Chapter 2.2
Security, Trust, and Privacy on Mobile Devices and Multimedia Applications

Edgar R. Weippl
Secure Business Austria, Austria

Bernhard Riedl
Secure Business Austria, Austria

ABSTRACT

While security in general is increasingly well addressed, both mobile security and multimedia security are still areas of research undergoing major changes. Mobile security is characterized by small devices that, for instance, make it difficult to enter long passwords and that cannot perform complex cryptographic operations due to power constraints. Multimedia security has focused on watermarks and the creation of digital evidences; as we all know, there are yet no good solutions to prevent illegal copying of audio and video files. In this chapter we focus on addressing the attributes of security, trust, and privacy on mobile devices and multimedia applications.

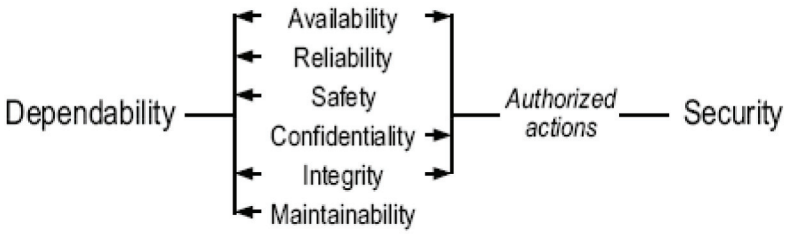
INTRODUCTION

Traditionally, there are three different fundamental attributes of security: confidentiality, integrity, and availability (CIA). Following Avizienis et al. (2004), security as well as dependability define the requirements of a reliable system (cf., Figure 1). In their opinion every system may fail, but can still be regarded reliable, if the frequency of failures is acceptable. Moreover only authorized actions should be served by a trusted system.

Security can also be seen as the summary of hardware, information, communication, and organizational aspects (Olovsson, 1992). Hardware security encompasses all aspects of physical security and emanation. Compromising emanation refers to unintentional signals that, if intercepted and analyzed, would disclose the information

DOI: 10.4018/978-1-61350-323-2.ch2.2

Figure 1. Dependability and security attributes (Avizienis, 2004)



transmitted, received, handled, or otherwise processed by telecommunications or automated systems equipment (NIS, 1992).

Information security includes computer security and communication security. Computer security deals with the prevention and detection of unauthorized actions by users of a computer system (Gollmann, 1999). Communication security encompasses measures and controls taken to deny unauthorized persons access to information derived from telecommunications and ensure the authenticity of such telecommunications (NIS, 1992).

Organizational or administration security is highly relevant even though people tend to neglect it in favor of fancy technical solutions. The most appropriate security measurements can be bypassed; for instance, by a successful social engineering attack on a user inside the system, who tells an attacker the necessary passwords (Thornburgh, 2004; Maris, 2005).

Both personnel security and operation security pertain to this aspect of security.

BACKGROUND

Whether a system is "secure" or not merely depends on the definition of the requirements. As nothing can ever be absolutely secure, the definition of an appropriate security policy based on the requirements is the first essential step to implement security.

Systematic Categorization of Requirements

All requirements that we perceive can be traced back to one of the three major security requirements: confidentiality, integrity and availability. A fourth requirement, non-repudiation, can be seen as a special case of integrity and availability (i.e., the integrity of message which was sent from A to B), whereas a fifth requirement, privacy, is a special case of confidentiality.

Confidentiality

The perhaps most well known security requirement is confidentiality. It means that users may obtain access only to those objects for which they have received authorization, and will not get access to information they must not see. The security policies guaranteeing confidentiality are implemented by means of access control.

Closely related to confidentiality is the term of privacy. According to Westin (1968), "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Privacy can be reached by the concealment of the association between information and a certain user's identity (Taipale, 2004; Pfitzmann & Koehntopp, 2005). There are two cases of granting privacy: reversible and irreversible anonymity. In some cases, for example for a polling system, it is not necessary to re-establish