Chapter 8

Security Risks in E-Postage Systems

8.1 RISK MANAGEMENT

The primary goal of e-postage systems is to enable mailers to use the services of postal operators (universal and competitive), to determine the correct amount of postage for each service used, and to transfer the corresponding funds from the mailer to the postal operator in a secure and timely manner. Secondary goals are to provide the postal operators with accurate usage data, to supply mailers with accurate track and trace information and to protect the mailers' and recipients' privacy.

Important assets of an electronic postage system are the postal revenues, the related taxes such as sales tax, the service fees of the e-postage providers, the usage data of all mailers, the track and trace information for the mailers, and the payment information of mailers such as bank account and credit card information.

In order to design and operate secure e-postage systems through their entire system life-cycle, it is important during the design stage to anticipate the security threats to which the e-postage system will be exposed during the system lifetime and after the system's deployment to re-evaluate its residual risks on a regular basis. For any e-postage system under consideration, all this must be planned, organized and performed through an ongoing process called *risk management*. It is an iterative cycle of assessing risks, taking steps to reduce the identified risks to an acceptable level and maintaining that level of risk.

- During the *risk assessment stage* one needs to identify the relevant *assets* of the system and value them. Next, one identifies the possible *threats* that may harm the identified assets. Threats include unintentional disaster or malfunction as well as intelligent attacks. In order to understand the system exposure to intelligent attacks realistically, it is helpful to develop an *attacker model* describing which parts of the system are assumed to be accessible by an attacker in which ways and how strong in terms of resources the attacker is assumed to be. An example of a classification of attacker strength is given by Weingart

et al [120] of IBM, which is reproduced in Section 10.3.1 on page 213.

Unintentional threats can be valued by their likelihood. Intelligent attacks can be valued by the expected cost they incur on the perpetrator. Threats can exploit *vulnerabilities* of the e-postage system thereby imposing a *security risk* on the system. A security risk is all the bigger, the more valuable the targeted asset is, the more likely or the cheaper the threat is to incur, and the more severe or critical the expected compromise of or damage to the respective asset will be. This is illustrated by Figure 65 on page 184.

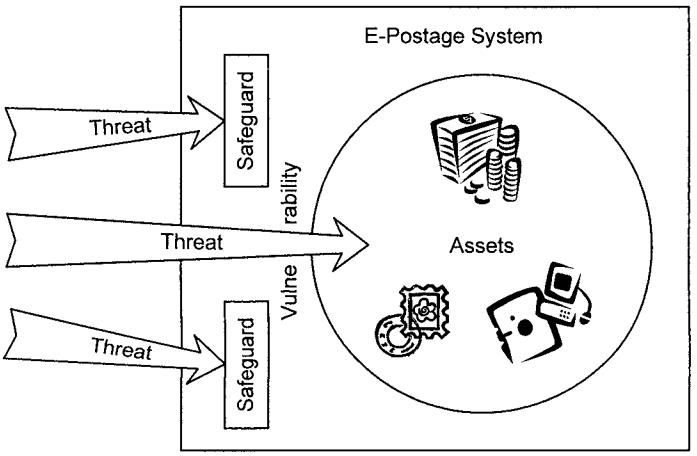

Figure 65. Illustration of Risk Management

- During the *risk reduction stage*, one needs to eliminate or reduce vulnerabilities by strengthening existing safeguards and controls or introducing additional ones. All changes to the system are reflected by the system documentation.
- The *risk maintenance stage* usually consists of a system security audit in which all security-critical subsystems and security safeguards are inspected to be in effect and working. The resulting system security report provides the basis on which the current system security level can be determined and compared to the level of system security that was achieved during the previous system security audit or when the e-postage system was first deployed. If new threats or new vulnerabilities are discovered, or existing safeguards are found to be no longer effective, then a new risk reduction stage is entered where appropriate