Continuous Authentication on Smartphones Using An Artificial Immune System

Nawaf Aljohani[1], Joseph Shelton, Kaushik Roy
Department of Computer Science, North Carolina A&T State University, Greensboro, U.S.A
naaljoha@aggies.ncat.edu[1]

Abstract

Most of the authentication systems require the users to provide their credential for authentication purposes by providing their passwords or their biometric data. However, as long as the user remains active in the system, there is no mechanisms to verify whether the user who provides the credential is still in control of the device or not. Most mobile devices rely upon passwords and physical biometrics to authenticate users only when they start using the device. Active authentication based on analyzing the user's touch interaction could be a reasonable solution to verify that a legitimate user is still in control of a smartphone or tablet. In this research, an Artificial Immune System (AIS) is proposed to apply to continuously authenticate the users based on touch patterns. Our results show that AIS is able to actively authenticate 96.89% of the users correctly.

Introduction

During the authentication process, a primary concern for users and designers is the level of security. The process of authenticating an individual must be both secure and effective to be applicable for a real world authentication system. In the event that the authentication process is compromised, other aspects in the system such as availability, confidentiality, and integrity would be easily compromised as well. Knowledge-based authentication systems, such as password or pin, have several drawbacks, but many systems still use this method to authenticate legitimate users due to their simplicity and flexibility. This research proposes an authentication method for the users based on finger swipe movements.

Touch screen technology is used in many mobile devices where users have the ability to access various data and resources at anytime. Most of the smartphones use PINs to authenticate the users. However, a traditional PIN typically consists of four to eight digits, making it easy to guess with its small password space and thus vulnerable to attacks [Chang *et al*., 2012]. Nowadays, most mobile devices use graphical password that have a larger and more accepted password space. Though graphical password increases the password space in touch screen handheld mobile devices, there are no further authentication processes after unlocking the touch screen. Thus, the attacker has the ability to access and control all the users' data and resources as long as the attacker gains access to a device after it is unlocked. This research aims to continuously authenticate the users without asking them to provide the login information multiple times while the smartphones or tablets are in use.

In this research, an artificial immune system (AIS) approach will be used to secure mobile devices. The immune system is considered to be a highly complex functional system that protects the body from foreign diseases causing pathogens [Shojaie and Moradi, 2008]. This immunology inspired researchers to develop the computational intelligence technique, which is called AIS. AIS has been used in solving complex computational problems, such as classification, recognition, and network security [Dudek, 2012]. This research makes use of an AIS which has the ability to continuously keep track of any changes in the environment based on recognizing the patterns of 'self' and predicting and detecting new patterns of 'non-self'.

This research uses a set of 11 behavioral touch features that were extracted while the users were interacting with their smartphones. This research uses touch data collected from 100 users and each subject has 100 instances [Sitová *et al*. 2016]. This research proposes the use of an AIS to continuously authenticate the smartphones users where the security of smartphone is enhanced.

Related Work

Sitová et al. proposed a set of behavioral features based on hand movement, orientation, and grasp to continuously authenticate mobile users [Sitová *et al*. 2016]. The data is collected from 100 participants under two conditions:

walking and sitting. The achieved equal error rates (EERs) are 7.16% (walking) and 10.05% (sitting) where walking interactions are more richer than sitting interactions due to the distinctive body movements caused by walking and hand-movement dynamics from taps. Sitová et al. believe that each mobile user has postural preferences for interacting with touch screen which can be used to authenticate the users. In their dataset, Sitová et al. designed 96 features and extracted data while users are walking and sitting. The dataset was divided into two types of features that grasp resistance and stability and the data was collected by using three sensors: accelerometer, gyroscope, and magnetometer [Sitová *et al*. 2016]. The user touch data was acquired using Samsung Galaxy S4 smartphone where the average duration of a user's interaction with touch screen was 11.6 minutes per session. Sitová et al. used scaled Manhattan (SM), scaled Euclidian (SE), and 1-class Support Vector Machines (SVM) to verify the users.

Frank et al. [Frank *et al*., 2013] determined whether or not a classifier could be used to continuously authenticate users based on their interaction with the touch screen. Authors in [Frank *et al*., 2013] proposed 30 behavioral touch features that could be collected from raw touch screen logs. These features were used to identify a user based on the way he/she interacts with the touch screen. Furthermore, Frank et al. explained the reasons that mobile devices are at higher risk than that of desktop computers due to that fact that mobile devices can be easily lost or stolen. Their dataset consists of 41 subjects and the data was collected from four different smart phones.

Feng et al. [Feng *et al*., 2012] introduced FAST: Fingergestures Authentication System using Touchscreen. Their idea was to extract data from touch screen interactions and validate the data by using a digital sensor glove. Their proposed approach relied on Random Forest (RF) and Bayesian network classifiers to authenticate mobile users continuously. Feng et al. used a dataset that consisted of 40 users and authors obtained a False Accept Rate (FAR) of 4.66%, while the False Reject Rate (FRR) was 0.13%.

Meng et al. [Meng *et al*., 2013] proposed a scheme based on touch dynamics that used a set of behavioral features to improve the accuracy of user authentication. Their dataset consisted of 21 features that were collected form users interaction with the touch screen. All data was extracted from 20 Android phones. Researchers in [Meng *et al*., 2013] found that a Neural Network (NN) achieved an average error rate of 7.8%. In addition, Meng et al. optimized the NN by implementing Particle Swarm Optimization (PSO) and they reported an average error rate of about 3%.

Proposed Approach

There are three types of AISs reported in the literature: 1) Negative selection, 2) Clonal selection, and 3) Immune Network [Watkins *et al*., 2002].

The main goal of the Negative Selection (NS) is to provide tolerance for self cells that indicate the ability to detect non self antigens. This idea is used in many areas such as network security, where NS generates detectors and then removes those that can detect self patterns. The rest of detectors can be used to detect anomaly. The detectors, which are randomly generated, are representation for matching the authorized users' patterns to create the self profile [Greensmith *et al*., 2010]. A detector is a set of intervals for each feature a detector is created for. Any self pattern number lies in the interval of a detector means that the detector detects the self pattern. As a result of that all detectors that detect self patterns must be removed. The remaining detectors are used to detect unauthorized users.

Clonal Selection (CS) differs from the NS approach by selecting the detectors that proliferate over those that do not. The main feature of CS is the new detectors that are the copies of their parents and reactivated detectors are eliminated afterwards. In this research, CS is implemented to authenticate smartphone users continuously instead of NS because CS, in some cases, gives better accuracy than NS due to the fact that the nearest created detectors cloned (See Figure 1). First, CS generates *n* detectors and searches for new patterns. CS selects the nearest detectors to be cloned using distance metric such as the Euclidean distance. CS clones the nearest detectors from the detectors and the new pattern. CS then finds best matching clone and assigns clone class to antigen. Finally, it deletes other superfluous clones and for each deletion, replaces with new randomly generated detectors [Greensmith *et al*., 2010]. In this research, we created 100 detectors and then remove those detectors that can detect self elements. Self elements in the dataset represent one subject. The remaining subjects are non-self elements. The detectors detect the self elements by exploring self subject's features patterns. Suppose the smartphone is unlocked by an attacker, detectors created by CS are used for continuously authenticating the user by tracking the user's interactions with touch screen. As long as the smartphone is unlocked, CS detectors are used to analyze the user's interactions via detectors. Once a certain number of detectors detect abnormal interactions, the device is locked due to unauthorized access. In our experiments, abnormal interactions must be detected by four detectors to detect unauthorized access.

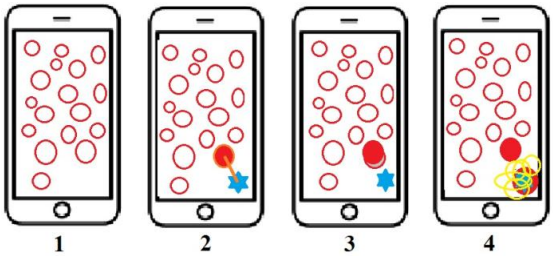

Figure 1. Clonal selection concept

Table 1. behavioral features [Sitová *et al*., 2016].

Name	Description
Systime	Absolute time-stamp
EventTime	Sensor event relative time-stamp
ActivityID	Belonged activity
Pointer_count	1: Single touch 2: Multi-touch
PointerID	0: Single touch; or first pointer in multi-touch 1: Second pointer in multi-touch
ActionID	0 or 5: DOWN 1 or 6: UP 2: MOVE
X	Touch location in X coordination
Y	Touch location in Y coordination
Pressure	Touch pressure
Contact_size	Touch contact size
Phone_orientation	0: Portrait and no rotate 1: device rotated 90 degrees counterclockwise 3: device rotated 90 degrees clockwise

Experimental Results

We conducted our experiments on TouchEvent dataset that has 11 behavioral features [Sitová *et al*. 2016]. A list of features is shown in Table 1. First, we ran the AIS with only two subjects, and we achieved an accuracy of 100%. The accuracy remains 100% as long as we are using 5 subjects. After adding 6th subject and its instances, the accuracy went down to 99.33%. Initially, we added a new subject to the dataset and ran AIS. The accuracies for all the users are shown in Table 2.

It is clear that at a certain point, adding users do not affect the accuracy of AIS as shown in Figure 2. For each run, AIS is executed for 1000 generations and the number of detectors is 100. Unauthorized user is detected if at least 4 generated detectors are able to detect the touch screen interactions.

We ran the AIS on the entire dataset for 20 times. For each run, we experimented it for 1000 generations. Also, for each run, we use 100 detectors. The best accuracy for 20 runs is 96.89% and the average is 93.81% (See Figure 3). The average of FRR out of 20 runs is 0.9381 which shows unauthorized users detections. The average of FARs on the other hand is 0.06.

Table 2. Results of adding each user

User	Accuracy	User	accuracy	User	accuracy
2	1	35	0.939246	68	0.919757
3	1	36	0.9409309	69	0.924135
4	1	37	0.9417141	70	0.920664
5	1	38	0.9473414	71	0.922134
6	0.993333	39	0.9471731	72	0.927492
7	0.993036	40	0.9375915	73	0.923671
8	0.991111	41	0.938403	74	0.923728
9	0.991444	42	0.941495	75	0.924533
10	0.994636	43	0.940016	76	0.919508
11	0.99447	44	0.941293	77	0.927949
12	0.991282	45	0.952014	78	0.930393
13	0.987418	46	0.940592	79	0.927764
14	0.970905	47	0.941241	80	0.923218
15	0.9675	48	0.941101	81	0.92879
16	0.964118	49	0.945453	82	0.922505
17	0.966471	50	0.944878	83	0.926952
18	0.965409	51	0.944246	84	0.897615
19	0.964263	52	0.939213	85	0.926551
20	0.950119	53	0.941237	86	0.927851
21	0.963009	54	0.946933	87	0.921804
22	0.9543478	55	0.936571	88	0.925723
23	0.9558696	56	0.946563	89	0.923815
24	0.9473167	57	0.939958	90	0.926972
25	0.9522769	58	0.955611	91	0.923371
26	0.9377635	59	0.954308	92	0.917491
27	0.9335714	60	0.931101	93	0.91647
28	0.9355788	61	0.913392	94	0.910208
29	0.9428851	62	0.919519	95	0.917088
30	0.9464194	63	0.914184	96	0.921645
31	0.9375403	64	0.916935	97	0.919436
32	0.9340909	65	0.922818	98	0.925315
33	0.9328699	66	0.921142	99	0.922192
34	0.9395126	67	0.922046		

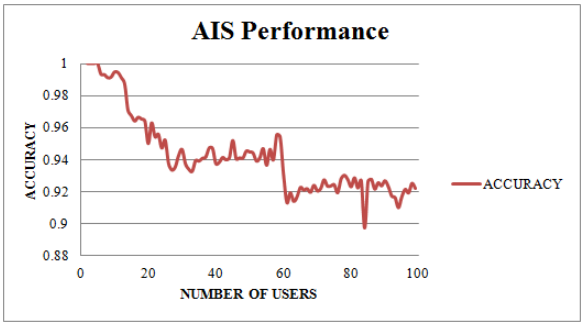

Figure 2. CS Performance

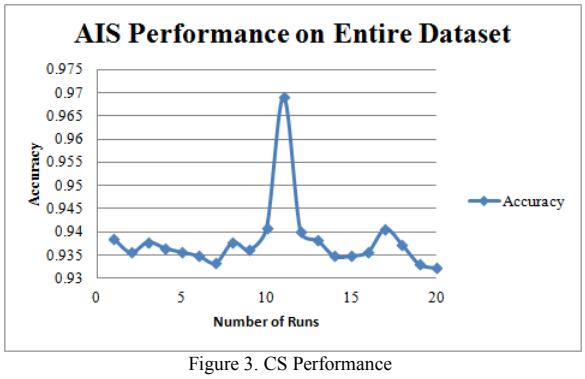

Figure 3. CS Performance

Conclusion and Future Work

We find from the experimental results that AIS can be used to authenticate smartphone users continuously. AIS approach has the flexibility in restricting the authentication process based on the sensitivity of the mobile devices by reducing the number of detectors. The best performance of CS on the entire dataset was 96.89%. However, there seems to be a promise with the increasing number of detectors for each run. This research uses CS for an AIS to continuously authenticate the users.

Future work will be focused on evaluating the impact of each behavioral feature on the overall accuracy. Furthermore, future work will evaluate the effect of increasing the number of detectors. This may improve accuracy by increasing the chance of detecting more unauthorized mobile interactions. Also, a comparison between CS and NS will be conducted. In addition, the performance of CS and NS will be compared with other classifies such as SVM.

Acknowledgements

This research is supported by the Army Research Office (Contract No. W911NF-15-1-0524).

References

[Chang *et al*., 2012] Chang, T. Y., Tsai, C. J., & Lin, J. H. (2012). A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. *Journal of Systems and Software*, *85*(5), 1157-1165.

[Dudek, 2012] Dudek, G. (2012). An artificial immune system for classification with local feature selection. *IEEE Transactions on Evolutionary Computation*, *16*(6),p.847-860.

[Feng *et al*., 2012] Feng, Tao, Ziyi Liu, Kyeong-An Kwon, Weidong Shi, Bogdan Carbunar, Yifei Jiang, and Nhung Nguyen. (2012). "Continuous Mobile Authentication Using Touchscreen Gestures." *2012 IEEE Conference on Technologies for Homeland Security (HST)*. Print.

[Frank *et al*., 2013] Frank, M., R. Biedert, E. Ma, I. Martinovic, and D. Song. (2013) "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication." IEEE Trans.Inform.Forensic Secur. IEEE Transactions on Information Forensics and Security 8.1 pp.136-48. Print

[Greensmith *et al*., 2010] Greensmith, J., Whitbrook, A., & Aickelin, U. (2010). Artificial immune systems. In *Handbook of Metaheuristics* (pp. 421-448). Springer US.

[Meng *et al*., 2013] Meng, Yuxin, Duncan S. Wong, Roman Schlegel, and Lam-For Kwok. (2013) "Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones." *Information.Security and Cryptology Lecture Notes in Computer Science*. pp. 331-50. Print.

[Shojaie *et al*., 2008] Shojaie, S., & Moradi, M. H. (2008). An evolutionary artificial immune system for feature selection and parameters optimization of support vector machines for ERP assessment in a P300-based GKT. In *Biomedical Engineering Conference, 2008. CIBEC 2008. Cairo International* (pp. 1-5). IEEE.

[Sitová *et al*., 2016] Sitová, Z., Šeděnka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P., & Balagani, K. S. (2016). HMOG: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Transactions on Information Forensics and Security*, *11*(5), 877-892.

[Watkins et al., 2002] Watkins, Andrew and Timmis, Jon (2002) *Artificial Immune Recognition System (AIRS):Revisions and Refinements*