CyBOK

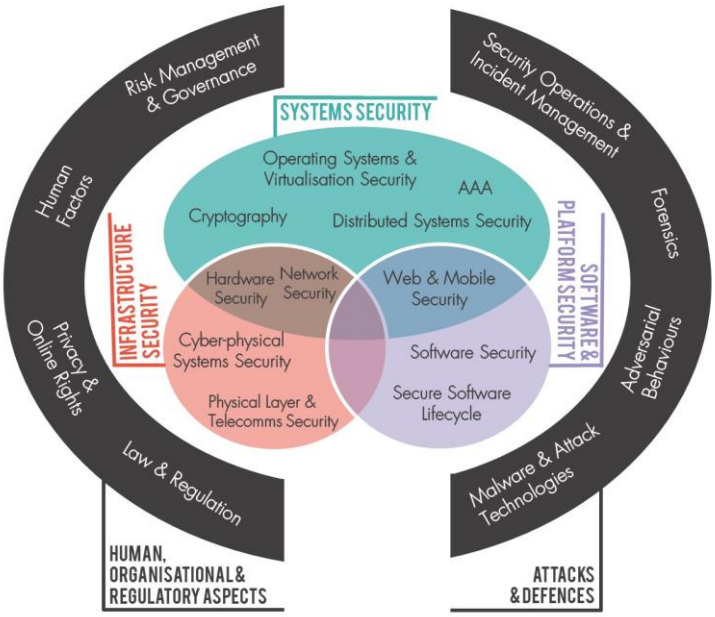
PHYSICAL LAYER & TELECOMMUNICATIONS SECURITY KNOWLEDGE AREA

(DRAFT FOR COMMENT)

AUTHOR: Srdjan Capkun – ETH Zurich

EDITOR: George Danezis – University College, London

Following wide community consultation with both academia and industry, 19 Knowledge Areas (KAs) have been identified to form the scope of the CyBOK as shown in the diagram below. The Scope document provides an overview of these top-level KAs and the sub-topics that should be covered under each and can be found on the project website: https://www.cybok.org/.



We are seeking comments within the scope of the individual KA; readers should note that important related subjects such as risk or human factors have their own knowledge areas.

It should be noted that a fully-collated CyBOK document which includes issue 1.0 of all 19 Knowledge Areas is anticipated to be released by the end of July 2019. This will likely include updated page layout and formatting of the individual Knowledge Areas.

Physical Layer and Telecommunications Security

Srdjan Capkun

January 2019

PHYSICAL LAYER SECURITY

1 Introduction

This chapter is a review of the most relevant physical-layer security topics. It first covers the main techniques that were developed to make use of the physical communication layer for confidentiality, integrity, access control and covert communication. These techniques, therefore, use the properties of physical layer modulations and signal propagation to enhance the security of systems. This is followed by a review of the techniques for the physical communication for device identification (i.e., device fingerprinting).

This chapter then continues with a review of the security issues related to the wireless physical layer, especially in those aspects that make wireless communication systems different from wired systems. In particular, jamming resilience and signal annihilation.

The security of global navigation systems and of terrestrial positioning systems is then covered in separate subsections as the security goals of these systems are different from communication systems and are mainly related to position spoofing resilience.

Finally, unintentional emanations from devices such as from computer displays computing systems are covered. followed by a brief review of spoofing of analogue sensors, which are in their nature different from communication systems, given that these interactions are not structured. Namely, they are not designed to carry information.

2 Physical Layer Schemes for Confidentiality, Integrity and Access Control

[1, c13][2][3][4][5]

Securing wireless networks is challenging due to the shared broadcast medium, which makes it easy for remote adversaries to eavesdrop, modify and block communication between wireless devices. However, wireless communication also offers some unique opportunities. Radio signals are affected by reflection, diffraction, or scattering, all of which contribute to the complex multipath behaviour of communicated signals. The channel response as measured at the receiver can, therefore, be modelled as having frequency and position-dependent random components. In addition, within the short time span and in the absence of interference, communicating parties measure highly correlated channel responses. These responses, can therefore, be used as shared randomness, unavailable to the adversary, and form a basis of secure communication.

2.1 Key Establishment based on Channel Reciprocity

One of the main security assumptions of physical-layer key establishment schemes is that the attacker is located at least half a wavelength away from the communicating parties. Given this, it can be assumed that the attacker's channel measurements will be de-correlated from those computed by the communicating parties. The attacker will, therefore, not have access to the measured secret randomness. If the attacker injects signals during the key generation, the signal that it transmits will, due to channel distortions, be measured differently at communicating parties, resulting in key disagreement.

Physical layer key establishment schemes are executed as follows. The communicating parties (Alice and Bob) first exchange pre-agreed, non-secret data packets. Each party then measures the channel response over the received packets. The key agreement is then typically executed in three phases.

Quantisation Phase: Alice and Bob create a time series of channel properties that are measured over the received packets. Example properties include received signal strength indicator (RSSI) and the channel impulse response (CIR). Any property that is believed to be non-observable by the attacker can be used. The measured time series are then quantised by both parties independently. This quantisation is typically based on fixed or dynamic thresholds.

Information Reconciliation Phase: Since the quantisation phase is likely to result in disagreeing sequences at Alice and Bob, they need to reconcile their sequences to correct for any errors. This is typically done by leveraging error correcting codes and privacy amplification techniques.

Key Verification Phase: In this last phase, the communicating parties confirm that they have established a shared secret key. If this step fails, the parties need to restart the key establishment.

Most of the research on physical-layer techniques has been concerned with the choice of channel properties and of the quantisation technique. Even if physical-layer key establishment techniques seem attractive, many have been shown to be vulnerable to active, physically distributed and multi-antenna adversaries. However, in a number of scenarios where the devices are mobile, and where the attacker is restricted, they can be a valuable replacement for or enhancement to traditional public-key key establishment techniques.

2.2 MIMO-supported approaches: Orthogonal Blinding, Zero-Forcing

Initially, physical-layer key establishment techniques were proposed in the context of single-antenna devices. However, with the emergence of multi-antenna, multiple input multiple output (MIMO) devices and beam-forming, researchers have proposed to leverage these new capabilities to further secure communication. Two basic techniques that were proposed in this context are orthogonal blinding and zero forcing. Both of these techniques aim to enable all of the transmitter to wirelessly send confidential data to the intended receiver, while preventing the colocated attacker from receiving this data. Although this might seem unfeasible, since as well as the intended receiver, the attacker can receive all transmitted packets. However, MIMO systems allow transmitters to 'steer' the signal towards the intended receiver. For beam-forming to be effective, the transmitter needs to know some channel information for the channels from its antennas to the antennas of the receiver. As described in [REF], these channels are considered to be secret to the

attacker. In Zero-Forcing, the transmitter knows the channels to the intended receiver as well as to the attacker. This allows the transmitter to encode the data such that they can be measured at the receiver, whereas the attacker measures nothing related to the data. In many scenarios, the knowledge of the channel to the attackers is unrealistic. In Orthogonal Blinding, the transmitter does not know the channel to the attacker but knows the channels to the receiver. The transmitter then encodes the data in a way that the receiver can decode them, whereas the attacker will receive data mixed with random noise. The attacker, therefore. cannot decode the data. As in [REF], in order to communicate securely, the transmitter and the receiver do not need to share any secrets. Instead, the transmitter only needs to know (or measure) the channels to the intended receivers. Like physical-layer key establishment techniques, these techniques have been show to be vulnerable to multi-antenna and physically distributed attackers. They have also been shown to be vulnerable to known-plaintext attacks.

2.3 Friendly Jamming

Similar to Orthogonal Blinding, Friendly Jamming schemes use signal interference generated by collaborating devices to either prevent an attacker from communicating with the protected device, or to prevent the attacker from eavesdropping on messages sent by protected devices. Friendly Jamming can, therefore, be used for both confidentiality and access control. Unlike Orthogonal Blinding, Friendly Jamming does not leverage the knowledge of the channel to the receiver. If a collaborating device (i.e., the friendly jammer) wants to prevent unauthorised communication with the protected device it will jam the receiver of the protected device. If it wants to prevent eavesdropping, it will transmit jamming signals in the vicinity of the protected device. Preventing communication with a protected device requires no special assumptions about the location of the collaborating devices. However, protecting against eavesdropping requires that the eavesdropper is unable to separate the signals from the protected device from those originating at the collaborating device. For this to hold, the channel from the protected device to the attacker should not be correlated with the channel from the collaborating device to the attacker. To ensure this, the protected device and the collaborating device need to be typically placed less than half a carrier wavelength apart. However, it has been shown that under some conditions, a multi-antenna attacker will still be able to separate these signals and recover the transmitted messages.

Friendly Jamming was originally proposed for the protection of those medical implants (e.g., already implanted pacemakers) that are unable to perform cryptographic operations. The main idea was that the collaborating device (i.e., 'the shield') would be placed around the user's neck, close to the pacemaker. This device would then simultaneously receive and jam all communication from the implant. The shield would then be able to communicate the received messages to any other authorised device using standard cryptographic techniques.

2.4 Using Physical Layer to Protect Data Integrity

Research into the use of physical layer for security is not only limited to the protection of data confidentiality. Physical layer can also be leveraged to protect data integrity. This is illustrated by the following scenario. Assuming that two entities (Alice and Bob) share a common radio communication channel, but do not share any secrets or authentication material (e.g., shared keys or authenticated public keys), how can the messages exchanged between these entities be

authenticated and how can their integrity be preserved in the presence of an attacker? Here, by message integrity, we mean that the message must be protected against any malicious modification, and by message authentication we mean that it should be clear who the sender of the message is.

One basic technique that was proposed in this context are integrity codes, a modulation scheme that provides a method of ensuring the integrity (and a basis for authentication) of a message transmitted over a public channel. Integrity codes rely on the observation that, in a mobile setting and in a multipath rich environment, it is hard for the attacker to annihilate randomly chosen signals.

Integrity codes assume a synchronised transmission between the transmitter and a receiver, as well as the receiver being aware that it is within the range of the transmitter. To transmit a message, the sender encodes the binary message using a unidirectional code (e.g., a Manchester code), resulting in a known ration of 1s and 0s within an encoded message (for Manchester code, the numbers of 1s and 0s will be equal). This encoded message is then transmitted using on-off keying, such that each 0 is transmitted as an absence of signal and each 1 as a random signal. To decode the message and check its integrity, the receiver simply measures the energy of the signal. If the energy in a time slot is above a fixed threshold, the bit is interpreted as a 1 and if it below a threshold, it is interpreted as a 0. If the ratio of bits 1 and 0 corresponds to the encoding scheme, the integrity of the message is validated. Integrity codes assume that the receiver knows when the transmitter is transmitting. This means that their communication needs to be scheduled or the transmitter needs to always be transmitting.

2.5 Low Probability of Intercept and Covert Communication

Low Probability of Intercept (LPI) signals are those that are difficult to detect for the unintended recipient. The simplest form of LPI is communication at a reduced power and with high directionality. As this communication limits the range and the direction of the communication, more sophisticated techniques were developed: Frequency Hopping, Direct Sequence Spread Spectrum and Chirping. In Frequency Hopping, the sender and the receiver hop between different frequency channels, thus trying to avoid detection. In Direct Sequence Spread Spectrum, the information signal is modulated with a high rate (and thus high bandwidth) digital signal, thus spreading its frequency. Finally, Chirps are high-speed frequency sweeps that carry information.

Covert communication is parasitic and leverages legitimate and expected transmissions to enable unobservable communication. Typically, this communication hides within the expected and tolerated deviations of the signal from its nominal form. One prominent example is embedding communicated bits within the modulation errors.

3 Physical-Layer Identification

[6]

Physical-Layer Identification techniques enable the identification of wireless devices by the unique characteristics of their analogue (radio) circuitry; this type of identification is also referred to as Radio Fingerprinting. More precisely, physical-layer device identification is the process of fingerprinting the analogue circuitry of a device by analysing the device's communication at the

physical layer for the purpose of identifying a device or a class of devices. This type of identification is possible due to hardware imperfections in the analogue circuitry introduced during the manufacturing process. These imperfections are remotely measurable as they appear in the transmitted signals. While more precise manufacturing and quality control could minimise these artifacts, it is often impractical due to significantly higher production costs.

Physical-layer device identification systems aim to identify (or verify the identity of) devices or their affiliation classes. These systems can be viewed as pattern recognition systems typically composed of: an acquisition setup to acquire signals from the devices under identification, also referred to as identification signals, a feature extraction module to obtain identification-relevant information from the acquired signals, also referred to as fingerprints, and a fingerprint matcher for comparing fingerprints and notifying the application system requesting the identification of the comparison results. Typically, there are two modules in an identification system: one for enrollment and one for identification. During enrollment, signals are captured from either each device or each (set of) class-representative device(s) considered by the application system. Fingerprints obtained from the feature extraction module are then stored in a database (each fingerprint may be linked to some form of unique ID representing the associated device or class). During identification, the fingerprints obtained from the devices under identification are compared with the reference fingerprints stored during enrollment. The task of the identification module can be twofold: either recognise (identify) a device or its affiliation class from among many enrolled devices or classes (1:N comparisons), or to verify that a device identity or class matches a claimed identity or class (1:1 comparison).

3.1 Device Under Identification

Physical-layer device identification is based on fingerprinting the analogue circuitry of devices by observing their radio communication. Consequently, any device that uses radio communication may be subject to physical-layer identification. So far, it has been shown that a number of devices (or classes of devices) can be identified using physical-layer identification. These include analogue VHF, Bluetooth, WiFi, RFID and other radio transmitters.

Although what makes a device or a class of devices uniquely identified among other devices or classes of devices is known to be due to imperfections introduced during the manufacturing phase of the analogue circuitry, the actual device's components causing this have not always been clearly identified in all systems. For example, VHF identification system based its work on the uniqueness of transmitter's frequency synthesisers (local oscillators), while in RFID systems some studies only suggested that the proposed identification system may rely on imperfections caused by the RFID device's antennas and charge pumps. Identifying the exact components may become more difficult when considering relatively-complex devices. In these cases, it is common to identify in the whole analogue circuitry, or in a specific sub-circuit, the cause of imperfections. For example, IEEE 802.11 transceivers were identified considering modulation-related features; the cause of hardware artifacts can then be located in the modulator subcircuit of the transceivers. Knowing the components that make devices uniquely identifiable may have relevant implications for both attacks and applications, which makes investigating these components an important ongoing problem and research direction.

3.2 Identification Signals

Considering devices communicating through radio signals, that is, sending data according to some defined specification and protocol, identification at the physical layer aims to extract unique characteristics from the transmitted radio signals and to use those characteristics to distinguish between different devices or classes of devices. We defined identification signals as those that are collected for the purpose of identification. Signal characteristics are mainly based on observing and extracting information from the properties of the transmitted signals such as amplitude, frequency, or phase over a certain period of time. These time-windows can cover different parts of the transmitted signals. Mainly, we distinguish between data and non-data-related parts. The data parts of signals directly relate to data (e.g., preamble, midamble, payload) transmission, which leads to considered data-related properties such as modulation errors, preamble (midamble) amplitude, frequency and phase and spectral transformations. The non-data-related parts of signals are not associated with data transmission. Examples include turn-on transients, near-transient regions and RF burst signals. These have been used to identify active wireless transceivers (IEEE 802.11, 802.15.4) and passive transponders (ISO 14443 HF RFID).

3.3 Features

Features are characteristics extracted from identification signals. They can be predefined or inferred. Predefined features relate to well-understood signal characteristics. They can be classified as in-specification and out-specification. Specifications are used for quality control and specify error tolerances. Examples of in-specification characteristics include modulation errors such as frequency offset, I/Q origin offset, magnitude and phase errors, as well as time-related parameters such as the duration of the response. Examples of out-specification characteristics include clock skew and the duration of the turn-on transient.

Different from predefined features, where the considered characteristics are known in advance prior to recording the signals, we say that features are inferred when they are extracted from signals, for example, by means of some spectral transformations such as Fast Fourier Transform (FFT) or Discrete Wavelet Transform (DWT), without a-priori knowledge of a specific signal characteristic. For example, wavelet transformations have been applied to signal turn-on transients and different data-related signal regions. The Fourier Transform has also been used to extract features from the turn-on transient and other technology-specific device responses. Both predefined and inferred features can be subject to further statistical analysis in order to improve their quality.

3.4 Device Fingerprints

Fingerprints are sets of features (or combinations of features) that are used to identify devices. The properties that fingerprints need to present in order to achieve practical implementations are (similar to other biometrics): (i) Universality. Every device (in the considered device-space) should have the considered features. (ii) Uniqueness. No two devices should have the same fingerprints. (iii) Permanence. The obtained fingerprints should be invariant over time. (iv) Collectability. It should be possible to capture the identification signals with existing (available) equipment. When considering physical-layer identification of wireless devices, we also consider: (v) Robustness.

Fingerprints should not be subject, or at least, they should be evaluated with respect to external environmental aspects that directly influence the collected signal such as radio interference due to other radio signals, surrounding materials, signal reflections, absorption etc., as well as positioning aspects such as the distance and orientation between the devices under identification and the identification system. Furthermore, fingerprints should be robust against device-related aspects such as temperature, voltage level, and power level. Many types of robustness can be acceptable for a practical identification system. Generally, obtaining robust features helps build more reliable identification systems. (vi) Data-Dependency. Fingerprints can be obtained from the features extracted from a specific bit pattern (the data-related part of the identification signal) transmitted by the device under identification (e.g., the claimed ID sent in a packet frame). This dependency has particularly interesting implications if the fingerprints can be associated with both devices and the data transmitted by those devices. This might strengthen authentication and help prevent replay attacks.

3.5 Attacks on Physical-Layer Identification

The majority of studies have focused on exploring feature extraction and matching techniques for physical-layer device identification. Only recently has the security of these techniques started to be addressed. Different groups have shown that their identification system may be vulnerable to hill-climbing attacks if the number of signals used for building the device fingerprint is not carefully chosen. This attack consists of repeatedly sending signals to the device identification system with modifications that gradually improve the similarity score between these signals and a genuine target signal. They have also demonstrated that transient-based approaches could easily be disabled by jamming the transient part of the signal while still enabling reliable communication. Furthermore, impersonation attacks on modulation-based identification techniques have been developed and have shown that low-cost software-defined radios as well as high-end signal generators could be used to reproduce modulation features and impersonate a target device with a success rate of 50-75%. Modulation-based techniques are vulnerable to impersonation with high accuracy, while transient-based techniques are likely to be compromised only from the location of the target device. The authors have pointed out that this is mostly due to the presence of wireless channel effects in the considered device fingerprints; therefore, the channel needs to be taken into consideration for successful impersonation.

Generally, these attacks can be divided into two groups: signal re(p)lay and feature replay attacks. In a signal replay attack, the attacker's goal is to observe analogue identification signals of a target device, capture them in a digital form (digital sampling), and then transmit (replay) these signals towards the identification system by some appropriate means. The attacker does not modify the captured identification signals, that is, the analogue signal and the data payload are preserved. This attack is similar to message replay in the Dolev-Yao model. Unlike in signal replay attacks, where the goal of the attack is to reproduce the captured identification signals in their integrity, a feature replay attack creates, modifies or composes identification signals that reproduce only the features considered by the identification system. The analogue representation of the forged signals may be different, but the features should be the same (similar).

4 Jamming and Jamming-Resilient Communication

[7][8]

Communication jamming is an interference that prevents the intended receiver(s) from successfully recognising and decoding the transmitted message. This happens when the jammer injects a signal which, when combined with the legitimate transmission, prevents the receiver from extracting the information contained in the legitimate transmission. Jamming can be surgical and affect only message preamble, thus preventing decoding, or it can be comprehensive and aim to affect every symbol in the transmission.

Depending on their behaviour, jammers can be classified as constant ot reactive. Constant jammers transmit permanently, irrespective of the legitimate transmission. Reactive jammers are the most agile as they sense for a transmission and then jam it. This allows them to save energy and remain undetected. Jammer strength is typically expressed in terms of their output power and their effectiveness as the jamming-to-signal ratio at the receiver. Beyond a certain jamming-to-signal ratio, the receiver will not be able to decode the information contained in the signal. This ratio is specific to particular receivers and communication schemes. The main parameters that influence the success of jamming are jammers' and transmitters' transmitting power, their antenna gains, communication frequency, and their respective distances to the receiver. These parameters will determine the jamming-to-signal ratio.

Countermeasures against jamming involve concealing from the adversary what frequencies are being used for communication at what time. This uncertainty forces the adversary to jam a wider portion of the spectrum and, therefore, weakens his impact on the legitimate transmission, effectively reducing the jamming-to-signal ratio. The most common techniques include Chirp, Frequency Hopping Spread Spectrum (FHSS) and Direct-Sequence Spread Spectrum (DSSS). Typically, these techniques rely on pre-shared secret keys, in which case we call them 'coordinated'. Recently, to enable jamming resilience in scenarios in which the keys cannot be pre-shared (e.g., broadcast), uncoordinated FHSS and DSSS schemes were also proposed.

4.1 Coordinated Spread Spectrum Techniques

Coordinated spread spectrum techniques are common jamming countermeasures in a number of civilian and military applications. They are used not only to increase resilience to jamming, but also to cope with interference from neighbouring devices. Spreading is used in practically all wireless communication technologies, in 802.11, cellular, Bluetooth, and global satellite positioning systems.

Spread spectrum techniques are typically effective against jammers that cannot cover the entire communication spectrum at all times. These techniques make a sender spread a signal over the entire available band of radio frequencies. The attacker's ability to impact the transmission is limited by the achieved processing gain of the spread-spectrum communication. This gain is the ratio at which interference can be suppressed relative to the original signal, and is computed as the ratio of the spread signal radio frequency bandwidth to the unspread information (baseband) bandwidth.

Spread-spectrum techniques use randomly generated sequences to spread information signals over a wider band of frequencies. This signal is then transmitted and then despread by the receivers by correlating it with the spreading sequence. For this to work, it is essential that the transmitter and receiver share the same secret spreading sequence. In FHSS, this sequence is the set of central frequencies and the order in which the transmitter and receiver switch between them in synchrony. In DSSS, the data signal is modulated with the spreading sequence; this process effectively mixes the carrier signal with the spreading sequence, thus increasing the frequency bandwidth of the transmitted signal. This process allows for both narrow band and wide band jamming to be suppressed at the receiver. Namely, unless the jammer can guess the spreading code, its jamming signal will be spread at the receiver, whereas the legitimate transmission will be despread, allowing for its detection. The secrecy of the spreading codes is, therefore, crucial for the jamming resilience of spread spectrum systems. This is why a number of civilian systems that use spreading with public spreading codes, such as GPS and 802.11b remain vulnerable to jamming.

4.2 Uncoordinated Spread Spectrum Techniques

In broadcast applications and in applications in which communication cannot be anticipated as scheduled, there is still a need to protect this communication from jamming.

To address these scenarios, uncoordinated spread spectrum techniques were proposed: Uncoordinated Frequency Hopping and Uncoordinated Direct Sequence Spread Spectrum. These techniques enable anti-jamming broadcast communication without pre-shared secrets. Uncoordinated Frequency Hopping relies on the fact that even if the sender hops in a manner that is not coordinated with the receiver, the throughput of this channel will be non-zero. In fact, if the receiver is broadband, it can recover all the messages transmitted by the sender. UFH, however, introduces new challenges. Given that the sender and the receiver are not synchronised, and short message fragments transmitted within each hop are not authenticated, the attacker can inject fragments that make the reassembly of the packets unfeasible. To prevent this, UFH includes fragment linking schemes that make this reassembly possible even under poisoning.

UDSSS follows the principle of DSSS in terms of spreading the data using spreading sequences. However, in contrast to anti-jamming DSSS, where the spreading sequence is secret and shared exclusively by the communication partners, in UDSSS, a public set of spreading sequences is used by the senders and the receivers. To transmit a message, the sender repeatedly selects a fresh, randomly selected spreading sequence from the public set and spreads the message with this sequence. Hence, UDSSS requires neither message fragmentation at the senders nor message reassembly at the receivers. The receivers record the signal on the channel and despread the message by applying sequences from the public set, using a trial-and-error approach. The receivers are not synchronised to the beginning of the sender's message and thus record for (at least) twice the message transmission time. After the sampling, the receiver tries to decode the data in the buffer by using code sequences from the set and by applying a sliding-window protocol.

4.3 Signal Annihilation

Unlike jamming where the primary goal of the attacker is to prevent information from being decoded at the receiver, signal annihilation suppresses the signal at the receiver by introducing destructive

interference. The attacker's goal is to insert a signal which cancels out the legitimate transmitter's signal at the antenna of the receiver. This typically means that the attacker will generate a signal identical to the legitimate transmission only with a different polarity. Jamming attacks typically increase the energy on the channel and are thus more easily detected than signal annihilation, which reduces the energy typically below the signal detection threshold.

5 GNSS Security

[9]

Global Navigation Satellite Systems (GNSS) such as GPS and Galileo provide global navigation service through satellites that are orbiting the Earth at approximately 20,000km. These satellites are equipped with high-precision atomic clocks which allow the satellites to remain synchronised. Satellites transmit navigation messages at central frequencies of 1575.42MHz (L1) and 1227.60MHz (L2). Direct Sequence Spreading is used to enable acquisition and to protect the signals carrying these messages from spoofing and jamming attacks. Civilian codes are public and, therefore, do not offer such protection, whereas military and special interest codes are kept confidential. Navigation messages carry data including satellite clock information, the ephemeris (information related to the satellite orbit) and the almanac (the satellite orbital and clock information). Satellite messages are broadcasted and the reception of messages by four or more satellites will allow a receiver to calculate its position. This position calculation is based on trilateration. The receiver measures the times of arrival of the satellite signals, converts them into distances (pseudoranges), and then calculates its position as well as its clock offset with respect to the satellite clocks.

5.1 GPS Spoofing Attacks

A GPS signal spoofing attack is a physical-layer attack in which an attacker transmits specially crafted radio signals that are identical to authentic satellite signals. Civilian GPS is highly vulnerable to signal spoofing attacks. This is due to a lack of any signal authentication and the publicly known spreading codes for each satellite, modulation schemes, and data structure. In a signal spoofing attack, the objective of an attacker may be to force a target receiver to (i) compute an incorrect position, (ii) compute an incorrect time or (iii) disrupt the receiver. Due to the low power of the legitimate satellite signal at the receiver, the attacker's spoofing signals can easily overshadow the authentic signals. In a spoofing attack, the GPS receiver typically locks (acquires and tracks) onto the stronger attacker's signal, thus ignoring the satellite signals.

An attacker can influence the receiver's position and time estimate in two ways: (i) by manipulating the contents of the navigation messages (e.g., the satellites' locations, navigation message transmission time) and/or (ii) by modifying the arrival time of the navigation messages. The attackers can manipulate the receiver time of arrival by temporally shifting the navigation message signals while transmitting the spoofing signals. We can classify spoofing attacks based on how synchronous (in time) and consistent (with respect to the contents of the navigation messages) the spoofing signals are in comparison to the legitimate GPS signals currently being received at the receiver's true location.

Non-Coherent and Modified Message Contents: In this type of an attack, the attacker's signals are both unsynchronised and contain different navigation message data in comparison to the authentic signals. Attackers who use GPS signal generators to execute the spoofing attack typically fall into this category. An attacker with a little know-how can execute a spoofing attack using these simulators due to their low complexity, portability and ease of use. Some advanced GPS signal generators are even capable of recording and replaying signals, although not in real-time. In other words, the attacker uses the simulator to record at a particular time and at a given location and later replays it. As they are replayed at a later time, the attacker's signals are not coherent and contain different navigation message data from the legitimate signals currently being received.

Non-Coherent but Unmodified Message Contents: In this type of attack, the navigation message contents of the transmitted spoofing signals are identical to the legitimate GPS signals currently being received. However, the attacker temporally shifts the spoofing signal, thereby manipulating the spoofing signal time of arrival at the target receiver. For example, attackers capable of real-time recording and replaying of GPS signals fall into this category, as they will have the same navigation contents as those of the legitimate GPS signals, although shifted in time. The location or time offset caused by such an attack on the target receiver depends on the time delay introduced both by the attacker and due to the propagation time of the relayed signal. The attacker can precompute these delays and successfully spoof a receiver to a desired location.

Coherent but Modified Message Contents: The attacker generates spoofing signals that are synchronised to the authentic GPS signals. However, the contents of the navigation messages are not the same as those of the currently seen authentic signals. For example, Phase-Coherent Signal Synthesizers are capable of generating spoofing signals with the same code phase as the legitimate GPS signal that the target receiver is currently locked on to. Additionally, the attacker modifies the contents of the navigation message in real-time (and with minimal delay) and replays it to the target receiver. A variety of commercial GPS receivers have been shown to be vulnerable to this attack and, in some cases, it even caused permanent damage to the receivers.

Coherent and Unmodified Message Contents: Here, the attacker does not modify the contents of the navigation message and is completely synchronised to the authentic GPS signals. Even though the receiver locks on to the attacker's spoofing signals (due to the higher power), there is no change in the location or time computed by the target receiver.

Therefore, this is not an attack in itself, but is an important first step in executing the seamless takeover attack.

The seamless takeover attack is considered one of the strongest attacks in the literature. In a majority of applications, the target receiver is already locked onto legitimate GPS satellite signals. The goal of an attacker is to force the receiver to stop tracking the authentic GPS signals and lock onto the spoofing signals without causing any signal disruption or data loss. This is because the target receiver can potentially detect the attack based on the abrupt loss of the GPS signal. In a seamless takeover attack, first, the attacker transmits spoofing signals that are synchronised with the legitimate satellite signals and are at a power level lower than the received satellite signals. The receiver is still locked onto the legitimate satellite signals due to the higher power and hence there is no change in the ship's route. The attacker then gradually increases the power of the spoofing signals until the target receiver stops tracking the authentic signal and locks onto the

spoofing signals. Note that during this takeover, the receiver does not see any loss of lock; in other words, the takeover was seamless. Even though the target receiver is now locked onto the attacker, there is still no change in the route, as the spoofing signals are both coherent with the legitimate satellite signals as well as there being no modification to the contents of the navigation message itself. Now, the attacker begins to manipulate the spoofing signal such that the receiver computes a false location and begins to alter its course. The attacker can either slowly introduce a temporal shift from the legitimate signals or directly manipulate the navigation message contents to slowly deviate the course of the ship to a hostile destination.

5.2 GNSS Spoofing Detection

If an attacker controls all the signals that arrive at the receiver's antenna(s), the receiver cannot detect spoofing. However, if the attack is remote, and the attacker cannot fully control the signals at the receiver, different anomaly detection techniques can be used to detect spoofing. In particular, automatic gain control (AGC) values, received signal strength (RSS) from individual satellites, carrier phase values, estimated noise floor levels and the number of visible satellites can all be used to detect spoofing. Particulary interesting are the techniques based on tracking and analysing the autocorrelation peaks that are used for detecting GNSS signals. Distortion, the number and the behaviour over time of these peaks can be used to detect even the most sophisticated seamless takeover attacks.

The detection of GNSS spoofing can be improved if the spoofing signals are simultaneously received by several receivers. This can be used for the detection of spoofing as well as for spoofer localisation. If the receivers know their mutual distances (e.g., are placed at fixed distances), the spoofer needs to preserve those distances when performing the spoofing attack. When a single spoofer broadcasts its signals, it will result in all the receivers being spoofed to the same position, therefore enabling detection. This basic detection technique can be generalised to several receivers, allowing even the detection of distributed spoofers.

Finally, GNSS spoofing can be made harder through the authentication and hiding of GNSS signals. Although current civilian GNSS systems do not support authentication, digital signatures as well as hash-based signatures such as TESLA can be added to prevent the attacker from generating GNSS signals. This would, however, not prevent all spoofing attacks as the attacker can still selectively delay navigation messages and, therefore, modify the computed position. This attack can be prevented by using spreading with delayed key disclosure. Even this approach still does not fully prevent spoofing by broadband receivers that are able to relay full GNSS frequency bands between locations.

Military GPS signals are authenticated, and try to achieve low-probability of intercept as well as jamming resilience via the use of secret spreading codes. This approach prevents some spoofing attacks, but still fails to fully prevent record-and-relay attacks. In addition, this approach does not scale well as secret spreading codes need to be distributed to all intended receivers, increasing the likelihood of their leakage and reducing usability.

6 Distance Bounding and Secure Positioning

Secure distance measurement (i.e., distance bounding) protocols were proposed to address the issue of verifying proximity between (wireless) devices. Their use is broad and ranges from the prevention of relay attacks to enabling secure positioning.

Securing distance measurement requires secure protocols on the logical layer and a distance measurement technique resilient to physical-layer attacks. To attack distance measurement, an attacker can exploit both the data-layer and the physical-layer weaknesses of distance measurement techniques and protocols. Data-layer attacks can be, to a large extent, prevented by implementing distance bounding protocols. However, physical-layer attacks are of significant concern as they can be executed independently of any higher-layer cryptographic primitive that is implemented.

6.1 Distance Bounding Protocols

[10]

Secure distance measurement protocols aim to prevent distance shortening and enlargement attacks. When they only prevent distance shortening, they are also called distance bounding protocols, where at the end of the protocol a secure upper bound on the distance is calculated. These protocols are typically executed with different trust assumptions. Devices measuring the distance (typically named verifier and prover) can be mutually trusted, in which case the protocol aims to prevent distance manipulation by an external attacker. If one of the devices, the prover, is untrusted, it will try to manipulate the measured distance. Other scenarios include the untrusted prover being helped by third parties to cheat on its distance. The distance bounding literature describes four main types of attack 'frauds' corresponding to the above scenarios: distance fraud, mafia fraud, terrorist fraud and distance hijacking.

The earliest investigations of distance bounding protocols started with the work of Beth and Desmedt, and of Brands and Chaum. These protocols, as well as many that followed, are designed as cryptographic challenge-response protocols with round-trip time of flight (RTT) measurements. One of the key insights of Brands and Chaum was to minimise the processing at the prover so that the prover cannot cheat on its distance to the verifier. Namely, this protocol requires that the prover only computes single bit XOR during the time-critical phase of the protocol. This translates into strong security guarantees as long as the prover cannot implement a faster XOR than is assumed by the verifier. Hancke and Kuhn proposed an alternative protocol that uses register selection as a prover processing function. This design reduces the number of protocol steps by allowing the verifier and the prover to pre-agree on the nonces that will be used in the protocol exchange. Many protocols followed these two designs, notably addressing other types of fraud (especially terrorist fraud), as well as the robustness to message loss, performance in terms of protocol execution time, and privacy of distance measurement.

6.2 Distance Measurement Techniques

Establishing proximity requires estimating the physical distance between two or more wireless entities. Typically, the distance is estimated either by observing the changes in the signal's physical

properties (e.g., amplitude, phase) that occur as the signal propagates or by estimating the time taken for the signal to travel between the entities.

Radio signals experience a loss in their signal strength as they travel through the medium. The amount of loss or attenuation in a signal's strength is proportional to the square of the distance travelled. The distance between the transmitter and the receiver can, therefore, 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 account for accurately. This directly affects the accuracy of the computed distance and, therefore, advanced models such as the Rayleigh fading and log-distance path loss models are typically used to improve the distance estimation accuracy. Bluetooth-based proximity sensing tags (e.g., Apple iBeacon and Passive Keyless Entry and Start Systems) use the strength of the received Bluetooth signal, also referred to as the Received Signal Strength Indicator (RSSI) value, as a measure of proximity.

Alternatively, these devices can measure the distance between them by estimating the phase difference between a received continuous wave signal and a local reference signal. The need to keep track of the number of entire elapsed cycles is eliminated by using signals of different frequencies, typically referred to as multi-carrier phase-based ranging. Due to their low complexity and low power consumption, phase-based ranging is used in several commercial products.

Finally, the time taken for radio waves to travel from one point to another can be used to measure the distance between devices. In RF-based RTT-based distance estimation, the distance d between two entities is given by $d = (t_{rx} \quad t_{tx}) \quad c$, where c is the speed of light, t_{tx} and t_{rx} represent the time of transmission and reception, respectively. The measured time-of-flight can either be one-way time-of-flight or a round-trip time-of-flight. One-way time-of-flight measurement requires the clocks of the measuring entities to be precisely synchronised. Errors due to mismatched clocks are compensated for in the round-trip time-of-flight measurement.

The precise distance measurement largely depends on the system's ability to estimate the time of arrival and the physical characteristics of the radio frequency signal itself. The ranging precision is roughly proportional to the bandwidth of the ranging signal. Depending on the required level of accuracy, time-of-flight-based distance measurement systems use either impulse-radio ultra wideband (IR-UWB) or chirp spread spectrum (CSS) signals. IR-UWB systems provide centimetre-level precision, while the precision of CSS systems is of the order of 1 - 2 m. There are a number of commercially available wireless systems that use chirp and UWB round-trip time-of-flight for distance measurement today.

6.3 Physical-Layer Attacks on Secure Distance Measurement

[11][12][?]

With the increasing availability of low-cost software-defined radio systems, an attacker can eavesdrop, modify, compose and (re)play radio signals with ease. This means that the attacker has full control of the wireless communication channel and, therefore, is capable of manipulating all the messages transmitted between two entities. In RSSI-based distance estimation, an attacker can manipulate the measured distance by manipulating the received signal strength at the verifier. The attacker can simply amplify the signal transmitted by the prover before relaying it to the verifier.

This will result in an incorrect distance estimation at the verifier. Commercially available solutions claim to secure against relay attacks by simply reducing or attenuating the power of the transmitted signal. However, an attacker can simply circumvent these countermeasures by using higher gain amplifiers and receiving antennas.

Similarly, an attacker can also manipulate the estimated distance between the verifier and the prover in systems that use the phase or frequency property of the radio signal. 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, i.e., 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 values range from 0 to 2 and then roll over, the maximum measurable distance also rolls over after a certain value. An attacker can leverage this maximum measurable distance property of the system in order to execute the distance decreasing relay attack. During the attack, the attacker simply relays (amplifies and forwards) the verifier's interrogating signal to the prover. The prover determines the phase of the interrogating signal and re-transmits a response signal that is phase-locked with the verifier's interrogating signal. The attacker then receives the prover's response signal and forwards it to the verifier, although with a time delay. The attacker chooses the time delay such that the measured phase differences reach a maximum value of 2p before rolling over. In other words, the attacker is able to prove to the verifier that the prover is in close proximity (e.g., 1 m away) even though the prover is far away from the verifier.

In time-of-flight (ToF)-based ranging systems, the distance is estimated based on the time elapsed between the verifier transmitting a ranging packet and receiving an acknowledgement back from the prover. In order to reduce the distance measured, an attacker must decrease the signal's round trip time of flight. Based on the implementation, an attacker can reduce the estimated distance in a time-of-flight-based ranging system in more than one way. Given that the radio signals travel at the speed of light, a 1 ns decrease in the time estimate can result in a distance reduction of 30cm.

The first type of attack on time-of-flight ranging leverages the predictable nature of the data contained in the ranging and the acknowledgement packets. A number of time-of-flight ranging systems use pre-defined data packets for ranging, making it easy for an attacker to predict and generate his own ranging or acknowledgment signal. An attacker can transmit the acknowledgment packet even before receiving the challenge ranging packet. Several studies have shown that the de-facto standard for IR-UWB, IEEE 802.15.4a does not automatically provide security against distance decreasing attacks. It has been shown that an attacker can potentially decrease the measured distance by as much as 140 metres by predicting the preamble and payload data at more than 99% accuracy even before receiving the entire symbol. In a 'Cicada' attack, the attacker continuously transmits a pulse with a power greater than that of the prover. This degrades the performance of energy detection-based receivers, resulting in reduced distance measurements. In order to prevent these attacks it is important to avoid predefined or fixed data during the time critical phase of the distance estimation scheme.

In addition to having the response packet dependent on the challenge signal, the way these challenge and response data are encoded in the radio signals affects the security guarantees provided by the ranging or localisation system. An attacker can predict the bit (early detect) even

before receiving the symbol completely. 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 (e.g., early-detection), the attacker stops transmitting the arbitrary signal and switches to transmitting the bit corresponding to the predicted symbol, i.e., the attacker 'commits' to the predicted symbol, commonly known as late commit. In this scenario, the attacker need not wait for the entire series of pulses to be received before detecting the data being transmitted. After a certain time period, the attacker would be able to correctly predict the symbol.

As described previously, round-trip time-of-flight systems are implemented either using chirp or impulse radio ultrawideband signals. Due to their long symbol lengths, both implementations have shown to be vulnerable to early-detect and late-commit attacks. In the case of chirp-based systems, an attacker can decrease the distance by more than 160 m and in some scenarios even up to 700 m. Although IR-UWB pulses are of short duration (typically 2-3 ns long), the data symbols are typically composed of a series of UWB pulses. Furthermore, the IEEE 802.15.4a IR-UWB standard allows long symbol lengths ranging from 32 ns to as long as 8 s. Therefore, even the shortest 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, it is clear that in order to guarantee proximity and secure a wireless proximity system against early-detect and late-commit attacks, it is necessary to keep the symbol length as short as possible.

The design of a physical layer for secure distance measurement remains an ongoing issue. However, research so far has yielded some guiding principles for its design. So far, only radio RTT with single-pulse or multi-pulse UWB modulation has been shown to be secure against physical-layer attacks. As a result, the IEEE 802.15.4z working group started the standardisation of a new physical layer for UWB secure distance measurement.

6.4 Secure Positioning

[13]

Secure positioning systems allow positioning anchors (also called verifiers) to compute the correct position of a node (also called the prover) or allow the prover to determine its own position correctly despite manipulations by the attacker. This means that the attacker cannot convince the verifiers or the prover that the prover is at a position different from its true position. This is also called spoofing-resilience. A related property is secure position verification, which means that the verifiers can verify the position of an untrusted prover. It is generally assumed that the verifiers are trusted. No restrictions are put on the attacker, as it fully controls the communication channel between the provers and the verifiers.

The analysis of broadcast positioning techniques, such as GNSS has shown that these techniques are vulnerable to spoofing if the attacker controls the signals at the antenna of the GNSS receiver.

To tackle this, two main approaches have been proposed: Verifiable Multilateration and Secure Positioning based on Hidden Stations.

Verifiable Multilateration relies on secure distance measurement / distance bounding. It consists of distance bound measurements to the prover from at least three verifiers (in 2D) and four verifiers (in 3D) and of the subsequent computations performed by the verifiers or by a central system.

Verifiable Multilateration has been proposed to address both secure positioning and position verification. In the case of secure positioning, the prover is trusted and mafia-fraud-resilient distance bounding is run between the prover and each of the verifiers. The verifiers form verification triangles/triangular pyramids (in 3D) and verify the position of the prover within the triangle/pyramid. For the attacker to spoof a prover from position P to P' within a triangle/pyramid, the attacker would need to reduce at least one of the distance bounds that are measured to P. This follows from the geometry of the triangle/pyramid. As distance bounding prevent distance reduction attacks, Verifiable Multilateration prevents spoofing attacks within the triangle/pyramid. The attacker can only spoof P to P' that is outside of the triangle/pyramid, causing the prover and the verifiers to reject the computed position. Namely, the verifiers and the prover only accept the positions that are within the area of coverage, defined as the area covered by the verification triangles/pyramids. Given this, when the prover is trusted, Verifiable Multilateration is resilient to all forms of spoofing by the attacker. Additional care needs to be taken when managing the errors and computing the position when the distance measurement errors are taken into account.

When used for position verification, Verifiable Multilateration is run with an untrusted prover. Each verifier runs a distance-fraud resilient distance-bounding protocol with the prover. Based on the obtained distance bounds, the verifiers compute the prover's position. If this position (within some distance and position error bounds) falls within the verification triangle/pyramid, the verifiers accept it as valid. Given that the prover is untrusted, it can enlarge any of the measured distances, but it cannot reduce them as this is prevented by using distance-bounding protocols. As in the case of secure positioning, the geometry of the triangle/pyramid then prevents the prover from claiming a false position. Unlike in the case of secure positioning, position verification is vulnerable to cloning attacks, in which the prover shares its key with its clones. These clones can then be strategically placed onto the verifiers and fake any position by enlarging the distances to each individual verifier. This attack can be addressed using tamper-resistant hardware or device fingerprinting.

Another approach to secure positioning and position verification is to prevent the attacker from deterministically spoofing the computed position by making the positions of the verifiers unpredictable for the attacker (either a malicious prover or an external attacker). The verifier positions can, therefore, be hidden or the verifiers can be mobile. When the verifiers are hidden, they should only listen to the beacons sent by the nodes so as not to disclose their positions. Upon receiving the beacons, the base stations compute the nodes' location with TDOA and check if this location is consistent with the time differences.

7 Compromising Emanations and Sensor Spoofing

[14][15][16][17][18][19]

Electronic devices emit radio and audio signals, heat, create vibrations, all of which could correlate with confidential information that the devices process or store. These emanations, or more generally side channels, are common and have been extensively studied.

Remote sensor spoofing is the flip side of compromising emanations. In these attacks, the attacker injects signals that spoof the value measured by the sensor and, therefore, influence the system. This is particularly critical in autonomous systems. For example, GNSS spoofing can be seen as a

special case of sensor spoofing where the time of the signal's arrival is being spoofed by the attacker.

7.1 Compromising Emanations

The first public demonstration of low-cost attacks on commercial systems using compromising emanations was done in 1985 by Wim van Eck. This attack demonstrated that information displayed on monitors can be successfully eavesdropped from the distance of hundreds of metres. This demonstration prompted research into the sources of these emanations as well as into protective measures.

Detailed studies of the sources and features that led to these compromises were later performed, demonstrating that compromising emanations from analogue and digital displays resulted from information being transmitted through analogue video cables and through high-speed digital serial interface (DVI) cables. More recent studies show that these emanations are not restricted to cables. Recent attacks demonstrated that high-frequency sounds caused by vibrating electronic components (capacitors and coils) in a computer's voltage regulation circuit can be used to infer prime factors and, therefore, RSA keys. Sound emanating from the keys on a keyboard can be used to work out what the user is typing. Finally, reflections from different objects in the vicinity of computer screens such as spoons, bottles and the user's retina can be used to read the displayed information.

7.2 Sensor Compromise

Analogue sensors have been shown to be particularly vulnerable to spoofing attacks. Electromagnetic interference has been used to manipulate the output of medical devices as well as to compromise ultrasonic ranging systems. Ultrasonic signals have been used to inject silent voice commands, and acoustic waves have been used to affect the output of MEMS (Microelectromechanical systems) accelerometers. These kinds of spoofing attacks have just started being investigated and will likely impact many future cyber-physical systems.

8 Cellular Networks

[20]

Cellular networks provide voice, data and messaging communication through a network of base stations, each covering one or more cells. The security provisions of these networks are mainly governed by the standards adopted by the GSM Association and later by the Third Generation Partnership Plan (3GPP).

8.1 Cellular Network Generations

Second-generation (2G) 'GSM' networks were introduced during the 1990s, and restricted their services to voice and text messaging. 2G networks were capable of carrying data via a circuitswitched data service (CSD), which operated in a manner similar to the dial-up modems, only over cellular networks. The further development of email and web services resulted in a need for enhanced speeds and services

3GPP improved 2G GSM standard with a packet-switched data service, resulting in the General Packet Radio Service (GPRS). Like GSM, GPRS made use of the Home Location Register (HLR), a component responsible for subscriber key management and authentication. However, GPRS enhanced GSM by adding the Serving GPRS Support Node (SGSN) for data traffic routing and mobility management for better data traffic delivery. Third-generation (3G) cellular networks, also known as Universal Mobile Telecommunications Systems (UMTS), introduced a number of improvements to the 2G networks, including security enhancements, and increased uplink and downlink speeds and capacities. Fourth=generation (4G) cellular networks, also known as Long Term Evolution (LTE) introduced further increases in transmission speeds and capacities.

8.2 Standardised Security Measures

One of the main security properties that cellular networks aim to protect is the confidentiality of the communication of the link between the mobile station, and the base station and correct billing. The security of cellular networks has evolved with the network generations, but each generation has the same overarching concept. Subscribers are identified via their (Universal) Subscriber Identity Modules their international mobile subscriber identity (IMSI) number and its related secret key. IMSI and the keys are used to authenticate subscribers as well as to generate the necessary shared secrets to protect communication with the cellular network.

2G security focused on the confidentiality of the wireless links between mobile stations and base stations. This was achieved through authentication via a challenge-response protocol, 2G Authentication and Key Agreement (AKA). This protocol is executed each time a mobile station initiates a billable operation. 2G AKA achieved authentication based on a long-term key K_i shared between the subscriber's SIM card and the network. This key is used by the network to authenticate the subscriber and to derive a session key K_c. This is done within in a challenge response protocol, executed between the SGSN and the mobile station. Before the execution of the protocol, SGSN receives from the HLR the K_c, a random value *RAND* and an expected response *XRES*. Both K_c and *XRES* are generated within the HLR based on *RAND* and K_i. When the mobile station attempts to authenticate to the network, it is sent *RAND*. To authenticate, the mobile station combines its long-term key K_i (stored on its SIM card) with the received *RAND* to generate *RES* and K_c. The mobile station sends *RES* to the SGSN, which compares it to *XRES*. If the two values match, the mobile station is authenticated to the network. The SGSN then sends K_c to the base station to which the mobile station is connected to in order to protect the mobile-to-base station wireless link.

2G AKA offered very limited protection. It used an inadequate key size (56-64 bits), and weak authentication and key generation algorithms (A3,A5 and A8) which were, once released, broken, allowing for eavesdropping and message forgery. Furthermore, AKA was designed to provide only one-way authentication of mobile stations to the network. As the network did not authenticate to the mobile stations, this enabled attacks by fake base stations, violating users' location privacy and the confidentiality of their communications.

In order to address these 2G security shortcomings, 3G networks introduced new 3G Authentication and Key Agreement (3G AKA) procedures. 3G AKA replaced the weak cryptographic algorithms that were used in 2G and provided mutual authentication between the

network and mobile stations. As in 2G, the goal of the protocol is the authentication (now mutual) of the network and the mobile station. The input into the protocol is a secret key *K* shared between the HLR and the subscriber.

The outcome of the protocol are two keys, the encryption/confidentiality key *CK* and the integrity key *IK*. The generation of two keys allows the network and the mobile station to protect the integrity and confidentiality of their communications using two different keys, in line with common security practices. CK and IK are both 128 bits long which is considered adequate.

The authentication and key derivation are performed as follows. The HRL first generates the random challenge *RAND*, from which come the expected response *XRES*, the keys *CK* and *IK,* and the authentication token *AUTN*. It then sends these values to the SGSN. The SGSN sends the *RAND* as well as the *AUTN* to the mobile station (also denoted as User Equipment - UE), which then uses its long-term key *K* to generate the response *RES* and to verify if *AUTN* was generated by the HLR. The *AUTN* is from the shared key and the counter maintained by both the HLR and the mobile station. Upon receiving the *RES* from the mobile station, the SGSN compares it with *XRES* and if they match, forwards *CK* and *IK* to the base station. Base and mobile stations can now use these keys to protect their communications.

3G, however, still did not resolve the vulnerabilities within the operators' networks. *CK* and *IK* are transmitted between different entities in the network. They are transmitted between the SGSN and the associated base station as well as between different base stations during mobility. This allows network attackers to record these keys and, therefore, eavesdrop on wireless connections.

The 4G(LTE) security architecture preserved many of the core elements of the 2G and 3G networks, but aimed to address the shortcomings of 3G in terms of protecting the in-network traffic through protecting network links and redistributing different roles. For example, the long-term key storage was moved from the HLR to the Home Subscriber Server (HSS). The mobility management was moved from the SGSN to the Mobility Management Entity (MME).

Cross-Reference of Topics VS Reference Material

	kopka2003 [21]	gratzer2016 [22]	...	...
?? ??				
?? ??	c4			
?? ??	c11,c12			
?? ??	c7	II.5		
...				

References

[1] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*, 1st ed. Springer Publishing Company, Incorporated, 2009.

[2] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, “A practical man-in-the-middle attack on signal-based key generation protocols,” in *Computer Security – ESORICS 2012*, S. Foresti, M. Yung, and F. Martinelli, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 235–252.

[3] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, “They can hear your heartbeats: Non-invasive security for implantable medical devices,” in *Proceedings of the ACM SIGCOMM 2011 Conference*, ser. SIGCOMM ’11. New York, NY, USA: ACM, 2011, pp. 2–13. [Online].
Available: http://doi.acm.org/10.1145/2018436.2018438

[4] N. Anand, S.-J. Lee, and E. W. Knightly, “Strobe: Actively securing wireless communications using zero-forcing beamforming,” in *2012 Proceedings IEEE INFOCOM*, March 2012, pp. 720– 728.

[5] S. Capkun, M. Äagalj, R. Rengaswamy, I. Tsigkogiannis, J. Hubaux, and M. Srivastava, “Integrity codes: Message integrity protection and authentication over insecure channels,” *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 4, pp. 208–223, Oct 2008.

[6] B. Danev, D. Zanetti, and S. Capkun, “On physical-layer identification of wireless devices,” *ACM Comput. Surv.*, vol. 45, no. 1, pp. 6:1–6:29, Dec. 2012. [Online]. Available: http://doi.acm.org/10.1145/2379776.2379782

[7] D. Adamy, *EW 101: a first course in electronic warfare*. Artech House, 2001.

[8] C. Popper, “On secure wireless communication under adversarial interference,” PhD thesis, ETH Zurich.

[9] A. Ranganathan, “Physical-layer techniques for secure proximity verification and localization,” PhD thesis, ETH Zurich.

[10] G. Avoine, M. A. Bingöl, I. Boureanu, S. capkun, G. Hancke, S. Kardas¸, C. H. Kim, C. Lauradoux, B. Martin, J. Munilla, A. Peinado, K. B. Rasmussen, D. Singelée, A. Tchamkerten, R. Trujillo-Rasua, and S. Vaudenay, “Security of distance-bounding: A survey,” *ACM Comput. Surv.*, vol. 51, no. 5, pp. 94:1–94:33, Sep. 2018. [Online]. Available: http://doi.acm.org/10.1145/3264628

[11] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, “So near and yet so far: Distance-bounding attacks in wireless networks,” in *Security and Privacy in Ad-Hoc and Sensor Networks*, L. Buttyán, V. D. Gligor, and D. Westhoff, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 83–97.

[12] A. Ranganathan and S. Capkun, “Are we really close? verifying proximity in wireless systems,” *IEEE Security Privacy*, vol. 15, no. 3, pp. 52–58, 2017. [Online]. Available: doi.ieeecomputersociety.org/10.1109/MSP.2017.56

[13] S. Capkun and J. . Hubaux, “Secure positioning in wireless networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, Feb 2006.

[14] M. G. Kuhn and C. M. G. Kuhn, “Compromising emanations: Eavesdropping risks of computer displays,” 2003.

[15] M. Backes, T. Chen, M. Duermuth, H. P. A. Lensch, and M. Welk, “Tempest in a teapot: Compromising reflections revisited,” in *2009 30th IEEE Symposium on Security and Privacy*, May 2009, pp. 315–327.

[16] D. Genkin, A. Shamir, and E. Tromer, “Rsa key extraction via low-bandwidth acoustic cryptanalysis,” in *Advances in Cryptology – CRYPTO 2014*, J. A. Garay and R. Gennaro, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 444–461.

[17] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, “Ghost talk: Mitigating emi signal injection attacks against analog sensors,” in *2013 IEEE Symposium on Security and Privacy*, May 2013, pp. 145–159.

[18] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, “Dolphinattack: Inaudible voice commands,” in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’17. New York, NY, USA: ACM, 2017, pp. 103–117. [Online]. Available: http://doi.acm.org/10.1145/3133956.3134052

[19] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, “Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks,” in *2017 IEEE European Symposium on Security and Privacy (EuroS P)*, April 2017, pp. 3–18.

[20] D. Forsberg, G. Horn, W.-D. Moeller, and V. Niemi, *LTE Security*, 2nd ed. Wiley Publishing, 2012.

[21] H. Kopka and P. W. Daly, *Guide to LaTeX (Tools and Techniques for Computer Typesetting*. Addison-Wesley Professional, 2003.

[22] G. GrÃtzer, *More Math Into LaTeX*. Springer, 2003.

[23] D. E. Knuth, *The TeXbook*. Addison-Wesley, 2003.