ZEMFA: Zero-Effort Multi-Factor Authentication based on Multi-Modal Gait Biometrics

Babins Shrestha
VISA Inc.
Austin, TX, USA
babishre@visa.com

Manar Mohamed
Miami University
Oxford, OH, USA
mohamem@miamioh.edu

Nitesh Saxena
University of Alabama at Birmingham
Birmingham, AL, USA
saxena@uab.edu

***Abstract*—In this paper, we consider the problem of transparently authenticating a user to a local terminal (e.g., a desktop computer) as she approaches towards the terminal. Given its appealing usability, such *zero-effort authentication* has already been deployed in the real-world where a computer terminal or a vehicle can be unlocked by the mere proximity of an authentication token (e.g., a smartphone). However, existing systems based on a single authentication factor contains one major security weakness — unauthorized physical access to the token, e.g., during lunch-time or upon theft, allows the attacker to have unfettered access to the terminal.**

We introduce *ZEMFA*, a *zero-effort multi-factor authentication* system based on multiple authentication tokens and multi-modal behavioral biometrics. Specifically, *ZEMFA* utilizes two types of authentication tokens, a smartphone and a smartwatch (or a bracelet) and two types of gait patterns captured by these tokens, mid/lower body movements measured by the phone and wrist/arm movements captured by the watch. Since a user's walking or gait pattern is believed to be unique, only that user (no impostor) would be able to gain access to the terminal even when the impostor is given access to both of the authentication tokens. We present the design and implementation of *ZEMFA*. We demonstrate that *ZEMFA* offers a high degree of detection accuracy, based on multi-sensor and multi-device *fusion*. We also show that *ZEMFA* can resist active attacks that attempt to mimic a user's walking pattern, especially when multiple devices are used.

***Index Terms*—Authentication, Biometrics, Walking-pattern, Phone, Wearables, Sensors, Context.**

I. Introduction

Balancing the security and usability of user authentication is an important challenge facing the security community. One classical problem pertains to transparently authenticating a user to a local terminal (e.g., a desktop computer) as she approaches towards the terminal. Such *Zero-effort authentication* (*ZEA*) [8] represents a rapidly emerging paradigm, in which a verifier device authenticates a prover device in physical proximity of the verifier while requiring *no extra effort* by the user of the prover device. The user, carrying the prover, usually just walks towards the verifier and the verifier gets unlocked automatically. In this approach, the prover and verifier devices pre-share a security association, and simply execute a challenge-response based protocol for the verifier to authenticate the prover.

The zero-effort requirement is intended to improve the usability of the authentication process, which may increase the chances of adoption. Indeed, *ZEA* systems are already getting deployed in many real-world application scenarios. For example, BlueProximity [2] allows a user to unlock the idle screen lock in her computer merely by physically approaching the computer while in possession of a mobile phone, without having to perform any other action, such as typing in a password. Other *ZEA* systems include: "Passive keyless entry and start" systems like "Keyless-Go" [33], PhoneAuth [10], and access control systems based on wearable devices [49]. Android also allows automatic unlocking of a smartphone using "Trusted devices" [16]. A Bluetooth watch, fitness tracker, or car speaker system can be used as a trusted device to unlock the phone.

However, the zero-effort nature of existing single-factor *ZEA* systems opens up a fundamental vulnerability — unauthorized physical access to the prover device, e.g., during lunch-time or upon theft, would allow an attacker to have unfettered access to the verifier device. Since the prover device does not require any authorization from the user prior to responding to the verifier device in a *ZEA* authentication session, mere possession of a lost or stolen prover device is sufficient to gain access to the verifier device. Since users' personal devices and items (e.g., smartphones or car keys) are prone to loss or theft, this issue makes the *ZEA* systems inherently weak and insecure. Speaking about statistics, digital trends [35] reports that Americans lost $30 billion worth of mobile phones in 2011. Moreover, the trend has been increasing as reported by Lookout [29] that 3.1 million Americans consumers were victims of smartphone theft which is double the number reported in 2012 by Consumer Reports [48].

This raises an important research challenge: *how to protect the ZEA systems in the face of loss or theft of prover devices, while still keeping the authentication process transparent and zero-effort for the user?* In this paper, we aim to address this challenge with *ZEMFA*, a *zero-effort multi-factor authentication* system based on multiple prover devices and multi-modal behavioral biometrics. Specifically, *ZEMFA* utilizes two types of prover devices, a smartphone and a smartwatch (or a bracelet) and two types of gait patterns captured by these tokens, mid/lower body movements measured by the phone and wrist/arm movements captured by the watch. Since a user's walking pattern is believed to be unique, only that user (no impostor) would be able to gain access to the

978-1-7281-3265-5/19/$31.00 ©2019 IEEE

verifier device in a *ZEA* session, even when the impostor has access to both of the prover devices. Since the user has to nevertheless walk towards the verifier device as part of the *ZEA* authentication process, *no additional effort* is imposed on the user, thereby preserving the zero-effort and user-transparency requirement.

While walking-based biometrics schemes have been studied in prior literature for other application settings (as reviewed in Section III), our main novelty lies in three important aspects:

1) The specific application domain of our work which uses walking biometrics to transparently enhance the security of zero-effort authentication.
2) The use of *multiple sensors* available on the current breed of devices (e.g., accelerometer, gyroscope and magnetometer).
3) The use of *multiple devices* carried by the user, in particular, an "in-pocket" smartphone and a "wrist-worn" smartwatch. Each of these devices capture unique physiological and behavioral facets of the user's walking pattern (e.g., phone captures hip movement and watch captures hand movement).

Such a use of multi-factor authentication improves both the robustness against accidental errors as well as malicious impersonation attempts. The attacker against our scheme has to steal both the devices as well as mimic the user's walking patterns with respect to both devices (i.e., arm and hip movements).

Our Contributions: The primary contributions of this paper are three-fold:

1) *Design of a Multi-Factor ZEA System*: We introduce, design and implement *ZEMFA*, a multi-modal walking biometrics approach tailored to enhance the security of *ZEA* systems against stolen prover devices (*still* with *zero-effort*). Our *ZEMFA* system uses an Android smartphone and/or an Android smartwatch to extract walking biometrics to authorize a *ZEA* authentication session. *ZEMFA* works with a total of 336 features derived from 8 sensors of each of the 2 devices. Our system can also support authentication just based on one of the devices (phone or watch) and the gait pattern captured by that device.
2) *Evaluation under Benign Settings and Passive Attacks*: We demonstrate that *ZEMFA* offers a high degree of detection accuracy, based on multi-sensor and multi-device *fusion*. Our results show that walking biometrics can be extracted with a high overall accuracy when using one of the devices (phone or watch), and became almost error-free when both devices were used together (i.e., 0.2% false negatives and 0.3% false positives on average). This suggests that *ZEMFA* can be highly accurate in detecting a valid user as well as an unauthorized entity who (accidentally or deliberately) walks towards the authentication terminal.
3) *Evaluation under Active Imitation Attacks*: We show that *ZEMFA* can resist active attacks that deliberately attempt to mimic a user's walking pattern, including a state-of-the-art *treadmill-based attack* [24]. In particular, our results suggest that, especially when using both devices (phone and watch), such attacks would become very difficult in practice (4.55% false positives on average) even when the attacker capabilities are very high.

II. Background

In this section, we define and present the existing threat model for a Zero-effort authentication (*ZEA*) system. Then, we enumerate the design goals of our proposed system.

A. Zero-Effort Authentication

A *ZEA* system relies upon the authentication factor "something you have". A *ZEA* scheme involves a user who carries a prover device ($\mathcal{P}$) and needs to validate her identity to a verifier device ($\mathcal{V}$). $\mathcal{P}$ and $\mathcal{V}$ typically communicate over a short-range wireless communication channel such as Bluetooth. $\mathcal{P}$ and $\mathcal{V}$ share a prior security association (shared key K) and the messages between them are encrypted and authenticated. In particular, a *ZEA* authentication session runs a challenge-response authentication protocol that authenticates $\mathcal{P}$ to $\mathcal{V}$. That is, $\mathcal{V}$ sends a random challenge C to $\mathcal{P}$, and $\mathcal{P}$ returns back a response R which is an authenticated encryption of C, in order to prove the possession of the shared key K. The user does not need to perform any explicit action or gestures in the authentication process. Simply walking towards $\mathcal{V}$, while carrying $\mathcal{P}$, establishes the authentication.

B. Threat Model

In *ZEA* threat model, $\mathcal{P}$ and $\mathcal{V}$ are assumed to be honest (i.e., uncompromised and non-malicious). The communication channel between $\mathcal{P}$ and $\mathcal{V}$ is protected with encryption and authentication tools. Further, we assume that the attacker cannot manipulate $\mathcal{P}$'s hardware and that the sensor data is trustworthy. Trusted Platform Module [37] technique can be used to assure the integrity of a device.

In a realistic threat model, an attacker should be assumed to be in possession of the $\mathcal{P}$ devices. The attacker may obtain the $\mathcal{P}$ devices either by stealing it or via a lunchtime attack [11]. In this model, existing *ZEA* systems are completely broken since the attacker can just access $\mathcal{V}$ by using the $\mathcal{P}$ devices.

ZEA systems are known to be vulnerable to relay attacks. This is because the user usually carries $\mathcal{P}$ and gets verified when she simply comes near to $\mathcal{V}$ over radio-frequency (RF) signals. A relay attacker's goal is to relay these RF signals from $\mathcal{P}$ to $\mathcal{V}$ such that the attacker is authenticated without possessing $\mathcal{P}$. Security researchers have proposed various techniques to defend against relay attacks such as using distance time bounding [3], [19], [42] or using context information from the environment [17], [45], [50]. As such, the threat model assumes that a relay attack prevention technique has already been deployed and preventing relay attacks is an orthogonal problem. However, such a technique can not defend against the theft or loss of the $\mathcal{P}$ device (this is the vulnerability we aim to address in this paper).

C. Design Goals and Metrics

For a *ZEA* scheme that remains secure even under the event of loss or theft of the $\mathcal{P}$ device, like the one proposed in this paper, following design criteria must be considered:

1) *Lightweight*: The scheme should be lightweight in terms of the various resources available on the device, such as memory computation and battery power.
2) *Efficient*: The approach should not incur perceptible delay. Users should not be required to wait for a long period to get authenticated.
3) *Robust*: The scheme should be robust to errors and attacks. The system must authenticate with high probability when an authorized user with $\mathcal{P}$ is authenticating to $\mathcal{V}$ while the unauthorized users must be denied access to $\mathcal{V}$. It must also be robust towards the active attackers who may intentionally attempt to bypass the system (e.g., mimic the user's walking pattern on our proposed scheme).
4) *Transparent & Zero-Effort:* Since the approach is zero-effort, the authentication should be transparent to the users. The users should not be required to perform additional tasks (such as typing passwords/pins) or explicit gestures. These actions may degrade the usability of the system, and reduce chances of adoption.

III. Related Work

The field of gait biometrics has been well-studied in research literature. Compared to the existing work, our novelty lies in the use of gait biometrics for the *ZEA* systems, and in the way we extract the gait patterns, i.e., using multiple commodity devices and multiple sensors therein. In this section, we review the existing literature on gait biometrics.

Many researches have explored the use of accelerometer to authenticate the users based on their walking pattern. These work mostly use electronic motion recording (MR) devices such as MR100 wearable sensor [34], ZSTAR [34], [47], ADXL202JQ accelerometers [30], MMA7260 [43], etc. These work analyze the accelerometer reading by attaching such MR sensors at different location of the body such as waist [1], [30], [34], [43] (device wore in a belt), lower leg [13], [46], shoe [7], [20], [36], [55], pockets (chest/hip) [14], [54], upper limb/forearm [14], gloves [23], [40], [44], and so on. In most of these work, the MR device was tied to the specific body parts as most of these devices were not wearable.

Vildjiounaite et al. [54] used accelerometer module (MR sensor) and placed it in chest pocket, hip pocket and hand to authenticate users based on their walking pattern. To perform their experiment, they made mock-ups of "clothes with pockets" from pieces of textile which the users put on over their normal clothes. Gafurov et al. [14], [15] also used a "Motion Recording Sensors" (MRS) to collect accelerometer data. In their work [15], they tried to spoof the user's walking pattern by performing the experiment in two rounds. First, the targeted user walked in front of the attacker twice. Then, the attacker walked alone twice mimicking the user. They showed that such minimal effort impersonation attack on gait pattern does not increase the chances of impostors being accepted significantly. In our work, the attacker watched the victim's walking pattern in person, recorded the pattern in video, and got feedback from his colleagues during training. Further they used MRS attached to the belt while we used commercial devices such as smartphone and smartwatch.

Stang et al. [47] also explored the gait based authentication approach using ZSTAR accelerometer sensor and analyzed if the impostors could imitate the walking pattern. They recruited 13 participants to imitate users. Each participant was given 15 attempts on each template to attack. The impostors did not see the original walking but they were given a simple description of the gait. The participants were provided with the visual feedback such that they could see the template gait graph and their gait graph continuously plotted on a big screen. After each attempt a match score between 0 and 100 was displayed based on correlation such that 100 is a perfect match. They reported 3 persons exceeded the correlation threshold once, 2 persons exceeded the threshold twice, 1 person exceeded it three times and 1 person managed to exceed as much as 9 times in 15 attempts. Therefore, they concluded that it is easy to walk like another person.

Another attempt to mimic walking pattern was made by Mjaaland et al. [34]. They trained seven impostors to imitate a specific victim. They used two wearable sensors: the Motion Recording 100 (MR100), and the Freescale ZSTAR sensor to record the accelerometer sensor values. They attached these sensors on belt and asked the participants to wear the belt which could be mounted to any person's hip such that the device would always have the same-orientation. They conducted short-term hostile scenario and long-term hostile scenario. In the former scenario, they trained six participants for two weeks, five hours every day while in the latter scenario, they trained the seventh participants for six weeks. In both scenarios, the impostors were not able to imitate the victim's walking pattern. They concluded that there is a physiologically predetermined boundary to every individual's mimicking performance such that if one successfully adopted gait characteristics improved an attacker's performance, other characteristics worsen in a chain-like effect.

Muaaz and Mayrhofer evaluated the security of the gait based authentication system using smartphone [38], [39]. They developed an Android application which used smartphone accelerometer to capture gait data. They used acceleration magnitude to estimate gait cycle length and detect gait cycle. Finally, they used Dynamic Time Warping (DTW) distance metric to identify the users and the attackers. They tested the performance of the system with 35 participants with gait data recorded in two different sessions with an average gap of 25 days. Then, they hired five professional actors, specialized in mimicking body movements, to impersonate victims and perform attacks. They observed zero false positive with the impersonation attacks. Similar to Mjaaland et al. [34], they claimed that during impersonation attack, the attackers lost regularity between their steps which made impersonation even harder for attackers.

Similar to our work, Kumar et al. [24] also used an Android smartphone with an app to record sensor data as described in Section VII-B. They only used features extracted from accelerometer sensors while we used features from eight different sensors. From the 47 features extracted from accelerometer sensor only, they ranked their features based on information gain based attribute evaluator [18] and selected 17 top ranked features only. In our work, we explored the best result for the combination of all 336 feature subset. Since they were using features extracted from accelerometer sensor only, the features might be highly correlated and reported that that their system's FAR increased from 5.8% to 43.66%. In our work, the best feature subset consists of the eight uncorrelated features with correlation less than ± 0.1. An attacker would need more sophisticated device than a treadmill to control more gait characteristics (defined in Section VII-B).

Researchers have also explored accelerometer and/or gyroscope sensors available on current smartwatches for the purpose of gait detection. Arki wristband by Zikto can authenticate users by their arm swing size, average tempo, rotation angle, frequency and many other features [41]. Lamiche et al. [26] used accelerometer to continuously authenticate user based on gait patterns and key stroke dynamics. Johnston et al. [21] used the accelerometer sensor embedded in the smartwatch, while Kumar et al. [25] used the accelerometer and the gyroscope sensor. In contrast to us, Kumar et al. only used the sensors from smartwatch and did not consider the use of multiple devices (both phone and watch). The authors only extracted a total of 76 features (32 features from the accelerometer readings and 44 features from the gyroscope readings), while we work with a total of 336 features, resulting in much lower FNR and FPR. Also, unlike our work, Kumar et al. did not study active attacks and only reported the performance under the zero-effort or random attack. Moreover, the targeted applications for the two works are different (*ZEA* vs. continuous authentication).

TABLE I
Sensors utilized for walk biometrics.

Sensor Name	**Sensor Type**	**Description**
Accelerometer (A)	Motion	The acceleration force including gravity
Gyroscope (Gy)	Motion	The rate of rotation
Linear Acceleration (LA)	Motion	The acceleration force excluding gravity
Rotation Vector (R)	Motion	The orientation of a device
Gravity (G)	Motion	The gravity force on the device
Game Rotation (GRV)	Position	Uncalibrated rotation vector
Magnetic Field (M)	Position	The ambient magnetic field
Orientation (O)	Position	The device orientation

IV. Our Approach: Multi-Factor Walk-Unlock ZEA

To protect the unlocking of $\mathcal{V}$ in the face of loss or theft of $\mathcal{P}$ in a *ZEA* scheme, we propose to authenticate the user based on a gait-based authentication system. In other words, we propose to authenticate the user with her unique walking pattern. Different categories of sensors are embedded nowadays into smartphones and smartwatches such as motion, position and environment sensors. Android OS, one of the most popular smart device operating systems, provides APIs to support different categories of these sensors. We leverage these sensors, especially motion and position sensors, to identify that the $\mathcal{P}$ device is undergoing a particular activity, in a specific motion and orientation, as if the prover device is being carried/worn by the legitimate user. This activity detected by the $\mathcal{P}$ device is transparent to the user since it is performed implicitly while the user walks towards $\mathcal{V}$.

While many types of $\mathcal{P}$ devices may be used to detect the user's walking activity prior to authorizing a *ZEA* session, in this paper, we capture the walking biometrics using an "in-pocket" device and/or a "wrist-worn" device, both devices having multiple on-board sensors. Specifically, in such a walk-unlock *ZEA* (*ZEMFA*) scheme, we aim to authenticate the user in a robust manner using machine learning classifiers based on data drawn from multiple sensors from multiple devices such as smartphone (in-pocket) and smartwatch (wrist-worn). There are other applications which support *ZEA* and provide multi-factor authentication besides proximity of the device such as ZEBRA [31] and Sound-Proof [22]. However, these applications have different application scenarios. ZEBRA [31] uses correlation between keystroke events and wrist movements, geared towards authentication to terminals in shared workspace. Sound-Proof [22] verifies the proximity of devices based on ambient audio as second factor, geared for authentication to remote websites.

In our *ZEMFA* system, we use multiple devices, i.e., a smartphone and a smartwatch, to authenticate the user. However, to analyze the efficiency and robustness of our system systematically, we show walking pattern extraction:

1) using the in-pocket smartphone,
2) using the wrist-worn smartwatch, and
3) using combination of the above two.

The second setting is suitable for situations where the user may leave her phone on the desk space or the car dashboard, and will need to be logged in just by using her watch. Although currently most of the smartwatches work along with companion devices (smartphones), we believe that in the future such devices would be usable as stand-alone devices.

The threat model of *ZEMFA* is in line with that of *ZEA* (Section II-B), except that the former aims to be secure even under the adversarial possession of $\mathcal{P}$. Since in the proposed scheme, $\mathcal{P}$ can be either a smartphone or a smartwatch or both, the attacker may therefore possess only one of the devices or both devices. After the attacker possesses $\mathcal{P}$ (one or both devices), it will try to unlock $\mathcal{V}$. Further, a *ZEMFA* attacker may be active in the sense that it may try to authenticate itself as the valid user by mimicking the walking pattern of the user as measured by $\mathcal{P}$ device(s). We allow such an attacker to observe (and record) the user in an attempt to imitate the user's walking habits.

In the *ZEMFA* system, we assume that a relay attack prevention technique has already been deployed (like in a *ZEA* system). That is, no relay attacks are possible between $\mathcal{P}$ and $\mathcal{V}$. Similarly, we assume that no relay attacks are possible between the $\mathcal{P}$ devices (phone and watch). Also, we assume that the two $\mathcal{P}$ devices are securely paired with each other and that all communication between them has been protected with traditional cryptographic mechanisms.

Given this threat model, in the following sections, we will show that the *ZEMFA* system satisfies all of our design goals (Section II-C), i.e., being lightweight, efficient, robust and transparent.

V. Data Collection: Design and Procedures

To develop and evaluate our system for authenticating the users based on their walking pattern, we need to collect the sensors data from the users' smartphones and smartwatches while they are walking. We developed a framework that encompasses two Android apps and a web app. The web app utilizes Google Cloud Messaging (GCM) to send commands to the smartwatch. One of the Android apps is installed on the smartphone and the other is installed on the smartwatch.

1) *Web App:* We used GCM to send start/stop commands to the smartphone, which upon receiving start/stop recording the sensors data and send start/stop recording trigger to the smartwatch. We created a simple HTML page with a text box to record the user information, a start recording button, and a stop recording button. The experimenter first inputs the user information in the text box and hits the start recording button when the user starts walking towards $\mathcal{V}$. When the user touches $\mathcal{V}$, the experimenter hits the stop recording button. We used GCM for the purpose of data collection only (in real-life implementation, GCM is not needed).
2) *Smartphone App:* The app on the smartphone waits for the GCM commands. As soon as it receives the GCM start command, it sends a start recording trigger to the smartwatch and starts recording the sensors value. As soon as it receives the GCM stop command, it sends a stop recording trigger to the smartwatch and stops recording the sensors value.
3) *Smartwatch App:* The app on the smartwatch waits for the smartphone's triggers. Once it receives a start recording trigger, it starts recording the sensors values and keeps on recording until it receives a stop recording trigger. The recorded sensor values are stored in the smartwatch.

The sensors utilized in our implementation, from both the smartphone and the smartwatch, are listed in Table I.

For data collection, we recruited 18 students in our University through word of mouth. Among these participants, 15 were male while 3 were female. To avoid any kind of inconsistency, we used only one smartphone (LG Nexus 5 (D820) [51]) and one smartwatch (LG G watch R (W110) [52]). Both devices have Android OS version 6.0.1.

We conducted the experiment following the University's IRB guideline. The participants were clearly informed about the experiment such as the data being collected, the purpose of the experiment, and that they can refuse to participate in the middle of the experiment or even request to delete their collected data during or after the experiment has been conducted. Our University's IRB approved the project.

After the participants were detailed about the experiment, we asked these volunteers to wear the smartwatch on their (left/right) hand where they normally wear their watch and put the smartphone in their (left/right) pocket where they normally put it during walking. We asked each volunteer to walk from a door to the computer in a lab setting as if they are trying to log in. The experimenter sent the GCM command to the smartphone to start the sensors recording when the user started walking. As soon as the user touches the keyboard as if the user is trying to log into the computer, the experimenter sent another GCM command to stop the sensors recording. We noticed that some users log into the machine standing while others sit on a chair before they touch the keyboard. One participant even placed his phone on the desk before he logged into the machine.

We collected the data from these volunteers for a period of time ranging from 30 to 60 days based on their availability. We asked each user to walk from the door to the computer in our lab for five times each day. We collected the data from each user for 10 days resulting in 50 samples of walking data from each user.

VI. Gait Biometrics Detection: Design and Evaluation

In order to evaluate the performance of the proposed gait biometrics as an authentication scheme, we utilized the machine learning approach based on the underlying readings of the motion sensors, and the position sensors from both of the phone and the watch.

A. Preliminaries

Classifier: In our analysis, we utilized the Random Forest classifier. Random Forest is an ensemble approach based on the generation of many classification trees, where each tree is constructed using a separate bootstrap sample of the data. To classify a new input, the new input is run down on all the trees and the result is determined based on majority voting. Random Forest is efficient, can estimate the importance of the features, and is robust against noise [32]. Random Forest outperforms other classifiers including support vector machines which are considered to be the best classifier currently available [6], [28], [32].

Features: For each of the used sensor instances, we calculated the mean, the standard deviation and the range of each of the axis (X, Y, Z), the square of each axis (X^2, Y^2, Z^2) and the square root of the sum of squares for that instance's axes components (X, Y, Z) of all the instances in the sample that corresponds to a single walk instance. Twenty one features are extracted from each of the used sensors, which give us a total of 336 features.

The 336 features or subset of them were used as input to train the classifier to differentiate a user from other users. In the classification task, the positive class corresponds to the gait of the legitimate user and the negative class corresponds to impersonator (other user). Therefore, true positive (TP) represents the number of times the legitimate user is granted access, true negative (TN) represents the number of times the impersonator is rejected, false positive (FP) represents the number of times the impersonator is granted access and false negative (FN) represents the number of times the correct user is rejected.

As performance measures for our classifiers, we used false positive, false negative, precision, recall and F-measure (F1 score), as shown in Equations (1) to (2). FP/precision measures the security of the proposed system, i.e., the accuracy of the system in rejecting impersonators. FN/recall measures the usability of the proposed system as high FN leads to high rejection rate of the legitimate users. F-measure considers both the usability and the security of the system. To make our system both usable and secure, ideally, we would like to have FP and FN as close as 0 and recall, precision and F-measure as close as 1.

$$precision = \frac{TP}{TP + FP}; \qquad recall = \frac{TP}{TP + FN} \tag{1}$$

$$F\text{-}measure = 2 * \frac{precision * recall}{precision + recall} \tag{2}$$

In order to build a classifier to authenticate the user based on her gait biometrics, we used *leave-one-out cross validation*. We hold out one subject as an impostor to be tested, and use the other 16 impostors for training. We then repeat the process 17 times for each specific subject and report the average of the results. Using this methodology, the actual impostor data used for testing does not contaminate the training data. For training, we randomly selected data samples from the 16 impostors dataset. We limited the number of samples selected from 16 imposter dataset to equal to the number of samples from the user under consideration so that their is no biasness in the training model.

B. *Classification Results*

As mentioned in Section V, we collected data from 18 users. From each user, we collected 50 samples of walking data. In order to build a classifier to authenticate a user based on her gait biometrics, We divided the collected data into 18 sets based on the users' identities (ids).

The classification results are obtained after running a leave-one-out cross validation as specified in Section VI-A and are summarized in Table II. The first part of Table II ("All Sensors") shows the results of using all the features extracted using sensors from the phone, the watch and both devices. We found that combining the features from the phone and the watch sensors decreases the false negative rate from 5% in case of only watch to 4.3% and decreases the false positive from 13% in case of only phone, 15.5% in case of using only watch to 10.2%.

The second part of Table II ("Overall Best") shows the results obtained by finding the sensor subset that provides the best overall average. We found that utilizing only accelerometer, gravity, gyroscope, magnetometer and rotation vector sensors from phone rather than using all phone sensors decreases the false negative and the false positive by around 1%. Similarly, using only accelerometer, gravity, gyroscope and magnetometer sensors from watch instead of using all watch sensors decreases the false negative rate from 5% to 4.3% and the false positive rate from 15.5% to 15.0%. Furthermore, we found utilizing only phone accelerometer, phone gyroscope, phone magnetometer, watch accelerometer and watch magnetometer sensors improves the classification accuracy (i.e., decrease both the false negative and the false positive rates by 3.3% and 1.4%, respectively). These features subset also contained the subset of features which were not correlated to each other. We leverage these uncorrelated features to prevent our *ZEMFA* system against a sophisticated form of active impersonation attack [24], as we will describe in Section VII-B.

Finally, we checked the classification accuracy by selecting for each user the subset of sensors that provides the best results. The results of this model are shown in the last three rows of Table II ("Individual"). We found out that the classifier performance improved over the previous two models. Moreover, both the average false positive and the average false negative rates dropped to around 2.5% when we used the best subset from both of the devices.

In summary, the results obtained from the classification models show that the gait biometrics can be detected in a robust manner and thus will serve as an effective method for authenticating the users. The results show that the fusion of the phone and the watch sensors significantly enhances the performance of detecting the gait biometrics. This is reflected in very low false positives and false negatives. We noticed that phone magnetometer and phone gyroscope sensors were the most dominating sensors to identify users as they occurred in most of the best sensor subset for each individual. These two sensors were followed by phone accelerometer sensor. Among the sensors from watch, the watch accelerometer was found most frequently in the best sensor subset. The list of sensors ranked according to their occurrence in best sensor subset is shown in Appendix Table IV.

VII. Resistance to Active Attacks

A. *Human Impostor Attack*

In a human-based impostor attack, the adversary tries to manually mimic a victim's walking pattern so that it can fool the *ZEMFA* system. Our model assumes that the attacker already has the physical possession of the $\mathcal{P}$ devices (phone and/or watch). Such kinds of attacks have been explored in the literature by few researchers [15], [34], [47]. However, most of

TABLE II
PERFORMANCE FOR THE CLASSIFIER FOR THREE DIFFERENT CATEGORIES. THE FIRST THREE ROWS SHOW THE PERFORMANCE OF THE CLASSIFIER USING ALL THE SENSORS. THE NEXT THREE ROWS SHOW THE RESULTS OF USING THE SENSORS SUBSET THAT PROVIDES THE BEST AVERAGE RESULTS. THE LAST THREE ROWS SHOW THE RESULT OF USING THE BEST SENSORS SUBSET FOR EACH USER. HIGHLIGHTED CELLS EMPHASIZE THE MOST INTERESTING RESULTS.

		FNR	**FPR**	**F-Measure**	**recall**	**precision**
		Avg (std. dev.)				
All Sensors	**Phone Only**	0.028 (0.018)	0.130 (0.068)	0.913 (0.067)	0.890 (0.094)	0.852 (0.047)
	Watch Only	0.050 (0.020)	0.155 (0.065)	0.884 (0.067)	0.862 (0.097)	0.829 (0.046)
	Both	0.043 (0.012)	0.102 (0.055)	0.934 (0.042)	0.957 (0.058)	0.924 (0.039)
Overall Best	**Phone Only**	0.019 (0.012)	0.116 (0.064)	0.929 (0.052)	0.907 (0.064)	0.862 (0.044)
	Watch Only	0.043 (0.024)	0.150 (0.062)	0.892 (0.063)	0.872 (0.091)	0.831 (0.046)
	Both	0.010 (0.003)	0.088 (0.043)	0.953 (0.023)	0.929 (0.025)	0.880 (0.032)
Individual	**Phone Only**	0.027 (0.019)	0.101 (0.057)	0.948 (0.036)	0.929 (0.028)	0.874 (0.038)
	Watch Only	0.058 (0.029)	0.138 (0.058)	0.923 (0.040)	0.915 (0.041)	0.841 (0.042)
	Both	0.025 (0.012)	0.052 (0.036)	0.976 (0.016)	0.944 (0.001)	0.905 (0.027)

TABLE III
PERFORMANCE FOR THE IMPOSTOR ATTACK ON TWO DIFFERENT VICTIM USERS FOR THE CLASSIFIER TRAINED WITH THE BEST SUBSET FOR THE INDIVIDUAL VICTIM USER. HIGHLIGHTED CELLS EMPHASIZE THE MOST INTERESTING RESULTS.

		Victim V_1		**Attacker**	**Victim V_2**		**Attacker**
		F-measure	**FPR**	**FPR**	**F-Measure**	**FPR**	**FPR**
Individual	**Phone Only**	0.970	0.040	0.182	0.968	0.060	0.917
	Watch Only	0.960	0.060	0.000	0.968	0.060	0.000
	Both	1.000	0.000	0.091	1.000	0.000	0.000

these works use accelerometer devices (e.g., MR100 wearable sensor) (not a phone or a watch used in our scheme), and these devices are worn on the waist tied to the belt [15], [34] or on the limbs near the shoes [47]. Therefore, we analyze how our system will perform when an attacker with similar physical characteristics attempts to learn and imitate an individual's walking pattern.

During the walking biometrics data collection, we recorded videos of eight different users. The attacker (a researcher, serving the role of an expert attacker) chose two of the users as victims (we call them V_1 and V_2) who exhibited the simplest walking pattern or distinctive visible characteristics, upon careful visual inspection. These victims also have a similar physical build to that of the attacker. Hence, we claim this as the "best case attack". If the attacker can not succeed in attacking such simplistic walking patterns with similar built, then it would be harder for the attacker to succeed in attacking more complex walking patterns.

In our experiment, the attacker watched the video several times so as to learn the feet and the hand movement pattern of the user. While practicing, the attacker also tried to match the time duration from the start to the end of the victim's walk, using the video. After the attacker felt comfortable with the timing and the walking pattern, we collected the data for the attacker with $\mathcal{P}$ walking towards $\mathcal{V}$. The attacker was provided the visual feedback while imitating the walk pattern.

To measure the performance of the impostor in mimicking the victim, we first trained a random forest classifier with the victim's data using 10-fold cross validation. We analyzed the classifier's accuracy with features from the phone only, the watch only and both devices. We trained our classifiers with the subset of features that provided the best performance for the individual user (victim). Then, we tested these classifiers against the impostor attacker's data to determine the success rate of the attacker. The results are shown in Table III.

With the classifier models built with individual best subset features, the attacker could not imitate the hand motion resulting low attack success rate when both devices' features were used. In other words, *ZEMFA* could resist the impostors to a high degree when the best subset of features from both devices were used for each individual user.

In summary, these results show that the *ZEMFA* system that leverages both phone and watch, and employs individualized classifiers can be highly resistant to walking imitation attacks. This is a significant security advantage of a multi-device *ZEMFA* scheme.

B. Treadmill Attack

To perform a more powerful attack on the victim's walking pattern so as to successfully fool the *ZEMFA* system, we followed the work by Kumar et al. [24]. This research represents the state-of-the-art attack against gait biometrics and is therefore an ideal platform to evaluate our system against. In this attack, the attacker already has the sample of a victim's gait pattern. First, the authors extract different features from the accelerometer sensor of the smartphone to authenticate users based on their walking pattern to create a baseline model called Gait Based Authentication System ($GBAS$). Then, they attack on the $GBAS$ system using a treadmill. In this attack, instead of imitating the victim's walking pattern, the attacker uses treadmill to control different gait characteristics (GCAT) such as speed, step length, step width and thigh lift to match the features extracted from the victim's walking pattern. To setup this attack, the attacker first analyzes the feature subsets that dominates the decision making process of the machine-learning classifiers [24]. Among these dominant features subset, the attacker then analyzes how these features are correlated with each other. From this analysis, the attacker tries to manipulate only one feature among the correlated features set. Now the attacker has final set of five features which it needs to manipulate to fool the classifier. Correlation analysis of the features is the foundation for this attack. The experimenter creates an imitator profile based on these final five features mapped to the four GCAT. This mapping is also created using correlation between GCAT and the dominating feature set. For example, if speed is directly correlated with the mean of X-axis of the accelerometer (ACC_{X_M}) then to increase or decrease the ACC_{X_M}, the imitator needs to increase or decrease the walking speed, respectively.

We did not recreate a treadmill attack as discussed above. However, to thwart such attacks using treadmill to control different gait characteristics, we calculated the correlation values among each pair of features using Pearson's Correlation Coefficient [27]. We observe that the features from the phone are more correlated with the features from the phone while the features from the watch are more correlated with the features from the watch. This means that the attacker cannot use one device to alter the feature of the other device, however, it may be able to alter the features from a single device if it knows the correlation among the features from the same device.

We next analyzed how the features from a single device are correlated with the other features from the same device. From our correlation analysis, we see that the features extracted from a single sensor were more correlated to each other than the features extracted from different sensors. For example, mean, standard deviation and range of the accelerometer sensor were more correlated with each other, compared to those taken from gyroscope or magnetometer. Using the correlation analysis, we derived the best feature subset such that each feature is correlated to each other in a given feature subset by less than ± 0.1 (i.e., the subset of uncorrelated features). It will be harder for an attacker to correlate/match all the features with different gait characteristics if the number of uncorrelated features becomes too big [24]. Further, manipulating one gait characteristic may influence more than one feature vector which do not have any correlation, increasing the difficulty of the treadmill attack.

To increase the performance of the classifier in defending the treadmill attack, we analyzed to find out the super set of the subset containing maximum number of uncorrelated features set. The best feature subset for the overall best classifier in Section VI that is trained with features from both devices consists of eight uncorrelated features. This increased the accuracy of the classifier during the benign case while still being robust to the treadmill attackers. Furthermore, the treadmill attackers may use more sophisticated devices to provide better gait characteristics that may alter different features. We can defend this by increasing the correlation threshold (currently set to 0.1) for finding uncorrelated feature set. This will provide larger number of features that are correlated to each other by that threshold value. Note that the correlation of 0 to 0.1 is considered near-zero correlation while that between 0.1 and 0.3 is considered weak correlation [5], [12]. Hence, using the correlation threshold of 0.3 will still give the feature subset with weak correlation that attacker may not be able to attack using the treadmill technique.

VIII. Discussion

Adherence to Design Criteria: Our *ZEMFA* system is compliant with the design goals established in Section II-C. First, *ZEMFA* is triggered and sensor data is polled only when $\mathcal{V}$ sends a challenge to $\mathcal{P}$ in a challenge-response authentication protocol. After $\mathcal{P}$ has authenticated the user, the system deactivates the sensors. The classifier model is to be built offline during the training phase. The sensor data is collected for no more than 10 seconds and the decision making process by the classifier is pretty simple (random forest classification). Hence, *ZEMFA* will have minimal influence on the power consumption and time delay satisfying our design goals of being lightweight and efficient.

From our results in Table II, *ZEMFA* yields very high F-measure with very low FNR and FPR during the benign case. The results from Table III shows that *ZEMFA* is resistant to impostor attacks. Further, the use of uncorrelated sensor features makes *ZEMFA* tolerant to treadmill attacks. This makes *ZEMFA* very robust to errors and attacks.

Finally *ZEMFA* works in the background while the user walks towards $\mathcal{V}$. Hence, *ZEMFA* preserves the transparency of *ZEA* even though it adds another layer of strong security to the system.

ZEA & Bluetooth: *ZEA* systems are dependent on Bluetooth, and so is *ZEMFA*. *ZEA* and *ZEMFA* systems will fail if Bluetooth of either $\mathcal{P}$ or $\mathcal{V}$ is turned off. If Bluetooth is turned on, $\mathcal{P}$ can authenticate to $\mathcal{V}$, even when $\mathcal{V}$ is on sleep mode. This is similar to computer getting awake by a Bluetooth mouse or keyboard.

Fallback Scenarios: We showed that our system is very effective with very low FNR. However, a user may be injured, stressed, sick, or carrying the phone in a purse or backpack, which may significantly alter the user's walking behavior. Such situations can lead to false negatives, as the legitimate user will be denied access to the system. In such cases, we can fallback to traditional password/key based approach for authentication.

Effect of Changing Apparel or Footwear: A user's walking pattern may get affected with the use of varying apparel or footwear. Our data collection experiment was conducted in lab for a period ranging from 30 to 60 days. Even though our participants must have worn changing apparel and shoes during the data collection process, our classification accuracies are still quite high. This suggests that our classification model may be robust to changes in walking patterns arising from changing clothing and footwear.

Limitations: We recruited 18 volunteers to participate in the experiment. Although a larger sample is preferred for biometrics study, the number of subjects in our study is comparable to that in the earlier study on biometric authentication [34], [47]. In our experiment, all of our participants followed same route from a door to a computer with distance around 6m. This process usually took them less than 10 seconds. In real world, the distance between $\mathcal{V}$ and $\mathcal{P}$ can be different when the authentication protocol is triggered by $\mathcal{V}$. In our experiment, we manually triggered the authentication protocol. Our application did not implement the automatic data collection. In real world, the authentication protocol must implement automatic data collection and may be triggered when $\mathcal{P}$ and $\mathcal{V}$ are within less than a certain threshold distance. The distance may be calculated using the RSSI (Received Signal Strength Indicator) value. Also, time taken for a user to reach $\mathcal{V}$ can also be different due to different obstacles in between the user's route to $\mathcal{V}$. Further, a user may be holding the phone in her hand or carrying it in her bag as the study of [9] shows, instead of keeping it in a pocket or holding some object restricting her arm movement. Also, calls or notifications may cause devices to vibrate while the authentication scheme is recording the sensor values. These are some scenarios which may affect the sensor data and the features extracted may be significantly different resulting in false negatives denying access to a legitimate user. For such false negative scenarios when a legitimate user is denied, we can fallback to the traditional password or key based system. In our experiment, we also did not consider people with disabilities (for example a person on a wheelchair or a crutches). Our proposed system will not work in such cases. Either different behavioral biometric authentication scheme needs to be implemented or we can fallback to the traditional password or key based system.

Implementing *ZEMFA* on Car Keys: The core idea of *ZEMFA* is not just limited to smartphones. Smart keys were introduced as early as 1998 by Mercedes-Benz under the name "Key-less Go" [33]. The car keys have evolved from physical keys to Remote Keyless Entry (RKE) which then led to Passive Keyless Entry (PKE) systems [53]. These keys operate via RF signals and modern key systems claim that they use encryption to prevent car thieves from decoding the RF signal [53]. In 2008, BMW and NXP Semiconductors announced the first multi-functional car key which is compatible with EMV (Europay, MasterCard, VISA) electronic payment standard. Such keys contained a dedicated cryptographic coprocessor. Busold et al. [4] introduced smartphone-based NFC-enabled car immobilizers. *ZEMFA* can be implemented on such systems where the key (either physical, RKE or PKE) has embedded sensors, processor and RF capability.

IX. Conclusion and Future Work

We proposed a multiple factor zero-effort authentication system geared for local terminals to protect traditionally-deployed single factor zero-effort authentication systems in the event of loss or theft of authentication tokens. Our system transparently authenticates the user to her authentication terminal as she walks towards the authentication terminal in order to unlock it. It leverages a smartphone and/or a smartwatch, and multiple embedded sensors therein, to reliably detect the unique multi-modal walking pattern of the user. Our results suggest that when using both devices together, the system offers almost error-free detection and makes it very difficult for even a powerful attacker to imitate a user's walking habit. Consequently, we believe that our approach can significantly enhance the security of current *ZEA* systems without degrading their usability.

Future work may explore other types of wearable devices (such as glasses or shoes, which may capture head or feet movements, respectively) to further extend our approach, study the implementation of similar techniques on car keys in keyless entry systems, and conduct broader data collection campaigns with larger and diverse population samples.

References

[1] H. J. Ailisto, M. Lindholm, J. Mantyjarvi, E. Vildjiounaite, and S.-M. Makela. Identifying people from gait pattern with accelerometers. In *Defense and Security*, pages 7–14. International Society for Optics and Photonics, 2005.

[2] BlueProximity. SourceForge Project. http://sourceforge.net/projects/blueproximity/.

[3] S. Brands and D. Chaum. Distance-bounding protocols. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages 344–359, 1994.

[4] C. Busold, A. Taha, C. Wachsmann, A. Dmitrienko, H. Seudié, M. Sobhani, and A.-R. Sadeghi. Smart keys for cyber-cars: secure smartphone-based nfc-enabled car immobilizer. In *Proceedings of the third ACM conference on Data and application security and privacy*, pages 233–242. ACM, 2013.

[5] K. G. Calkins. Correlation coefficients. Available online at https://www.andrews.edu/~calkins/math/edrm611/edrm05.htm.

[6] R. Caruana and A. Niculescu-Mizil. An empirical comparison of supervised learning algorithms. In *Proceedings of the 23rd international conference on Machine learning*, pages 161–168. ACM, 2006.

[7] M. Chen, B. Huang, and Y. Xu. Intelligent shoes for abnormal gait detection. In *Robotics and Automation, 2008. ICRA 2008. IEEE International Conference on*, pages 2019–2024. IEEE, 2008.

[8] M. D. Corner and B. D. Noble. Zero-interaction authentication. In *Proc. 8th annual international conference on Mobile computing and networking*, MobiCom '02, pages 1–11, 2002.

[9] Y. Cui, J. Chipchase, and F. Ichikawa. A cross culture study on phone carrying and physical personalization. In *International Conference on Usability and Internationalization*, pages 483–492. Springer, 2007.

[10] A. Czeskis, M. Dietz, T. Kohno, D. Wallach, and D. Balfanz. Strengthening user authentication through opportunistic cryptographic identity assertions. In *Proc. 2012 ACM conference on Computer and communications security*, pages 404–414, 2012.

[11] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic. Preventing lunchtime attacks: Fighting insider threats with eye movement biometrics. 2015.

[12] Explorable.com. Statistical correlation. Available online at https://explorable.com/statistical-correlation.

[13] D. Gafurov, K. Helkala, and T. Søndrol. Biometric gait authentication using accelerometer sensor. *Journal of computers*, 1(7):51–59, 2006.

[14] D. Gafurov and E. Snekkenes. Gait recognition using wearable motion recording sensors. *EURASIP Journal on Advances in Signal Processing*, 2009:7, 2009.

[15] D. Gafurov, E. Snekkenes, and P. Bours. Spoof attacks on gait authentication system. *Information Forensics and Security, IEEE Transactions on*, 2(3):491–502, 2007.

[16] Google.com. Set up your device for automatic unlock. https://support.google.com/nexus/answer/6093922. [Online; accessed 30-May-2017].

[17] T. Halevi, D. Ma, N. Saxena, and T. Xiang. Secure proximity detection for nfc devices based on ambient sensor data. In *Computer Security–ESORICS 2012*, pages 379–396. Springer, 2012.

[18] M. A. Hall and G. Holmes. Benchmarking attribute selection techniques for discrete class data mining. *Knowledge and Data Engineering, IEEE Transactions on*, 15(6):1437–1447, 2003.

[19] G. Hancke and M. Kuhn. An RFID distance bounding protocol. In *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005.*, pages 67–73, 2005.

[20] B. Huang, M. Chen, P. Huang, and Y. Xu. Gait modeling for human identification. In *Robotics and Automation, 2007 IEEE International Conference on*, pages 4833–4838. IEEE, 2007.

[21] A. H. Johnston and G. M. Weiss. Smartwatch-based biometric gait recognition. In *Biometrics Theory, Applications and Systems (BTAS), 2015 IEEE 7th International Conference on*, pages 1–6. IEEE, 2015.

[22] N. Karapanos, C. Marforio, C. Soriente, and S. Capkun. Sound-proof: Usable two-factor authentication based on ambient sound. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 483–498, 2015.

[23] Y. S. Kim, B. S. Soh, and S.-G. Lee. A new wearable input device: Scurry. *Industrial Electronics, IEEE Transactions on*, 52(6):1490–1499, 2005.

[24] R. Kumar, V. V. Phoha, and A. Jain. Treadmill attack on gait-based authentication systems. In *Biometrics Theory, Applications and Systems (BTAS), 2015 IEEE 7th International Conference on*, pages 1–7. IEEE, 2015.

[25] R. Kumar, V. V. Phoha, and R. Raina. Authenticating users through their arm movement patterns. *arXiv preprint arXiv:1603.02211*, 2016.

[26] I. Lamiche, G. Bin, Y. Jing, Z. Yu, and A. Hadid. A continuous smartphone authentication method based on gait patterns and keystroke dynamics. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–14, 2018.

[27] D. Lane. Computing Pearson's r, 2003. http://cnx.org/contents/9zcGzDDu@4/Computing-Pearsons-r.

[28] M. Liu, M. Wang, J. Wang, and D. Li. Comparison of random forest, support vector machine and back propagation neural network for electronic tongue data classification: Application to the recognition of orange beverage and chinese vinegar. *Sensors and Actuators B: Chemical*, 177:970–980, 2013.

[29] Lookout. Phone Theft In America, 2014. https://www.lookout.com/resources/reports/phone-theft-in-america.

[30] J. Mäntyjärvi, M. Lindholm, E. Vildjiounaite, S.-M. Mäkelä, and H. Ailisto. Identifying users of portable devices from gait pattern with accelerometers. In *Acoustics, Speech, and Signal Processing, 2005. Proceedings.(ICASSP'05). IEEE International Conference on*, pages ii–973, 2005.

[31] S. Mare, A. M. Markham, C. Cornelius, R. Peterson, and D. Kotz. Zebra: zero-effort bilateral recurring authentication. In *2014 IEEE Symposium on Security and Privacy*, pages 705–720. IEEE, 2014.

[32] R. A. Maxion and K. S. Killourhy. Keystroke biometrics with number-pad input. In *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*, pages 201–210, 2010.

[33] Mercedes-Benz. Mercedes-Benz TechCenter: KEYLESS GO, 2016. http://techcenter.mercedes-benz.com/_en/keylessgo/detail.html.

[34] B. B. Mjaaland, P. Bours, and D. Gligoroski. Walk the walk: attacking gait biometrics by imitation. In *Information Security*, pages 361–380. Springer, 2010.

[35] T. Mogg. Study reveals americans lost $30 billion worth of mobile phones last year, 2012. http://www.digitaltrends.com/mobile/study-reveals-americans-lost-30-billion-of-mobile-phones-last-year.

[36] S. J. Morris. *A shoe-integrated sensor system for wireless gait analysis and real-time therapeutic feedback*. PhD thesis, Massachusetts Institute of Technology, 2004.

[37] T. Morris. Trusted platform module. In *Encyclopedia of cryptography and security*, pages 1332–1335. Springer, 2011.

[38] M. Muaaz and R. Mayrhofer. Orientation independent cell phone based gait authentication. In *Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia*, pages 161–164. ACM, 2014.

[39] M. Muaaz and R. Mayrhofer. Smartphone-based gait recognition: from authentication to imitation. *IEEE Transactions on Mobile Computing*, 16(11):3209–3221, 2017.

[40] J. K. Perng, B. Fisher, S. Hollar, and K. S. Pister. Acceleration sensing glove. In *iswc*, page 178. IEEE, 1999.

[41] planetbiometrics.com. Korean firm includes gait biometric on new wearable. Available online at http://www.planetbiometrics.com/article-details/i/2442/, 2014.

[42] J. Reid, J. M. G. Nieto, T. Tang, and B. Senadji. Detecting Relay Attacks with Timing-based Protocols. In *Proc. 2nd ACM symposium on Information, computer and communications security*, ASIACCS '07, pages 204–213, 2007.

[43] L. Rong, Z. Jianzhong, L. Ming, and H. Xiangfeng. A wearable acceleration sensor system for gait recognition. In *Industrial Electronics and Applications*, pages 2654–2659, 2007.

[44] M. Sama, V. Pacella, E. Farella, L. Benini, and B. Riccó. 3did: a low-power, low-cost hand motion capture device. In *Proceedings of the conference on Design, automation and test in Europe: Designers' forum*, pages 136–141. European Design and Automation Association, 2006.

[45] B. Shrestha, N. Saxena, H. T. T. Truong, and N. Asokan. Drone to the Rescue: Relay-Resilient Authentication using Ambient Multi-Sensing. In *Proc. Eighteenth International Conference on Financial Cryptography and Data Security*, 2014.

[46] T. Søndrol. Using the human gait for authentication. Master's thesis, Gjøvik University College, 2005. Available online at https://brage.bibsys.no/xmlui/bitstream/handle/11250/143801/S%C3%B8ndrol%20-%20Using%20the%20human%20gait%20for%20authentication.pdf.

[47] Ø. Stang. Gait analysis: Is it easy to learn to walk like someone else? Master's thesis, Gjøvik University College, 2007. Available online at https://brage.bibsys.no/xmlui/bitstream/handle/11250/143833/Stang%20-%20Gait%20analysis%20-%20Is%20it%20easy%20to%20learn%20to%20walk%20like%20someone%20else.pdf.

[48] D. Tapellini. Smart phone thefts rose to 3.1 million in 2013, 2014. http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.

[49] B. Tognazzini. The apple iwatch. Blog posting in AskTOG: Interaction Design Solutions for the Real World, Feb 2013. http://asktog.com/atc/apple-iwatch/.

[50] H. T. T. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi. Comparing and fusing different sensor modalities for relay attack resistance in Zero-Interaction Authentication. In *IEEE International Conference on Pervasive Computing and Communications, PerCom 2014*, 2014.

[51] L. USA. Lg nexus 5: Made for what matters — lg usa. Available online at http://www.lg.com/us/cell-phones/lg-D820-Black-nexus-5.

[52] L. USA. Lg watch r (w110): Design comes full circle — lg usa. Available online at http://www.lg.com/us/smart-watches/lg-W110-lg-watch-r.

[53] J. Van De Moosdijk and D. Visser. Car security: remote keyless "entry and go". 2009. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.182.5180&rep=rep1&type=pdf.

[54] E. Vildjiounaite, S.-M. Mäkelä, M. Lindholm, R. Riihimäki, V. Kyllönen, J. Mäntyjärvi, and H. Ailisto. Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices. In *Pervasive Computing*, pages 187–201. Springer, 2006.

[55] T. Yamamoto, M. Tsukamoto, and T. Yoshihisa. Foot-step input method for operating information devices while jogging. In *Applications and the Internet, 2008. SAINT 2008. International Symposium on*, pages 173–176. IEEE, 2008.

APPENDIX

A. *Best Sensors*

The sensors list according to number of times each sensor appeared on the best sensor subset for each individual is shown in Table IV. We noticed that phone magnetometer sensor appeared most often followed by phone Gyroscope and accelerometer, respectively. Hence, it seems position sensors such as magnetometer and gyroscope are more important in authenticating users via phone gait biometrics than motion sensors such as accelerometer. Among the sensors from watch, we noticed the watch accelerometer to be the most frequent in the best sensor subset.

TABLE IV
TOP 10 SENSORS RANKED ACCORDING TO NUMBER OF TIMES THEY APPEARED IN THE BEST SENSOR SUBSET FOR DIFFERENT INDIVIDUAL.

Sensors	**Count**
phoneMagnetometer	28
phoneGyroscope	26
phoneAccelerometer	25
watchAccelerometer	24
phoneGravity	18
watchMagnetometer	18
phoneRotVector	15
watchGRV	13
watchGyroscope	13
watchGravity	10