Chapter III
Security and Trust in Mobile Multimedia

Edgar R. Weippl
Vienna University of Technology, 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 digital rights management and watermarks; as we all know, there are yet no good solutions to prevent illegal copying of audio and video files.

INTRODUCTION TO SECURITY

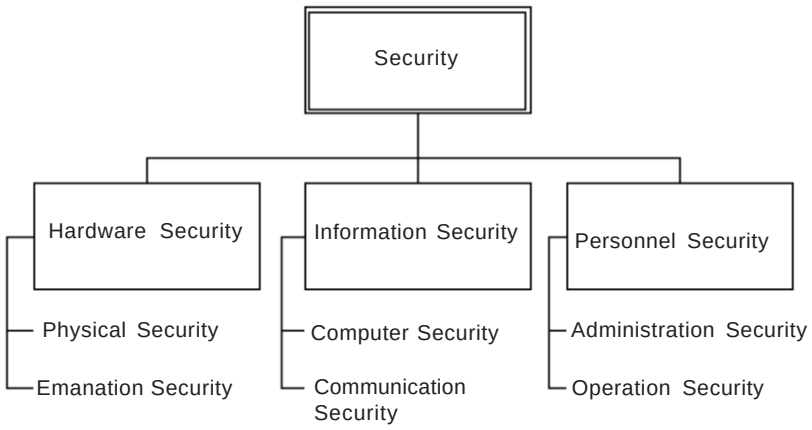
Traditionally, there are at least three fundamentally different areas of security illustrated in Figure 1 (Olovsson, 1992): Hardware security, information security and organizational security. A forth area, that is outside the scope of this chapter, are legal aspects of security.

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

Figure 1. Categorization of areas in security



Systematic Categorization of Requirements

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.

Security requirements can generally be defined in terms of four basic requirements: secrecy, integrity, availability, and non-repudiation. All other requirements that we perceive can be traced back to one of these four requirements. The forth requirement, non-repudiation, could also be seen as a special case of integrity, (i.e., the integrity of log data recording who has accessed which object).

Secrecy

The perhaps most well known security requirement is secrecy. 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 secrecy are implemented by means of access control.

Integrity

The integrity of the data and programs is just as important as secrecy but in daily life it is frequently neglected. Integrity means that only authorized people are permitted to modify data (or programs). Secrecy of data is closely connected to the integrity of programs of operating systems. If the integrity of the operating system is violated, then the reference monitor may not work properly any more. The reference monitor is a mechanism which insures that only authorized people are able to conduct operations. It is obvious that secrecy of information cannot be guaranteed any longer if this mechanism is not working. For this reason it is important to protect the integrity of operating systems just as properly as the secrecy of information.

The security policy guaranteeing integrity is implemented by means of access control as like previously discussed.