Chapter 2.25
Communication Security Technologies in Smart Organizations

Raphael C. W. Phan
Swinburne University of Technology (Sarawak Campus), Malaysia

ABSTRACT

In this chapter, we discuss the security technologies that are important in guaranteeing the good quality of communication within smart organizations. We first briefly review the various forms of communication that can be used in the current information age, before outlining the possible threats that can be faced in each communication medium. We then describe the relevant security technologies that help to protect communication media from common threats, as well as the security tools available in the market that implement these technologies. The topics discussed in this chapter would serve to educate the smart organizations towards securing their various means of communication, which is vital for a business establishment to exist and coexist with peers and partners.

INTRODUCTION

Smart organizations are knowledge-driven, internetworked, dynamically adaptive to new organizational forms, agile in ability to create and exploit opportunities offered by the new economy (Filos & Banahan, 2000). Being internetworked, therefore, some form of communication has to exist between two or more parties. This communication has to be effective and dependable, and furthermore the parties would have to know what is basically happening behind the scenes, and be ever ready to upgrade their knowledge with the latest in technology. Otherwise, this may result in communication breakdowns and hence prevent transactions from being accomplished or contracts from being sealed properly with peers and business partners. What this means is dependability of the communication process, and is the focus of this chapter.

Dependability means that our system can be trusted to perform the service for which it has been

designed, and can be decomposed into specific aspects as follows. Reliability characterizes the ability of a system to perform its service correctly when asked to do so. Availability means that the system is available to perform this service when it is asked to do so. Safety is a characteristic that quantifies the ability to avoid catastrophic failures that might involve risk to human life or excessive costs. Finally, security is the ability of a system to provide the following services (Stallings, 1999; Menezes, van Oorschot, & Vanstone, 1996) to communicating parties:

- Confidentiality: Ensures that the communicated information is accessible only by authorized parties.
- Authentication: Ensures that the origin of the message is correctly identified.
- Integrity: Ensures that only authorized parties can modify the communicated information, or enables parties to detect any unauthorized modifications to the information.
- Non-Repudiation: Ensures that neither party can deny having made any previous communications.

This chapter presents a discussion of security technologies available today to ensure the dependability of the communication process, which is vital within smart organizations since its parties are internetworked with each other, and therefore prone to network attacks and exploits by malicious crackers. One of the most important ways that smart organizations use to communicate is via the Internet. Performing transactions online via the Internet is an effective means (VeriSign, 2002) by which organizations can advertise and perform transactions with customers and other parties. However, online transactions will only be popular if the public trusts in their security (Amazon, 2003; Bolivia, 2003; Harris, 1998; Rawal, 2003; Tedeschi, 2000). Therefore, for an organization to be able to compete and advance, it needs knowledge, and hence careful management, of the various security technologies (Anderson, 2001; Garfinkel & Spafford, 1997) that help protect and safeguard public trust in its online transactions. The interested reader is also referred to the chapter on "New Challenges in Smart Organizations: Demands of Mobility" that also appears in this book for a discussion of other relevant future trends.

At the end of this chapter, we hope that the reader would have obtained a general perspective of communications security technologies that can be used in smart organizations. In particular, the objectives of this chapter include:

- Understanding of the various types of communication techniques
- Understanding of the possible threats faced by the communication process
- Familiarity with communication security technologies such as encryption, digital signatures, and message authentication codes (MACs)
- Familiarity with common software and hardware tools used to provide security technologies

BACKGROUND

Security is an important criteria these days, especially with in current information age in which information is available and accessible everywhere, in any form and with any means. The largest depository of information is the Internet, where infinite information is speedily available at one's fingertips.

With this vastness and freedom of information also comes the threats of abuse and misuse by malicious parties whose intent could be to deceive, steal, impersonate, cheat, or merely intrude into others' privacy.