Context-based Co-presence Detection Techniques: A Survey

Mauro Conti[†], and Chhagan Lal[‡]
Department of Mathematics, University of Padua, Padua, Italy [†‡]
Department of Computer Science and Engineering, Manipal University Jaipur, Jaipur, India[‡]
Email:[†]conti@math.unipd.it, [‡]chhagan@math.unipd.it, [‡]Corresponding Author

***Abstract*—In this paper, we present a systematic survey on the contextual information based proximity detection techniques. These techniques are heavily used for improving security and usability in Zero-Interaction based Co-presence Detection and Authentication (ZICDA) systems. In particular, this survey includes a discussion on the possible adversary and communication models along with the existing security attacks on ZICDA systems. It also reviews the state-of-the-art proximity detection techniques that make use of contextual information. The proximity detection techniques are commonly referred as *Contextual Co-presence* (COCO) protocols. The COCO protocols dynamically collect and use contextual information to improve the security of ZICDA systems during the proximity verification process. Finally, we summarize the significant challenges and suggest possible innovative and efficient future solutions for securely detecting co-presence between devices in the presence of adversaries. The proximity verification techniques presented in the literature usually involve several trade-offs between metrics such as efficiency, security, deployment cost, and usability. At present, there is no ideal solution which adequately addresses the trade-off between these metrics. Therefore, we trust that this review gives an insight into the strengths and shortcomings of the known research methodologies and pave the way for the design of future practical, secure, and efficient solutions.**

***Index Terms*—Relay attack, Zero-interaction authentication, Context-aware, Sensor modalities, Distance bounding, RFID, Proximity detection.**

I. Introduction

Nowadays, there are many industrial applications which grant specific services and privileges based on the physical proximity of the communicating devices. For instance, we use a contactless smart key to unlock our car, even to start the engine without inserting the key. These industrial applications use the most popular short-range communication technologies known as Radio Frequency Identification (RFID) [1] and Near Field Communication (NFC) [2], for establishing contact between the communicating pairs. Other widely used applications that use short-range contactless smartcards that are based on RFID or NFC includes supply chain management, e-passport [3], access cards (such as building, parking, highway toll fee collection and public transport [4]), medical implants, Point-of-Sale (PoS) systems [5], to name a few. Moreover, the smartcard-based access control systems that require proximity verification and authentication are also being deployed in safety and security-critical infrastructures such as military research facilities and nuclear power plants. Therefore, it is essential to secure such systems against all types of adversaries. The main reason for the popularity of contactless authentication systems compared to contact-based smartcard systems is their higher overall user experience concerning ease in manageability and usability. However, due to the inherent weaknesses in underlying wireless communication, the RFID/NFC systems are exposed to a wide variety of security and privacy attacks [6]. Thus, it subverts the security and usability advantages offered by these authentication systems.

The so-called relay attacks are one of the many distance hijacking attacks that exploit the radio communication technology of RFID/NFC systems [7] [8] [9]. In relay attacks, a proxy device (often referred to as *ghost*) that emulates a contactless smartcard is placed near the reader to impersonate a victim's card within the proximity to the reader. On the other end of communication point, a mole (often referred to as *leech*) acts as a reader is placed near to the victim card [10]. Both of these malicious devices are in control of an adversary. The proxy forwards all the messages to the mole which act as a fake authentic reader for the victim card. The distance between the proxy and mole can be increased as far as the communication delay is kept sufficiently short. Example of instances that show the vast existence of relay attacks are demonstrated in [11]. Authors in [11] show a successful relay attack over more than 300 miles, and the authors in [8] demonstrate relay attacks on passive keyless entry and start for over 50 meters. Furthermore, in [12], the successful relay attacks over more than 110 meters are shown using three NFC smartphones.

To overcome the above mentioned inherent vulnerabilities and attacks on contactless communication systems, various researchers are working towards different defense techniques. The proposed techniques try to preserve the fundamental properties such as zero-interaction and usability of the systems while ensuring the protection from the distance hijacking attacks. The two most commonly found defense techniques in the state-of-the-art are the contextual co-presence [13] [14] and the distance bounding [15] [16] [17] protocols. Both these protocols provide zero-interaction authentication [18] by using co-presence detection as an additional security measure on the top of the basic authentication process.

In this paper, the co-presence detection techniques that are based on distance bounding protocols are considered out of the scope. We aim to review only the applications that make use of resource-constrained (e.g., smartcards and smart keys) and commodity devices (e.g., smartphones and tablets) as provers and verifiers. However, the distance bounding needs to be

implemented at the lowest possible layer in the communication stack. It is because even a small error in estimating processing time at the prover-side can lead to significant deviations in the distance bound. Thus, implementing distance bounding on commodity devices like ordinary smartphones might be a challenge. However, we direct the interested readers toward the following comprehensive distance bounding research works [19] [20].

A. Motivation and Contributions

Considering the higher potential damage such as an unauthorized entry in a secure and sensitive facility, stealing a car, credit card frauds, and skipping tolls, which could be caused by exploiting the vulnerabilities in co-presence systems. Thus, these systems require robust and secure authentication models. Over the years, researchers have proposed many solutions based on distance bounding and context-aware information protocols, which develop patches to fix the identified vulnerabilities. To the best of our knowledge, this is the first attempt which provides an extensive overview of the attacks and their prevention techniques for ZICDA access control systems. However, some efforts have been made to describe the problem and its possible solutions within one specific protocol such as distance bounding protocols for distance-based attacks [19], or within a particular communication technology like RFID [21]. But, these state-of-the-art survey articles does not sufficiently cover the details of all the ongoing attacks and their proposed solutions on proximity-based systems. For instance, in [22], authors discuss the feasibility of implementation and the corresponding security implications for various active and passive relay attacks. Also, in [23], the authors present a brief survey on multiple attacks and their countermeasures using distance bounding protocols with IEEE 802.15.4a (i.e., Impulse Radio Ultra-Wideband). Furthermore, [22] and [23] are outdated given the extensive research that has been done in the last few years on the security of co-presence systems. It is because the attack vector has been increased significantly in recent years due to the rapid deployment of zero-interaction systems in various real-world scenarios (e.g., health-care, PoS, and keyless car entry). Hence, we firmly believe that a comprehensive survey is essential for an audience who plans to initiate their research work in this direction. Our paper does not attempt to solve any new challenges but presents an overview and discussion on security threats and their countermeasures in ZICDA systems. We believe that we have taken here the required initial steps that will help understand how to maximize the use of contextual information to provide flexibility, and to strengthen decision making in access control systems.

In this paper, we provide the first comprehensive survey on co-presence detection techniques. To this end, the significant contributions of our work are as follows.

- We discuss the critical security problems that affect the use of contactless smartcards in ZICDA systems. We review security threats, vulnerabilities, and attacks specific to these systems. In particular, we survey the literature over the period 2000-2018 by focusing our attention on the impact analysis of security attacks performed on ZICDA systems.
- We present a general architecture for ZICDA system, which includes its characteristics, deployment challenges, and applications. Furthermore, we discuss the communication and adversary system models that are being used in ZICDA systems. In particular, we assist interested readers in understanding the existing challenges in the deployment of ZICDA systems, estimate the possible damages caused by the adversaries, and improve the techniques for proximity detection and containment processes. Furthermore, we provide an overview concerning feasibility, robustness, and effectiveness for the existing and potential attacks over ZICDA systems, and we examine the risks for users of these systems.
- Finally, we present a survey of the state-of-the-art security solutions for detecting co-presence using contextual information (i.e., contextual co-presence protocols). We further extend our study by including the co-presence detection techniques that also emphasize on the importance of privacy preservation during the access control authentication process in Location-Based Services (LBS). Please note that in this paper only context-aware security solutions for ZICDA systems have been considered for the survey process. We have not surveyed the context-aware solutions that are being used for improving the security and privacy of users in other application domains such as mobile applications [24] [25], Internet of Things (IoT) [26], Industrial IoT [27], and future wireless networks [28]. Additionally, we discuss how the existing approaches ensure fundamental security requirements and protect communications in the ZICDA systems. Finally, we present the open challenges and strategies for future research work in the area.

B. Organization

The rest of the paper is organized as follows. In Section II, we present the overview of ZICDA systems, which include its characteristics and applications. In the same section, we also discuss details about communication model, authentication system, and adversary model used for proximity verification of communicating devices in a ZICDA system. Furthermore, at the end of the Section II, we discuss all the existing attacks and their impacts on the ZICDA systems. In Section III, we review existing solutions, which are proposed for detecting the co-presence between the communicating devices. We broadly discuss the proximity detection techniques that are based on contextual co-presence protocols. In Section IV, we present open issues and directions for future work. Finally, Section V concludes our work.

II. Zero-Interaction based Co-presence Detection and Authentication

In this section, we present the overview of a generic functional model of Zero-Interaction based co-presence Detection and Authentication (ZICDA) access control system. First, we introduce the deployment techniques that have been used in a

ZICDA system. Then, we discuss the standard communication and adversary model for ZICDA systems.

A. Overview of ZICDA system

A ZICDA system represents a specific set of contactless access control systems in which the access-seeking entity (e.g., smartcard, smartkey, and smartphone) will implicitly prove their co-presence with the verifier along with its authentication credentials. For instance, Passive Keyless Entry (PKE) system, which is also named as "Smartkey" system is an automobile's electronic lock to its doors and ignition system. In PKE system, the driver carries a token (i.e., smartkey) that communicates (using RFID technology) with car's access control system to unlock the doors and activate the ignition, only if, the token's authenticity and proximity are successfully verified.

Verifying the proximity along with the authenticity is necessary for ZICDA systems. Otherwise, these systems become vulnerable to various type of Man-In-the-Middle (MIM) attacks such as eavesdropping, distance-hijacking, data corruption and manipulation, and relay attacks. One way to detect proximity is through received signal strength, but an adversary can easily manipulate signal strength through active relays. Authors in [21] provide study depicting that different types of proximity-based access control systems are susceptible to MIM attacks. Mainly, the relay attacks are successful in ten car models from eight different vendors [8]. In addition to vehicular systems, these attacks can easily target credit/debit cards and smartphones, which uses NFC technology and contactless smartcards.

B. Communication Technologies

In ZICDA systems, due to the resource-constrained nature of prover (e.g., smartcard and smartkey), the following three short-range and low-energy sensor technologies are commonly used for communication between prover and verifier: (i) Radio Frequency Identification (RFID), (ii) Near Field Communication (NFC), and (iii) Bluetooth Low Energy (BLE). Among these three, NFC is used in a large array of applications because it combines the security of BLE with the short-range data transfer capabilities of RFID. For NFC to work, one must tap or wave the smartphone (acts as NFC reader) against an NFC tag to secure an object's context or to perform an action. For example, you could purchase chocolates just by tapping your NFC reader against the box of chocolates. NFC-capable devices such as a smartphone can work as a reader as well as a tag. It is predicted that NFC will be used as a key technology in realizing the Internet of Things (IoT) [29] paradigm. It is due to the enhanced security features of NFC such as a user can easily pair an NFC tag with another form of authentication on hand (like the license in your wallet) to create a two-pronged authentication system. The above feature is particularly relevant in the health-care world [30], and it is even being mandated by the Drug Enforcement Administration (DEA) as a standard security practice.

NFC is generally viewed as a finely honed subset of Radio Frequency Identification (RFID). NFC operates at the same frequency (i.e., 13.56 MHz) as high-frequency RFIDs, and it performs many of the similar operations as RFID tags (and readers) and contactless smartcards. The NFC can operate in the following communication modes.

- Read/Write: In this mode, an NFC-enabled reader/writer device (such as a smartphone) can read information from the smart objects, and act upon the received information to improve services provided by these smart objects. By performing a simple touch of these devices to the smart objects, the users can perform various tasks such as short message service (SMS) texts without typing, automatically connect to websites via a retrieved URL, and get information about various relevant offers or obtain coupons. This mode is beneficial for realizing the Internet of Things (IoT) services.
- Peer-to-Peer: In this mode, one NFC-enabled reader/writer device can communicate with another NFC-enabled reader/writer device. One of the reader/writer devices behaves as a tag to create the communication link.
- Card emulation: While working in this mode, an NFC-enabled reader/writer device can replace a contactless smartcard, which enables NFC devices to be used within the existing smartcard infrastructure for services such as making payments at PoS, access control at building entrance or for a vehicle, toll gates, and medical implants.

As NFC is a subset of RFID, the standards and protocols for NFC are based on RFID standards as outlined in FeliCa, ISO/IEC 14443 [31] and some are parts of ISO/IEC 18092. These standards govern the use of proximity cards using RFID technology.

C. Communication and Adversary Models

Figure 1 shows a generic communication model for ZICDA systems. The communication model consists of two devices namely prover (P) and verifier (V). To get access to the system, P has to authenticate itself to V and also prove that P is in close proximity to V. The authentication process between the devices, i.e., P and V, triggers automatically when both devices are nearby to each other. The communication traffic between P and V is encrypted using a pre-shared secret key, which is generated using either shared-key or private/public key model. The P encrypt its authentication information using the secret key before transmitting it to V. Depending upon the application and system implementation, a "credential verification" function make the authentication decision for P at V either locally or remotely as shown in Figure 1. For example, in a PoS application, a user (i.e., P) performs the contactless payment using her NFC-enabled smartphone at a PoS terminal. In this specific application, the "credential verification" function is stored at the web server of a bank whose credit card is being used for the payment at PoS terminal. Other applications such as locking/unlocking a car using a smartkey, where the "credential verification" function is integrated with the terminal device itself. In ZICDA access control systems, the smartcard (i.e., a user token such as an access card, key or mobile phone) acts as P, and the terminal

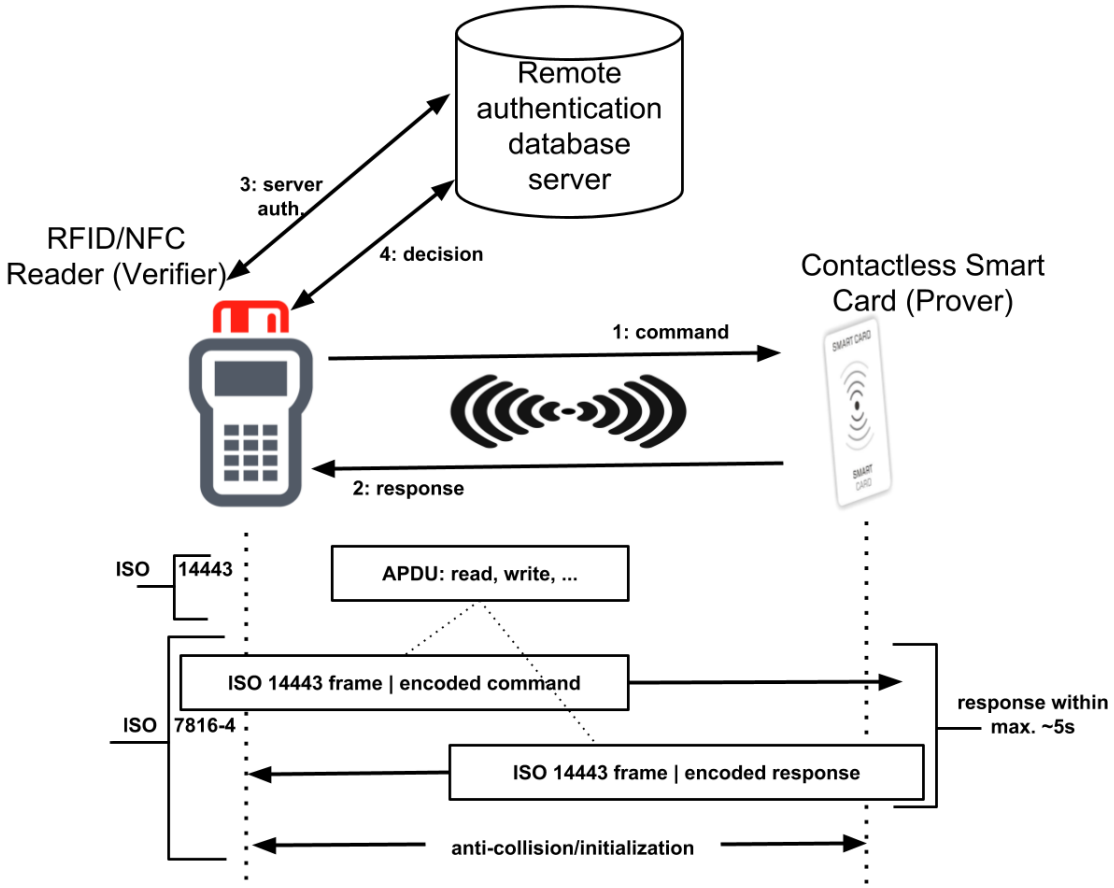


Fig. 1. Communication model for ZICDA systems

(i.e., a desktop computer, wall-mounted device or car system) plays the role of V.

The adversary model for ZICDA systems is shown in Figure 2. We assume that an adversary possesses following standard Dolev-Yao [32] features and capabilities: a) adversary (A) has complete control over the communication channel used for authentication process between P and V, and b) A has no physical access or possession of P and V, nor can A compromise the functionality of P and V devices. Therefore, none of the benign entities in the communication protocol of ZICDA system can be tampered with or compromised. However, A is allowed to stay close to V and P. The main aim of A is to fool V into concluding that P is in proximity.

Figure 2 illustrates that an adversary (A) which resides in the proximity of P and V can perform various types of distance hijacking (i.e., distance-reduction or distance-enlargement) attacks on the wireless channel between P and V. First, A can intelligently place one device, called mole (A_v), in the proximity to P without P knowing about it. Then, A places another device called, proxy (A_p), close to V which emulates a contactless smartcard. Both A_v and A_p communicate using a high bandwidth channel. In this way, A takes the form of a "mole-and-proxy" (or often called "ghost-and-leech") duo (A_v, A_p), and it relays messages to and forth between V and P. This process leads V to conclude that P is in proximity and vice-versa. Therefore, such a simple adversary model can fully compromise the security and privacy of an ordinary ZICDA system without requiring any physical access to the communicating devices nor does it requires the authentication credentials.

D. Attacks vector for ZICDA Systems

Due to technological advancements in mobile devices and radio frequency communications, a broad array of applications such as contactless payments, keyless entry systems, smart posters, to name a few, are deployed rapidly for mass-market users. These applications use contactless authentication along with the proximity verification between the communicating devices for ensuring secure access control. The increased overall user experience regarding ease in manageability and usability are the main attractions of these applications. Unfortunately, the radio channel used for communication is vulnerable to various security and privacy attacks such as eavesdropping [33], relay attack [34] [35], impersonation [36], and distance hijacking [37]. Thus, these attacks limit the usability of co-presence techniques in various application domains. To provide security against all types of attacks in ZICDA systems is a challenging task. Ideally, a ZICDA system

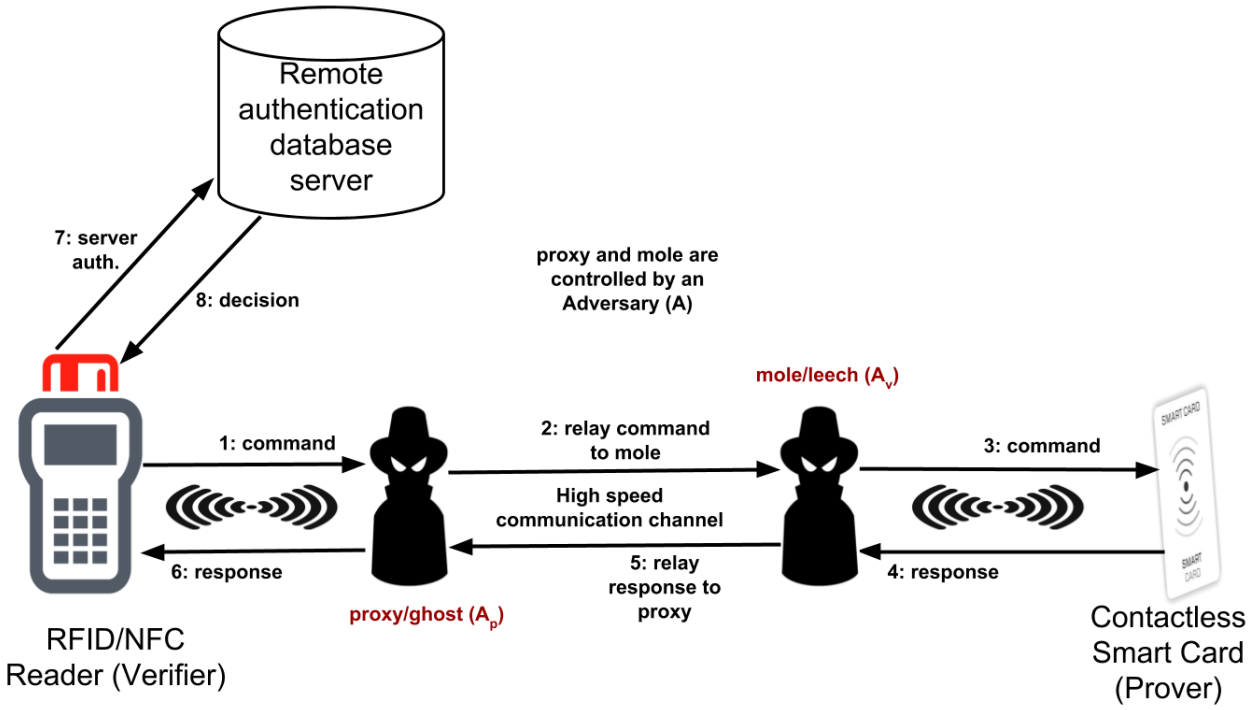


Fig. 2. Adversary model for ZICDA systems

should be protected against the following attacks.

- *Mafia fraud: Mafia fraud* attack [38], also called relay or wormhole attack is first introduced by [39] and [40]. In this attack, the V and P are honest and far apart, and an adversary tries to shorten the physical distance between them. The adversary uses a similar attack scenario as described in Figure 2, the attacker places a proxy verifier (V') near P and a proxy prover (P') near V. These proxies create an extended high bandwidth communication link between V and P by relaying all the communication messages between them. In this way, P' and V' make V and P to falsely conclude that both are in close proximity. Traditional cryptographic-based security techniques cannot prevent the *Mafia fraud* attacks because the proxies (i.e., P' and V') need not to perform any decryption or encryption on communication messages nor they require to run any authentication process with V and P. Thus, these proxies can create an effective, transparent communication link between V and P. This attack has been successfully demonstrated in various ZICDA Systems in which NFC/RFID techniques are used for communication between V and P.
- *Distance fraud:* In *Distance fraud* attacks [15], a sole fraudulent prover (P') convince the honest verifier (V) that she is at a different (usually shorter) distance than she really is. Unlike *Mafia fraud* attack, here the prover itself is dishonest, and only the verifier is a victim. *Distance fraud* attacks are most effective and disastrous for real-time location-based systems (RTLS)[1]. Application instances of RTLS include manufacturing, logistics, and supply chain management, where expensive components or parts of a final product and other important entities involved are being tracked throughout the whole logistics process. A practical example of how *Distance fraud* attacks can adversely affect the RTLS is shown in Figure 3. In this scenario, three nodes (i.e., Vx, Vy and Vz) perform continuous tracking of the current location of the node P using its received signal strength. We can see from Figure 3 that if node P wants to be malicious, it could pretend to be at position P' at the same time when it is at P. To perform this action, P decreases its signal strength when communicating with node Vz while it increases the signal strength when communicating with Vy. In this case, the verifier nodes Vy and Vz are unable to detect the fraud of P because she is a legitimate node,

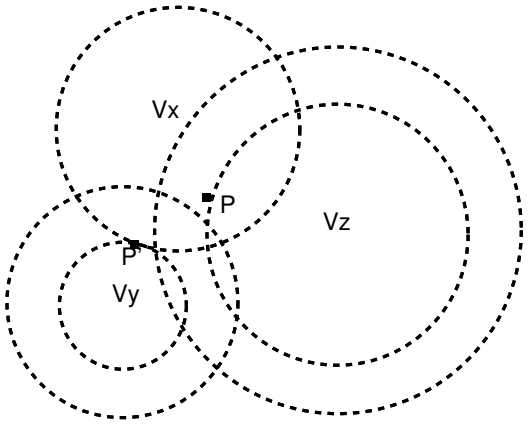


Fig. 3. Distance fraud attack

[1]RTLS are automated systems that determine the locations of assets.

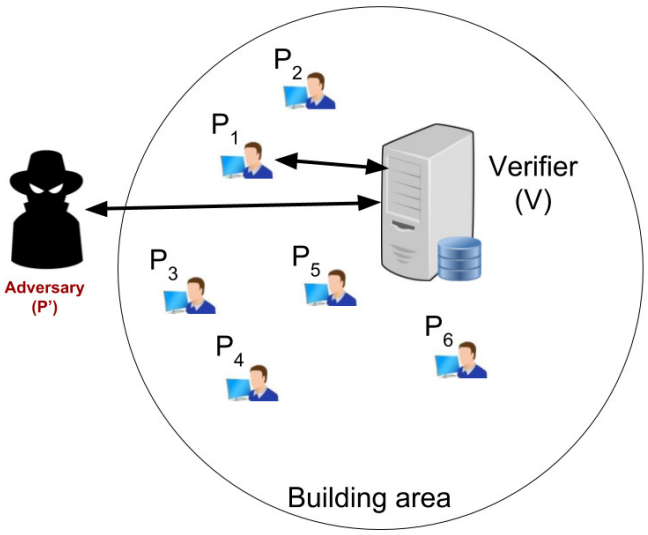


Fig. 4. Distance-hijacking attack

and she authenticates herself with true credentials.

- *Terrorist fraud:* A slightly different version of *Distance fraud* attack in which a dishonest prover (P') attacks the system with the help of a third party attacker (A) is called *Terrorist fraud* [41]. In *Terrorist fraud* attack, the P', which is far apart from an honest verifier (V), conspires with A, who is close to V to masquerade as the honest prover by providing A with selected credentials for authentication. Let's consider an example, assume that A is a terrorist who wants to cross the border. P' helps A in answering the questions of the immigration officer (i.e., V). Another example could be the one in which A help P' in applications such as location forging. Assume a scenario involving electronic monitoring using an ankle bracelet. *Terrorist fraud* attack enables the subject (i.e., P') of the electronic monitoring system (i.e., V) to leave her residence with the help of A who stays close to V.
- *Distance-hijacking:* In Distance-hijacking attack [37], a dishonest far-away prover (P') exploits one or more honest close-by provers' $\{P_1, P_2, \cdots, P_n\}$ to provide a verifier V with false information about the distance between P' and V. Consider a real-world scenario as shown in Figure 4, in which several employees (i.e., $\{P_1, P_2, \cdots, P_n\}$) work in a secure building. A mainframe system (i.e., V) containing sensitive information is located inside the building. Any authorized employee can get access to V through their contactless smartcard. To complete the authorization process with V, an employee needs to be in the building along with her valid credentials. Now, assume that an adversary (P'), which has a (stolen) smartcard is sitting outside the building along with a powerful antenna. To access V, P' already has the valid security credentials, but P' also need to prove that she is inside the building. For this purpose, P' performs eavesdropping over the communication channel of the distance bounding protocol, which is running between the employee P_1 and V. Distance bounding works in two phases; in the first phase, the P needs to prove to V that both are in proximity to each other. After successful completion of the first phase, P authenticates itself to V using valid credentials. To perform distance-hijacking attack, P' jam the communication link between P_1 and V as soon as the first phase of the distance bounding is completed. Then P' will complete the second phase on behalf of P_1 using her (stolen) credentials. In this way, V now believes that the P' is in the building with valid credentials, thus she is granted the access.
- *Location cheating [42]:* It is a colluding attack in which a close-by helper and a far-away dishonest prover (P') collude to prove that P' is close to verifier (V). Location-based services (LBS) led by foursquare[2], GasBuddy[3], GyPSii[4], Loopt[5], and Dark Sky[6] has attracted a lot of attention in recent years. The LBS uses the geographical position of a user to enrich user experience in a variety of contexts such as location-based searching and location-based mobile advertising. To attract more users, the location-based mobile social networking services provide rewards and offers to the user when it checks into certain venues or locations. This gives incentives to users to engage in location-cheating for their benefits. Dishonest provers may obtain undeserving benefits at specific venues (i.e., places like coffee shops, restaurants, shopping malls, to name a few) by making multiple false location check-ins at different times.
  For example, Foursquare connect users to local businesses like shops or restaurants by using their current location information. Many business owners offer concrete benefits such as free vouchers, special offers, and cash rewards to the most active registrants visiting their shops or restaurants. In such a scenario, a P' can perform location-cheating attack by taking help from her friend sitting in or near a restaurant. The close-by helper of P' will use the credentials of P' and prove her presence along with the authentication to trick the V. A vast array of LBS services use GPS locations that can be obtained from a user's smartphone. In such services, a user performs location-cheating [42] by exploring the open source operating systems of smartphones (e.g., Android) to modify global-positioning-system-(GPS)-related application programming interfaces (APIs). Once tempering is done, a user can cheat on her location using falsified GPS information.

III. Context-aware Co-presence Detection Techniques

In this section, we present a comprehensive survey of existing context-based co-presence detection techniques that address one or more security threats discussed in Section II-D. The basis of provisioning contextual security in ZICDA systems is the fact that all devices residing in the proximity

[2]http://www.foursquare.com
[3]https://www.gasbuddy.com/
[4]http://www.gypsii.com
[5]http://www.loopt.com
[6]https://darksky.net/app/

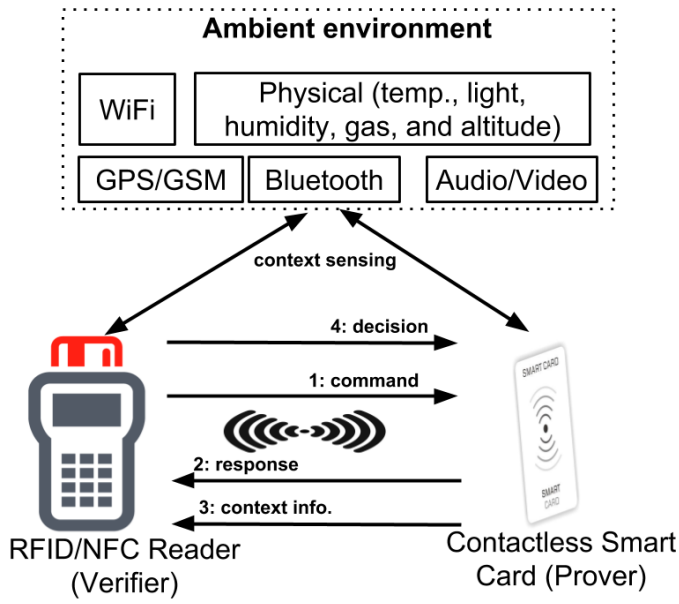


Fig. 5. Context-based co-presence Detection System

with each other will always "see" (nearly) the same physical and ambient environment (i.e., availability of suitable context). With the recent advancements in the hardware of mobile devices, these devices are now equipped with one or more inbuilt "sensors" such as microphones (for audio), wireless networking interfaces (for WiFi connectivity), global positioning system (for location), Bluetooth (for short-range communications), and other physical environment sensors (humidity, gas, temperature and pressure/altitude). The data collected using these sensors can be used as supplemental information to improve security decisions in ZICDA systems. With the information extracted from these sensors, the security decisions can be taken dynamically at the time the decisions are made. For this purpose, during the authentication process in ZICDA systems, two honest communicating devices can exchange and compare the dynamically gathered supplemental information to determine their co-presence towards each other.

A. System Model for Context-based Access Control in ZICDA Systems

Figure 5 depicts the generic system model for ZICDA systems that are based on contextual co-presence detection techniques. The main aim of most of the context-based ZICDA systems is to provide security against relay attacks. We can see from Figure 5 that the P and V will "see" (almost) the same ambient environment if they lie in close proximity. When either one of them leaves their common ambient environment, the context gathered by P and V will not match during the co-presence detection process, and the access to the system will be denied (please refer to Figure 5).

The general working methodology framework for ZICDA system models is shown in Figure 5. The framework functions in two phases, in the first phase, when a P enters in the transmission range (aka proximity) of a V, P sends a trigger to V. Once triggered, V start the authentication process with P by sending one (or more) challenge(s) (ch) to P, upon reception of ch, P generate (using her private key) a response (rsp) and send the rsp back to V. After successful authentication, in the second phase, V and P initiate a context sensing process for a pre-defined set of contexts for a fixed duration of t. The context information collected by P within duration t can be represented by a vector (ρ) such that $\rho = \{\rho_1, \rho_2, \rho_3 \cdots \rho_n\}$, where n is the number of sensor modalities used to form the contextual information. Similarly, $\nu = \{\nu_1, \nu_2, \nu_3 \cdots \nu_n\}$ is the corresponding vector of n sensor modalities collected by V. Based on the similarity index calculated using vectors ρ and ν at V, the access of P to the system is either allowed or denied. The effectiveness and correctness of the calculations for the similarity index at V depends upon the feature extraction, classification, and machine learning methods used in the process. The use of contextual security in the authentication process not only improves the security of the system but also provides flexibility in access control decisions.

A point worth mentioning here is the "initial delay" in authentication process incurred due to the use of contextual security. Due to this, a trade-off arises between system access delay and its usability, i.e., a high delay will lead to lower usability and vice-versa. This initial delay can be minimized to some extent using the following approaches: (i) reduce the number of context during the context-aware authentication. However, it will decrease the level of security provided by the system, and (ii) V can perform the credential and contextual authentication processes for P in parallel, but if P uses a low battery power device for authentication then this method posses a high energy consumption and P needs to perform frequent recharges, thus it reduces the usability of the system.

B. Context-based Co-presence Detection Framework

The basic requirements to achieve contextual security in any access control system are (i) availability of contextual information, (ii) efficient integration of available contextual information in runtime, and (iii) instant availability of contextual information to security analysts. In practice, a typical major obstacle in incorporating context into a security monitoring program is the availability of the contextual information in a format that supports integration with log and alert data. Additionally, the contextual information needs to be validated to ensure that it is accurate and has integrity. The ideal platform integrates the data and information in real or near real-time to allow not just the linkage of the data and knowledge efficiently and effectively, but it also enables rules and complex event processing that occurs due to the use of contextual information. Finally, the platform must have the capability to make the integrated information quickly and readily available to security analysts to present a "scenario" (as discussed in the earlier contactless smartcard examples) that provides all of the information required to validate, respond to, and mitigate incidents.

Figure 6 shows the interaction between the major components involved in a generic Contextual Co-presence Security Framework (CCSF). The existing proximity detection techniques either use the whole or parts of the CCSF to verify the

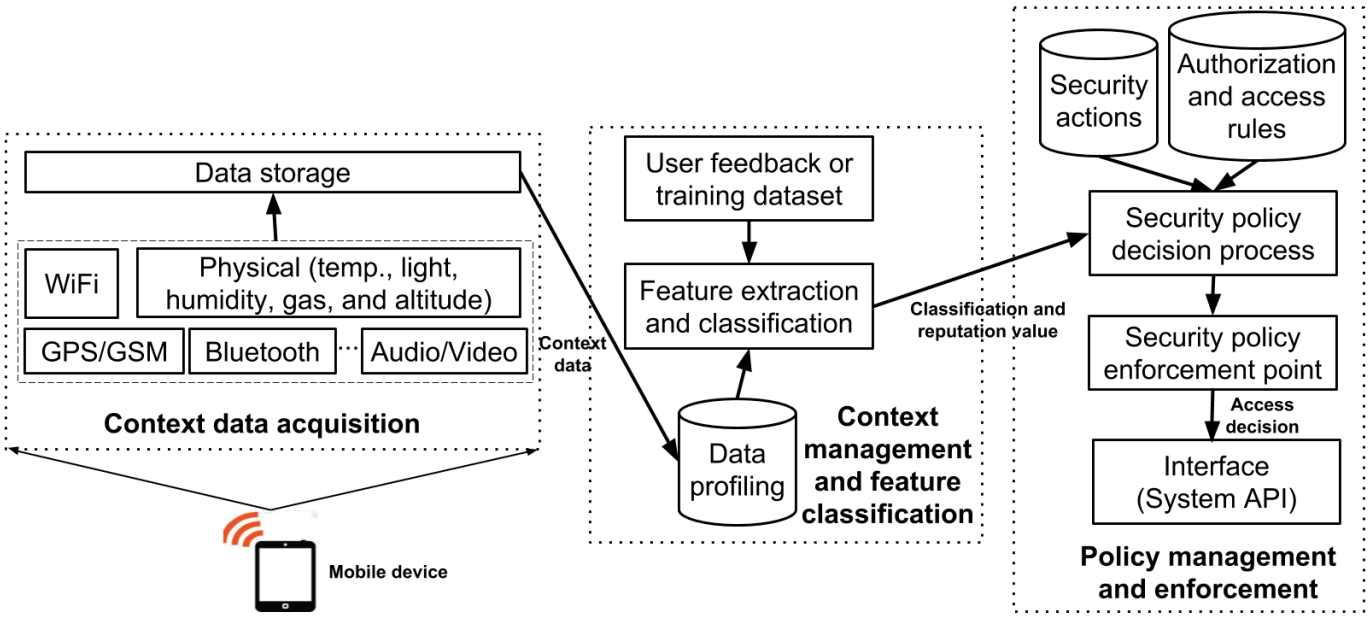


Fig. 6. Overview of a Generic Contextual Co-presence Security Framework

co-presence between the communicating devices. The CCSF apply context profiling and machine learning algorithms on real-world reference dataset that is collected in an uncontrolled environment, and it evaluates the effectiveness of automatic and adaptive context classification for detecting co-presence. For an access control system, the CCSF architecture is used for training the classifier using the ground truth data. The trained classifier will then used as a context comparator to compare the contextual data that is received from a prover and verifier at runtime. The CCSF can be instantiated depending upon the requirements and applications of the underlying access control system. We can see in Figure 6 that the CCSF mainly consists of three major components namely, context data acquisition, context management, and feature classification, and policy management and enforcement. Below, we briefly discuss the functioning and interactions among these three components.

- **Context data acquisition:** The CCSF architecture is driven by the contextual information collected by this component. The accuracy of the assessment of co-presence detection depends highly on the data collection and aggregation process used by the data acquisition module. The contextual security refers to the use of additional information (i.e., context) to improve the security at the time when security decisions are made. Therefore, the context data sensing is done dynamically at the time when a decision must be made for an access control system. Depending upon the type of the application, the communicating entities involved in the context-aware authentication process needs to gather a set of predefined contextual data types using their corresponding inbuilt sensors. The sensed data by the verifier and the prover devices is then compared to verify the co-presence between them. The comparator must be trained, in advance, using the ground truth data (or reference data) to provide precise interpretation, analysis, and decision making. The task of collecting the ground truth data is the main aim of the context data acquisition component of CCSF. Once collected, the reference data is passed to the next component of CCSF (called context management and feature classification) for training the classifier.

To gather contextual data, one can install an easy-to-use and secure application on a large number of user devices. The user devices involved in the data collection process could be smartphones, tablets, or a specific purpose device such as [43]. Data collection is a critical phase of the framework because the number and quality of the ground truth data that has been collected have a high impact on the accuracy of the assessment of co-presence detection. Data collection is a time-consuming, expensive, and cumbersome process. To collect the reference data, an onsite assert deployment is required. The data collection could be done using the dedicated users (employees or suppliers) or an approach such as crowd-sourcing, where data collection is done by soliciting contributions from a large group of people (self-selected volunteers or part-time workers). In both cases, the users will have to carry the data collection device with required sensing capabilities (hardware or software). The former approach is expensive, and the collected dataset will be of small size, but the data will be trustworthy and of high quality. While, the latter will collect data that is inexpensive and it will have higher data quantity, but it will be less secure and of low quality. In particular, to build a robust and accurate CCSF, the collected reference data should have characteristics such as high quality and quantity, accuracy, timelinesses, and variability. Furthermore, there are strict government issued guidelines (to support user or information privacy) such as General Data Protection Regulation (GDPR) that needs to be followed during the process of data acquisition. Collecting real-world

reference data to train the classifiers and update them periodically is one of the biggest challenges in context-aware access control systems. Once the training phase is complete and CCSF is ready to use, it is deployed in the corresponding real-world applications. After CCSF system deployment, the data collection component will collect sensor data dynamically, only at the time when a prover asks access for the access control system.

- **Context management and feature classification:** During the context-aware authentication phase the predefined contextual data is collected by prover and verifier devices, and it is sent to the context management and feature classification (CMFC) module. The CMFC module consists of three components: data profiler, classifier, and training dataset. Data profiling will help in quickly and thoroughly unveiling the true content and structure of the observed context data. The profiler will perform completeness, uniqueness, values distribution, range, and pattern analysis on received data to ensure that it is of adequate quality. Once analyzed properly, the profiler identifies the most promising features (i.e., feature selection) to build a feature vector describing the current context of the users. The classifiers such as decisions trees, Support Vector Machine (SVM), and K-Nearest Neighbours can be trained under supervised learning using a reference dataset. Once the training phase is over, the classifier uses the context feature vectors, which are generated by the profiler to classify new observations (i.e., sensor data) concerning the current applications security and privacy-related properties. The classifier outputs the classification estimates and its associated confidence value, and these are forwarded to policy management and enforcement component, which considers them while making access control decisions. The performance of the classifier will directly influence both, security and usability, of the underlying access control system. In particular, the security of a system is determined by the False-Positive rate (i.e., erroneously established co-presence between far-away devices), while the usability is represented by the False-Negative rate (i.e., incorrectly established non-co-presence between nearby devices).
- **Policy management and enforcement:** This component provide final decisions on the on-going context-aware authentication process between prover and verifier devices. The policy management module uses the in-built policies along with the received confidence value to enforce suitable policies on the verifier. Depending on the type and number of policies enforced by this module, different users can receive varying levels of security access on the same access control system. For instance, a server can be only accessed if the user is within its proximity, but once access to the server is granted, different users can have different rights on the functionalities of the server. In such a scenario, the proximity check is coupled with the individual users' security policies, and therefore, the policy enforcement at the time of context-aware authorization is required.

In the next section, we will discuss the state-of-the-art context-aware co-presence detection techniques that utilize, partially or wholly, multiple components from our above-discussed CCSF architecture.

C. Co-presence Detection using Contextual Information

In this section, we discuss the co-presence detection techniques that use contextual information during the proximity verification process to improve the security of the target access control system. The contextual information is collected using one or more sensor modalities that reside in the prover device(s). In recent years, the use of mobile devices for spontaneous communications increases significantly in various applications. Therefore, securing these communications from multiple attacks such as relay attack, eavesdropping, and impersonation becomes a vital precondition. For instance, an attacker can read, relay, and modify messages between communicating peers without either peer suspecting that the communication between them has been tempered. The use of contextual security as an additional layer on top of the traditional security can help to prevent such malicious third party attacks, as apparently, no user want their private information being leaked or tampered with. The primary motivation for the researchers to develop context-aware solutions is the rapidly ongoing technological and hardware advancements that enable many RFID/NFC tags to be equipped with many low-cost sensing capabilities. Over recent years, sensors with various sensing capabilities have been incorporated in RFID tags [77] [78]. For instance, Intel's Wireless Identification and Sensing Platform (WISP) [79] [80] has developed tag with various sensing capabilities, and this extends the use of RFID beyond simple identification. With the help of these advanced RFID devices, one can efficiently provide numerous promising applications for pervasive sensing and computation. It also paves the way towards providing improved security and privacy services by leveraging contextual information from the existing physical environment.

We followed the review methodology provided in Systematic Literature Review (SLR) [81] with a specific focus on research works relevant to context-based co-presence detection techniques in the ZICDA systems. The SLR is employed to carry out a wide-ranging and systematic study of the co-presence detection techniques in the ZICDA systems. We now present the research methodology steps which we have used to gather the required research articles that are included in this survey.

- *Question formalization:* This survey identifies the most related benefits, issues, and challenges in the field of co-presence detection techniques in zero-interaction access control systems. In particular, this paper tries to address the following research questions: (i) what are the applications that could benefit from the context-aware authentication in access control system?, (ii) what types of attacks can be performed on ZICDA systems that could threaten the efficient usage of contextual information to improve the security in these systems?, (iii) Are the state-of-the-art techniques that use context-aware co-presence

TABLE I
CONTEXT-AWARE CO-PRESENCE DETECTION TECHNIQUES - I

Proposals	Communication channel	Sensor modalities	Privacy preservation support	Application specific	Description
[44]	RFID	magnetometers, accelerometer, GPS	No	No	design context-aware selective unlocking mechanisms and secure transaction verification
[45], [46]	RFID/NFC	audio, ambient light	No	No	determine the proximity by correlating certain sensor data extracted from the two devices
[47]	RFID	GPS	Yes	PoS	location-aware secure transaction verification scheme
[48] [49]	RFID	audio	No	PKES	sound-based proximity-detection method
[50]	RFID/NFC	WiFi (radio waves)	No	No	authenticate co-located devices based on their shared radio environment
[51] [52]	RFID/NFC	temperature, single-bit round-trip	N/A	No	elliptic curve-based mutual authentication protocol
[53]	Bluetooth /RFID/NFC	audio, WiFi, and GPS	No	No	comparing and fusing different sensor modalities in ZIA systems
[54] [55]	Bluetooth /NFC	ambient noise and luminosity	No	IoT domains	secure ZIA pairing suitable for IoT and wearable devices
[56]	N/A	GPS, WiFi	Yes	mobile applications	detection against device misuse and sensory malware
[57]	N/A	audio and luminosity	N/A	proofs-of-presence (PoPs)	solutions against context guessing attacks in LBS
[58] [59]	RFID/NFC	accelerometer, gyroscope	N/A	access control systems	authorized reference trajectories on Transparent Authentication (TA) schemes
[60]	WiFi	trajectory through a road network (gyroscope signal, and GPS)	Yes	VANETs	technique to verify the ongoing co-presence of vehicles in an urban environment
[13]	RFID/NFC	WiFi, Bluetooth, GPS, and audio)	No	No	investigate the performance of different sensor modalities for co-presence detection

TABLE II
CONTEXT-AWARE CO-PRESENCE DETECTION TECHNIQUES - II

Proposals	Communication channel	Sensor modalities	Privacy preservation support	Application specific	Description
[61] [62] [63] [64]	Bluetooth/ RFID/NFC	artificial ambient environments (infrared light, sound, etc)	N/A	time-restricted contactless transactions	evaluated the effectiveness of 17 ambient sensors
[65]	N/A	bidirectional sensing and comparing button presses and releases behaviour	N/A	EMV contactless payments	detection based on sensing button presses on the user's smartphone by both transaction devices
[66]	Bluetooth	magnetometer	N/A	device pairing	pairing smartphones by exploiting correlated magnetometer readings
[67] [68] [69]	NFC	accelerometer	No	Yes	PoS and context-based technique to prevent mafia attack in mobile NFC payment
[70]	NFC	audio and light	Yes	payment cards	secure proximity detection techniques
[71]	N/A	electromagnetic signals	Yes	LBS	privacy-preserving proximity testing
[72]	RFID/NFC	ambient temperature, precision gas, humidity, and altitude	No	PoS	use of purely ambient physical sensing capabilities in authentication systems
[73]	RFID/NFC	Features-fusion [53], and decisions-fusion	No	No	systematic assessment of co-presence detection in the presence of context-manipulating attacker
[74]	RFID/NFC	speech recognition, and location sensing/ classification	Yes	payment systems	defend against unauthorized reading and relay attacks
[75]	RFID	features-fusion and decisions-fusion based on majority voting	Yes	ETC systems	unauthorized reading and relay attacks detection in RFID ETC systems
[64]	WiFi, Bluetooth, infra-red	accelerometer	No	smartcard	continuous two-factor authentication
[14] [76]	Bluetooth	audio	No	online banking	a usable and deployable two-factor authentication mechanism

could provide the needed level of efficiency and security along with the desired usability in the target application, and (iv) what challenges and solutions can be envisioned concerning the high security and usability with low complexity in the co-presence detection techniques in the coming years?.

- *Article selection process:* The research papers selection is made in three stages, which includes automated keyword-based search, selection of the papers based on their title, abstract, and quality of the publication, and elimination of irrelevant papers. In the automated keyword-based search stage, we perform the searching process using the online searching on most popular scientific publication databases, which includes IEEE explorer, ScienceDirect, research gate, ACM, Springer, and Wiley. The following keywords or strings are used for the searching process: (i) ("Copresence" OR "Proximity" OR "zero-interaction") AND ("relay" OR "attack" OR "security" OR "access-control"). As a result of our search process, we found 292 articles that belong to the category of journals, conference proceedings, and books chapter. These research articles were published between 2000 to the first quarter of 2019. In the second stage (paper selection), only the peer-reviewed and English language written papers have been selected to ensure that only the good quality publications are included in our review process. After the second stage, 211 articles were left. Finally, in the elimination stage, we removed the papers that do not fall into the scope of our survey, such as the co-presence detection techniques that use distance bounding approaches [82] [83], and the applications that uses contextual information for purposes other than co-presence detection and in applications other than ZICDA systems [84] [85]. In the end, we have selected a total of 81 research articles for our survey process.

Tables I and II depicts the main state-of-the-art context-aware co-presence detection techniques. The tables have the following columns: (i) *proposals*, it provides the reference of the research work, (ii) *communication channel* used between prover and verifier for verification process that allows or denies prover's access to a ZICDA system, (iii) *sensor modalities*, the context parameters that are used to generate the contextual information, which is used for proximity detection during the authentication process between prover and verifier, (iv) *privacy preservation support*, it specifies whether a proposed proximity detection scheme also considers the privacy concern of prover (where applicable), it is because the contextual information used for proximity detection could leak sensitive information (e.g., location, and audio) about the prover, (v) *Application specific*, it specifies whether the proposed scheme is only applicable to a specific application (e.g., PoS, health-care, and building automation), or it is a generic scheme (e.g., NFC-based applications), and (vi) *description*, it provides a brief description about the proposed scheme.

The use of contextual information to improve the security of access control applications is not a new technique. For example, the banking authentication system uses time and location as contextual information to provide an additional security layer in online transactions. In this scenario, assume a customer that wants to transfer all her funds to a third-party account. The transaction appears genuine, i.e., the customer has authenticated itself correctly to the bank, she is accessing an account for which she is authorized, and the third-party bank account appears valid too. However, the access location or time of the transaction looks suspicious, e.g., the account has been accessed from a location which is far from the home location of the customer or the activation time of the transaction is not consistent with the previous transactions timestamp pattern of the customer. Therefore, without the additional context, the bank is unable to determine if the activity is fraudulent or not.

The use of contextual information to improve the security of access control systems has rapidly increased in recent years, and it is mainly due to the advancements in the mobile device and communication techniques, which makes the availability of the content more accessible to these systems. In [86], the authors propose an approach that provides additional security using context in role-based access control (RBAC) systems. In particular, the main aim is to combine contextual security (by using location and time as context) and role-based access control to retail business processes, which uses the RFID technology for inter-communication. Furthermore, in [87], authors propose a context-aware security architecture for emerging applications, and in [88] a context-aware remote security control for mobile communication devices has been proposed. In both these works, the contextual information such as location, time, and network access points (like WiFi) is used to improve security. It is done by dynamically setting the security policies for individuals based on their current threat levels.

In [47] and [75], authors propose context-based security techniques that uses onboard tag sensors to collect contextual information (location and speed). The proposed techniques minimize the likelihood of unauthorized reading and relay attacks in RFID Electronic Toll Collection (ETC) and banking access control systems. In [75], the context data sensed through GPS sensors is used to develop a context-aware selective unlocking technique for tags at ETC such that they can selectively respond to reader challenges.

In [50], authors propose a proximity-based authentication technique called "Amigo". To authenticate co-present mobile devices, Amigo uses knowledge of their shared radio environment as proof of physical proximity. The key advantages of Amigo include the following: (i) it does not require any additional hardware, (iii) it does not require user involvement in the authentication process, and (iii) it is not vulnerable to eavesdropping. The main idea is that the co-present devices will simultaneously monitor a common set of ambient radio sources (WiFi access points or cell phone base stations) to perceive a similar radio environment. An evaluation conducted using WiFi-enabled laptops show that Amigo is robust against a range of passive and active attacks. To further strengthen the fact that co-present devices will see the common radio environment, fluctuations in the signal strength of existing ambient radio sources are considered in [89]. It shows a

reduction in false positives and false negatives in the system.

In [90], authors present a system called NearMe. NearMe discovers what is already nearby and to augment context for ubiquitous computing. For this purpose, NearMe server determines proximity by comparing a list of WiFi access points and signal strengths called "WiFi signatures" from its clients. To use NearMe, each client has to perform the following three functions: (i) register with proximity server, (ii) report recent WiFi signature, and (iii) query nearby places and peoples. A similar proximity testing system which uses WiFi access points and Bluetooth signals to generate "location tags" is introduced in [71]. The system was implemented and evaluated on the Android platform. Along with security, it also guarantees the privacy preservation for the clients involved in it.

Based on the audio and light data collected from the ambient sensors that are available in NFC enabled smartphones, a secure proximity technique is presented in [70]. The main aim is to prevent relay attacks at point of sale (PoS) systems, where just bringing the NFC enabled smartphone close to PoS is sufficient to complete a transaction. In particular, authors propose a transaction verification mechanism that can determine the proximity (or lack thereof) between honest verifier and prover by comparing specific sensor data (audio or light), which is extracted from the communicating devices. In [49], a secure radio channel between communicating devices based on similar audio patterns has been proposed to develop an unobtrusive but cryptographically strong security mechanism. Furthermore, in [74], authors use ambient audio for secure device pairing on android mobile phones. In this work, audio is used as a metric to generate a secure cryptographic key that establishes communication between mobile distributed devices.

The use of Secret Handshakes as context information rapidly increases in a large array of applications that uses RFID or contactless cards for access control purposes. The intuition behind its use as the content is as follows. Let's assume a typical usage scenario such as RFID or contactless card-based entry in a secure facility. When a prover wishes to enter in an access-controlled building, she often subconsciously (thus, increases the usability of the system) does a fixed set of motions such as her left/right-hand reaches for her wallet, draws her purse out or wave it near the door's reader, and take a pause. From the above use-case, one can observe if it is possible for the RFID chip or contactless technology in the access cards to somehow internally detect a pattern, which depicts precisely when, how, and in what order these actions were being performed. If this is the case, then it is possible to install appropriate logic on the RFID tags and contactless cards that would only allow access when these actions are matched.

Based on the secret handshakes mechanism, several techniques have been proposed over the years to combat various distance-based attacks (please refer to Section II-D). To detect and prevent Man-In-The-Middle (MITM) attacks, authors in [69] propose a technique for device-to-device (e.g., phone and handset) authentication that includes an additional layer in a traditional security suite. It is done by adding additional information in terms of shared movement patterns. A user can simply generate various patterns by shaking the devices together, and these patterns can be easily captured using accelerometer sensors that are embedded in the communicating devices. In particular, two methods that combine cryptographic primitives with accelerometer data analysis are proposed to establish secure radio channels by creating authenticated secret keys. Further, in [45], authors propose context-aware mechanisms to defend against the RFID unauthorized reading (by using owner's posture recognition as context information) and relay attack reading (by using audio as context information). Similarly, in [59] and [53], authors propose gesture and motion recognition based techniques to defend against ghost-and-leech (a.k.a. proxying, relay, or man-in-the-middle) attacks in RFID tags and other contactless cards. All these techniques increase the resilience of access control systems against a set of proximity-based attacks. However, the issue of user privacy caused by the gesture recognition process which involves the sensitive user data (i.e., user's biometric information) is not adequately addressed in these works.

For the first time, authors in [13] systematically investigate the impact of using a single as well as a set of sensor modalities on proximity detection systems. First, a standard data collection and processing framework similar to the one we have described in Figure 6 is developed. The proposed framework runs in realistic everyday setting to collect data, which is then used to train the classifier. Second, the authors compare the performance of four commonly available sensor modalities (i.e., WiFi, Bluetooth, GPS, and audio) using various combinations, first individually and then in the sets of two and four. The work provides a comparison regarding resisting relay attacks in zero-interaction based access control systems for each combination. The authors claim that WiFi data as the context is better in opposing relay attacks when compared to other sensor modalities, and the fusing of multiple modalities further improve resilience against relay attacks. However, the fusion of various modalities retains a high level of system usability up to a certain point. We argue that with the increase in the number of sensor modalities, the time required to authenticate a prover and the complexity of context-aware algorithms deployment increases. Thus, it decreases the usability and feasibility of an access control system. In [13], to make the proximity detection techniques more robust and versatile, the authors motivate the need for a stronger adversarial model in which the adversary can compromise the integrity of context sensing mechanisms. For instance, an attacker can create fake Wifi access points, add random noise, and it can modify the purely ambient physical sensing capabilities [72] such as ambient temperature, precision gas, humidity, pressure, and altitude.

One of the most comprehensive works towards analyzing, extending, and systematizing state-of-the-art tasks on context-aware proximity detection under a stronger, but a realistic adversarial model is presented in [73]. In this work, authors present a systematic assessment of proximity detection in the face of context-manipulating adversaries. It has been shown that not only the content manipulation is possible, but an attacker can consistently control and stabilize the values of multiple, heterogeneous (e.g., acoustic and ambient physical

environment) sensors using low-cost, off-the-shelf equipment. Thus, an attacker who can manipulate the context gains a significant advantage in defeating access control systems that are based on contextual security techniques.

Authors in [14] propose a representative approach called *Sound-Proof*, a usable two factor authentication that leverages ambient sound to detect co-presence between the *phone* (used as a second authentication factor) and the *browser* (a login terminal such as a banking website) running on a different mobile device such as laptop or tablet. Sound-Proof claims to found an optimal trade-off between the usability (i.e., it does not require an interaction between the user and her phone) and security (i.e., secure login on a browser in the presence of remote attackers). In particular, Sound-Proof uses the audio signatures collected from the microphones of the two devices. Sound-Proof provides a useful security enhancement on top of the traditional password-only authentication technique that is commonly used to perform online banking transactions. The only essential requirement in Sound-Proof is that the user should keep her phone near to the laptop while doing the login tasks. However, a weakness of the Sound-Proof is identified by authors in [76]. In [76], authors show that to perform an attack, the remote attacker does not have to predict the ambient sounds near the phone as assumed in the Sound-Proof, instead, it can deliberately make or wait for the phone to produce predictable or previously known sounds (e.g., ringer, notification or alarm sounds). Therefore, exploiting the weakness as mentioned above, a full attack system can be launched to compromise the security of Sound-Proof successfully.

Authors in [91] aims to authenticate messages in VANETs through physical context comparison. The physical context consists of the surface of the road that includes road conditions such as bumps and potholes which can be measured using the accelerometer. Later, the context is used to derive a secret key, which is shared between the co-present vehicles. However, the entropy of the context to generate the secret key and the effect of different road surfaces remains unexplored. Thus, it makes the security guarantees of the system unclear. Recently, authors in [60] propose an approach to verify the ongoing co-presence between two vehicles in an urban environment. The method exploits the characteristics of a trajectory (using gyroscope signals, GPS, etc.) through a road network. The aim is to allow authenticity checks for safety-critical applications. The approach requires a vehicle to share the same route as a leading vehicle to become a verified following vehicle. Co-present vehicles gain knowledge of verified neighbors as well as the capability to authenticate their VANET messages. The construction only reveals a driver's trajectory to other co-present vehicles, and therefore, it protects passengers privacy against an eavesdropping attacker. The proposed approach operates transparent to pseudonym schemes, and thus, it cannot be exploited to attribute different messages to the same sender. The proposal has been implemented as an Android application to evaluate its performance in experiments involving two cars.

D. Co-presence Detection in Location-Based Services

One of the primary goals of pervasive computing is to build service applications that are sensitive to the user's current context information. For example, location-based apps such as Swarm, Foursquare, Glympse, and Google-now, which uses the user location as a context to dynamically provide various services (e.g., information of nearby places, friends, and shops). One way to provide such services is to determine proximity by measuring absolute locations and compute distances. However, computing perfect location threatens user privacy, and it is also not necessarily easy to calculate, especially indoors, where GPS on user devices does not work well, which is usually a place where people spend most of their time. These Location-Based Services (LBS) use the approximate geographical position to enrich user's Quality of Experience (QoE) concerning various contexts such as location-based searching and location-based mobile advertising. To attract more users, service providers give real-world rewards to the user when it does check-in at a specific venue or location. These rewards motivate users to cheat on their real locations. In particular, LBSs can be defined as an array of services available with mobile devices (e.g., smartphones, tablets, and smart-watch), tailoring their functionality to current positions or trajectories of users or vehicles [92].

In [42], authors investigate vulnerabilities leading to possible location cheating attacks in LBS applications and discuss possible countermeasures for the same. By using Foursquare as a use-case scenario, a new location cheating attack is proposed, which can easily cheat the current location verification techniques. The paper shows that if an attacker carefully studies the open-source operating systems for mobile devices such as Android to modify GPS-related application programming interfaces (APIs), then the attacker can cheat their location by altering the GPS information. While LBSs offer great opportunities for a large array of customer-oriented services, but at the same time, it also presents significant privacy threats to the users. To strengthen the mechanisms for preventing location-cheating in LBS, authors in [57] propose Proofs of Presence (PoP) based resilient techniques against malicious users. The paper present facts indicating that the use of context-aware PoPs for verification of users' location claims is vulnerable to *context guessing attacks*. Furthermore, it proposes two countermeasures to mitigate *context-guessing attacks*. The first countermeasure called "surprisal filtering" is based on profiling and estimating the entropy associated with individual PoPs. The second countermeasure suggests the use of longitudinal observations of ambient physical properties of the context. In [93], the authors investigate and discuss the trade-off issues between users' location privacy protection and their Quality of Service (QoS) for the LBSs.

The basis of LBS comes from spatial and temporal big data, which is provided by an enormous amount of mobile devices through GPS and various communication networks (e.g., cellular networks and WiFi). Using LBS to perform co-presence detection poses a significant threat to user privacy. To address this issue, various privacy preservation LBS schemes have been proposed in recent literature. For example, the authors in [92] first investigate the privacy issues in LBSs concerning possibilities of sensitive data leakage and then propose an approach that preserves query data intending to provide accurate LBS answers with zero-server-knowledge

on query data. In most of the state-of-the-art schemes for privacy preservation in LBS, a single trusted anonymizer is placed between the users and the location service provider (LSP). However, it limits privacy guarantees and incurs high communication overhead when used in continuous LBSs. It is because once the anonymizer is compromised, it may put the user data at risk. Authors in [94] propose a dual privacy preserving technique for continuous LBSs to protect the users' trajectory and query content privacy. In this approach, multiple anonymizers are placed between users and LSP, which are combined with Shamir threshold mechanism, dynamic pseudonym mechanism, and K-anonymity technique. Similarly, to achieve an adequate balance among user privacy, usability, and efficiency in LBSs, authors in [95] proposes SPOIL, which is a practical location privacy approach for LBSs. In particular, the idea is that a client (i.e., mobile device) shifts user-intended point-of-interests (POIs) to some neighboring POIs and query the mapping server using the shifted POIs.

IV. Open Issues and Directions for Future Work

In this section, we present the lessons learned from our survey that includes an array of security threats to the ZIA systems, and the state-of-the-art context-based co-presence detection techniques that have been proposed to improve the security and privacy of various applications which uses these systems. Additionally, we discuss open issues and directions for future work that could lead to possible improvements in securing the ZICDA systems.

Based on our survey, the context-aware co-presence detection is emerging as a promising approach for defense against the relay attacks, which is considered as a significant threat to ZICDA systems. In context-based co-presence detection techniques, the contextual information is gathered from the surrounding environments that mainly includes audio-radio environment (e.g., ambient audio, WiFi, Bluetooth, infrared, and GPS, and combinations thereof) and physical environment (temperature, pressure, humidity, gas and altitude, and combinations thereof). Apart from contextual information based techniques, the distance bounding (DB) protocols have also shown significant potential in resisting various distance-hijacking attacks [96] [97]. However, the use of distance bounding protocols in resource-constrained devices such as sensors, low-end smartphones, and smartcards are not suitable [98]. It is due to the multitude of hardware components and the multi-process architecture that is being used to implement the distance bounding techniques, which leads to unpredictable performance behaviour. In particular, these protocols interact at the physical layer, thus, the dedicated hardware is mandatory for practical implementations. Therefore, widespread deployment of DB protocols must await manufacturer endorsement.

In the state-of-the-art, various types of context information that could be extracted from different sensor modalities such as magnetometers, accelerometer, GPS, and gyroscope, is used as contextual information to discover the co-presence between prover and verifier. Researchers have used single or a set of sensor modalities to generate some contextual signature that when matched up to a given threshold, the prover and verifier are considered within each others proximity. It can be deduced from the surveyed techniques that the use of multiple modalities provides more resistance to relay attacks and higher accuracy (i.e., lower false positives and false negatives). However, as the number of modality increases in the contextual set, the usability of the system decreases and the cost of the deployment increases. Additionally, the availability of the multiple sensor modalities depends on the device capabilities and the surrounding environment where the co-presence is being checked.

Despite the availability of a broad array of context-aware co-presence detection techniques, the various types of distance-hijacking attacks still threaten the secure and efficient deployment of different emerging applications, e.g., secure message exchange in VANETs [91], two-factor authentication for user identification [99], and secure device pairing and service creation in IoT [100] [101]. The correct implementation and functionality of these applications are based on the concept of contextual co-presence. Below, we discuss the challenges and future research directions that require significant research attention to improve the security of ZICDA systems and the privacy of its users.

- **Integration of proximity proofs:** To integrate context-based co-presence schemes in a target system, the first requirement is the availability of the adequate context. However, having context availability alone is not sufficient. It should be in the correct format or mechanism, and it should be validated to ensure that it is accurate and has integrity. Once the contextual information is available in an accurate, up-to-date, and validated format, it needs to be integrated based on key values, and a platform is required that enables the log. Additionally, alert data to be linked together with the contextual information is necessary to allow for efficient integration of contextual information in real-time. Finally, the system must have the capability to make the integrated information quickly and readily available to security analysts to present a "scenario", which provides all of the information required to validate, respond to, and mitigate possible security-related incidents. Performing the integration is easy if the system components (e.g., prover and verifier) only need software updates. But in cases where hardware updates are required, the development of the appropriate infrastructure is necessary. In particular, how to deploy contextual co-presence detection solutions cost-effectively and efficiently remains a research problem to address for future researchers.
- **Usable solutions:** The use of contextual information is rapidly increasing in various domains which include financial (e.g., Point-of-Sale, and multi-factor authentication for online and offline transactions) as well as non-financial (e.g., supply chain management, smartcard-based access, and medical implants) applications. Therefore, high usability becomes an essential requirement. However, the use of multiple sensor modalities for context

gathering not only increases the cost of deployment, but it also decreases the usability of the system, which directly effects the quality-of-service (QoS) perceived by the end-users. Therefore, selecting an optimal yet minimal set of sensor modalities that effectively consider the tradeoff between the security, cost, and usability of the system remains an open issue.

- **Resistance against context manipulations:** Most of the state-of-the-art co-presence detection or relay attack resistance mechanisms consider the simplest adversary model (i.e., Dolev-Yao systems). Hence, these mechanisms might not be able to defend the system in the presence of an active adversary (i.e., context manipulating attackers). The existing research shows that it is trivial to modify, consistently control, and stabilize the context data gathered from different (single or multiple) audio-radio and physical environments using low-cost, off-the-shelf equipment [73]. Therefore, extensive research is required to ensure the robustness of the access control systems against distance hijacking attacks. For instance, the classifier and machine learning algorithms that are being used to train the system should consider the possibility of a strong adversary during the training phase. Also, the size of the training data set should be large enough, and it should exhibit the characteristics of the real-world data.
- **Privacy preserving proximity detection:** In most of the available co-presence detection approaches, the context information consists of sensitive user data such as location, audio, and behavioral patterns. Therefore, it is essential to ensure the use of such contextual information in a privacy-preserving manner. However, it is hard to ensure privacy in co-presence systems due to the need for precise information that these systems require to perform the co-presence evaluation. For instance, it is hard to use the incomplete GPS information [102] and still do an accurate assessment for co-presence. Authors in [103] have done the evaluation of five ZIA techniques for realistic deployment scenarios that include smart vehicle, smart office, and smart office consists of heterogeneous devices with mobility. Their evaluation results show that the features that are extracted based on ambient audio give better results. However, using audio as the context has privacy implications in scenarios such as smart home and hospitals. Hence, novel solutions are required to ensure privacy preservation during context-based proximity detection systems.
- **Security soundness:** The security analysis of all the context-based solutions for authentication in ZICDA systems has been usually performed by measuring the effectiveness of the solutions concerning False Positive Rate (FPR), False Negative Rate (FNR) and Equal Error Rate (EER) metrics. It is because, if a solution has higher EER, then the probability that an adversary gets access to the system and that a genuine user is denied the access is also higher. Depending upon the application scenario (e.g., banking, and intelligent transportation system), even an error rate of 1% is considered unacceptable. Authors in [104] concludes based on their implementation and performance evaluation, which weighs 17 Android device sensors, that none of these could provide stringent security against relay attacks. However, some of these sensors might be well suited for low-risk application scenarios only. Such scenarios do not have any strict limits on transaction time, unlike banking transactions, where the recommended duration to complete a transaction is within the range of 300 to 400 milliseconds [105]. The importance of error rates in securing zero-interaction systems has also been investigated at large scale by authors in [103]. Their research claims that depending upon the target scenario, the error rates could lie between 0.6% and 52.8%. This shows the need for more accurate and adaptable context-based mechanisms to ensure the security of critical application domains that uses context to improve the security of their system. One way to improve the error rates is to ensure that the proposed scheme is robust and adaptive. In particular, it should automatically adapt to the internal parameters of the surrounding environment, and it should be evaluated on the context that is collected from heterogeneous scenarios and devices.
- **Practical applicability:**In the literature, the researchers have shown the weak security (mainly against relay attacks) of proximity detection techniques on simulated as well as physical testbeds [22] [106]. To improve the security of proximity detection techniques, various context-based solutions have been proposed in the literature. However, most of these solutions have evaluated in simulated environments and that with strong assumptions (e.g., high availability of context information, proximity range, and higher transaction verification time). Moreover, there are some recent research efforts [104] [103] that have already shown various security weaknesses of the state-of-the-art context-aware solutions for real-world applications. Most of the existing solutions are application-specific. Hence, their security and adaptiveness may vary dramatically for different scenarios. Therefore, a proposed technique should explicitly mention the application domains for which they are designed. Schemes that automatically adapt their contextual features and parameters to their environment are desirable. In particular, it is crucial to verify the particle applicability of any context-aware proximity detection solutions [107] before their deployment in real-world applications. Finally, it would be beneficial to evaluate the solution with a user study to assess its effectiveness, along with potential usability issues.
- **Energy-efficient context-aware techniques:** Recently, the use of context-based techniques has been envisioned in various next-generation applications of Industrial Internet of Things (IIoT) [108] [109], Internet of Things (IoT) [110] [111], and vehicular ad-hoc networks (VANETs) [112] [60]. It is because these applications generate large about of data and are consists of a set of sensors that can be used for extracting contextual information. The use of context-based solutions to improve security and privacy aspects in these applications

have been researched in recent years. However, the sensors used in these environments are resource-constrained and heterogeneous by nature. Therefore, the traditional context-aware techniques cannot be directly used, and need to be modified to suit the low processing and storage requirements of the devices in these application domains. For instance, the ambient audio is considered one of the best context [103] to perform more accurate proximity detection. However, the computational costs while processing audio operations have to be considered when resource-constrained IoT devices are involved in the system.

V. Conclusions

When a user tries to access a system, one can simplify the security decisions by basing it on binary choices (i.e., Yes or No). However, for the rapidly increasing thefts against logging credentials that are caused by the human or the system related errors, such binary decisions are not enough to protect the system. Therefore, if the verifier can base the security decisions on the who, when, where, when, what, and why behind the user's access request, it can develop usable security and privacy solutions for users without sacrificing the level of protection. This paper examines several ways that make use of a context-aware model, which feeds additional information to the Security Analytic Engine (SAE) to create efficient and flexible security decisions. In this paper, we start with the discussion on various real-world applications (e.g., PKE systems, contactless smartcard-based access control systems, contactless payment systems, inventory management, medical implants, and e-passport) and security threats (relay attack, terrorist fraud, location cheating, and impersonation) with respect to the ZICDA access control systems. We provided a comprehensive survey that includes all the state-of-the-art context-based co-presence detection techniques along with their merits and limitations. With the set of future research directions and challenges that we have discussed, we hope that our work will motivate fledgling researchers towards tackling the security, usability, and privacy issues of ZICDA systems.

Acknowledgements

This work is supported in part by EU LOCARD Project under Grant H2020-SU-SEC-2018-832735. The work of M. Conti was supported by the Marie Curie Fellowship through European Commission under Agreement PCIG11-GA-2012-321980.

References

[1] K. Finkenzeller, "RFID handbook: Fundamentals and applications in contactless smart cards and identification," *John Wiley and Sons, Inc., New York, NY, USA, 2 edition*, 2003.

[2] "ISO/IEC 18092 (ECMA-340), information technology telecommunications and information exchange between systems near field communication interface and protocol (NFCIP-1)," *Available: http://www.iso.org/*, 2004.

[3] "International civil aviation organization (ICAO). document 9303 machine readable travel documents (MRTD). part i: Machine readable passports," 2005.

[4] "London transport oystercard," *Available: http://www.oystercard.com*.

[5] "Mastercard paypass." *Available: http://www.paypass.com*.

[6] N. Akinyokun and V. Teague, "Security and privacy implications of nfc-enabled contactless payment systems," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ser. ARES '17. ACM, 2017, pp. 47:1–47:10. [Online]. Available: http://doi.acm.org/10.1145/3098954.3103161

[7] S. Drimer and S. J. Murdoch, "Keep your enemies close: Distance bounding against smartcard relay attacks," pp. 7:1–7:16, 2007.

[8] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," 2010, http://eprint.iacr.org/2010/332.

[9] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical NFC peer-to-peer relay attack using mobile phones," pp. 35–49, 2010.

[10] Z. Kfir and A. Wool, "Picking virtual pockets using relay attacks on contactless smartcard," pp. 47–58, 2005.

[11] L. Sportiello and A. Ciardulli, "Long distance relay attack," pp. 69–85, 2013.

[12] T. Korak and M. Hutter, "On the power of active relay attacks using custom-made proxies," pp. 126–133, April 2014.

[13] H. T. T. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi, "Using contextual co-presence to strengthen zero-interaction authentication: Design, integration and usability," *Pervasive and Mobile Computing*, vol. 16, pp. 187 – 204, 2015, selected Papers from the Twelfth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom 2014).

[14] N. Karapanos, C. Marforio, C. Soriente, and S. Čapkun, "Soundproof: Usable two-factor authentication based on ambient sound," in *Proceedings of the 24th USENIX Conference on Security Symposium*, ser. SEC'15. Berkeley, CA, USA: USENIX Association, 2015, pp. 483–498. [Online]. Available: http://dl.acm.org/citation.cfm?id=2831143.2831174

[15] S. Brands and D. Chaum, *Distance-Bounding Protocols*. Springer Berlin Heidelberg, 1994, pp. 344–359.

[16] S. Bengio, G. Brassard, Y. G. Desmedt, C. Goutier, and J.-J. Quisquater, "Secure implementation of identification systems," *Journal of Cryptology*, vol. 4, pp. 175–183, Jan 1991.

[17] T. Beth and Y. Desmedt, *Identification Tokens — or: Solving The Chess Grandmaster Problem*. Springer Berlin Heidelberg, 1991, pp. 169–176.

[18] M. D. Corner and B. D. Noble, "Zero-interaction authentication," in *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '02. ACM, 2002, pp. 1–11.

[19] A. Brelurut, D. Gerault, and P. Lafourcade, "Survey of distance bounding protocols and threats," in *Foundations and Practice of Security*. Cham: Springer International Publishing, 2016, pp. 29–49.

[20] G. Avoine, M. A. Bingl, I. Boureanu, S. apkun, G. Hancke, S. Karda, C. H. Kim, C. Lauradoux, B. Martin, J. Munilla, A. Peinado, K. Rasmussen, D. Singele, A. Tchamkerten, R. Trujillo-Rasua, and S. Vaudenay, "Security of distance-bounding: A survey," *ACM Computing Surveys*, vol. 4, 2017.

[21] H. Jannati, "Analysis of relay, terrorist fraud and distance fraud attacks on RFID systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 11, pp. 51–61, Dec. 2015.

[22] G. P. Hancke, K. E. Mayes, and K. Markantonakis, "Confidence in smart token proximity: Relay attacks revisited," *Comput. Secur.*, vol. 28, no. 7, pp. 615–627, Oct. 2009.

[23] M. Poturalski, M. Flury, P. Papadimitratos, J. P. Hubaux, and J. Y. L. Boudec, "Distance bounding with IEEE 802.15.4a: Attacks and countermeasures," *IEEE Transactions on Wireless Communications*, vol. 10, no. 4, pp. 1334–1344, April 2011.

[24] Y. Zhauniarovich, G. Russello, M. Conti, B. Crispo, and E. Fernandes, "MOSES: Supporting and enforcing security profiles on smartphones," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 3, pp. 211–223, May 2014.

[25] A. K. Sikder, H. Aksu, and A. S. Uluagac, "6thSense: A context-aware sensor-based attack detector for smart devices," in *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association, 2017, pp. 397–414. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/sikder

[26] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, "Context-aware computing, learning, and big data in internet of things: A survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 1–27, Feb 2018.

[27] I. Bisio, C. Garibotto, A. Grattarola, F. Lavagetto, and A. Sciarrone, "Exploiting context-aware capabilities over the internet of things for industry 4.0 applications," *IEEE Network*, vol. 32, no. 3, pp. 101–107, May 2018.

[28] Q. N. Nguyen, M. Arifuzzaman, K. Yu, and T. Sato, "A context-aware green information-centric networking model for future wireless communications," *IEEE Access*, vol. 6, pp. 22 804–22 816, 2018.

[29] R. Parada and J. Melia-Segui, "Gesture detection using passive RFID tags to enable people-centric IoT applications," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 56–61, February 2017.

[30] M. Wazid, A. K. Das, M. K. Khan, A. A. D. Al-Ghaiheb, N. Kumar, and A. Vasilakos, "Secure authentication scheme for medicine anti-counterfeiting system in IoT environment," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–13, 2017.

[31] W. Issovits and M. Hutter, "Weaknesses of the ISO/IEC 14443 protocol regarding relay attacks," in *2011 IEEE International Conference on RFID-Technologies and Applications*, Sept 2011, pp. 335–342.

[32] D. Dolev and A. C. Yao, "On the security of public key protocols," in *Proceedings of the 22Nd Annual Symposium on Foundations of Computer Science*, ser. SFCS '81. IEEE Computer Society, 1981, pp. 350–357.

[33] G. P. Hancke, "Practical eavesdropping and skimming attacks on high-frequency RFID tokens," *J. Comput. Secur.*, vol. 19, no. 2, pp. 259–288, 2011.

[34] G. Hancke, "A practical relay attack on ISO 14443 proximity cards," Tech. Rep., 2005.

[35] D. Cavdar and E. Tomur, "A practical NFC relay attack on mobile devices using card emulation mode," in *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, May 2015, pp. 1308–1312.

[36] G. Avoine and A. Tchamkerten, *An Efficient Distance Bounding RFID Authentication Protocol: Balancing False-Acceptance Rate and Memory Requirement*. Springer Berlin Heidelberg, 2009, pp. 250–261.

[37] C. Cremers, K. B. Rasmussen, B. Schmidt, and S. Capkun, "Distance hijacking attacks on distance bounding protocols," in *2012 IEEE Symposium on Security and Privacy*, May 2012, pp. 113–127.

[38] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, *Practical and Provably Secure Distance-Bounding*. Springer International Publishing, 2015, pp. 248–258.

[39] C. JH, "On numbers and games," *Academic Press*, 1976.

[40] 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, Feb 2006.

[41] S. Vaudenay, "On modeling terrorist frauds," in *Proceedings of the 7th International Conference on Provable Security - Volume 8209*, ser. ProvSec 2013. Springer-Verlag New York, Inc., 2013, pp. 1–20.

[42] W. He, X. Liu, and M. Ren, "Location cheating: A security challenge to location-based social network services," in *2011 31st International Conference on Distributed Computing Systems*, June 2011, pp. 740–749.

[43] "Sensordrone: The 6th sense of your smartphone...& beyond!" *Available: https://www.kickstarter.com/projects/453951341/sensordrone-the-6th-sense-of-your-smartphoneand-be*, 2016.

[44] M. Di and S. Nitesh, "A context-aware approach to defend against unauthorized reading and relay attacks in RFID systems," *Security and Communication Networks*, vol. 7, no. 12, pp. 2684–2695, 2011.

[45] T. Halevi, H. Li, D. Ma, N. Saxena, J. Voris, and T. Xiang, "Context-aware defenses to RFID unauthorized reading and relay attacks," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, pp. 307–318, 2013.

[46] 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*, 2012, pp. 379–396.

[47] D. Ma, N. Saxena, T. Xiang, and Y. Zhu, "Location-aware and safer cards: Enhancing RFID security and privacy via location sensing," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 2, pp. 57–69, 2013.

[48] W. Choi, M. Seo, and D. H. Lee, "Sound-proximity: 2-factor authentication against relay attack on passive keyless entry and start system," *Journal of Advanced Transportation*, no. 13, 2018.

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

[50] A. Varshavsky, A. Scannell, A. LaMarca, and E. de Lara, "Amigo: Proximity-based authentication of mobile devices," in *UbiComp 2007: Ubiquitous Computing*, 2007, pp. 253–270.

[51] P. Urien and S. Piramuthu, "Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks," *Decis. Support Syst.*, vol. 59, pp. 28–36, Mar. 2014.

[52] P. Urien and S. Piramuthu, "Identity-based authentication to address relay attacks in temperature sensor-enabled smartcards," in *Smart SysTech 2013; European Conference on Smart Objects, Systems and Technologies*, June 2013, pp. 1–7.

[53] 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 *2014 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, March 2014, pp. 163–171.

[54] 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 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '14. ACM, 2014, pp. 880–891.

[55] M. Miettinen, J. Huang, T. D. Nguyen, N. Asokan, and A.-R. Sadeghi, "POSTER: Friend or foe? context authentication for trust domain separation in IoT environments," in *WISEC*, 2016.

[56] M. Miettinen, S. Heuser, W. Kronz, A.-R. Sadeghi, and N. Asokan, "ConXsense: Automated context classification for context-aware access control," in *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '14. New York, NY, USA: ACM, 2014, pp. 293–304.

[57] M. Miettinen, N. Asokan, F. Koushanfar, T. D. Nguyen, J. Rios, A.-R. Sadeghi, M. Sobhani, and S. Yellapantula, "I know where you are: Proofs of presence resilient to malicious provers," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '15. ACM, 2015, pp. 567–577.

[58] M. Juuti, C. Vaas, I. Sluganovic, H. Liljestrand, N. Asokan, and I. Martinovic, "STASH: Securing transparent authentication schemes using prover-side proximity verification," in *2017 14th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, June 2017, pp. 1–9.

[59] A. Czeskis, K. Koscher, J. R. Smith, and T. 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*, ser. CCS '08. ACM, 2008, pp. 479–490.

[60] C. Vaas, M. Juuti, N. Asokan, and I. Martinovic, "Get in line : Ongoing co-presence verification of a vehicle formation based on driving trajectories," in *3rd IEEE European Symposium on Security and Privacy (EuroSP)*, 2018.

[61] I. Gurulian, K. Markantonakis, C. Shepherd, E. Frank, and R. N. Akram, "Proximity assurances based on natural and artificial ambient environments," in *Innovative Security Solutions for Information Technology and Communications*, P. Farshim and E. Simion, Eds. Cham: Springer International Publishing, 2017, pp. 83–103.

[62] I. Gurulian, C. Shepherd, E. Frank, K. Markantonakis, R. N. Akram, and K. Mayes, "On the effectiveness of ambient sensing for detecting NFC relay attacks," in *2017 IEEE Trustcom/BigDataSE/ICESS*, Aug 2017, pp. 41–49.

[63] I. Gurulian, R. N. Akram, K. Markantonakis, and K. Mayes, "Preventing relay attacks in mobile transactions using infrared light," in *Proceedings of the Symposium on Applied Computing*, ser. SAC '17, 2017, pp. 1724–1731.

[64] I. Gurulian, K. Markantonakis, R. N. Akram, and K. Mayes, "Artificial ambient environments for proximity critical applications," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ser. ARES '17. ACM, 2017, pp. 5:1–5:10.

[65] I. Gurulian, G. P. Hancke, K. Markantonakis, and R. N. Akram, "May the force be with you: Force-based relay attack detection," in *Smart Card Research and Advanced Applications*, T. Eisenbarth and Y. Teglia, Eds., 2018, pp. 142–159.

[66] R. Jin, L. Shi, K. Zeng, A. Pande, and P. Mohapatra, "MagPairing: Pairing smartphones in close proximity using magnetometers," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1306–1320, June 2016.

[67] M. Mehrnezhad, F. Hao, and S. F. Shahandashti, "Tap-tap and pay (TTP) : Preventing man-in-the-middle attacks in NFC payment using mobile sensors," 2016.

[68] N. Saxena and J. Voris, "Still and silent: Motion detection for enhanced RFID security and privacy without changing the usage model," in *Radio Frequency Identification: Security and Privacy Issues*, S. B. Ors Yalcin, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 2–21.

[69] R. Mayrhofer and H. Gellersen, "Shake well before use: Authentication based on accelerometer data," in *Pervasive Computing*, A. LaMarca, M. Langheinrich, and K. N. Truong, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 144–161.

[70] 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*, S. Foresti, M. Yung, and F. Martinelli, Eds., 2012.

[71] J. D. Nielsen, J. I. Pagter, and M. B. Stausholm, "Location privacy via actively secure private proximity testing," in *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, March 2012, pp. 381–386.

[72] B. Shrestha, N. Saxena, H. T. T. Truong, and N. Asokan, "Drone to the rescue: Relay-resilient authentication using ambient multi-sensing," in *Financial Cryptography and Data Security*, N. Christin and R. Safavi-Naini, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 349–364.

[73] B. Shrestha, N. Saxena, H. Truong, and N. Asokan, "Sensor-based proximity detection in the face of active adversaries," *IEEE Transactions on Mobile Computing*, pp. 1–1, 2018.

[74] M. Di and S. Nitesh, "A context-aware approach to defend against unauthorized reading and relay attacks in RFID systems," *Security and Communication Networks*, vol. 7, no. 12, pp. 2684–2695, 2011.

[75] D. Ma and A. K. Prasad, "A context-aware approach for enhanced security and privacy in RFID electronic toll collection systems," in *2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, July 2011, pp. 1–6.

[76] B. Shrestha, M. Shirvanian, P. Shrestha, and N. Saxena, "The sounds of the phones: Dangers of zero-effort second factor login based on ambient audio," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: ACM, 2016, pp. 908–919. [Online]. Available: http://doi.acm.org/10.1145/2976749.2978328

[77] D. J. Yeager, J. Holleman, R. Prasad, J. R. Smith, and B. P. Otis, "NeuralWISP: A wirelessly powered neural interface with 1-m range," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 3, no. 6, pp. 379–387, Dec 2009.

[78] A. P. Sample, D. J. Yeager, and J. R. Smith, "A capacitive touch interface for passive RFID tags," in *2009 IEEE International Conference on RFID*, April 2009, pp. 103–109.

[79] A. P. Sample, D. J. Yeager, P. S. Powledge, and J. R. Smith, "Design of a passively-powered, programmable sensing platform for UHF RFID systems," in *2007 IEEE International Conference on RFID*, March 2007, pp. 149–156.

[80] J. R. Smith, A. P. Sample, P. S. Powledge, S. Roy, and A. Mamishev, "A wirelessly-powered platform for sensing and computation," in *Proceedings of the 8th International Conference on Ubiquitous Computing*, ser. UbiComp'06, 2006, pp. 495–506.

[81] B. Kitchenham, "Procedures for performing systematic reviews," Department of Computer Science, Keele University, UK, Keele University. Technical Report TR/SE-0401, 2004.

[82] M. Poturalski, M. Flury, P. Papadimitratos, J. Hubaux, and J. Le Boudec, "Distance bounding with ieee 802.15.4a: Attacks and countermeasures," *IEEE Transactions on Wireless Communications*, vol. 10, no. 4, pp. 1334–1344, April 2011.

[83] R. Trujillo-Rasua, B. Martin, and G. Avoine, "Distance bounding facing both mafia and distance frauds," *IEEE Transactions on Wireless Communications*, vol. 13, no. 10, pp. 5690–5698, Oct 2014.

[84] Y. Duan, J. Lu, J. Feng, and J. Zhou, "Context-aware local binary feature learning for face recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 40, no. 5, pp. 1139–1153, May 2018.

[85] R. Iqbal, T. A. Butt, M. O. Shafique, M. W. A. Talib, and T. Umer, "Context-aware data-driven intelligent framework for fog infrastructures in internet of vehicles," *IEEE Access*, vol. 6, pp. 58 182–58 194, 2018.

[86] M. Y. Wu, C. K. Ke, and W. L. Tzeng, "Applying context-aware RBAC to RFID security management for application in retail business," in *2008 IEEE Asia-Pacific Services Computing Conference*, Dec 2008, pp. 1208–1212.

[87] M. J. Covington, P. Fogla, Z. Zhan, and M. Ahamad, "A context-aware security architecture for emerging applications," in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 2002, pp. 249–258.

[88] G. An, D. Seo, J. Kim, K. Kim, and D. Seo, "Context-based remote security control for mobile communication device," in *2010 10th International Symposium on Communications and Information Technologies*, Oct 2010, pp. 815–820.

[89] A. Varshavsky, A. LaMarca, and E. de Lara, "Enabling secure and spontaneous communication between mobile devices using common radio environment," in *Eighth IEEE Workshop on Mobile Computing Systems and Applications*, March 2007, pp. 9–13.

[90] J. Krumm and K. Hinckley, "The nearme wireless proximity server," in *UbiComp 2004: Ubiquitous Computing*, N. Davies, E. D. Mynatt, and I. Siio, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 283–300.

[91] J. Han, M. Harishankar, X. Wang, A. J. Chung, and P. Tague, "Convoy: Physical context verification for vehicle platoon admission," in *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications*, ser. HotMobile '17. New York, NY, USA: ACM, 2017, pp. 73–78. [Online]. Available: http://doi.acm.org/10.1145/3032970.3032987

[92] S. Wang, Q. Hu, Y. Sun, and J. Huang, "Privacy preservation in location-based services," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 134–140, MARCH 2018.

[93] K. G. Shin, X. Ju, Z. Chen, and X. Hu, "Privacy protection for users of location-based services," *IEEE Wireless Communications*, vol. 19, no. 1, pp. 30–39, February 2012.

[94] S. Zhang, G. Wang, and Q. Liu, "A dual privacy preserving scheme in continuous location-based services," in *2017 IEEE Trustcom/BigDataSE/ICESS*, Aug 2017, pp. 402–408.

[95] C. Di, S. Xiaodong, G. Hailong, L. Hao, and Z. Shilei, "SPOIL: Practical location privacy for location based services," in *2017 IEEE 17th International Conference on Communication Technology (ICCT)*, Oct 2017, pp. 574–578.

[96] C. Dimitrakakis and A. Mitrokotsa, "Distance-bounding protocols: Are you close enough?" *IEEE Security Privacy*, vol. 13, no. 4, pp. 47–51, July 2015.

[97] A. Yang, E. Pagnin, A. Mitrokotsa, G. P. Hancke, and D. S. Wong, "Two-hop distance-bounding protocols: Keep your friends close," *IEEE Transactions on Mobile Computing*, vol. 17, no. 7, pp. 1723–1736, July 2018.

[98] I. Boureanu and S. Vaudenay, "Challenges in distance bounding," *IEEE Security Privacy*, vol. 13, no. 1, pp. 41–48, Jan 2015.

[99] A. Basu, R. Xu, M. S. Rahman, and S. Kiyomto, "User-in-a-context: A blueprint for context-aware identification," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Dec 2016, pp. 329–334.

[100] 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 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '14, 2014, pp. 880–891.

[101] E. de Matos, L. A. Amaral, R. T. Tiburski, M. C. Schenfeld, D. F. G. de Azevedo, and F. Hessel, "A sensing-as-a-service context-aware system for internet of things environments," in *2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC)*, Jan 2017, pp. 724–727.

[102] L. Heng, A. R. Kumar, and G. Gao, "Private proximity detection using partial GPS information," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 52, no. 6, pp. 2873–2885, December 2016.

[103] M. Fomichev, M. Maass, L. Almon, A. Molina, and M. Hollick, "Perils of zero-interaction security in the internet of things," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 3, no. 1, pp. 10:1–10:38, Mar. 2019. [Online]. Available: http://doi.acm.org/10.1145/3314397

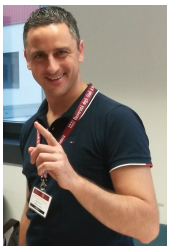
[104] C. Shepherd, I. Gurulian, E. Frank, K. Markantonakis, R. N. Akram, E. Panaousis, and K. Mayes, "The applicability of ambient sensors as proximity evidence for nfc transactions," in *2017 IEEE Security and Privacy Workshops (SPW)*, May 2017, pp. 179–188.

[105] M. Emms, B. Arief, L. Freitas, J. Hannon, and A. van Moorsel, "Harvesting high value foreign currency transactions from emv contactless credit cards without the pin," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '14. ACM, 2014, pp. 716–726. [Online]. Available: http://doi.acm.org/10.1145/2660267.2660312

[106] G. P. Hancke, "Practical attacks on proximity identification systems (short paper)," in *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, ser. SP '06. Washington, DC, USA: IEEE Computer Society, 2006, pp. 328–333. [Online]. Available: https://doi.org/10.1109/SP.2006.30

[107] I. Gurulian, K. Markantonakis, E. Frank, and R. N. 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)*, Aug 2018, pp. 481–489.

[108] Z. Pan, S. Hariri, and J. Pacheco, "Context aware intrusion detection for building automation systems," *Computers Security*, vol. 85, pp. 181 – 201, 2019.
[109] F. Al-Turjman and S. Alturjman, "Context-sensitive access in industrial internet of things (iiot) healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2736–2744, June 2018.
[110] A. Arfaoui, O. R. M. Boudia, A. Kribeche, S.-M. Senouci, and M. Hamdi, "Context-aware access control and anonymous authentication in wban," *Computers Security*, 2019.
[111] B. Chatterjee, N. Cao, A. Raychowdhury, and S. Sen, "Context-aware intelligence in resource-constrained iot nodes: Opportunities and challenges," *IEEE Design Test*, vol. 36, no. 2, pp. 7–40, April 2019.
[112] G. Costantino, F. Martinelli, I. Matteucci, A. Bertolino, A. Calabro, and E. Marchetti, "Cars: Context aware reputation systems to evaluate vehicles' behaviour," in *2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*, March 2018, pp. 446–453.



Mauro Conti is Full Professor at the University of Padua, Italy, and Affiliate Professor at the University of Washington, Seattle, USA. He obtained his Ph.D. from Sapienza University of Rome, Italy, in 2009. After his Ph.D., he was a Post-Doc Researcher at Vrije Universiteit Amsterdam, The Netherlands. In 2011 he joined as Assistant Professor the University of Padua, where he became Associate Professor in 2015, and Full Professor in 2018. He has been Visiting Researcher at GMU (2008, 2016), UCLA (2010), UCI (2012, 2013, 2014, 2017), TU Darmstadt (2013), UF (2015), and FIU (2015, 2016). He has been awarded with a Marie Curie Fellowship (2012) by the European Commission, and with a Fellowship by the German DAAD (2013). His research is also funded by companies, including Cisco and Intel. His main research interest is in the area of security and privacy. In this area, he published more than 200 papers in topmost international peer-reviewed journals and conference. He is Area Editor-in-Chief for IEEE Communications Surveys & Tutorials, and Associate Editor for several journals, including IEEE Transactions on Information Forensics and Security, and IEEE Transactions on Network and Service Management. He was Program Chair for TRUST 2015, ICISS 2016, WiSec 2017, and General Chair for SecureComm 2012 and ACM SACMAT 2013. He is Senior Member of the IEEE.

Chhagan Lal is Postdoc fellow in Department of Mathematics, University of Padua, Italy. He obtained his Bachelors in Computer Science and Engineering from MBM Engineering College, Jodhpur, India in 2006. He obtained his Masters degree in Information Technology with specialization in Wireless communication from Indian Institute of Information Technology, Allahabad in 2009, and Ph.D. in Computer Science and Engineering from Malaviya National Institute of Technology, Jaipur, India in 2014. He has been awarded Canadian Commonwealth scholarship in 2012 under Canadian Commonwealth Scholarship Program to work in University of Saskatchewan in Saskatoon, Saskatchewan, Canada. His current research areas include Blockchain Analysis, Security in Wireless networks, Software-defined networking, Underwater acoustic networks, and context-based security solutions for Internet of Things (IoT) networks.