# E-Business Systems Security in Intelligent Organizations

**Denis Trček**
*Jožef Stefan Institute, Slovenia*

## INTRODUCTION

Security as we perceive it today became a topic of research with the introduction of *networked information systems*, or networked ISs, in the early 1980s. In the mid-1990s 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 efforts to provide it were 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 networked ISs 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, ISs have to be highly integrated and open. Appropriate treatment of these contradictory issues is not a trivial task for managers of contemporary intelligent organizations. It requires new approaches, especially in light of new technologies.

## BACKGROUND

Proper management of security in *e-business systems* requires a holistic methodology that can be viewed on three planes: technology, organization, and legislation (Trček, 2006). ISs security management starts with the identification of threats and threats analysis. A typical approach is based on risk probability and derived 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.
- The organizational plane takes human resources management into account. It emphasizes the organizational issues and socio-technical nature of contemporary IS, where various modern methodologies play a central role.
- In parallel, it is necessary to address legal issues. Not only national, but also international legislation in this area is becoming increasingly broad and complex. Each and every security policy has to take this into account, especially cryptography regulations, digital signature issues, privacy issues, and intellectual property rights.

## METHODOLOGICAL APPROACHES TO E-BUSINESS SYSTEMS

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 & Jones, 2001); and physical mechanisms. For devices with weak processing capabilities like smart-cards, 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 have to be physically protected, but physical protection cannot be eliminated.

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 CRLs. These 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.

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

| |
|---|
| • **Security Mechanisms:** Symmetric and asymmetric algorithms, one-way hash functions, physical mechanisms<br>• **Security Services:** Authentication, confidentiality, integrity, non-repudiation, access control, auditing<br>• **Security Infrastructure:** Public key infrastructure, commercial off-the-shelf solutions (firewalls, intrusion detection systems), technologies IPSec, SSL, S/MIME, EAP, RADIUS, and WPA |

- **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 necessary procedures, form a so-called *public key infrastructure* or PKI (Arsenault & Turner, 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 intrusion detection systems (Kemmerer & Vigna, 2002) are deployed for detecting acts that differ from normal, known patterns of operation, or for detecting wrong behavior. Further, IPSec (Thayer, Doraswamy, Glenn, 1998), which is a security enhancement for IP protocol, is becoming a norm to prevent masquerade, monitoring of a communication, modification of data, and session overtaking. IPSec is suitable for virtual private networks, or VPNs, where one can establish secure private networks using public networks such as the Internet. Further, secure sockets layer protocol, or SSL (Freier, Karlton, & Kocher, 1996), provides a common security layer for Web and other applications and is available by default in Web browsers. It provides authentication, confidentiality, and integrity with the possibility of negotiating crypto primitives and encryption keys. Last but not least, secure/multipurpose Internet mail extensions standard, or S/MIME (Ramsdell, 1999), is often deployed as security enhancement for ordinary e-mail. It provides authentication, confidentiality, integrity, and non-repudiation.

Increased penetration of wireless communications into business environments brings new topics on the agenda that are specific to *wireless security* (Miller, 2001). In this area it is nowadays common to deploy physical/link level security by using IEEE 802.1X standard (IEEE, 2004). 802.1X is a framework for authentication, access control, and key-exchange. Its authentication deploys Extensible Authentication Protocol, or EAP (Aboba, Blunk, Vollbrecht, Carlson, & Levkowitz, 2004), which is usually used together with RADIUS server (Rigney, Willens, Rubens, & Simpson, 2000) for remote authentication and accounting. In addition, a derivative of 802.1X, called WiFi Protected Access, or WPA, is very common. Despite these technologies, wireless networks are inherently more vulnerable than wired networks, thus wireless access points are often put outside corporate firewalls.

However, even superior technological solutions will be in vain, if the complementary organizational and legal issues are not treated properly. Therefore, the second plane that is concentrated on organizational issues through human resources management has to be properly covered by *security policy*. In addition, the third plane has to be taken into account to assure that all efforts are aligned with existing legislation.

The first standard in the area of security policies was BS 7799 (BSI, 1995), with its most current international successor being ISO (2005). This standard plays a central role as far as security policy management is concerned. However, to implement successfully security policy, it is essential to support managers of contemporary intelligent organizations with appropriate techniques. The organizational plane is characterized by a complex interplay between human factor and technology. The two constituent parts are coupled in many ways, such as by interactions. A large number of these interactions form various feedback loops. There are also soft factors that have to be taken into account, for example, human perception of various phenomena like trust. Therefore, to support decision making properly with regard to security, one has to deal with physical and information flows. Additionally, decisions are often to be made in circumstances where there is not enough time or resources to test decisions in a real environment; often such checks are not possible at all. Therefore, support from computer simulations is highly desirable.

The methodology that can be used to support the resolution of the previously mentioned problems is *business dynam-*