Are We Really Close? Verifying Proximity in Wireless Systems

Aanjhan Ranganathan and Srdjan Capkun | ETH Zurich

Current proximity verification and ranging systems are vulnerable to distance modification attacks that can lead to loss of property. Design recommendations for securely proving proximity in wireless systems are presented.

It's Friday, late afternoon, and Jane is delighted that her hectic work week has ended. On her way home, she stops at a nearby store. Her flying drone follows a few meters behind, filming her movements and making her feel safer. In the store, Jane selects her groceries and then simply taps her credit card on the payment terminal to purchase them. A second later, a beep indicates that the card was sensed to be in the terminal's proximity and that the payment transaction was successful. Jane picks up her bags and heads to the car. As she approaches it, the door unlocks and the trunk opens, allowing her to unload the goods without having to search for her keys. When she arrives home, her house door unlocks and opens after it senses that her keys are in close proximity. Her friends come over for dinner, and as they physically enter her home, their devices automatically gain access to her Wi-Fi connection as well as to multimedia that Jane selected for them. Jane doesn't worry about strangers accessing her data because it's only accessible by devices physically located in her home.

Today, we live in a physical world in which diverse applications depend on location and proximity information. The above story illustrates this through a mix of existing and future applications.

Contactless access tokens (such as contactless smart/proximity cards and key fobs) are prevalent in numerous systems, including public transport ticketing, parking and highway toll fee collection, payment systems, electronic passports, physical access control, and personnel tracking. In a typical access control application, an authorized person simply taps a smart card against a card reader set up at the entrance to gain access to an infrastructure. Smart card–based physical access control and authentication are deployed even in safety- and security-critical infrastructures such as nuclear power plants and defense research organizations. Similarly, in an electronic payment scenario, the consumer places a contactless card in close proximity (a few centimeters) to the payment terminal to make secure payments. Furthermore, modern automobiles use passive keyless entry systems (PKESs) to unlock, lock, or start the vehicle—without any user interaction—when the key fob is in close proximity. PKESs also enhances security in scenarios such as a user forgetting to manually lock the car or a jamming attack. In all these systems, proximity between two entities is verified based on their ability to communicate with each other.

Even though the communication range for many such wireless systems is assumed to be limited, several works have demonstrated that they're vulnerable to relay attacks.[1,2] In a relay attack (see Figures 1 and 2), an attacker uses a proxy device to relay the communications between two legitimate entities without requiring any knowledge of the actual data being transmitted and, therefore, independent of any cryptographic primitives implemented. In one study, researchers were able to unlock a car and drive away even though the legitimate key was several hundred meters away from the vehicle.[1]

1540-7993/17/$33.00 © 2017 IEEE

In addition to relay attacks, an attacker can also modify the measured distance by manipulating or building specialized radio hardware or by colluding with other entities. Thus, distance modification attacks have serious implications: an attacker can gain entry into a restricted area, make fraudulent payments, or steal a car by simply relaying the communications between the reader and the card that's several meters away—all without the card owner's knowledge.

Given the implications of such attacks, there's a clear need for proximity systems that are secure against modern-day cyber-physical attacks. To prove proximity in wireless systems, estimating the physical distance between two or more entities is fundamental.

Establishing Proximity

Establishing proximity requires estimating the physical distance between two or more wireless entities. Typically, this is done by either observing the changes in the signal's physical properties (amplitude, phase, and so on) that occur as the signal propagates, or estimating the time the signal takes to travel between the entities.

Received Signal Strength–Based Distance Estimation

Radio signals lose signal strength as they travel through media such as free space or air (see Figure 3). The amount of signal strength lost or attenuated is proportional to the square of the distance traveled. Mathematically, the exact distance *d* between the transmitter and the receiver can be calculated based on the free-space path loss equation. In reality, the signal experiences additional losses due to its interaction with objects in the environment, which are difficult to accurately account for. This directly affects the computed distance's accuracy; therefore, advanced models such as Rayleigh fading and log distance path loss are typically used to improve distance estimation accuracy. Bluetooth-based proximity sensing tags (for example, Apple iBeacon; developer.apple.com/ibeacon), which are prevalent today, use the received Bluetooth signal's strength—also referred to as the received signal strength indicator (RSSI) value—as a proximity measure. For example, an alarm might sound if the tagged key or item exceeds a set threshold for RSSI values, indicating that the item might be farther away than necessary. Current automobile PKESs also use received signal strength (RSS) distance estimation to infer proximity.

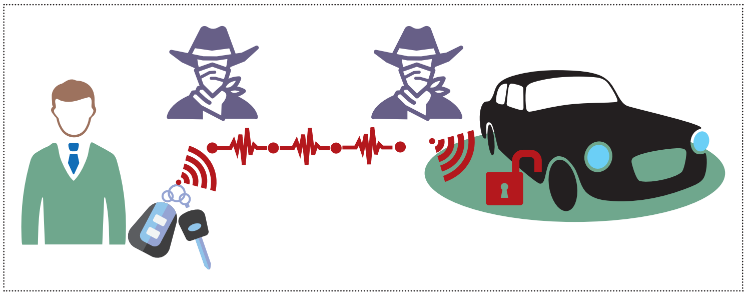

Figure 1. Relay attack on passive keyless entry systems in automobiles. In relay attacks, the attacker uses a proxy device to relay communications between two legitimate entities without knowing the data being transmitted (and independent of any cryptographic primitives).

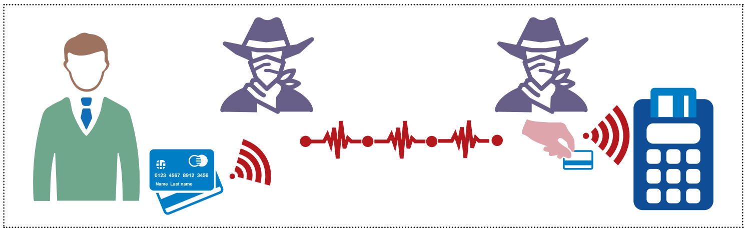

Figure 2. Relay attack on contactless payment systems.

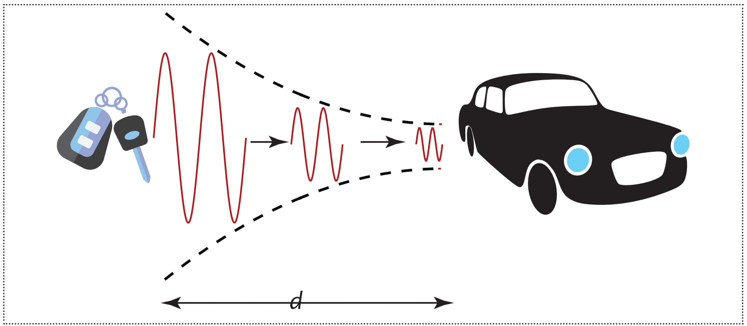

Figure 3. Received signal strength (RSS)-based distance estimation. As radio signals travel through air, they lose strength proportional to the square of the distance *d* traveled.

Phase-Based Distance Estimation

An alternative way to measure distance is to use the phase of the RF signal. Two devices can measure the distance between them by estimating the phase difference between a received continuous wave signal and a local reference signal. Consider the scenario of a car trying to estimate its proximity to a key fob. The car begins ranging by transmitting a continuous wave sinusoid signal. The key fob locks its local oscillator to this incoming signal and transmits it back to the car. The car measures the distance based on the difference in the phase of the received signal and its own reference signal (shown in Figure 4). The need to keep track of the number of whole cycles elapsed is eliminated by using signals of different frequencies, which is typically referred to as multicarrier phase–based ranging.

Due to its low complexity and low power requirements, multicarrier phase ranging (for example, Atmel AVR2152; www.atmel.com) is a cost-optimized

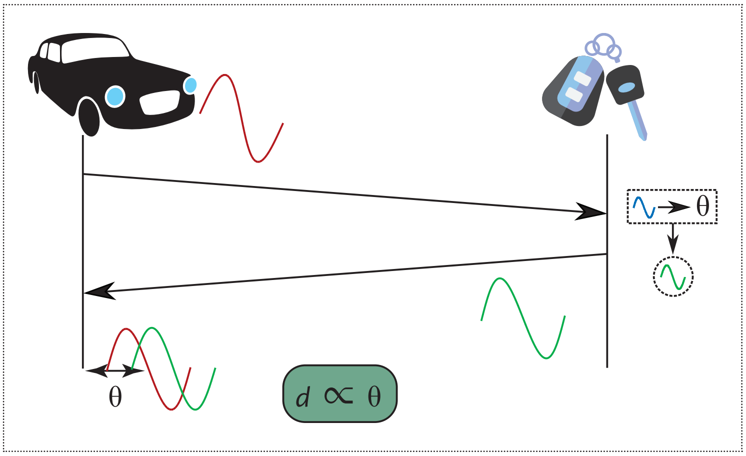

Figure 4. Phase-based distance estimation. Two devices can measure the distance between them by estimating the phase difference between a received continuous wave signal and a local reference signal.

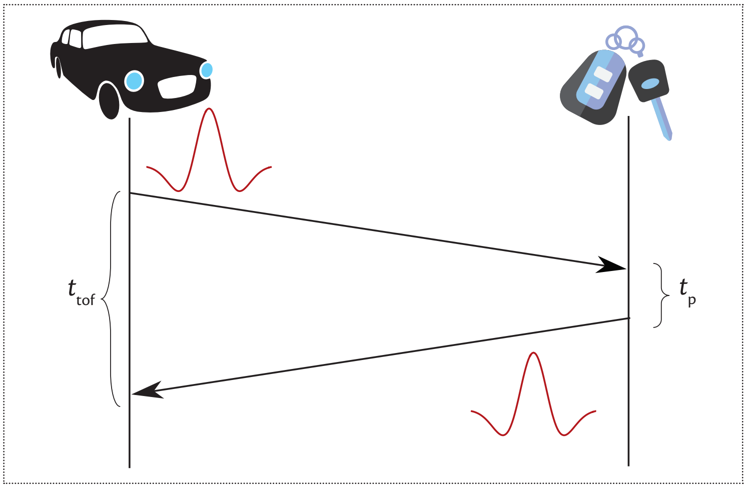

Figure 5. Ultrawideband time of flight–based ranging. Round-trip time is the time that elapses between transmitting a ranging data packet and receiving an acknowledgment in return. t_{tof} is measured round-trip time; t_{p} is processing delay.

solution for many applications, including the positioning of ultra-high-frequency RFID systems. Furthermore, by leveraging the proliferation of 802.11 Wi-Fi networks and the availability of carrier phase information directly from the network cards, several indoor localization schemes now use commodity Wi-Fi cards to achieve centimeter-level precision.[3,4] Note that a majority of today's radar systems use techniques similar to phase-based ones to determine target objects' distance and speed.

Time of Flight–Based Distance Estimation

The time taken for radio waves to travel from one point to another can also be used to measure distance. In time of flight (ToF)-based distance estimation, knowing the signal's propagation speed (for instance, radio signals travel at approximately the speed of light), the distance d between two entities is given by $d = (t_{\text{rx}} - t_{\text{tx}}) \cdot c$, where c is the speed of light and t_{tx} and t_{rx} represent the time of transmission and reception, respectively. The measured ToF can be either one way or round-trip. One-way ToF measurement requires the clocks of the measuring entities to be tightly synchronized. Errors due to mismatched clocks are compensated for in round-trip ToF measurement.

Round-trip time is the time that elapses between transmitting a ranging data packet and receiving an acknowledgment in return. For example, as shown in Figure 5, the distance between the car and the key fob is given by $d = c \cdot (t_{\text{tof}} - t_{\text{p}})/2$, where t_{tof} is the measured round-trip time and t_{p} is the processing delay (that is, the time the key fob takes to receive, process, and transmit the acknowledgment back to the automobile). The precise distance measurement largely depends on the system's ability to estimate the time of arrival and the RF signal's physical characteristics. As a general rule, the ranging precision is directly proportional to the ranging signal's bandwidth. Depending on the required accuracy level, ToF-based distance measurement systems use either impulse-radio ultrawideband (IR-UWB) or chirp spread spectrum (CSS) signals. IR-UWB systems provide centimeter-level precision; the precision of CSS systems is on the order of 1 to 2 m. Several commercially available wireless systems use round-trip ToF for distance measurement, including PulsON (www.timedomain.com), 3db Midas (www.3db-technologies.com), DecaWave (www.decawave.com), and Zebra (www.zebra.com).

Attacking Proximity

All these proximity-based wireless access control and authentication systems are insecure and vulnerable to distance modification attacks. An attacker can exploit both data-layer and physical-layer weaknesses to manipulate the distance. Data-layer attacks can often be prevented by implementing strong cryptographic primitives. However, physical-layer attacks are of significant concern because they can be executed independent of any higher-layer cryptographic primitive. Today, with the increasing availability of low-cost software-defined radio systems, an attacker can easily eavesdrop, modify, compose, and (re)play radio signals. Thus, the attacker has full control of the wireless communication channel and can manipulate any message transmitted between the two entities.

We focus in this article on physical-layer distance manipulation attacks. More specifically, we focus on distance reduction attacks, which have been proven detrimental to the security of various systems and have resulted in loss of property. As described previously, an attacker can steal a car or make fraudulent payments by simply reducing the distance measured even when the automobile or payment card owner is far away. We describe how an attacker can manipulate the measured distance independent of any higher-level cryptographic authentication implemented, thereby gaining unauthorized access. To maintain generality, we will hereafter refer to the entity that estimates the distance as the *verifier* (for example, an automobile or a payment terminal) and the entity whose proximity is estimated as the *prover* (for example, a key fob or a contactless payment card).

Attacks on RSS- and Phase-Based Proximity Systems

In an RSS-based distance estimation attack, an attacker can manipulate the measured distance by manipulating the RSS at the verifier. For example, as illustrated in Figure 6, the attacker can simply amplify the signal transmitted by the prover before relaying it to the verifier. This will result in an incorrectly estimated distance at the verifier. Commercially available solutions such as SecuKey (www.secukey.org) claim to secure modern PKESs against relay attacks by reducing or attenuating the transmitted signal's power. An attacker can trivially circumvent such countermeasures by using higher-gain amplifiers and receiving antennas. Furthermore, applications such as NearLock (nearlock.me) and BlueProximity (sourceforge.net/projects/blueproximity) rely on the received Bluetooth signal strength to estimate distance between the laptop and the phone, and based on this, the laptop is automatically locked or unlocked. These systems are also vulnerable to amplify and relay attacks such that an attacker could unlock a laptop even with the authentic user far away.

Similarly, an attacker can manipulate the estimated distance between the verifier and prover in systems that use the radio signal's phase or frequency property. For instance, the attacker can exploit the maximum measurable property of phase- or frequency-based distance measurement systems and execute distance reduction attacks. The maximum measurable distance—the largest value of distance d_{max} that can be estimated using a phase-based proximity system—directly depends on the maximum measurable phase. Given that the phase value ranges from 0 to 2π and then rolls over, the maximum measurable distance also rolls over after a certain value.

An attacker can leverage the system's maximum measurable distance property to execute a distance-decreasing relay attack. During the attack, the attacker relays (amplifies and forwards) the verifier's interrogating signal to the prover. The prover determines the interrogating signal's phase and retransmits a response signal that is phase-locked with the verifier's interrogating signal. Then, as illustrated in Figure 6, the attacker receives the prover's response signal and forwards it to the verifier—but with a time delay (Δ_t). The attacker chooses a time delay such that the measured phase difference reaches its maximum value of 2π and rolls over. Prior work has shown that it's possible to reduce the measured distance by more than 50 m.[5] In other words, the attacker proved to the verifier that the prover was in close proximity (approximately 1 m away) even though the prover was more than 50 m from the verifier.

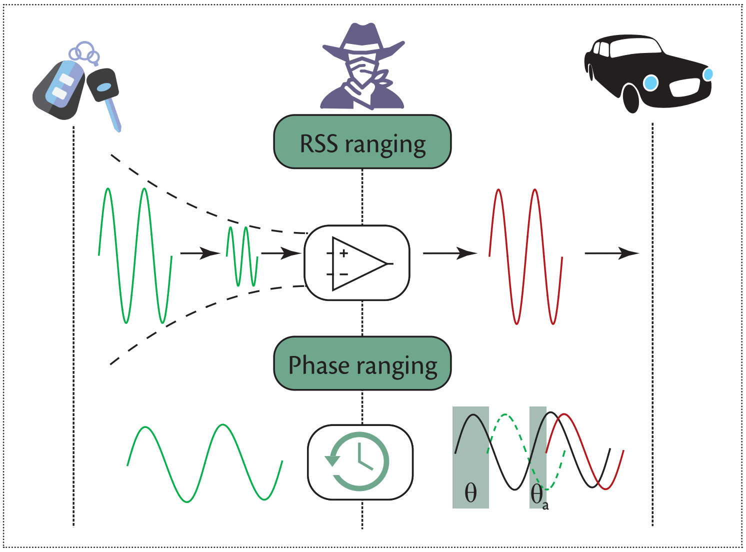

Figure 6. RSS indicator and phase-ranging attacks. In RSS-ranging systems, the attacker can simply amplify the signal transmitted by the prover (the entity whose proximity is estimated) before relaying it to the verifier (the entity that estimates the distance). In phase-ranging systems, the attacker doesn't amplify the signal but instead forwards it to the verifier with a time delay long enough to force the measured phase-difference to roll over.

Attacks on Time-of-Flight Systems

We now consider the security of ToF-based distance measurement. Recall that in ToF-based ranging systems, distance is estimated based on the time elapsed between the verifier transmitting a ranging packet and receiving an acknowledgement back from the prover. To reduce the distance measured, an attacker must decrease the signal's round-trip ToF. An attacker can reduce estimated distance by leveraging deterministic signaling or long symbol lengths. Remember that a 10-ns decrease in the time estimate can result in a distance reduction of 1.5 m.

Leveraging deterministic signaling. This first attack type leverages the predictable nature of the data in ranging and acknowledgment packets. For instance, several ToF

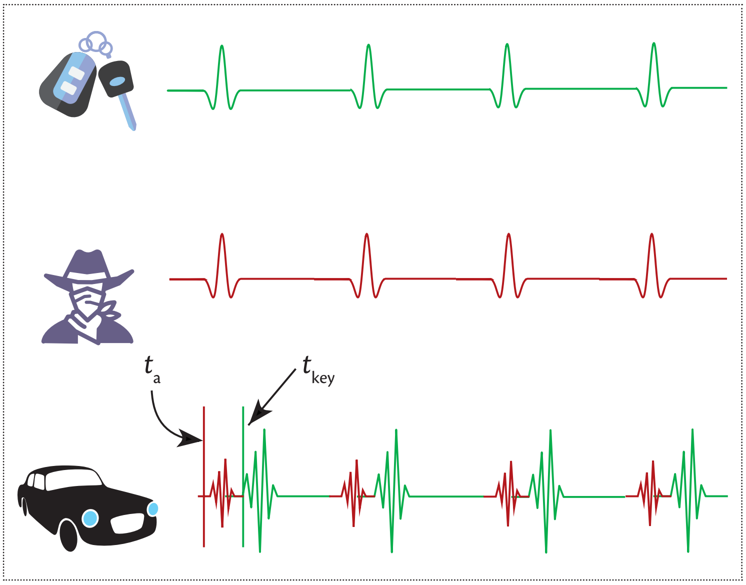

Figure 7. Cicada attack. The attacker continuously transmits a "1" impulse with a power greater than the prover's. This degrades the performance of energy detection–based receivers, resulting in reduced distance measurements.

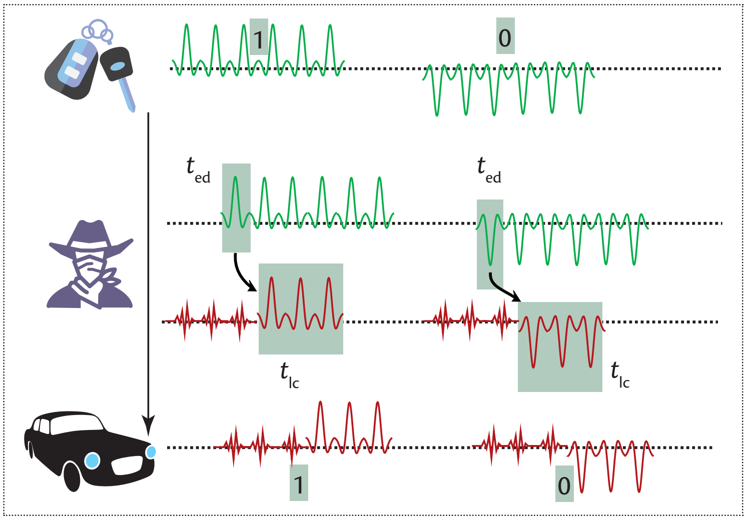

Figure 8. Early-detect and late-commit attacks. An attacker can predict the bit (early detect; t_{ed}) even before completely receiving the symbol. The attacker then stops transmitting the arbitrary signal and switches, or "commits," to the bit corresponding to the predicted symbol (late commit; t_{lc}). Even though the received symbol contains an arbitrary signal at first, the car will correctly decode the symbol with the data that was committed late by the attacker.

ranging systems use predefined data packets for ranging, making it trivial for attackers to predict and generate their own ranging or acknowledgment signal and then transmit the acknowledgment packet even before receiving the challenge ranging packet.

Studies have shown that the de facto standard for IR-UWB, IEEE 802.15.4a, doesn't automatically provide security against distance-decreasing attacks.[6–8] Attackers were able to decrease the measured distance by as much as 140 m by predicting the preamble and payload data with more than 99 percent accuracy even before receiving the entire symbol. For example, in a Cicada attack, the attacker continuously transmits a "1" impulse with a power greater than that of the prover. This degrades the performance of energy detection–based receivers, resulting in reduction of the distance measurements as illustrated in Figure 7. To prevent such attacks, it's important to avoid predefined or fixed data during the time-critical phase of the distance estimation scheme.

Leveraging long symbol lengths. In addition to having the response packet depend on the challenge signal, the way in which the challenge and response data are encoded in the radio signals affects the security guarantees provided by the ranging or localization system. An attacker can predict the bit (early detect) even before receiving the symbol completely.[9] Furthermore, the attacker can leverage the robustness property of modern receivers and transmit an arbitrary signal until the correct symbol is predicted. Once the bit is predicted, the attacker stops transmitting the arbitrary signal and switches to the bit corresponding to the predicted symbol; that is, the attacker "commits" to the predicted symbol (late commit). Figure 8 illustrates early-detect and late-commit attacks. Imagine that the key fob transmits 1s and 0s using a series of UWB pulses. In such a scenario, the attacker needn't wait for the entire series of pulses to be received before detecting the data being transmitted. After a time t_{ed}, the attacker would be able to correctly predict the symbol. Meanwhile, the attacker can transmit an arbitrary signal toward the car while trying to determine the signal transmitted by the key. Once the symbol is determined, the attacker transmits the correct signal to the car. Modern receivers are designed to be robust, and therefore, they're capable of detecting the symbol correctly even if all the pulses aren't received. The attacker exploits this property—even though the received symbol contains an arbitrary signal at first, the car will correctly decode the symbol with the data that was committed late by the attacker.

As previously described, round-trip ToF systems are implemented either using CSS or IR-UWB signals. Due to their long symbol lengths, both implementations are vulnerable to early-detect and late-commit attacks.[6,10] With chirp-based systems, an attacker can decrease the distance by more than 160 m and, in some scenarios, up to 700 m. Although IR-UWB pulses are short (typically 2 to 3 ns), data symbols (such as challenges and responses) are typically exchanged using a series of UWB pulses. Furthermore, the IEEE 802.15.4a

Table 1. Summary of distance estimation methods and their ability to prove proximity.

Method	Attack	Proof of proximity*
Received signal strength	Amplify and relay	None
Phase or frequency	Delay and relay	None
Time of flight (ToF)		
802.15.4a chirp spread spectrum	Early detect, late commit	Partial
802.15.4a impulse-radio ultrawideband (IR-UWB)	Early detect, late commit	Partial
Short symbol IR-UWB	No attack†	Yes

**The proof-of-proximity estimate holds true only if a challenge–response protocol is implemented.*

†In addition to keeping symbol durations short, it's necessary to implement specialized modulation and decoding techniques to prevent attacks such as Cicada.[8]

IR-UWB standard allows long symbol lengths, ranging from 32 ns to 8 µs. Therefore, even the smallest symbol length of 32 ns allows an attacker to reduce the distance by as much as 10 m by performing early-detect and late-commit attacks.

Thus, to guarantee proximity and secure wireless proximity systems against early-detect and late-commit attacks, the symbol length must remain as short as possible.

Proving Proximity

Proving proximity in wireless systems isn't a trivial task and must satisfy numerous design requirements to be secure, which we detail here.

Round-Trip Time of Flight

First, it's important to select the distance estimation approach that will be hardest for the attacker to manipulate. Both RSS- and phase-based distance estimation techniques allow the attacker to falsify proximity by simply amplifying or delaying the radio signals without any knowledge of the actual data being exchanged. However, in ToF-based distance estimation, attackers can't succeed just by forwarding the signals; they must actively receive, interpret, reconstruct, and transmit the appropriate signal back to the verifier. Thus, round-trip ToF-based distance estimation raises the bar for the attacker and should be considered a first design choice for proving proximity in wireless systems.

Challenge–Response Protocol

Even though round-trip ToF-based distance estimation significantly raises the bar for the attacker, securing it isn't easy. A primary attack vector in such systems is to exploit the fixed response or acknowledgment currently used by several wireless systems. Therefore, it's essential to prevent the attacker from guessing and transmitting the acknowledgment packet even before receiving the verifier request. In other words, a challenge–response protocol must be implemented in which the round-trip time is measured as the time elapsed between transmitting a randomly chosen challenge and receiving a corresponding response back from the prover. Note that currently proposed standards such as IEEE 802.15.4a/f (www.ieee802.org) don't have a provision for authenticated acknowledgments. Because there's no support for challenge–response protocols, systems implementing these standards are vulnerable to not only physical-layer Cicada attacks but also simple message replay attacks.

Short Symbol Duration

As a final requirement, it's essential to keep the symbol duration as short as possible to prevent early-detect and late-commit attacks. IR-UWB systems use very short pulses to transmit and receive data, making them preferable over other signaling techniques for securely proving proximity. However, currently proposed standards (IEEE 802.15.4a/f) allow long symbol durations; therefore, system implementations based on these standards remain vulnerable to distance reduction attacks. On the other hand, short symbol durations restrict devices from reliably operating over longer distance measurements. Some commercial systems (www.3db-technologies.com) implement a proprietary IR-UWB physical layer with short symbol lengths in addition to specialized modulation and time-of-arrival estimation techniques; they claim a maximum possible distance reduction of less than a meter while still being able to estimate proximity from more than 200 m.

We summarize our observations in Table 1. Our conclusion is that ToF-based distance measurement using short symbol length IR-UWB signals is the best way to securely guarantee proximity.

With the rapid deployment of wireless systems today, various applications ranging from payment systems to access control for critical infrastructures depend on location and proximity information. And with the advent of the Internet of Things and autonomous cyber-physical systems, this dependency on location and proximity will only increase. Therefore, it's essential to design and implement proximity systems that are secure against modern day cyber-physical attacks. After surveying the various approaches currently used to determine proximity and analyzing their resilience against distance modification attacks, we conclude that ToF-based distance measurement using short symbol length IR-UWB signals is the best way to securely prove proximity. ■

References

1. A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," *Proc. Network and Distributed System Security Symp.* (NDSS 11), 2011; eprint.iacr.org/2010/332.pdf.
2. L. Francis et al., "Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones," *Proc. 6th Int'l Conf. Radio Frequency Identification: Security and Privacy Issues* (RFIDSec 10), 2010, pp. 35–49.
3. D. Vashisht, S. Kumar, and D. Katabi, "Decimeter-Level Localization with a Single WiFi Access Point," *Proc. USENIX Conf. Networked Systems Design and Implementation* (NSDI 16), 2016, pp. 165–178.
4. R. Miesen et al., "360 Degree Carrier Phase Measurement for UHF RFID Local Positioning," *Proc. IEEE Int'l Conf. RFID-Technologies and Applications* (RFID-TA 13), 2013; doi.org/10.1109/RFID-TA.2013.6694499.
5. H. Ólafsdóttir, A. Ranganathan, and S. Capkun, "On the Security of Carrier Phase-Based Ranging," ArXiv e-prints, 2016; arxiv.org/abs/1610.06077.
6. M. Poturalski et al., "Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures," *IEEE Trans. Wireless Communications*, vol. 10, no. 4, 2011, pp. 1334–1344.
7. M. Flury et al., "Effectiveness of Distance-Decreasing Attacks against Impulse Radio Ranging," *Proc. 3rd ACM Conf. Wireless Network Security* (WiSec 10), 2010, pp. 117–128.
8. M. Poturalski et al., "The Cicada Attack: Degradation and Denial of Service in IR Ranging," *Proc. IEEE Int'l Conf. Ultra-Wideband* (ICUWB 10), 2010; doi.org/10.1109/ICUWB.2010.5616900.
9. J. Clulow et al., "So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks," *Proc. 3rd European Workshop Security in Ad-Hoc and Sensor Networks* (ESAS 06), 2006, pp. 83–97.
10. A. Ranganathan et al., "Physical-Layer Attacks on Chirp-Based Ranging Systems," *Proc. 5th ACM Conf. Security and Privacy in Wireless and Mobile Networks* (WiSec 12), 2012, pp. 15–26.

Aanjhan Ranganathan is a senior researcher in the System Security Group at ETH Zurich and a visiting assistant professor at Northeastern University. His research focuses on the physical-layer security of wireless systems, including secure localization and ranging, GPS security, and (anti-)jamming techniques. Ranganathan received a PhD in computer science from ETH Zurich. Contact him at aanjhan@northeastern.edu.

Srdjan Capkun is a full professor in the Department of Computer Science at ETH Zurich and director of the Zurich Information Security and Privacy Center. His research interests include system and network security, particularly wireless security. Capkun received a PhD in communication systems from the École Polytechnique Fédérale de Lausanne. Contact him at capkuns@inf.ethz.ch.