Chapter 6
Identity-Based Cryptography: Applications, Vulnerabilities and Future Directions

Jenny Torres
University Pierre and Marie Curie, France

Michele Nogueira
Federal University of Parana, Brazil

Guy Pujolle
University Pierre and Marie Curie, France

ABSTRACT

Since computer systems and communication become each time more pervasive, information security takes attention, requiring guarantees for data authentication, integrity and confidentiality. Pervasive communication and computer systems intend to provide access to information and services anytime and anywhere, demanding cryptographic systems more practical and that consider the characteristics of emerging network paradigms, such as wireless communication, device constraints and mobility. Identity-Based Cryptography (IBC) is an asymmetric key cryptographic technology that employs as user's public key any unique information related to the identity of the user. IBC efficiently manages keying material and provides an easy way to issue a pair of keys applying user information. However, it assumes the existence of a Trusted Third Party (TTP), called Private Key Generator (PKG), which is responsible for generating the corresponding user private key. Relying on a TTP and using an identity as the base of the scheme result in different weaknesses on the system, as the inherent key escrow problem. This chapter investigates those weaknesses, and it points out the stat-of-the-art of proposed solutions to avoid them. This chapter also provides an overview of Identity-Based Encryption (IBE), Identity-Based Signature (IBS) and Identity-Based Key Agreement (IBKA), emphasizing IBE due to being an open problem for many years. This chapter concludes highlighting IBC applications and future trends.

DOI: 10.4018/978-1-61350-507-6.ch006

INTRODUCTION: CONTEXT AND GOALS

Conventional and emerging applications, such as *m-government, m-commerce and m-health*, require more and more information protection for supporting the development of the Information Society (Underwood, 2010). Such applications consider *information* as their main resource, presenting security requirements challenges in order to ensure an adequate protection to network elements and data communication. Further, the fast development of communication technology has resulted in changes on the way that people perform daily activities, allowing them to access information anywhere and anytime, and producing new requirements for security information (Perry, 2001).

Since information systems and sophisticated communication infrastructures become extensive, the number of threats in the network increases every day. These threats can be classified in two specific types, called attacks and intrusions. An attack is any action that explores a weakness of the system in order to compromise the integrity, confidentiality, availability and non-repudiation of the information. An intrusion also exploits weaknesses of the system, but it results from a successful attack. Nevertheless, the main goal is to disrupt services to access or alter confidential information and, then, use it in a malicious way. Attacks can occur in different levels of the network protocol stack, such as attacks that compromise servers on the application level, or denial of services (DoS) and sniffing on the communication level (Avizienis, 2004).

Nowadays, there are an unlimited number of security technologies, being cryptography the most used for achieving information security in the emerging information society. Cryptography has emerged in the last 20 years as an important discipline that provides the base for information security in many applications. Cryptographic techniques are now in widespread use, especially in financial services, in public sector and in personal privacy, such as in e-mail (Menezes, 1996). The main goal of cryptography is to guarantee *confidentiality, integrity, authenticity* and *non-repudiation*. These characteristics can be achieved trough the cryptographic primitives: Encryption, Digital Signature and Key Agreement. *Encryption* supports *confidentiality*. *Digital Signature* provides *authentication*, *integrity* and *non-repudiation*. And *Key Agreement* defines an easier way to distribute secret keys in order to establish a secure communication (Gorantla, 2005).

Due to the cryptography importance and the changes in information security caused by emerging networks, this chapter proceeds as follows. First of all it presents a general view about the background on cryptography. Next, it reviews IBC concepts, emphasizing the main primitives: signature, encryption and key agreement. Then, the chapter presents the main vulnerabilities and attacks on IBC. Further, it analyzes the main solutions applied to mitigate IBC weaknesses. Finally, this chapter provides future trends for this subject considering Internet context and emerging applications, such as cloud computing, mobile computing applications and nanocomputing. The chapter concludes with our point of view in relation to IBC based on this theoretical study.

BACKGROUND

The protection of sensitive information against unauthorized access or fraudulent changes has been a primary concern throughout centuries. The ability to protect the confidentiality of information, to prevent unauthorized access to data or services and to prevent the unauthorized modification of data is a fundamental requirement of security, as well as the ability to know whom you are talking to. Modern communication techniques, using computers connected through networks, make all