HANDBOOK OF RESEARCH ON

WIRELESS SECURITY

Yan Zhang, Jun Zheng, & Miao Ma

Volume I

Detailed Table of Contents

to enabling secure and private service discovery in these environments, including the dynamic population of participants, the lack of a universal trust mechanism, and the limited capabilities of the devices. To ensure secure service discovery while addressing privacy issues, trust-based models are inevitable. We survey secure service discovery in the broadband wireless environment. We include case studies of two protocols which include a trust mechanism, and we summarize future research directions.

Chapter III

The recent developments in the mobile technology (mobile phones, middleware, wireless networks, etc.) created a need for new methods of protecting the code transmitted through the network. The oldest and the simplest mechanisms concentrate more on the integrity of the code itself and on the detection of unauthorized manipulation. The newer solutions not only secure the compiled program, but also the data that can be gathered during its "journey," and even the execution state. Some other approaches are based on prevention rather than detection. In the chapter we present a new idea of securing mobile agents. The proposed method protects all components of an agent: the code, the data, and the execution state. The proposal is based on a zero-knowledge proof system and a secure secret sharing scheme, two powerful cryptographic primitives. Next, the chapter includes security analysis of the new method and its comparison to other currently most widespread solutions. Finally, we propose a new direction of securing mobile agents by straightening the methods of protecting integrity of the mobile code with risk analysis and a reputation system that helps avoiding a high-risk behavior.

Chapter IV

The broad aim of identity management (IdM) is to manage the resources of an organization (such as files, records, data and communication infrastructure, and services) and to control and manage access to those resources in an efficient and accurate way. Consequently, identity management is both a technical and process orientated concept. The concept of IdM has begun to be applied in identities related applications in enterprises, governments, and Web services since 2002. As the integration of heterogeneous wireless networks becomes a key issue in towards the next generation (NG) networks, IdM will be crucial to the success of NG wireless networks. A number of issues, such as mobility management, multioperator, and securities require the corresponding solutions in terms of user authentication, access control, and so forth. IdM in NG wireless networks is about managing the digital identity of a user and ensuring that users have fast, reliable, and secure access to distributed resources and services of an NGN and the associated service providers, across multiple systems and business contexts.

Along with other security vulnerabilities, defense against denial-of-service attacks is a critical component of any security system. Unlike in wired networks where denial-of-service attacks have been extensively studied, there is a lack of research for preventing such attacks in wireless networks. In addition to various vulnerabilities, some factors leading to different types of denial-of-service attacks and some defense mechanisms are discussed in this chapter. This can help to better understand the wireless network vulnerabilities and subsequently more techniques and procedures to combat these attacks may be developed by researchers.

Chapter XI

This chapter deals with challenges raised by securing transport, service access, user privacy, and accounting in wireless environments. Key generation, delivery, and revocation possibilities are discussed and recent solutions are shown. Special focus is on efficiency and adaptation to a mobile environment. Device domains in personal area networks and home networks are introduced to provide personal digital rights management (DRM) solutions. The value of smartcards and other security tokens are shown and a secure and convenient transmission method is recommended based on the mobile phone and near field communication technology.

Chapter XII

Architecture and protocols for authentication, authorization, and accounting (AAA) are one of the most important design considerations in 3G/4G telecommunication networks. Many advances have been made to exploit the benefits of the current systems based on the protocol RADIUS, and the evolution to migrate into the more secure, robust, and scalable protocol DIAMETER. DIAMETER is the protocol of choice for the IP multimedia subsystem (IMS) architecture, the core technology for the next generation networks. It is envisioned that DIAMETER will be widely used in various wired and wireless systems to facilitate robust and seamless authentication, authorization, and accounting. In this chapter, we provide an overview of the major AAA protocols of RADIUS and DIAMETER, and we discuss their roles in practical 1xEV-DO network architectures in the three major network tiers: access, distribution, and core. We conclude the chapter with a short summary of the current and future trends related to the DIAMETER-based AAA systems.

Chapter XIII

Converging networks and mobility raise new challenges towards the existing authentication, authorisation, and accounting (AAA) systems. Focus of the research is towards integrated solutions for seamless service access of mobile users. Interworking issues between mobile and wireless networks are the basis for detailed research on handover delay, multidevice roaming, mobile networks, security, ease-of-use, and anonymity of the user. This chapter provides an overview over state-of-the-art in authentication for mobile systems, and suggests extending AAA-mechanisms to home and community networks, taking into account security and privacy of the users.

Chapter XIV

Wireless networks are gaining popularity that comes with the occurrence of several networking technologies raising from personal to wide area, from centralized to distributed, and from infrastructure-based to infrastructure-less. Wireless data link characteristics such as openness of transmission media make these networks vulnerable to a novel set of security attacks, despite those that they inherit from wired networks. In order to ensure the protection of mobile nodes that are interconnected using wireless protocols and standards, it is essential to provide an in-depth study of a set of mechanisms and security models. In this chapter, we present the research studies and proposed solutions related to the authentication, privacy, trust establishment, and management in wireless networks. Moreover, we introduce and discuss the major security models used in a wireless environment.

Chapter XV

In the design and analysis of authentication and key agreement protocols, provable secure formal methods play a very important role, among which the Canetti-Krawczyk(CK) model and the universal composable(UC) security model are very popular at present. This chapter focuses on these two models and consists mainly of three parts. (1) There is an introduction to the CK model and the UC model. (2) There is also a study of these two models, which includes an analysis of the CK model and an extension of the UC security model. The analysis of the CK model presents its security analysis, advantages, and disadvantages, and a bridge between this formal method and the informal method (heuristic method) is established; an extension of the UC security model gives a universally composable anonymous hash certification model. (3) The applications of these two models are also presented. With these two models, the four-way handshake protocols in 802.11i and Chinese WLAN security standard WAPI are analyzed.

Chapter XVI

In a wireless environment, multimedia transmission is often affected by the error rate, delaying, terminal's power or bandwidth, and so forth, which brings difficulties to multimedia content protection. In the past decade, wireless multimedia protection technologies have been attracting more and more researchers. Among them, wireless multimedia encryption and watermarking are two typical topics. Wireless multimedia encryption protects multimedia content's confidentiality in wireless networks, which emphasizes improving the encryption efficiency and channel friendliness. Some means have been proposed, such as the format-independent encryption algorithms that are time efficient compared with traditional ciphers, the partial encryption algorithms that reduce the encrypted data volumes by leaving some information unchanged, the hardware-implemented algorithms that are more efficient than software based ones, the scalable encryption algorithms that are compliant with bandwidth changes, and the robust encryption algorithms that are compliant with error channels. Compared with wireless multimedia encryption, wireless multimedia watermarking is widely used in ownership protection, traitor tracing, content authentication, and so forth. To keep costs low, a mobile agent is used to partition some of the watermarking tasks. To counter transmission errors, some channel encoding methods are proposed to encode the watermark. To keep robust, some means are proposed to embed a watermark into media data of low bit rate. Based on both watermarking and encryption algorithms, some applications arise, such as secure multimedia sharing or secure multimedia distribution. In this chapter, the existing wireless multimedia encryption and watermarking algorithms are summarized according to the functionality and multimedia type, their performances are analyzed and compared, the related applications are presented, and some open issues are proposed.

In this chapter, a system-on-chip design of the newest powerful standard in the hash families, named Whirlpool, is presented. With more details, an architecture and two VLSI implementations are presented. The first implementation is suitable for high-speed applications while the second one is suitable for applications with constrained silicon area resources. The architecture permits a wide variety of implementation tradeoffs. Different implementations have been introduced and each specific application can choose the appropriate speed-area trade-off implementation. The implementations are examined and compared in the security level and in the performance by using hardware terms. Whirlpool with RIPEMD, SHA-1, and SHA-2 hash functions are adopted by the International Organization for Standardization (ISO/IEC) 10118-3 standard. The Whirlpool implementations allow fast execution and effective substitution of any previous hash families' implementations in any cryptography application.

Section II
Security in 3G/B3G/4G

The fourth generation of mobile networks (4G) will be a technology-opportunistic and user-centric system combining the economic and technological advantages of different transmission technologies to provide a context-aware and adaptive service access anywhere and at any time. Security turns out to be one of the major problems that arise at different interfaces when trying to realize such a heterogeneous system by integrating the existing wireless and mobile systems. Indeed, current wireless systems use very different and difficult to combine proprietary security mechanisms, typically relying on the associated user and infrastructure management means. It is generally impossible to apply a security policy to a system consisting of different heterogeneous subsystems. In this chapter, we first briefly present the security of candidate 4G access systems, such as 2/3G, WLAN, WiMax and so forth. In the next step, we discuss the arising security issues of the system interconnection. We namely define a logical access problem in heterogeneous systems and show that both the technology-bound low-layer and the overlaid high-layer access architectures exhibit clear shortcomings. We present and discuss several proposed approaches aimed at achieving an adaptive, scalable, rapid, easy-to-manage, and secure 4G service access independently of the used operator and infrastructure. We then define general requirements on candidate systems to support such 4G security.

Chapter XIX

The integration of heterogeneous mobile/wireless networks using an IP-based core network materializes the beyond 3G (B3G) mobile networks. Along with a variety of new perspectives, the new network model raises new security concerns, mainly because of the complexity of the deployed architecture and the heterogeneity of the employed technologies. In this chapter, we examine and analyze the security architectures and the related security protocols, which are employed in B3G networks focusing on their functionality and the supported security services. The objectives of these protocols are to protect the involved parties and the data exchanged among them. To achieve these, they employ mechanisms that provide mutual authentication as well as ensure the confidentiality and integrity of the data transferred over the wireless interface and specific parts of the core network. Finally, based on the analysis of the security mechanisms, we present a comparison of them that aims at highlighting the deployment advantages of each one and classifies the latter in terms of (a) security, (b) mobility, and (c) reliability.

Chapter XX

This chapter analyzes the security architecture designed for the protection of the universal mobile telecommunication system (UMTS). This architecture is built on the security principles of 2G systems with improvements and enhancements in certain points in order to provide advanced security services. The main objective of the 3G security architecture is to ensure that all information generated by or relating to a user, as well as the resources and services provided by the serving network and the home environment, are adequately protected against misuse or misappropriation. Based on the carried analysis, the critical points of the 3G security architecture, which might cause network and service vulnerability, are

identified. In addition, the current research on the UMTS security and the proposed enhancements that aim at improving the UMTS security architecture are briefly presented and analyzed.

Chapter XXI

Motivated by the requirements for higher data rate, richer multimedia services, and broader radio range, wireless mobile networks are currently in the stage evolving from the second-generation (2G), for example, global system for mobile communications (GSM), into the era of third-generation (3G) or beyond 3G or fourth-generation (4G). Universal mobile telecommunications system (UMTS) is the natural successor of the current popular GSM. Code division multiple access 2000 (CDMA2000) is the next generation version for the CDMA-95, which is predominantly deployed in the North America and North Korea. Time division-sychrononous CDMA (TD-SCDMA) is in the framework of 3GPP2 and is expected to be one of the principle wireless technologies employed in China in the future. It is envisioned that each of three standards in the framework of international mobile telecommunications-2000 (IMT-2000) will play a significant role in the future due to the backward compatibility, investment, maintenance cost, and even politics. In all of the potential standards, access security is one of the primary demands as well as challenges to resolve the deficiency existing in the second generation wireless mobile networks such as GSM, in which only one-way authentication is performed for the core network part to verify the user equipment (UE). Such access security may lead to the "man-in-middle" problem, which is a type of attack that can take place when two clients that are communicating remotely exchange public keys in order to initialize secure communications. If both of the public keys are intercepted in the route by someone, that someone can act as a conduit and send in the messages with a fake public key. As a result, the secure communication is eavesdropped on by a third party.

Chapter XXII

The global system for mobile communications (GSM) is the most popular standard that implements second generation (2G) cellular systems. 2G systems combined with general packet radio services (GPRS) are often described as 2.5G, that is, a technology between the 2G and third (3G) generation of mobile systems. GPRS is a service that provides packet radio access for GSM users. This chapter presents the security architecture employed in 2.5G mobile systems, focusing on GPRS. More specifically, the security measures applied to protect the mobile users, the radio access network, the fixed part of the network, and the related data of GPRS, are presented and analyzed in details. This analysis reveals the security weaknesses of the applied measures that may lead to the realization of security attacks by adversaries. These attacks threaten network operation and data transfer through it, compromising end-users and network

security. To defeat the identified risks, current research activities on the GPRS security propose a set of security improvements to the existing GPRS security architecture.

Chapter XXIII

Security measures of mobile infrastructures have always been important from the early days of the creation of cellular networks. Nowadays, however, the traditional security schemes require a more fundamental approach to cover the entire path from the mobile user to the server. This fundamental approach is so-called end-to-end (E2E) security coverage. The main focus of this chapter is to discuss such architectures for IEEE 802.16e (Mobile-WiMAX) and major 3G cellular networks. The end-to-end implementations usually contain a complete set of algorithms and protocol enhancements (e.g., mutual identification, authentications, and authorization), including the VLSI implementations. This chapter discusses various proposals at the protocol level.

Chapter XXIV

This chapter outlines how cellular authentication can be utilized for generic application security. It describes the basic concept of the generic bootstrapping architecture that was defined by the 3rd generation partnership project (3GPP) for current networks and outlines the latest developments for future networks.The chapter will provide an overview of the latest technology trends in the area of generic application security.

Chapter XXV

Network mobility (NEMO) enables seamless and ubiquitous Internet access while on board vehicles. Even though the Internet Engineering Task Force (IETF) has standardized the NEMO basic support protocol as a network layer mobility solution, few studies have been conducted in the area of the authentication, authorization, and accounting (AAA) framework that is a key technology for successful deployment. In this chapter, we first review the existing AAA protocols and analyze their suitability in NEMO environments. After that, we propose a localized AAA framework to retain the mobility transparency as the NEMO basic support protocol and to reduce the signaling cost incurred in the AAA procedures. The proposed AAA framework supports mutual authentication and prevents various threats such as replay

attack, man-in-the-middle attack, and key exposure. Performance analysis on the AAA signaling cost is carried out. Numerical results demonstrate that the proposed AAA framework is efficient under different NEMO environments.

olume I

Section III
Security in Ad Hoc and Sensor Networks

Mobile ad hoc network (MANET) is a self-configuring and self-maintaining network characterized by dynamic topology, absence of infrastructure, and limited resources. These characteristics introduce security vulnerabilities, as well as difficulty in providing security services to MANETs. To date, tremendous research has been done to develop security approaches for MANETs. This work will discuss the existing approaches that have intended to defend against various attacks at different layers. Open challenges are also discussed in the chapter.

Providing privacy is often considered a keystone factor for the ultimate take up and success of mobile ad hoc networking. Privacy can best be protected by enabling anonymous communication and, therefore, this chapter surveys existing anonymous communication mechanisms for mobile ad hoc networks. On the basis of the survey, we conclude that many open research challenges remain regarding anonymity provisioning in mobile ad hoc networks. Finally, we also discuss the notorious Sybil attack in the context of anonymous communication and mobile ad hoc networks.

The pervasiveness of wireless communication recently gave mobile ad hoc networks (MANET) significant researchers' attention, due to its innate capabilities of instant communication in many time and mission critical applications. However, its natural advantages of networking in civilian and military environments make it vulnerable to security threats. Support for anonymity in MANET is orthogonal to a critical security challenge we faced in this chapter. We propose a new anonymous authentication protocol for mobile ad hoc networks enhanced with a distributed reputation system. The main objective is to provide mechanisms concealing a real identity of communicating nodes with an ability of resistance

to known attacks. The distributed reputation system is incorporated for a trust management and malicious behavior detection in the network.

Chapter XXIX

The increasing diffusion of wireless portable devices and the emergence of mobile ad hoc networks promote anytime and anywhere opportunistic resource sharing. However, the fear of exposure to risky interactions is currently limiting the widespread uptake of ad hoc collaborations. This chapter introduces to the challenge of identifying and validating novel security models/systems for securing ad hoc collaborations by taking into account the high unpredictability, heterogeneity, and dynamicity of envisioned wireless environments. We claim that the concept of trust management should become a primary engineering design principle, to associate with the subsequent trust refinement into effective authorization policies, thus calling for original and innovative access control models. The chapter overviews the state-of-the-art solutions for trust management and access control in wireless environments, by pointing out both the need for their tight integration and the related emerging design guidelines (e.g., exploitation of context awareness and adoption of semantic technologies).

Chapter XXX

Security has become a primary concern in mobile ad hoc networks (MANETs). The characteristics of MANETs pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and nonrepudiation. Cryptographic techniques are widely used for secure communications in wired and wireless networks. Most cryptographic mechanisms, such as symmetric and asymmetric cryptography, often involve the use of cryptographic keys. However, all cryptographic techniques will be ineffective if the key management is weak. Key management is also a central component in MANET security. The purpose of key management is to provide secure procedures for handling cryptographic keying materials. The tasks of key management include key generation, key distribution, and key maintenance. Key maintenance includes the procedures for key storage, key update, key revocation, key archiving, and so forth. In MANETs, the computational load and complexity for key management are strongly subject to restriction by the node's available resources and the dynamic nature of network topology. A number of key management schemes have been proposed for MANETs. In this chapter, we present a survey of the research work on key management in MANETs according to recent literature.

Mobile-IP ad hoc networks (MANETs) have gained popularity in the past few years with the creation of a variety of ad hoc protocols that specifically offer quality of service (QoS) for various multimedia traffic between mobile stations (MSs) and base stations (BSs). The lack of proper end-to-end security coverage, on the other hand, is a challenging issue as the nature of such networks with no specific infrastructure is prone to relatively more attacks, in a variety of forms. The focus of this chapter is to discuss a number of attack scenarios and their remedies in MANETs including the introduction of two entities, ad hoc key distribution center (AKDC) and decentralize key generation and distribution (DKGD), which serve as key management schemes.

The integration of wireless communication and embedded video systems is a demanding and interesting topic which has attracted significant research efforts from the community of telecommunication. This chapter discusses the challenging issues in wireless video surveillance and presents the detailed design for a novel highly-secure video surveillance system over ad hoc wireless networks. To this end, we explore the state-of-the-art in the cross domains of wireless communication, video processing, embedded systems, and security. Moreover, a new media-dependent video encryption scheme, including a reliable data embedding technique and real-time video encryption algorithm, is proposed and implemented to enable the system to work properly and efficiently in an open and insecure wireless environment. Extensive experiments are conducted to demonstrate the advantages of the new systems, including high security guarantee and robustness. The chapter would serve as a good reference for solving the challenging issues in wireless multimedia and bring new insights on the interaction of different technologies within the cross application domain.

Intrusion detection in ad hoc networks is a challenge because of the inherent characteristics of these networks, such as, the absence of centralized nodes, the lack of infrastructure, and so forth. Furthermore, in addition to application-based attacks, ad hoc networks are prone to attacks targeting routing protocols,

which is a novel problem. Issues in intrusion detection in ad hoc networks are addressed by numerous research proposals in literature. In this chapter, we first enumerate the properties of ad hoc networks which hinder intrusion detection systems. Second, significant intrusion detection system (IDS) architectures and methodologies proposed in the literature are elucidated. Strengths and weaknesses of these works are then studied and explained. Finally, the future directions, which will lead to the successful deployment of intrusion detection in ad hoc networks, are discussed.

Chapter XXXIV

In this chapter we present the growing challenges related to security in wireless sensor networks. We show possible attack scenarios and evidence the ease of perpetrating several types of attacks due to the extreme resource limitations that wireless sensor networks are subjected to. Nevertheless, we show that security is a feasible goal in this resource-limited environment. To prove that security is possible we survey several proposed sensor network security protocols targeted to different layers in the protocol stack. The work surveyed in this chapter enable several protection mechanisms vs. well documented network attacks. Finally, we summarize the work that has been done in the area and present a series of ongoing challenges for future work.

Chapter XXXV

The applications of wireless sensor networks (WSNs) are continuously expanding. Recently, consistent research and development activities have been associated to this field. Security ranks at the top of the issues that should be discussed when deploying a WSN. This is basically due to the fact that WSNs are, by nature, mission-critical. Their applications mainly include battlefield control, emergency response (when a natural disaster occurs), and healthcare. This chapter reviews recent research results in the field of WSN security.

Chapter XXXVI

Since routing is a fundamental operation in all types of networks, ensuring routing security is a necessary requirement to guarantee the success of routing operations. A securing routing task gets more challenging as the target network lacks an infrastructure-based routing operation. This infrastructure-less nature that invites a multihop routing operation is one of the main features of wireless sensor networks that raises the importance of secure routing problem in these networks. Moreover, the risky environment, application

criticality, and resources limitations and scarcity exhibited by wireless sensor networks make the task of secure routing much more challenging. All these factors motivate researchers to find novel solutions and approaches that would be different from the usual approaches adopted in other types of networks. The purpose of this chapter is to provide a comprehensive treatment of the routing security problem in wireless sensor networks. The discussion flow of the problem in this chapter begins with an overview on wireless sensor networks that focuses on routing aspects to indicate the special characteristics of wireless sensor networks from routing perspective. The chapter then introduces the problem of secure routing in wireless sensor networks and illustrates how crucial the problem is to different networking aspects. This is followed by a detailed analysis of routing threats and attacks that are more specific to routing operations in wireless sensor networks. A research-guiding approach is then presented to the reader that analyzes and criticizes different techniques and solution directions for the secure routing problem in wireless sensor networks. This is supported by state-of-the-art and familiar examples from the literature. The chapter finally concludes with a summary and future research directions in this field.

Localization of sensor nodes is very important for many applications proposed for wireless sensor networks (WSN), such as environment monitoring, geographical routing, and target tracking. Because sensor networks may be deployed in hostile environments, localization approaches can be compromised by many malicious attacks. The adversaries can broadcast corrupted location information and they can jam or modify the transmitting signals between sensors to mislead them to obtain incorrect distance measurements or nonexistent connectivity links. All these malicious attacks will cause sensors to not be able to, or wrongly, estimate their locations. In this chapter, we summarize the threat models and provide a comprehensive survey and taxonomy of existing secure localization and verification schemes for wireless sensor networks.

One of severe security threats in wireless sensor network is false data injection attack, that is, the compromised sensors forge the events that do not occur. To defend against false data injection attacks, six en-route filtering schemes in a homogeneous sensor network are described. Furthermore, a one sink filtering scheme in a heterogeneous sensor network is also presented. We find that deploying heterogeneous nodes in a sensor network is an attractive approach because of its potential to increase network lifetime, reliability, and resiliency.

Weiser envisioned ubiquitous computing with computing and communicating entities woven into the fabrics of every day life. This chapter deals with the survivability of ambient resource-constrained wireless computing nodes, from fixed sensor network nodes to small devices carried out by roaming entities, for example, as part of a personal area network of a moving person. First, we review the assets that need to be protected, especially the energy of these unplugged devices. There are also a number of specific attacks that are described; for example, direct physical attacks are facilitated by the disappearing security perimeter. Finally, we survey the protection mechanisms that have been proposed with an emphasis on cryptographic keying material and trust management.

Fault tolerance is one of the premier system design desiderata in wireless ad hoc and sensor networks. It is crucial to have a certain level of fault tolerance in most ad hoc and sensor applications, especially for those used in surveillance, security, and disaster relief. In addition, several network security schemes require that the underlying topology provide fault tolerance. In this chapter, we will review various fault tolerant techniques used in topology design for ad hoc and sensor networks, including those for power control, topology control, and sensor coverage.

Section IV
Security in Wireless PAN/LAN/MAN Networks

Security is always an important factor in wireless connections. As with all other existing radio technologies, the Bluetooth standard is often cited to suffer from various vulnerabilities and security inefficiencies, while attempting to optimize the trade-off between performance and complementary services including security. On the other hand, security protocols like IP secure (IPsec) and secure shell (SSH) provide strong, flexible, low cost, and easy to implement solutions for exchanging data over insecure communication links. However, the employment of such robust security mechanisms in wireless realms enjoins additional research efforts due to several limitations of the radio-based connections, for example link bandwidth and unreliability. This chapter will evaluate several Bluetooth personal area network (PAN) parameters, including absolute transfer times, link capacity, throughput, and goodput. Experiments shall employ both Bluetooth native security mechanisms, as well as the two aforementioned protocols. Through a plethora of scenarios, utilizing both laptops and palmtops, we offer a comprehensive in-depth comparative analysis of each of the aforementioned security mechanisms when deployed over Bluetooth communication links.

study on fast authentication solutions found in the literature as well as the industry that address this problem. These proposals focus on solving the mentioned problem for intradomain handoff scenarios where the access points belong to the same administrative domain or provider. Interdomain roaming is also becoming common-place for wireless access. We need fast authentication solutions for these environments that are managed by independent administrative authorities. We detail such a solution that explores the use of local trust relationships to foster fast authentication.

Mass deployment of radio-frequency identification (RFID) technology is now becoming feasible for a wide variety of applications ranging from medical to supply chain and retail environments. Its main draw-back until recently was high production costs, which are now becoming lower and acceptable. But due to inherent constraints of RFID technology (in terms of limited power and computational resources) these devices are the subject of intensive research on how to support and improve increasing demands for security and privacy. This chapter therefore focuses on security and privacy issues by giving a general overview of the field, the principles, the current state of the art, and future trends. An improvement in the field of security and privacy solutions for this kind of wireless communications is described as well.

Wireless communications are becoming ubiquitous in homes, offices, and enterprises with the popular IEEE 802.11 wireless LAN technology and the up-and-coming IEEE 802.16 wireless MAN technology. The wireless nature of communications defined in these standards makes it possible for an attacker to snoop on confidential communications or modify them to gain access to home or enterprise networks much more easily than with wired networks. Wireless devices generally try to reduce computation overhead to conserve power and communication overhead to conserve spectrum and battery power. Due to these considerations, the original security designs in wireless LANs and MANs used smaller keys, weak message integrity protocols, weak or one-way authentication protocols, and so forth. As wireless networks became popular, the security threats were also highlighted to caution users. A security protocol redesign followed first in wireless LANs and then in wireless MANs. This chapter discusses the security threats and requirements in wireless LANs and wireless MANs, with a discussion on what the original designs missed and how they were corrected in the new protocols. It highlights the features of the current wireless LAN and MAN security protocols and explains the caveats and discusses open issues. Our aim is to provide the reader with a single source of information on security threats and requirements, authentication technologies, security encapsulation, and key management protocols relevant to wireless LANs and MANs.

An overview of the technical and business aspects is given for the corporate deployment of services over WiMAX. WiMAX is considered to be a strong candidate for the next generation of broadband wireless access; therefore its security is critical. This chapter provides an overview of the inherent and complementary benefits of broadband deployment over a long haul wireless pipe, such as WiMAX. In addition, we explore end-to-end (E2E) security structures necessary to launch secure business and consumer class services. The main focus of this chapter is to look for the best security practice to achieve E2E security in both vertical and horizontal markets. The E2E security practices will ensure complete coverage of the entire link from the client (user) to the server. This is also applicable to wireless virtual private network (VPN) applications where the tunneling mechanism between the client and the server ensures complete privacy and security for all users. The same idea for E2E security is applied to client-server-based multimedia applications, such as in IP multimedia subsystem (IMS) and voice over IP (VoIP), where secure client/server communication is required. In general, we believe that WiMAX provides the opportunity for a new class of high data rate symmetric services. Such services will require E2E security schemes to ensure risk-free high data-rate uploads and downloads of multimedia applications. WiMAX provides the capability for embedded security functions through the 802.16 security architecture standards. IEEE 802.16 is further subcategorized as 802.16d (fixed-WiMAX) and 802.16e (mobile-WiMAX). Due to the mobility and roaming capabilities in 802.16e and the fact that the medium of signal transmission is accessible to everyone, there are a few extra security considerations applied to 802.16e. These extra features include PKMv2, PKM-EAP authentication method, AES encryption wrapping, and so forth. The common security features of 802.16d and 802.16e are discussed in this chapter, as well as the highlights of the security comparisons between other broadband access, 3G technologies, and WiMAX.

During the last few years, mobile broadband access has been a popular concept in the context of fourth generation (4G) cellular systems. After the wide acceptance and deployment of the wired broadband connections, such as DSL, the research community in conjunction with the industry have tried to develop and deploy viable mobile architectures for broadband connectivity. The dominant architectures which have already been proposed are Wi-Fi, UMTS, WiMax, and flash-OFDM. In this chapter, we analyze these protocols with respect to their security mechanisms. First, a detailed description of the authentication, confidentiality, and integrity mechanisms is provided in order to highlight the major security gaps and threats. Subsequently, each threat is evaluated based on three factors: likelihood, impact, and risk.

The technologies are then compared taking their security evaluation into account. Flash-OFDM is not included in this comparison since its security specifications have not been released in public. Finally, future trends of mobile broadband access, such as the evolution of WiMax, mobile broadband wireless access (MBWA), and 4G are discussed.

Authentication is an important part of the authentication, authorization, and accounting (AAA) schemes, and the extensible authentication protocol (EAP) is a universally accepted framework for authentication commonly used in wireless networks and point-to-point protocol (PPP) connections. The main focus of this chapter is the technical details to examine how EAP is integrated into the architecture of next generation networks (NGN), such as in worldwide interoperability for microwave access (WiMAX), which is defined in the IEEE 802.16d and IEEE 802.16e standards and in current wireless protocols, such as IEEE 802.11i. This focus includes an overview of the integration of EAP with IEEE 802.1x, remote authentication dial in user service (RADIUS), DIAMETER, and pair-wise master key version (2PKv2).