ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Stegano Pin: Indirect Method for Pin Entry Security

[1] S.Pallavi, [2] D.Shekar Goud
[1] M.Tech Student, [2] Associate Professor
[1][2] Dept Of ECE, Ellenki College of Engineering &Technology, Patelguda, Patancheru, Medak (dist), India

***Abstract*— Users typicalIy reuse the same personalized identification number(PIN) for muItiple systems and in numerous sessions. Direct PIN entries are highly susceptible to shoulder—surfing attacks as attackers can effectively observe PIN entry with concealed cameras. Indirect PIN entry methods proposed as counter measures are rarely deployed because they demand a heavier cognitive workload for users. To achieve security and usability, a practicaI indirect PIN entry method called SteganoPIN is presented. The human—machine interface of SteganoPIN is two numeric keypads, one covered and the other open, designed to physically block shoulder surfing attacks. After locating a long —term PIN in the more typical layout, through the covered permuted keypad, a user generates a one—time PIN that can safely be entered in plain view of attackers. Forty—eight participants were involved in investigating the PIN entry time and error rate of SteganoPIN. Our experimental manipulation used a within—subject factorial design with two independent variables: PIN entry system (standard PIN, SteganoPIN) and PIN type (system—chosen PIN, user—chosen PIN). The PIN entry time in SteganoPIN (5.4—5.7 s) was slower but acceptable, and the error rate (0—2. °) was not significantly different from that of the standard PIN. SteganoPIN is resilient to camera—based shoulder—surfing attacks over multiple authentication sessions. It remains limited to PIN —based authentication.**

Keywords: **Raspberry-pi, ultrasonic sensor, camera, keypad, display.**

INTRODUCTION

A. Personalized Identification Number Entry security Problem: Personal identification number (PIN), typicalIy constructed and memorized, are widely used as numerical passwords for user authentication or various unlocking purposes. Their application is increasing because modern touch screens can facilitate convenient implementation of the PIN entry interface on a variety of commodity machines and devices, including automated teller machines (ATMs), point—of—sale (POS) terminals, debit card terminals, digital door— locks, smart phones, and tablet computers. Unfortunately, when a user directly enters a secret PIN into such systems, security is easily compromised, particularly in public places. Nearby people can observe PIN entry by shoulder—surfing with or without concealed cameras. The human—only shouIder—surfing attacker is defined as a weak adversary who has no automatic recording device, but may use manual tools such as a paper and pencil. The camera—based shoulder—surfing attacker is defined as a stronger adversary assisted by an automatic recording tool, such as a wearable camera, to record and analyze entire transactions effectively even at long range. Moreover, adversaries who have already mounted shoulder—surfing attacks and collected multiple PIN candidates can attempt to impersonate a user. The active—guessing attacker is an adversary who attempts guesses with PIN candidates. Such an attacker can become more powerful when he/she repeats camera— based observation of the same user and system. Remote connected observation is also becoming a concern because high—resolution cameras are being distributed and networked in public places. The recent trend of targeting attacks and the advent of wearable computers make repeated camera—based shoulder surfing attacks an increasingly realistic threat to the PIN user interface.

LITERATURE SURVEY

To deal with these PIN entry non-technical attacks, one promising intervention is through the user interface. The main aspect has been incorporating indirect key entry measures to separate the visible keyed entry parts from the secret ones. Earlier research with passwords investigated cognitive authentication within the limitations of humans. Roth et al, used two colors for indirect PIN entry and the method was called Binary PIN. In each round, the system colored a random half of the numeric keys black and the other half while so users could enter the color of the PIN key by pressing a separate color key. Multiple rounds were played to enter a single digit of the PIN and repeated until all PIN digits were entered. Later Wiedenbeck el al. presented the convex hull click (H) for graphical passwords. In CH C, the long-term secret was pass-icons, and a random challenge used a number of random-located icons including both pass and fake icons. For authentication, users created a mental image of a convex hull linking pass-icons and clicked inside during multiple rounds. Weinshall introduced the cognitive authentication scheme (CAS) for graphical passwords, In CAS, a random challenge was a set of pictures including a password and fakes, randomly arranged on a table. Users traced a visual path based on the password pictures on the table and entered its destination value in multiple rounds. De Luca

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, November 2017

et aL. presented Color PIN, which used a set of colored characters as a random challenge assigned to numeric keys on a keypad. In each round, three different-colored characters were assigned to each numeric key while each character was duplicated on three numeric keys in different colors. In Color PIN, the secret PIN was actually color-digit combinations. The user entered a secret-colored character of a PIN key using a separate alphabetic keyboard repeatedly until the whole PIN was entered.

PROPOSED SYSTEM

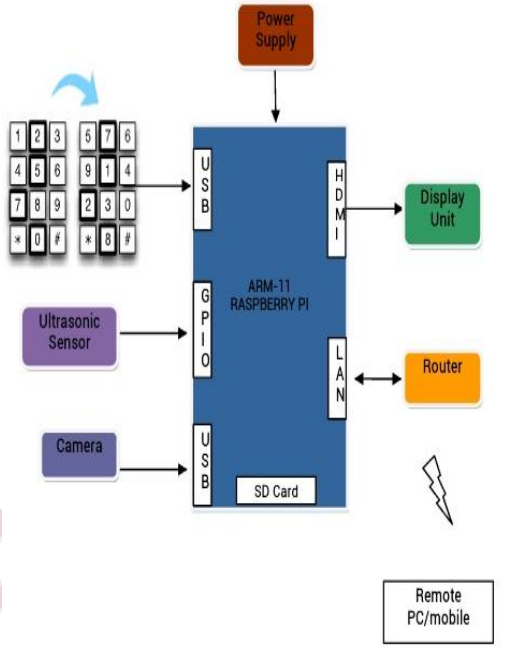

Fig:1:Block diagram

METHODOLOGY

Micro controller: This section forms the control unit of the whole project. This section basically consists of a Microcontroller with its associated circuitry like Crystal with capacitors, Reset circuitry, Pull up resistors (if needed) and so on. The Microcontroller forms the heart of the project because it controls the devices being interfaced and communicates with the devices according to the program being written.

Raspberry Pi: The Raspberry Pi delivers 6 times the processing capacity of previous models. This second generation Raspberry Pi has an upgraded Broadcom BCM2836 processor, which is a powerful ARM Cortex-A7 based quad-core processor that runs at 900MHz. The board also features an increase in memory capacity to 1Gbyte.

Liquid-crystal display (LCD) is a flat panel display, electronic visual display that uses the light modulation properties of liquid crystals. Liquid crystals do not emit light directly. LCDs are available to display arbitrary images or fixed images which can be displayed or hidden, such as preset words, digits, and 7-segment displays as in a digital clock.

Ultrasonic sensor: The sensor is primarily intended to be used in security systems for detection of moving objects, but can be effectively involved in intelligent children's toys, automatic door opening devices, and sports training and contact-less-speed measurement equipment. Infrared sensors are characterized by high sensitivity, low cost and are widely used. But, these sensors can generate false alarm signals if heating systems are active or temperature change speed exceeds some threshold level. Moreover, infrared sensors appreciably lose sensitivity if small insects penetrate the sensor lens. Ultrasound motion detection sensors are characterized by small power consumption, suitable cost and high sensitivity. That it why this kind of sensor is commonly used in home, office and car security systems. Existing ultrasound sensors consist of multiple passive and active components and are relatively complicated for production and testing. Sensors often times require a laborious tuning process.

Fig.2: Ultrasonic sensor

USB Camera: USB Camera is connected to the USB slot of the board, for live video streaming and if incorrect PIN is entered, it will capture the user's picture through the camera and sends it to the authorized person's mail using USB Wi Fi which connects the device to the router to access it over Wi-Fi network, At the users end, we will have live videos and captured user's pictures on the display who entered the wrong pin.

Fig.3: USB Camera

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, November 2017

USB Keypad: The USB keypad is connected to the USB port of the Raspberry Pi board to enter the PIN for accessing the system. Here there are two keypads are used in this project. One numeric keypad is a standard keypad in regular layout and the other is a small separate keypad in a random layout. The random layout keypad is called the challenge keypad because it permutes ten numeric keys as a random challenge. The challenge keypad varies according with the Ultrasonic Sensor. A user must use this challenge keypad to derive a fresh OTP. The user first locates a long-term PIN in regular layout and subsequently maps the key locations into the challenge keypad for OTP derivation. The user then enters the OTP on a regular layout keypad called the response keypad. The procedure can be repealed if the PIN length is greater than the limitation of the users short-term memory or if the OTP is forgotten before entry. When the user revisits the challenge keypad explicitly, the system must refresh the random challenges. Due to the random mapping between the two keypads, the system can verify the user's PIN from the OTP entry.

PC Monitor: The HDMI-VGA cable is attached updated raspberry-pi and the LJ R interface of the cable is attached updated. The face of the character getting captured can be visible on up-to-date. The Raspberry Pi has a HDMI port which you can plug without delay into a display or tv with an HDMI.

RESULT

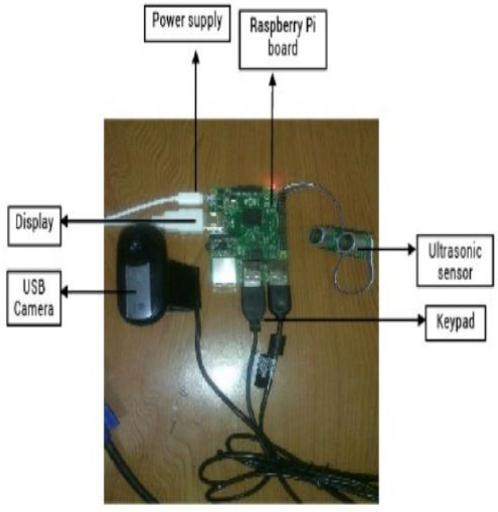

Fig.4:Hardware Kit

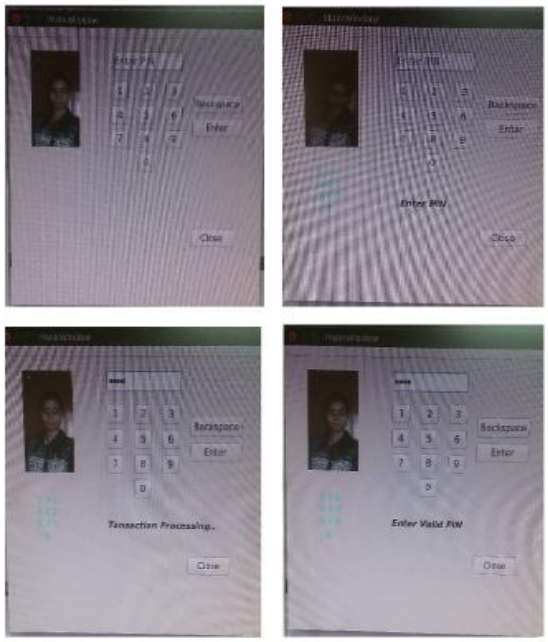

Fig.5: Snapshots of project

CONCLUSION AND FUTURE SCOPE

The project SteganoPIN: Indirect Method for PIN Entry Security has been successfully designed and tested. It has been developed by integrating features of all the hardware components and software used. Presence of every module has been reasoned out and placed carefully thus contributing to the best working of the unit, Secondly, using highly advanced Raspberry pi board and with the help of growing technology, the project has been successfully implemented.

The final section of the report outlines some features that could potentially be implemented in future releases. The current set of features implement is a minimum to what a consumer would expect. However, the security features can be further increased with the help of advanced board. This PIN Security system found its application in various sector. Depending upon application and other attributes like cost and coverage area particular pin security system can be used. The proposed system provides the combination of existing system to provide better security. Further, the use of GSM and GPS Modules made it more efficacious. With the help of GSM, the PIN entered is recorded in the SIM card and if such pin is entered incorrectly, then a message is sent to the user mobile number and through the GPS module the location of the host can be found out.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 10, November 2017

BIBLIOGRAPHY

Books Referred:

[1] Charles severance, "Eben upton: Raspberry pi", published by IEEE computer society, October 2013.

[2] Valeriu, Florin and Adrian-Viorel, Control System for Video Advertising Based on Raspberry Pi, 2014.

[3] Brian, Sudo Pi Cooler / Heater, 2014.Heate

Websites Referred:

[1] http://www.raspberry-projects.com

[2] http://codeduino.com/tutorials /arduino-vs-raspberry-pi/news /hardware/arduino-vs-raspberry-pi/

[3] http://www.zdnet.com/raspberry-pi-11 -reasons-why-its-the-perfect-small -server-70000 206/

[4] http://en.wikipedia.org/wiki/raspberry_pi

IEEE Papers Referred:

[1] J. Long and J. Wiles, No Tech Hacking: A 6u/de to Sac/ a/ Engineering,Dumpster Diving and Shoulder Surfing. Boston, MA, U : ng re . 2008.

[2] T. Kwon, S. Shin, andS. Na," "Covert allention shoulder surfing: Human adversaries are more powerful than expected," /FEE Trans. Syst., Man, Cybern, Syst., vol. 44, no. 6, pp. 716-727, Jun. 2014.

[3] T. Kwon and J. Hong, "Analysis and improvement of a PIN entry method resilient to shoulder-surfing and recording attacks," IEEE Trans. Inf Forensics security, vol. 10, no. 2, pp. 278-292, Feb. 2015.