Chapter 1
Introduction to Information Security

The NIST Computer Security Handbook [NIST, 1995] defines the term *computer security* as "protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)." The security concepts of confidentiality, integrity and availability are also called the CIA triad.

Confidentiality of information is typically seen as assurance that sensitive information is accessed only by authorized users. This task can be achieved by various mechanisms such as encryption and access control.

Integrity of information is typically seen as assurance that information is not modified by unauthorized users in a way that authorized users will not be able to identify the modification. This task can be achieved by various mechanisms such as digital signatures and message authentication code.

Availability is the task of ensuring that a system provides its services to its users at any point in time. Usually a system includes many mechanisms to ensure its availability, such as use of several independent power sources and multiple communication lines.

Nonrepudiation, access control, authentication, and privacy are concepts that are considered part of computer security as well.

Nonrepudiation ensures that a user who sends a message cannot deny that she is the originator of the message and furthermore, that the receiver of the message can prove in a court of law that she received the message from the sender.

Access control is the task of controlling which information and services a user may access after being identified. An access control mechanism can be used only if the user has been initially identified by the system. In many systems, every authorized action of the user is recorded by an *audit* mechanism.

Authentication is the task of verifying the identity of users who connect to a computerized system. This task can be achieved by the user's providing a unique secret

A. Shabtai et al., *A Survey of Data Leakage Detection and Prevention Solutions*, SpringerBriefs in Computer Science, DOI 10.1007/978-1-4614-2053-8_1,

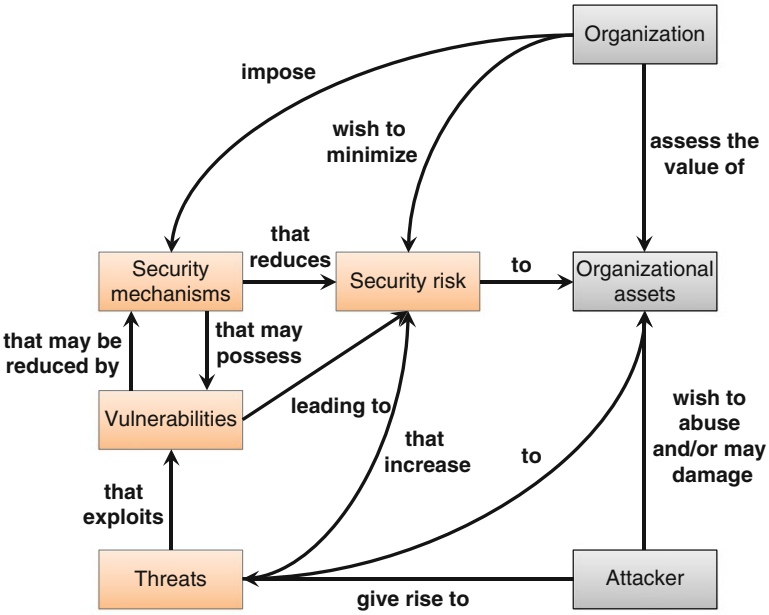

Fig. 1.1 Relationship among security terminology players (adapted from Stallings and Brown (2007))

such as a password (the user proves "what she knows"), using a unique token that the user possesses (the user proves "what she has"), or using some kind of biometric identification mechanism such as fingerprint (the user proves "what she is").

Privacy relates to the task of certifying that a user has control of information collected about her and exposed to others. It is difficult to define the specific mechanisms used to ensure such user privacy. The entire system must be designed so that the user's privacy will not be violated.

Ensuring computer security is an extremely challenging task [Elovici, 2012]. In many cases, the security requirements are clear; however, it is less clear how to use the various mechanisms to meet these requirements. The security mechanism in many cases may become the next sensitive part of the system. For example, forcing the user to use a complex password may result in the user's writing a note with the password attached to the computer screen. Computer security is a continuous battle between the attackers who identify new security holes and vulnerabilities in systems and the organization's security department who must prevent them.

This book uses the security terminology proposed in [Stallings, 2007], which is presented in Figure 1.1. It is described here in the context of data leakage and data misuse.

The security terminology described in Figure 1.1 includes three physical players (organization, attackers, and organizational assets) and four logical players (security mechanisms, vulnerabilities, threats and security risks). The *organization* assesses the value of each of its organizational assets (database, server, etc.) In this book, the assets are mainly data and information which are stored in files or databases. The *organization* tries to minimize the *security risks* by putting the appropriate *security mechanisms* in place (firewall, intrusion prevention system, etc.) This book will focus mainly on security mechanisms that are related to information leakage detection and prevention. The *attackers* try to create *security threats* to compromise the *organization's assets*. In this book, the main goal of the attackers is to leak or misuse confidential information. The *organizational assets* are exposed to *security threats*. On the one hand, *security mechanisms* reduce existing *vulnerabilities*, yet on the other hand may create additional *vulnerabilities*. The *organization* also creates *vulnerabilities*, for instance, by not complying with its security policy. For example, in the context of this book, a user who provides his or her credentials to an unauthorized person makes the system vulnerable to attacks. *Vulnerabilities* are exploited by the *attackers*, in turn leading to risks to the *organizational assets*. In the context of this book, vulnerabilities will be used by the attacker in order to leak or misuse confidential information.

The following *computer and network security incident* taxonomy that is widely accepted by the computer and network security community describes all key players involved in security attack incidents. Each taxonomy description is accompanied by examples which relate to the topic of the book. The different parts of the taxonomy are:

- **Attacker**: an adversary that attempts to attack a computer, communication network, or both to fulfill an objective. In the data leakage context, the attacker may be an internal employee or an external attacker attempting to leak sensitive information.
- **Tool**: the means and methods that are used to perform the attack by exploiting the vulnerability in a computer, communication network or both, including *physical attack* (for example, physically accessing a computer and copying data) or *running a script or a malicious application* (for example, a Trojan horse uploading sensitive information to a remote server).
- **Vulnerability**: a weakness or flaw in the design, implementation or configuration of a system, communication network, or business process that in many cases is known only to the attackers. A common example is a super user such as the database administrator (DBA) or system administrator, who usually has full access to systems and data.
- **Action**: an act taken by the attackers to perform the attack and achieve the objective. For example, an action can be stealing user name and password using social engineering.
- **Target**: the component of the computer, communication network, or both that is the aim of the attack and usually includes a vulnerability. In the context of this book a target can be a server with confidential information.

- **Unauthorized result**: an unauthorized consequence of an event that will eventually lead to information leakage, data misuse or both.
- **Objectives**: the results expected by the attacker. In this book, the objective is either to leak or misuse confidential information.

Data leakage and data misuse are considered an emerging security threats to organizations, especially when carried out by insiders. In many cases, it is very difficult to detect insiders because they misuse their credentials to perform an attack. How can a security mechanism detect an insider who leaks confidential information to which she is exposed during her regular tasks in the organization? The vulnerabilities of internal systems are known to the insider and, in some cases, she might know which security mechanisms are used.

This book aims to provide a structural and comprehensive overview of current research and practical solutions in the DLP domain. Existing solutions have been grouped into different categories based on a taxonomy described in the book. The taxonomy presented characterizes DLP solutions according to various aspects such as leakage source, data state, leakage channel, deployment scheme, prevention and detection approaches, and action taken upon leakage.