Security in Wireless Communication Networks

Yi Qian, Feng Ye, and Hsiao-Hwa Chen
John Wiley/IEEE Press, 2021: ISBN: 9781119244363,374 pages

Reviewer: Bo Rong

Over the last decade, wireless networks have experienced significant growth due to the proliferation of mobile devices and new development of radio technologies. Since the very beginning, security for wireless communication networks has always been regarded as a critical issue. In recent research frenzy on 5G and V2X communications, security plays a pivotal role as wireless Internet access serves as critical infrastructures to facilitate the digital transcations. This book timely provides a comprehensive introduction to the security in wireless communication networks, with respect to not only general concepts, but also practical principles and cases in specific wireless communication systems.

Chapter one delivers the general concept of computer networks, highlights the role of wireless communications in the whole picture of networking architecture, and classifies the wireless systems based on coverage, topology, and mobility. This chapter serves as a precursor to the rest of the book by providing the background of different types of wireless networks, including wireless personal area networks (WPAN), wireless local area networks (WLANs), and wireless wide area networks (WWAN). It also explains the security threats in wireless networks and discusses the relationship between network security and wireless security.

Chapter two gives an overview on the security concepts used in the rest of this book, including security attacks, security services, and security mechanisms. The authors first presents the classification of security attacks in terms of passive attacks (e.g.,eavesdropping and traffic analysis) and active attacks (e.g., masquerade, replay, modification, and denial of service). They then introduce security services, or the features in system design against possible security attacks, such as confidentiality, integrity, availability, access control, authentication, and non-repudiation. Finally, to achieve security service in a system, a list of popular security mechanisms, such as the encipherment, digital signature, etc. are discussed in the remaining part of the chapter.

Chapter three goes into the mathematical background related to wireless security, including number theory and modern algebra, modular arithmetic and divisors, finite fields, polynomial arithmetic, Fermat's Little Theory, Euler Totient Function, Euler's Theory, etc. The knowledge above is critical for the ones to understand cryptography, such as advanced encryption standards and public-key cryptographic systems. In addition, the fundamental principles and exemplary cases are concisely presented from the perspective of mathematics.

After the mathematical background, chapters four and five deal with cryptographic techniques. Chapter four first introduces some symmetric key cryptographic techniques by illustrating a few classical cryptographic algorithms with substitution and transposition techniques. It then presents the basic concept of modern stream/block cipher as well as Feistel cipher structure. Chapter five explains more cryptographic techniques using block ciphers and public key algorithms, including advanced encryption standard, block cipher mode of operations, public key infrastructure, RSA algorithm, etc.

Chapter six introduces message authentication and digital signature to protect the integrity of the message and the identity of the sender and receiver, respectively. First, this chapter discusses MAC and hash functions thoroughly, both widely used to provide message authentication. Then, it goes into the characteristics of digital signature and a series of digital signature standards, such as DSA, RSA, and ECDSA. These can protect the sender and receiver against each other. Within the above mechanisms, key management and distribution play a critical role. The rest of the chapter gives a general idea and some examples of key management schemes. Both symmetric and asymmetric key distributions have been illustrated. The key distribution mechanisms adopt symmetric and public key mechanisms for different purposes. Besides, practical communication systems with massive users need hierarchical key distribution mechanisms.

The rest chapters from seven to 15 focus on the security of specific wireless communication systems, covering the popular systems, such as WLAN, Bluetooth, ZigBee, RFID, GSM, UMTS, LTE, and 5G. As the emerging vehicle-to-everything (V2X) communications are receiving great attention, Chapter 15 discusses the security of V2X communications.

Chapter seven discusses the security of Wireless Local Area Network (WLAN), or interchangeably Wi-Fi. It starts with an introduction of WLAN in terms of the operating modes and the security challenges. WLAN is more vulnerable to attacks than wired connections due to the lack of physical connections. The authors illustrate a few generations of WLAN security protocols, which evolved from the original Wired Equivalent Privacy defined by the IEEE 802.11, Wi-Fi Protected Access (WPA), to the recent WPA3 to improve the security. They also analyze the implementation details of these security protocols. This chapter can serve as a good reference for professionals with a special interest in WLAN security.

Chapter eight deals with Bluetooth security. Bluetooth is an open standard designed for wireless personal area networks (WPAN). Bluetooth technology enables many wireless devices, such as smartwatches, wireless headphones, wireless keyboards, etc. Bluetooth standard specifies authentication, authorization, and confidentiality for securing data transmission. In this chapter, the authors analyze the security mode, trust level, and service level configurations that enable flexibility of Bluetooth security policies and highlight that Bluetooth specifications do not ensure secure connections from all adversary penetrations. If using Bluetooth technology in an organization, it is important to develop security policies to address the use of Bluetooth-enabled devices and the responsibilities of users.

Chapter nine discusses the security of Zigbee. The authors first give an overview of Zigbee standards related to different network layers, and then mainly analyzed the key cryptographic mechanisms. As Zigbee adopts symmetric-key cryptographic mechanisms, the authors especially emphasize that the secure storage and distribution of keys is the premise of ensuring the security of Zigbee. In practice, the security provided by Zigbee standards is not enough. For example, if a Zigbee device joins a network, intruders can intercept unprotected keys. Moreover, an attacker may easily get physical access to a Zigbee device and extract privileged information due to the low-cost nature. Security must be carefully considered to provide those applications.

Chapter 10 deals with the security of RFID. The authors first give an overview of RFID subsystems, different types of RFID tags, and the frequency bands. They then analyze the security attacks, risks, and objectives of RFID systems are analyzed. RFID systems are vulnerable to some attacks (e.g., counterfeit tag, eavesdropping, and electronic collisions) and privacy risks (e.g., disclosure of location information of users). The security objectives of the RFID system include confidentiality, integrity, non-repudiation, and availability. Due to the low cost and physical constraints of RFID tags, mitigation mechanisms to security risks are limited. This chapter then elaborates on the lightweight cryptographic algorithms, anti-collision algorithms, and physical protection available for RFID. The authors claim that it is imperative to provide security services to RFID systems.

Chapter 11 deals with the security of Global System for Mobile (GSM) Communications. Since the early 1990s, as the most widely used cellular mobile phone system in the world, GSM can provide services like voice communications, short messaging, etc. This chapter starts with the GSM system architecture and then discusses the network access security features and algorithms. Despite the popularity, the GSM system is exposed to quite a few threats. In this chapter, the authors mainly discuss the attacks caused by the vulnerability of security algorithms, as well as some possible security improvements. Unfortunately, GSM made very few improvements on these aspects before phasing out recently.

Chapter 12 introduces the security of Universal Mobile Telecommunications System (UMTS). UMTS is a successor of GSM with better security. Several security mechanisms are reused but with modifications. After introducing UMTS architecture, the chapter discusses the security mechanisms of UMTS, such as the authentication and key agreement, data confidentiality and integrity, and user identity confidentiality. Compared to the GSM, UMTS adds integrity protection. Algorithms f8 and f9 ensure confidentiality and integrity, respectively. Both algorithms are based on block cipher KASUMI. Readers may be interested in some additional security features of UMTS, such as mobile device identification, location services, and user-to-USIM authentication, which are discussed at the end of the chapter.

Chapter 13 illustrates Long-Term Evolution (LTE) security. It starts with the introduction of the LTE system architecture which is based on GSM and UMTS. A key difference with its predecessors is that LTE separates the control plane and user plane, differing LTE security from GSM and UMTS. The authors then depict LTE security in terms of security architecture, security mechanisms, and algorithms. LTE covers more keys and security algorithms, such as AES and ZUC, to ensure the security of complex systems. The authors also highlighted the LTE security for interworking with legacy systems as well as non-3GPP access. LTE has strong security implemented comparing with the previous generation system. LTE will continue to serve as an important part of the next-generation wireless system.

Chapter 14 discusses the security of 5th generation (5G) wireless network systems. 5G started large-scale commercial deployment around 2020 and is the next-generation mobile wireless telecommunications beyond 4G/International Mobile Telecommunications (IMT)-Advanced Systems. The authors illustrate some current development, challenges, and future directions of 5G wireless network security. They especially analyze some new security requirements and challenges introduced by the advanced features of the 5G wireless network systems. Due to the ongoing development of 5G, this chapter only discusses some present solutions and research results concerning the security of 5G wireless network systems. Quite a few challenges in 5G wireless network security, including new trust models, new security attack models, privacy protection, etc., call for continuous development of 5G security. This chapter briefly analyzes these challenges in the final part of the chapter.

In recent years, as a key component of Intelligent Transportation Systems, vehicle-to-everything (V2X) communications have received great attention. The rapid development of wireless technologies (e.g., DSRC, LTE, and 5G) enables V2X communications in different applications. To integrate the variety of wireless technologies, and meet special requirements for V2X communications, security and privacy have become a top priority. Therefore, the last chapter of the book sets off to discuss the security of V2X communications. Standards such as IEEE WAVE and LTE-V2X set a general guideline for V2X security implementations. New cryptography schemes, such as group signature and trusted-based schemes, are under development. This chapter covers all these topics. As an emerging type of wireless communication system, quite a few unsolved security challenges exist in V2X communications. The authors discuss some key challenges, including efficient schemes, hardware enhancement, and integration of AI algorithms, etc., at the end of the chapter.

In conclusion, “Security in Wireless Communication Networks” covers a wide range starting from the general wireless communication network architecture and basic concepts of network security to the mathematical background and practical techniques, and further to the specific security issues in different wireless networks, such as WLAN, LTE, 5G, etc. Comprehensively covering the security issues, security mechanisms, design principles, and techniques in wireless communication networks. This book intends to be a self-contained and one semester textbook on wireless security for either undergraduate senior level or graduate level courses. This book can also serve as a reference for practitioners and researchers in the field to get an idea of the current and future research focus in the emerging wireless security area.