Drone to the Rescue: Relay-Resilient Authentication using Ambient Multi-Sensing

Babins Shrestha[1], Nitesh Saxena[1], Hien Thi Thu Truong[2], and N. Asokan[2,3]

[1] University of Alabama at Birmingham, USA
[2] University of Helsinki, Finland
[3] Aalto University, Finland

Abstract. Many mobile and wireless authentication systems are prone to relay attacks whereby two non co-presence colluding entities can subvert the authentication functionality by simply relaying the data between a legitimate prover ($\mathcal{P}$) and verifier ($\mathcal{V}$). Examples include payment systems involving NFC and RFID devices, and zero-interaction token-based authentication approaches. Utilizing the contextual information to determine $\mathcal{P}$-$\mathcal{V}$ proximity, or lack thereof, is a recently proposed approach to defend against relay attacks. Prior work considered WiFi, Bluetooth, GPS and Audio as different contextual modalities for the purpose of relay-resistant authentication.

In this paper, we explore *purely ambient physical sensing capabilities* to address the problem of relay attacks in authentication systems. Specifically, we consider the use of four new sensor modalities, *ambient temperature*, *precision gas*, *humidity*, and *altitude*, for $\mathcal{P}$-$\mathcal{V}$ proximity detection. Using an off-the-shelf ambient sensing platform, called *Sensordrone*, connected to Android devices, we show that *combining* these different modalities provides a robust proximity detection mechanism, yielding very low false positives (security against relay attacks) and very low false negatives (good usability). Such use of multiple ambient sensor modalities offers unique security advantages over traditional sensors (WiFi, Bluetooth, GPS or Audio) because it requires the attacker to *simultaneously* manipulate the multiple characteristics of the *physical* environment.

Keywords: relay attacks, proximity detection, environmental sensors

1 Introduction

Many mobile and wireless systems involve authentication of one communicating party (prover $\mathcal{P}$) to the other (verifier $\mathcal{V}$). Such authentication typically takes the form of a challenge-response mechanism whereby $\mathcal{V}$ proves the possession of the key K that it pre-shares with $\mathcal{P}$ by encrypting or authenticating a random challenge (using K) sent by $\mathcal{P}$. Example instances include payment transactions between NFC/RFID devices and point-of-sale systems, and zero-interaction authentication [4] scenarios between a token and a terminal (e.g., phone and laptop, or car key and car). Unfortunately, the security and usability benefits provided by these authentication systems can be relatively easily subverted by means of

different forms of relay attacks which involve two non co-present colluding attackers to simply relay the protocol messages back and forth between $\mathcal{P}$ and $\mathcal{V}$.

One scenario for such relay attacks [9,13,15] is applicable to zero-interaction authentication. Here, an attacker (ghost) relays the challenge from $\mathcal{V}$ to a colluding entity (leech). The leech then relays the received challenge to $\mathcal{P}$, and the response from $\mathcal{P}$ in the other direction. This way a ghost and leech pair can succeed in impersonating as $\mathcal{P}$. Another scenario relates to payment tokens and point-of-sale readers. It involves a malicious reader and an unsuspecting payment token owner intending to make a transaction [6, 8]. In this scenario, the malicious reader, serving the role of a leech and colluding with the ghost, can fool the owner of the payment token $\mathcal{P}$ into approving to $\mathcal{V}$ a transaction which she did not intend to make (e.g., paying for a diamond purchase made by the adversary in a jewellery store while the owner only intends to pay for food at a restaurant). The main difference in the two scenarios relates to user awareness – in the first scenario, the user does not intend to authenticate at all, whereas, in the second scenario, the user does intend to authenticate but ends up authorizing a different transaction than the one she intends to.

A known defense to relay attacks, commonly found in research literature, is the use of distance bounding protocols. A distance bounding protocol is a cryptographic challenge-response authentication protocol which allows the verifier to measure an upper-bound of its distance from the prover [1]. Using this protocol, $\mathcal{V}$ can verify whether $\mathcal{P}$ is within a close proximity thereby detecting both terrorist fraud and mafia fraud attacks. [8,9]. However, these protocols may not be currently feasible on commodity devices (such as NFC phones, car keys, payment tokens) due to their high sensitivity to time delay or need for special-purpose hardware.

Recent research suggests a potentially more viable defense to relay attacks, capitalizing upon the emerging sensing capabilities of modern devices ($\mathcal{P}$ and $\mathcal{V}$) [10, 11, 18, 29]. The idea is to use the on-board device sensors to extract contextual information based on which $\mathcal{P}$-$\mathcal{V}$ proximity, or lack thereof, could be determined. Prior work demonstrated the promising feasibility of using different types of sensors for this purpose, including WiFi [29], GPS [10], and Audio [11].

In this paper, we explore **purely ambient physical sensing** capabilities present on upcoming devices to address the problem of relay attacks in authentication systems. More specifically, we consider the use of four new sensor modalities, *ambient temperature*, *precision gas*, *humidity*, and *altitude*, for $\mathcal{P}$-$\mathcal{V}$ proximity detection. Using an off-the-shelf ambient sensing platform, called Sensordrone[4], connected to Android devices, we show that combining these different modalities provides a robust proximity detection mechanism, yielding very low false positives (security against relay attacks) and very low false negatives (good usability). Such use of multiple ambient sensor modalities offers unique security advantages over traditional sensors (WiFi, GPS, Bluetooth or Audio) because it requires the attacker to simultaneously manipulate the multiple characteristics

[4] `http://www.sensorcon.com/sensordrone/`

of the physical environment. These ambient sensors also yield rapid response times and very low battery consumption, whereas traditional sensors can have noticeable scanning times and battery drainage. These ambient sensors may also be seamlessly combined to work with traditional sensors to further improve security.

To demonstrate the feasibility of our approach, we use an additional environmental sensing platform (Sensordrone). However, the devices participating in the protocol themselves ($\mathcal{P}$ and $\mathcal{V}$) may be equipped with various environmental sensors in the future [3, 32]. Android platform already supports broad category of environmental sensors that includes barometer, photometer and thermometer [17] such that phones and other devices that come equipped with these sensors will already have an interface to provide data to corresponding application.

Our Contributions: The main contributions of this paper are as follows:

- *Environmental Sensors for Relay Attack Prevention:* We present the first exploration of the use of purely environmental sensors for relay attack prevention in mobile and wireless systems. Given that these sensors are already available on many smartphones in the form of extension devices [26], our work shows how such sensors can be effectively leveraged for relay attack security once they become commonplace in the near future (either in embedded or extension form).
- *Experiments and Multiple Modality Combinations:* We design a simple data collection application, utilizing Sensordrone, that allows us to collect the data at different locations and demonstrate the feasibility of our approach with four different sensor modalities and off-the-shelf classifiers. We report on several experiments to evaluate our approach. Our results suggest that although each individual sensor modality may not provide a sufficient level of security and usability for the targeted applications, multiple modality combinations result in a robust relay attack defense (low false positives) as well as good usability (low false negatives).

2 Related Work

The main idea of zero interaction authentication is that legitimate entities, i.e. $\mathcal{P}$ and $\mathcal{V}$, should be in physical proximity at the authentication moment. There are some examples of the system such as card/mobile payment system, dual factors authentication e.g. PhoneAuth [5] or zero interaction authentication to lock/unlock terminal e.g. BlueProximity.[5]

Distance bounding techniques [1] that were proposed as a solution to relay attack have some limitations mentioned in previous works such as its difficulty to deploy on commodity devices [11] and its dependence on low-level implementation which is vulnerable to attackers [10, 14]. An alternative solution using ambient environment has been investigated recently. This is based on the assumption that $\mathcal{P}$ and $\mathcal{V}$ will have similar ambient environment when they are

[5] `http://sourceforge.net/projects/blueproximity/`

co-present whereas they will see significant differences in their respective ambient environments when they are not co-present. Some prior works rely on commodity devices which are equipped with various traditional sensors such as WiFi, Bluetooth, and sound microphones.

Radio Frequency (RF) sensing (WiFi, Bluetooth etc.) is a commonly used sensor modality for co-presence detection. For example, Varashavsky et al. [29] proposed the use of the common radio environment (WiFi) as a basis to deriving shared secret between co-located devices. They introduced an algorithm Amigo that extends the Diffie-Hellman key exchange with verification of co-present devices. Each device generates a signature based on sensed radio environment data after performing a Diffie-Hellman key exchange and shares it with the other device for proximity verification. Krumm et al. [16] proposed "NearMe" that uses WiFi for proximity detection. GPS is also a radio-based sensor used for location detection.

Halevi et al. [11] developed techniques using ambient audio and light for proximity detection. They analyzed different methods such as time-based, frequency-based and time-frequency based similarity detection using raw audio data. Their results show that ambient sound is slightly better than ambient light. Other audio based context sensing approaches include [20, 24]. Nguyen et al. in [19] used pattern based audio alignment to detect and compare ambient audio to provide secure communication between mobile phones. Schurmann and Sigg [24] also presented secure communication based on ambient audio.

A solution based on sensing the purely physical environment holds the promise of being fast and energy-efficient. Narayanan et al. [18] mention the possibility of using some physical environmental sensors but do not report any concrete experiments or techniques.

3 Background and Overview

In this section, we review the proximity-based authentication approach that forms the focus of this paper and the underlying threat model, followed by an overview of our relay attack defense based on ambient multi-sensing.

3.1 Functional Model for Proximity-based Authentication

Figure 1 shows a general model of proximity-based authentication. The model consists of a prover $\mathcal{P}$ who wants to authenticate itself to verifier $\mathcal{V}$ and convince $\mathcal{V}$ that it is close to $\mathcal{P}$. The authentication process between $\mathcal{P}$ and $\mathcal{V}$ is typically run when they are in close proximity to each other. $\mathcal{V}$ makes use of a back-end "comparator" function to make the authentication decision (it could reside on the verifier device or on a remote machine such as a bank server in the case of payment transactions). $\mathcal{P}$ and $\mathcal{V}$ have pre-shared secret keys K and K', respectively, with the comparator. In an authentication session, $\mathcal{V}$ sends a *challenge* to $\mathcal{P}$ which computes a *response* based on the *challenge* and K.

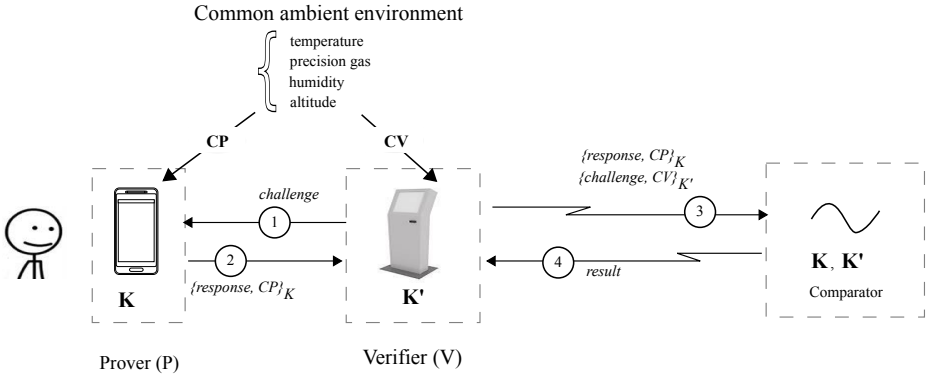

Fig. 1. A functional model of proximity based authentication.

$\mathcal{P}$ returns the *response* to $\mathcal{V}$ which uses the comparator function to decide if *response* is acceptable.

This functional model is applicable to various real-world scenarios such as payment at a point-of-sale (POS) terminal and zero interaction authentication (ZIA) for access control to locking/unlocking a car or a desktop computer. In the payment scenario, the payment card plays the role of $\mathcal{P}$, and the POS terminal plays the role of $\mathcal{V}$. The issuer of the payment card plays the role of the comparator. In ZIA the user token (key or mobile phone) acts as $\mathcal{P}$ and the terminal (car or desktop computer) plays the role of $\mathcal{V}$. The comparator functionality is integrated in the terminal itself and therefore K' is not needed.

3.2 Threat Model

We assume a standard Dolev-Yao adversary model [7] where the adversary $\mathcal{A}$ has complete control over all communication channels. However, $\mathcal{A}$ is not able to compromise $\mathcal{P}$, $\mathcal{V}$ or the comparator, i.e., none of the legitimate entities involved in the protocol have been tampered with or compromised. The goal of $\mathcal{A}$ is to carry out relay attack by convincing $\mathcal{V}$ that the $\mathcal{P}$ is nearby when in fact $\mathcal{P}$ is far away. Figure 2 shows how $\mathcal{A}$, in the form of a relay-attack duo ($\mathcal{A}_p$,$\mathcal{A}_v$) can relay messages between the legitimate $\mathcal{P}$ and $\mathcal{V}$ with $\mathcal{A}_p$ acting as a dishonest verifier and $\mathcal{A}_v$ acting as a dishonest prover.

3.3 Our Approach: Relay Attack Defense with Ambient Multi-Sensing

Figure 1 shows our countermeasure against relay attack which is based on the natural assumption that two entities will sense similar ambient environments when they are co-present. When $\mathcal{P}$ sends an authentication trigger to $\mathcal{V}$, they both start sensing their respective contexts using ambient physical sensor modalities, resulting in CP and CV, respectively, as the sensed data. This sensor data may be acquired using an additional (uncompromised) device, connected over a secure channel, to $\mathcal{P}$ and $\mathcal{V}$ (such as Sensordrone) or via the sensors embedded within $\mathcal{P}$ and $\mathcal{V}$. We consider physical ambient sensor modalities, such

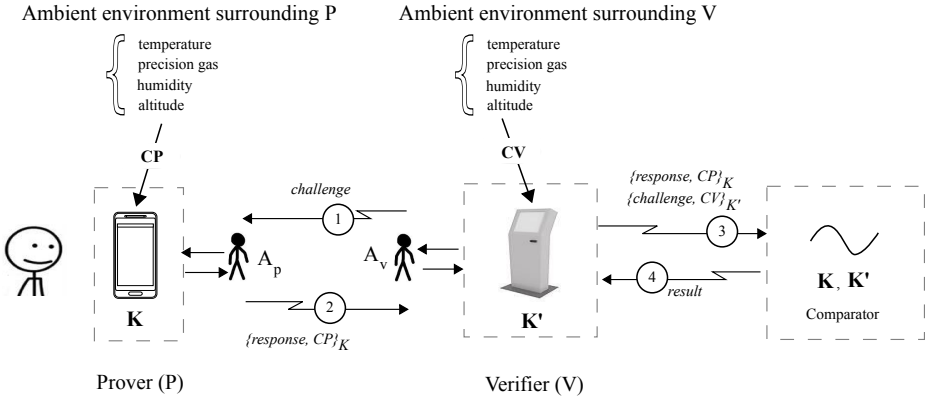

Fig. 2. Relay attack in proximity based authentication.

as *temperature*, *precision gas*, *humidity* and *altitude*. $\mathcal{P}$ will attach CP to *response*. Similarly $\mathcal{V}$ will convey CV along with *challenge* in its message to the comparator. In case multiple sensors are used (say n), CP would be the vector $CP_1, CP_2, ..., CP_n$, and similarly, CV would be the vector $CV_1, CV_2, ..., CV_n$.

Using the keys K, K', the comparator can recover and validate CP and CV, and compare them (in addition checking that *response* matches *challenge*). We recall that in scenarios where the comparator is integrated with $\mathcal{V}$, K' is not used.

Figure 2 illustrates the presence of the relay attack duo $\mathcal{A}$ =($\mathcal{A}_p$,$\mathcal{A}_v$). Assuming that $\mathcal{A}$ cannot subvert the integrity of context sensing and the comparator can reliably tell the difference between co-presence and non co-presence by examining CP and CV, our countermeasure based on context sensing will thwart a Dolev-Yao $\mathcal{A}$. In the rest of this paper, we describe our experiments to evaluate whether a comparator can reliably distinguish co-presence and non co-presence based on context information CP and CV sensed using physical ambient sensors.

4 Sensor Modalities

We explore the use of various ambient sensor modalities to determine whether two devices are co-present or not. In this paper, we are focusing on ambient temperature, precision gas, humidity and altitude, and combinations thereof, which are readily provided by Sensordrone (see Figure 3). In this section, we describe the functioning details of these sensors.

Ambient temperature: It is the temperature in a given localized surrounding. Ambient temperature of different locations might be different as it changes with sensor being indoors or outdoors, and differs from one room to another with Air Conditioning adjusted at different levels. We recorded the current temperature, in Celsius scale, at different locations. Sensordrone uses silicon bandgap sensor to record the ambient temperature. The principle of the bandgap sensor is that the forward voltage of a silicon diode is temperature-dependent [31].

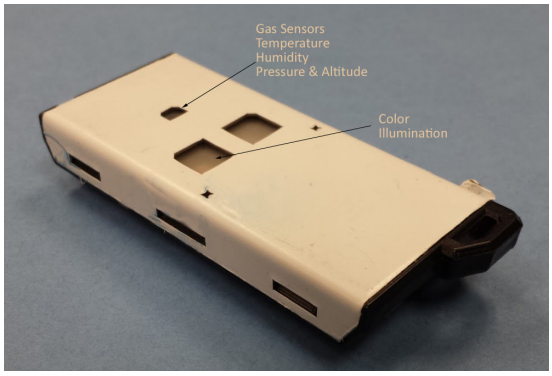

Fig. 3. Sensordrone device with different sensors (ambient temperature, precision gas, humidity and altitude are utilized in this paper). Device dimensions: 2.67 x 1.10 x 0.49 inch^3.

Humidity: It is the amount of moisture in the air which is used to indicate the likelihood of precipitation or fog. Humidity can serve as the contextual information about the location since the amount of water vapor present in the environment may differ when moving from one location to the other. Capacitive Polymeric Sensor is used to detect the humidity of the surrounding. It consists of a substrate (glass, ceramic or silicon) on which a thin film of polymer or metal oxide is deposited between two conductive electrodes. The change in the dielectric constant of a capacitive humidity sensor is nearly directly proportional to the relative humidity of the surrounding environment [22].

Precision Gas: Ambient air consists of various gases, primarily Nitrogen and Oxygen. The gaseous content of a particular location may differ from that of another location. The Sensordrone device comes with pre-calibrated Carbon Monoxide (CO) sensor, which measures the CO content of the atmosphere. We used the default calibration of the device that monitors CO to get the context information of the location. The values were measured in "ppm (parts per million)".

Altitude and Pressure: Atmospheric Pressure of a particular location is the pressure caused by the weight of air at that location above the measurement point. With increase or decrease in elevation, the weight of air above the location changes and so does the pressure at that location. Although the variation of pressure can be obtained from the altitude, it changes drastically with the weather. Hence, pressure at a location can serve as an indicator for that location and time. In our experiments, the pressure was recorded in "mmHg (millimeter of Mercury)" using Micro electromechanical (MEMS) Pressure Sensor. When there is a change in pressure from the air on a diaphragm within the sensor, the piezoresistive sensors senses the change with alternating piezoelectric current which is used to determine the actual pressure.

This is also used to determine the altitude. Since the pressure value at any given location is directly proportional to the amount of gases above the device and the amount of gases above the device is inversely proportional to the altitude, the altitude value can be derived from the pressure sensor using the equations 1. The units for station pressure must be converted to millibars (mb) or hectopascals (hPa) before using following expression to convert the pressure values into altitude [21].

$$h_{altitude} = \{1 - (\frac{P_{station}}{1013.25})^{0.190284}\} * 145366.45 \quad (1)$$

The $h_{altitude}$ measurements are in feet, and are multiplied by 0.3048 to convert them to meters.

Although Sensordrone provides both pressure and altitude readings, we only use altitude to classify the location as altitude is derived from pressure. We found that as the readings are taken at a more precise scale, the classifiers result improves. In our dataset, we measured pressure in *mmHg* and altitude in *m*. The pressure values did not vary much and were not very useful in providing accuracy to the classifier while altitude provided a clear difference between two locations allowing classifier to more accurately make predictions.

Excluded Sensors: Although there are other sensors available on the Sensordrone device, we did not use the data from those sensors for two reasons: either they did not convey information about the ambient context or may not work when blocked. The sensors excluded from our experiments include:

Object Temperature: This sensor uses Infrared to obtain the temperature of a nearby object (line of sight object temperature). The application of this sensor includes measuring the temperature of coffee cup or that of an oven. This measures the information about a specific object but not about the ambient environment.

Recently, Urien and Piramuthu [28] proposed the use of such an object temperature sensor to defend against relay attacks. In their approach, surface temperature of the prover measured by the prover and the verifier is used complementary to distance-based validation measured by round-trip times. This is an interesting idea complementary to our approach, which may be used to combine device-specific physical characteristics with environment-specific characteristics.

Illuminance (Light): Ambient light intensity might seem like a useful modality to convey the environmental information. Given the fact that light sensors are already present in most of the current smartphones and tablets, this is an appealing capability to obtain the environment information. In fact, this attribute was investigated by Halevi et al. in [11], who claimed that it can provide reasonably robust way of proximity detection. However, its use suffers from the fact that light intensity greatly varies depending upon the position of the source of light and the light sensor facing towards it. Also, the devices will not provide light measurements when their sensors are blocked, such as when the devices are stowed inside purses or backpacks.

Proximity Capacitance and External Voltage: The proximity capacitance sensor is basically for touch sensing or proximity detection like when used on touch pads or capacitive touch screens. The device detects changes in capacitive flux if there is a material within a close proximity of the sensor. The sensor is capable of estimating distances to an object as well as detecting minute changes in water content of the material [25]. The external voltage sensor gives the measure of a battery voltage level. None of these sensors reflect the ambient context and, hence, are not useful for our purpose.

5 Experiments and Results

We developed a simple prototype for Android devices to evaluate our $\mathcal{P}$-$\mathcal{V}$ co-presence detection approach using different ambient sensor modalities. We collected data from different locations. We used two Sensordrone devices along with two android phones (Samsung Galaxy Nexus and Samsung Galaxy S IV) to collect the data. Sensordrone sends the sensor readings to phone via Bluetooth. The phone is just a user interface (UI) for the Sensordrone device (the UI shown in Figure 4) and does not play any role in altering the sensor values. Our app on the phone records the Sensordrone readings to a file for further analysis.

5.1 Data Collection

The main goal here is to identify if two devices are co-present or not using the sensor data. We collect the data from two devices and use a classifier to determine if these devices are at the same location or at different locations. For this, we needed to collect the sensor data when the devices are in close physical proximity as well as when they are at different locations.

To collect the sensor data described in Section 4, we modified the original app provided in [23] to *record* the data to a file for further analysis (UI is shown in figure 5). The data from all the sensors used in our experiments (ambient temperature, precision gas, humidity, and altitude) was recorded and labeled according to the location and time of the place. The data was also marked how the device was held, i.e, either in hand or in pocket (although this information was not used in our current experiments; it can be useful when working with the light sensor in the future). The experiment was conducted in a variety of places, not just confined to labs and typical university offices. The locations included: parking lots, office premises, restaurants, chemistry labs, libraries as well as halls with live performance and driving on interstate highways. We collected a total of 207 samples at 21 different locations. The different samples collected from the same place are "paired" to generate co-presence data instances whereas those from different places are paired to generate non-copresence data instances. We ended up with 21320 instances of which 20134 instances belonging to non co-presence class and 1186 instances belonging to co-presence class.

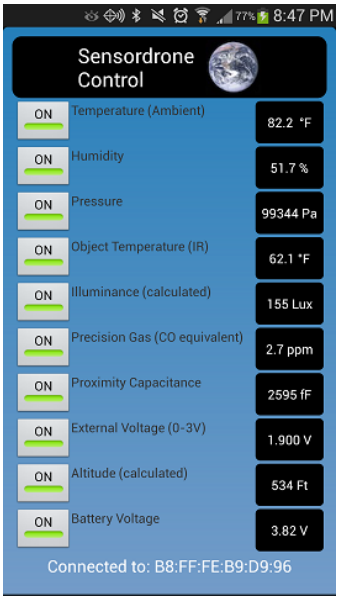

Fig. 4. Original Sensordrone app displaying sensor values

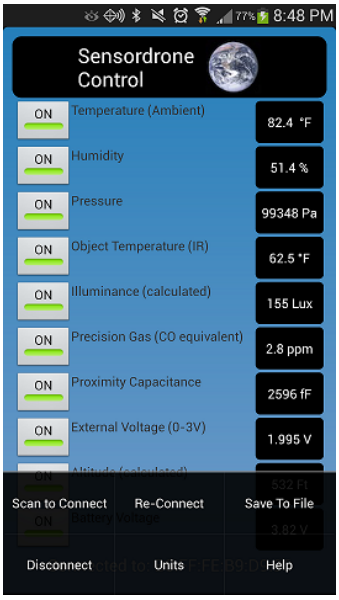

Fig. 5. Modified Sensordrone app to record the sensor values

5.2 Feature Calculation and Analysis Methodology

Let L_i and L_j be a sensor reading captured by two devices at locations i and j. The Hamming distance is calculated as follows:

$$D(i,j) = |L_i - L_j| \tag{2}$$

Given a sensor modality k (k is in range of (1, n) where n is the number of sensor modalities) and $L_i^{(k)}$ and $L_j^{(k)}$ from two samples, we have $D^{(k)}(i,j) = |L_i^{(k)} - L_j^{(k)}|$. With the data corresponding to n modalities, we obtain a feature vector of n elements of $D^{(k)}(i,j) \mid 1 \leq k \leq n$.

We consider co-presence detection as a classification task and carry out our investigation using the Weka data mining tool [12]. All experiments have been performed using ten-fold cross validation and Multiboost [30] as the classifier. We choose Random Forest [2] as the weak learners in all experiments since it performs best among different base learners we have tried with our dataset (e.g., Simple Logistics, J48, and Random Forest). From each experiment, we record the 2x2 confusion matrix, containing the number of True Positives (TP), True Negatives (TN), False Positives (FP) and False Negatives (FN). We denote co-presence class to be the positive class, and non co-presence to be the negative class.

We use the *F-measure* (Fm), false negative rate (FNR), and false positive rate (FPR) to measure the overall classification performance (equations 3, 4, 5).

$$Fm = 2 * \frac{precision * recall}{precision + recall}, \tag{3}$$

$$precision = \frac{TP}{TP + FP}, \ recall = \frac{TP}{TP + FN} \tag{4}$$

$$FNR = \frac{FN}{FN + TP}, \ FPR = \frac{FP}{FP + TN} \tag{5}$$

Classifiers produce reliable results when the data is balanced over all classes. Our dataset is highly biased towards the non co-presence class which is 17 times larger than the co-presence class. Therefore, we generate balanced data for classification by randomly partitioning the non co-presence class into 17 subsets. Each such subset together with the co-presence class constitutes a resampled set for classification. We run experiments with 10 resampled sets, chosen randomly.

Each of the different sensors alone may not be fully effective for the purpose of co-presence detection, and therefore, we also explore whether combinations of different sensors improve the classification accuracy. To analyze which combination provides the best result, we would need to analyze all 15 different combinations of four different sensors. However, to reduce the underlying computations, we first analyze the accuracy provided by each individual sensor. Then we combine best two modalities and view how the accuracy of the classifier changes. We keep on adding the modalities to see the change in the accuracy until all the modalities are fed into the classifier for co-presence detection.

5.3 Results

The results of experiments for different combinations of modalities are provided in Table 1. They suggest that, although each individual modality on its own does not perform sufficiently well for the purpose of co-presence detection, combinations of modalities, especially combining all the modalities together, is quite effective, with very low FNR and FPR, and high overall Fm. Altitude performs the best in classifying single modality, and also ranked the best by Chi-squared attribute evaluation but still has unacceptable FNR and FPR ($FNR = 8.57\%$, $FPR = 16.25\%$, $Fm = 0.881$) for our targeted applications demanding high usability and high security. The result of the combination of all modalities is clearly the best ($FNR = 2.96\%$, $FPR = 5.81\%$, $Fm = 0.957$. The intermediary combinations of different modalities used in experiments are also based on the ranks of each modality (evaluated by Chi-squared test). The results for the best combinations, Humidity-Altitude and Humidity-Gas-Altitude, are also presented in Table 1.

6 Discussion

Having demonstrated the feasibility of our approach to relay attack prevention, we now provide a discussion of several other key aspects relevant to our proposal.

Table 1. Classification results for different combinations of environmental sensors

	FNR(%)	FPR(%)	Precision	Recall	Fm
Single sensor modality					
Temperature (T)	23.74	32.40	0.705	0.763	0.733
Precision Gas (G)	15.26	30.36	0.739	0.847	0.790
Humidity (H)	16.25	29.81	0.740	0.838	0.786
Altitude (A)	8.57	16.25	0.851	0.914	0.881
Combination of multiple sensor modalities					
HA	7.93	9.85	0.905	0.921	0.913
HGA	5.30	6.83	0.934	0.947	0.940
THGA	2.96	5.81	0.944	0.970	0.957

6.1 Response Time

The response time of our approach based on environmental sensors is negligible as we require only one sample for each sensor which can be instantaneously polled at the time of authentication. As such, the approach would not incur any delay by incorporating the contextual sensor data into the authentication process for proximity detection. This is one of the key advantages of our scheme over the use of traditional sensors, such as WiFi, GPS, and Bluetooth, which need considerable time to scan the context [27].

6.2 Battery Power Consumption

All the sensors we have used are low-power sensors, and are turned on all the time in the Sensordrone device. Enabling these sensors data stream will have minimal influence on the power consumption [25]. The Gas Sensors comes with pre-calibrated for Carbon Monoxide (CO), which is what we used in our experiments. Enabling the CO data stream will have minimal influence on power consumption while enabling other gas sensors may use a lot of power.

6.3 Adversarial Settings

The modalities used in this paper are purely environmental (i.e., they directly measure the natural environmental characteristics). Therefore, it might be very difficult for an adversary to manipulate these modalities so as to bypass the proximity detection mechanism. It may be challenging to change the outside temperature but adversary may change the room temperature using Air Conditioning or heater. To change the humidity, adversary needs to change the moisture content of the environment. This could also be hard to achieve when devices are outside. Although, the adversary can change the humidity of the

room, he still needs to control it such a way that both devices get the reading within a threshold. The attack assertions might be similar for pressure, altitude and precision gas modalities. An adversary may have to fill up the room with heavier or lighter gases inside a room to change the pressure/altitude readings while he can fill up room with the gas used for measurement (Carbon monoxide in our experiment) to alter the precision gas reading.

Since we are using more than one modality in our approach (ideally all, when available), changing only one of the modality is not going to work for an adversary. The adversary needs to change multiple modalities simultaneously for successful attack. This could present a significant challenge for the adversary. As the number of modalities to be altered by an adversary is increased, the likelihood of being noticed by the users also increases.

6.4 Privacy

In settings where a third-party comparator (such as a bank server) is used for making approval decisions, a natural concern is about the privacy of the user, such as location privacy. The information provided should not be specific enough to reveal the user's exact location while it should be precise enough to verify that he is in close proximity with other device to which it is compared to. The other approaches that have been studied to prevent relay attack use either artificial (WiFi [16, 18], GPS, Bluetooth) or semi-natural (audio [11, 20, 24]) modalities. Such modalities, when analyzed, can reveal the location of a user compromising the privacy of the user. For example, a user when connected to the WiFi hotspot/ Bluetooth devices of clinic or a club will provide the information that he is connected to the WiFi/Bluetooth devices of that area. Even an audio sample of few seconds can reveal the location if a user is in a concert or in a class attending a lecture. Audio snippets (although short) may also reveal the conversations a user might be having at the time of authentication.

In contrast to traditional sensors, environmental modalities may not reveal such potentially sensitive information about the users unless the user is at specific locations with unique and fixed environmental characteristics, such as being at the top of Mt. Everest where the altitude is 8848m. Even revealing multiple modalities to the remote server may not reveal much information about the user's location or user's conversations. Further work is needed to ascertain the level of privacy environmental sensors can provide.

6.5 Other Sensors

We demonstrated the feasibility of using four different modalities to provide the ambient information about the location. However, the set of modalities is not limited to ones we explored. It is also possible to incorporate other sensor types, such as odor sensors, to provide the environment information while not revealing the user's exact location. The modalities that we used in our experiment are all environmental whilst it is also possible to use them in conjunction with artificial modalities such as WiFi, Bluetooth, GPS, and Audio [27].

7 Conclusions

In this paper, we developed a co-presence detection approach based on information collected from multiple different environmental sensors. This approach is geared for preventing relay attacks, a significant threat to many proximity-based authentication systems. While each individual sensor does not seem sufficient for the security and usability requirements of the targeted applications, their combinations form a robust relay attack defense. The other key advantages of our approach include: security (manipulating multiple environmental attributes simultaneously could be a challenging task for the attacker), efficiency (fast response time and negligible power drainage), and privacy (user-specific sensitive information may not be leaked or may be hard to infer).

Acknowledgments

This work was partially supported by a Google Faculty Research Award, and a US NSF grant (CNS-1201927). We thank the FC'14 anonymous reviewers for their useful feedback.

References

1. S. Brands and D. Chaum. Distance-bounding protocols. In *Advances in Cryptology - EUROCRYPT, International Conference on the Theory and Applications of Cryptographic Techniques*, 1993.
2. L. Breiman. Random forests. *Mach. Learn.*, 45(1):5–32, Oct. 2001.
3. P. Clarke. Sensirion preps multi-gas sensor 'nose' for smartphones. Available online at `http://www.electronics-eetimes.com/en/sensirion-preps-multi-gas-sensor-nose-for-smartphones.html?cmp_id=7&news_id=222919117`.
4. M. D. Corner and B. D. Noble. Zero-interaction authentication. In *Proceedings of 8th annual international conference on Mobile computing and networking*, MobiCom'02, pages 1–11, New York, NY, USA, 2002. ACM.
5. A. Czeskis, M. Dietz, T. Kohno, D. Wallach, and D. Balfanz. Strengthening user authentication through opportunistic cryptographic identity assertions. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, pages 404–414, New York, NY, USA, 2012. ACM.
6. Y. Desmedt, C. Goutier, and S. Bengio. Special uses and abuses of the fiat-shamir passport protocol. In *A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology (CRYPTO)*, 1988.
7. D. Dolev and A. C.-C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–207, 1983.
8. S. Drimer and S. J. Murdoch. Keep your enemies close: Distance bounding against smartcard relay attacks. In *16th USENIX Security Symposium*, August 2007.
9. A. Francillon, B. Danev, and S. Capkun. Relay attacks on passive keyless entry and start systems in modern cars. Cryptology ePrint Archive, Report 2010/332, 2010. `http://eprint.iacr.org/`.

10. L. Francis, G. Hancke, K. Mayes, and K. Markantonakis. Practical nfc peer-to-peer relay attack using mobile phones. In *Proceedings of the 6th international conference on Radio frequency identification: security and privacy issues*, RFIDSec'10, pages 35–49, Berlin, Heidelberg, 2010. Springer-Verlag.
11. T. Halevi, D. Ma, N. Saxena, and T. Xiang. Secure proximity detection for NFC devices based on ambient sensor data. In *Proceedings of 17th European Symposium on Research in Computer Security, ESORICS 2012*, pages 379–396, 2012.
12. M. Hall et al. The weka data mining software: an update. *SIGKDD Explor. Newsl.*, 11(1):10–18, Nov. 2009.
13. G. Hancke. Practical attacks on proximity identification systems (short paper). In *IEEE Symposium on Security and Privacy*, 2006.
14. G. P. Hancke and M. G. Kuhn. Attacks on time-of-flight distance bounding channels. In *Proceedings of the first ACM conference on Wireless network security*, WiSec '08, pages 194–202, New York, NY, USA, 2008. ACM.
15. Z. Kfir and A. Wool. Picking virtual pockets using relay attacks on contactless smartcard. In *Security and Privacy for Emerging Areas in Communications Networks (Securecomm)*, 2005.
16. J. Krumm and K. Hinckley. The nearme wireless proximity server. In *UbiComp 2004: Ubiquitous Computing*, pages 283–300. Springer, 2004.
17. R. Meier. *Professional Android 4 application development.* John Wiley & Sons, 2012.
18. A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh. Location privacy via private proximity testing. In *Proceedings of the Network and Distributed System Security Symposium, NDSS*, 2011.
19. N. Nguyen, S. Sigg, A. Huynh, and Y. Ji. Pattern-based alignment of audio data for ad hoc secure device pairing. In *16th International Symposium on Wearable Computers, ISWC*, pages 88–91. IEEE, 2012.
20. N. Nguyen, S. Sigg, A. Huynh, and Y. Ji. Using ambient audio in secure mobile phone communication. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*, pages 431–434. IEEE, 2012.
21. N. Oceanic and A. Association. Pressure altitude. Available online at `http://www.wrh.noaa.gov/slc/projects/wxcalc/formulas/pressureAltitude.pdf`.
22. D. K. Roveti. Choosing a humidity sensor: A review of three technologies this discussion of the operating principles of capacitive, resisitive, and thermal conductivity humidity sensors also addresses their advantages, disadvantages, and applications. *Sensors-the Journal of Applied Sensing Technology*, 18(7):54–58, 2001.
23. M. Rudolph. Sensordrone-control. Available online at `https://github.com/Sensorcon/Sensordrone-Control`, March 2013.
24. D. Schurmann and S. Sigg. Secure communication based on ambient audio. *IEEE Transactions on Mobile Computing*, 12(2):358–370, 2013.
25. Sensordrone. Sensorcon: Sensordrone, preliminary specifications, rev. d : Specifications & user guide. Available online at `http://developer.sensordrone.com/forum/download/file.php?id=10`, November 2012.
26. M. Treacy. 10 environmental sensors that go along with you. Available online athttp://www.treehugger.com/clean-technology/environmental-sensors.html, February 2009.
27. 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.

28. P. Urien and S. Piramuthu. Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks. *Decision Support Systems*, (0):–, 2013.
29. A. Varshavsky, A. Scannell, A. LaMarca, and E. de Lara. Amigo: Proximity-based authentication of mobile devices. In *Proceedings of the 9th International Conference on Ubiquitous Computing (UbiComp)*, pages 253–270. Springer, 2007.
30. G. I. Webb. Multiboosting: A technique for combining boosting and wagging. *Mach. Learn.*, 40(2):159–196, Aug. 2000.
31. R. Widlar. An exact expression for the thermal variation of the emitter base voltage of bi-polar transistors. *Proceedings of the IEEE*, 55(1):96–97, 1967.
32. S. Yurish. Smartphone sensing: What sensors would we like to have in the future smartphones? Available online at `http://www.iaria.org/conferences2012/filesSENSORDEVICES12/Yurish_Smartphone_Sensing.pdf`.