Eleyon
SOUTH ASIAN JOURNAL OF ENGINEERING AND TECHNOLOGY
Full Length Article

Android based Access Control Systems using Sensory-Data

[a]R.Saranya,[b] A. Mohammad Isbulla, [b] C. Sowntharajan, [b]R. Suriya,

[a] *Assistant Professor, Dept. of CSE, Surya Engineering College, Erode, Tamil Nadu, India*
[b] *UG Scholar, Dept. of CSE, Surya Engineering College, Erode, Tamil Nadu, India*

***Corresponding Author**
R.Saranya

ABSTRACT: We investigate the accelerometer and gyroscope motion sensor-based cross-site input inference attacks that may compromise the security of many mobile Web users, and quantify the extent to which they can be effective. We formulate our attacks as a typical multi-class classification problem and build an inference framework that trains a classifier in the training phase and predicts the user's new inputs in the attacking phase. To make our attacks effective and realistic, we design unique techniques and address major data quality and data segmentation challenges. We intensively evaluate the effectiveness of our attacks using 98 691 keystrokes collected from 20 participants. Overall, our attacks are effective, for example, they are about 10.8 times more effective than the random guessing attacks regarding inferring letters. We also perform experiments to evaluate the effect of using the data perturbation defence techniques on decreasing the accuracy of our input inference attacks. Our results demonstrate that researchers, smartphone vendors, and app developers should pay serious attention to the motion sensor-based cross-site input inference attacks that can be pervasively performed, and start to design and deploy effective defence techniques.

Introduction

Smartphones have been severely targeted by cybercrimes, and their sensors have created many new vulnerabilities for attackers to compromise users' security and privacy. One typical vulnerability is that high-resolution accelerometer and gyroscope motion sensors could be used as side channels for attackers to infer users' sensitive keyboard tappings on smartphones. Such input inference attacks are feasible because motion sensor data are often correlated to the tapping behaviours of users and the positions of keys on a keyboard. Some researchers have studied the effectiveness of input inference attacks performed by malicious native apps on smartphones, but their threat models, focuses, and challenges are different from ours (Section II-B). While input inference attacks can be performed by malicious native apps, they can indeed be more pervasively performed by malicious webpages

Existing System:

Access card authentication is critical and essential for many modern access control systems, which have been widely deployed in various governments, commercial and residential environments. Access control systems can be divided into two broad categories. The first category is based on mechanical matching, such as keys and combination locks. Access control systems if and only if the blade of the key matches the keyway of the lock or the correct numerical sequence for combination lock has been dialled. Electronic authentication including barcode, magnetic stripe, biometrics and etc. Although advanced biometric authentication methods such as fingerprint and iris identification can further identify the user who is requesting authorization, they incur high system costs and access privileges cannot be transferred among trusted users. Anovel electronic proximity authentication framework that enhances the security level of existing RFID-based access control systems with backward compatibility.

Proposed System:

Dynamic data into the traditional authentication information by using sensors such as accelerometer, gyroscope and etc.This authentication framework is adaptive to the change of encryption complexity of the access control systems and could be adopted with minor modification of existing infrastructure. Dynamic authentication significantly increases the key space for proximity authentication systems with the integration of low-cost sensors. We have fully implemented and built a running prototype of the proposed dynamic authentication framework.

The Intel Wireless Identification and Sensing Platform (WISP). Based on the running prototype, we have extensively evaluated our design in terms of system accuracy and usability in the real-world settings. The identification information on access cards normally are static. The addition of dynamic sensory data from onboard sensors, Significantly increase the security key space *P* and hence the level of security for existing electronic authentication systems. A wide variety of sensors including accelerometer, gyroscope and etc. Can be used in our system.

SYSTEM ARCHITECTURE:

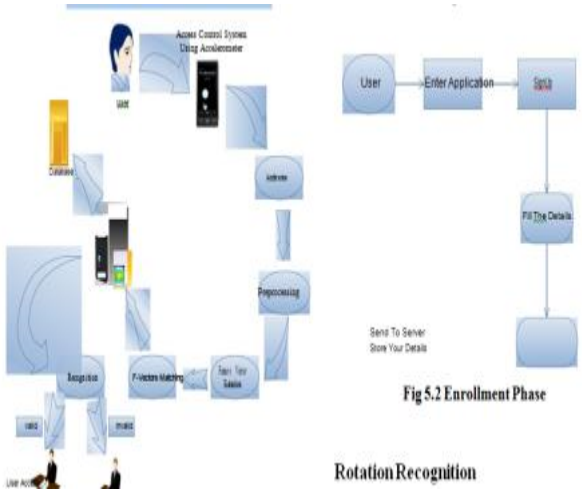
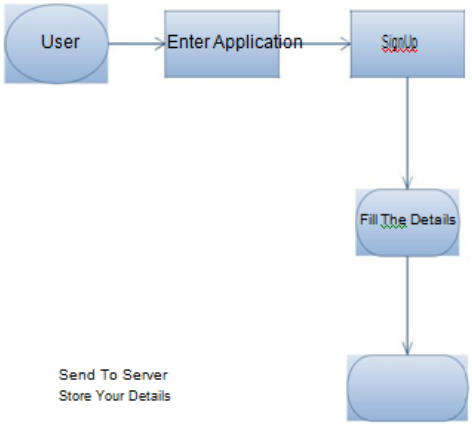


Fig 5.2 Enrollment Phase

MODULES

Enrollment Phase

The aim of this phase is to allow a user and a server to negotiate a shared secret to authenticate succeeding logins for this user. The user begins using Accelerometer sensor for the Access control Systems. The following figure 5.2 shows the enrollment phase.



Rotation Recognition

Dynamic authentication with sensory information design. In this section, we further elaborate on the detailed sensor rotation recognition algorithms. By comparing the sample data of accelerometer. We find that output of the accelerometer exhibits a more complex behavior. This is because gyroscope measures the angular velocity and tends to generate an impulse during one single basic rotation, which could be treated as a special case of the output of the accelerometer. Therefore in this section, we use the sensory data of accelerometer to illustrate the whole rotation recognition algorithms and discuss how to deal with the sensory data of gyroscope.

Data Pre-Processing

The first step of rotation recognition is data pre-processing. The main goals are to separate and filter each individual basic rotation from a series of raw accelerometer data. In order to separate the individual basic rotations, we first need to identify the pause between two consecutive rotations. During such pauses, the three-axis readings of an accelerometer would remain relatively stable and unchanged for a short period of time. In order to accurately recognize such pauses and separate different basic rotations, we adopt a

sliding windowapproach. In this approach, the accelerometer readings in the first *tw*second are buffered into the sliding window. All data in the sliding window are then fitted by a first-order polynomial function. If the coefficient of first-order polynomial is less than a threshold (1 in our implementation), we consider the accelerometer remain stationary within the time frame of this window. Followed by this pause detection in the current window, the window would slide for a step of *ts*seconds, with *ts*duration of new data appended to the end of the sliding window while the first *ts*duration of sensory data are discarded. Empirically, we set *tw*= 1*s* and *ts*= 0.3*s* in our system implementation. In this way, we have achieved accurate separation of basic rotations in one complete authentication. To visualize above data pre-processing step, one authentication with 4 basic rotations that performed slowly on our prototype implementation. The shaded regions represent sliding windows at three pauses. The accelerations on three axes of the accelerometer are rather stable during pauses between different basic rotations.

After identifying pauses between basic rotations, we then use least square estimation to fit the raw readings for each individual basic rotation from the accelerometer.

Feature Vector Extraction

After separating basic rotations for one single authentication, we match them with standard feature vectors. As feature based classification of time-series data has a simple model and lower computation, we choose this method for rotation recognitions. First, feature vectors (F-Vectors) for each individual basic rotation are extracted based on their fitting functions created in the previous section. Specifically, we extract the start and end sensory data, the maximal and minimal sensor readings and the corresponding time of these events within one basic rotation for a three-axis accelerometer.

A sufficiently large feature vector for use in the authentication protocol. In our approach, the feature vector will be used to authenticate a key or to directly generate a key, and thus it needs to be of high entropy from an attacker's point of view, i.e. involve a large amount of uncertainty. We argue that shaking is an appropriate movement for creating entropy: it creates varying sensor readings, because it is one of the human movement patterns that includes the highest frequency components. Slower movements will intuitively not generate as much entropy.

F-Vectors Matching

After extracting feature vectors, we then try to match the extracted feature vector with standard feature vectors in the database to recognize a specific basic rotation. Standard feature vectors with given *n* could be mathematically calculated and automatically generated since the acceleration components on three axes represent a trigonometric relationship with acceleration of gravity. Taking the rotation as an example, after the accelerometer clockwise rotates π degrees, the acceleration components *Ax*and *Ay* during such rotation can be calculated as $Ax = G\cos\theta$and $Ay = G\sin\theta(\theta \in [\alpha, \alpha+\pi])$. Therefore, it is easy for users to reset their keys without any modification on access cards. In order to match extracted F-vectors of a basic rotation to standard ones in database, we use Euclidean distance to measure the closeness of these two vectors.

Accessing Service

User enter the browser and Register to server then server through mail on password then user receive the mail and send to server .then server verify both password ,if correct the password open the view all detail ,else if not match that password means you won't allow the site inside.

Conclusion

In this paper, we propose a dynamic authentication with sensory information for the access control systems. Different from existing schemes of authentication in access control systems, which mainly based on static information on cards, our dynamic authentication method combines sensory information from onboard sensors and conventional static ID information. Two case studies of the dynamic authentication are proposed. We theoretically analyzes their highly increased key space, which exponentially multiplied static key space in existing authentication methods. To evaluate performance of our design, we built a prototype system and validate authentication mechanism experimentally. In experiments, the proposed authentication algorithm showed a 95% high

accuracy rate within different users. In the simulation part, we comprehensively study the impact of sensory data sample size and sensory data loss, which found to be critical factors from experiments on authentication algorithm. Most simulation results validate our algorithm effectively. Growing popularity of electronically based authentication in proximity access control systems calls for a higher security.

References

[1] Y. Shu, Y. Gu, and J. Chen, "Sensory-Data-Enhanced Authentication for RFID-based Access Control Systems," in IEEE MASS, 2012.

[2] A. Juels, "RFID security and privacy: A research survey," IEEE Journal on Selected reas in Communications, vol. 24, no. 2, pp. 381–394, 2006.

[3] R. Mayrhofer and H. Gellersen,"Shake well before use: Authentication based on accelerometer data," Pervasive Computing, pp. 144– 161, 2007.

[4] M. Burmester, T. Van Le, B. DeMedeiros, and G. Tsudik, "Universally composable RFID identification and authentication protocols," ACM Transactions on Info. and System Security, vol. 12, no. 4, p. 21, 2009.

[5] J. Kong, H. Wang, and G. Zhang, "Gesture recognition model based on 3D accelerations," in IEEE ICCSE, 2009.

[6] S. Mitra and T. Acharya, "Gesture Recognition: A survey," IEEE Transactions on Systems, Man and Cybernetics, 2007.

[7] S. Zhou, Q. Shan, F. Fei, W. J. Li,C. P. Kwong, P. C. K. Wu, B. Meng, C. K. H. Chan, and J. Y. J. Liou, "Gesture recognition for interactive controllers using MEMS motion sensors," in IEEE NEMS, 2009.

[8] T. Park, J. Lee, I. Hwang, C. Yoo, L. Nachman, and J. Song, E-gesture: a collaborative architecture for energy- efficient gesturerecognition with hand-worn sensor and mobile devices," in ACM SenSys, 2011.

[9] A. P. Sample, D. J. Yeager, P. S. Powledge, A. V. Mamishev, andJ. R. Smith, "Design of an RFID-based battery-free programmablesensing platform," IEEE Trans. Instrum. Meas., 2008.

[10] M. Buettner and D. Wetherall, "Anempirical study of UHF RFID performance," in ACM MobiCom, 2008.

[11] A. P. Sample, D. J. Yeager, and J.R. Smith, "A capacitive touch interface for passive RFID tags," in IEEE RFID, 2009.3