Indonesian Journal of Electrical Engineering and Computer Science
Vol. 8, No. 3, December 2017, pp. 730 ~ 732
DOI: 10.11591/ijeecs.v8.i3.pp730-732

NFC Secured Offline Password Storage

Senthil Kumar M*, V Mathivanan
Department of Information Technology, AMET University, Chennai

Abstract

In this paper is all about constructing a device called "One-WORD" that aims to solve this problem. One-word is an offline password keeper aimed at saving and encrypting the passwords in a more secure manner. The main device contains the encrypted passwords while a secure NFC smartcard and a personal pin-code allows the decryption. Even if an attacker is able to get hold the smartcard, or the device it is completely useless without the personal code.

Keywords*: NFC, Communication, Smartcard*

1. Introduction

Security in an organizational environment like a university is always a solicitude. According to the National Association of Campus Card Users of the approximately 231 schools they have on record 197 of them are using magstripe technology, and 62 have already moved to some form of non contact technology [1-3]. Various methods have been engaged over the years to meet the security needs of universities. Some of the methods of security have included keys, badges, magstripe cards, smartcards, and currently the emerging trend is NFC [4-5]. Each of these methods has a role in security dependent on cost versus security

2. Existing Problem

Log-In and Passwords are integral part of our daily lives. They will prevent malicious users from doing harmful things with our personal data. People tend to use the same credentials for the different websites they visit. However recent news has taught us that credentials stored by websites are compromises on daily basis, which means that once an attacker gets your credential set, he can use it on other websites. This is why using different passwords for different websites is important. Remembering many different passwords is difficult. One option is software based password database [6-8]. But it must be stored on your computer or smartphone memory, which is still vulnerable and a malicious user can get access to the database without you knowing it.

3. Proposed Method

One-word is an offline password keeper aimed at saving and encrypting the passwords in a more secure manner. The main device contains the encrypted passwords while a secure NFC smartcard and a personal pin-code allows the decryption. Even if an attacker is able to get hold the smartcard, or the device it is completely useless without the personal code.

To enter the log-in credentials on the webpage, the user must first connect the device to the PC using USB cable, enter a 4-digit pin number (only the first time) and place the smartcard within the card slot, and should simply speak the name of the website. The device recognizes the website name, using an android app and enters the username and password automatically like a keyboard.

The advantages of our devices are.

1) It cannot be attacked by viruses or malicious programs
2) It is impossible to change the firmware as it is an offline device, increasing robustness of the solution.
3) NFC smartcard approach allows multiple users to use the device each with their own pins and smartcard

Received June 29, 2017; Revised August 15, 2017; Accepted September 23, 2017

4) Speech recognition allows the device to be used in any computer. There is no need to install additional software.

NFC Smartcard

The device is constructed with NFC transponder chip that enables it to read and write the smartcard. The card holds very little details regarding the user, and thus using it gives no security risk. NFC is a secure and universal contactless communication technology evolved from RFID. NFC operates in the 13.56MHz radio frequency band and the communication typically happens at 10 cm or lesser distance. Thus the communication happens only when the card is very close proximity to the device [9-10].

Speech Recognition & Bluetooth

The device uses bluetooth to communicate with an app running on an android smartphone. Speech recognition is done by the android app and relays the information to our device via bluetooth. In addition to this, the app also lets the user to control and configure the device.

Capacitive Touch GUI

A set of capacitive touch buttons and a graphics display allows the user to enter the pin number via simple touch gestures. The device status is indicated using a set of onboard color LED's.

Onboard Storage & Multiuser Support

The device has an onboard Quad-SPI flash memory, which is used to store the encrypted passwords as well as other audio files. The device can be used by more than one user. Each user needs to have a unique smartcard and PIN number A survey on query processing in mobile database is discussed in [11].

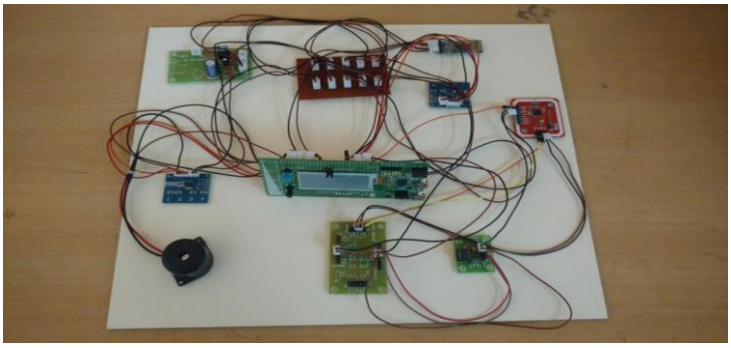
USB Keyboard Profile

The device is equipped with USB connectivity that implements the USB keyboard profile according to the USB specification. This helps it to automatically type the characters in the user name and password field of the login page.

Secure USB Mass Storage Device

The device can also be used as a mass storage peripheral, used to store text files in an encrypted manner. To transfer the file to the PC, the user must be authenticated before any file transfer is possible. Even if an attacker is able to capture the file, he will see only the encrypted data and not the original data generating a digital signature based on new cryptographic scheme for user authentication and security is explained in [12]. The authentication process involves pin number and NFC smartcard verification.

4. Implementation of Hardware Subsystem



5. Conclusion

NFC is mostly continue its path of being highly utilized in every fields because of its easy to use for people. It is also very bendable when compared to identification devices of the previous, allowing various types of identification. The result is NFC will be widely used for identification and multiple protocols will be utilized in the future.

References

[1] Smart Card Alliance. *EMV and NFC complementary technologies that deliver secure payments and value added functionality*. 2012.
[2] developer.android.com, Accessed on Sept, 2014.
[3] Erick Macias and Josh Wyatt. *Texas instruments-nfc active and passive peer-to-peer communication*. 2014.
[4] Gerald Madlmayr, Christan Kantner. NFC devices: Security and Privacy. *Availability Reliability and Security*. 2008
[5] Maximilian Engelhardt, Florian Pfeiffer, Klaus Finkenzeller and Erwin Biebl. *Extending ISO/IEC 14443 type A eavesdropping range using higher harmonics*. 2013
[6] Nikolaos Alexiou, Stylianos Basagiannis and Sophia Petridou. *Security analysis of NFC relay attacks using probabilistic model checking*. 2014
[7] Antonio J Jara, Alberto F Alcolea, Miguel A Zamora and Antonio FG Skarmeta. *Evaluation of the security capabilities on nfc-powered devices*. 2010
[8] www.naccu.org, Accessed on Sept, 2014
[9] www.ncpc.org, Accessed on Sept, 2014
[10] Manickasankari N, Arivazhagan D & Vennila G. A survey on query processing in mobile database. *Indian Journal of Science and Technology*. 2014; 7: 32.
[11] Ganeshkumar K and Arivazhagan D. Generating a digital signature based on new cryptographic scheme for user authentication and security. *Indian Journal of Science and Technology*. 2014; 7(S6): 1-5.