Survey on Shoulder Surfing Resistant Pin Entry by Using Base Pin and Base Text

Mr.C. Senthil Kumar[1], Ms.T. Abinaya[2], Ms.G. Jaisri[3], Ms.V.K. Keerthi[4], Ms.L. Nirmala[5]

[1]Associate Professor, Dept. of ECE, Dr.NGP Institute of Technology, Coimbatore, TamilNadu, India
[2,3,4,5] Student, Dept. of ECE, Dr.NGP Institute of Technology, Coimbatore, TamilNadu, India

---***---

Abstract – *People uses their same personalized identification number (PIN) for multiple systems and in numerous sessions. Directly by entering their PIN are highly susceptible to shoulder-surfing attacks as others can effectively observe PIN entry with concealed cameras. Various PIN entry methods are proposed to achieve better performance but that produce heavy workload for users. Therefore to achieve high security and easy access, we present a practical indirect PIN entry method called Base Pin and Base text. The human–machine interface of Base Text which is designed to physically block shoulder surfing attacks. The system generates a one-time PIN that can safely be entered in plain view of attackers.*

Key Words: RFID System, Microcontroller, GSM, PIN, Password, Shoulder surfing, ATM.

1. INTRODUCTION

The main objective of this system is to develop a secure ATM in future. In general, all the keypad based authentication system having several possibilities of password guessing by means of shoulder movements. Shoulder-surfing is an attack on password by unauthorized persons which is hard to detect for the past decades. This problem has come up with a new solution by using base text which will display in the screen, with the generated words that will be added to the original pin. Another way is to develop with the GSM application between the user and Automated Teller Machine counter for communicating a password via the wireless medium.

2. LITERATURE SURVEY

KAI CAO [1] presents standard targets are typically used for structural (white-box) evaluation of fingerprint readers. However, there is no standard method for behavioral (black-box) evaluation of fingerprint readers in operational settings where variations in finger placement by the user are encountered. The goal of the research is to design and fabricate 3D targets for repeatable behavioral evaluation of fingerprint readers. 2D calibration patterns with known characteristics (e.g., sinusoidal gratings of pre-specified orientation and frequency, and fingerprints with known singular points and minutiae) are projected onto a generic 3D finger surface to create electronic 3D targets. A state-of-the-art 3D printer (Stratasys Objet350 Connex) is used to fabricate wearable 3D targets with materials similar in hardness and elasticity to the human finger skin. The 3D printed targets are cleaned using 2M NaOH solution to obtain evaluation-ready 3D targets.

LI LU [2] states the behavioural biometrics such as sliding dynamics and pressure intensity make use of on-screen sliding movements to infer the user's patterns. In this paper, it present Safeguard, an accurate and efficient smartphone user reauthentication (verification) system based upon on-screen finger movements. The computation and processing is performed at back-end which is transparent to the users. The key feature of the proposed system lies in fine-grained on-screen biometric metrics, i.e., sliding dynamics and pressure intensity, which are unique to each user under diverse scenarios. It first implement the scheme through five machine learning approaches and finally select the support vector machine (SVM)-based approach due to its high accuracy. Further analyse Safeguard to be robust against adversary imitation. It also validate the efficacy of our approach through implementation on off-the-shelf smartphone followed by practical evaluation under different scenarios. It process a set of more than 50 000 effective samples derived from a raw dataset of over 10 000 slides collected from each of the 60 volunteers over a period of one month.

MIANXIONG DONG [3] states in mobile social networks (MSN), with the aim of conserving limited resources, egotistic nodes might refuse to forward messages for other nodes. Different from previous work which mainly focuses on promoting cooperation between selfish nodes, we consider it from a more pragmatic perspective in this paper. Be specific, regard selfishness as a native attribute of a system and allow nodes to exhibit selfish behaviour in the process of message forwarding. Apparently, selfishness has a profound influence on routing efficiency, and thus novel mechanisms are necessary to improve routing performance when self-centred nodes are considered. First approach is to measure encounter opportunities between nodes. Then quantify receiving capabilities of nodes based on their available buffer size and energy. Taking both forwarding and receiving capabilities into account, they finally present a forwarding set mechanism, which could be deduced to a multiple knapsack problem to maximize the forwarding profit.. In fact, it chives a surprisingly high routing performance while consumes low transmission cost and resource in MSN.

JIN HONG [4] presents a user authentication scheme based on personal identification numbers (PINs) that is both secure and practically usable is a challenging problem. The most difficulty lies with the susceptibility of the PIN entry process to direct observational attacks, such as human shoulder-surfing and camera-based recording. The paper starts with an examination of a previous attempt at solving the PIN entry problem, which was based on an elegant adaptive black-and-white colouring of the 10-digit keypad in the standard layout. Even though the method required uncomfortably many user inputs, it had the merit of being easy to understand and use. Our analysis that takes both the experimental and theoretical approaches reveals multiple serious shortcomings of the previous method, including round redundancy, unbalanced key presses, highly frequent system errors, and insufficient resilience to recording attacks. The lessons learned through our analysis are then used to improve the black and white PIN entry scheme.

NAPA SAE-BAE [5] studies a simple and effective method for signature verification. An online signature is represented with a discriminative feature vector derived from attributes of several histograms that can be computed in linear time and requires constant space. This was first tested on the well-known MCYT-100 and SUSIG data sets. The results show that the performance of the proposed technique is comparable and often superior to state-of-the-art algorithms despite its simplicity and efficiency. By testing the proposed method a data set was collected from an uncontrolled environment and over multiple sessions. Experimental results on this data set confirm the effectiveness of the proposed algorithm in mobile settings. The results demonstrate the problem of within-user variation of signatures across multiple sessions and the effectiveness of cross session training strategies to alleviate these problems.

KATHERINE ISBISTER [6] investigates on multitouch gestures on touch sensitive devices. A canonical set of 22 multitouch gestures was defined using characteristics of hand and finger movement. Then, a multitouch gesture matching algorithm was developed. Two different studies were performed to evaluate the concept. The experiment was performed in order to explore feasibility of multitouch gestures for user authentication. In addition, the tests demonstrated a desirable alignment of usability and security as gestures that were more secure from a biometric point of view were rated as more desirable in terms of ease, pleasure, and excitement. Second, a study involving a three-session experiment was performed. Results indicate that biometric information gleaned from a short user-device interaction remains consistent across gaps of several days, though there is noticeable degradation of performance when the authentication is performed over multiple sessions. In addition, it shows that user-defined gestures yield the highest recognition rate among all other gestures.

XI ZHAO [7] states behavioural biometrics have recently begun to gain attention for mobile user authentication. The feasibility of touch gestures as a novel modality for behavioural biometrics has been investigated. Here they proposed to apply a statistical touch dynamics image trained from graphic touch gesture features to retain discriminative power for user authentication while significantly reducing computational time during online authentication. Systematic evaluation and comparisons with state-of-the-art methods have been performed on touch gesture data sets. Implemented as an Android App, the usability and effectiveness of the proposed method have also been evaluated.

TAEKYOUNG KWON [8] states when a user interacts with a computing system shoulder surfing attacks are of great concern. Previous methods presumed limited cognitive capabilities of a human adversary as a deterrent, but there was a drawback. He shows that human adversaries, even without a recording device, can be more effective at eavesdropping than expected, in particular by employing cognitive strategies and by training themselves. This approach called covert attentional shoulder surfing indeed can break the well known PIN entry method previously evaluated to be secure against shoulder surfing. Another contribution in the paper is the formal modelling approach by adapting the predictive human performance modelling tool for security analysis and improvement.

VENUGOPAL V. VEERAVALL [9] presents classical problem of quickest change detection is studied with an additional constraint on the cost of observations used in the detection process. The change point is modelled as an unknown constant, and minimax formulations are proposed for the problem. The objective in these formulations is to find a stopping time and an ON–OFF observation control policy for the observation sequence, to minimize a version of the worst possible average delay, subject to constraints on the false alarm rate and the fraction of time observations are taken before change. An algorithm called DE-Cu Sum is proposed and is shown to be asymptotically optimal for the proposed formulations, as the false alarm rate goes to zero. Numerical results are used to show that the DE-Cu Sum algorithm as good trade off curves and performs significantly better than the approach of fractional sampling, in which the observations are skipped using the outcome of a sequence of coin tosses, independent of the observation process. This study is guided by the insights gained from an earlier study of a Bayesian version of this problem.

ALEX C. KOT [10] propose here a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity. In the enrollment, two fingerprints are captured from two different fingers. It captures positions from one fingerprint to the other fingerprint, and the reference points from both fingerprints. The system requires two fingerprints from the same two fingers which are used for the authentication. A two-stage fingerprint matching process will match the two query fingerprints against a combined minutiae template. The complete feature of a single fingerprint will not be compromised when the database is stolen. Furthermore, because of the similarity in topology, it is difficult for the attacker to distinguish a combined minutiae template from the original minutiae templates. They are able to convert the combined fingerprints of a same person into a real-look alike combined fingerprint. Finally, a new virtual identity is created for the two different fingerprints, which can be matched using minutiae-based finger print matching algorithms.

JOSEPH A. O'SULLIVAN [11] states in the recent advancement, the electrocardiogram (ECG) is an trending biometric modality and as such deserves a systematic review and discussion of the associated methods and findings. They reviewed most of the techniques that have been applied to the use of the electrocardiogram for biometric recognition. In particular, they categorize the methodologies based on the features and the classification schemes. Finally, a comparative analysis of the authentication performance of a few of the ECG biometric systems is presented, using our inhouse database. The comparative study includes the cases where training and testing data come from the same and different sessions (days). The authentication results show that most of the algorithms that have been proposed for ECG-based biometrics perform well when the training and testing data come from the same session. However, when training and testing data come from different sessions, a performance degradation occurs. Multiple training sessions were incorporated to diminish the loss in performance. That notwithstanding, only a few of the proposed ECG recognition algorithms appear to be able to support performance improvement due to multiple training sessions. By doing the investigation they found only three of the algorithms produced equal error rates (EERs) in the single digits, including an EER of 5.5% using a method proposed by them.

PATRIZIO CAMPISI [12] presents Data security and privacy are crucial issues to be addressed for assuring a successful deployment of biometrics-based recognition systems in real life applications. In this paper, a template protection scheme exploiting the properties of universal background models, eigen-user spaces, and the fuzzy commitment cryptographic protocol is presented. A detailed discussion on the security and information leakage of the proposed template protection system is given. The effectiveness of the proposed approach is investigated with application to online signature recognition. The given experimental results, evaluated on the public MCYT signature database, show that the proposed system can guarantee competitive recognition accuracy while providing protection to the employed biometric data.

HAIYING SHEN [13] states in mobile ad hoc networks (MANETs), tasks are conducted based on the cooperation of nodes in the networks. However, since the nodes are usually constrained by limited computation resources, selfish nodes may refuse to be cooperative. Reputation systems and price-based systems are two main solutions to the node non cooperation problem. A reputation system evaluates node behaviours by reputation values and uses a reputation threshold to distinguish trustworthy nodes and untrustworthy nodes. The transactions of a packet forwarding service. is generally controlled by using virtual cash, literally a price based system. Although these two kinds of systems have been widely used, very little research has been devoted to investigating the effectiveness of the node cooperation incentives provided by the systems. Here they used game theory to analyse the cooperation incentives provided by the two systems. They find that the strategies of using a threshold to determine the trustworthiness of a node in the reputation system and of rewarding cooperative nodes in the price-based system may be manipulated by clever or wealthy but selfish nodes. Illumined by the investigation results, we propose and study an integrated system. Theoretical and simulation results show the superiority of the integrated system over an individual reputation system and a price-based system in terms of the effectiveness of cooperation incentives and selfish node detection.

VISHAL M PATEL[14]presents a solution that refers to the problem of continuously verifying the identity of an user for the purpose of securing the device with the help of Active authentication (AA). They address the problem of quickly detecting intrusions with lower false detection rates in mobile AA systems with higher resource efficiency. The Quickest Change Detection (QCD) algorithms for the detection which quickly detect intrusions in mobile AA systems is by Bayesian and Minimax versions. The following algorithms are extended with an update rule to facilitate low frequency sensing which leads to low utilization of resources. The proposed framework effectiveness is demonstrated using three publicly available unconstrained face and touch gesture based AA datasets. It is shown that the proposed QCD-based intrusion detection methods can perform better than many state of- the-art AA methods in terms of latency and low false detection rates.

3. CONCLUSIONS

This project is made with pre planning, that it provides flexibility in operation. This innovation has made the more desirable and economical. This project "ATM SHOULDER-SURFING RESISTANT PIN ENTRY BY USING BASE PIN AND BASE TEXT" is designed with the hope that it is very much economical and help full to security purpose for banking sector, ATM center, hotels and shopping etc.. This project helped us to know the periodic steps in completing a project work. Thus we have completed the project successfully.

REFERENCES

[1] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Trans. Syst., Man, Cybern., Syst., vol. 44, no. 6, pp. 716–727, Jan. 2014.

[2] N. Sae-Bae, N. Memon, K. Isbister, and K. Ahmed, "Multitouch gesture based authentication," IEEE

Trans. Inf. Forensics Security, vol. 9, no. 4, pp. 568–582, Apr. 2014.

[3] D. Guru and H. Prakash, “Online signature verification and recognition: An approach based on symbolic representation,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 31, no. 6, pp. 1059–1073, Jun. 2009.

[4] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, “Cancelable templates for sequence-based biometrics with application to on-line signature recognition,” IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 40, no. 3, pp. 525–538, May 2010.

[5] E. Argones Rua, E. Maiorana, J. Alba Castro, and P. Campisi, “Biometric template protection using universal background models: An application to online signature,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 269–282, Feb. 2012

[6] U. Park, R. R. Jillela, A. Ross, and A. K. Jain, “Periocular biometrics in the visible spectrum,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 96–106, Mar. 2011

[7] E. A. Rua, E. Maiorana, J. A. Castro, and P. Campisi, “Biometric template protection using universal background models: An application to online signature,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 269–282, Feb. 2012.

[8] X. Zhao, T. Feng, W. Shi, and I. Kakadiaris, “Mobile user authentication using statistical touch dynamics images,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 11, pp. 1780–1789, Nov 2014.

[9] T. Banerjee and V. Veeravalli, “Data-efficient quickest change detection in minimax settings,” IEEE Transactions on Information Theory, pp. 6917 – 6931, Oct 2013

[10] K. Wei et al., “Camf: Context-aware message forwarding in selfish mobile social networks,” IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 8, pp. 2178–2187, Aug. 2014.