ISSN (Online) : 2249 - 054X

International Journal of Computing and Corporate Research

Multi Disciplinary Journal for Publication of Review and Research Papers

International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M12-052013
VOLUME 3 ISSUE 3 May 2013

PHOTOGRAPHIC GADGET BASED VERIFICATION SCHEMES

Karun Madan, Surya World Institute of Engg. & Tech, Bapror

Abstract

Hand gesture password might be the most native and intuitive way to communicate between public and machines, since it closely mimics how human beings interact with each other. Its intuitiveness and naturalness have seeded many applications in exploring mass data, computer based games and video games, virtual reality, health care, etc. There are so many areas where Photographic gadget based verification schemes can be used. These areas engross online banking operations and gadget verification etc where an end user can be presented with verification data and capture the data by using a phone Photographic gadget or another Photographic gadget equipped device. In this paper we will converge on the research over Photographic gadget-based verification and compare the different verification schemes and suggest improvements to possible threats.

Introduction

Today, conventional authentication, e.g. passwords, is no longer believed secure in the internet, banking and business sector. Easy-to-guess passwords, such as birthdays or names of spouse or something similar like age etc, are easily exposed by automated password-collecting series. The worldwide adoption of mobile banking will depend on the secure, reliable and effortless user interfaces.

Since the day, the need of authentication has been felt in its infant days, password based verification is becoming prevalent due to ease of use. Though, it creates lot of issues [9]. For instance, consider an end user who has many accounts which are operated through password based verification.

In this case the end user has to remember all their usernames and passwords, which will be easier said than done. On the other hand, if the end user uses one password for all of his accounts it will be prove to be a single point of failure. Another alternative is to use a Photographic gadget based verification scheme. These schemes make use of optically transferring data, which can be united with other schemes like sort of optical challenge-response and budding scheme like one time passwords (OTP). In Photographic gadget based verification, different variants of equipment is used such as web Photographic gadgets, Photographic gadget equipped mobile phones and dedicated gadgets.

Photographic gadget equipped cell phones would be a good choice in Photographic gadget based verification schemes as they are available to all end users at all times and thus provide high availability. Dedicated gadgets provide high security and high usability, on the other hand these gadgets needs to be distributed to all end users [5]. Cell phones have several communication means which include Infra Red (IR), Bluetooth, Wireless Fidelity (Wi-fi), Photographic gadget, manual input and sound. Optical channels comes to picture when we have to transfer massive data in a short interval. Also, these channels are much more efficient and less error prone than sound specially when work in noisy environment. On the other hand, Photographic gadgets are becoming more common in computers, laptops, cell phones etc [13]. Infrared is a short range medium for specially radio communication which works around 1 meter [8]. It is substituted by Bluetooth technology, which is most common today. In radio communication, Bluetooth focus on three security concerns which are confidentiality, verification and authorization by using some kind of encryption techniques. WiFi provides high speed internet via radio waves [6].

Background

Nowadays, many verification schemes can be applied in different situations. We pick to study Photographic gadget based verification schemes because Photographic gadgets are becoming popular in gadgets like PC, laptops, cell phones etc, thus provide high availability, usability and has the potential to perform secure and safe cryptographic operations in many applications[13]. We have picked to study Seeing is Believing, pixel harmonizing and optical character recognition in Photographic gadget based verification schemes. There are also other schemes available like Two click-Auth, QR-TVN and business-related outcomes which are explained below not in much detail but slight overview.

Two click-Auth

This business-related outcome has high usability due to its ease of its use and easy distribution to end users. This outcome can be employed with an identity management system to solve the matter of those end users having many passwords and IDs to remember [13]. This scheme is based on optical challenge response outcome in which a webcam and Photographic gadget equipped cell phone is used for the purpose of verification. This outcome uses two-dimensional bar-codes to provide communication between Photographic gadget-equipped cell phone and webcam.

QR-TVN

QR-TVN uses a scheme which is well-appropriate for web based applications; it uses two dimensional QR codes based on the common transaction-signing with the help of a trusted gadget. This gadget can be a cell phone with a display and a Photographic gadget with a modest resolution. Transactions can be performed totally offline without any network connection if some kind of smart card technology is used with QR-TVNs. By not requiring any kind of network capabilities on the trusted gadget, mobile TANs properties can be improved to extent. It offers security by using secure encryption techniques in case if an attacker gains access to the trusted gadget [1]. Quick Response Transaction Verification Numbers is a essence of TVN which use one time password to make the transaction more safe and secure compare to the conventional static password.

Verification Aspects

There are many verification schemes. The verification schemes are grouped under three classes. These schemes can be blended with each other to offer multimodal verification [7]. □ Memory aspects: some-thing you should know (Passwords, PIN etc) □ Possession aspects: some-thing you must have (Smart Cards, Tokens etc) □ Intrinsic aspects: some-thing unique you are (Biometrics etc)

Memory Aspects

In password based verification scheme the end user present an identity and secret to authenticate him/her self. If the blend of id/password is correct then the end user will be verified, otherwise he has been cast off [2]. Memory aspects include passwords, more secure one time passwords (OTP), PIN etc. These schemes are mostly used almost everywhere for verification purposes.

Possession Aspects

In this scheme, end user put the card into the specified card reader, the card reader reads the end user information through chip and use that information for verification purposes. Possession aspects are smart cards, USB-sticks, dedicated gadgets etc. Let us think about smart card to understand the concept of possession based verification. Smart cards are quite analogous to a credit card (all credit cards are not smart cards but only few) having an embedded programmable micro chip for safe end user verification.

The end user uses this challenge with his given card and four digits PIN to generate result with some kind of cryptographic operation. This result is then sent towards the server. The server verifies the result by carry out the same operation, if the result of the end user and server matches, the end user will be authenticated [9].

Smart cards are mostly use in online transaction and other banking and need a card reader for performing secure & safe transactions [4]. Possession aspects can be pooled with one time passwords (OTP) and some challenge response schemes. In these kinds of verification schemes the end user provides username and the verification server generates some random challenge in response to this.

Intrinsic Aspects

During verification fictitious acceptance and fictitious rejection may occur. Fictitious acceptance rates can be decreased by allowing less variation while fictitious rejection rates can be decreased by allowing variation.These aspects involve physiological or behavioral attributes of end users for the purpose of verification. Physiological attributes include finger print, facial attribute, retina scan etc. And the behavioral attributes include key stroke dynamics, features etc.

Both types of failures can be diminished by balancing allowed variation [3]. The biometric samples of these attributes are enrolled in database which then put side by side with the given sample to authenticate specific end user.

Conclusion

We have seen the Photographic gadget based verification schemes including pixel harmonizing, optical character recognition and Seeing is Believing. Conventional authentication, e.g. passwords, is no longer believed secure and safe in the internet banking or business sector. Another alternative is to use a Photographic gadget based verification scheme. These schemes make use of optically transferring data, which can be united with other schemes like sort of optical challenge-response and budding scheme like one time passwords (OTP). Availability is high in all schemes because gadgets which we have used are cell phones. If dedicated gadgets are used instead of cell phones, availability will be naturally low. We have picked these features based on the facts that these are the most fundamental in the Photographic gadget based verification schemes which we have picked to study in our project. Two-directional verification is required for both parties to verify each other in order to prevent both from intruders. Trusted platform modules make sure the information integrity within the gadget by using public/private keys. Pixel harmonizing and OCR must require Photographic gadget based gadgets at user end. Usability involves ease of use which is much higher in pixel harmonizing and OCR due to the fixed gadget configurations.

References

[1] G. Starnberger, L. Froihofer and K. M. Goeschka, “QR-TVN: Secure Mobile Transaction Verification”, International Conference on Availability, Reliability and Security, 2009

[2] SANS Organization, “Verification Schemes”. [Online]. Available: http://www.sans.org/reading_room/whitepapers/authntication/overview-verification-schemes-protocols_118

[3] National Institute of standards and

Technology, "Biometric Verification". [Online]. Available: http://www.itl.nist.gov/div893/biometrics/Biom etricsfromthemovies.pdf

[4] Tech Target, "Security token and smart card verification". [Online]. Available: http://searchsecurity.techtarget.com/tip/0,289 483,sid14_gci1338503,00.html

[5] A. Vapen, D. Byers, N. Shahmehri,2-clickAuth-Optical challenge-Response Verification, ARES, 2010

[6] IEEE Standard Association. [Online]. Available: http://standards.ieee.org/getieee802/802.11.html

[7] Risk Management Framework. [Online]. Available: https://buildsecurityin.uscert.gov/bsi/articles/best-practices/risk/250-BSI.html http://docstore.mik.ua/orelly/networking/firewa ll/ch10_03.htm.

[8] Infrared Data Association http://www.irda.org

[9] Password based verification http://www.ece.cmu.edu/~adrian/projects/usenix2000/node2.html