# On scalable security model for sensor networks protocols

B. Księżopolski
*Faculty of Mathematics, Physics and Computer Science, M. Curie-Skłodowska University, Lublin, Poland*
Z. Kotulski
*Polish Academy of Sciences, Institute of Fundamental Technological Research, Warsaw, Poland &*
*Warsaw University of Technology, Faculty of Electronics and Information Technology, Warsaw, Poland*

ABSTRACT: Distributed sensor networks meet many different barriers that reduce their efficient applicability. One of them is requirement of assurance of the information security when it is transmitted, transformed, and stored in the electronic service. It is possible to provide an appropriate level of security applying the present-day information technology. However, the level of the protection of information applied to the whole network is often much higher than it is necessary to meet potential threats. Since the level of security strongly affects the performance of whole system, the excessive protection decreases the system's reliability and availability and, as a result, the global security of the construction. In this paper we present a model of scalable security for digital information transmission systems for the sensor network. In our model the basic element is the risk management procedure leading to an adequate protection level.

## 1 INTRODUCTION

Advanced teleinformatic technologies nowadays provide a wide range of possibilities of development of industry or the institutions of public services. The big stress is put on the development of well-available information services called "e-everything", like: e-government, e-money, e-banking, e-construction. These mentioned processes are fulfilled mainly by electronic way, thanks to which one can increase their availability, efficiency, and reliability, decreasing simultaneously the expenses of functioning.

Implementation of the public/firmware services is connected with the proper level of security of information exchanged between the parties of protocols realizing their main functions. Among teleinformatic technologies and cryptographic modules there are ones protecting different information security services, e.g.: confidentiality, integrity, non-repudiation, and anonymity of data (both, anonymity of the origin or destination of the data). The important problem seems to be the establishing the level of information security satisfied by the services in a given protocol. Every use of any network service is connected with information exchange, which in the case of successful attack causes different threats to the whole process. Estimation of the security levels for each phase of the communication or cryptographic protocol could help in solving this problem. However, such an approach seems to be only a partial solution, because thanks to a given service one can send information of different level of threats. A common practice is to use exaggerated tools of information security, which decrease an efficiency, system availability and introduce redundancy. Another effect of exaggeration of the security mechanisms is increasing the system complexity, which later influences implementation of a given project in practice, especially increasing expenses and decreasing efficiency.

The solution of this inconsistency seems to be the introduction of scalable security model, which can change security level depending on particular conditions of a given case. In the paper a mechanism, which can modify the level of information security for each phase of a protocol, is presented. Parameters, which influence modification of the security level, are: the risk of successful attack, probability of successful attack and some measures of independence (leading to completeness) of security elements. The used security elements, which take care of the protection of information, are based mainly on PKI (Public Key Infrastructure) services and cryptographic modules.

As an additional aspect of the scalable security model, especially dedicated to the sensor networks security and reliability, we consider the scalable security through the networks' topology. We introduce a certain core sub-network with higher protection and cross-validation mechanisms to detect incidents wherever in the network. This is especially important in wireless networks with probable natural alternate communication breaks and restorations.

## 2 SECURITY SERVICES

In practice, realization of electronic processes is connected with fulfilment of many technological, legal and formal standards. While projecting the systems we can take care of different security services (Lambrinoudakis et al. 2003, NIST 2004). Among them we can specify: confidentiality of data, integrity of data, anonymity (or, more generally, privacy) of parties of the protocol, non-repudiation of senders and recipients, authorization of data and entities, secure data storage, management of privileges, public trust, freshness. Every security service has got its own characteristics (see Table 1).

Table 1: Characteristics of security services.

| Group of services | Name of services | Characteristics |
|---|---|---|
| Integrity | *Integrity of data* | Guarding against improper information modification or destruction |
| Non-repudiation | *Non-repudiation of action* | Non-repudiation of sending the message |
| | *Non-repudiation of sender* | Non-repudiation of sender's identity |
| | *Non-repudiation of receiver* | Non-repudiation of recipient's identity |
| Confidentiality | *Confidentiality of data* | Preserving authorized restriction on information access and disclosure |
| Authorization | *Authorization of parties of the protocol* | Correct authorization of parties of protocol is required to participate at the protocol |
| Privileges | *Management of privileges* | A function in protocol depends on the permission level |
| Anonymity | *Network anonymity* | Anonymity of message sender (with network anonymity) |
| | *Anonymity of data* | Anonymity of message sender (without network anonymity) |
| Availability | *Availability of services* | Ensuring timely and reliable access to and use of information |
| Public trust | *Trust between parties of the protocol* | Possibility of public verification of action in a protocol between parties of the protocol |
| | *TTP trust (Trusted Third Party)* | Possibility of public verification of action in a protocol with TTP usage |
| Secure storage | *Secure storage of data* | Confidential and permanent storage of information |
| Freshness | *Data freshness* | Data freshness implies that data is recent, no old massages are replicated |
| | *Key freshness* | Each shared cryptographic key is fresh |

The system conditions, which are described by the security services, can be provided by many different security elements. To obtain appropriate security level we can use different security mechanisms. Some specific mechanisms as well as systematic reviews of the security tools can be found at the literature (Menezes et al. 1997, Anderson 2001, Groves 2001, Pietro et al. 2002, Patel et al. 2002, Chlamtac et al. 2003, Kulesza & Kotulski 2003, Hu & Sharma 2005). In this paper we concentrate on describing conditions for appropriate selection of the countermeasures adequate for a certain level of threats.

## 3 SYSTEM ASSUMPTION

Before we outline the model of scalable security, it is worth describing the system architecture and potential security assumption.

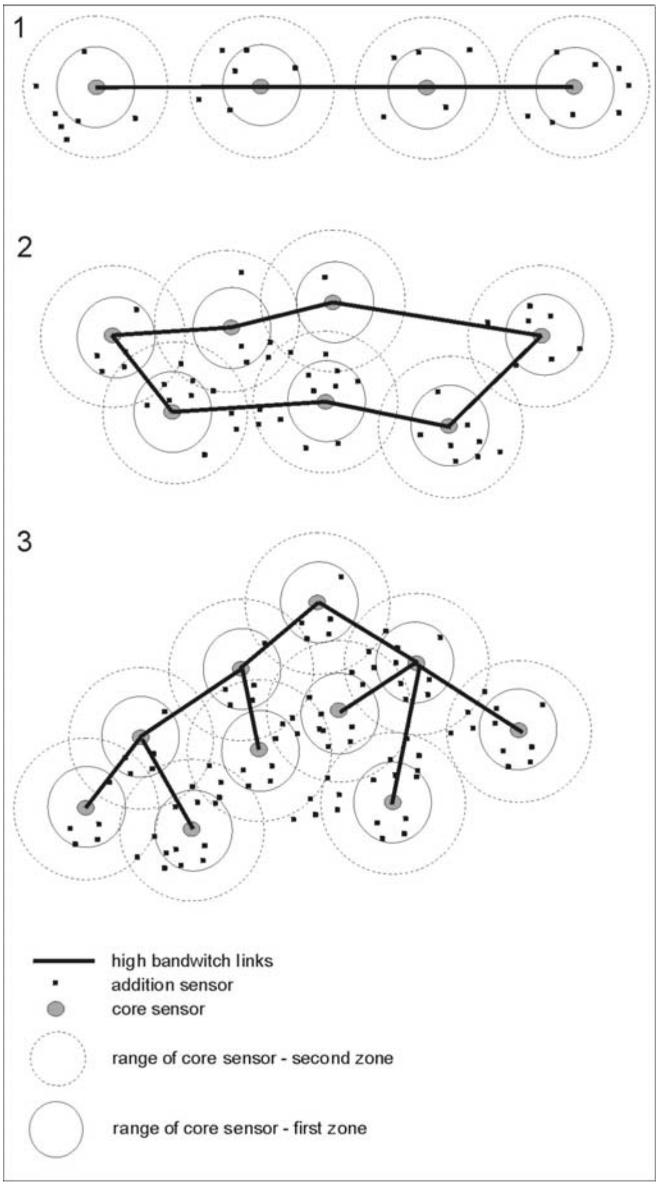
1
2
3
high bandwitch links
addition sensor
core sensor
range of core sensor - second zone
range of core sensor - first zone

Figure 1: System communication architecture.

### *3.1 System architecture*

In this paper we consider a sensor network, which is built of two kinds of sensors: core sensors and additional sensors. The core sensors are constructed of some highly efficient devices, so they can realize all security requirements by using advanced mechanisms of information protection. The devices are linked to each other with high bandwidth network connections by means of which the data can be very fast transported between the core sensors. The core sensors are crucial in our scalable security model of security because they are responsible for the additional sensors' management.

The additional sensors sub-network is based on small devices that have limited communication and calculations possibilities. Especially, they have limited energy storage. An example of such a device that could play a role of the additional sensor is the sensor used in SmartDust (Perrig et al. 2001) program; its basic characteristics are presented in Table 2.

The communication between the additional sensor and the core sensor is performed by means of wireless network, using earlier defined communication (secure) protocols (Feeney 1999, Perrig et al. 2001, 2003).

Table 2: Characteristics of prototype SmartDust nodes

| | |
|---|---|
| CPU | 8-bit, 4 MHz |
| Storage | 8 KB instruction flash |
| | 512 bytes RAM |
| | 512 bytes EEPROM |
| Communication | 916 MHz radio |
| Bandwidth | 10 Kilobits per second |
| Operating System | TunyOS |
| OS code space | 3500 bytes |
| Available code space | 4500 bytes |

In such a network, the system communication architecture can be freely modified, see Figure 1, but firstly, the technical requirements of using communication protocol must be taken into consideration. However, they are out of scope of this paper; we implicitly assume that they give no additional constraints on the security services within cryptographic protocols.

### 3.2 *Security Assumptions*

In this section we specify the possible security services, which can be used at the sensor network. As mentioned above, in our security model one can distinguish two groups of sensors: the core sensors and the additional sensors. The core sensor are considered as highly efficient devices and can run any security services, which can be realized by the whole variety of information protection mechanisms (Menezes et al. 1997, Groves 2001, Patel et al. 2002, Pietro et al. 2002, Kulesza & Kotulski 2003). For the core sensors one can realize any assumptions of information protection defined in a given system.

In the case of very low efficiency of the additional sensors, the limitations on possible security services are very significant. However, using security protocols appropriate for low efficiency sensor networks, see e.g. (Perrig 2001), one can provide such security services as: system availability, authorization of sensors, confidentiality of transmitted information, and freshness and integrity of the measured data.

## 4 MODEL OF SCALABLE SECURITY

A successful realization of an electronic process strongly depends of the proper level of security. During the project phase of the process among others, the security mechanisms are also established. For the sake of security, they are usually overestimated in comparison to real risk. One can notice that even in the same electronic process there are differences in the pieces of information sent, their priorities and values. Thus, they are subjects of different threats, which in the case of successful attack will affect some certain parts of the security protocol. In the case of small threat there is a chance of decreasing some redundant tools of information security, what in effect can improve the system efficiency, data availability and, as a consequence, can increase the system overall security and reduce its costs of operating.

In this paper we present for the sensor network the model of two-stage scalability, containing the scalability of core and additional sensors.

### 4.1 *Core sensors*

Under our assumption of the practically unlimited resources of the core sensors sub-network, its scalability can be fully realized. To describe the level of security of electronic process in such a network we propose the semi-empirical formula, where the security depends on several intuitively interpreted factors. Thus, the security level can be modified by means of the proper choice of the parameters. In the presented conception of scalable security, the protection of information is a scalar quantity, which is a function of three multiplicative components, that is:

$$F_S = \sum_{i}^{a} \sum_{j}^{b} \sum_{x}^{c} (L_{ij}^{x})[\omega_{ij}^{x}(1 - P_{ij}^{x})](\omega_{ij}^{x} L_{ij}^{x})^{Z} \ , \tag{1}$$

where *s* is the security level, which is realized by a given version of protocol; *i* is the number of subprotocols in a given protocol; *j* is the number of steps of parameters in a given subprotocol; *x* is a concrete security service; $\omega_{ij}^{x}$ is the weight describing an average cost of loses after a successful attack for a given service, $\omega_{ij}^{x} \in (0,1)$; $L_{ij}^{x}$ is the value of security elements for a given service, $L_{ij}^{x} \in (0,1)$; $P_{ij}^{x}$ is the probability of an attack on a given service, $P_{ij}^{x} \in (0,1)$; $Z$ is a degree of convergence of security elements, $Z \in (0,25)$.

The three multiplicative factors of the Equation 1 can be interpreted as the essential security elements, namely:

*The protection level:* $L_{ij}^{x}$;

*The risk of attack on a given service:* $[\omega_{ij}^{x}(1-P_{ij}^{x})]$;

*The dependence of security elements:* $(\omega_{ij}^{x}L_{ij}^{x})^{Z}$.

As it is seen, in the Equation 1 every parameter from the above list is calculated for all subprotocols constituting the main protocol and for all steps included in the cryptographic subprotocols.

All these three parameters have a good interpretation based on real functioning of the electronic information system. Their values can be either estimated from behaviour of the operating system and its environment, or calculated under some hypotheses concerning threats and countermeasures.

The first parameter in the Equation 1 is a definition of the protection level for a given cryptographic service in a certain step of the subprotocol. Thus, one can create dependency of possible security elements and define for each of the others the value of the parameter *L*. For every step of the process one can select any security mechanisms. The impact of the mechanism on the security services is defined just by the parameter *L*. The total value of the parameter *L* is a sum such parameters calculated for all chosen security elements, which guarantee sufficient security level of a given service. As we assumed, for the core sensors sub-network all possible security mechanisms can be used for creating the overall security system (Księżopolski &. Kotulski 2005); it is possible due to high efficiency of the core sensors.

The second parameter shows a risk of attack on a given security service. This is a product of average losses caused by a successful attack and a probability of attack on a given security service. The parameter, which is set up for every step of the subprotocols, is the weight for particular services $\omega_{ij}^{x}$. The weight can be changed in particular processes, because the losses due to a successful attack can be different for certain, transported information. The probability of an incident occurrence *P* is defined for all steps described by a given protocol.

The third parameter from the list describes independence of security elements used to gain a proper protection level. The security elements are somehow tied; neglecting some information protection mechanisms in the initial subprotocols strongly influences other subprotocols. The degree of convergence can also be changeable; it depends on e.g. a number of subprotocols, security level.

The security level of electronic processes mainly depends on the used elements of protection of information required by security services.

### 4.2 *Additional sensors*

In the considered sensor network the essential role play the additional sensors. They make possible making measurements in a huge number of spatial points, due to low cost of the sensor devices and easy sensor location. However, application of the scalable security procedure for the additional sensors is strongly constrained by technical conditions. Therefore we propose the new procedure of the security level switching in the scheme, based on the methodology, which uses the cross-validation of the results of measurements obtained, by the core sensors and the additional sensors. We assume that the results obtained from the core sensors are reliable (due to their cryptographic protection sufficient at actual environmental conditions). The measurements obtained from the additional sensors should agree (in a certain sense) with the measurements of corresponding core sensors. To verify this agreement we apply the cross-validation procedure, which should prepared in a way adequate for the concrete structure where the sensors are located. Generally, such a procedure can be planned for an individual core sensor and its surrounding, several core sensors or the whole sensors network.

To describe the scalable security model for the additional sensors sub-network assume that it works with an adequate security level, collecting the measurements. We consider if the level should be changed. The procedure of changing the security level is based on calculation of the difference (the total sum of differences) between the results measured by a core sensor and the analogous result estimated from the measurements of the surrounding additional sensors. This difference can be calculated, at any time *t*, by means of following formula:

$$\Delta(m,t) = \sum_{j=1}^{n} \left| g\left(m_j^{c}(t)\right) - f\left(m_i^{ad}(t), \gamma_{ji}; i = 1,\dots,k\right) \right|, \quad (2)$$

where *t* is the moment of time when the measurement is taken; *j* is the number of core sensor; *i* is the number of additional sensor; $m_j^{c}(t), j = 1,\dots,n$ are the values measured by core sensors; $m_i^{ad}(t), i = 1,\dots,k$ are the values of parameters measured by additional sensors (all at a certain moment $t$); $g_j, j = 1,\dots,n$ are some scaling functions; $f$ is a certain model function that relates results of measurements by additional sensors to the result of measurements by the core sensor $\gamma_{ji} \in [0,1], j = 1,\dots,n, i = 1,\dots,k$ are the weights that define an impact of *i*-th additional sensor on the $j$-th core sensor. In the particular model presented in Figure 1, the value of $\gamma_{ji}$ is equal 1 if the $i$-th additional sensor is the first zone of the $j$-th core sensor, 0.5 if in the second zone, and 0 otherwise (we could also assume some continuous scaling of the ranges of additional sensors).

Equation 2 is a counterpart of the formula, which in statistics makes possible the cross-validation of experimental data (Hildebrand et al. 1977, Stone 1978). In this method some selected data point (a result of measurement) is verified on the basis of the values of other measurements due to application of some regression dependencies. For the cross-verification of the measurements in the sensor networks we can use not only the statistical regression, but also some physical dependencies (formulae) resulting from the known model of the measured engineering structure.

The reasoning in the method is the following. If we observe the agreement of the results, that is the difference is below a certain earlier determined level, we leave the security level unchanged. If the difference excides this level, we increase the required security level for additional sensors and switch on certain security services for the additional sensors network (suspecting an attack on the additional sensors). Then we continue an action according to some alert procedure, deciding whether we observed the attack or some abnormal behaviour of the structure.

Extending the model, we can assume that the level of system standby depends on deviations between estimated and measured values. Along with growing deviation, the system of appropriate additional sensor is set up on a higher threat level. That level controls the security mechanisms used in the network of additional sensor. The defined alarm levels are connected with specified security mechanisms, which fulfil a given process assumptions.

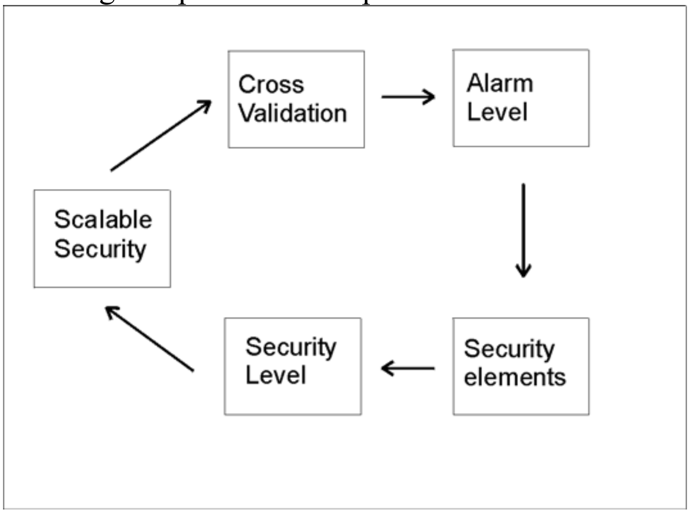

Figure 2: The scalable security cycle for additional sensor

When the additional sensors sub-network increases the protection level, the specified security mechanisms are established. These selected mechanisms will be used to calculate the protection level for the defined group of sensor. Calculation of the additional sensors sub-network protection level is similar to the analogous calculation for the core sensors, to this end it is used in Equation 1. For the additional sensors sub-network it should be created special combination of security mechanisms, which will be adequate to abilities of the used devices. Thus, this combination should be preceded by a detailed analysis.

The mentioned procedures are realized by a cyclical process. Therefore, after defining the protection level, the security level of the core sensors is defined. The described cycle is presented in Figure 2.

To complete the model we assume that in a case of expected threats (some general alert), the security level of the additional sensors sub-network can be increased manually by the operator.

## 5 RISK ANALYSIS

The scalable security for the additional sensors sub-network can be realized as a risk analysis cyclic process (see Figure 3). As mentioned above, the components needed in the risk management process are complex, based on many information protection items (ISO/IEC FDIS 13335-1). The steps in the cyclic process in Figure 3, extended with the scalability mechanism, are the following.

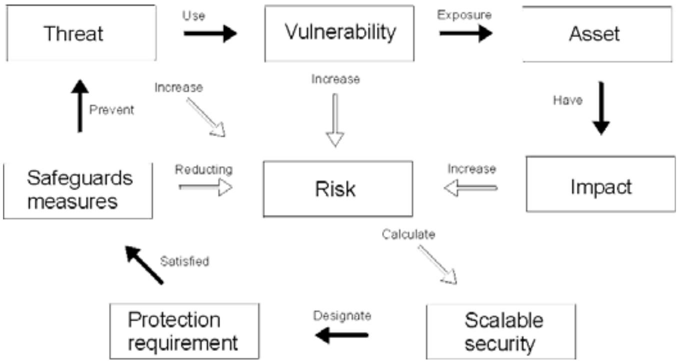

Figure 3: The cycle and relationship of security elements for risk management

### 5.1 *Assets*

The basic step in setting up security process is analysing the organization assets. One has to establish the level of vulnerabilities of assets and on this base one will set up proper security elements.

### 5.2 *Threats*

Potential threats can cause harm on gathered assets by a given organization. The harms can be caused by attack on information taking part in process or on the system. The threats must use vulnerabilities in assets and then can cause some harm. Threats can be divided into human and environmental, and next into deliberate and accidental. For setting up the threats one should define the level of such a threat and calculate the probability of such an incident occurrence.

### 5.3 *Vulnerabilities*

A weakness of an asset that can be exploited by one or more threats is known as Vulnerability. Vulnerabilities associated with assets include weaknesses in the physical layout, organization, procedures, management, hardware, software, information etc. Vulnerability itself does not cause harm but only in the case of an attack.

### 5.4 *Impact*

Impact is the result of some information security incident, caused by a threat, which affects assets. The impact could be a destruction of certain assets, damage security system and compromise of confidentiality, integrity, availability, non-repudiation, authenticity, reliability etc. Possible indirect impact includes financial losses, company image, etc.

### 5.5 *Safeguards*

Safeguards are practices, procedures or mechanisms that may protect against a threat, reduce vulnerability, and reduce the impact of an information security incident.

### 5.6 *Risk*

The risk is characterized by a combination of two factors, the probability of the incident occurring and its impact. Any change to assets, threats, vulnerabilities and safeguards may have significant effects on risk.

### 5.7 *Scalable Security*

Additional item in the risk management process one can attach scalable security (Księżopolski & Kotulski 2005). Every analysis of information protection often shows new vulnerable structures in the system, which causes additional security elements. These protections are often overestimated, what in a general case lowers efficiency, availability of system, and excess redundancy. Thanks to scalable security one can change security level depending on given requirements of the electronic process.

All of the mentioned elements are closely connected and their relationship is precisely presented by standards (NIST 2004, FIPS 140-2, ISO/IEC FDIS 13335-1 ISO/IEC 19790) and analysed in research papers (Patel et al. 2002, Lambrinoudakis et al. 2003, Księżopolski & Kotulski 2005). Consideration on security of systems is a never-ending process. The risk analysis cannot be stopped, because the threats can never be completely eliminated.

## 6 THE MODEL USAGE

The model of scalable security proposed in this paper can be used only if within the sensor network the core sensors sub-network could be created. The core sensors must be linked to each other by high bandwidth connection. As an example of possible application of our model of security in real structure we could consider a bridge along which we can distribute the sensors to measure displacements of the structure as well as other parameters of its functioning. It is obvious that we can find some safe places where the core sensors could be located (and linked to the communication wired or optical fibre system). However, to have more detailed measurements we should also locate sensors in some exposed places (lines, guy ropes, moving elements, etc.). Thus, the additional sensors in our model, which measure densely distributed and very local values of parameters, could be placed in any positions, in particular in the locations where the solid physical connections to the core sensors are difficult or impossible to realize. The number of used additional sensors could reach up even to a couple of thousands (Chlamtac et al. 2003, Hu & Sharma 2005). The reliability of the measurements obtained from the additional sensors verified by the cross-validation procedure with the core sensors according to the methodology described in the above.

## REFERENCE

Anderson, R. 2001. *Security Engineering. A Guide to Building Dependable Distributed Systems*. John Wiley & Sons. New York.

Chlamtac, I., Conti, M. & Liu, J. 2003. Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks* 1: 13-64.

Feeney, L. 1999. A taxonomy for routing protocols in mobile ad hoc networks. *Technical Report T99/07. Swedish Institute of Computer Science.*

FIBS PUB 140-2. Security Requirements for Cryptographic Modules.

Groves, J. 2001. Security for Application Service Providers. *Network Security* 1: 6-9.

Hildebrand, D.K., Laing, J.D. & Rosenthal, H. 1977. *Prediction Analysis of Cross Classifications,* J.Wiley & Sons, New York.

Hu, F. & Sharma, N.K. 2005. Security considerations in ad hoc sensor networks. *Ad Hoc Networks* 3:69-89.

ISO/IEC FDIS 13335-1. Information technology – Security techniques – Concepts and models for managing and planning ICT security.

ISO/IEC 19790. Security techniques – Security requirements for cryptographic modules.

Księżopolski, B. & Kotulski, Z. 2005. On a concept of scaled security: PKI-based model with supporting cryptographic modules, in: J.Wachowicz [ed.]. *Electronic Commerce Theory and Applications* 73-83. Technical co-sponsorship: IEEE, Gdańsk.

Kulesza, K. & Kotulski, Z. 2003. On Automatic Secret Generation and Sharing for Karin-Greene - Hellman Scheme. In Sołdek, J. & Drobiazgiewicz, L. (ed.), *Artificial Intelligence and Security in Computing Systems*: 281-292.

Lambrinoudakis, C., Gritzalis, S., Dridi, F. & Pernul, G. 2003. Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. *Computer Communication* 26: 1873-1883.

Menezes, A. & Oorschot, P. & Vanstone, S. 1997. *Handbook of Applied Cryptography.* Boca Raton: CRC Press.

NIST. 2004. Guide for Mapping Types of Information and Information Systems to Security Categories.

Patel, A., Gladychev, P., Katsikas, S., Gritzalis, S. & Lekkas, D. 2002. Support for Legal Framework and Anonymity in the KEYSTONE Public Key Infrastructure Architecture. *KEYSTONE report.*

Perrig, A., Szewczyk, R., Wen, V., Culler, D. & Tygar, J. 2001. SPINS: security protocols for sensor networks. *Seventh Annual ACM International Conference on Mobile Computing and Networks.* Rome: Italy.

Perrig, A., Hu, Y-C. & Johnson, D. 2003. Efficient security mechanisms for routing protocols. *Proceedings of the 10th Annual Network and Distributed System Security Symposium*.

Pietro, R., Mancini, L.V. & Jajodia, S. 2002. Secure selective exclusion in ad-hoc wireless network., In Ghonaimy, M.A., Mahmoud, T., Heba, E-H. & Aslan, K. (eds.), *Security in Information Society: Vision and Perspective: 423-434.* Boston.

Stone, M. 1978. Cross-Validation: A Review, *Math.Operat.-Forschung Statist., Ser. Statistic*, 9: 127-139.