Hindawi
Journal of Advanced Transportation
Volume 2018, Article ID 1935974, 13 pages
https://doi.org/10.1155/2018/1935974

Research Article

Sound-Proximity: 2-Factor Authentication against Relay Attack on Passive Keyless Entry and Start System

Wonsuk Choi, Minhye Seo, and Dong Hoon Lee

Graduate School of Information Security, Korea University, Seoul, Republic of Korea

Correspondence should be addressed to Dong Hoon Lee; donghlee@korea.ac.kr

Received 28 June 2017; Accepted 7 December 2017; Published 31 January 2018

Academic Editor: Emanuele Crisostomi

Passive keyless entry and start system has been widely used in modern cars. Car owners can open the door or start the engine merely by having the key in their pocket. PKES was originally designed to establish a communication channel between the car and its key within approximately one meter. However, the channel is vulnerable to relay attacks by which attackers unlock the door even if the key is out of range. Even though relay attacks have been recognized as a potential threat for over ten years, such attacks were thought to be impractical due to highly expensive equipment; however, the required cost is gradually practical. Recently, a relay attack has been demonstrated with equipment being sold only under $100. In this paper, we propose a sound-based proximity-detection method to prevent relay attacks on PKES systems. The sound is eligible to be applied to PKES because audio systems are commonly available in cars. We evaluate our method, considering environments where cars are commonly parked, and present the recording time satisfying both usability and security. In addition, we newly define an advanced attack, called the record-and-playback attack, for sound-based proximity detection, demonstrating that our method is robust to such an attack.

1. Introduction

Passive key entry and start (PKES) system is a service that aims to provide car owners with convenience. In a traditional way, they insert their keys directly in order to open car doors and start the engine. Accordingly, keys must be removed from pockets and bags before using their car. The PKES system allows them to unlock and start engine without needing to remove the key from their pocket or bag. This implies that they do not have to locate their key while standing in front of their car. PKES was first introduced by Mercedes-Benz in 1998 [1]. Since then, car manufacturers have been applying the system in modern cars. In PKES, cars communicate with the corresponding key only when they are in proximity, using a short-range channel. In other words, cars communicate with their paired key only if the car owner with the key is close to the car. Then, cars verify the key over the established communication channel. Because car and its key share a secret value for authentication, keys without the secret value are not authenticated correctly, even when they are in close proximity to the car. Despite the convenience of PKES, its vulnerability has been recently discovered [2, 3], which is our motivation to construct a new method.

In various areas, researchers have studied relay-attack-resilient proximity-verification methods using either a distance-bounding protocol or context-based method [4–15]. Unfortunately, however, these existing methods have each limitation to be applied into PKES. A distance-bounding protocol measures distance based on received signal strength indicator (RSSI), ultrasonic sound, or radio frequency (RF) signal. These factors are inappropriate to be used for proximity verification in PKES. The RSSI-based or ultrasonic-sound-based method are vulnerable to attacks where the "verifier" (i.e., the car) is deceived into thinking that even a distant "prover" (i.e., the key) is nearby, by amplifying or relaying signals [8, 16]. The RF-based method is unsuitable for PKES (since radio waves move at the speed of light, the variation of processing time causes measurement error a lot), because the processing time of the prover should be invariant [8]. Context-based proximity-detection methods depend on two types of contextual information: wireless signals (e.g., Bluetooth and

Wi-Fi) and environmental signals (e.g., light and ambient sound). Because cars are often in environment where wireless signal is rare, it is inappropriate to use the wireless signal as contextual information. Moreover, it is difficult to exploit the similarity in light between the car and a key, because keys are often in a bag or a pocket. However, sound exists anywhere, and even in silence cars can make sounds easily since they already have a buzzer. And a key can record similar sounds to a car even when it is in a bag or pocket. Recently, there have been several services using sounds to detect proximity to user's smartphone [17, 18].

In this paper, we propose a sound-based proximity-detection method to prevent relay attacks on PKES. In addition, we newly define an adversary model for sound-based proximity verification, which is called record-and-playback attack. We evaluate the fact that our method is robust to this novel attack and that the proposed method performs accurately. Our contributions are detailed as follows.

1.1. Our Contribution. We first propose a method designed to prevent relay attacks on PKES system in modern cars. We utilize sound-based proximity detection to construct our method.

(i) Our method is able to prevent the attack which existing sound-based approach is reportedly vulnerable to [10]. We show that our method prevents such attacks by emitting random sounds, while also recording ambient sound.

(ii) We newly define a record-and-playback attack that thwarts sound-based approaches. In addition, we demonstrate that our method is robust to such an attack.

(iii) We conducted a series of experiments using commercial off-the-shelf products (i.e., microphones and loudspeakers). With these products, we show how practically feasible attacks on PKES systems are prevented.

The rest of the paper is organized as follows. In Section 2, we first describe the motivation of this paper. In Section 3, we introduce the preliminary background for this paper. In Sections 4 and 5, we provide a system model and explain our method, respectively. Section 6 presents the result of the evaluation of our method. Related works are discussed in Section 7. The limitations of this paper and future works are presented in Section 8. Finally, we conclude this paper in Section 9.

2. Motivation

With PKES, the car owner is passively authenticated based on the proximity of a car to its corresponding key, which belongs to the car owner. The car (i.e., the verifier) detects the proximity of the corresponding key by using a short-range communication channel, such as Bluetooth or radio frequency identification (RFID) [19, 20]. Then, an authentication protocol—KeeLoq, for instance [21]—is executed between the car and the key, such that the car owner does not need to do anything for being authenticated.

Unfortunately, short-range communication channel is insufficient for guaranteeing the correct proximity of the owner, because the communication range can be extended. For example, the communication range of Bluetooth is approximately ten meters; however, malicious attackers can scan and attack a Bluetooth device from up to a mile away using signal-extending device called BlueSniper Rifle [22]. Indeed, Francillon et al. demonstrated that relay attacks could be used against PKES in modern cars [3]. They successfully relayed a signal from a car to its corresponding key using two loop antennas connected together with a cable. Moreover, attackers can opt to use an amplifier in the middle of the cable to improve the signal power. Francillon et al. succeeded at opening the door and starting the engine of a car, despite the fact that the key was 60 m away. In theory, they added that such an attack is possible at distances of up to 1.5 km. In spite of these concerns, relay attacks on PKES have been regarded as impractical. Designers consider relay attacks too difficult and costly for attackers to deploy. However, Bilton claimed that the tools required for such a relay attack are available for only USD$17 [23]. Furthermore, a recent robbery involved thieves perpetrating a relay attack in Frankfurt, Germany [2]. The robbers succeeded at opening a car door with a relay attack and proceeded to steal a number of valuables from inside the car. Fundamentally, PKES works by detecting the proximity of the key with a short-range communication channel. This makes it possible to deploy a relay attack. By relaying signal, it is possible for a car to communicate with its corresponding key at extended distances, ultimately unlocking the door and even starting the engine.

3. Background

In this section, we explain the PKES system and the metrics used for similarity measurements.

3.1. Passive Keyless Entry and Start (PKES) System. Waraksa et al. first proposed the PKES system to enable drivers to automatically lock, unlock, and start a car. The system unlocks the car as the driver approaches it, carrying the corresponding key. It likewise locks the car whenever the key is out of range. Because the system does not require any action on the part of the driver, it is called "passive."

With PKES, a car communicates with its corresponding key using magnetically coupled RF signals. Thus, a communication channel is established when the key is in close proximity to the car. The car and its corresponding key use two types of RFID tags: low-frequency (LF) and ultrahigh-frequency (UHF) RFID tags. The car uses an LF channel to send messages to the key, instructing it to "wake up" and accept "challenges." The key uses a UHF channel to send messages to the car in response. The UHF RFID tag is used to save battery power [24]. Because the communication range of the LF RFID tag is approximately 1-2 m, the key wakes up only when it is close to the car (there are several categories

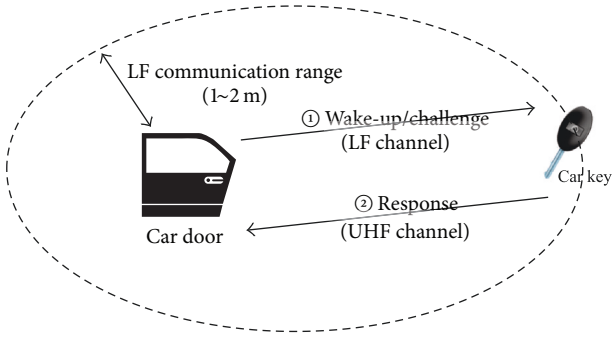


Figure 1: Authentication flow for the PKES system.

of RFID technology based on used frequencies, and each has both advantages and disadvantages) [25]. Figure 1 illustrates how the PKES system works. The car periodically broadcasts a wake-up signal using the LF channel. If the key is within range of the car, an authentication protocol is executed (e.g., KeeLoq (sometimes called a hopping code or a rolling code) is a block cipher that uses a nonlinear feedback shift register (NLFSR); it accepts 64-bit keys and encrypts 32-bit blocks, which was used in many remote keyless entry systems) to generate a challenge and receive the response. Both the car and the corresponding key share a symmetric key for authentication, and this is set by the manufacturer. PKES is now a widely used system. However, as described in Section 2, attackers can unlock the car door even without having the symmetric key, simply by relaying LF and UHF channels.

3.2. Sound Similarity. To detect the proximity of a car to its key, the similarity of sound can be used, when both the key and the car record sound concurrently. In this subsection, we describe three typical metrics for measuring the similarity between two recorded sounds: the Euclidean distance, cross-correlation, and cosine similarity [26]. We evaluated our method using these metrics. In what follows, $X = (x_1, x_2 \cdots x_n)$ and $Y = (y_1, y_2 \cdots y_n)$ denote two signals represented as n-points in a discrete time series (i.e., the recorded sound). For simplicity, we assume that both series have the same length.

Euclidean Distance. The Euclidean distance (or Euclidean metric) is the most common sound-similarity metric. Geometrically, the Euclidean distance refers to the length of a straight line between two points in Euclidean space. In two dimensions, if $a = (a_1, a_2)$ and $b = (b_1, b_2)$, then the Euclidean distance is given as follows:

$$d(a,b) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2}. \quad (1)$$

A value of $d(a,b) = 0$ indicates that the two points are exactly same. Values higher than 0 refer to the Euclidean distance between the two points. We can measure the sound similarity between $X = (x_1, x_2, \ldots, x_n)$ and $Y = (y_1, y_2, \ldots, y_n)$ using the Euclidean distance as follows:

$$d(X,Y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2}. \quad (2)$$

The resulting distance ranges from 0, when they are exactly the same, to any positive integer. The degree by which two time series differ increases in proportion to the Euclidean distance.

Cross-Correlation. Cross-correlation is frequently used to measure the similarity between two series. The concept of correlation is important to understanding of cross-correlation. The correlation between two variables refers to the degree of linearity between them. A correlation of 0 indicates that two variables are independent, and a correlation of 1 indicates that the two variables are exactly the same. Correlation ranges from −1 to 1, where the former refers to two variables that are the same but with opposite signs.

Cross-correlation is a measure of the similarity of two series as a function of the lag of one relative to the other. For two discrete time series, $X = (x_1, x_2, \ldots, x_n)$ and $Y = (y_1, y_2, \ldots, y_n)$, the cross-correlation is as follows:

$$X\mathrm{Corr}_{X,Y}[l] = \sum_{m=0}^{n-1} (x_m \cdot y_{m-l}), \quad (3)$$

where $l \in [0, n-1]$ denotes the lag.

To accommodate for different amplitudes of the two series, the cross-correlation can be normalized as follows:

$$X\mathrm{Corr}'_{X,Y}[l] = \frac{X\mathrm{Corr}_{X,Y}[l]}{\sqrt{X\mathrm{Corr}_{X,X}[0] \cdot X\mathrm{Corr}_{Y,Y}[0]}}, \quad (4)$$

where $X\mathrm{Corr}_{X,X}[0]$ is the so-called autocorrelation of X and $X\mathrm{Corr}'_{X,Y}[l] \in [-1, 1]$.

A value of $X\mathrm{Corr}_{X,Y}[l] = 1$ indicates that, at lag l, two signals have the same shape, even if their amplitudes are different; −1 indicates that two signals have the same shape but opposite signs; and 0 indicates that the two signals are uncorrelated.

Accordingly, we can measure the sound similarity with a cross-correlation metric. The following absolute value for the maximum cross-correlation $\widehat{X\mathrm{Corr}'_{X,Y}}$ can be used as a metric for similarity.

$$\widehat{X\mathrm{Corr}'_{X,Y}} = \arg\max_l \left(\left| X\mathrm{Corr}'_{X,Y}[l] \right| \right). \quad (5)$$

A value of $X\mathrm{Corr}'_{X,Y} = 0$ indicates that the two series X and Y are uncorrelated; 1 indicates that the two series are exactly the same.

Cosine Similarity. The cosine similarity is a measure of the similarity between two vectors by measuring the cosine of the angle between them. A cosine of 0° is 1, and it is less than 1 for

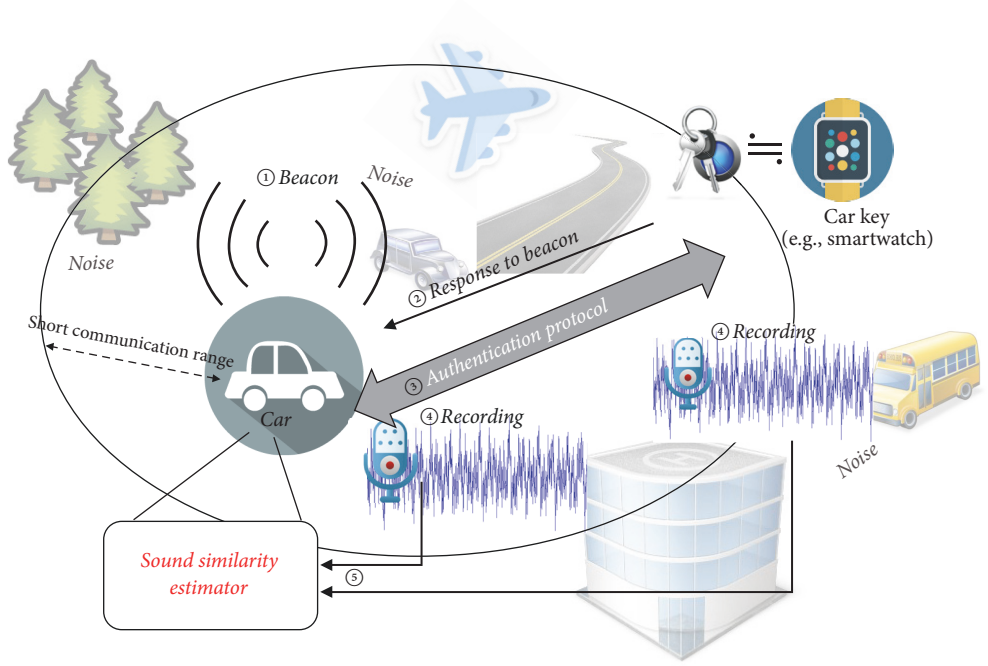


Figure 2: System model.

any other angle. The cosine similarity is thus a judgment of the orientation, rather than the magnitude. Two vectors with the same orientation have a cosine similarity of 1, two vectors at 90° have a similarity of 0, and two vectors diametrically opposed have a similarity of −1.

For two time series X and Y, the similarity between them is calculated as follows:

$$\mathrm{CS}(X,Y) = \frac{\sum_{i=1}^{n} x_i y_i}{\sqrt{\sum_{i=1}^{n} x_i^2 \times \sum_{i=1}^{n} y_i^2}}. \tag{6}$$

The resulting similarity ranges from −1 (exactly opposite), to 1 (exactly the same), with 0 indicating decorrelation. Values within this range indicate the intermediate similarity or dissimilarity.

4. System Model

We present a system model in which our method enables a car to verify proximity of its key. The basic concept is for a car and its key to concurrently record ambient sounds as shown in Figure 2. The car would measure similarity between the two recorded sounds and then proximity of the car key is determined based on the result. In contrast to existing PKES, our method needs both entities to have a microphone by which they record sounds; accordingly, it seems that our method might have a limitation to be directly applied into current cars. Even though car has enough ability to record sounds or it is relatively easier to install an additional device for it, it is hard for current car keys to record sound and transmit it wirelessly. Recently, however, most car manufactures have released their telematics services to provide convenience with car users [27]. Through smart devices, car owners are able to unlock the door or start the engine at a distance from their cars, which implies that cars have been already connected with smart devices. In fact, smartwatch would be a promising type to replace car keys because users would always wear it [28–30]. We expect this kind of devices will gradually replace conventional car keys and our method will be suitable. To better explain our method, we detail each procedure by which the car verifies its corresponding key based on proximity of the car key.

(i) The car periodically broadcasts a beacon message via a short-range communication channel (e.g., the LF RFID channel).

(ii) If a car key is within the communication range, the car key responds to the beacon.

(iii) The car and its key perform an authentication protocol using the preshared secret (i.e., symmetric key).

(iv) If the car keys are authenticated, they simultaneously record ambient sounds, and then the keys transmit the recorded audio file to the sound-similarity estimator module of the car.

(v) The estimator module measures the similarity of the two audio files—the audio file from the car and the one from the key—thereby detecting the proximity of a car to the key.

If the car key is authenticated and its proximity is verified, the door would be unlocked. It is noted that our method is designed for Steps (iv)-(v) and (i)–(iii) are the same procedures as existing PKES.

4.1. Concern of Interference. Because our method is designed to verify proximity based on recorded ambient sounds, a concern of interference by noise might exist. In this subsection, we describe how our method works even under noisy condition which might cause interference. It is important to understand the fact that a car and its key do not communicate with each other through sounds in our method. Ambient sounds to be recorded are only used to check if they are close to each other. In other words, our method is designed based on the fact that the entities which are close to each other would listen to the same or very similar ambient sounds. As a result, no matter how noisy environment is, a car and its key would record the same sounds; rather, noisy sounds can be helpful to extract unique characteristics for their proximity because that noise would be location-specific information.

Furthermore, even in case of multiple cars, our method would work properly. For example, multiple cars are using our method at a parking lot and they record the same ambient sounds nearby. In this case, all of the cars may record the same or very similar ambient sounds so that it might seem difficult to distinguish the proper car key. Even though, however, a car key has the same sound signature, the car key would be blocked by the authentication protocol that is performed before our method. Please recall that our method is designed for a car to verify proximity of its key, by which the existing authentication protocol would be supported.

4.2. Adversary Model. The main goal of attackers on our method is to unlock the door or start engine without car owner's knowledge. Because the existing PKES is able to prevent passive attacks, we only consider active attacks on our method. Accordingly, adversaries have abilities to modify replay messages and relay signals. In our adversary model, adversaries are divided into two types based on how they acquire ambient sounds which will be used for comparison with one measured from a target car. The first type of adversaries (Type I) is the attack that tries to unlock the door when the driver and car key are only a moderate distance away (e.g., as the driver walks through the parking lot). The other type of adversaries (Type II) is the attack that records the ambient sound near the car and then plays back the recorded audio in the vicinity of the car key. The detailed descriptions of each adversary are as follows.

Adversary Model Type I (Out-of-Range Attack). Type I adversary model represents attackers who have the ability to execute a relay attack on PKES. After the driver parks his/her car and locks the door, he/she would walk away. At this point, both a car and its key are likely to record very similar sounds. That is, Type I adversaries have the chance to unlock the door before the driver moves too far away, by relaying signals from the car to its corresponding key. We define this as an out-of-range attack.

Adversary Model Type II (Record-and-Playback Attack). Type II adversary model represents the attack that records the ambient sound near the car and then plays back the recorded audio in the vicinity of the car key. Even though the car is distant from its corresponding key (e.g., when the driver works at an office), Type II adversaries would manipulate the ambient sound by relaying it such that both the car and key record a similar sound (hence, a record-and-playback attack). Because we define this type of attacks for the first time, we detail each step in record-and-playback attack as follows. Moreover, two colluding attackers A and B are required in this attack. We refer to this as a record-and-playback attack.

(i) Attackers A and B, who are close to the car and its key, respectively, establish a long-distance communication channel.

(ii) Attacker A records the ambient noise near the car, encodes the sound, and transmits this audio file to Attacker B via the long-distance communication channel.

(iii) Attacker B decodes and plays the audio file, such that the key records audio that is similar to the ambient noise near the car.

4.3. Our Assumptions. Our method is designed based on the following assumptions:

(1) First, our method assumes that, like the existing PKES system, both the car and key have a preshared secret (i.e., a symmetric key).

(2) Further, because our method aims to prevent relay attacks (as described in Section 2), we assume that attackers have the ability to relay short-range communications between the car and the key.

(3) Finally, we assume that the key has sufficient resources to record and transmit audio files. A smartwatch, for example, would work as such a key with our method [29, 30].

5. Our Method

Our method is designed to accurately detect the physical proximity of a car to its key. To do so, the method first executes one of the existing authentication protocols for PKES. After this initial authentication, both the car and the key start to record ambient sounds concurrently. The car key sends the recorded sounds to the car; then, the car verifies proximity of the key based on the similarity result of the two recorded audios. We describe each step in our method as follows.

5.1. Symmetric-Key Based Authentication. In PKES, a car authenticates its corresponding key with a preshared symmetric key. As explained in Section 3.1, an RFID communication channel is used such that the car periodically checks whether the key is nearby. When the key and the car are both within the RFID communication range, they execute a predefined authentication protocol. KeeLoq is the standard protocol used with existing PKES system [21]. If the car key is authenticated, the following steps are taken to ensure physical proximity between the car and its corresponding key.

5.2. Ambient Sound Recording. Before the car and its key record ambient sounds, car makes other random sounds to enhance entropy of ambient sounds to be recorded such as horn. This is because that the car cannot make sure of the verified proximity if the entropy is low. For the random sound the car emits, n frequencies are randomly selected within the human audio spectrum, ranging within 20–20,000 Hz as follows:

$$f_i \in_R [20, 20000], \quad 1 \le i \le n. \tag{7}$$

For the selected frequencies f_i, the corresponding length of time during which each frequency plays is also selected randomly, as follows:

$$t_i \in_R (0, T),$$
$$\text{s.t.} \sum_{i=1}^{n} t_i = T, \tag{8}$$

where T is the total time during which the random sound plays. The car and its corresponding key both record ambient sound, whereas only the car emits the random sound. As a result, two audio files are generated, REC_{car} and REC_{key}.

5.3. Recorded-Signal Transmission. The key generates a message authentication code (MAC) for the recorded audio file REC_{key}, by using a preshared secret k for the MAC. Then, the key transmits REC_{key} and $\text{MAC}_k(\text{REC}_{\text{key}})$ to the car. Because the MAC is coupled with the key's audio file, the car can verify the integrity of REC_{key} to confirm that REC_{key} was recorded exclusively by the appropriate key.

5.4. Proximity Detection. The car thus receives REC_{key} from the corresponding key and estimates the similarity between REC_{car} and REC_{key}. The estimation function F (described in Section 3.2) is used to calculate the similarity score as follows:

$$\text{Score}_{\text{Similarity}} = F\left(\text{REC}_{\text{Key}}, \text{REC}_{\text{car}}\right). \tag{9}$$

After this similarity estimation, the car compares the similarity score to a threshold that has been set in advance. If the score is higher than this threshold, the method concludes that the key is in close proximity to the car. Accordingly, the doors of the car will be safely unlocked.

6. Experimental Results

We evaluated our method by performing a series of experiments. We assessed the error rate when detecting the proximity of the key to the car. We used typical metrics to assess this error rate—that is, the False Negative (FN) rate and the False Positive (FP) rate [31]. The FN rate represents the probability that our method will (falsely) determine that the key is not close to the car even though, in fact, it is. The FP rate represents the probability that our method (falsely) judges that the key is near the car when, in fact, it is not. False Positives can arise, for instance, when the two audio files are recorded at different times. Our experiments yielded an equal error rate (i.e., the rate at which both the FN rate and FP rate are the same) of 0.0024. Because our method is executed with the existing symmetric-key-based authentication protocol, such an error rate should be considered trustworthy.

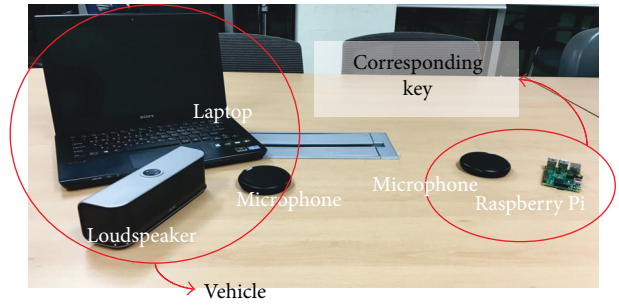


Figure 3: Experimental setup.

6.1. Experimental Setup. We tested our method with a laptop and a Raspberry Pi to represent the car and its corresponding key, respectively. Figure 3 shows our experimental setup, and Table 1 explains the function of each component and its specifications. To record sounds, we selected a sampling rate in accordance with the Nyquist–Shannon sampling theorem [32]. Because sound is audible up to a frequency of 20 KHz, the sampling rate should be greater than 40 KHz. Our method records sound at 44.1 KHz, because this is the minimum sampling rate in common, satisfying greater than 40 KHz. Notably, a higher sampling rate requires more memory and battery power.

6.2. Basic Experiment. In this section, we discuss the process of finding an optimal recording time for our method. With this recording time, we show that our method has a sufficiently low error rate for proximity detection. With PKES, the car door is unlocked only if the driver is carrying the key within one meter from the car. Accordingly, we evaluated our method such that the car (i.e., the laptop) is within a meter from the key (i.e., the Raspberry Pi). We selected an outdoor parking lot as the most common parking location and performed the experiment during the daytime. We tested our method by changing the recording time from 1 s to 5 s at intervals of 1 s. Furthermore, 500 pairs of audio files were recorded to evaluate each candidate recording time. In order to estimate the similarity between each pair of audio files, we used the metrics described in Section 3.2. Tables 2–4 show the error rates for our method with three different similarity metrics: Euclidean distance, cosine similarity, and cross-correlation. In these tables, rows represent the recording time and columns represent the thresholds. From these three metrics, we can see that the error rate with cross-correlation is much lower than it is with the others. Even when the threshold was between 0.2 and 0.3, the error rate was almost 0. That is, cross-correlation outperformed the other similarity metrics. Thus, only cross-correlation was used to estimate the sound similarity in subsequent evaluations.

In addition, a longer recording time resulted in a lower error rate, and vice versa. This implies a tradeoff between

Table 1: Components of experimental setup.

Name	Specifications	Explanation
Laptop	CPU Intel i7 2.9 GHz RAM 16 GB running Window 8.1	Represents a car that emits a beacon sound (challenge). Both the ambient noise and a challenge are recorded simultaneously with the key, and the sound-similarity estimation algorithm is applied.
Raspberry Pi	Type B+ RAM 1 GB running Contiki OS	Represents a key that records both the ambient noise and a challenge (beacon sound) simultaneously with the car. Then, audio file is transmitted to the sound-similarity estimator in the car.
Microphone	Frequency response 20 Hz–18 KHz	Used for both the laptop (car) and the Raspberry Pi (key) to record sounds.
Loudspeaker	Frequency response 20 Hz–20 KHz	Used by the laptop (car) to emit a beacon sound (challenge).
Mobile phone	Apple iPhone 6s and SAMSUNG Galaxy Note 2	Used for a record-and-playback attack. The two mobile phones are connected to one another in speaker mode via a cellular (3G) network.

Table 2: FN and FP for the Euclidean distance.

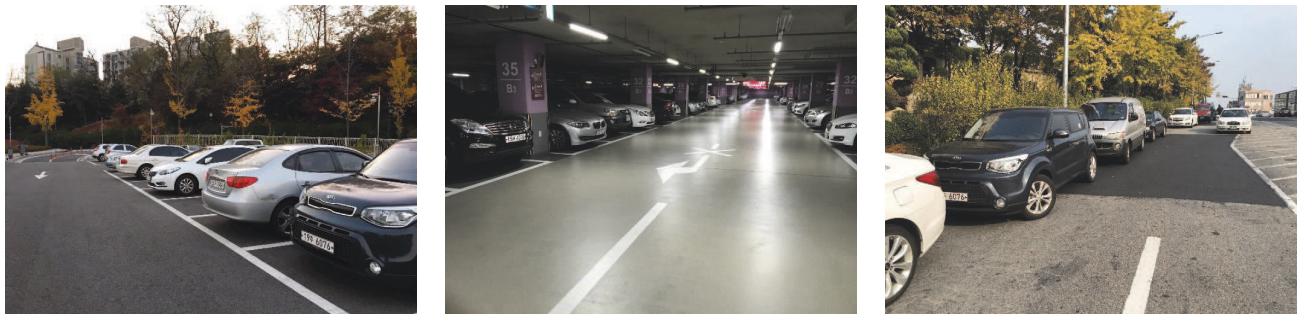
	1 s	2 s	3 s	4 s	5 s
1	0.00/1.00	0.00/1.00	0.00/1.00	0.00/1.00	0.00/1.00
10	0.39/0.77	0.00/1.00	0.07/1.00	0.02/1.00	0.00/1.00
20	0.95/0.03	0.11/0.92	0.94/0.96	0.25/0.99	0.00/1.00
30	0.99/0.00	0.97/0.01	0.98/0.06	0.65/0.76	0.16/0.85
40	0.99/0.00	0.99/0.00	0.98/0.01	0.93/0.35	0.76/0.15
50	0.99/0.00	0.99/0.00	0.99/0.00	0.98/0.07	0.95/0.00
60	0.99/0.00	1.00/0.00	0.99/0.00	0.98/0.01	0.98/0.00
70	0.99/0.00	1.00/0.00	1.00/0.00	0.99/0.00	0.99/0.00
80	1.00/0.00	1.00/0.00	1.00/0.00	0.99/0.00	0.99/0.00

Table 3: FN and FP for the cosine similarity.

	1 s	2 s	3 s	4 s	5 s
0.1	0.55/0.05	0.46/0.00	0.86/0.00	0.40/0.00	0.75/0.00
0.2	0.76/0.00	0.79/0.00	0.97/0.00	0.76/0.00	0.96/0.00
0.3	0.82/0.00	0.94/0.00	0.99/0.00	0.92/0.00	1.00/0.00
0.4	0.87/0.00	0.98/0.00	1.00/0.00	0.98/0.00	1.00/0.00
0.5	0.92/0.00	0.99/0.00	1.00/0.00	0.99/0.00	1.00/0.00
0.6	0.96/0.00	1.00/0.00	1.00/0.00	1.00/0.00	1.00/0.00
0.7	0.99/0.00	1.00/0.00	1.00/0.00	1.00/0.00	1.00/0.00
0.8	0.99/0.00	1.00/0.00	1.00/0.00	1.00/0.00	1.00/0.00
0.9	0.99/0.00	1.00/0.00	1.00/0.00	1.00/0.00	1.00/0.00

Table 4: FN and FP for the cross-correlation.

	1 s	2 s	3 s	4 s	5 s
0.1	0.00/0.60	0.00/0.04	0.00/0.01	0.00/0.01	0.00/0.01
0.2	0.01/0.06	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00
0.3	0.01/0.00	0.00/0.00	0.04/0.00	0.00/0.00	0.00/0.00
0.4	0.10/0.00	0.02/0.00	0.33/0.00	0.01/0.00	0.03/0.00
0.5	0.44/0.00	0.23/0.00	0.77/0.00	0.13/0.00	0.28/0.00
0.6	0.74/0.00	0.63/0.00	0.97/0.00	0.61/0.00	0.79/0.00
0.7	0.81/0.00	0.94/0.00	0.99/0.00	0.94/0.00	0.99/0.00
0.8	0.99/0.00	0.99/0.00	0.99/0.00	0.99/0.00	0.99/0.00
0.9	0.99/0.00	1.00/0.00	1.00/0.00	1.00/0.00	1.00/0.00



(a) Outside parking (b) Underground parking (c) Road-side parking

Figure 4: Three different environmental conditions.

Table 5: FN and FP rate in different environmental conditions.

	FN	FP
Outdoor parking	0.000	0.001
Underground parking	0.000	0.006
Road-side parking	0.005	0.000

usability and security. We set the optimal recording time at 2 s, to satisfy both usability and security, because we expect that car owners can easily wait 2 s to unlock a door with an error rate close to 0. Therefore, we used 2 s as the recording time for subsequent evaluations.

6.3. Environment Conditions. In this subsection, we focus on environments where cars are commonly parked. We selected three typical locations, as shown in Figure 4: (i) an outdoor parking lot, (ii) an underground parking lot, and (iii) road-side parking. Each environment has distinct ambient noise: wind and the buzz of conversation in the outdoor parking lot; frictional sound between the tires and surface, fan noise, and siren noise in the underground parking lot; and the noise from passing cars when the car is parked on the side of the road.

Figure 5 shows the error rates for our method (with cross-correlation, recorded for 2 seconds). Because the road noise is much louder, it was sometimes difficult for the car key to recognize the beacon sound. On the other hand, it was easier for the car to recognize its own beacon sound, because the car's microphone and loudspeaker were close together. This explains why the error rate with road-side parking was relatively higher. Nevertheless, the equal error rate with road-side parking was only 0.0037, meaning that our method is robust to environmental dynamics.

In addition, the thresholds for the equal error rates in each environment were different. Figure 5(d) shows an equal error rate of 0.0024 when all data was evaluated regardless of the environment. The threshold for the equal error rate was set at 0.272. We thus applied this threshold (i.e., 0.272) to each environment. Table 5 shows the FN and FP rates for each environment, with a threshold of 0.272.

A threshold of 0.272 is therefore suitable, because the error rates shown in Table 5 are adequate for proximity detection.

6.4. Sound Level. As we described in Section 4.1, loud condition would help our method clearly verify the proximity. In this subsection, we provide the experimental measurements on the decibel levels of sounds to show how error rates change. Our method was evaluated either indoors or outdoors to get the decibel level we want. The decibel levels were measured including random sounds the car emits to increase in our method. It is noted that lower sound than 60 dB was available inside of building. Figure 6 shows FN and FP rate in different sound levels. These error rates are calculated with the same threshold applied above (i.e., threshold of 0.272). In this result, we can see that every sound level has 0 of FP rate. As sound level is higher, our method has lower error rate, in which our method has FN of 0.004 under the decibel level of 90 dB.

6.5. Out-of-Range Attack. In this subsection, we evaluate the robustness of our method to adversary models. Because our method is designed to detect close proximity, we regard a car key that is farther than 1 m as invalid. Unfortunately, our method cannot exactly distinguish the difference between 1 m and 2 m, because the sound heard at both distances is almost identical. On the other hand, if the key is far from the car, our method can distinguish between the audio files because the key cannot properly recognize the beacon sound. Figure 7 shows the impact of the sound-similarity score on the distance. As the distance increases, the similarity score decreases. Indeed, when the key was 15 m away from a car, the mean of the sound-similarity score was almost 0. Table 6 shows the FP rate corresponding to the distance between the car and the key.

Although the error rate at 15 m is significantly higher, it is unrealistic for attackers to unlock the door at such a distance because the driver would be close enough to notice the attack. Accordingly, out-of-range attacks within 15 m are impractical, whereas those deployed from more than 15 m away are easily detected with our method. Therefore, we conclude that our method is robust to Type I attacks, as described in Section 4.2.

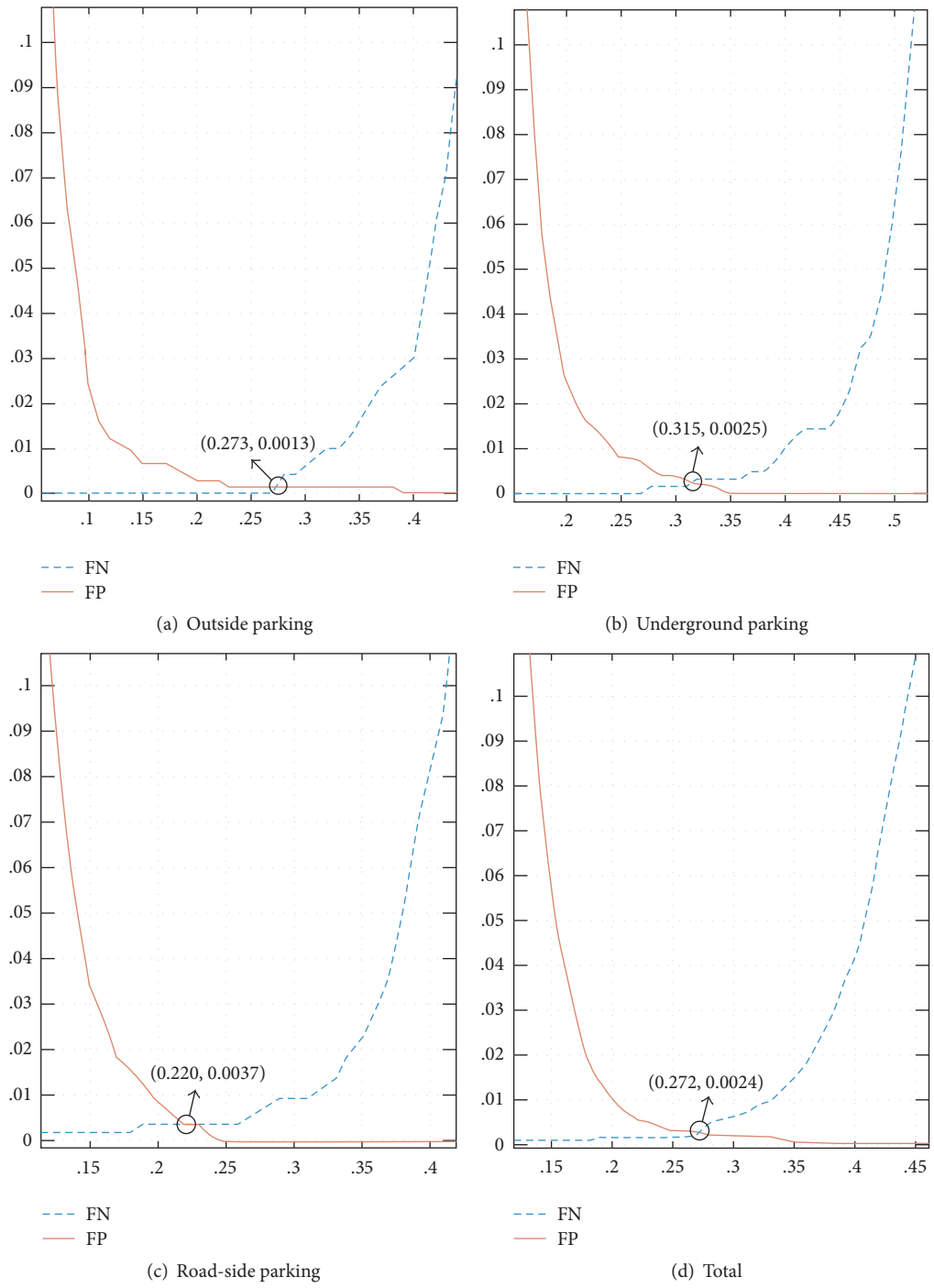


FIGURE 5: False Negative rate and False Positive rate as a function of the threshold. (a) is the result at an outdoor parking lot, where the equal error rate is 0.0013 at a threshold of 0.273. (b) is the result at an underground parking lot, where the equal error rate is 0.0025 at a threshold of 0.315. (c) is the result at a road-side parking lot, where the equal error rate is 0.0037 at a threshold of 0.220. (d) is the result regardless of the environmental condition, where the equal error rate is 0.0024 at a threshold of 0.272.

6.6. Record-and-Playback Attack. In this subsection, we evaluate the robustness of our method to a record-and-playback attack. Because record-and-playback attacks occur when a car and a key are far away from each other, we first selected typical locations of cars and keys. We used the same three car locations as described above, and we selected three common places where keys might be found: (i) a coffee shop, (ii) an office, and (ii) a gym locker room. We thus evaluated our method in nine paired environments.

For a record-and-playback attack, the attackers must stream two-way audio between the car and the key in real-time. Consequently, we used two mobile phones to record

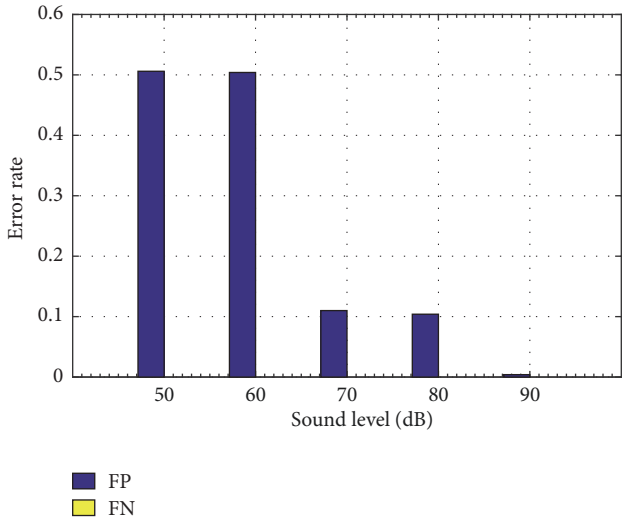


Figure 6: FN and FP rate in different sound levels.

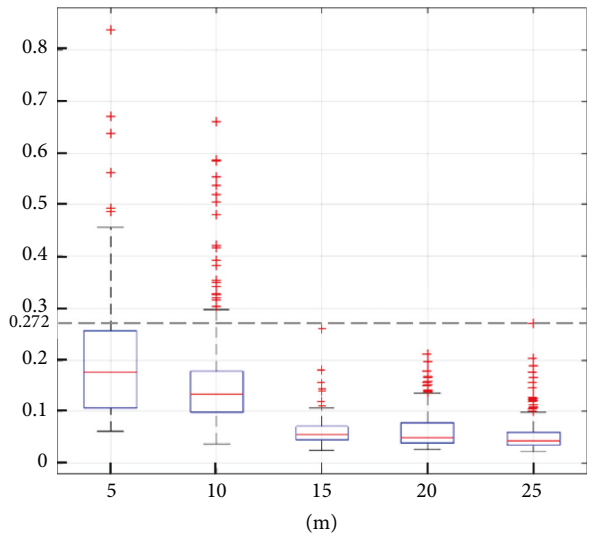


Figure 7: Impact of the sound-similarity score on the distance.

Table 6: FP rates corresponding to the distance between the car and the car key.

	5 m	10 m	15 m	20 m	25 m
FP	0.213	0.096	0	0	0

and play back sound. One mobile phone (Phone A) was placed near the car and recorded both the ambient noise and the beacon sound. It then relayed the recorded audio to the second mobile phone (Phone B), which was placed near the key. Then, Phone B played the relayed audio file such that it could be recorded by the key. In addition, we set the distance between Phone B and the key's microphone to 10 cm. The mobile phones were connected via a cellular network, and they were set to speaker mode.

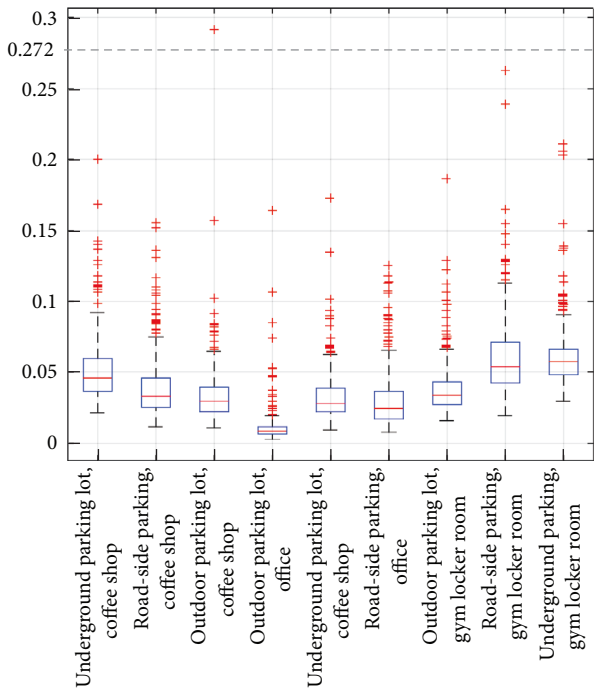


Figure 8: Impact of the sound-similarity scores on the paired environments.

Figure 8 shows the impact of the sound-similarity scores on the paired environments. The reason why all of the sound-similarity scores were lower than the threshold (0.272) is that the car and the key recorded different ambient noise, while it is difficult to relay the beacon sounds clearly to the corresponding key.

7. Related Works

Systems that enable passive authentication, including PKES, are vulnerable to relay attacks [3, 33]. In this section, we introduce related works that focus on physical-proximity detection, where the goal is to prevent relay attacks.

Received Signal Strength Indicator (RSSI). RSSI systems have been used to estimate the distance between a verifier and a prover by processing signal strength information. For example, if a verifier determines that the prover's signal strength, they can be considered close to one another. Krumm and Horvitz proposed an RSSI-based system using the Wi-Fi signal strength [34]. With their system, a wireless access point (AP) measures the Wi-Fi signal strength of users' devices. From these measurements, both the user's motion and the distance between the user and the AP can be inferred. Fishkin and Roy proposed an RFID-based method that uses the relation between the RSSI and variations in the energy signature to determine the level of trust [35]. However, both of the above methods are vulnerable to attackers who amplify the broadcasting power or change the directional characteristics of the devices [8].

Distance-Bounding Protocol. Several security methods have been proposed based on a distance-bounding protocol in order to prevent three types of attacks [4–6, 8, 11, 13–15, 36, 37]. For historical reasons, these are known as Distance Fraud, Mafia Fraud, and Terrorist Fraud [38, 39]. The goal of a distance-bounding protocol is to enable a verifier to establish an upper bound on its physical distance to a prover. With the distance-bounding protocol, the verifier sends an unpredictable challenge to the prover. The prover then generates a response to the challenge and sends this value to the verifier. Based on the round-trip time measured by the verifier, the distance between the verifier and prover can be derived. There are two types of distance-bounding protocols. The first uses an ultrasonic communication channel to transfer data. This method is more accurate at measuring the distance between the verifier and prover. However, it is more vulnerable to relay attacks that use a faster communication channel than ultrasonic communication [16]. The second type of distance-bounding protocol uses RF communication channels. Even though RF communication channels are resilient to relay attacks, both the verifier and the prover must be strictly time-synchronized and the prover's processing must be invariant [8].

Context-Based Proximity Detection. Contextual information varying over time or location can also be used to verify whether a prover is close to a verifier, assuming that copresent devices acquire similar information. In addition, context-based detection assumes that attackers cannot infer the information needed for verification at a distance. For example, GPS coordinates and/or RF packets can be used as contextual information for proximity detection [40–43].

Varshavsky et al. proposed a proximity-detection method that uses RF packets and RSSI as contextual information [43]. Shrestha et al. proposed a method that exclusively relies on contextual information such as temperature, precision gas, humidity, and altitude [41]. Because it is difficult for exclusively contextual information to be compromised, their method is resilient to attacks. Truong et al. proposed a method that uses modalities that can be measured from the sensors of smartphones [42]. They used Wi-Fi signal strength, Bluetooth signal strength, GPS, and audio as contextual information. Miettinen et al. proposed a method that uses ambient noise and luminosity, both of which can be easily measured with wearable devices [40]. They used this information both to establish a secure channel between the verifier and the prover and to detect proximity.

Sound-Based Proximity Detection. In the context of a near-field communication (NFC) financial transactions, bank servers can validate transactions when both the NFC phone and reader are precisely at the same location, thereby preventing relay attacks against such systems. Halevi et al. proposed a method that can detect proximity using ambient sound in NFC payment systems [33]. Thiel et al. proposed a proximity-detection method with mobile phones that is based on sound beacons in an inaudible spectrum around 18 KHz [44]. Even though both the above methods are similar to ours, their method cannot be easily applied to PKES systems. Moreover, they are not resilient to record-and-playback attacks. Schürmann and Sigg proposed a method that establishes a secure communication channel among devices based on similar audio patterns using a fuzzy-cryptography scheme [45]. They extracted features from ambient audio and used these features to generate a shared cryptographic key between devices, without exchanging information regarding the ambient audio itself. Karapanos et al. proposed a two-factor authentication method using sound-based proximity detection [10]. When clients login to websites with this method, they first submit their username and password. Then, smartphones carried by the clients are used as the secondary authentication (i.e., a what-you-have authentication). Both the smartphone and a laptop record ambient sound at the same time, after which both audio files are sent to an authentication server. The authentication server estimates the sound similarity in order to confirm the proximity of devices. Thus, even if attackers know the client's username and password, they cannot be authenticated because they do not have the client's smartphone. This method is practical for applications with two-factor authentication systems. However, their method is vulnerable to same-media attacks and the record-and-play attack we described above.

8. Limitations and Future Work

In this section, we discuss limitations of our method and future work. We have evaluated our method under various environmental conditions, but there are still other environmental conditions that remain to need to be tested. For example, during the day, sound bends away from the ground, whereas during the night, it bends toward the ground. Accordingly, an experimental result on this phenomenon seems to be needed.

Moreover, we should imagine an attacker who has the ability to emit loud noise near both the car and its key at the same time. This noise might be able to overwhelm the ambient noise and the random sound; as a result, both the car and its key may record the artificial noise generated by the attacker. We shall explore this type of attack in future work.

We can also enhance the performance of our method by combining it with the existing researches. In case of an out-of-range attack, we might combine our method with the research by Lu et al., who proposed a method that enables mobile phones to model sound events [46]. They demonstrated that their system was capable of recognizing meaningful sound events occurring in the everyday lives of users (e.g., walking outdoors and highway driving). By applying their research to our method, the car will recognize the environment it is in. Then, a dynamic threshold can be set based on the recognized environment, thus decreasing the error rate.

To counter a record-and-playback attack, we can combine our method with that of Das et al., who proposed a method to identify smartphones through imperfections in acoustic components [47]. Their method was able to distinguish between different loudspeakers even when they play the same sound. Accordingly, by applying their research to our

method, the car will be able to distinguish between different sources of recorded sounds (i.e., whether sounds are coming from a car or a mobile phone).

Finally, with our method, the random sound emitted by the car risks annoying people in the vicinity. Thus, inaudible frequencies (i.e., 18–20 KHz) might be used for the beacon sound, such that the sound is imperceptible to humans but not to the car and the key.

9. Conclusion

In this paper, we described PKES system and its vulnerability (i.e., relay attack). The relay attack has been a critical issue. In fact, thieves even utilized the relay attack to steal valuables from a car. The main reason why PKES system is vulnerable to the relay attack is that the communication neighborhood would not be proof of physical proximity. We proposed a method which enables detecting physical proximity, making it possible to prevent relay attacks on PKES systems. Because our method detects physical proximity based on sound similarity, we presented a system model for our method and defined a new adversary model (i.e., a record-and-playback attack).

In addition, we evaluated our method by taking environmental conditions into consideration. In other words, we selected typical locations of cars and keys for our evaluations. We showed that our method has high accuracy in detecting physical proximity of a car to a key and is robust to both an out-of-range attack and a record-and-playback attack. We discussed several methods that could be applied into our method in order to improve accuracy in detecting physical proximity [46, 47], which we leave for future work.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korean government (MSIP) (R7117-17-0161, Anomaly Detection Framework for Autonomous Vehicles).

References

[1] "Keyless-go," https://www.mbusa.com/mercedes/owners/videos/detail/videoId-554cd68b2c51d310VgnVCM2000007d1843-35RCRD . Online; accessed 18-11-2015.

[2] "Massenhaft autos per funksignal geklaut," http://hessenschau.de/panorama/diebe-klauen-luxusautos-in-serie-per-funkwellenverstaerker,neue-autodiebstahl-methode-100.html. Online; accessed 18-11-2015.

[3] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," *In NDSS*, 2011.

[4] S. Brands and D. Chaum, "Distance-bounding protocols," in *Advances in Cryptology-Eurocrypt '93*, vol. 765 of *Lecture Notes in Computer Science*, pp. 344–359, Springer, Berlin, Germany, 1994.

[5] S. Čapkun, L. Buttyán, and J.-P. Hubaux, "Sector: secure tracking of node encounters in multi-hop wireless networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 21–32, Association for Computing Machinery, Washington, DC, USA, October 2003.

[6] S. Drimer, S. J. Murdoch et al., "Keep your enemies close: Distance bounding against smartcard relay attacks," in *In USENIX Security*, vol. 2007, 2007.

[7] S. Gezici, Z. Tian, G. B. Giannakis et al., "Localization via ultra-wideband radios: a look at positioning aspects of future sensor networks," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 70–84, 2005.

[8] G. P. Hancke and M. G. Kuhn, "An RFID distance bounding protocol," in *Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm 2005*, pp. 67–73, Greece, September 2005.

[9] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370–380, 2006.

[10] N. Karapanos, C. Marforio, C. Soriente, and S. Capkun, "Sound-proof: Usable two-factor authentication based on ambient sound," https://arxiv.org/pdf/1503.03790.

[11] J.-Y. Lee and R. A. Scholtz, "Ranging in a dense multipath environment using an UWB radio link," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 9, pp. 1677–1683, 2002.

[12] J. Munilla, A. Ortiz, and A. Peinado, "Distance bounding protocols with void-challenges for RFID," *In Printed handout at the Workshop on RFID Security–RFIDSec 6*, vol. 6, 2006.

[13] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09)*, pp. 410–419, Chicago, Ill, USA, November 2009.

[14] N. Sastry, U. Shankar, and D. Wagner, "Secure Verification of Location Claims," in *Proceedings of the ACM Workshop on Wireless Security*, pp. 1–10, San Diego, Calif, USA, September 2003.

[15] N. O. Tippenhauer and S. Čapkun, "ID-based secure distance bounding and localization," in *In Computer Security–ESORICS 2009*, vol. 5789, pp. 621–636, Springer, Berlin, Germany, 2009.

[16] S. Sedighpour, S. Čapkun, S. Ganeriwal, and M. Srivastava, "Implementation of attacks on ultrasonic ranging systems," in *Proceedings of ACM Conference on Networked Sensor Systems (SenSys)*, p. 312, San Diego, California, USA, November 2005.

[17] "Starbucks korea lets customers place orders with their mobile phone, more countries to follow," http://www.nfcworld.com/2014/06/04/329509/starbucks-korea-lets-customers-place-orders-mobile-phone-countries-follow/. Online; accessed 18-11-2015.

[18] "Worldwide craze for o2o, south korea's yap goes global with o2o," http://www.prnewswire.com/news-releases/worldwide-craze-for-o2o-south-koreas-yap-goes-global-with-o2o-30004-2702.html. Online; accessed 18-11-2015.

[19] J. C. Haartsen, "Bluetooth radio system," *IEEE Personal Communications*, vol. 7, no. 1, pp. 28–36, 2000.

[20] R. Want, "An introduction to RFID technology," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25–33, 2006.

[21] F. J. Bruwer, W. Smit, and G. J. Kuhn, "Microchips and remote control devices comprising same," US Patent 5517187, 1996.

[22] J. Hering, "The bluesniper "rifle"," in *Proceedings of the 12th DEFCON*, Las Vegas, Nevada, 2004.

[23] "Car thieves using $17 power amplifier to hack keyless entry system," http://www.itproportal.com/2015/04/20/car-thieves-using-17-power-amplifier-hack-keyless-entry-system/. Online; accessed 18-11-2015.

[24] A. I. Alrabady and S. M. Mahmud, "Some attacks against vehicles' passive entry security systems and their solutions," *IEEE Transactions on Vehicular Technology*, vol. 52, no. 2, pp. 431–439, 2003.

[25] D. Dressen, "Considerations for rfid technology selection," *Atmel Applications Journal*, vol. 3, pp. 45–47, 2004.

[26] X. Yu, X. Pan, W. Yang, W. Wan, and J. Zhang, "Audio similarity measure based on Renyi's quadratic entropy," in *Proceedings of the 2010 International Conference on Audio, Language and Image Processing, ICALIP 2010*, pp. 722–726, Shanghai, China, November 2010.

[27] "Gm onstart," https://www.onstar.com/us/en/get-onstar/equipped-vehicles.html. Online; accessed 18-11-2015.

[28] "7 Apple Watch apps that replace your car keys," https://www.computerworld.com/article/2923929/wearables/7-apple-watch-apps-that-replace-your-car-keys.html. Online; accessed 03-12-2017.

[29] "CES 2015: Audi and LG have built a smartwatch that controls a car," http://www.mirror.co.uk/news/technology-science/technology/ces-2015-audi-lg-built-4932283. Online; accessed 18-11-2015.

[30] "Tim cook wants the apple watch to replace your car keys," http://jalopnik.com/tim-cook-wants-the-apple-watch-to-replace-your-car-keys-1688487763. Online; accessed 03-12-2017.

[31] Ron Kohavi and Foster Provost, "Glossary of terms," *Journal of Machine Learning Research*, vol. 30, no. 2-3, pp. 271–274, 1998.

[32] E. J. Candès and M. B. Wakin, "An introduction to compressive sampling: a sensing/sampling paradigm that goes against the common knowledge in data acquisition," *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp. 21–30, 2008.

[33] 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: 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10–12, 2012. Proceedings*, vol. 7459 of *Lecture Notes in Computer Science*, pp. 379–396, Springer, Berlin, Germany, 2012.

[34] J. Krumm and E. Horvitz, "LOCADIO: inferring motion and location from Wi-Fi signal strengths," in *Proceedings of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MOBIQUITOUS '04)*, pp. 4–13, Boston, Mass, USA, August 2004.

[35] K. P. Fishkin and S. Roy, "Enhancing rfid privacy via antenna energy analysis," *In RFID Privacy Workshop*, 2003.

[36] C. H. Kim and G. Avoine, "Rfid distance bounding protocol with mixed challenges to prevent relay attacks," in *In Cryptology and Network Security*, pp. 119–133, Springer, Berlin, Germany, 2009.

[37] G. Sinan, T. Zhi, and B. Giannakis Georgios, "Localization via ultra-wideband radios. IEEE," *IEEE Signal Processing Magazine*, vol. 35, no. 2, pp. 131–135, 2005.

[38] C. Cremers, K. B. Rasmussen, B. Schmidt, and S. Capkun, "Distance hijacking attacks on distance bounding protocols," in *Proceedings of the 33rd IEEE Symposium on Security and Privacy, S and P 2012*, pp. 113–127, San Francisco, CA, USA, May 2012.

[39] Y. Desmedt, "Major security problems with the "unforgeable" (feige)-fiat-shamir proofs of identity and how to overcome them," in *In SecuriCom*, vol. 88, pp. 15–17, 1988.

[40] M. Miettinen, N. Asokan, T. D. Nguyen, A.-R. Sadeghi, and M. Sobhani, "Context-based zero-interaction pairing and key evolution for advanced personal devices," in *Proceedings of the 21st ACM Conference on Computer and Communications Security, CCS 2014*, pp. 880–891, Association for Computing Machinery, Scottsdale, AZ, USA, November 2014.

[41] B. Shrestha, N. Saxena, H. T. T. Truong, N. Asokan, and N. Asokan, "Drone to the rescue: Relay-resilient authentication using ambient multi-sensing," in *In Financial Cryptography and Data Security*, vol. 8437, pp. 349–364, Springer, Berlin, Germany, 2014.

[42] 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 *Proceedings of the 2014 12th IEEE International Conference on Pervasive Computing and Communications, PerCom 2014*, pp. 163–171, Budapest, Hungary, March 2014.

[43] A. Varshavsky, A. Scannell, A. LaMarca, and E. de Lara, "Amigo: Proximity-Based Authentication of Mobile Devices," in *Ubi-Comp 2007: Ubiquitous Computing*, vol. 4717 of *Lecture Notes in Computer Science*, pp. 253–270, Springer, Berlin, Heidelberg, 2007.

[44] B. Thiel, K. Kloch, and P. Lukowicz, "Sound-based proximity detection with mobile phones," in *Proceedings of the 3rd International Workshop on Sensing Applications on Mobile Phones (PhoneSense '12)*, p. 4, ACM, Toronto, Canada, November 2012.

[45] D. Schürmann and S. Sigg, "Secure communication based on ambient audio," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 358–370, 2013.

[46] H. Lu, W. Pan, N. D. Lane, T. Choudhury, and A. T. Campbell, "SoundSense: scalable sound sensing for people-centric applications on mobile phones," in *Proceedings of the 7th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys '09)*, pp. 165–178, Krakov, Poland, June 2009.

[47] A. Das, N. Borisov, and M. Caesar, "Do you hear what i hear? Fingerprinting smart devices through embedded acoustic components," in *Proceedings of the 21st ACM Conference on Computer and Communications Security, CCS 2014*, pp. 441–452, Scottsdale, AZ, USA, November 2014.