1

Overview of the Book

COPYRIGHTED MATERIAL

Mobile telecommunications systems have evolved in a stepwise manner. A new cellular radio technology has been designed once per decade. Analogue radio technology was dominant in the 1980s and paved the way for the phenomenal success of cellular systems. The dominant second-generation system Global System for Mobile Communications (GSM, or 2G) was introduced in the early 1990s, while the most successful third-generation system, 3G – also known as the Universal Mobile Telecommunications System (UMTS), especially in Europe – was brought into use in the first years of the first decade of the new millennium.

At the time of writing, the fourth generation of mobile telecommunications systems is being commercially deployed. Its new radio technology is best known under the acronym LTE (Long Term Evolution). The complete system is named SAE/LTE, where SAE (System Architecture Evolution) stands for the entire system, which allows combining access using the new, high-bandwidth LTE technology with access using the legacy technologies such as GSM, 3G and High Rate Packet Data (HRPD). The technical term for the SAE/LTE system is Evolved Packet System (EPS), and we shall be using this term consistently in the book. The brand name of the new system has been chosen to be LTE, and that is the reason why the title of the book is *LTE Security*.

With the pervasiveness of telecommunications in our everyday lives, telecommunications security has also moved more and more to the forefront of attention. Security is needed to ensure that the system is properly functioning and to prevent misuse. Security includes measures such as encryption and authentication, which are required to guarantee the user's privacy as well as ensuring revenue for the mobile network operator.

The book will address the security architecture for EPS. This is based on elements of the security architectures for GSM and 3G, but it needed a major redesign effort owing to the significantly increased complexity, and new architectural and business requirements. The book will present the requirements and their motivation and then explain in detail the security mechanisms employed to meet these requirements.

To achieve global relevance, a communication system requires world-wide interoperability that is easiest to achieve by means of standardization. The standardized part of the system guarantees that the entities in the system are able to communicate with each other even if they are controlled by different mobile network operators or manufactured

LTE Security, Second Edition. Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller and Valtteri Niemi.
© 2013 John Wiley & Sons, Ltd. Published 2013 by John Wiley & Sons, Ltd.

by different vendors. There are also many parts in the system where interoperability does not play a role, such as the internal structure of the network entities. It is better not to standardize wherever it is not necessary because then new technologies can be introduced more rapidly and differentiation is possible among operators as well as among manufacturers, thus encouraging healthy competition.

As an example in the area of security, communication between the mobile device and the radio network is protected by encrypting the messages. It is important that we standardize how the encryption is done and which encryption keys are used, otherwise the receiving end could not do the reverse operation and recover the original content of the message. On the other hand, both communicating parties have to store the encryption keys in such a way that no outsider can get access to them. From the security point of view, it is important that this be done properly but we do not have to standardize how it is done, thus leaving room for the introduction of better protection techniques without the burden of standardizing them first. The emphasis of our book is on the standardized parts of EPS security, but we include some of the other aspects as well.

The authors feel that there will be interest in industry and academia in the technical details of SAE/LTE security for quite some time to come. The specifications generated by standardization bodies only describe *how* to implement the system (and this only to the extent required for interoperability), but almost never inform readers about *why* things are done the way they are. Furthermore, specifications tend to be readable by only a small group of experts and lack the context of the broader picture. This book is meant to fill this gap by providing first-hand information from insiders who participated in decisively shaping SAE/LTE security in the relevant standardization body, 3rd Generation Partnership Project (3GPP), and can therefore explain the rationale for the design decisions in this area.

The book is based on versions of 3GPP specifications from March 2012 but corrections approved by June 2012 were still taken into account. New features will surely be added to these specifications in later versions and there will most probably also be further corrections to the existing security functionality. For the obvious reason of timing, these additions cannot be addressed in this book.

The book is intended for telecommunications engineers in research, development and technical sales and their managers as well as engineering students who are familiar with architectures of mobile telecommunications systems and interested in the security aspects of these systems. The book will also be of interest to security experts who are looking for examples of the use of security mechanisms in practical systems. Both readers from industry and from academia should be able to benefit from the book. The book is probably most beneficial to advanced readers, with subchapters providing sufficient detail so that the book can also be useful as a handbook for specialists. It can also be used as textbook material for an advanced course, and especially the introductory parts of each chapter, when combined, give a nice overall introduction to the subject.

The book is organized as follows. Chapter 2 gives the necessary background information on cellular systems, relevant security concepts, standardization matters and so on. As explained earlier, LTE security relies heavily on security concepts introduced for the predecessor systems. Therefore, and also to make the book more self-contained, Chapters 3–5 are devoted to security in legacy systems, including GSM and 3G, and security aspects of cellular–WLAN (Wireless Local Area Network) interworking.

Chapter 6 provides an overall picture of the EPS security architecture. The next four chapters provide detailed information about the core functionalities in the security architecture. Chapter 7 is devoted to authentication and key agreement which constitute the cornerstones for the whole security architecture. Chapter 8 shows how user data and signalling data are protected in the system, including protecting confidentiality and integrity of the data. A very characteristic feature in cellular communication is the possibility of handing over the communication from one base station to another. Security for handovers and other mobility issues is handled in Chapter 9. Another cornerstone of the security architecture is the set of cryptographic algorithms that are used in the protection mechanisms. The algorithms used in EPS security are introduced in Chapter 10.

In the design of EPS, it has been taken into account already from the beginning how interworking with access technologies that are not defined by 3GPP is arranged. Also, interworking with legacy 3GPP systems has been designed into the EPS system. These two areas are discussed in detail in Chapter 11.

The EPS system is exclusively packet based; there are no circuit-switched elements in it. This implies, in particular, that voice services have to be provided on top of Internet Protocol (IP) packets. The security for such a solution is explained in Chapter 12.

Partially independently of the introduction of EPS, 3GPP has specified solutions that enable the deployment of base stations covering very small areas, such as in private homes. This type of base station may serve restricted sets of customers (e.g. people living in a house), but open usage in hotspots or remote areas is also envisaged. These home base stations are also planned for 3G access, not only for LTE access. Such a new type of base station may be placed in a potentially vulnerable environment not controlled by the network operator and therefore many new security measures are needed, compared to conventional base stations. These are presented in detail in Chapter 13.

Chapter 14 introduces the security for relay nodes, a new feature introduced in Release 10 of 3GPP specifications. Relay nodes enable extensions for network coverage.

Chapter 15 addresses machine-type communication (MTC), also called machine-to-machine communication. The chapter provides an introduction to MTC security at the network level, the application level and the level of managing security credentials. First enhancements for the benefit of MTC appeared in 3GPP Release 10, after which further enhancements were done in Release 11 and still more are in the pipeline for Release 12. These all are discussed in the chapter.

Finally, Chapter 16 contains a discussion of both near-term and far-term future challenges in the area of securing mobile communications.

Many of the chapters depend on earlier ones, as can be seen from the descriptions given here. However, it is possible to read some chapters without reading first all of the preceding ones. Also, if the reader has prior knowledge of GSM and 3G systems and their security features, the first four chapters can be skipped. This kind of knowledge could have been obtained, for example, by reading the book *UMTS Security* [Niemi and Nyberg 2003]. The major dependencies among the chapters of the book are illustrated in Figure 1.1.

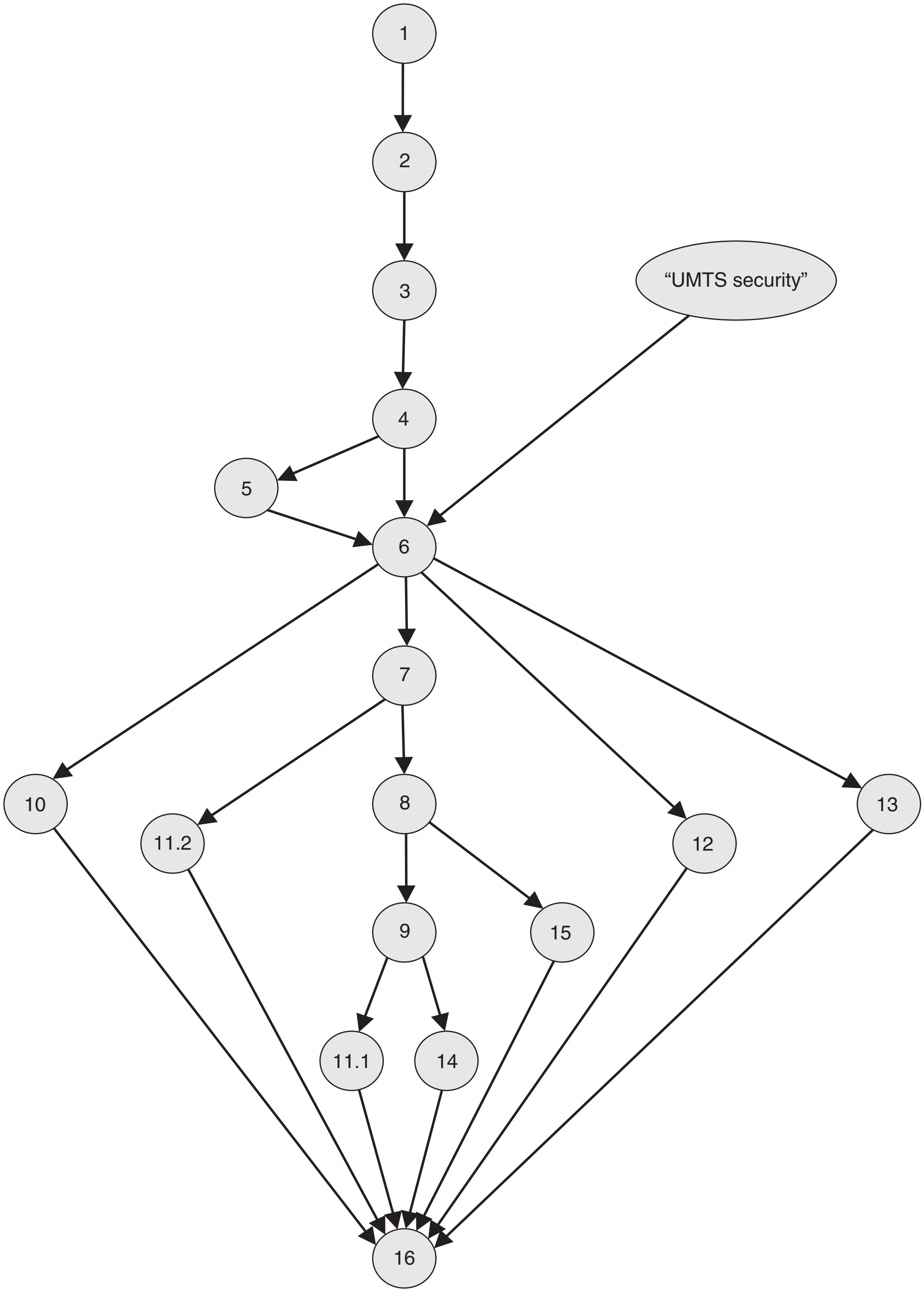

Figure 1.1 Major dependencies among chapters.