Chapter 4.13
E-Business Systems Security for Intelligent Enterprise

Dennis Trcek
University of Primorska, Koper, Slovenia

INTRODUCTION AND BACKGROUND

Security became a topic of research with the introduction of *networked information systems*, or networked IS, in the early eighties. In the mid-nineties the proliferation of the Internet in the business area exposed security as one of the key factors for successful online business, and the majority of effort to provide it was focused on technology. However, due to lessons learned during this period, the paradigms have since changed, with increasing emphasis on human factors. It is a fact that security of information systems is becoming part of the core processes in all e-business environments. While data is clearly one of the key assets and has to be protected accordingly, IS have to be highly integrated and open. Appropriate treatment of these issues is not a trivial task for managers of intelligent enterprises and requires new approaches, especially in light of new technologies.

Proper management of security in *e-business systems* requires a holistic methodology with a two-plane approach, technological and organizational. In every case IS security management starts with the identification of threats and threats analysis - a typical example is based on risk probability and damage estimates (Raepple, 2001). Following this, the approach differs according to the plane:

- The technological plane takes into account machine-related interactions. This plane is about deployment of appropriate *security services* that are based on *security mechanisms*. To become operational, key management issues (i.e., handling of cryptographic algorithms' keys) have to be resolved. Finally, human-to-machine interactions have to be addressed carefully.
- In parallel, it is necessary to properly address the organizational plane where human resources management plays a central role. This plane emphasizes the organizational issues and socio-technical nature of contemporary IS, where modern methodologies play a central role.

FUTURE TRENDS: TECHNOLOGICAL PLANE OF IS SECURITY MANAGEMENT

From the technological point of view, the prevention of threats is achieved by use of security mechanisms and security services (ISO, 1995). Mechanisms include symmetric and asymmetric cryptographic algorithms, for example, AES (Foti, 2001) and RSA (RSA Labs, 2002); one-way hash functions such as SHA-1 (Eastlake, 2001); and physical mechanisms. For devices with weak processing capabilities like smart-card, elliptic curve-based systems such as ECDSA (ANSI, 1998) can be used. Regarding physical security, using cryptographic algorithms one can only reduce the amount of data that has to be physically protected, but the physical protection cannot be avoided.

To ensure that a particular public key indeed belongs to the claimed person, a trusted third party called *certification authority*, or CA, has to be introduced. The CA issues *public key certificates* that are digitally signed electronic documents, which bind entities to the corresponding public keys (certificates can be verified by CA's public key). CA also maintains certificate revocation lists, or CRL that should be checked every time a certificate is processed in order to ensure that a private/public key is still valid. The de iure and de facto standard for certificate format is X.509 standard (ITU-T, 2000).

By use of security mechanisms, the following security services are implemented:

- Authentication: Ensures that the peer communicating entity is the one claimed.
- Confidentiality: Prevents unauthorized disclosure of data.
- Integrity: Ensures that any modification, insertion, or deletion of data is detected.
- Access Control: Enables authorized use of resources.
- Non-Repudiation: Provides proof of origin and proof of delivery, where false denying of the message content is prevented.
- Auditing: Enables detection of suspicious activities and analysis of successful breaches, and serves as evidence when resolving legal disputes.

To enable these services, a certain infrastructure has to be set up. It includes a Registration Authority (RA) that serves as an interface between a user and CA, identifies users, and submits certificate requests to CA. In addition, a synchronized time base system is needed for proper operation, along with a global directory for distribution of certificates and CRLs. All these elements, together with appropriate procedures, form a so-called *public key infrastructure* or PKI (Arsenault, 2002).

To provide security, mostly commercial off-the-shelf solutions are used. Such solutions typically include firewalls, which are specialized computer systems that operate on the border between the corporate network and the Internet, where all traffic must pass through these systems (Cheswick & Bellovin, 1994). Further, real-time

Table 1. Summary of basic security-related elements—technological plane

- *Security Mechanisms*: Symmetric and asymmetric algorithms, one-way hash functions, physical mechanisms
- *Security Services*: Authentication, confidentiality, integrity, non-repudiation, access control, auditing
- *Security Infrastructure*: Public key infrastructures, commercial off-the-shelf solutions (firewalls, intrusion detection systems, IPSec, SSL, S/MIME