Keylogging-Resistant Visual Authentication Protocols

Prof. Priyanka Mane[1] Prabhakar Avhad[2] Devarsh Khedkar[3] Ravikant Jadhav[4] Abhijit Gogre[5]
[1,2,3,4,5]Genba Sopanrao Moze College of Engineering, Balewadi, India

Abstract— The design of secure authentication protocols is reasonably tough, considering that varied types of root kits reside in Personal Computers (PCs) to appear at user's behaviour and to form PCs untrusted devices. Involving human in authentication protocols, whereas promising, is not easy due to their restricted capability of computation and learning. Therefore, wishing on users to spice up security basically degrades the usability. On the alternative hand, quiet assumptions and rigorous security vogue to boost the user experience can end in security breaches which is able to hurt the users' trust. Throughout this paper, we've got an inclination to demonstrate but careful image vogue can enhance not entirely the protection but together the usability of authentication. To that end, we've got an inclination to propose a pair of visual authentication protocols: one could also be a one-time-password protocol, and additionally the choice could also be a password-based authentication protocol. Through rigorous analysis, we've got an inclination to verify that our protocols unit of measurement proof against many of the tough authentication attacks applicable among the literature. What's additional, exploitation AN intensive case study on a model of our protocols, we've got an inclination to spotlight the potential of our approach for real world deployment: we've got an inclination to be ready to deliver the products a high level of usability whereas satisfying tight security wants.

Key words: Keylogging, QR Code, Shoulder-Surfing Attack

I. INTRODUCTION

Threats against electronic and monetary services are often classified into 2 major classes: certificate stealing and channel breaking attacks. Credentials like users identifiers, passwords, Associate in Nursingd keys are often taken by an wrongdoer after they area unit poorly managed. for instance, a poorly managed pc (PC) infected with a malicious package (malware) is a straightforward target for certificate attackers. On the opposite hand, channel breaking attacks which permit for listening traffic on communication between users and a monetary institution are another sort of exploitation. Whereas classical channel breaking attacks are often prevented by the right usage of a security channel like IPSec and secure sockets layer (SSL), recent channel breaking attacks area unit tougher. Indeed, "key logging" attacks or those who utilize session hijacking, phishing and pharming, and visual fraudulence can't be addressed by merely facultative coding. A key lumberjack could be a package designed to capture all of a user's keyboard strokes, and so build use of them to impersonate a user in monetary transactions. for instance, whenever a user sorts in her arcanum in a very bank's sign-in box, the key lumberjack intercepts the arcanum. The threat of such key loggers is pervasive and may be gift each in personal computers and public kiosks. There are a unit continuously cases wherever it's necessary to perform monetary transactions employing a public pc though the largest concern is that a user's arcanum is probably going to be taken in these computers. Even worse, key loggers, usually root kitted, area unit arduous to observe since they're going to not show up within the task manager method list.

II. RELATED WORK

A. Paper Name: The Search to Exchange Passwords: A Framework for Comparative Analysis of Net Authentication Schemes (2012)

Authors are evaluated 20 years of proposals to exchange text passwords for general user authentication on the net employing a broad set of twenty-five usability, deploy ability and security advantages that a perfect theme may give. The scope of proposals we have a tendency to survey is additionally intensive, together with parole management package, federate login protocols, graphical parole schemes, psychological feature authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and life science.

B. Paper Name: Safe Slinger: Easy-to-Use and Secure Public-Key Exchange (2011)

Users frequently expertise a crisis of confidence on the web. Is that email or instant message really originating from the claimed individual? Such doubts area unit ordinarily resolved through a leap of religion, expressing the desperation and helplessness of users. to ascertain a secure basis for on-line communication, we have a tendency to propose Safe Slinger, a system investment the proliferation of smart phones to change individuals to firmly and in private exchange their public keys.

C. Paper Name: Investment Personal Devices for Stronger Parole Authentication (2011).

Author proposed A Mobile Authentication to detect such attacks that separates a user's secret input from the consumer laptop, and offers group action integrity. The laptop continues to be used for many of the interaction however has access solely to temporary secrets, whereas the user's long-run secret is input through a freelance personal device, e.g., a mobile phone that makes it obtainable to the laptop solely when encoding below the meant far-end recipient's public key.

D. Coming Up With Leakage-Resilient Parole Entry on Bit Screen Mobile Devices (2013).

In this paper, Author had projected a user authentication theme named Cover- Pad for parole entry on bit screen mobile devices. Cowl Pad improves outpouring resilience by safely delivering hidden messages, that break the correlation between the underlying parole and also the interaction data discernible to AN somebody. It's additionally designed to retain most advantages of heritage passwords that is vital to a theme, meant for sensible use. The usability of Cover- Pad is evaluated with AN extended user study which has further take a look at conditions associated with time pressure, distraction, and mental employment. These take a look at conditions simulate common things for a parole entry theme used on a day to day, that haven't been evaluated within the previous

literature. The results of user study show the impacts of those take a look at conditions on user performance likewise because the utility of the projected theme.

E. GAnGS: Gather, attest 'n cluster Securely (2008).

Authors presents GAnGS, a fully-implemented system for exchanging authentic data between mobile devices once they area unit physically gift within the same location. GAnGS is ascendible, acceptable for 2 or a lot of devices. we have a tendency to implement 2 user friendly variants of GAnGS on Nokia N70 camera phones. the primary variant, GAnGSP, is predicated on AN un-trusted communication hub. The second variant, GAnGS-T, wants no infrastructure. each variants use Bluetooth for peer-to-peer wire- less communication throughout the knowledge exchange.

III. PROBLEM STATEMENT

We will propose and analyze the use of authentication protocols to show how visualization can enhance usability and security. Moreover, these protocols help to overcome many attack problems. Our main focus is to highlight the potential of our approach for real-world deployment whether we can achieve a high level of usability with satisfactory and acceptable results

IV. GOALS AND OBJECTIVES

1) Increase the security of wireless sensor network while transmitting the data.
2) To detect Black holes before sending data from source to destination.

V. EXISTING SYSTEM

To mitigate the key logger attack, virtual or onscreen keyboards with random keyboard arrangements square measure wide employed in follow. Each techniques, by rearranging alphabets every which way on the buttons, will frustrate straightforward key loggers. Sadly, the key logger, that has management over the whole laptop, will simply capture each event and skim the video buffer to form a mapping between the clicks and also the new alphabet. Another mitigation technique is to use the keyboard golf stroke interference technique by heavy the keyboard interrupt vector table. However, this system isn't universal and might interfere with the software package and native drivers. Considering that a key logger sees users' keystrokes, this attack is sort of just like the shoulder-surfing attack. to forestall the shoulder-surfing attack, several graphical positive identification schemes are introduced. However, the common theme among several of those schemes is their unusability: they're quite difficult for someone to utilize them. for a few users, the usability is as necessary because the security, so that they refuse to alter their on-line dealings expertise for higher security. The shoulder-surfing attack, however, is totally different from keylogging within the sense that it permits associate assailant to envision not solely direct input to the pc however additionally each behaviour a user makes like touching some components of screen.

VI. DISADVANTAGES OF EXISTING SYSTEM

1) Existing system has less security
2) Usability of the existing system was not good.
3) Existing system does not resist challenging attacks, such as the key-logger and malware attacks.

VII. PROPOSED SYSTEM

Our approach to determination the matter is to introduce associate degree intermediate device that bridges an individual's user and a terminal. Then, rather than the user directly invoking the regular authentication protocol, she invokes a lot of refined however easy protocol via the intermediate serving to device. Each interaction between the user associate degreed an intermediate serving to device is visualised employing a fast Response (QR) code. The goal is to stay user-experience a similar as in gift authentication ways the maximum amount as potential, whereas preventing key logging attacks. Thus, in our protocols, a user doesn't have to memorise additional info except a standard security token like word or personal identification variety (PIN), and in contrast to the previous literature that defends against should-surfing attacks by requiring advanced computations and intensive inputs. a lot of specifically, our approach visualizes the safety method of authentication employing a smartphone-aided increased reality. The visual involvement of users during a security protocol boosts each the safety of the protocol and is re-assuring to the user as a result of she feels that she plays a job within the method. To firmly implement visual security protocols, a Smartphone with a camera is employed. Rather than execution the whole security protocol on the private pc, a part of security protocol is moved to the smartphone. This visual image of some a part of security protocols enhances security greatly and offers protection against hard-to-defend against attacks like malware and keylogging attack, whereas not degrading the usability. However, we tend to note that our goal isn't securing the authentication method against the shoulder-surfing aggressor United Nations agency will see or compromise at the same time each devices over the shoulder, however rather to create it laborious for the mortal to launch the attack.

Contribution to projected System: we tend to area unit generating QR code from Encrypted text that may be useful for creating system a lot of sturdy towards hacker. once login with success on-line looking portal are show to user from that user can purchase the merchandise. we tend to area unit giving color choice theme at the time of login for validation of the user.

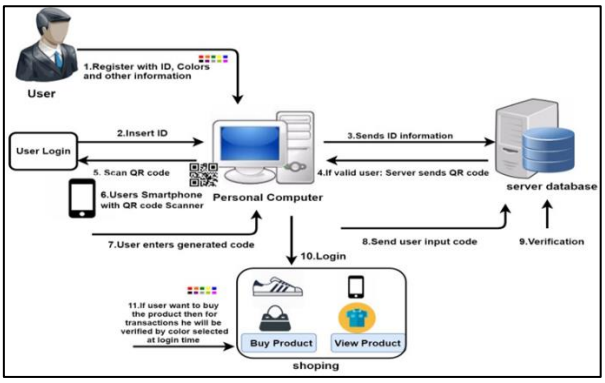

Fig. 1: System Architecture

VIII. ADVANTAGES

1) In this project we demonstrate how visualization can enhance not only security but also usability by proposing two visual authentication protocols
2) Improve the user experience
3) Resist challenging attacks, such as the key-logger and malware attacks.

IX. ALGORITHM AND MATHEMATICAL MODEL

A. AES Algorithm

The secret writing method uses a collection of specially derived keys referred to as spherical keys. These ar applied, beside different operations, on associate array of information that holds specifically one block of information the information to be encrypted. This array we tend to decision the state array.

Algorithm Take the subsequent AES steps of secret writing for a 128-bit block:

1) Derive the set of spherical keys from the cipher key.
2) Initialize the state array with the block information (plaintext).
3) Add the initial spherical key to the beginning state array.
4) Perform 9 rounds of state manipulation.
5) Perform the tenth and final spherical of state manipulation.
6) Copy the ultimate state array out because the encrypted information (QR code).

These algorithmic program ar wont to file content ar convert plaint text to cipher text (QR code)

B. System Methodology

Let W be the full system that consists
Input = {U,M, C, k, S, Pvk, Pbk, M}.

1) Let u is that the set of variety of users.
   U= {u1,u2,…..un}.
2) k is that the secret key used for secret writing.
3) M is that the message sent from the set M.
4) C is that the cipher-text within the set C
5) S is that the signature generated for causation message.
6) Pvk is that the non-public key.
7) Pbk is that the public key.

C. Functions

1) Encrk (): associate secret writing algorithmic program that takes a key k and a message M from set M and outputs a cipher-text C within the set C.
2) Decrk (•): a cryptography algorithmic program that takes a ciphertext C in C and a key k, and outputs a plain-text (or message) M within the set M.
3) Sign (•): a signature generation algorithmic program that takes a non-public key Pvk and a message M from the set M, and outputs a signature σ.
4) Verf (•): a signature verification algorithmic program that takes a public key Pbk and a signed message (M, σ), and returns valid or invalid.
5) QREnc (•): a QR coding algorithmic program that takes a string S in S and outputs a QR code.
6) QRDec (•): a QR secret writing algorithmic program that takes a QR code and returns a string S in S.

X. CONCLUSION AND FUTURE SCOPE

In this project, we analyzed and will propose the user driven visualization to improve security and user-friendliness of authentication protocols. Moreover, we have shown two realizations of protocols that not only improve the user experience but also resist challenging attacks, such as the keylogger and malware attacks. Our protocols utilize simple technologies available in most out-of-thebox Smartphone devices. We will developed Android application of a prototype of our protocol and demonstrate its feasibility and potential in real-world deployment and operational settings for user authentication. Our work indeed opens the door for several other directions that we would like to investigate as a future work. In addition, we will study methods for improving the security and user experience by means of visualization in other contexts, but not limited to authentication such as visual decryption and visual signature verification. Finally, reporting on user studies that will benefit from a wide deployment and acceptance of our protocols would be a parallel future work to consider as well.

REFERENCES

[1] D. Boneh and X. Boyen, "Short Signatures without Random Oracles," Proc. Advances in Cryptology (EUROCRYPT), pp. 56-73, 2004.
[2] J. Bonneau, C. Herley, P.C. Van Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," Proc. IEEE Symp. Security and Privacy (SP), pp. 553-567, 2012.
[3] J. Brown, "ZBar Bar Code Reader, ZBar Android SDK 0.2," http://zbar.sourceforge.net/, Apr. 2012.
[4] C.-sH.O. Chen, C.-W. Chen, C. Kuo, Y.-H. Lai, J.M. McCune, A. Studer, A. Perrig, B.-Y. Yang, and T.-C. Wu, "GAnGS: Gather, Authenticate'n Group Securely," Proc. ACMMOBICOM, pp. 92103, 2008.
[5] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. 12th European Symp. Research in Computer Security (ESORICS), 2008.
[6] D. Crockford, "The Application/JSON Media Type for Javascript Object Notation (JSON)," RFC 4627, http://www.ietf.org/rfc/ rfc4627.txt, 2006.
[7] D. Davis, F. Monrose, and M. Reiter, "On User Choice in Graphical Password Schemes," Proc. 13th Conf. USENIX Security Symp, 2004.

