer , Leendert an Doorn, Xiaolan Zhang "Trustworthy and Personalized Computing on Public Kiosks" in MobiSys'08, June 17-20, 2008.

[6] Scott Garriss Ram, Stefan Berger,Reiner Sailer, Leendert van Doorn, Xiaolan Zhang,Carnegie Mellon AMD,Pittsburgh, Austin. "Towards Trust Worthy Kiosk Computing" in Eighth IEEE Workshop on Mobile Computing Systems and Applications

[7] Min Wu, Simson Garfinkel ,Rob Miller "Secure Web Authentication with Mobile Phones" inMIT Computer Science and Artificial Intelligence Laboratory, 200 Technology Square, Cambridge MA, 02139 USA.

[8] Nisarg Gandhewar, Rahila Sheikh "Google Android: An Emerging Software Platform For Mobile Devices" in International Journal on Computer Science and Engineering.

[9] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K.Reiter, Aviel D.Rubin"The Design and Analysis Of Graphical Passwords" inProceedings of the 8th USENIX Security Symposium.

[10] Sonia Chiasson, Alain Forget, Elizabeth Stobert "Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords" in ACM CCS'09 November 9–13, 2009.

[11] Steven M. Bellovin and Michael Merritt "Encrypted Key Exchange:Password-Based Protocols Secure Against Dictionary Attacks" in 1992 IEEE

[12] David P. Jablon "Extended Password Key Exchange ProtocolsImmune to Dictionary Attack" in 1997 IEEE

[13] D.Amaravathi,P.Swathi"Secure Authentication Scheme in Wireless Networks" in IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[14] WelderufaelBerhaneTesfay, Todd Booth, and Karl Andersson "Reputation Based Security Model for Android Applications" in 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[15] Xiao Ling-Zi, ZHANG Yi-Chun"A Case Study of Text-Based CAPTCHA Attacks" in 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover