Survey on Camera based Communication for Location-Aware Secure Authentication and Communication

Hannes Plank*, Christian Steger†, Thomas Ruprechter*, Gerald Holweg*, Norbert Druml*
*Infineon Technologies Austria AG, Graz, Austria
†Institute for Technical Informatics, Graz University of Technology, Austria
{hannes.plank, thomas.ruprechter, gerald.holweg, norbert.druml}@infineon.com, steger@tugraz.at

***Abstract*—Contactless communication and authentication in the RF-domain is still impaired from relay attacks. Countermeasures like distance bounding protocols are difficult to implement properly and are still continuously broken by sophisticated attacks. This work reviews a variety of approaches to counteract relay attacks by adding location-awareness to the security concept. Camera based optical line of sight communication is an alternative to RF communication and provides location-awareness by the ability of sensing communication partners. Concepts and methods of this field are introduced and their contribution to location-aware security analyzed.**

Finally, we present OptiSec3D, which is our novel approach to use Time-of-Flight 3D cameras for secure communication. Our proposed system combines state-of-the-art cryptographic security with 3D depth recognition and camera based optical communication. Various attack scenarios are identified and discussed. We show how our system can improve the security of previous camera-based communication systems and how it can drastically reduce the risk of relay attacks.

***Keywords*—Time-of-Flight, contactless authentication, camera based communication, security, 3D sensing**

I. Introduction

The demand for secure contactless authentication and communication methods is growing steadily. Applications range from mobile payment, access control, device pairing, electronic passports to keyless car entry and start systems. In these applications, the devices face the challenge to establish a secure connection over an insecure channel. While cryptographic methods, like Diffie-Hellman key exchange, digital signatures and message authentication can be combined to a secure protocol, the risk of relay attacks persists.

An example of a relay attack on a keyless car entry system is illustrated in Fig. 1. An attacker relays the communication between an entry token to the car. Access can be gained without the owner's presence. Francillon et al. [1] successfully executed this attack on 10 different car models and were able to gain entry and to start the engine. Distance bounding protocols can limit the maximum allowed distance between two communication partners, but have been successfully attacked. If both communication partners can determine their relative position in a reliable way, the vulnerability against relay-attacks might improve [2].

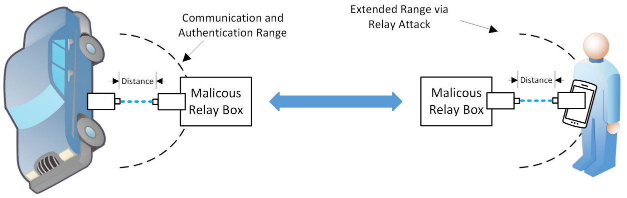
Communication and Authentication Range
Extended Range via Relay Attack
Distance
Malicous Relay Box
Malicous Relay Box
Distance

Fig. 1. Concept of a relay attack on passive keyless car entry systems

This work discusses security aspects of location-awareness with a focus on camera based communication systems. Camera based communication systems can have the ability to sense their communication partner, and visually detect attackers. However, most approaches have a limited range and just rely on the optical channel for security. We introduce our OptiSec3D approach, which overcomes the boundaries of other camera based communication systems by using Time-of-Flight 3D cameras. Our security concept relies on state-of-the-art hardware-accelerated cryptography in combination with Time-of-Flight 3D sensing and its optical communication ability.

II. Time-of-Flight 3D Sensing

Time-of-Flight is a sensing technology that provides distance information by measuring the travel time of emitted light. There are two fundamental Time-of-Flight principles, the direct and the indirect measurement approaches. The indirect method, which is illustrated in Fig. 2, measures distance information by analyzing the phase shift between the emitted modulated infrared light and the reflected light with the help of

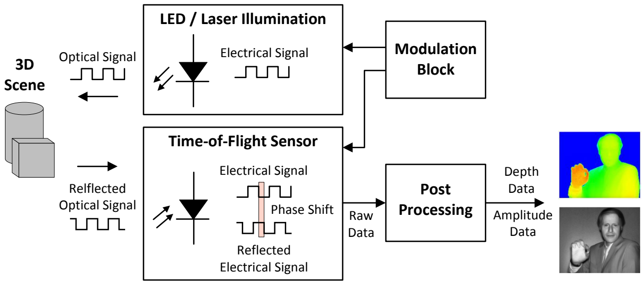

Fig. 2. The concept of PMD-based Time-of-Flight 3D sensing, obtained with changes from [3].

photonic mixing devices (PMD), as explained by the authors in [4].

Thanks to this concept (monocular, no baseline required, little power consumption), PMD-based Time-of-Flight cameras can be easily miniaturized and integrated into small embedded devices in a very robust way. The raw data, which is gathered by the sensor, is then post processed by a processing pipeline. The outcome of this pipeline is 3D depth information of the scenery and amplitude information, which can be used as a robust infrared image. Given these features, future Time-of-Flight camera systems will enable the concept of *ubiquitous real-time geometry devices* that provide 3D data for our everyday applications.

III. Location-Awareness in the RF-domain

This section reviews approaches aiming to tackle the remaining problems of secure communication over an insecure channel by introducing distance or location-awareness. Relay attacks, also named mafia fraud attacks, prove to be sever and difficult to avoid. As listed by Fischlin et al. [5], relay attacks have been successfully implemented on applications such as Bluetooth [6], [7], smartcards [8], [9], [10], [11], electronic passports [12], voting systems [13] and passive keyless car entry systems [1].

Distance bounding protocols [14] are the most common protection against relay attacks. The core concept is to introduce an upper bound on the distance between communication partners. This bound is usually enforced by timing the delay between a sent message the reply of the partner. This limited reply time hampers an attacker to rely the message to a third party which is not within this boundary.

Brelurut et al. [15] provide a recent survey about distance bounding protocols. According to Clulow et al. [16], some hardware is not fit to handle the tight timing constraints of distance bounding. Sometimes, the clocks are not precise enough to reliably employ distance bounding. The protocols are often just implemented in software layers, which also doesn't allow strict distance bounding. This is due the fact that the time a message travels through the air is very low compared to the response time of an electronic device. An attacker can be faster at relaying messages, spoofing the original distance. There are approaches, like Clulow et al. outlined in [16], to avoid this by using probabilistic models about timing behavior to detect attackers. Despite the past research effort, which resulted in over 40 distance bounding protocols, they still show vulnerability against attacks [16], [17]. Cremers et al. [17] proposed distance hijacking attacks, where the attacker uses unsuspecting third parties to verify the distance measurement.

If two devices are not just aware of their distance, but can securely determine their relative location, their vulnerability for relay attacks might be reduced [2]. Using the characteristics of wireless networks for indoor localization has been well researched and was surveyed by Zhu et al. [18]. A lot of work has been accomplished on the localization in Wifi networks. The challenge of Wifi positioning is that Wifi networks were not designed for localization. The main motivation for Wifi localization is not security, but indoor navigation and location based services.

Wifi fingerprinting is a well-established technique, offering coarse localization. It requires a time-consuming calibration of the signal strength indicator (RSSI) in the network [19]. Because of the Wifi signal characteristics, the RSSI depends on the location. The problem with Wifi fingerprinting is that it requires an RSSI map of the Wifi access point and is thus volatile to environmental changes. SecureAngle [20] is a system to overcome fingerprinting based techniques by using multi-antenna access points to create unique angle signatures of the clients. There are approaches to enrich Wifi-based localization with additional signals, cf. Niu et al. with Zigbee [21]. Tippenhauer et al. [22] show that Wifi-based localization can be spoofed by replaying localization signals. There are countermeasures possible but according to Tippenhauer, Wifi-based localization cannot be reliably used in security applications.

A different paradigm for localization is sound positioning [23]. According to Clulow [16], sound positioning offers precise localization due to the slower propagation speed of sound. Sound-based security mechanisms are however vulnerable to relay attacks because the communication can be relayed over a faster medium.

Visible light communication (VLC) has recently gained momentum through the rise of the Internet of Things (IoT). The security aspects of visible light communications are discussed by Rohner et al. [24] in their survey. Physical security features of the visible light channel were introduced by Mostafa et al. in [25] and [26]. They use null-steering, artificial noise and beamforming to mitigate eavesdropping.

IV. Camera-Based Communication

There are several approaches to use cameras for optical communication. The obvious benefit for secure communication is that due to the optical line-of-sight communication principle, an attacker needs to be within the field of view of the cameras. This section provides an overlook on camera communication principles. Security aspects of camera communication are reviewed in Section V.

Analyzing image data can lead to recognition of the communication partner and validation of its location. The limited frame-rate of common image sensors is compensated by the high numbers of pixels. This guarantees enough bandwidth for a lot of applications. The most common way to use 2D cameras for communication is using displays to stream 2D barcodes. This principle is known as pixelated multiple input, multiple output (MIMO) and was first introduced by Hranilovic and Kschischang [27]. A good overview on barcode generation and streaming is provided by Kokan and Gupta [28]. Hao et al. [29] propose a system to use colored barcodes to reach a good performance on small displays like smartphones.

It is also possible to embed imperceptible information into the display output. Li et al. [30] demonstrate a method of encoding information with pixel translucency changes. Humans are unable to see the modulation but cameras can use it for communication.

The previously introduced concepts were based on sending information over a display device. With the Bokode method [31], it is possible to transmit information to cameras just with a single point light source. When cameras are out-of-focus, light sources arrive as focus spots on the sensor. In the Bokode system, the light rays of the point source are arranged in a coded pattern. When the rays arrive at the out-of-focus camera, this pattern is projected onto the sensor. This enables a two way optical communication link without bulky displays. The distance of Bokode is restricted similarly as conventional barcode displaying methods, however the angle is also restricted to under 20 degrees.

While optical data streaming with 2D-cameras works with sufficient reliability and bandwidth, these systems are either bulky or limited in range and angle. The next section introduces the communication ability of Time-of-Flight 3D cameras and how it can tackle the flaws of 2D camera based communication.

A. Communication with Time-of-Flight 3D Cameras

In the past years, depth sensing cameras became increasingly popular and sophisticated. The smallest system are Time-of-Flight cameras, which are close to becoming largely available in consumer devices [32]. To best of our knowledge, the only attempt to use Time-of-Flight cameras for communication has been accomplished by Yuan et al. [33]. Yuan proposes a system, which enables a one-way communication link from an array of LEDs to a ToF camera. The signal from the Time-of-Flight illumination unit is sensed by IR-photodiodes, amplified and sent back phase-modulated via the LED array.

Our communication method [34] uses Time-of-Flight cameras for communication and mutual depth sensing. Unlike the previously introduced MIMO approaches, the signal originates from the Time-of-Flight illumination unit, which is a single laser or LED. The information is transmitted by using the camera's phase-shifting feature. Hence just two Time-of-Flight cameras without any additional communication hardware are required for our approach. The necessary bandwidth is reached by employing high frame-rates and adapting the Time-of-Flight post-processing pipeline. We developed a proof-of-concept prototype, as shown in Fig. 3, which demonstrates the communication ability of Time-of-Flight cameras. This optical communication principle is used by our proposed OptiSec3D security concept, which is explained further in Section VI.

V. Cameras in Secure Communication

While imaging devices are frequently used in biometric access control systems (face-, iris- hand-, and veinscanning), the use for secure device authentication is not so well explored. The Seeing-is-Believing (SiB) system of McCune et al. [35] is the first use of cameras for secure device authentication to our knowledge. It is based on generating a barcode, containing a hash of a device's public key. The visual channel is assumed to be secure in this work, and the rest of the authentication runs over an insecure RF-channel. Saxena et al. improve the SiB principle to devices with limited displaying capabilities like LEDs.

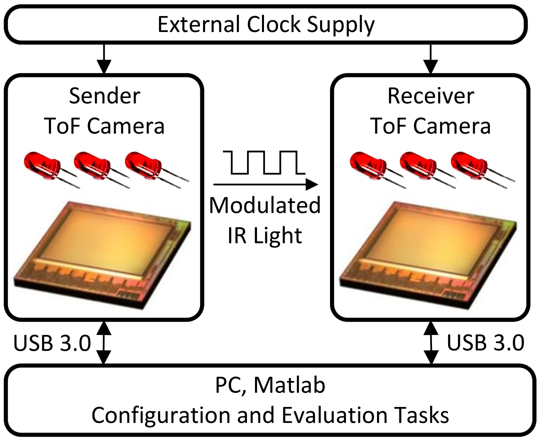

Fig. 3. The design principle of our proof-of-concept prototype.

The SBVLC system proposed from Zhan et al. [36] aims to be an alternative to NFC by securely transmitting barcodes using smartphones. The authors create and test a 2D/3D geometric security model, to analyze the eavesdropping possibility. A similar concept is CamTalk [37], which like the other approaches, relies on the presumption that the visual channel is relatively immune to attacks.

These camera based secure communication approaches presume that two good devices face each other. It is however a possible attack scenario that a user unknowingly points a device at a malicious relay box. Camera to display communication suffers practical restrictions, such as range and system size. We thus developed the OptiSec3D security concept, which is based on Time-of-Flight 3D sensing. It is introduced in the next section and aims to defeat the identified relay attack scenarios, while being more convenient than 2D-camera based systems.

VI. The OptiSec3D Security Concept

The OptiSec3D security concept enables secure communication and unified cryptographic and 3D location-aware authentication between two devices over the optical channel. Infineon's REAL3™ camera system, which is based on Time-of-Flight technology of PMDTechnologies, is used for secure communication and 3D-sensing. The proposed system combines several security features to a novel concept: **State-of-the-art cryptography** can counteract most of the known attack scenarios but is vulnerable against relay attacks. Relay attack attempts on the proposed system are very easy to detect due to the **nature of optical line of sight data transmission** alone. With the ability of the communication partners to sense each other by depth imaging, this adds the security feature of **machine recognition**. 3D authentication, integrity tracking and continuous **secure mutual position checking** can effectively defeat relay attacks.

A. State-of-the-Art Cryptographic Authentication and Communication

The common way to establish a secure connection over an insecure channel is to agree to a common secret. This common secret is used to derive a common key which is used to efficiently encrypt messages with a symmetric encryption method such as AES. The limited bandwidth of a Time-of-Flight camera based communication system calls for a cryptographic key exchange and authentication protocol requiring as little data exchange as possible. Elliptic curve based cryptography (ECC) allows to securely use short keys and is thus suited well for our purpose. The Elliptic Curve based Diffie-Hellman (ECDH) key exchange protocol enables the communication partners Alice and Bob to establish their common secret, while communicating over the insecure optical channel. The common key can't be derived by a third party in an easy way as it requires solving the Diffie-Hellman problem, which is mathematically complex. If however an attacker manages to listen and to alter the messages between Alice and Bob, this exchange is compromised. To counter these man-in-the-middle attacks, the messages need to be authenticated by using a digital signature. Digital signatures can prove that a message originates from a certain communication partner.

When a common secret is securely established, it is used to derive a common key for fast symmetric encryption. Message authentication codes (MAC) ensure the integrity of encrypted messages. A checksum of the message and a shared secret are combined by Alice and attached to the message. Bob uses the shared secret to compute the MAC himself and compares it with Alice's version. A nonce is a number which changes during every transaction. Adding this number to the unencrypted message prevents the attacker from recording and replaying messages.

These cryptographic principles are combined to a protocol. Numerous established light-weight cryptographic protocols are already available. The protocol is embedded into the security concept of OptiSec3D and provides cryptographic trust on the message-transfer level. A hardware security controller can be used as security anchor, e.g., for secure key-storage and numerous hardware accelerated cryptographic operations.

B. 3D Recognition

Using the depth (and maybe amplitude) images gathered by the Time-of-Flight cameras, it is possible for the communication partners to recognize each other. An initial 3D geometry recognition ensures a higher level of security. Not only the geometry of the communication partner is detected, but also the expected source of modulated light. This alone makes relay attacks very hard, because an attacker would need to be able to emit light from the same location as the communication partner.

An example is the contactless payment use-case, where a payment device detects the 3D shape of a payment terminal. Since the shape and source of light are stored in a database, the device detects a relay attack if the information originates from a second malicious device.

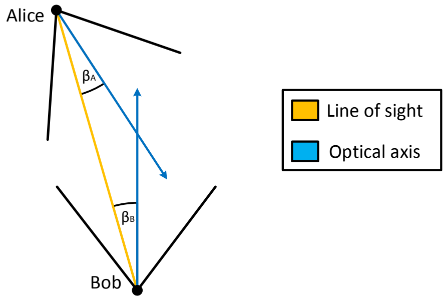

Fig. 4. Alice and Bob both measure their distance (length of the line of sight) and the angles β_A and β_B.

It is sufficient for just one device to sense a malicious device to prevent relay attacks. In the case of a payment terminal, it does not make sense to track the customer in 3D because an attacker would look the same. Whether 3D recognition is performed continuously or just at the beginning of the communication phase is subject to an evaluation.

C. 3D Integrity Checking

Integrity tracking of the communication partner ensures that no third party can secretly alter or relay the transmission after the initial 3D-recognition.

Assuming that geometrical appearance does not change during the communication, time-consuming continuous 3D recognition can be replaced by tracking geometrical changes. As depth image based simultaneous localization and mapping (SLAM) approaches like Kinect Fusion by Izadi et al. [38] proofed to be reliable, it is possible to estimate the relative camera pose between two captured depth frames. This allows communication partners to be in motion while the system is still capable to detect an interfering malicious device.

D. 3D Position Verification

While 3D recognition can prevent a relay attack originating from a different location, it does not cover an imposing device with the same geometric properties. The countermeasure against this attack scenario is to track the relative position of the other device during the communication. Due to the strong signal of the modulated light source, each system can detect the distance and angle (β) between the line of sight (LOS) and the optical axis, as shown in Fig. 4. Each device regularly forwards the other's measured distance and angle β as encrypted message. These measured parameters are supposed to be similar for each device and dissimilar parameters indicate relay attacks. Because it is very hard to spoof Time-of-Flight depth measurements, this is the most important security feature of OptiSec3D and can be enough to avert relay attacks.

E. 3D Secure Communication Protocol

The introduced security concepts are combined to a secure communication protocol. Unlike traditional security protocols, the proposed protocol includes the Time-of-Flight technology

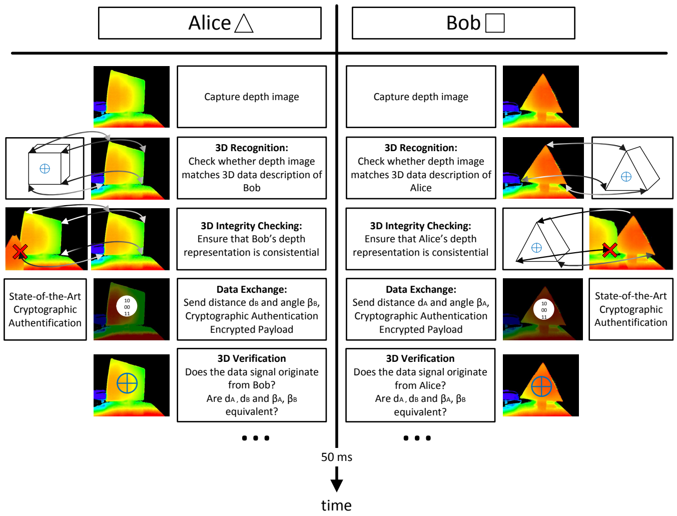
Alice △
Bob □
Capture depth image
Capture depth image
3D Recognition: Check whether depth image matches 3D data description of Bob
3D Recognition: Check whether depth image matches 3D data description of Alice
3D Integrity Checking: Ensure that Bob's depth representation is consistential
3D Integrity Checking: Ensure that Alice's depth representation is consistential
State-of-the-Art Cryptographic Authentification
10 00 11
Data Exchange: Send distance d_B and angle β_B, Cryptographic Authentication Encrypted Payload
Data Exchange: Send distance d_A and angle β_A, Cryptographic Authentication Encrypted Payload
10 00 11
State-of-the-Art Cryptographic Authentification
3D Verification Does the data signal originate from Bob? Are d_A, d_B and β_A, β_B equivalent?
3D Verification Does the data signal originate from Alice? Are d_A, d_B and β_A, β_B equivalent?
• • •
• • •
50 ms
time

Fig. 5. Activities during a time-frame to implement the 3D security protocol

by introducing phases of communication and depth measurements and evaluation. The secure communication is managed by a state-of-the-art cryptographic protocol, as described in Section VI. Fig. 5 illustrates the idea of a future time-frame in the protocol. The Time-of-Flight cameras alternate between communication and depth sensing. It employs the previously discussed 3D security features. It is not possible to transmit information and sense depth at the same time.

An important part of the security protocol is to exchange encrypted messages containing the measured distance and angle β of the communication partner. Relay attacks are detected, if the measured positions are inconsistent.

VII. Evaluation of Potential Threats

As mentioned in Section III, relay attacks are one of the biggest remaining risks for secure communication and authentication applications. The OptiSec3D concept aims to make these attacks unfeasible, and hence we identify and analyze relay attack scenarios in this section.

A. *General relay attack*

Due to the nature of optical communication, an attacker would need to get into the view of the camera systems. This is so unlikely that previous camera based security approaches, which were introduced in Section V, assume this channel to be sufficiently secure [35]. The longer reachable distance and small lightsource (compared to a display) of Time-of-Flight cameras, can make this kind of attack feasible if there are no countermeasures. The OptiSec3D approach hence does not rely on the optical channel for security.

The 3D recognition can estimate the expected position of the light source. Signals originating from any different location are not accepted. This restricts the communication coarsely to the line of sight between the illumination unit and image sensor. As the other attack scenarios show, 3D recognition is only an additional feature and not mandatory to prevent relay attacks.

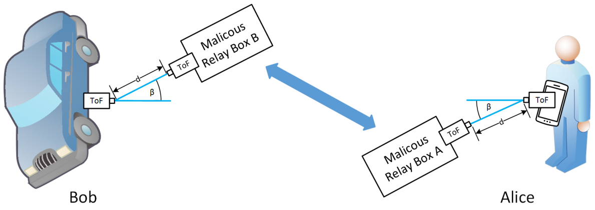

Fig. 6. Distance and angle checking: A relay attack on OptiSec3D would need to recreate the exact angle β and distance d with relay box B.

B. *Relay attack with 3D spoofing*

In this scenario, an attacker tries to influence the camera system to take a wrong depth measurement. There have been attacks to depth sensing systems in the field of biometric face-scanning, using 3D-masks [39]. However spoofing depth measurements without physically changing the environment are nearly impossible due to the nature of the Time-of-Flight depth sensing principle. The next scenario shows, why OptiSec3D is not just immune to spoofing, but also secure against relay attacks even if a relay box geometrically impersonates a valid communication partner.

C. *Relay attack with a malicious duplicate device*

This scenario describes an attack, where the communication partner has been replaced with a malicious relay box. This attack is prevented by mutual distance and angle measurement and verification, as described in Section VI-D. Fig. 6 illustrates the situation for an attacker. Relay box B would need to have the exact relative position as Alice and relay box A. Even then, the attack could be detected by 3D recognition.

D. *Relay attack by laser reflection*

We consider this an unlikely attack scenario. It involves an attacker pointing a modulated IR laser beam onto a communication partner to override its light source. Despite the fact that a IR-laser could create a signature similar to the illumination unit of a Time-of-Flight system, this attack faces the same issues as the previous duplicate device attack scenario.

VIII. Conclusion

In this work, we addressed relay attacks, which still pose a threat to RF-based secure communication. Concepts to enhance security in this field through location-awareness were reviewed. We showed camera based communication efforts, and how they could benefit security applications.

Finally, we introduced our OptiSec3D security concept. It is a work-in-progress concept, supported by a proof-of-concept prototype. Attack scenarios were identified and analyzed in this work. We conclude, that our system can immensely reduce the risk of relay attacks.

Future work involves the implementation of the OptiSec3D concept in form of a secure communication system, which can be easily integrated into embedded systems.

Acknowledgment

The authors would like to thank the Austrian Federal Ministry for Transport, Innovation and Technology as well as the ARTEMIS Joint Undertaking, which funded the research activities under the grant agreement n° 852328 and n° 621429 respectively.

References

[1] A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," in *Network and Distributed System Security Symposium (NDSS)*, February 2011.

[2] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, *Advances in Cryptology - CRYPTO 2009: 29th Annual International Cryptology Conference*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, ch. Position Based Cryptography, pp. 391–407.

[3] N. Druml, G. Fleischmann, C. Heidenreich, A. Leitner, H. Martin, T. Herndl, and G. Holweg, "Time-of-Flight 3D Imaging for Mixed-Critical Systems," in *13th International Conference on Industrial Informatics (INDIN)*, July 2015, pp. 1432–1437.

[4] R. Lange and P. Seitz, "Solid-state time-of-flight range camera," *IEEE Journal of Quantum Electronics*, vol. 37, no. 3, pp. 390–397, March 2001.

[5] M. Fischlin and C. Onete, *Applied Cryptography and Network Security: 11th International Conference (ACNS)*. Springer Berlin Heidelberg, 2013, ch. Terrorism in Distance Bounding: Modeling Terrorist-Fraud Resistance, pp. 414–431.

[6] A. Levi, E. Çetintaş, M. Aydos, Ç. K. Koç, and M. U. Çağlayan, *Computer and Information Sciences - ISCIS 2004*, ch. Relay Attacks on Bluetooth Authentication and Solutions.

[7] K. Haataja and P. Toivanen, "Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures," *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 384–392, January 2010.

[8] S. Drimer and S. J. Murdoch, "Keep your enemies close: Distance bounding against smartcard relay attacks," in *USENIX Security Symposium on USENIX Security Symposium*, ser. SS'07, 2007. [Online]. Available: http://dl.acm.org/citation.cfm?id=1362903.1362910

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

[10] Z. Kfir and A. Wool, "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard," in *Security and Privacy for Emerging Areas in Communications Networks*, September 2005, pp. 47–58.

[11] M. Roland, J. Langer, and J. Scharinger, "Applying relay attacks to Google Wallet," in *5th International Workshop on Near Field Communication (NFC)*, February 2013, pp. 1–6.

[12] T. R. Martin Hlavac, "A Note on the Relay Attacks on e-passports: The Case of Czech e-passports," in *IACR Eprint archive*, 2007. [Online]. Available: http://eprint.iacr.org/2007/244.pdf

[13] Y. Oren and A. Wool, "Rfid-based electronic voting: What could possibly go wrong?" in *RFID, IEEE International Conference*, April 2010.

[14] S. Brands and D. Chaum, "Distance-bounding Protocols," in *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT)*, 1994, pp. 344–359.

[15] A. Brelurut, D. Gerault, and P. Lafourcade, "Survey of Distance Bounding Protocols and Threats," in *International Symposium on Foundations & Practice of Security (FPS)*, 2015.

[16] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, *Security and Privacy in Ad-Hoc and Sensor Networks*, 2006, ch. So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks.

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

[18] L. Zhu, A. Yang, D. Wu, and L. Liu, *International Conference on Life System Modeling and Simulation*. Springer Berlin Heidelberg, 2014, ch. Survey of Indoor Positioning Technologies and Systems.

[19] L. Schauer, F. Dorfmeister, and M. Maier, "Potentials and limitations of WIFI-positioning using Time-of-Flight," in *International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, Oct 2013.

[20] J. Xiong and K. Jamieson, "SecureAngle: Improving Wireless Security Using Angle-of-arrival Information," in *ACM SIGCOMM Workshop on Hot Topics in Networks*, ser. Hotnets-IX, New York, NY, USA, 2010, pp. 11:1–11:6.

[21] J. Niu, B. Wang, L. Shu, T. Duong, and Y. Chen, "ZIL: An Energy-Efficient Indoor Localization System Using ZigBee Radio to Detect WiFi Fingerprints," *IEEE Journal on Selected Areas in Communications*, 2015.

[22] N. O. Tippenhauer, K. B. Rasmussen, C. Pöpper, and S. Čapkun, "Attacks on public wlan-based positioning systems," in *International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '09. New York, NY, USA: ACM, 2009, pp. 29–40.

[23] C. De Marziani, J. Urefia, A. Hernandez, M. Mazo, F. Alvarez, J. Garcia, J. Villadangos, and A. Jimenez, "Simultaneous measurement of times-of-flight and communications in acoustic sensor networks," in *IEEE International Workshop on Intelligent Signal Processing*, September 2005, pp. 122–127.

[24] C. Rohner, S. Raza, D. Puccinelli, and T. Voigt, "Security in visible light communication: Novel challenges and opportunities," *Sensors & Transducers Journal*, 2015.

[25] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *IEEE International Conference on Communications (ICC)*, June 2014, pp. 3342–3347.

[26] A. Mostafa and L. Lampe, "Physical-Layer Security for MISO Visible Light Communication Channels," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1806–1818, September 2015.

[27] S. Hranilovic and F. Kschischang, "A pixelated mimo wireless optical communication system," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 12, no. 4, pp. 859–874, July 2006.

[28] S. G. Vidyashree Kokane, "A Survey on Barcode Generation and Modulation Techniques," *IEEE Journal of Selected Topics in Quantum Electronics*, 2013.

[29] T. Hao, R. Zhou, and G. Xing, "Cobra: Color barcode streaming for smartphone systems," in *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '12. New York, NY, USA: ACM, 2012, pp. 85–98.

[30] T. Li, C. An, X. Xiao, A. T. Campbell, and X. Zhou, "Real-Time Screen-Camera Communication Behind Any Scene," in *13th Annual International Conference on Mobile Systems, Applications, and Services*, 2015.

[31] A. Mohan, G. Woo, S. Hiura, Q. Smithwick, and R. Raskar, "Bokode: imperceptible visual tags for camera based interaction from a distance," *ACM Transactions on Graphics (TOG)*, vol. 28, no. 3, p. 98, 2009.

[32] Google, "ATAP Project Tango – Google," 2 2014. [Online]. Available: http://www.google.com/atap/projecttango/

[33] W. Yuan, R. Howard, K. Dana, R. Raskar, A. Ashok, M. Gruteser, and N. Mandayam, "Phase messaging method for time-of-flight cameras," in *IEEE International Conference on Computational Photography (ICCP)*, May 2014.

[34] H. Plank, M. Almer, R. Lobnik, C. Steger, T. Ruprechter, H. Bock, J. Haid, G. Holweg, and N. Druml, "OptiSec3D - A new Paradigm in Secure Communication and Authentication featuring Time-of-Flight," in *International Conference on Embedded Wireless Systems and Networks (EWSN)*, February 2016.

[35] J. McCune, A. Perrig, and M. Reiter, "Seeing-is-believing: using camera phones for human-verifiable authentication," in *IEEE Symposium on Security and Privacy*, May 2005, pp. 110–124.

[36] B. Zhang, K. Ren, G. Xing, X. Fu, and C. Wang, "SBVLC: Secure barcode-based visible light communication for smartphones," in *INFOCOM, 2014 Proceedings IEEE*, April 2014, pp. 2661–2669.

[37] M. Xie, L. Hao, K. Yoshigoe, and J. Bian, *Security and Privacy in Communication Networks: 9th International ICST Conference, SecureComm 2013, Sydney, NSW, Australia, September 25-28, 2013, Revised Selected Papers*. Springer International Publishing, 2013, ch. CamTalk: A Bidirectional Light Communications Framework for Secure Communications on Smartphones, pp. 35–52.

[38] S. Izadi, D. Kim, O. Hilliges, D. Molyneaux, R. Newcombe, P. Kohli, J. Shotton, S. Hodges, D. Freeman, A. Davison, and A. Fitzgibbon, "KinectFusion: Real-time 3D Reconstruction and Interaction Using a Moving Depth Camera," in *ACM Symposium on User Interface Software and Technology*, 2011, pp. 559–568.

[39] N. Erdogmus and S. Marcel, "Spoofing Face Recognition With 3D Masks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1084–1097, July 2014.