E-BUSINESS SECURITY DESIGN USING PROCESS SECURITY REQUIREMENTS SEPTET

S. Nachtigal
Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK

Keywords: e-Business, perimeter security, business process–based security, information security requirements.

Abstract: In the e-business environment, the traditional business models for information systems security are no longer appropriate, and fit neither the new organisational environment nor the new organisational security needs. Existing security tools and mechanisms, developed upon the traditional perimeter security paradigm, and based on hardware and software products, are not sufficient since they do not relate to specific parameters that characterise the business process. The modern business environment needs different security approach. Based on such a new approach, which is e-process security design paradigm, a methodology to provide security for an e-business organisation is presented here. The methodology makes use of the newly introduced security requirements septet for e-business process.

1 INTRODUCTION

The business environment has adopted the IT (Information Technology) advances since the very early stages of computer developments. The advanced IT solutions are widely used in business environment both as an infrastructure, supporting the organisation's business and operational activities, and as a means of protecting the organiational assets, especially the information assets.

Although these technological changes have also changed the business mode and the organisational structures as well, the organisational information systems security approach in e-business organisations has not changed since the 1980s, with the introduction of the communication networks into and between the organisations operations. Different types of organisations require different access mode to their information—the academic environment, for example, needs a freely–accessed information environment, while the military environment is an example of quite an opposite, access–blocked information.

This access–blocked solution has been achieved by providing a hard-to-penetrate perimeter, which is still in practice today (Bragg et al., 2004). Perimeter, which is a collection of tools, mechanisms and techniques, is built to protect the organisational internal resources from the external access. The security perimeter is applicable on the organisation's boundaries, so it can protect the organiation from the external world threats.

Tools and mechanisms (such as firewalls, IDSs and IPSs), which are used in perimeter approach network security, are designed to block all malicious contents from entering into the organisational perimeter, but practically these safeguards do allow many types of traffic to pass and actually provide a false sense of security (Andreu, 2006), (Bragg et al., 2004).

Also, the users themselves face problems while using those technology–based solutions in a proper way. Furnell (Furnell, 2005) argues that the technology–based solutions are often used badly. These include bad practice with passwords, poorly maintained anti-virus protection, hardware/software–based or applications-embedded security solutions, irresponsible users, lack of awareness and security misunderstanding (Furnell, 2005).

In e-business mode of doing business all the processes are considered to be e-processes, namely:

- performed electronically by means of information technologies only/mainly;

Nachtigal S. (2007).
E-BUSINESS SECURITY DESIGN USING PROCESS SECURITY REQUIREMENTS SEPTET.
In *Proceedings of the Second International Conference on Security and Cryptography*, pages 408-413
DOI: 10.5220/0002128304080413

- across the whole organisational environment;
- inside and outside organisation's boundaries.

E-business organisation performs its business activities by means of e-processes, based on Internet infrastructure and technologies.

The uniqueness in running an e-business is in its 'openness' to the environment, which is achieved by means of the various connections and communication channels with the external world. Although this 'openness' makes the e-business mode of doing business much more dangerous than the traditional way, it is essential. The whole business is dependent on proper business processes execution, which are performed mostly by technological means, with end-user (customers, company's employees, company's suppliers' employees, etc.) involvement. Therefore, the security issue becomes one of the most (if not the most) important issues for e-business organisation.

The e-business security perception changes from 'blocking' and 'preventing' in the traditional business to 'opening' and 'enabling' the modern e-process. The e-business process–based security paradigm (Nachtigal and Mitchell, 2006) provides a possibility to secure the modern e-business organisations.

This paper presents a newly introduced set (septet) of e-business security requirements, as a part of a newly suggested process-based security paradigm, which is an alternative for perimeter security approach. Also, the way of this security requirements septet implementation is demonstrated in this paper.

The remainder of this paper is structured as follows: after the principles of the process-based security paradigm are presented in the next section, the seven e-business security criteria are described and discussed in section three, followed by the description of their implementation in section four, related works discussion (section five) and conclusions.

2 THE PRINCIPLES OF E-BUSINESS PROCESS SECURITY PARADIGM

The basis for that approach is the assumption that for e-business to exist its processes must be secured. Hence, the security safeguards design will be differentiated between business processes according to their specific characteristics. The process–based security approach (Nachtigal and Mitchell, 2006) includes the following key elements:

- the security is designed and provided for each single e-process;
- e-process design is considered to be a result of two different aspects elements:
  - business logic definition;
  - information flows transportation and exchange
- the two aspects elements are analysed and security mechanisms and tools are designed according to their security requirements criteria.

2.1 e-Business Security Criteria

The three commonly accepted (Gollman, 2003), (Harris, 2003), (Tettero, 2000), (Moffett et al., 2004) generic security criteria, or security objectives, are:

- confidentiality;
- integrity;
- availability.

These three security requirements, according to Tettero (Tettero, 2000) and Harris (Harris, 2003), come to ensure the following:

- ***confidentiality***—to obtain secrecy and to prevent unauthorized disclosure of information and data to unauthorised person;
- ***integrity*** is achieved when data and information are correct and appropriate as meant by the process designer (and can not be modified by unauthorised person), and accuracy and reliability of information and systems are in place;
- ***availability*** comes to say that data, information and other elements of information systems are accessible and useable upon the demand of authorised user.

Following the process–based security approach in the e-business environment, these three security objectives are not sufficient. The modern business environment is mostly characterised by its connectivity, which was not the case for the traditional type organisations. The security requirements triad described above fits the traditional business environment. In order to provide the required security for an e-business organisation, additional security requirements have to be in place. According to this research perception, the e-business security is associated with its e-process security. Hence, these additional security requirements have to be considered and provided for e-processes, namely—additional security requirements are needed to ensure that business logic and information flows will be secure. That conclusion, which is one of this research statements, is based on a detailed analysis of the e-business organisation nature and operations, and its e-processes analysis and characteristics.

Based on that analysis, the following set of seven security requirements is suggested to provide security for the e-business information systems:

1. in order to ensure privacy and non-disclosure of the contents (both of the companies and the customers) the ***confidentiality*** (***C***) objective has to be achieved;
2. in order to ensure that data, information and actions (performed by information technology, namely—software) will not be modified by unauthorised users and/or means and/or technology, the ***integrity*** (***I***) objective has to be achieved;
3. on order to ensure that the whole system (with all relevant elements of technology managed according to specific strategy and policy) will be accessible and capable to execute the process, the ***availability*** (***A***) objective has to be achieved;
4. a new security objective for business logic security is suggested here—***robustness*** (***R***)— for correct performing of the business logic;
5. an additional new security objective for business logic security is suggested here—***resistivity*** (***R***)— to ensure that the business logic is checked against possible logic-based abuse and it is designed in such a way that it will resist the various possible abuse attempts that have a possibility to cause harm to the e-business information systems;
6. a new security objective of ***compliance*** (***C***) is suggested here to ensure that an e-process is able to interact with other companies' e-processes; the security objective of ***compliance*** is needed also to ensure that the process security design is compliant with security regulations, standards and laws;
7. in order to make possible to manage the e-business process security, to track actions, to keep metrics for security planning and design an objective of ***accountability*** (***A***) is needed.

To conclude, the e-business process security objectives suggested by this research are:

1. Confidentiality (***C***);
2. Integrity (***I***);
3. Availability (***A***);
4. Robustness (***R***);
5. Resistivity (***R***);
6. Compliancy (***C***);
7. Accountability (***A***).

That seven security objectives set (septet)—***CIARRCA*** or $\boldsymbol{I}(RCA)^2$— makes possible to meet the e-business process security requirements covering all the relevant aspects, as described above.

In order to ensure that the security objectives septet $\boldsymbol{I}(RCA)^2$ will be indeed achieved, the development and design of any e-process should be performed in a systematic way—methodology—where all the relevant security requirements issues will be considered, following process-based approach and focusing on security objectives.

3 SECURITY OBJECTIVES ANALYSIS

The security requirements analysis is actually the practical realisation of the business process–based paradigm. This analysis needs to be performed separately for the business logic and for the information flows of the process.

3.1 Business Logic Security Objectives Analysis

Here we have to check the business logic in regard with the business logic security objectives, which are Robustness, Resistivity and Compliance. These objectives come to ensure that the e-business logic is correctly defined in such a way that it is workable, compliant with all the relevant standards and laws, and does not make possible for users and processes—both authorised and unauthorised—to abuse the logic and to compromise the process and/or its outcomes in any way. Here the business rules are analysed in respect with the e-process interactions and interfaces with other processes, contacts between the participants' elements (users, customers, databases), access rules and policies, possible conflicts, previously reported business logic flaws. Also, the compliance with security standards and ability to comply with other companies' e-processes rules and policies are analysed.

The business logic security (BizLogic security) should be established, based on the security objectives RRC analyses. Practically, that will start with the threat-source modeling for ***each one of the BizLogic security objectives (RRC) for each one of the processes***. The results of this threat-source analysis (which can be presented as shown in table 1 for each of the RRC objectives)) pave the way for the next analysis steps.

The final purpose of the BizLogic analyses is to establish a set of security means for the organisation's business logic by achieving the RRC (Robustness, Resistivity, Compliance) business security objectives. These will be based on findings of the threat-source analysis and summarised separately for each objective, as presented by Table 2, for example.

Table 1: Process 1: Robustness/Resistivity/Compliance analysis.

Threat analysis	Threat-source		
Possible attacks	1	..	N
Potential damage			
Security design			

Table 2: Process 1:
Business logic security—Robustness/Resistivity/Compliance criteria summary.

Security measures	**Robustness (R)**
Standards	list of security mechanisms
Legal issues	”
Policies	”
Procedures	”
Unique requirements	”

As a result of these steps, performed for each single e-process separately, the security tools and mechanisms of e-business logic will be established. On a conceptual level, this set could be presented by Table 3 below.

Table 3: Single process Business Logic security means.

Security objectives	Processes		
Robustness	1	..	N
Resistivity			
Compliance			
Accountability			

3.2 Information Flow Security Analysis

The process is decomposed into information flows, and the security analysis is performed separately for each of these information flows in regard with the relevant security requirements.

Information Flows, as being an element of an e-process, are presented by the following characteristics:

- content—structured (specific sequence of data fields) or unstructured (natural language);
- participants' elements—classified as
  – active—companies' employees, private customers;
  – passive—databases, services providers (systems administrator, network manager, programmers, ISP's employees);
- origin—one of the participants, either active or passive;
- destination—one of the participants, either active or passive;
- execution means—technology (software, hardware, communication).

Actually, there is an interaction between participants, origin and destination: the 'participant' feature includes both the 'origin' and the 'destination' features—'origin'/'destination' is usually a customer, or employee, or another process. In case of another process, the interaction between a specific information flow of the e-process under discussion and between another process (practically meaning an information flow of another process) is realised through a database, which is, again, one of the participants in this model. Hence, the information flows features are the following:

- content;
- participants;
- execution means.

According to this research approach, all these information flow characteristics need to be identified and discussed in regard with Information Flows security objectives—the CIA (Confidentiality, Integrity, Availability) objectives. Each of these security objectives should be ranked according to degree of its criticality related to a specific Information Flow. The ranks will be presented by Table 4 below.

Table 4: CIA Criticality Rank.

Item	**Confidentiality (C)**	**Integrity (I)**	**Availability (A)**	**Total score**
InfoFlow 1	r1	r2	r3	sum of row ranks
InfoFlow 2	r4	r5	r5	sum of row ranks
...				
...				
InfoFlow n				
Total security objective rank				

These ranks will be related to and expressed in terms of threat modeling (such as suggested by Swidersky and Snyder (Swiderski and Snyder, 2004)) and risk analysis. The results for each information flow will be presented by Table 5.

Table 5: Information Flow security analysis.

Item	Description	Threat modeling	Risk analysis
Content	data fields/text		
Employee			
Customer			
Database			
Sys Admin			
Net Man			
Programmer			
ISP			

Practically, the threat modeling and analysis need to be performed for each and every information flow separately.

Based on these analysis tables the following security applications might be developed:

- security patterns for specific types of information flow in a specific given environment;
- access/performance rights rule as a function of a specific information flow, security threats, security risks.

Again, the purpose of the analysis, presented by Table 5, is to produce sufficient information for analysing the information flows security objectives in terms of ***CIAA***. Hence, an additional table (Table 6, see page 6) is suggested as a tool for analysing information flows security objectives.

3.3 The Septet Methodology Application in a Case Study

The suggested e-business security requirements septet has been tested by applying it in a real life situation. For that purpose a big airline company was chosen as one of this research case studies. The case study company operates an e-business activity for purchasing flight tickets and vacations by their customers.

The septet has been applied as an alternative method to design the company's e-business information systems security. The application analysis (which is still in progress) includes also a comparative study of the practicality and efficiency between the suggested methodology and the traditional ways of information systems security design.

4 RELATED WORK

Not many research works on business security issues, related to security requirements, are published, and just few of them are related to e-business process specifically. However, there is a range of suggested approaches.

Table 6: Information Flow security analysis.

Item	Confidentiality (C)	Integrity (I)	Availability (A)	Accountability (A)
Content	security mechanisms	security mechanisms	security mechanisms	security mechanisms
Employee				
Customer				
Database				
Sys Admin				
Net Man				
Programmer				
ISP				
:				

Herrmann and Pernul (Herrmann and Pernul, 1999) suggest a framework that supports business-process re-engineering in order to improve security and integrity. A three layered architecture is suggested for business process specification, while 'security' and 'integrity' are considered as two separated requirements.

Jones et al. (Jones et al., 2000) consider e-business important requirements in terms of trust and dependability as related to business partners.

Bodin et al. (Bodin et al., 2005) suggest a method for the optimal allocation of a budget for maintaining and enhancing the security of an organizations information system by using the ratings of the Confidentiality, Data integrity and Availability criteria, while the availability criterion is broken down into three subcriteria: Authentication (of the right users), Non-repudiation (a user cannot deny using the system, if in fact he or she did actually use it), and Accessibility or non-denial of service.

TROPOS methodology, which is a specification language for modelling early requirements for software developers (Giorgini et al., 2005), (Susi et al., 2005), is suggested also to be used for security requirements models design (Massaccia et al., 2005), (Susi et al., 2005). This methodology may be useful in the advanced phases of security design and development, namely the phase of applications/software development for business tasks.

5 CONCLUSION

The newly suggested septet of e-business process security requirements $\boldsymbol{I}(RCA)^2$ (Confidentiality, Integrity, Availability, Robustness, Resistivity, Compliance, Accountability) provides a practical way of designing the e-business security safeguards in terms of policies, standards, mechanisms and tools. Using this requirements septet on a single process basis, makes possible to provide the differentiated and realistic security design for separated functional domains, while taking in account the real functional and business needs.

REFERENCES

Andreu, A. (2006). *Professional Pen testing for web applications*. Wiley Publishing, Inc.

Bodin, L., Gordon, L., and Loeb, M. (2005). Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM archive*, 48:78 – 83.

Bragg, R., Phodes-Ousley, M., and Strassberg, K. (2004). *Network Security: The Complete Reference*. McGraw-Hill/Osborne.

Furnell, S. (2005)). Why users cannot use security. *Computers & Security*, 24:274–279.

Giorgini, P., Mylopoulos, J., and Sebastiani, R. (2005). Goal-oriented requirements analysis and reasoning in the tropos methodology. *Engineering Applications of Artificial Intelligence*, 18:159–171.

Gollman, D. (2003). *Computer Security*. John Wiley & Sons.

Harris, S. (2003). *CISSP All-In-One Exam Guide*. McGraw-Hill/Osborne Media, second edition.

Herrmann, G. and Pernul, G. (1999)). Viewing business-process security from different perspectives. *International Journal of Electronic Commerce*, 3(3):89–103.

Jones, S., Wilikens, M., Morris, P., and Nasera, M. (2000)). Trust requirements in e-business. *COMMUNICATIONS OF THE ACM*, 43(12):81–87.

Massaccia, F., Prestb, M., and Zannone, N. (2005). Using a security requirements engineering methodology in practice: The compliance with the italian data protection legislation. *Computer Standards & Interfaces*, 27:445–455.

Moffett, J. D., Halley, C. B., and Nuseibeh, B. (2004). Core security rewuirements artefacts. ISSN 1744-1986 2004/23, Departmenet of Computing, Faculty of Mathematics and Computing, The Open University, Walton Hall, Milton Keynes, MK7 6AA, UK.

Nachtigal, S. and Mitchell, C. (2006). Modelling e-business security using business processes. In *ICETE 2006 - International Joint Conference on E-Business and Telecommunications, SECRYPT*. INSTICC.

Susi, A., Perini, A., and Mylopoulos, J. (2005). The tropos metamodel and its use. *Informatica*, 29:401–408.

Swiderski, F. and Snyder, W. (2004). *Threat Modeling*. Microsoft Press.

Tettero, O. (2000). *Intrinsic Information Security. Embedding Security Issues in the Design Process of Telematicd Systems*. Telematica Instituut Fundamental Research Series, No. 006(TI/FRS/006).