OPay: an Orientation-based Contactless Payment Solution Against Passive Attacks

Mahshid Mehr Nezhad
Warwick University, United Kingdom
mahshid.mehr-nezhad@warwick.ac.uk

Feng Hao
Warwick University, United Kingdom
feng.hao@warwick.ac.uk

Abstract

The usage of contactless payment has surged in recent years, especially during the Covid19 pandemic. A Passive relay (PR) attack against a contactless card is a well-known threat, which has been extensively studied in the past with many solutions available. However, with the mass deployment of mobile point-of-sale (mPoS) devices, there emerges a new threat, which we call mPoS-based passive (MP) attacks. In an MP attack, the various components required in a PR attack, including an NFC reader, a wireless link, a remote card emulator, and a remote payment terminal, are conveniently combined into one compact device, hence the attack becomes much easier. Since the attacker and the victim are in the same location, the previous distance bounding or ambient sensor-based solutions are no longer effective. In this paper, we propose a new orientation-based payment solution called OPay. OPay builds on the observation that when a user makes a legitimate contactless payment, the card and the terminal surface are naturally aligned, but in an attack scenario, this situation is less likely to occur. This allows us to distinguish the legitimate payments from passive attacks based on measuring the alignment of orientations. We build a concrete prototype using two Arduino boards embedded with NFC and motion sensors to act as a card and a payment terminal respectively. To evaluate the feasibility, we recruited twenty volunteers in a user study. Participants generally find OPay easy to use, fast and reliable. Experiments show that OPay can substantially reduce the attack success rate by 85-99% with little inconvenience to real users. To our best knowledge, OPay is the first solution that can prevent both the PR and MP attacks, while preserving the existing usage model in contactless payment.

1 Introduction

Contactless payment is a widely deployed technology that uses Near Field Communication (NFC) for making transactions. In a contactless transaction, two entities are involved: a tag and a reader. A tag is embedded in a payment device (e.g., credit/debit cards, mobile phones and key fobs), and a reader is a point-of-sale (PoS) terminal that communicates with the payment device via NFC.

It is well known that existing contactless cards are vulnerable to passive relay (PR) attacks [2, 9, 12, 13, 27]. In this attack, an attacker uses an NFC reader to interrogate a victim's card in close proximity and relays the card's response to a remote card emulator via a wireless link to make a purchase at a remote payment terminal. Due to the passive nature of contactless cards, anyone who is near the victim can launch this attack without the victim's awareness. The user may discover this attack later when they receive the bank statements, but the money has already been stolen. Such attacks can be difficult to trace, especially when the payments are made at unattended terminals, e.g., a self-service kiosk [26].

Passive attacks against contactless cards have become increasingly concerning in recent years for two reasons. First, the spending limit for a contactless payment has increased significantly. When contactless cards were first introduced in the UK in 2007, they were limited to only £10 in a transaction. However, this limit quickly rose to £20 in 2012, £30 in 2015, £45 in 2020, and it will increase to £100 by the end of 2021 as announced by the UK Treasury [14]. With the increasing limit, contactless cards are becoming a more attractive target. Second, the number of mobile PoS (mPoS) terminals has been quickly growing, e.g., Sumup [1], Square[2], and iZettle[3]. These devices are compact, low-cost, wireless, and easy to set up. They enable anyone who has a bank account to set up a payment terminal. While mPoS devices bring great convenience to retailers and small businesses to set up their own payment terminals, they can also be easily misused. We use the Sumup device as an example. In our experiments, we entered an arbitrary amount under the spending limit on a Sumup device and were able to discretely deduct the amount from a user's card which was kept in their bag or pocket. This proof-of-concept attack was tested against the cards of the

[1] https://sumup.co.uk/
[2] https://squareup.com/
[3] https://www.izettle.com/

authors, but the same attack can be trivially extended to steal money from anyone.

Currently, the primary countermeasure implemented in Sumup and other mPoS devices is making an audible "beep" sound when a payment is made. This serves to alert the card owner that a transaction has been made. However, with the example of Sumup, we show that the beep sound can be easily muted through reverse-engineering the Sumup app (which we explain later). A secondary countermeasure is to trace the bank account associated with the mPoS terminal and hopefully recover the stolen money. However, numerous examples of frauds in the banking industry suggest that recovering stolen money is not any easy task [1]. For example, attackers may use mPoS terminals to wirelessly steal money from people in multiple crowded places like train stations, shopping malls, or concerts, at the same time, so that they can steal a significant amount of money within a short period of time. They will simply withdraw or transfer out the money before being discovered. In reality, criminals often hire unsuspecting (young and old) people as mules and use their bank accounts as intermediaries to transfer illicit funds. All these make it difficult to trace the real attackers.

We consider an mPoS-based passive (MP) attack as a new form of passive attacks. To some extent, an MP attack can be seen as a variant of the PR attack. A PR attack involves an NFC reader, a wireless link, a remote card emulator, and a remote terminal. In an MP attack, these different parts are conveniently combined into one compact mPoS device. This greatly reduces the sophistication of the equipment and skills required to carry out an attack.

As a result of this new variant of the passive attack, many solutions proposed in the past to defend against PR attacks are no longer effective. Common solutions in the literature are based on the assumption that the victim's card and the real terminal are far apart in two distinct environments. More concretely, they adopt distance-bounding protocols [8] or use sensors to measure the ambient environment (e.g., temperature [25], light [18], audio [18, 30], humidity [25], GPS [30], magnetic field [19] and infrared light [15, 17]) to ensure the two devices are in close proximity. However, in an MP attack, the fact that the card and the mPoS terminal are already in close proximity renders these solutions ineffective.

Besides the distance-bounding and ambient-sensor-based solutions, some researchers proposed to prevent the PR attacks by involving explicit user actions to activate the payment processes. For example, Tap-Tap and Pay (TTP) [23] requires a user to gently tap the card (or the mobile phone) against the terminal twice in succession to initiate a contactless payment. Shake on It (Shot) [29] requires the NFC card and the reader to be held together to establish a physical contact via accelerators and vibrators. Proximity and Relay Attack Detection (PRAD) [16] works by requiring the user to press buttons on NFC devices to activate the transaction. While these solutions are useful in certain applications, they are less suitable in the context of contactless payment since they modify the usage model of how a user normally makes a contactless card payment.

To effectively prevent passive attacks against contactless cards, a practical solution should satisfy the following requirements. First, it should prevent both PR and MP attacks, taking into account that the victim's card and the real terminal may be in close proximity and in the same environment. Second, it should be fast, allowing the transaction to be completed within 500 ms according to the EMV requirement [15]. Third, it should preserve the usage model, allowing users to naturally complete a transaction as normal.

To the best of our knowledge, there is no existing solution which satisfies all of these requirements. Therefore, we present a solution that meets this goal. Without loss of generality, we focus on the more dangerous MP attack, but the same solution is also applicable for preventing the PR attack. The key idea in our solution is to make use of the accelerator and gyroscope sensors to derive the orientation of an NFC device. When a user makes a contactless payment by placing the card on the top or in front of an mPoS terminal, the orientations of the card and the terminal are naturally aligned. However, in an attack scenario where the victim's card is in a bag or pocket, the card and the terminal are less likely to be aligned. Hence, based on analyzing the orientations, we can tell a legitimate payment apart from an illegitimate one. We also build a concrete prototype and conduct a user study to evaluate the feasibility of our solution. The user study indicates that our solution is easy to use, and can substantially reduce the attack success rate from the current 100% to only 1-15%, whiling incurring only a small 4.76% false rejection rate. We summarize our contributions as follows.

- We present OPay, an orientation-based payment solution against passive attacks in contactless payments. Our solution is the first that addresses both PR and MP attacks, supports a fast transaction under 500 ms, and does not change the usage model.
- We build a concrete prototype of OPay by using Arduino boards with embedded NFC, accelerometer, and gyroscope sensors to implement a payment card and a terminal respectively. All our code is open source here.
- We conduct user studies to evaluate the usability and performance of our OPay prototype. The studies show that our solution is easy to use with low false positive and negative rates.

The rest of the paper is organized as follows. In Section 2, we discuss the overview of mPoS terminals and their vulnerabilities. In Section 3, we describe the threat model and the OPay system, followed by the system prototype and evaluation in Section 4. OPay is compared with related work in Section 5. We finally discuss the limitations and future work of OPay in Section 6 and conclude the paper in Section 7.

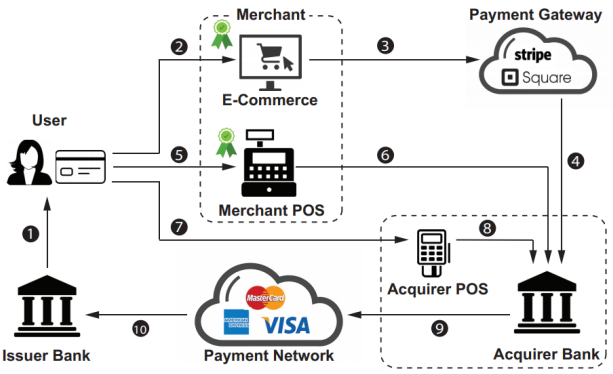


Figure 1: Payment card ecosystem [24]

2 Mobile point-of-sale (mPoS) terminal

Fig. 1 shows the payment ecosystem and the relationships between the users, merchants, and banks [24]. The issuer bank issues payment cards to the users (step 1). Each card has a shared secret key with the issuer bank. The key is mainly used to protect the transaction data via Message Authentication Code (MAC), but it can also be used to encrypt data based on using AES and a key derivation function [10]. A user can make a transaction in three different ways: 1) using an e-commerce service (steps 2 and 3) over the internet via a payment gateway, 2) using a PoS terminal developed by a third party such as a merchant PoS (step 5), or 3) using a PoS terminal provided by the acquirer bank (step 7). The acquirer bank manages an account for the merchant to receive and route the transaction information (steps 4, 6, and 8) and ensures that funds are deposited into the merchant's account once the transaction is completed via the payment network (steps 9 and 10). In OPay, we focus on the transactions that use PoS terminals developed by a third party (steps 1, 5, 6, 9, and 10) that require the use of a mobile phone to transmit the data from the mPoS terminal to the issuer bank via a payment network.

In this ecosystem, merchants can use mPoS terminals to accept users' payments using contact or contactless cards. These terminals can be bought online by any individual and it takes less than 5 minutes to set up. The Sumup device that we have purchased costs only £19. We explain the Sumup setup process in the following. The setup processes for other mPoS products are similar.

The first step to set up a terminal is to sign up for an online account. This is done by filling out information about the business, merchant, and bank details. The business information includes name, address, and category (e.g., retail, services, beauty, wellness, etc.). However, the important information to verify a business such as company registration number, VAT ID (Value Added Tax Identification Number), proof of address and business, and legal identification documents is optional. This is to allow any individual to set up an mPoS terminal. The merchant information includes name, date of birth, and address. Finally, the bank details include the sort code and account number. These are needed to deposit payouts after the transaction fee is deducted from the transaction amount (e.g. 1.69% for contactless transactions using a Sumup device).

When the Sumup online account is set up, the merchant needs to install the Sumup app on their mobile phone and pair it with the terminal via Bluetooth. The mobile phone would serve as an intermediary that connects the mPoS terminal to the acquirer bank. To initiate a payment, the merchant first specifies an amount on the mPoS device, up to a spending limit. The user then pays for the amount, either using contactless payment or inserting a chip-and-PIN card. The transaction data will be sent from the mPoS terminal to the mobile phone via Bluetooth, and then further relayed to the payment network via the Internet. When a chip-and-PIN card is inserted, a PIN is also required. However, in the case of contactless payment, no PIN is required. This is particularly risky for many users since the payment can be made contactlessly without their cooperation or even awareness. To test the feasibility of this passive attack, we placed the contactless cards inside bags and used an mPoS device to approach the bags from outside at a close distance. Our findings show that we can always successfully trigger a contactless payment. In this proof-of-concept demonstration, we used our own bank cards. However, the attack can be extended to steal money from anyone.

To prevent an mPoS terminal from making a contactless payment deduction from an unaware user (either maliciously or by accident), the Sumup device makes a beep sound whenever a contactless payment is conducted. This makes a covert passive attack difficult without alarming the user. It is possible to use a physical sound dampener to lower the volume of the beep. However, we show we can completely disable the beep sound by software means. Through reverse-engineering the Sumup app and analyzing the code, we find out that the volume of the beep sound is controlled by the mobile phone app, in a method called paySoundEffect under the AudioMangers class. Thus, if we can modify this method, we can completely control the beep sound. This requires us to modify the mPoS app; this is easily doable for the Sumup app on an Android phone.

Modifying the Sumup app involves a few simple steps. First, we decompile the Sumup app using two openly available tools: apktool[4] and a standard Java decompiler[5]. The first tool produces Smali code, while the second produces Java code. We use two different tools as they are complementary. Smali code is more difficult to read, therefore we use the Java code to understand the application code and identify the part in the source code that needs to be altered. We then make the

[4]https://ibotpeaches.github.io/Apktool/
[5]http://www.javadecompilers.com/

actual change in the Smali code. The main changes include removing the playSoundEffect method and all the calls to it. This modification has the effect of completely muting the beep sound. After the modified Smali code is recompiled, we use the APK Easy tool[6] to add a self-signed certificate, which is required by Android. Finally, we install the modified app directly on the mobile phone. We repeat the passive attack experiments and find that the attack works as before except that the beep sound from the mPoS terminal has been completely muted. This shows relying on a beep sound to alert the victim is not safe and a more secure solution is required.

3 Our proposed OPay system

In this section, we propose an orientation-based payment system called OPay. The main idea of OPay is to use the orientation data of the payment device and the mPoS terminal in order to approve or deny a transaction based on the similarity of their measurements. The intuition is that when a user makes a contactless payment, the orientation of their card is naturally aligned with that of the payment terminal. In case of an attack, when an attacker uses an mPoS terminal to approach an uncooperative user, it is less likely that the orientations of the two devices will be aligned. Our goal is not to completely stop the passive attacks, but to significantly increase the chance of detection without adding inconvenience to users in legitimate payment scenarios.

3.1 Overview

Fig. 2 shows an overview of the architectural design of our system. In OPay, both the payment device and the mPoS terminal collect readings from the accelerometer and gyroscope sensors to independently calculate the orientations. The mPoS terminal sends a challenge to the card to initiate the NFC communication and to request a contactless payment. The card responds with signed transaction data, generated with Message Authentication Code (MAC), e.g., using HMAC [28] and a MAC key k derived from the shared key between the card and the issuer bank. Then, the terminal forwards the transaction data to an issuer bank via a payment network. MAC protects the transaction data from being modified by the terminal or any entity in the transmission path. This follows the existing data flow in the EMV specification [6]. OPay does not change this flow but adds an encrypted blob of the card's orientation data, Ori(c), e.g., using AES-CBC [28] and a symmetric encryption key derived from the shared key between the card and the issuer bank [10]. The card's secret key shared with the bank is protected by the tamper-resistant chip, and hence cannot be accessed by the attacker (otherwise the bank cards can be cloned).

[6]https://github.com/stevenahoy/apk-easy-tool

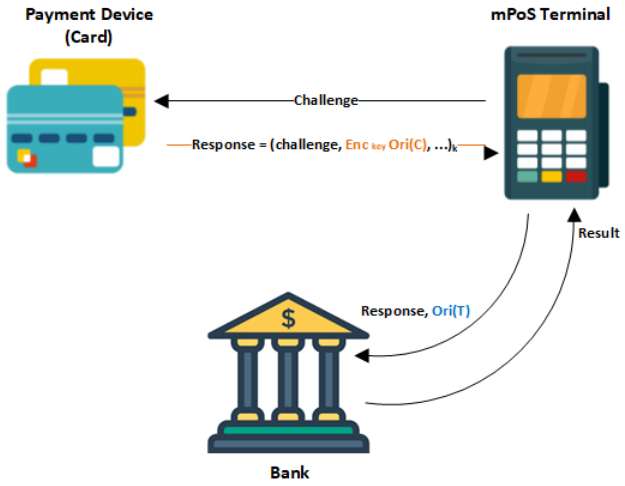


Figure 2: Architecture of OPay

As we will explain later, the orientation data consist of 4 float numbers (float-16), hence are only 8 bytes. Accordingly, the mPoS terminal sends its own orientation measurement to the bank. If the difference between the two orientations is smaller than a threshold, the bank approves the transactions; otherwise, the transaction is denied, and the user needs to try again.

This solution preserves the existing usage model as a user makes a payment naturally as normal. However, to an attacker, it raises the bar for a successful attack. Without OPay, a passive attacker can steal money with 100% success on the first attempt. However, with OPay, as we will show, while legitimate users can still normally make a successful payment on the first attempt, an attacker will need to make multiple attempts, which can significantly increase the chance of attack detection. For example, if the contactless payment fails consecutively three times due to the misalignment of the orientations, it will trigger an alert at the issuer bank, which in turn can send an SMS message to the user's phone to inform a suspicious activity.

3.2 Threat model

We consider an mPoS-based passive (MP) attack as the main threat. As compared to the PR attack, the attacker owns a PoS terminal and can carry out the attack much more easily. Previous solutions to prevent the PR attacks, based on distance bounding and ambient environments, no longer work, since the card and the real terminal are actually in the same location during the MP attack. In our threat model, the mPoS terminal holder is malicious and aims to steal money from the user by getting close to their payment device. It is called passive because the attack can be done without the user's knowledge. The malicious terminal reads the victim's card passively to

make a contactless transaction. The amount of the payment is a variable up to the spending limit (£100 in the UK from the end of 2021). This attack can be performed in crowded places such as bus and train stations, a shopping mall, or a concert.

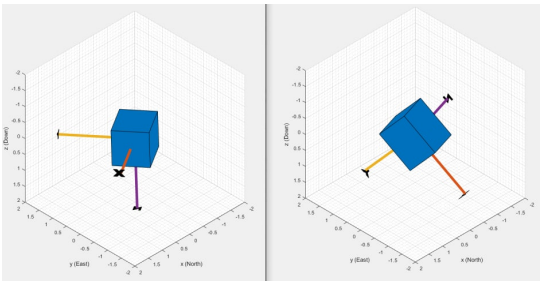
Random Guessing Attack: In this scenario, the attacker has no knowledge of the card's orientation, e.g., when the card is kept inside the user's bag. The attacker randomly chooses an orientation angle in the 3D space and rotates it until they succeed in aligning the two devices. In a random guessing attack, the attacker has a limited chance of success in each try and therefore needs to make several tries until the transaction is approved. Consecutively failed attempts will substantially increase the chance of detection by the bank.

Targeted Guessing Attack: We also consider the scenario that the attacker has partial knowledge of the card's orientation, e.g., when the card is kept in a wallet in the user's pocket. Depending on the visibility of the pocket, the attacker knows that the orientation of the card may be limited to a certain range and hence can have a higher chance of success in guessing the card's orientation. However, our solution still raises the bar for the attacker significantly. As opposed to merely approaching the victim's card within the NFC range (typically 10 cm) from any direction in any angle to make a contactless deduction, the attacker now needs to place the mPoS device near the victim's pocket with parallel alignment to the card's orientation. This significantly increases the chance of the exposure of the attack to the user and the nearby people.

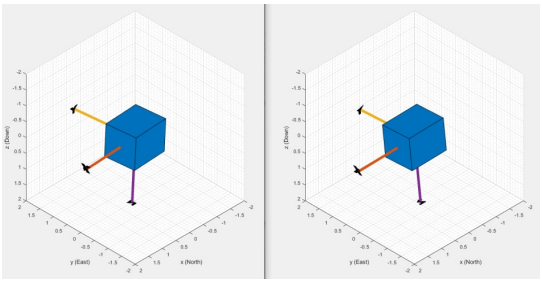
Attacks Beyond Scope: The malicious mPoS terminal holder may be equipped with a portable x-ray scanner and be able to see through opaque objects (e.g., bags) to analyze the orientation of the card. OPay is vulnerable to this kind of attack. However, the constant use of x-ray will present a health threat to the attacker, which can serve as a deterrence. It can also raise suspicion when used in public places. We note that certain cameras (e.g., OnePlus 8 Pro) claim to have an "x-ray vision", but they merely adjust the color filter lens to let through infrared light, hence cannot see through opaque objects as x-ray does [4]. OPay is also vulnerable to Denial-of-Service (DoS) attacks when an attacker intends to disrupt or manipulate the communication channel. As the malicious mPoS terminal holder intends to communicate with the payment device to steal money, they do not have the intention to disrupt the communication channel. Therefore, DoS attacks are out of the scope of this paper.

3.3 Orientation Estimation

For orientation estimation, three types of sensors are commonly used: accelerometer, gyroscope, and magnetometer. They measure acceleration, angular velocity, and local magnetic field respectively. It is expected that combining all three sensors may give the best result. To verify whether this combination is suitable in the context of our application, we chose



(a) Fusing accelerometer, gyroscope and magnetometer



(b) Fusing accelerometer and gyroscope

Figure 3: Display of the orientation alignments between two aligned devices

an MPU-9250 Multi-Chip Module (MCM) which has all these sensors. The MPU-9250 is a 9-axis Motion Tracking device that combines a 3-axis gyroscope, a 3-axis accelerometer, and a 3-axis magnetometer. In our prototype, this module was embedded in an Arduino board, connected to a laptop for data collection. When we put the two Arduino boards together in close proximity to simulate a contactless payment process, we found fusing all three sensors gave a misalignment but fusing only accelerometer and gyroscope data gave the expected alignment (see Figure 3). This is because when the two devices are placed in close proximity, the magnetometer measurements will be distorted due to the co-presence of a nearby magnetometer. Therefore, in our prototype, we only use the accelerometer and gyroscope data, which are fused by applying the six-axis Kalman filter algorithm [21] to estimate orientation.

We consider the definition of orientation as an angular displacement that can be described in terms of point or frame rotation. In point rotation, the coordinate system is static and the point moves. In frame rotation, the point is static and the coordinate system moves. We use the latter to describe the orientation. Therefore, orientation is a rotation that takes a quantity in a parent reference frame to a child reference frame. We consider the geodetic coordinate system (earth) as the reference frame (parent), and the North-East-Down (NED) coordinate system as the coordinate frame (child) where the positive x-axis points north, y-axis points east, and the z-axis

points downward. To define three-dimensional frame rotation (axis of rotation), we rotate sequentially about the z, y, x axes respectively.

Orientation is usually represented as a quaternion, rotation matrix, a set of Euler angles, or rotation vector [21]. We use unit quaternions to represent orientation as they are more compact [7]. A quaternion is defined as a four-part hyper-complex number used in a four-dimensional vector space over the real numbers R^4. It is represented in the form of the following:

$$q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \tag{1}$$

where a, b, c, and d are real numbers, and i, j, and k are the basis elements, satisfying the equation:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1 \tag{2}$$

Every element of q has a unique representation based on a linear combination of the basis elements i, j, and k. We define an axis of rotation and an angle of rotation for each rotation (orientation) as below:

$$q = cos\ (\theta/2) + sin\ (\theta/2)(b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \tag{3}$$

where θ is the angle of rotation and $(b\mathbf{i} + c\mathbf{j} + d\mathbf{k})$ is the axis of rotation.

3.4 Similarity Comparison

There are multiple ways to measure distances between unit quaternions. Polar forms, dot product, and L_2 distance are the most popular forms [21]. Although these representations are in different forms, they are functionally equivalent. For simplicity, we choose dot-product of the two quaternions for comparing and measuring the angle between them. Having the $q_t = a_t + b_t\mathbf{i} + c_t\mathbf{j} + d_t\mathbf{k}$ as the orientation of the mPoS terminal and $q_c = a_c + b_c\mathbf{i} + c_c\mathbf{j} + d_c\mathbf{k}$ representing the orientation of the card, the dot-product between them is defined as:

$$q_t \cdot q_c = a_t a_c + b_t b_c + c_t c_c + d_t d_c \tag{4}$$

The result of the dot-product is a scalar within the range $-1 \leqslant q_t \cdot q_c \leqslant +1$. Considering Equation (3) and using the absolute value of the dot product in Equation (4), we can calculate the angle (in range of 0 and 90 degrees) between the two devices as follows.

$$\theta = \cos^{-1}(|q_t \cdot q_c|) \tag{5}$$

To show the correlation of the angle between the dot-product, we collected data for different orientation sets between the card and the terminal, with a varying angle from 0 to 180 degrees. As one of the devices (the mPoS terminal) is fixed on the table, we rotated the other device (payment device/card) from 0 to 180 degrees. Fig. 4 shows the results

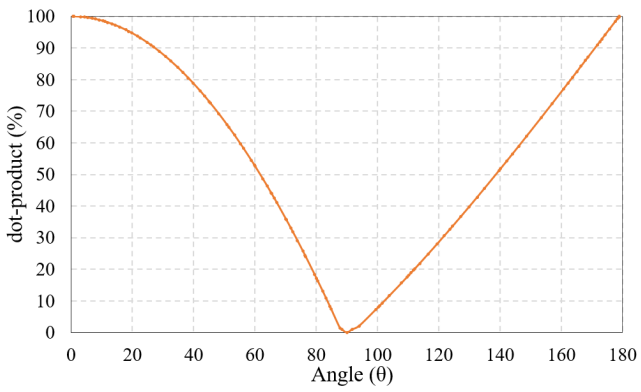


Figure 4: The Correlation between the angle of rotation and dot-product of quaternions

where the x-axis is the degree of rotation and the y-axis is the dot-product in the range of 0 and 1. It can be seen from the diagram that the card and the terminal are in perfect alignment (i.e., $|q_t \cdot q_c| = 1$) when the angle is at 0 and 180 degrees and are perpendicular to each other (i.e., $|q_t \cdot q_c| = 0$) when the angle is at the 90 degrees. In our design, we consider the situation that a user may make a transaction by either placing the front or back of their card on the PoS terminal. We treat them as being equivalent, hence, the angles of 0 and 180 degrees are both considered as aligned. In other applications, they can be treated differently if the user can distinguish the front and back of a card/device. In Figure 4, the values of the dot product are not completely symmetric according to the 90 degrees. This is because we embed the motion sensors on one side of the Arduino board, and the prototype of the card is not completely symmetric with reference to the board plane.

3.5 Threshold Calculation

To either accept or reject a transaction, the bank needs to make a decision based on comparing the orientation angles between the two devices. To calculate the threshold for the comparison, we use the False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR is the percentage of instances in which unauthorized transactions are incorrectly accepted. FRR is the percentage of instances in which authorized transactions are incorrectly rejected. The chosen threshold should give an appropriate trade-off between the security of the system and the usability experienced by users. In Section 4.3, we conduct a user study to determine the threshold and report the corresponding system performance.

4 System prototype and evaluation

We implemented a proof-of-concept prototype for the OPay system and conducted a user study to evaluate the system

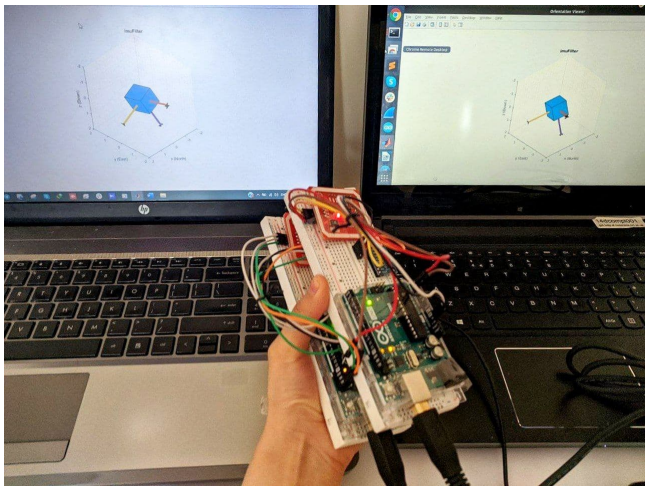


Figure 5: A prototype of the proposed solution. The orientations of the two devices are derived from the accelerometer and gyroscope data and are displayed in a simulated contactless payment.

performance.

4.1 Implementation

In the prototype, we developed two Arduino boards, one for the mPoS terminal and one for the card (payment device). On each of these boards, we used an MPU-9250 sensor for capturing the accelerometer and gyroscope data and a PN-532 NFC RFID module (version 3) for establishing the NFC communication between the two boards. Arduino Uno microcontrollers were used for programming these sensors. We used the P2P NFC communication between the two PN-532 modules in an Inter-integrated Circuit (I2C) mode, programming one NFC module as the initiator (acting as an mPoS terminal), and the other as the target (acting a payment card).

When the user holds the card near the NFC field of the mPoS terminal to make a simulated contactless payment, the NFC sensor embedded on the terminal detects the presence of another NFC sensor in close proximity, and hence initiates the NFC communication between the two devices. The motion sensors embedded on the two Arduino boards independently record the accelerometer and gyroscope measurements. In our proof-of-concept implementation, the collected sensor data on each board are transmitted via a serial port cable to a laptop for further processing. The orientations of the two Arduino boards which represent the card and the terminal respectively are derived based on Section 3.3 and then compared. Based on the similarity, the transaction is either approved or rejected. The implemented prototype is shown in Fig. 5.

Demographic	**Participants(%)**
Gender	
Male	12 (60%)
Female	8 (40%)
Age	
18-25	5 (25%)
26-35	9 (45%)
36-45	4 (20%)
46-55	2 (10%)
Occupation	
University Students	9 (45%)
University/Industry Employee	7 (35%)
Unemployed	4 (20%)

Table 1: Participant demographics. Total number of participants $N = 20$

4.2 User study

Our user study involved 20 volunteers of different backgrounds from within and outside the university. Table 1 summarizes the demographics of the participants. Our user study was ethically approved by our university scientific research ethics committee. We also followed the UK government guideline on COVID-19 to assure the safety of our participants. While wearing face-covering during all times of the study, we provided hand sanitizers, antibacterial wipes, and face masks to all of our participants and sanitized all surfaces after each user experiment.

In our user study, each of the participants performed three experiments, and in each experiment, the data collection was repeated five times. In the first experiment, we fixed the terminal board on the table, and asked users to hold the card board to make a simulated contactless payment as they normally do in real life (see Fig. 6 a). In the second and third experiments, we asked the participants to act as attackers, considering the two attack settings: when the card-board is placed in a bag and when it is in a pocket. Fig. 6 b and Fig. 6 c show the in-bag and in-pocket attack scenarios, respectively. The same experiment was repeated five times. The recorded sensor data were saved into a file for further analysis.

Figure 6: User study setup: a) OPay payment setup; b) random guessing attack; c) targeted guessing attack

4.3 Performance

Error rates: as discussed in Section 3.5, we use FAR and FRR to evaluate the performance of OPay. Fig. 7 shows the FRR and FAR results with reference to a threshold angle of varying degrees. For the targeted guessing attack, the equal error rate (EER) where the FRR and FAR curves intersect is 12%. For the random guessing attack, the EER is only 1%. As an example, if we choose $\theta = 5^\circ$ as the threshold, we have FRR $= 4.76\%$. For the targeted guessing attack, FAR $= 15.24\%$, and for the random guessing attack, FAR $= 0.96\%$. This result is encouraging as it shows that we can substantially reduce the attack success rate from the current 100% to about 1-15% (that is a reduction by 85-99%). Hence, the attacker must make multiple tries, which will significantly increase the chance of detection by the issuer bank, which will in turn inform the user, e.g., by sending an SMS or a notification on the user's phone. The 4.76% false rejection rate is reasonably small. On average, the user will need to make $1/(1-4.76\%) = 1.05$ attempts to make a successful payment. This is hardly an inconvenience. In real-life contactless payment transactions, a cardholder is occasionally declined at the first attempt and needs to make a second attempt for the payment due to various reasons, e.g., distorted signals or interference with other nearby cards or NFC devices [11].

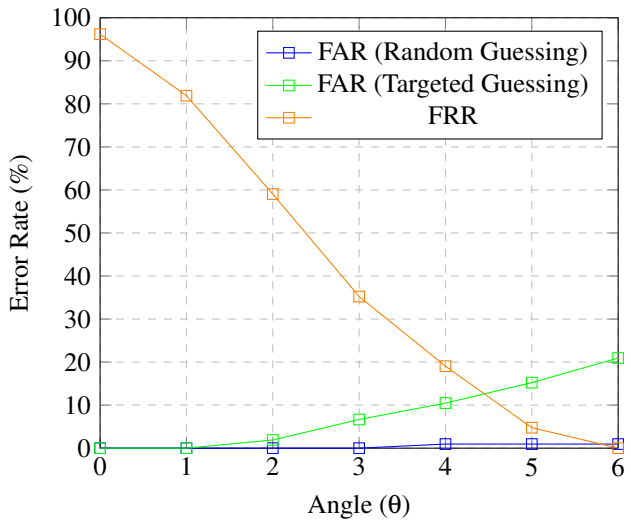


Figure 7: Error rates based on user studies

Timing: In terms of timing, our orientation detection requires collecting 5 samples of quaternions to derive the orientation of the device. It takes only 0.132 seconds to read data from the accelerometer and gyroscope sensors as shown in Table 2. The remaining operations involve fusing the accelerometer and gyroscope measurements and calculating the orientation, which takes 0.082 and 0.014 seconds respectively. Overall, the total duration is 0.228 seconds. From the user feedback, participants in our user study generally do not feel a difference in latency from a normal transaction. We note that providing a fast payment experience is important, and EMV requires a contactless payment to be completed within 0.5 seconds.

Code	Total Time (s)	% Time
Read Sensor Data	0.132	58.1%
Sensor Data Fusion	0.082	36.2%
Orientation Calculation	0.014	5.7%
Total	**0.228**	**100%**

Table 2: Orientation Estimation Duration

4.4 Usability

After the experiments, we conducted an anonymous survey using a questionnaire. In the questionnaire, we asked our participants to rate both the normal contactless payment scenario and the OPay contactless payment scenario in terms of usability. We adopted a widely used System Usability Scale (SUS) framework to assess the user's satisfaction with usability [3]. The SUS questionnaire contains ten questions. The answer to each question scales from 1 to 5 (from strongly disagree to strongly agree). Table 3 shows the SUS questions along with the scores for both payment methods. The overall SUS score for the normal contactless payment scenario (without OPay) is 83. The score for the OPay contactless payment system is 78.62. The slight drop in the SUS score is mainly because the proof-of-concept prototype of the sensor-enabled card uses an Arduino board and is bulkier than a normal bank card. One user commented: "The prototype boards are heavy and there are jumpers on it that make it difficult". Another user also commented: "I find it difficult for people with certain conditions, like people with Parkinson's, or old people with shaking hands." Nonetheless, we are still encouraged by the SUS score of 78.62, which shows the user's general satisfaction with our prototype. We expect the SUS score will increase if the implementation of the card prototype can be made more compact.

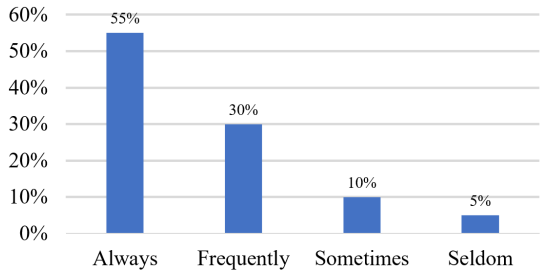
In OPay, users make a contactless payment naturally as normal. The measurement of the motion sensor data is transparent and seamlessly integrated into the payment process. All these make users feel that the OPay system is as fast as a normal payment. A user commented: "To me, it is not different compared to the standard contactless payment scenario." The normal payment usage model is preserved as no additional action is required.

In the questionnaire, we also ask users the frequency of using contactless payments in real life, among the choices of "always", "frequently", "sometimes" and "seldom". The majority of the participants (55%) chose "always", and 30% chose "frequently". Overall, most participants have had experience with using contactless payment (see Fig. 8a). By using

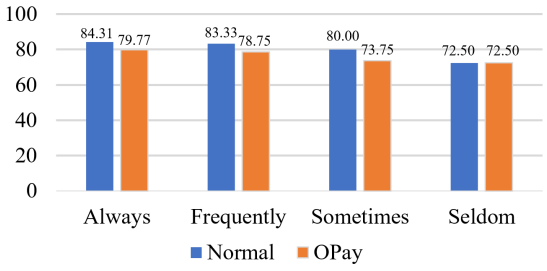
Questions	Average Rate without OPay	Average Rate with OPay	Questions	Average Rate without OPay	Average Rate with OPay
1. I think I would like to use this system frequently	4.25	4.45	2. I found the system unnecessarily complex	1.5	1.8
3. I thought the system was easy to use	4.52	4.5	4. I think that I would need the support of a technical person to be able to use this system	1.55	1.9
5. I found the various functions in this system were well integrated	4	4.15	6. I thought there was too much inconsistency in the system	1.9	1.85
7. I would imagine that most people would learn to use this system very quickly	4.55	3.85	8. I found the system very cumbersome to use	1.55	2.05
9. I felt very confident using this system	3.95	4.35	10. I need to learn a lot of things before I could get going with this system	1.55	1.75

Table 3: SUS Questions and Results

the Spearman correlation method, we find a positive correlation between the OPay SUS score with the participant's previous experience of using contactless (see Fig.e 8b), i.e., the more experience of using contactless payment, the higher the SUS score (Spearman correlation coefficient $\rho = 0.301$ and two-tailed $p < 0.0001$). Similarly, as shown in Fig. 8b, there is also a positive correlation between the SUS score for a normal contactless payment system and the frequency of the usage ($\rho = 0.285$ and $p < 0.0001$).



(a) Frequency of using contactless payment



(b) Correlation with SUS scores

Figure 8: Summary of participants' frequency of contactless payment usage and correlation with SUS scores

5 Related Work

Contactless payment is one application of the NFC technology for making an electronic payment. Other NFC applications include contactless access cards, keyless doors, keyless entry cars, etc. Passive relay (PR) attack is a common threat to all these systems. Solutions proposed in the past can be generally divided into three categories: based on 1) distance bounding; 2) user activation and 3) ambient environment. For the specific contactless payment application discussed in this paper, we focus on reviewing solutions in the last two categories. It is well known that distance bounding protocols are extremely sensitive to processing delays [27]. More efficient protocols apply symmetric cryptography, but require the two devices to have a pre-shared secret key. This is not applicable in our scenario since the card and the payment terminal have no pre-shared secret. Furthermore, in an MP attack, the card and the terminal are already in close distance. Hence, distance bounding is not applicable here.

User activation. This category of solutions involves an explicit user action to activate the payment process. For example, Mehrnezhad et al. [23] proposed a "Tap-Tap and Pay" (TTP) solution, in which a user initiates an NFC payment by physically tapping their payment device against the reader twice in succession to start the payment process. Czeskis et al. [5] require the user to perform a specific gesture (e.g. alpha, key/hip twist, single/double circle, and triangle) with their card to activate an authentication process. Their solution is designed for RFID access cards, but it can also be applied to prevent relay attacks in contactless payment. Gurulian et al. [16] require the user to press buttons on the user's payment device to activate a contactless payment process. All these solutions can prevent PR attacks and MP attacks since an explicit user action is required. However, this changes the existing usage model in contactless payments.

Ambient environment. This category of solutions uses sensors to measure the ambient environment to make sure the card and the reader are in the same environment or the same location. Halevi et al. [18] proposed to measure the audio and light in the ambient environment. Ma et al. [22] proposed

Papers	Category	Required Sensor(s)	Duration (s)	FRR(%)	FAR(%)	Preserves existing usage model	Prevents same env/location attacks
Czeskis et al. [5]	User activation	Accelerometer	1	0	0	No	Yes
Gurulian et al. [16]	User activation	Force Sensitive Resistors	Seconds	0.1	0.1	No	Yes
Mehrnezhad et al. [23]	User activation	Accelerometer	0.6–1.5	9.99	9.99	No	Yes
Gurulian et al. [17]	Ambient env	Infrared sensor	0.5	0.5	0.5	Yes	No
Gurulian et al. [15]	Ambient env	AAE Sensors	0.5	1.72	18.06	Yes	No
Ma et al. [22]	Ambient env	GPS	10	67.5	67.5	Yes	No
Halevi et al [18]	Ambient env	Audio	1-2	0	0	Yes	No
		light	1-2	5	6.5	Yes	No
Shrestha et al. [25]	Ambient env	Temperature (T)	Instant	23.74	32.40	Yes	No
		Gas (G)	Instant	15.26	30.36	Yes	No
		Humidity (H)	Instant	16.25	29.81	Yes	No
		Altitude (A)	Instant	8.57	16.25	Yes	No
		HA	Instant	7.93	9.85	Yes	No
		HGA	Instant	5.30	6.83	Yes	No
		THGA	Instant	2.96	5.81	Yes	No
OPay	Orientation	Accelerometer, Gyroscope	0.228	4.76	0.96-15.24	Yes	Yes

Table 4: Comparing OPay with other solutions

to use the GPS data to ensure the card and the reader are in the same location. Shrestha et al. [25] proposed to measure the ambient environment using a range of sensors, including temperature (T), gas (G), humidity (H), and altitude (A). They further proposed to combine the sensors to improve results, e.g., GA which combines gas and altitude. Other combinations include HGA and THGA. Instead of measuring the natural environment, Gurulian et al. [15] proposed to use infrared light to create an artificial ambient environment (AAE) and the infrared sensor to measure the environment. In a follow-up work [17], they proposed a similar solution of using vibration as an alternative AAE and six AAE sensors (accelerometer, gravity, gyroscope, linear acceleration, magnetic field, and rotation vector) to measure the surrounding environment.

While these ambient-sensors-based solutions can detect PR attacks when the card and remote terminal are located in two distinct environments, they have two limitations. First, the ambient environment is not a secret and can be easily manipulated as demonstrated by Truong et al. [30]. In an MP attack, the attacker has the freedom to manipulate the sounding environment of the mPoS device. For example, if the victim's card is kept in a bag and a light sensor is used to sense the ambient environment, the attacker can use a piece of clothing to wrap around the terminal to easily create the same dark ambient environment. Second, these solutions are generally designed for the scenario that the card and the reader are located in two remote locations with distinct environments, and therefore would not work when the devices are located in the same place, e.g., in an mPoS-based passive attack.

Comparison. OPay is a new orientation-based solution that does not require an explicit user action nor depends on the ambient environment. The user action involved in the payment is implicit and has been seamlessly integrated into a natural payment process. Therefore, it preserves the existing usage model. Table 4 compares OPay with related works. As compared to other solutions, OPay is reasonably fast, taking only 0.228 seconds in our prototype. The error rates (FRR $= 4.76\%$, FAR $= 0.96\%$ for the random guessing attack and FAR $= 15.24\%$ for the target guessing attack) present a reasonable trade-off in security and usability. It substantially reduces the chance of a successful attack with little inconvenience to users in a legitimate transaction. Some other works report better error rates than ours. However, we should highlight that a direct comparison of the error rates may not be appropriate since the test conditions are different. As an example, in Czeskis et al. [5], although the authors reported 0% FRR and 0% FAR, their user study involved only three participants, and all three participants were trained to practice a certain handshake before starting the experiments. In our user study, none of the twenty participants had any prior training on how to use OPay. They were asked to make a simulated contactless payment as they would normally do in a real-life transaction. In general, ambient environment-based solutions preserve the existing usage model but are not effective when the attacker's device and the victim's card have the same or similar environment, or share the same location. Solutions based on user activation can prevent the same environment/location attacks but change the existing usage model. To our best knowledge, OPay is the first solution that protects not only PR attacks but also MP attacks where the attacker is in the same environment or location as the victim, while preserving the existing usage model.

6 Discussion

Feasibility of adding sensors: As shown in Table 4, using sensors is common in the proposed solutions to prevent passive attacks in contactless payments. The main research question pursued in this paper is to identify which set of sensors we

should use to prevent attacks without changing the existing usage model. We note that some commercialized bank cards have already been equipped with sensors, e.g., fingerprint sensor in Mastercard Biometric Card[7], which shows the feasibility of embedding sensors on bank cards. (However, note that the Master Biometric card requires the user to press the fingerprint sensor to make a payment, hence changing the existing usage model.)

Usability: SUS is a widely used framework to assess users' satisfaction with the usability of computer systems [3]. It has been used in previous studies [19, 20] to compare the usability among similar systems for pairing. We chose SUS over other usability tests such as Single Ease Question (SEQ) in order to establish a comparable benchmark for the usability of contactless payment systems. In our user study, we decided to use the original SUS questions without modification [3]. Users generally found the questions easy to understand. However, some users were puzzled by the word "inconsistency" in Q6 and "cumbersome" in Q8 (see Table 3), which shows a limitation of using SUS in our usability study. However, it is well-known that SUS questions are phrased for general purposes, and in a specific context, users may occasionally find the wording of some questions to not fit exactly [3].

Extension: In future, we plan to investigate the feasibility of using OPay for wearable payment devices such as NFC-enabled jewellery and key fobs that are vulnerable to both PR and MP attacks. Applying OPay to these devices requires some adaptation of the definition of orientation for each device as the usage model varies with different payment devices.

7 Conclusion

In this paper, we proposed OPay, a novel orientation-based solution to prevent both passive replay attacks and mPoS-based passive attacks against contactless payment devices. We built a concrete prototype and conducted a user study to evaluate its feasibility. The users generally found our solution as easy-to-use as in a normal contactless payment experience; it was sufficiently fast, taking only 0.228 second; it substantially reduced the attack success rate from the currently 100% to between 1-15% with only a small 4.76% false rejection rate. These make OPay a useful solution to fight against fraud in contactless payment systems.

8 Acknowledgement

We thank all the participants who contributed to our experiments. We also thank the anonymous reviewers of this paper.

[7] https://www.mastercard.us/en-us/business/overview/safety-and-security/authentication-services/biometrics/biometrics-card.html

References

[1] Ross Anderson. Security engineering: a guide to building dependable distributed systems. John Wiley & Sons, 2020.

[2] David Basin, Ralf Sasse, and Jorge Toro-Pozo. The emv standard: Break, fix, verify. arXiv preprint arXiv:2006.08249, 2020.

[3] John Brooke. Sus: a "quick and dirty'usability. Usability evaluation in industry, 189, 1996.

[4] Android Central. No, the oneplus 8 pro doesn't have an x-ray camera — here's what's actually happening. Available at https://www.androidcentral.com/no-oneplus-8-pro-doesnt-have-x-ray-camera. Accessed 15 June 2021.

[5] Alexei Czeskis, Karl Koscher, Joshua R Smith, and Tadayoshi Kohno. Rfids and secret handshakes: Defending against ghost-and-leech attacks and unauthorized reads with context-aware communications. In Proceedings of the 15th ACM conference on Computer and communications security, pages 479–490, 2008.

[6] Joeri De Ruiter and Erik Poll. Formal analysis of the emv protocol suite. In Joint Workshop on Theory of Security and Applications, pages 113–129. Springer, 2011.

[7] James Diebel. Representing attitude: Euler angles, unit quaternions, and rotation vectors. Matrix, 58(15-16):1–35, 2006.

[8] Saar Drimer, Steven J Murdoch, et al. Keep your enemies close: Distance bounding against smartcard relay attacks. In USENIX security symposium, volume 312, 2007.

[9] Martin Emms, Budi Arief, Troy Defty, Joseph Hannon, Feng Hao, et al. The dangers of verify pin on contactless cards. School of Computing Science Technical Report Series, 2012.

[10] LLC EMVCo. Emv integrated circuit card specifications for payment systems book 2 security and key management version 4.3, 2011.

[11] United Kingdom Finance. The problems with contactless cards. Available at http://www.contactlesspaymentcards.com/problems-with-contactless-cards.php. Accessed 8 September 2021.

[12] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical nfc peer-to-peer relay attack using mobile phones. In International

Workshop on Radio Frequency Identification: Security and Privacy Issues, pages 35–49. Springer, 2010.

[13] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical relay attack on contactless transactions by using nfc mobile phones. In Radio Frequency Identification System Security, pages 21–32. IOS Press, 2012.

[14] United Kingdom Government. 2021 budget plan. Available at https://www.gov.uk/government/publications/budget-2021-documents. Accessed 01 June 2021.

[15] Iakovos Gurulian, Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes. Preventing relay attacks in mobile transactions using infrared light. In Proceedings of the Symposium on Applied Computing, pages 1724–1731, 2017.

[16] Iakovos Gurulian, Gerhard P Hancke, Konstantinos Markantonakis, and Raja Naeem Akram. May the force be with you: Force-based relay attack detection. In International Conference on Smart Card Research and Advanced Applications, pages 142–159. Springer, 2017.

[17] Iakovos Gurulian, Konstantinos Markantonakis, Eibe Frank, and Raja Naeem Akram. Good vibrations: artificial ambience-based relay attack detection. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pages 481–489. IEEE, 2018.

[18] Tzipora Halevi, Di Ma, Nitesh Saxena, and Tuo Xiang. Secure proximity detection for nfc devices based on ambient sensor data. In European Symposium on Research in Computer Security, pages 379–396. Springer, 2012.

[19] Rong Jin, Liu Shi, Kai Zeng, Amit Pande, and Prasant Mohapatra. Magpairing: Pairing smartphones in close proximity using magnetometers. IEEE Transactions on Information Forensics and Security, 11(6):1306–1320, 2015.

[20] Alfred Kobsa, Rahim Sonawalla, Gene Tsudik, Ersin Uzun, and Yang Wang. Serial hook-ups: a comparative usability study of secure device pairing methods. In Proceedings of the 5th Symposium on Usable Privacy and Security, pages 1–12, 2009.

[21] M Kok, JD Hol, and TB Sch"on. Using inertial sensors for position and orientation estimation. Foundations and Trends in Signal Processing, 11:1–153, 2017.

[22] Di Ma, Nitesh Saxena, Tuo Xiang, and Yan Zhu. Location-aware and safer cards: enhancing rfid security and privacy via location sensing. IEEE transactions on dependable and secure computing, 10(2):57–69, 2012.

[23] Maryam Mehrnezhad, Feng Hao, and Siamak F Shahandashti. Tap-tap and pay (ttp): Preventing the mafia attack in nfc payment. In International Conference on Research in Security Standardisation, pages 21–39. Springer, 2015.

[24] Sazzadur Rahaman, Gang Wang, and Danfeng Yao. Security certification in payment card industry: Testbeds, measurements, and recommendations. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pages 481–498, 2019.

[25] Babins Shrestha, Nitesh Saxena, Hien Thi Thu Truong, and N Asokan. Drone to the rescue: Relay-resilient authentication using ambient multi-sensing. In International Conference on Financial Cryptography and Data Security, pages 349–364. Springer, 2014.

[26] Babins Shrestha, Nitesh Saxena, Hien Thi Thu Truong, and N Asokan. Sensor-based proximity detection in the face of active adversaries. IEEE Transactions on Mobile Computing, 18(2):444–457, 2018.

[27] Luigi Sportiello and Andrea Ciardulli. Long distance relay attack. In International Workshop on Radio Frequency Identification: Security and Privacy Issues, pages 69–85. Springer, 2013.

[28] Douglas R Stinson. Cryptography: theory and practice. Chapman and Hall/CRC, 2005.

[29] Ahren Studer, Timothy Passaro, and Lujo Bauer. Don't bump, shake on it: The exploitation of a popular accelerometer-based smart phone exchange and its secure replacement. In Proceedings of the 27th Annual Computer Security Applications Conference, pages 333–342, 2011.

[30] Hien Thi Thu Truong, Xiang Gao, Babins Shrestha, Nitesh Saxena, N Asokan, and Petteri Nurmi. Comparing and fusing different sensor modalities for relay attack resistance in zero-interaction authentication. In 2014 IEEE International Conference on Pervasive Computing and Communications (PerCom), pages 163–171. IEEE, 2014.