IEEE TRANSACTIONS ON
EMERGING TOPICS
IN COMPUTING

Received 25 June 2014; revised 20 October 2014; accepted 2 December 2014. Date of publication 17 December, 2014;
date of current version 6 March, 2015.

Digital Object Identifier 10.1109/TETC.2014.2379991

User-Habit-Oriented Authentication Model: Toward Secure, User-Friendly Authentication for Mobile Devices

JAMIE SETO, YE WANG, AND XIAODONG LIN, (Senior Member, IEEE)

Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON L1H 7K4, Canada

CORRESPONDING AUTHOR: X. LIN (xiaodong.lin@uoit.ca)

ABSTRACT Mobile device security has become increasingly important as we become more dependent on mobile devices. One fundamental security problem is user authentication, and if not executed correctly, leaves the mobile user vulnerable to harm like impersonation and unauthorized access. Although many user authentication mechanisms have been presented in the past, studies have shown mobile users preferring usability over security. Furthermore, mobile users often unlock their devices in public spaces, inevitably resulting in a high possibility of user credentials disclosure. Motivated by the above, we introduce a novel user-habit-oriented authentication model, where mobile users can integrate their own habits (or hobbies) with user authentication on mobile devices. The user-habit-oriented authentication turns a tedious security action into an enjoyable experience. In addition, we propose a rhythm-based authentication scheme, providing the first proof of concept toward secure user-habit-oriented authentication for mobile devices. The proposed scheme also takes the first step toward using the theory of mind into security field. Experimental results show that the proposed scheme has high accuracy in terms of false rejection rate. In addition, the proposed scheme is able to protect from attacks caused by credential disclosure, which could be fatal if it was done through the traditional schemes.

INDEX TERMS Authentication, habit-oriented, mobile, theory of mind, security, usability.

I. INTRODUCTION

Mobile devices are becoming more integrated in our lives. They are no longer just used to make phone calls, but a device that aids us in our daily lives. We use it to connect with social media, make mobile payment, carry sensitive information like phone addresses. And with each new implement and feature, we become more dependent on it. It has been evidenced by Cisco VNI Global Mobile Data Traffic Forecast that the number of global mobile devices and connections in 2013 has grown to 7 billions, which will exceed the world's population by 2014 [1]. Thus, it's no surprises that threats began to emerge. One fundamental security problem is user authentication, and if not executed correctly, leaves the mobile user vulnerable to harm like impersonation or unauthorized access.

User authentication often involves users proving evidences like digital identity (e.g. user name) and a corresponding credential (e.g. password) to verify themselves online. Password based approach is the easiest and cheapest way to authenticate a user; however, it's susceptible to dictionary attack, brute-force attack, and software cracking. While combining letters, number, and special symbols to create long and complicated passwords does somewhat detour attacks and delays attackers from compromising accounts, it isn't user-friendly. Researcher and industries have proposed many alternatives to this problem such as OTP (One Time Password), grid unlock pattern, and biometric [2], but they also have their limitations and weaknesses. For instance, because of complex algorithms for matching a scan in biometric, it is possible to have false positives or reject genuine ones caused by immaculate particles like sweat or dirt. As such, only a few device support this approach now as it requires special hardware, which can be costly for small or even large businesses. It is also difficult to change and reinstate a unique physical characteristic (e.g. iris, fingerprint) once it has been compromised because we have only one set of them. Furthermore, there is no standard application programming interfaces (APIs) provided by mobile

computing platforms that an application can use to gather biometric information. And apparently it isn't hard to obtain a copy of a scan and fool the device too. The new iPhone5 is a great example, which utilities finger scanner technology. Since the launch of the Apples iPhone5, a collective of German students have successfully hacked its fingerprint-scanning security system by simply taking a fingerprint from a glass and using the imprint to fool the sensor [9]. Also, attacker are able to defeat facial recognition technology by fooling the smartphone authenticator into believing he/she is the person by simply using a high-resolution photo of the user. In addition to hardware and security concerns, biometric authentication methods raise questions of ethical and social issues. For instances, like many conventional forms of identifications there is a privacy concerns around collecting user's information. According to McAffee mobile security report for 2014, over 80% of Apps are collecting some sort of data whenever a person uses a mobile phone [6]. Furthermore, it's insanitary as germs of user's finger, for instance, can cultivate on the readers that are used to obtain biometric information. Meanwhile, OTP (One Time Password) and grid pattern lock are susceptible to smudges attacks (a method that can be used to discern password patterns based on smears on the touchscreen) and touch-logging/touch-stroke-loggers (similar to key-loggers malware on computers but track the sensitive input of the touchscreen). In fact, a researcher has demoed at the RSA Conference that various swiping motion can be used to infer when a user is entering a password, browsing through his/her home screen, or inputting text from a pull-up keyboard [7].

User authentication is crucial to mobile device security, but unfortunately, many studies have shown that mobile users prefer usability over security. Yet, a higher level of security often entails sacrificing usability. As such, most people don't lock their devices at all because of two reasons. Reason one, entering a passcode is inconvenient on a small screen like a mobile phone. Reason two, mobile users are limited to or given no user-friendly options.

Motivated by the aforementioned observations, we aim at securing mobile phones in a user-friendly manner by allowing mobile users to authenticate themselves using authentication services combined with their habit since it is likely that the user would prefer to use an authentication scheme that fits their habits. A preliminary version of this work has been reported in [8]. A habit is something a person develop unconsciously as oppose to a hobby, where you choose to perform the action and enjoy it at a leisure time. We take this uniqueness to establish ownership appropriately called User-Habit-Oriented Authentication model as illustrated in Fig. 1. This combination could change users' view on smart phone security as an enjoyable experiences rather than a tedious action, making users more likely to secure their phones. In other words, we think about user authentication in smart phone from a different perspective, particularly, considering mobile user personal habits. Also, habits are unique to each individual person and difficult to reproduce because it

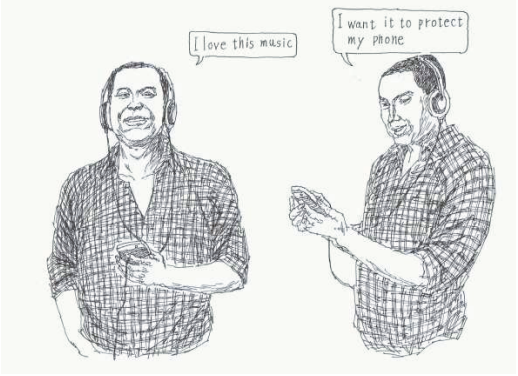


FIGURE 1. An example of user-habit-oriented authentication model.

happens in the unconscious layer of the human mind. To the best of our knowledge, this is the first effort toward user-habit-oriented authentication model for mobile devices in order to effectively address usability and security issues simultaneously; these have usually been considered conflicting from the mobile user perspective.

Due to the fact that many mobile users are also music lovers, in the paper, we further proposed a rhythm based authentication scheme, in which a music lover would tap a set of rhythm on his/her phone with his/her registered composition tempo to authenticate himself/herself. It's possible because smartphones are becoming more powerful (e.g. increasing CPU processing power, a wide variety of sensors built into it, and user-friendly touchscreen interface); and thus, we are able to accurately capture motion information from users. In this case, the accelerometer in most modern smartphone is an excellent instrument in collecting users' rhythm input. Security is usually imagined as a tedious and boring task, and mobile user are willing to give up their security in favour of ease of use. But through rhythm authentication, the image of authentication can be re-imagined as something exciting and appealing. This also makes it both convenient and reasonably secure, and will undoubtedly result in a major increase in the number of people locking their devices. This study provides the first proof of concept toward secure user-habit-oriented authentication for mobile devices, where mobile users can integrate their own habits with user authentication on mobile devices.

Rhythm based authentication can be considered as a type of cognitive behavior based authentication. Thus, it is a secure verification method due to the fact that the activity is ''hidden''; meaning there is no visual input like keyboard or keypad. Our experiments also have shown that even if the tapping procedure is observed by others, it is still very difficult to replicate the pattern because the authentication is based on the user's cognitive-behaviour. This is especially important property considering the fact that users often use their mobile phone, tablets, and e-reader in public spaces and frequently unlock their devices, which results in a high possibility of user credential disclosure. For instances, any passers-by could look over the user's shoulder when he/she

are entering his/her password. This is a problem that mobile users face every day. In traditional user authentication schemes, if the user's credential (e.g. password) is compromised, the scheme's security is gone. However, for our proposed rhythm based authentication, it is not easy for the bad guys to replicate the tapping motion of the user, even when they know the rhythm. This is because they may interpret the rhythm differently. An enthusiastic music lover would compose a more complex rhythm pattern as their brain are more tuned to the music, and pick up certain beats compared to a person who isn't extensively familiar to the genre of music they've registered (e.g. slow classical vs. fast pace techno music). User can also easily change their registered pattern with a new set of rhythm if it has gotten compromised as oppose to biometric scan, where user only have one set of fingers and eyes at their disposal. There are billions of possible rhythm combinations, all with a fair chance of being used; although, it may be skewed based on population or trend.

The rest of the paper is organized as follows. In Section II, we propose a rhythm based authentication scheme. The experimental evaluation of the proposed scheme is presented and discussed in Section III. Finally, we conclude the paper with an outlook on future works in Section IV.

II. PROPOSED RHYTHM BASED AUTHENTICATION SCHEME

In this section, we will first discuss the motivation for using habits (or hobbies) to secure smartphone. Then, we design a new rhythm based authentication scheme.

A. HABIT IS A SECURITY ARSENAL

Habit occurs in the subconscious mind whether it is good or bad. Hobbies develop from good habits; one that we get pleasure from doing and have the conscious to execute. The type of habits we are talking about is actions that are hardwired in our brains that can be taken into various form of output. For our case, tapping to a music rhythm is a habit for a music lover. The form of output is the different songs a person can tap. Thus, a mobile user can choose a song that he loves to protect his/her smartphone. Because an individual can interpret music in several different ways (e.g. a rock enthusiast comes up with a rhythm based on the subtle beats of the drum in the background while another focus on the secondary solo guitar), applying it to security is perfect as there is no form of authentication as we know that provides enjoyment and complexity as habit-oriented authentication does. Also, we assume that more users will be willing to apply a stronger security approach to protect their smartphones because of the usability of this scheme. Another benefit is it is changeable unlike biometric, but still remain unique to that individual because people have different cognitive processing.

B. OVERVIEW OF THE PROPOSED SCHEME

The proposed scheme consists of two phases: Registration and Authentication, as shown in Fig. 2.

In the registration phase, the user needs to set the personal rhythm that will be captured by accelerometer sensor of smartphone. The original data captured will then be processed using the ''data transformation'' and ''zero-shrinkage'', in which a binary sequence template is created and the number of input beats is obtained. The user then confirms his/her rhythm a second time. However, it is very challenging for a user to input the exactly same rhythm twice due to various causes, such as holding instability, human cognitive behavior variance and input errors. Also, it is very difficult to digitally capture user's behavior accurately given only a limited number of inputs. Therefore, to effectively validate two inputs and minimize the required number of input that are often seen during registration phase of other authentication methods, we proposed a fast verification algorithm consisting of ''threshold matching'', ''zero-shrinkage'' and ''e-error correction'' mechanisms. The registration process is completed once the two inputs match.

In the authentication phase, we propose a Fuzzy ARTMAP (FAM) based authentication scheme. FAM is an extension of ARTMAP neural network that performs incremental supervised learning of recognition categories in response to input vectors (analog or binary) presented in arbitrary order [11]. Compared with other artificial neural networks, FAM has many remarkable characteristics, including on-line learning, fast learning about rare events, many-to-one and one-to-many learning, extendibility and avoidance of local extremum. These characteristics make FAM an effective candidate for user authentication in this work. However, FAM system requires several logons samples to train the system before classifying, which greatly hampers the users' experience. To avoid this problem, we propose a two-step authentication model. For the first several login attempts, we will adopt the fast verification algorithm used in the registration phase. At the same time, the original data captured and the results from the fast verification algorithm will be used for the supervised learning of FAM. When FAM is well-trained, user authentication will switch from fast verification algorithm to FAM.

Notation: For notational simplicity, in this paper, all variables associated with template setting signal, verification signal and authentication signal are labelled by subscript text letter ''Template'', ''Verification'' and ''Authentication'', respectively, such as B_{Template}, and data that's been processed by zero-shrinkage are labelled by superscript text letter as ''ZS'', such as $B^{\text{ZS}}_{\text{Template}}$.

Prior to elaborate the proposed authentication, we first introduce the original data acquisition, which will impact the following algorithm design and performance to a large extent. After that, we will explain Registration Process and Authentication in detail based on the obtained original data.

C. ORIGINAL DATA ACQUISITION

Unlike traditional PC devices, a growing number of smartphones are equipped with a variety of powerful sensors,

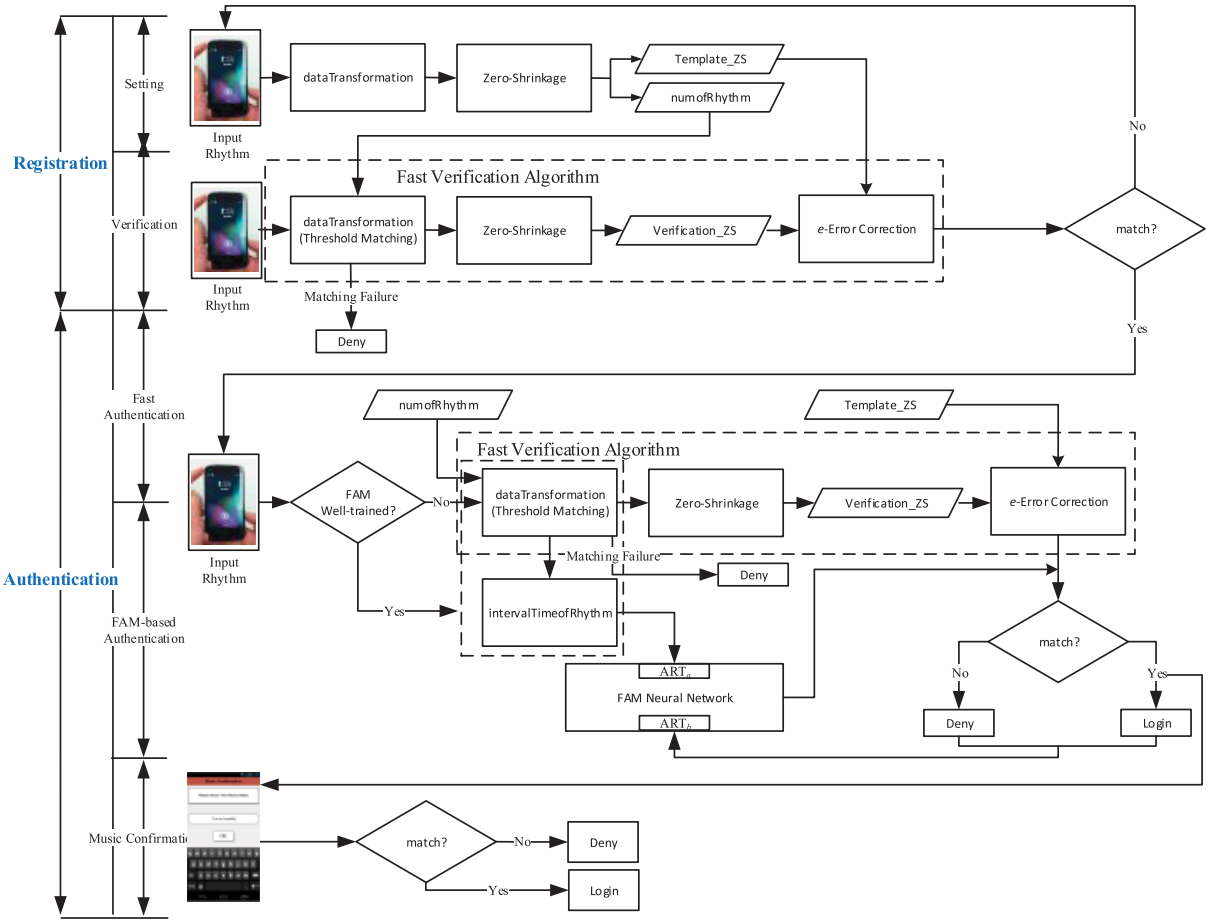


FIGURE 2. Workflow of the proposed authentication scheme.

such as accelerometer, digital compass, gravity, gyroscope, GPS, fingerprint sensor, and thermometer. These sensors make smartphones possible to capture diversity users' input. We intended to use the accelerometer sensor to capture the rhythm entered by users for our proposed authentication scheme. This is accomplished by measuring the force of acceleration, the angle, and direction phone being held while recording the settle vibration caused when the user taps the phones corner or back.

The accelerometer is one kind of common hardware sensors used to capture a users' shake motion. In most smartphones, the accelerometer adopts a standard 3-axis coordinate system that is defined relative to the device's screen and expresses them as data values, as shown in Fig. 3. The X axis and the Y axis are parallel with the screen, where the X axis is horizontal and points to the right, and the Y axis is vertical and points up. The Z axis is perpendicular to the screen and points outwards relative to the screen.

According to the coordinate system, the data captured by the accelerometer can be represented as a triple-tuple time series $\mathbf{S}(t) = \{X(t), Y(t), Z(t)\}$, where t is the input time, $X(t)$, $Y(t)$ and $Z(t)$ represent the instantaneous acceleration value of X axis, Y axis and Z axis, respectively.

TABLE 1. Optional mode for android accelerometer.

Accelerometer Sampling Mode	Frequency F_s (Sampling Time)
SENSOR_DELAY_FASTEST	200Hz (5.0ms)
SENSOR_DELAY_GAME	50Hz (20.0ms)
SENSOR_DELAY_UI	15.75Hz (63.5ms)
SENSOR_DELAY_NORMAL	5Hz (200ms)

Moreover, some Android accelerometers provide 4 sampling frequency to sample data $\mathbf{S}(t)$ as shown in Table 1.

By using certain sampling mode, the input signal will be transformed from analog signal to digital signal, where $\overline{\mathbf{S}}(n) = \mathbf{S}(n/F_s)$ and F_s is the sampling frequency. Generally, low sampling frequency means low process complexity, but it will sacrifice the accuracy and security. In order to record users' input as precise as possible, we adopt the mode of SENSOR_DELAY_FASTEST.

Tapping position is also an important factor to capture and process the original data because it influences the acceleration values on the three axis. Through a great deal measurements, we suggest three effective positions on smartphones as candidate input points, the top left corner (**Point A**), the top right (**Point B**), and the back of the smartphone (**Point C**), as shown in Fig. 3. When tapping a set of rhythm from

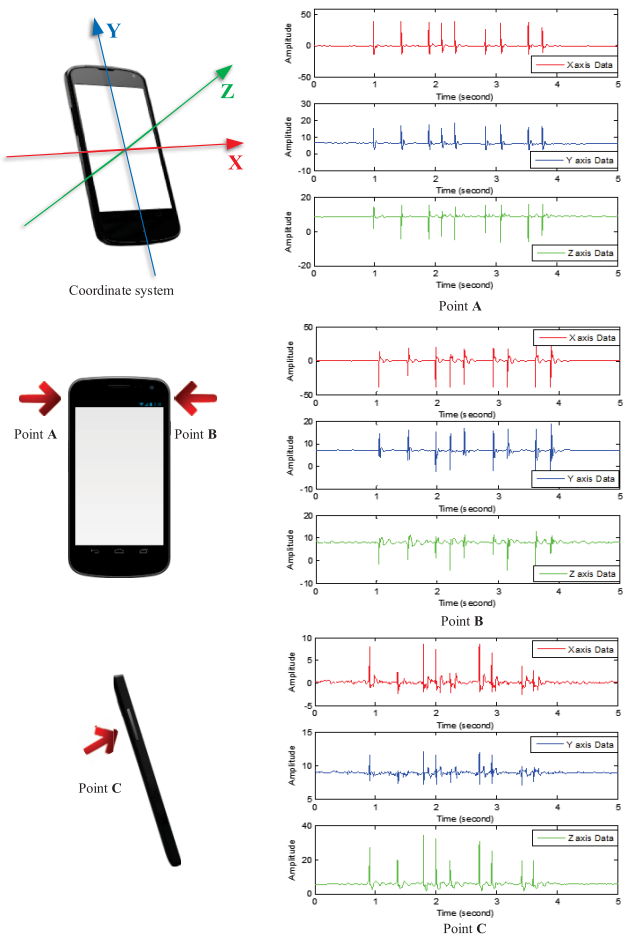


FIGURE 3. Illustration of data acquisition process (acquisition time: 5 seconds, accelerometer sampling mode: SENSOR_DELAY_FASTEST).

Point A and Point B, the corresponding impulses of both X axis and Y axis are distinguishable from the noise, while some beats on Z axis are lost. This is because the direction of acting force is mainly parallel to the screen. In contrast, when the set of rhythm is input from Point C, input becomes clear on Z axis. Thus, we will elaborate on how different input points affect our proposed scheme, in terms of both authentication accuracy and security in Section III. Note that when a rhythm is input on a specific point of the test smartphone, a sequence $\overline{\mathbf{S}}(n)$ is obtained and saved as the original data.

D. FAST VERIFICATION ALGORITHM

The registration process is performed during a user's initial log on. A well-designed authentication scheme is required to have a user-friendly registration process with less user operations, which is the key factor that impact the user's experience. Due to human cognitive behavior variance and input errors, it is very difficult for most users to input the same rhythms twice as opposed to traditional authentication schemes like password or grid pattern. Although some artificial intelligence system (such as Hidden Markov Model, HMM, or FAM) can learn the user's specific usage habits, it usually requires many samples to train the system, which sacrifices the users' experience [10]. Motivated by this factor, we propose a fast verification algorithm, by which user only needs to use two similar rhythms (the first one for template setting and the second one for verification) to complete the registration process with adjustable precision level. Moreover, the proposed fast verification algorithm is also in charge of providing effective sample data for the training of the FAM system in the authenticate phase.

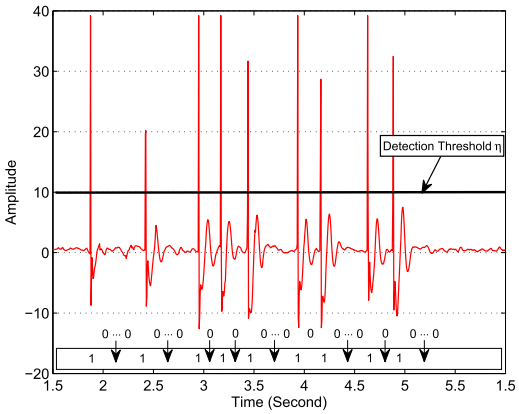


FIGURE 4. Illustration of data transformation and zero-shrinkage.

Fig. 4 shows an amplified original data from Point A. It can be observed that the captured original data consists of not only the rhythm input, but also the noise due to unstable smartphone holding. In addition, due to the sampling precision, the accelerometer maybe too sensitive in terms of capturing both rhythm's amplitude and duration (in milliseconds) between the first initial input and second confirmation input. We may have two relatively different signals because of this, when in fact, they are the same rhythm entered by the same user. To avoid false positives, the proposed fast verification algorithm includes a threshold comparison approach that transforms the original data to the binary data, aiming at reducing the noise and the randomness of signal amplitude; and three techniques, named zero-shrinkage, threshold matching and e-error correction, to control the tolerable precision between two consecutive samples.

1) DATA TRANSFORMATION

To reduce the uncertainty of the amplitude (due to the tapping speed), we first transform the original data from the real number $\overline{\mathbf{S}}(n)$ to the binary data $B_{\text{Template}}(n)$ by using a comparison threshold method. When the beat of a rhythm peak beyond the threshold η, whether it is larger or smaller, it will be labeled as 1. Otherwise, it will be labeled as 0.

According to the discussions in Section II-A, when we tap a rhythm on different points, the acceleration values on the three axis work differently, and therefore, we need to specify the threshold based on the merits. Particularly, when Point A and Point B are used, data $\overline{S}_x(n)$ from X axis

is dominated, and when Point C is used, data $\overline{S}_z(n)$ is considered. This process of data transformation can be performed using the following equations,

$$B_{\text{Template}}(n) = \begin{cases} 1 & \text{cond. 1} : \overline{S}_x(n) \geq \mathbb{E}\left[\overline{S}_x(n)\right] + \eta_{\text{A}} \\ & \text{cond. 2} : \overline{S}_x(n) > \overline{S}_x(n \pm m) \quad \text{Point A} \\ 0 & \text{otherwise} \\ 1 & \text{cond. 1} : \overline{S}_x(n) \leq \mathbb{E}\left[\overline{S}_x(n)\right] + \eta_{\text{B}} \\ & \text{cond. 2} : \overline{S}_x(n) \leq \overline{S}_x(n \pm m) \quad \text{Point B} \\ 0 & \text{otherwise} \\ 1 & \text{cond. 1} : \overline{S}_z(n) \geq \mathbb{E}\left[\overline{S}_z(n)\right] + \eta_{\text{C}} \\ & \text{cond. 2} : \overline{S}_z(n) > \overline{S}_z(n \pm m) \quad \text{Point C} \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

where $B_{\text{Template}}(n)$ is the transformed binary data and $\mathbb{E}[x]$ is the expected value of signal x. Furthermore, condition 1 means the data is greater or smaller than η plus the mean of original data and condition 2 implies it is the local extremum, and m defines the range of "local". In the rest of this paper, if no otherwise specified, we just discuss the method to process signals from Point A. All discussions on Point B and Point C are easily obtained by simple adjustments.

This data transformation process is only used for the user's first input, i.e. template setting stage, and we have no information about the acting force of user input. Therefore, a fixed value of η is necessary. Here, we suggest $\eta_{\text{A}} = \eta_{\text{C}} = 10$, and $\eta_{\text{B}} = -10$ because we found from our experiment that 10 is a statistically good threshold that can be reached by most mobile users.[1]

2) ZERO-SHRINKAGE

Using data transformation, we obtain the binary data B_{Template} consisting of two alternating symbols "0" and "1", where "0" represents the idle time waiting for input, and "1" refers to the rhythm user input. The time interval between two symbols is $1/F_s$ seconds. In order to control the precision level while maintaining useful information, we design a zero-shrinkage approach that reduces the number of symbols "0" in proportion but keeps "1" unchanged.

Specifically, we define d as the shrinkage factor. If $B_{\text{Template}}(n_i)$ and $B_{\text{Template}}(n_j)$ are two consecutive "1", n_i and n_j are respective index number, then the number of symbol "0" between $B_{\text{Template}}(n_i)$ and $B_{\text{Template}}(n_j)$ will be reduced to $[(n_j - n_i - 1)/d]$ after zero-shrinkage, where $[\cdot]$ is the rounding operation. We take Eq. (2) as an example to illustrate how the zero-shrinkage works.

$$\begin{aligned} B_{\text{Template}} &= [1, \underbrace{0, \ldots, 0}_{k_1}, 1, \underbrace{0, \ldots, 0}_{k_2}, 1] \xrightarrow{\text{Zero-Shrinkage}} \\ B^{\text{ZS}}_{\text{Template}} &= [1, \underbrace{0, \ldots, 0}_{[k_1/d]}, 1, \underbrace{0, \ldots, 0}_{[k_2/d]}, 1] \end{aligned} \tag{2}$$

As a result, the precision level can be controlled within d/F_s seconds. For example, when $F_s = 200$ Hz, and $d = 40$, the proposed scheme can tolerate at most 0.2 seconds error of users input. We denote the transformed template data and the number of the beats user input with $B^{\text{ZS}}_{\text{Template}}$ and N, respectively.

3) THRESHOLD MATCHING

In the verification and the following stages, as the template information have been obtained, we can relax the constraint of fixed threshold by using an adaptive threshold matching approach, thereby further lowering the number of times the user is required to input during the training stage. In Fig. 4, we can see that when user enters a beat from Point A, a positive impulse appears, which usually distributes on the relatively fixed interval (positive impulse $(\mathbb{E}(\overline{S}) + [0, 40])$). In addition, a positive impulse is immediately followed by a negative impulse $(\mathbb{E}(\overline{S}) + [-10, 0])$ because of counter acting force of holding hand. Utilizing these features, we can search a more proper threshold in case the tapping motions are unstable.

Specifically, we first set $\eta = \frac{\eta_{\text{A}}}{2} = 5$ to filter noisy signal. Then, perform the data transformation by Eq. (1), and denote the number of symbols "1" be N_{matching}. If condition $N_{\text{matching}} = N$ holds, the threshold matching stops. Otherwise, increase η with a small increment $\eta = \eta + \triangle$ and repeat the above process until N_{matching} equals to N or η is larger than the maximal threshold $\eta^{\max}$. If a threshold η cannot be determined, then the threshold matching sequences will iterate through an opposite direction by resetting $\eta = -1$. Those local minimum samples smaller than η plus $\mathbb{E}(\overline{S})$ will be labeled as symbols "1" and denote N_{matching} as the number of "1". Then gradually reduce $\eta = \eta - \triangle$ until condition $N_{\text{matching}} = N$ is satisfied or η reaches the minimal threshold $\eta^{\min}$. If there is no proper threshold to make condition $N_{\text{matching}} = N$ satisfied after threshold matching, the current input will be rejected.

4) *e*-ERROR CORRECTION

This is an additional precision control process used for the verification and authentication input. Denote the number of symbols "0" between any two consecutive "1" of $B^{\text{ZS}}_{\text{Template}}$ and $B^{\text{ZS}}_{\text{Verification}}$ be $Z^{\text{ZS}}_{\text{Template}}(k)$ and $Z^{\text{ZS}}_{\text{Verification}}(k)$, respectively, where $1 \leq k \leq N - 1$. If

$$|Z^{\text{ZS}}_{\text{Template}}(k) - Z^{\text{ZS}}_{\text{Verification}}(k)| \leq e, \quad \forall k \tag{3}$$

holds, then input $Z^{\text{ZS}}_{\text{Verification}}$ is considered similar to the rhythm template, where scalar e is the correction factor that can be adjusted. For example, when the template data is $B^{\text{ZS}}_{\text{Template}} = [1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1]$, and the verification input is $B^{\text{ZS}}_{\text{Verification}}[1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1]$, then $Z^{\text{ZS}}_{\text{Template}} = [2, 1, 2, 2]$ and $Z^{\text{ZS}}_{\text{Verification}} = [2, 2, 2, 2]$. If $e = 1$, then it means the two data are similar and the registration process takes affect.

E. FAM BASED AUTHENTICATION ALGORITHM

In this subsection, we propose an FAM-based authentication algorithm to further improve the performance of the rhythm

[1]It is also worth noting that this threshold may change according to the different sensor chips, and the suggested value is verified in Google Nexus 4.

authentication scheme. Compared with the fast authentication algorithm, the advantages of the FAM-based algorithm are four-folds: (1) it is independent on the algorithm parameters, such as d and e in the fast authentication algorithm, which makes the proposed authentication scheme more flexible for different users; (2) by means of the extendibility feature of the FAM system, it is easy to extend the proposed authentication scheme for more application scenarios, like multi-user authentication; (3) more characteristics of the rhythm input might be utilized as the input of the FAM system, to further improve the security and accuracy of the proposed authentication scheme; and, (4) a well-trained FAM system performs better in terms of computation complexity.

Review on Fuzzy ARTMAP: FAM is an extension of ARTMAP neural network that perform incremental supervised learning of recognition categories and multidimensional maps in response to input vectors (analog or binary) presented in arbitrary order. Fig. 5 shows the structure of FAM system that is composed by two adaptive resonance theory modules (ART_a and ART_b) units and a map field into a supervised learning structure, where ART_a takes the input data, ART_b is the supervisory data, and the map field forms the associative mapping relationship between ART_a and ART_b. Each ART system consists of three fields, F_0 is the input field to represent the current input vector; F_1 is the state field to represent the coded or weighted vector by F_0 or F_2 respectively; F_2 is the recognition field to represent the active category. Between each category node $j\,(j = 1, 2, \ldots, J)$ in field F_2 and all nodes in field F_1, there is a weight vector $\boldsymbol{\omega}_j = (\omega_{j,1}, \ldots, \omega_{j,M})$, where M is the data dimension in F_1 field. Specifically, in the proposed authentication scheme, we initialize the parameter $M = 2(N-1)$ and $\boldsymbol{\omega_j} = 1, \forall j$.

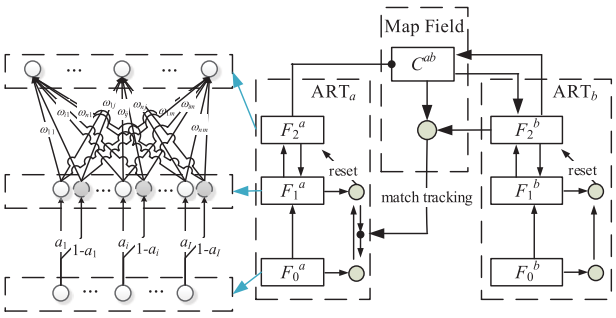


FIGURE 5. The structure of FAM.

In the proposed authentication scheme, FAM system works in two stages, training and authentication. During the training stage, ART_a receives the rhythm input verified by fast verification algorithm, and the input of ART_b is the corresponding verification results. Specifically, we adopt the duration time between two consecutive rhythms $Z_{\text{Authentication}}$ as the input of ART_a. Note that data $Z_{\text{Authentication}}$ is not processed by zero-shrinkage as oppose to $Z^{\text{ZS}}_{\text{Authentication}}$, in order to protect against loss detail information of user input as possible. The input of ART_b is one bit decision variable, denoted as "1 (login)" or "0 (deny)" based on the result of the fast verification algorithm. Correspondingly, the FAM network initializes two categories in F_2 field of both ART_a and ART_b, i.e. the value of two nodes j in F_2 field is either 0 or 1. After the training stage, we obtain an updated weight vector $\boldsymbol{\omega}_j, \forall j$ and a well-designed FAM system that can be used to authenticate the next user input.

1) TRAINING

In this stage, ART_a receives a stream of training rhythm patterns that was verified by the fast verification algorithm, and the normalization of $(N-1)$-dimensional $Z_{\text{Authentication}}$. In order to avoid the unattractive problem of category proliferation, complement coding that doubles the number of input data to a $2 \times (N-1)$-dimensional vector $Z^{\text{CC}}_{\text{Authentication}}$ is necessary, *i.e.*,

$$Z^{\text{CC}}_{\text{Authentication}} = \left[\frac{Z_{\text{Authentication}}}{D^{\max}}, \left(\frac{Z_{\text{Authentication}}}{D^{\max}}\right)^c\right] = \left[\frac{Z_{\text{Authentication}}}{D^{\max}}, \mathbf{1} - \frac{Z_{\text{Authentication}}}{D^{\max}}\right], \quad (4)$$

where $\mathbf{1}$ is $(N-1)$-dimensional vector with all elements of 1 and $D_{\max}$ is the predefined maximal interval between two consecutive rhythm.

Then, the input sample $Z^{\text{CC}}_{\text{Authentication}}$ connects to all nodes in F_2^a using the following choice function $T_j(x)$,

$$T_j(Z^{\text{CC}}_{\text{Authentication}}) = \frac{|Z^{\text{CC}}_{\text{Authentication}} \wedge \boldsymbol{\omega}_j|_1}{|\boldsymbol{\omega}_j|_1 + \alpha}, \forall j \quad (5)$$

where "$\wedge$" is a min operator, $|\cdot|_1$ is l_1 norm, and α is a bias parameter that is slightly larger than 0. To simplify we denote $T_j(Z^{\text{CC}}_{\text{Authentication}})$ be T_j, and $\forall j$ rearrange T_j in descending order, such that $T_{j_1} \geq T_{j_2} \geq \cdots \geq T_{j_J}$.

To begin with $i = 1$, substitute $\boldsymbol{\omega}_{j_i}$ into the following match function $M_j(x)$ and check against a vigilance parameter ρ,

$$M_{j_i}(Z^{\text{CC}}_{\text{Authentication}}) = \frac{|Z^{\text{CC}}_{\text{Authentication}} \wedge \boldsymbol{w}_{j_i}|_1}{|Z^{\text{CC}}_{\text{Authentication}}|_1} \geq \rho \quad (6)$$

where $\rho \in (0, 1]$. If Eq. (6) cannot be satisfied, set $i = i + 1$, and check the next category in the sorted category list. Otherwise, we say the resonance between ART_a and ART_b occurs. Then, the map field will check if category j_i is matched with the input of ART_b. If so, we say the current input is learned by FAM and the weight vector $\boldsymbol{\omega}_{j_i}$ is updated by the following equation,

$$\boldsymbol{\omega}^{\text{next}}_{j_i} = \beta(Z^{\text{CC}}_{\text{Authentication}} \wedge \boldsymbol{\omega}_{j_i}) + (1-\beta)\boldsymbol{\omega}_{j_i} \quad (7)$$

where $\beta \in [0, 1]$ is the learning rate. Eq. (7) guarantees that the $\boldsymbol{\omega}_j, \forall j$ is non-increasing during the whole training stage, and hence converges to a limit.

Otherwise, if category j_i is mismatched with the input of ART_b, a wrong resonance appears, and FAM will trigger matching tracking mechanism by increasing the vigilance parameter ρ as

$$\rho = M_{j_i}(Z^{\text{CC}}_{\text{Authentication}}) + \delta, \quad (8)$$

to break the current resonance, where δ is slightly larger than 0. Repeat the above procedure to find another category in F_2^a by setting $i = i + 1$. In the case where the FAM network cannot find out a right category to match the current training input from ART_b after going through all categories, a new category (labeled the same as the input of ART_b) will be created by $J = J + 1$ and $\boldsymbol{\omega}_J = \mathbf{1}$. For the new created category J, we can get $M_J(Z^{\text{CC}}_{\text{Authentication}}) = 1 \geq \rho$.

In our proposed scheme, FAM network is considered well-trained when the number of effective training samples (verified as the legitimate users by fast verification algorithm) has reached the predefined value.

2) AUTHENTICATION

After training, the FAM network can be used to verify the given input data with the specified vigilance parameter. Specifically, when a new authentication data is received and processed by threshold matching, we first check if $N_{\text{matching}} = N$ is satisfied. If so. the input data will be processed by component coding, and substituted into the matching function Eq. (6) that will calculate the matching value $M_j\left(Z^{\text{CC}}_{\text{Authentication}}\right)$ for each category in F_2^a. It later finds the category with the maximal matching value, i.e.,

$$j^* \in \arg\max_j M_j\left(Z^{\text{CC}}_{\text{Authentication}}\right) \tag{9}$$

Afterwards, check $M_j^*\left(Z^{\text{CC}}_{\text{Authentication}}\right)$ against the vigilance parameter ρ, if

$$M_{j^*}\left(Z^{\text{CC}}_{\text{Authentication}}\right) > \rho, \tag{10}$$

is satisfied and category j^* equals to 1, then the authentication is successful, and the user would be logged in. Otherwise, the user would be denied.

3) MUSIC CONFIRMATION

We further provide an optional authentication step, ''Music Confirmation'', for some security-aware users or in an insecure environment (e.g. public area). The optional step is able to increase the security of our proposed scheme significantly, while at little expense of user experience.

The illustration of the music confirmation step is shown in Fig. 6. When the input rhythm passed the proposed verification algorithm, a question page appears to ask the user to type the name of the music just input. Obviously, a legitimate user would be easy to answer what he/she has tapped is. However, it will be very difficult for attackers to guess the connection between the observed tapping motions and the corresponding music.

The security mechanism of our proposed optional step comes from a sophisticated concept in the field of psychology, coined as Theory of Mind [12]. According to the theory of mind, a huge gap exists between observing others' actions and inferring the real intention behind these actions. Imagine that as you are tapping rhythm on your smartphone, the corresponding music is playing through your mind, which consists of the voice of the singer, the melody, the rhythm, and even your specific feeling about the song. In fact, music lovers are usually hard to avoid colouring what they are tapping with dynamics, accentuation, and phrasing, depending on their personal musicality. On the other hand, all that an attacker can obtain is a bunch of disconnected beats, like a kind of bizarre Morse Code. Without any context behind it, they cannot derive the user's rhythm. Therefore, the loss of diversity information impedes attackers to set up the connection between what they observed and the right music.

FIGURE 6. Illustration of matching between music and rhythm.

On a related note, there was a famous experiment [13] that involved a group of subjects tapping out a rhythm of songs to another participant whose goal was to identify the song based on the rhythm they listened. Over the course of the experiment, only 2.5% of listeners could correctly identify the song (3 out of 120 trials). Taking from this ''Tapper and Listener'' experiment result, it would be harder for attackers to guess what the legitimate user taps out in our proposed scheme based on the following reasons:

- In Tapper and Listener experiment, two conditions are necessary. First, they selected 25 music well-known for both tapper and listener. Besides, the goal of tappers in this experiment is to make their partners understand what they try to convey as much as possible as they can, but our proposed scheme is for security purpose. Hence, people are allowed to choice their music piece reference that can be renowned or unknown to the attacker.
- Rhythm are based on a persons own understanding of a music piece.
- Users can intentionally break the connection between inputs and correct rhythm by selecting an irrelevant music to match their input rhythm to confuse attackers, and thereby eliminate the slight probability that attackers guess correctly.

III. EXPERIMENTS AND EVALUATIONS

To verify the feasibility and security, we invited 15 participants with different music comprehension level (5 basic, 5 intermediate, and 5 advanced) to test the proposed authentication scheme. The test smartphone and

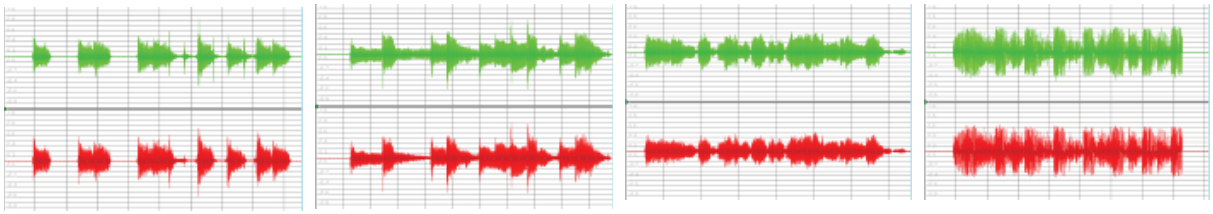


FIGURE 7. Waveforms of the referenced music.

TABLE 2. Experiment environment and parameters list.

Particants	
Musical Level	**Number**
Basic	5
Intermediate	5
Advanced	5
Smartphone Device	
Parameter	**Value**
Smartphone	Google Nexus 4
Operation System	Android 4.2.2 and 4.3
Processor	Qualcomm SnapdragonTMS4 Pro
RAM	2GB
Accelerometer	MPU-6050
Sampling Mode	SENSOR_DELAY_FASTEST
Reference Music	
Parameter	**Value**
Time of duration	$\leq$ 10 seconds
Music 1 (easy)	What Makes You Beautiful
Music 2 (normal 1)	SHE
Music 3 (normal 2)	Moves Like Jagger
Music 4 (hard)	The Hottest Ethnic Trend
Fast Verification Algorithm	
Parameter	**Value**
Threshold η	10
Threshold $\eta^{\max}$	40
Threshold $\eta^{\min}$	5
The range of local m	10
Threshold matching increment $\triangle$	0.1
Shrinkage factor d	40
Correction e	1
FAM-based Verification Algorithm	
Parameter	**Value**
Training samples	20
Maximal Interval $D^{\max}$	200 (1 second)
Bias parameter α	10^{-5}
Vigilance parameter ρ	0.8
Learning rate β	1 (Fast Learning)
Tracing increment δ	10^{-4}

authentication algorithm related parameters are list in Table 2. The experiments were divided into two parts. The first experiment is aimed at verifying the reliability and feasibility of our proposed scheme. We had each participant perform 100 verification trials, where we measure the False Rejection Rate (FRR), i.e. the percentage of failed login when authorized users try to login. The second experiment tests the resilience of the proposed authentication scheme against the credential disclosure. The balance between the security and useability of our proposed authentication scheme is also analyzed.

A. FEASIBILITY

People with music talent tend to like music. As a result, the proposed scheme will easily be adopted by them. To verify the feasibility of the proposed authentication scheme, we measure the FRR of each participants with 4 reference music pieces. The difficulty of these music pieces (where music 1 is easy and music 4 is hard) are evaluated according to the number of beats and their complexity of waveforms, as shown in Fig. 7. The first rhythm is based on a music piece called "What Makes You Beautiful," which includes 10 clear beats. The second rhythm is based on a music piece called "SHE," which includes 9 clear beats and 2-3 blurry beats. The third is based on a music piece called "Moves Like Jagger," which includes 11 clear beats and some blurry beats. The last rhythm is based on a music piece called "The Hottest Ethnic Trend," which includes 13 clear beats, and some blurry beats and background noise.

After the registration procedure, each participant is required to perform the 4 reference music pieces from Point A according to their personal understanding. The experiment results are shown in Table 3, which present value of FRR according to the different music levels of the participants. From the results we gathered, we found that there is the high correlate between the FRR and the person's level of music expertise. For instance, as the person's level of music proficiency increase, the FRR decreases greatly as one would expect, and vice versa. This is because a person who has a basic level of understanding of music will be less sensitive to the subtle music beats in a rhythm, while an intermediate and advance participate will be more sensitive to the rhythm. Therefore, users are able to reproduce a complex rhythm and achieve a lower FRR. People with music talent tend to like music. As a result, the proposed scheme will easily be adopted by them.

TABLE 3. False rejection rate (enter rhythm on the top left corner of the smartphone).

Music	**Basic**	**Intermediate**	**Advanced**
Music 1	0.16	0.01	0.008
Music 2	0.138	0.044	0.012
Music 3	0.15	0.04	0.01
Music 4	0.192	0.03	0.01
Average	0.16	0.031	0.01

As shown in the Table 3, the participants with basic understanding of music achieve an FRR average of 16%. In other words, most users will fall in this category, and miss the lock code 1 in every 7 tries. It is also worth noting that this average is shared across all 4 reference music pieces because the participants could not distinguish the difficult level of a piece and would register similar number of beats; thus, result in the same level of FRR percentage. The intermediate and advanced participant have an FRR average of 3% and 1% because they are able to distinguish the difficulty level of each reference music piece. Moreover, FRR percentage would increases slightly the more input of beats a person register.

B. RESILIENCE AGAINST CREDENTIAL DISCLOSURE

To evaluate the security of the proposed authentication scheme, we consider two possible user credential disclosure risk scenarios. The first case had the users' tapping motion disclosed, dubbed as ''Rhythm Credential Disclosure'', and the second case had the referral music (used as the baseline in our proposed scheme) disclosed, dubbed as ''Music Credential Disclosure''. In the following, we will discuss the effectiveness of our proposed scheme against such two credential disclosure risks according to the experiment results.

1) RHYTHM CREDENTIAL DISCLOSURE

There are two defensive approaches against rhythm credential disclosure attack in our propose authentication scheme. The first one allows user to input their rhythm credential in various places on the phone. For instance, tapping at point A or point B as previously mentioned in Fig. 3, because our proposed scheme can adopt different signal processing method for different input positions. For example, as to Point A and Point B, we extract the data from X axis, and different threshold matching parameters are used. For Point C, we extract the data from Z axis as users' input. In contrast to traditional authentication methods that must input the credential in a specific way (eg. keyboard, screen), the proposed scheme utilizes its ability to accept different inputs to add another security measure. For instances, it is difficult for a malicious attacker to hack the rhythm authenticated phone without prior knowledge of how a user held the device when entering their rhythm. This is because the method of entering the credential correlates the strength of the waves being read and processed.

Despite that, the proposed authentication scheme is still susceptible to shoulder-surfing to some extent. In this case, the way of how a person inputs his/her chosen rhythm greatly dictates the security of the proposed scheme. For example, tapping the rhythm credentials at the back of the phone is harder to observe. Compared to input at the top corner of the smartphone, the security perspective of inputting at the back of the phone seems to be promising option, because the motions will be less visible to an individual who may be watching the users enter their credentials.

If all else fail and the users' motions is disclosed, there is the ''Music Confirmation'' option to protect their rhythm credential. According to our design, the rhythm input and music determination are respectively performed at the back of the phone and on the touchscreen, whereby the whole authentication process is hard to be observed by the same attacker. Through the results of ''Tapper and Listener'' experiment, the rate of success in connecting the music and tapped rhythm is 2.5%, even though tappers select a well-known music and do their best to delivery correct information to listeners. In our proposed authentication scheme, users are free to select their favorite music (popular or special-interest), and tap the rhythm based on their own understanding, which will hamper the attacker effort of correctly matching the rhythm they observed with corresponding music piece. Therefore, it is believed that the successful rate to break our authentication scheme will be no more than the figure of 2.5%.

However, we want to see if there is any drawbacks with this method, and if those shortcomings are worth the trouble. For instances, maybe the rhythm data being captured is less accurate when enter from the backside as oppose to corner side. Or it is less usability for the user to enter from the back because of the way they have to hold their phone. We conducted an experiment to see if our hypothesis support our conclusion, and based on our analysis, decide on a good balance. Also, depending on the different security perspectives, we decided on the best security practices to use for each environment: public, home, and work spaces.

TABLE 4. False rejection rate (enter rhythm at the back of the smartphone).

Music	Basic	Intermediate	Advanced
Music 1	0.264	0.048	0.048
Music 2	0.18	0.064	0.032
Music 3	0.24	0.104	0.02
Music 4	0.188	0.208	0.04
Average	0.218	0.106	0.035

Table 4 shows the FRR of participants who enter their credentials at the back of the phone. From the result we gathered, we found that the FRR of our proposed authentication scheme becomes slightly higher for all music comprehension levels of participants. The basic, intermediate and advanced participants have an FRR average of 22%, 11% and 3.5%, respectively. However, there are two problems with having the user enter via the phone back. The first problem is the usability of the user's action. They have some of distraction to hold their phone, and therefore input errors increase. In addition, compared to input on the corner of the phone, the tapping speed becomes slower, which impacts the amplitude of accelerometer. As illustrated in Fig. 3, when user credential is input from Point C, the negative acceleration impulses caused by counter force are not as clear as entering from Point A or Point B. This results in the performance loss of threshold matching mechanism. For the first problem,

we observe that as participants become more adaptable to the authentication scheme, the FRR will decrease to some extent. From the experiment result, we can see some participants have lower failure rate when they input the second music in contrast to the first music. As to the second problem, some advanced signal processing approaches, such as edge detection, wavelet analysis, etc., might be helpful to mitigate the negative effects.

2) MUSIC CREDENTIAL DISCLOSURE

Another way in which user's credential is disclosed is when the referral music piece is stolen. For instance, when users are suffering from shoulder-surfing and the music confirmation is observed. Generally, users may just select a fragment of some music (several seconds) as a reference to remember their setting rhythm, and it is believed that attackers will have a hard time guessing the fragment completely since it overlaps with that the legitimate users used. Even in extreme situation, where it is assumed that the attacker know the same fragment of the music, the understanding about this fragment may be different. Fig. 8 illustrates this case. Three participants tapping the same piece of the hard reference music (The first 3 seconds of the Hottest Ethnic Trend). As shown in Fig. 8, we found that the waveforms of the three input rhythm are different, not only from the interval between two consecutive beats, but also from the number of the rhythm. According to our proposed algorithm, these three samples would be registered different from each other.

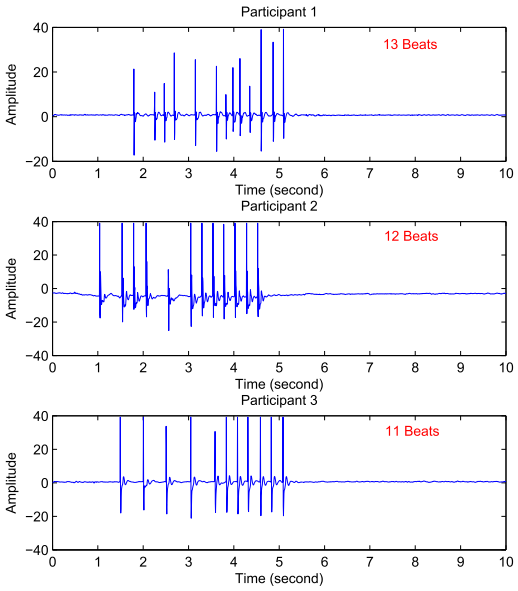


FIGURE 8. Waveforms of the first 3 seconds of the Hottest Ethnic Trend from different participants.

IV. CONCLUSION AND FUTURE WORK

In this paper, we have presented a user-friendly rhythm based authentication scheme. To the best of our knowledge, this is the first effort toward user-habit-oriented authentication model for mobile devices, where mobile users can integrate their own habits with user authentication on mobile devices. The user-habit-oriented authentication turns a tedious security action into an enjoyable experience. Compared with the traditional authentication methods, the proposed scheme can significantly enhance user-friendliness and significantly improve security, without adding extra hardware devices. This, in turn, satisfies the use-in-motion and user friendliness requirements in smartphone authentication. We have also implemented the proposed scheme on a popular mobile computing platform, Android, and performed experiments. The experimental results show that the proposed scheme has high accuracy in terms of false rejection rate.

In future work, we may extend this scheme to incorporate multiple online users. For instances, user will have the option to login to a site using rhythm base authentication as oppose to the weak password based authentication. We can also improve the accuracy and security of the capturing feature of rhythm authentication. We will also explore other possible alternative habits to use and study their feasibility on mobile authentication.

ACKNOWLEDGMENT

The authors would like to thank NSERC (Natural Sciences and Engineering Research Council of Canada) for financial support. Also, the authors would like to thank all the participants who took part in our experiments.

REFERENCES

[1] Cisco. (Feb. 2014). *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018*. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf

[2] A. Sethi, O. Manzoor, and T. Sethi, *User Authentication on Mobile Devices*, Cigital, Dulles, VA, USA, 2012.

[3] N. L. Clarke and S. M. Furnell, "Authenticating mobile phone users using keystroke analysis," *Int. J. Inf. Secur.*, vol. 6, no. 1, pp. 1–14, Jan. 2007.

[4] S. Furnell, N. Clarke, and S. Karatzouni, "Beyond the PIN: Enhancing user authentication for mobile devices," *Comput. Fraud Secur.*, vol. 2008, no. 8, pp. 12–17, Aug. 2008.

[5] M. Jakobsson, E. Shi, P. Golle, and R. Chow, "Implicit authentication for mobile devices," in *Proc. 4th USENIX Conf. Hot Topics Secur. (HotSec)*, 2009, pp. 9–15.

[6] McAfee. (Feb. 2014). *Who's Watching You?* [Online]. Available: http://www.mcafee.com/ca/resources/reports/rp-mobile-security-consumer-trends.pdf

[7] D. Drinkwater. (Feb. 2014). *RSA 2014: Touchlogging the New Attack Vector for Mobile Hackers*. [Online]. Available: http://www.scmagazine.com/rsa-2014-touchlogging-the-new-attack-vector-for-mobile-hackers/article/335997/

[8] J. Seto, Y. Wang, and X. Lin, "Toward secure user-habit-oriented authentication for mobile devices," in *Proc. IEEE Int. Conf. Global Commun. (GLOBECOM)*, Dec. 2014, pp. 1242–1248.

[9] *Has the iPhone 5S Fingerprint Scanner Already Been Hacked?* [Online]. Available: http://www.ctvnews.ca/sci-tech/has-the-iphone-5s-fingerprint-scanner-already-been-hacked-1.1468316, accessed Dec. 12, 2014.

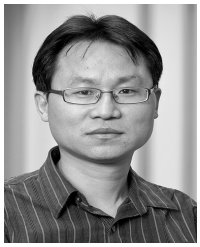
[10] R. A. Dora, P. D. Schalk, J. E. McCarthy, and S. A. Young, "Remote suspect identification and the impact of demographic features on keystroke dynamics," *Proc. SPIE*, vol. 8757, p. 87570B, May 2013.

[11] G. A. Carpenter, S. Grossberg, N. Markuzon, J. H. Reynolds, and D. B. Rosen, "Fuzzy ARTMAP: A neural network architecture for incremental supervised learning of analog multidimensional maps," *IEEE Trans. Neural Netw.*, vol. 3, no. 5, pp. 698–713, Sep. 1992.

[12] D. Premack and G. Woodruff, "Does the chimpanzee have a theory of mind?" *Behavioral Brain Sci.*, vol. 1, no. 4, pp. 515–526, 1978.
[13] E. L. Newton, "The rocky road from actions to intentions," Ph.D. dissertation, Dept. Psychol., Stanford Univ., Stanford, CA, USA, 1990.
[14] M. Dong, T. Kimata, K. Sugiura, and K. Zettsu, "Quality-of-experience (QoE) in emerging mobile social networks," *IEICE Trans. Inf. Syst.*, vol. E97-D, no. 10, pp. 2606–2612, Oct. 2014.

JAMIE SETO received the bachelor's degree in information technology from the University of Ontario Institute of Technology, Oshawa, ON, Canada, in 2013, where she is currently pursuing the master's degree with the Faculty of Business and Information Technology. Her research interests include smartphone security, authentication and identity management, and security and usability.

YE WANG received the Ph.D. degree in information and communication engineering from the Harbin Institute of Technology, Harbin, China, in 2013. He is currently a Post-Doctoral Fellow of Information Security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON, Canada. His research interests include wireless networking, cognitive radios networks, and radio resource management.



XIAODONG LIN (S'07–M'09–SM'12) received the Ph.D. degree in information engineering from the Beijing University of Posts and Telecommunications, Beijing, China, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, with the Outstanding Achievement in Graduate Studies Award. He is currently an Associate Professor of Information Security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON, Canada. His research interests include wireless network security, applied cryptography, computer forensics, software security, and wireless networking and mobile computing. He was the recipient of the Natural Sciences and Engineering Research Council of Canada (NSERC) Canada Graduate Scholarships-Doctoral and the Best Paper Awards of the 18th International Conference on Computer Communications and Networks in 2009, the 5th International Conference on Body Area Networks in 2010, and the 2007 IEEE International Conference on Communications.