International Journal on Wireless, Networking & Mobile Communication Innovations
Vol 2, Issue 1 - 2018

A STUDY ON WEB BASED SECURITY FOR M-BUSINESS USING FINGER PRINT TECHNOLOGY

C SAHAYA ANTO GLADINOBA[*], R PRASANTHRAJ[*], B PUNITHAVATHI[*]

ABSTRACT

Web security is an essential one for all the business those who provide web access. The OTP concept is used for all the business to access the data or information via identifying the customers or members. For example in banking sector, the customer identity verification by sending OTP by using mobile phone or laptop, or tablet or other PDA and the same way all other business concerns follow the OTP concepts for their electronic business and mobile business. In this paper, the finger print technology will be updated for e-business and m-business. The design of authentication system using thump verification will be concentrated and it will be the unique identity of all the people in the world.

KEYWORDS: OTP, Fingerprint Technology, M-Business, Web Security.

INTRODUCTION

M-BUSINESS

M-business is the new technology in the business world which can convey a lot of services and information through mobile, tabs and other similar devices to the user [1]. The user can benefit from this services from anywhere and anytime [1].

WEB APPLICATION SECURITY

It is an important tool which deals with the security of web based services, web applications and websites. The user is cautious about the security of his data whenever he uses any websites. Therefore this web security tool plays a major role [2].

AUTHENTICATION IN WEB SECURITY

PIN: A personal identification number (PIN, pronounced "pin"; often redundantly PIN number by mistake) is a numeric or alphanumeric password or code used in the process of authenticating or identifying a user to a system and system to a user [3].

PASSWORD: it's a way of authentication. The world is facing a lot of issues with the password security system which has put the security of user's data in doubt .Most of the general websites offers plain text password technology in which password cracking can be done easily and thus, the security of data in risk [4].

BIOMETRICS: Biometrics-based security, such as fingerprint authentication, is proven to be both more secure and convenient than passwords, making fingerprint sensing an increasingly common and product-differentiating feature in smart phones, tablets and PCs [5].

[*]Department of CSE, DMI – St. Eugene University. ***Correspondence E-mail Id:*** editor@eurekajournals.com

 ISSN: 2581-5113

However, fingerprint authentication also raises security concerns that can best be addressed with protections purpose-built for biometrics [5]. This technology is broadly used in smartphones and tablets nowadays which provides more security [5].

WEB SERVICES & BIOMETRICS

WEB SERVICE

A web service is any piece of software that makes it available over the internet and uses a standardized XML messaging system. XML is used to encode all communications to a web service. For example, a client invokes a web service by sending an XML message, and then waits for a corresponding XML response [7].

BIOMETRICS [8]

Biometrics (or biometric authentication) refers to the identification of humans by their characteristics or traits. Biometric identifiers are often categorized as physiological and behavioral characteristics. Physiological uniqueness is associated to the shape of their body. Examples are fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition, retina and so on. behavioral uniqueness is associated with the following: voice, in what manner a person walks, etc. finger print consists or ridges and valleys. it differs from people to people. The uniqueness of this fingerprint is determined by two factors.

1. Ridge ending and
2. Ridge bifurcation

A ridge ending is defined as the point where a ridge ends immediately. A ridge bifurcation is defined as the point where a ridge forks or diverges into branch ridges. A high-quality excellence fingerprint typically contains about 40–100 minutiae in each.

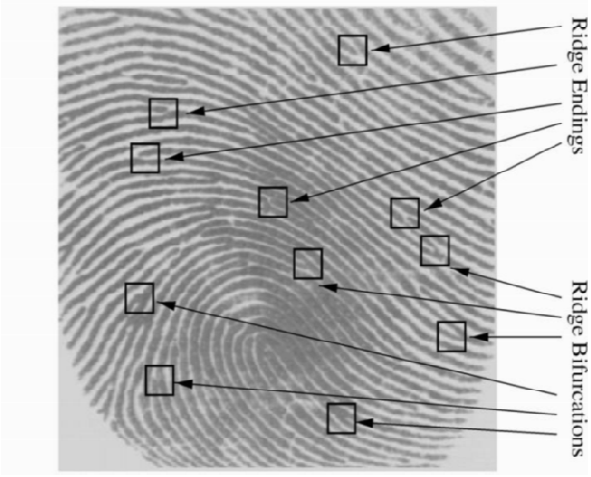

Figure 1.Examples of minutiae (b) Minutiae overlaid on a fingerprint image

In a gray-level fingerprint image, ridges and valleys in a local neighborhood form a sinusoidal shaped plane wave which has a clear frequency and orientation. A number of techniques that take benefit of this in order to propose enhance gray-level fingerprint images. However, they typically imagine that the local ridge orientations can be consistently predictable. In performance, this statement is not suitable for fingerprint images of reduced quality, which really restricts the applicability of these techniques.

BIOMETRIC ADVANTAGES & DISAFDVANTAGES

The following discussion based on advantages and disadvantages of biometric authentication compare with passwords protection. Ultimately, biometrics is all about security. As a feature, their

 ISSN: 2581-5113

main competitor is the password (or PIN code, on occasion), so a comparison between the two will reveal both their flaws and weaknesses.

ADVANTAGE: EASE OF USE [6]

A fingerprint or iris scan is much easier to use than a password, especially a long one. It only takes a second (if that) for the most modern Smartphone to recognize a fingerprint and allow a user to access the phone. In ultrasound scanners the security is more concentrated since it can measure the fingerprints in a deep manner. When a user puts his or her finger to the print-reading chip, an ultrasonic pulse bounces against it. The chip is coated with a layer of aluminum nitride, which can convert mechanical stress to electric energy or vice versa. By measuring the bounce from the ultrasound for longer period of time, the scanner can also sense the depth of the ridges and valleys. If we can sense deeper characteristics, not just the shape, of a fingerprint, you can better tell the difference between what's real or not," says Rob Rowe, vice-president of development at security technology firm HID Biometrics in Albuquerque, New Mexico.

DISADVANTAGE: YOU CANNOT REVOKE THE FINGERPRINT/IRIS/VOICE PRINT REMOTELY [6]

A big disadvantage of biometric security is that a user cannot remotely alter them. If you lose access to an email, you can always initiate a remote recovery to help you regain control. During the process, you will be able to change your password or add two-factor authentication to double your account's security.

Biometrics, however, doesn't work like that. You have to be physically near the device to change its initial, secure data set. A thief could steal your Smartphone, create a fake finger, and then use it to unlock the phone at will. Unless you quickly locked your phone remotely, a thief would quickly steal every bit of information on the device.

ADVANTAGE: THE MALICIOUS HACKER HAS TO BE NEAR YOU [6]

The biggest advantage of biometrics is that a malicious hacker has to be in your physical proximity in order to collect the information required to bypass the login. This narrows down the circle of possible suspects in case your biometric lock is somehow bypassed. The proximity also puts him at risk of getting caught red-handed, in a way that regular malicious hackers working from another continent cannot.

DISADVANTAGE: "MASTER FINGERPRINTS" CAN TRICK MANY PHONES AND SCANNERS [6]

When you first register a fingerprint, the device will ask you for multiple presses from different angles. These samples will then be used as the original data set to compare with subsequent unlocks attempts. However, Smartphone sensors are small, so they often rely on partial matches of fingerprints. Researchers have discovered that a set of 5 "master fingerprints" can exploit these partial matches, and open about 65% of devices. The number is likely to go down in real life conditions, but an open rate of even 10% to 15% is huge and can expose millions of devices.

DISADVANTAGE: BIOMETRICS LAST A LIFETIME [6]

You can always change your password if somebody learns it, but there's no way to modify your iris, retina or fingerprint. Once somebody has a working copy of these, there's not much you can do to stay safe, other than switching to passwords or using another finger. In one of the biggest hacks ever, the US Office of Personnel Management leaked 5.6 million employee fingerprints. For the people involved, a part of their identity will always be compromised.

 ISSN: 2581-5113

DISADVANTAGE: VULNERABILITIES IN BIOMETRIC AUTHENTICATION SOFTWARE [6]

A couple of years ago, security researcher discovered weaknesses in Android devices that allowed them to remotely extract a user's fingerprint, use backdoors in the software to hijack mobile payments or even install malware. What's more, they were able to do this remotely, without having physical access to the device. Since then, patches have come for the vulnerabilities, but bug hunters are constantly on the hunt for new ones.

CONCLUSION

We conclude this paper with the following information.

Convenience: The Beauty of Password Replacement

"Passwords are not only weak; passwords have a huge problem… if you get more and more of them, the worse it is," Bill Gates said at the 2007 RSA Conference. Passwords are a headache for everyone, whether at home or the office, on your PC or your cell phone.

Recent SAP Info research states that 82 percent of all SAP passwords are written down, and 40 percent of all employees share passwords on a frequent basis-not very secure. Passwords are also expensive. For example, it typically costs a company US$10 to $13 to reset an employee password, according to Forrester Research. Moreover, many people do not use passwords at all, given their inconvenience, and thus leave their electronic devices and the information on them unprotected.

Fingerprint sensors eliminate the need for the user to write down passwords, greatly reduce calls to help desks and ensure that only a pre-enrolled and authorized user gains access to a PC or cell phone, the data stored on the device, and the network to which it connects.

Fingerprint sensors add further convenience features to PCs and cell phones and are now being used in models to personalize the device, enabling functions like fast user switching, speed dialing (each finger is a different phone number) and fast application switching. In addition, in small form factor devices, the sensor can be used for device navigation, similar to a joystick. Password replacement is just the tip of the iceberg when it comes to convenience of fingerprint biometrics.

ACKNOWLEDGEMENT

We'd like to thank almighty God to bless us and support us then we thank the management of DMI St. Eugene University, Zambia for supporting us to do these kind of research.

REFERENCES

[1]. http://www.definitions.net/definition/m-business
[2]. "Web Application Security Overview". 2015-10-23.
[3]. https://en.wikipedia.org/wiki/Personal_identification_number
[4]. https://docs.oracle.com/cd/E19424-01/820-4811/gdzeq/index.html
[5]. http://www.synaptics.com/technology/security-suite
[6]. https://heimdalsecurity.com/blog/biometric-authentication/#Eye
[7]. https://www.tutorialspoint.com/webservices/what_are_web_services.htm
[8]. https://www.rroij.com/open-access/personal-authentication-using-fingerprintbiometric-system.php?aid=48464

 ISSN: 2581-5113