Flash Drives Using Finger Print Scanner and Data Validation Through Wi-Fi

Author

Fariza Aqila Zulkifly

Faculty of Computing & Informatics

Multimedia University, Malaysia

1 Executive Summary Of Research Proposal

Data breach is a concern issue nowadays. Confidential and sensitive information is viewed, copied, transferred or even transmitted to unwanted attackers. Whether it is through web application, USB keys or other means of devices, attackers will be able to find a way to hack into our system and steal our data. To ensure our information and data are protected against unauthorised access, a high level security portable system is developed. We find it impossible to transmit data from USB flash drives to our mobile phones, laptops and computers. This is because those USB flash drives are not inserted with Bluetooth devices or Wi-Fi. By enabling Wi-Fi and Bluetooth, users will be able to transmit data and information between those two devices.

A number of consequences might be faced by the users if security threats arise. It started by the application data sends virus through those applications in computer. Not only security at the users computer breaches but data theft is also possible. When the user wants to access the flash drive, one must place their thumb at the device and when the access is granted, the user can view the data. Wi-Fi enables the user to retrieve data without connecting the flash drive to the computer.

2 Introduction

USB flash drive is a portable data storage device. It is small in size, usually about 4 centimetres. The range of the memory is about 500 Megabytes to 32 Gigabytes. Flash drives that stores up to 1 Terabyte are also available. As we know, USB flash drives are not reliable at times. Virus and threats may hack into them and cause problem to users. All files may be corrupted and cannot be retrieved back. I believe a USB flash drive with finger print scanner will solve this problem. Each of us have a unique finger print and no duplication can be made. The reason why finger print is such an amazing tool for authentication is because the impression or mark left by the underside of the tips of the fingers or thumbs is formed by a pattern of ridges on the skin surface. This pattern is unique for each individual and therefore can serve as a means of identification. Biometrics is a measurement and use of unique physiological characteristics to identify an individual. One is Wireless Technology either Wi-Fi technology which we can send/receive File or Bluetooth Technology which we can send/receive data to USB flash drive with Bluetooth enabled devices like Mobiles, laptops and more.The current preferred mode of internet connection all over the world is Wi-Fi. One must have a wireless adapter on their computer to access this type of connection, . Wi-Fi provides wireless connectivity by emitting frequencies between 2.4GHz to 5GHz based on the amount of data on the network. Hot spots are areas which are enabled with Wi-Fi connectivity.

3 Justification of research

This research is important for people of all ages to deal with their problems when using USB flash drives that are available nowadays in the market. For instance, in a life of a University student, they have to deal with a lot of assignments and presentation that sometimes may have near datelines. Students are advice to prepare early to complete their tasks but as we know some students may wait until the last minute to finish their work. Some students will print their work at a print shop and some USB wll get corrupted due to virus and threats. Imagine if the student did not make a back up file for their work, they will lose everything once they inserted their flash drives in the computers. It will be a hassle for students to go back to their hostel clear their USB flash drives from Virus and download everything again to their flash drives. With a USB flash drive that have Wi-Fi, they will need not to insert the flash drive into the computer because we may not know sometimes threats and virus may

attack a computer due to applications. USB flash drives may provide an easy way to copy files to and from a computer and keep them in your pocket. When using phone or table, using a standard size flash drives may be tricky since most of these devices lack full-sized USB ports.

4 Research Objective

The Objectives of The Research are:
To provide a safe environment for users to store their information and projects.
To prevent users from having to lose their data because of unwanted threats and virus.
To prevent from information leaking to random users that might manipulate the information for their personal use and benefits.
To construct proper data validation for users to input data.
To create an easy access for user to transmit data.

5 Literature Review

Computer security, also known as cyber security or IT security, is the protection of information systems and data from theft or damage to the hardware, the software, and to the information on them, as well as from disruption that the users store or access . Security threats such as stealing information are not new here as it has become a huge concern over the past few years. Malaysia is one of the top-infected countries in Asia Pacific region. Nevertheless, dozens of technologies are available to promote IT security. To create a control environment, technologies such as anti-virus and data security software, firewalls, fault-tolerant and high availability computing technology, and programmed procedures can be make used of. Anti-virus software is software designed to check computer systems and flash drives for the presence of various threats.
Financial consequences to individuals and also organisations whenever incidents about computer or network security arises. Numerous attacks are on the move by prospects of financial gain. With valuable information or data, one can sells them and make profit out of it.
Protecting data and information systems from unauthorized users and access are what computer security is all about. Ethics, confidentiality and information are core goals. Besides the

more attack-resistant authentication schemes passwords are the most common and favoured first line of defence in security systems used by computers. The most critical element in a security system is the human factor.A password or passphrase is a secret word/phrase, string of characters, or some form of interactive message or signal that is used for authentication; to prove identity or gain access to a resource/place.

6 Research Methodology

The Method used is Theoretical. USB flash drives mainly deals with transferring and transmitting information and data. Security is highly needed in the web application business so that they won't loose integrity and maintain their confidentiality. Using principle associated and some knowledge, had systematically gave all the research details in this articles. To make sure security in a computer system we must differentiate between having enough rules too sustain good security and not having too many rules that would confused the users to take unclear actions that will jeopardise the security system. By having an easy finger print scanner, every user does not need to create a lengthy password that sometimes would be forgotten over a period of some time. The implementation of Wi-Fi will be able to transfer data without any in between device that may contain corrupted files or applications that contain malware, threats or virus. IT security is about protection of data and information from unauthorized users and access. Confidentiality, integrity and availability of information are core goals.

7 References

http://fingerprint-usb-review.toptenreviews.com/

http://www.orlandosentinel.com/business/technology/os-icloak-fingerprint-authentication-device-20150407-story.html

http://mobileoffice.about.com/od/workingontheroad/ss/bring-everything-on-a-usb-stick.htm

http://liliputing.com/2015/07/sandisk-connect-wireless-stick-usb-flash-drive-and-wifi-file-server.html

http://www.ievoreader.com/biometrics-explained

Gary McGraw and John Viega, "Building Secure Software: How to Avoid Security Problems the Right Way", Addison-Wesley Pub Co, ISBN 020172152X.

Dafydd Stuttard, Marcus Pinto, "The Web Application's Handbook Discovering and Exploiting Security Flaws", 2008, Wiley, ISBN 978-0470-17077-9.

Mike Howard and David LeBlanc, "Writing Secure Code", Microsoft Press, ISBN 0735617228. Gary McGraw and Greg Hoglund, "Exploiting Software: How to Break Code", Addison-Wesley Pub Co, ISBN 0201786958.

Asmawi, A ; Aflendey, L.S. ; Udzir, N.r. ; Mahmod, R., "Model-based system architecture for preventing XPath injection in database-centric web services environment", Computing and Convergence Technology (ICCCT), 2012, Page(s): 621-625.

Johari, R. ; Sharma, P., "A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation and Security Engine for SQL Injection", Communication Systems and Network Technologies (CSNT), 10.11 09/CSNT.2012.10 4, Page(s): 453-458.

Jeremiah Grossman, Robert "RSnake" Hansen, Petko "pdp" D. Petkov, Anton Rager, Seth Fogie, "Cross Site Scripting Attacks: XSS Exploits and Defense", 2007, Syngress, ISBN-IO: 1-59749-154-3. Joel Scambray, Mike Shema, Caleb Sima, "Hacking Exposed Web Applications", Second Edition, McGraw-Hili, 2006 - ISBN 0-07226229-0.

Atashzar, H. ; Torkaman, A ; Bahrololum, M. ; Tadayon, M.H., "A survey on web application vulnerabilities and countermeasures", Computer Sciences and Convergence Information Technology (ICCIT), 2011, Page(s): 647-652.

James S. Tiller, "The Ethical Hack: A Framework for Business Value Penetration Testing", Auerbach, ISBN 084931609X.