3 Wireless Security

W.-B. Lee

Feng Chia University, 100 Wen Hua Road, Taiwan

3.1 Introduction

Following the rapid development of the wireless communication services and the vast advancement of the mobile commerce community at large, security issues that are of crucial importance to the wired environment are resurfacing and creating a similar degree of impact. At heart, these security requirements for the wireless are essentially equivalent to the wired counterpart, which necessitates meeting the three fundamental demands below.

- Confidentiality: The assurance that the data is not revealed to unauthorized parties.
- Authentication: The assurance that the identities which the communicating entities proclaim are indeed their true identity.
- Integrity: The assurance that data received are exactly as sent by the genuine sender (i.e., contain no modification, insertion, deletion, or replay).

Furthermore, as our lives are gradually becoming more and more dependant on information and with wireless communication increasingly gaining dominance as the means for electronic and mobile commerce, one other additional security attribute that must be taken into account.

Non-repudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Although these topics are already intensely discussed, and many practical methods and mature approaches have taken shape, there are still significant differences that forbid us to fit these wired solutions onto the wireless systems due to a few intrinsic limitations. These limitations can be organized into two major categories, those relating to the mobile devices and those concerning wireless network environments.

3.1.1 Mobile Device

Due to power and size limitations, mobile device processors are usually consequently restricted, and incapable of performing complicated computations. On the other hand, memory capacity is equally limited, although extension memory card can be added, there are still of little assistance, and hardly help improve the

overall performance. These combined restrictions attach the following influences on security.

- Because the processor on mobile devices is on average computationally inferior to ordinary desktop computers, they usually do not accommodate adequate performance when dealing with computationally intensive public key encryption/decryption operations (e.g. RSA [3.1]).
- The memory storage on mobile devices is respectively smaller, thus placing restrictions on both the size of key length and digital certificate.

3.1.2 Wireless Network Environment

With respect to wired network, the wireless medium supports narrower bandwidth. Even as the 2.5G and 3G standards states to offer a transmission rate of up to 384kbps for the mobile transmission and 2Mbps for stationary communication, these figures are, for the most part, overly optimistic. Under realistic circumstances, various factors such as signal strength, environmental disturbances and communication density can alter the actual experience. Also, due to the openness of wireless channel, the coverage area of the wireless signal must also be carefully calculated to avoid possible eavesdropping or other active attacks. All in all, the influences, which limited bandwidth and radio wave have on security, are as follows:

- Because bandwidth is limited, the transmission load is naturally restricted. When the digital certificate or encrypted message becomes overly lengthy, transmission cost will rise, and users will experience extra waiting time. It is therefore important to minimize the payload transmitted.
- Due to the intrinsic property of wireless network, eavesdropping on the transmission content can easily be carried out without being causing detection, thus it is necessary to set up appropriate safety measures to lower the risk of privacy violation.

While porting security mechanisms seen in the wired network, for example encryption/decryption, digital signature etc., to achieve security requirements such as confidentiality, authentication and integrity on the wireless environment, we must lower the computation cost in order to comply to the mobile devices' computation capability, reduce the key lengths and the immense quantity of digital signature information to allow their storage within mobile devices, manage the bandwidth consumption to accommodate the relatively slow transmission rate, and also select radio wave coverage area to reduce the chance of information leakage.

This chapter focuses on the discussion of wireless related security issues. The use of public key cryptosystem is competently adapted to such tasks; nevertheless, in order for it to work correctly, a complete certification infrastructure must be in place to guarantee the validity of individual's public key. Thus we explain how such an infrastructure can be setup in the wireless environment. Section 3.2 will