IDENTIFYING SECURITY ELEMENTS FOR COOPERATIVE INFORMATION SYSTEMS

Nathalie Dagorn
Laboratory of Algorithmics, Cryptology and Security (LACS), 6 rue Richard Coudenhove-Kalergi, L-1359, Luxembourg
& ICN Business School, 13 rue Maréchal Ney, F-54000 Nancy, France

Keywords: Cooperation, Cooperative information system, Inter-organizational system, IOS, Security.

Abstract: This paper tackles security issues for cooperative information systems (CIS) by first identifying the major security requirements for this particular type of information systems, and then discussing the security techniques usually implemented to address these requirements as well as their limitations.

1 INTRODUCTION

Today, information systems overlap the organizational boundaries. For many organizations, the intra-organizational integration phase is complete (or is going well). In order to access new markets or to benefit from synergy effects enabling to reduce the costs, some organizations choose to merge with other powerful actors of their sector, to ally with partners or even with competitors. More and more activities of the organization also depend on activities realized outside its boundaries. Organizations thus turn now to an inter-organizational cooperation phase, for which many benefits in terms of effectiveness are expected. In this context, *cooperative information systems (CIS)* refer to any information system allowing an organization to cooperate in a usual way with one or more partner organizations such as suppliers, clients, subsidiaries of the group, etc.

In this paper, we tackle security issues for CIS: we first identify the major security requirements for this particular type of information systems, and then discuss the security techniques usually implemented (mastered or not) as well as their limitations.

The paper is structured as follows: Section 2 introduces the context and motivation of our research. Section 3 determines security requirements for twelve CIS identified as representative in previous work. Section 4 synthesizes the security techniques usually implemented to satisfy these requirements and outlines their limitations with respect to the specificities of CIS. Section 5 summarizes the paper results and sketches some directions for future work.

2 CONTEXT AND MOTIVATION OF OUR RESEARCH

On the one hand, CIS have been classified and analyzed during the last twelve years according to theoretical, structural, functional and economical perspectives (Dagorn, 2009 recapitulates these proposals). Some innovative work appears nowadays around concepts such as inter-organizational process efficiency (Saeed et al., 2005), inter-organizational performance (Straub et al., 2004; Bharadwaj et al., 2007), inter-organizational competitive dynamics (Chi et al., 2007), inter-organizational knowledge sharing (Apostolou et al., 2008), etc. But security issues often remain insufficiently considered, and these proposals seem to be inadequately or too weakly supported by existing security frameworks on the technical level.

On the other hand, at the heart of our subject, networked enterprises need CIS able to manage critical and/or large amounts of information in possibly heterogeneous technological environments and computing services. Thus, security requirements between partners are also of major importance on the organizational level: What information will the partners have access to in the CIS? Is confidentiality of transactions ensured…? These issues must be addressed before implementing a CIS. Security

Dagorn N. (2009).
IDENTIFYING SECURITY ELEMENTS FOR COOPERATIVE INFORMATION SYSTEMS.
In *Proceedings of the International Conference on Security and Cryptography*, pages 319-324
DOI: 10.5220/0002232403190324

issues affect all kinds of CIS and all cooperation levels. For a future partner, the first problem is to know the nature of information it will have to share with the other organizations using the CIS. This concern is particularly relevant for electronic marketplaces, where confidentiality of information transmitted through the CIS is a critical issue. Moreover, even if rules for information access and sharing were defined and accepted by all the partners, an intrusion into the CIS remains possible, which might reveal useful information to competitors (prices, etc.).

This is why we aim to identify some security elements (requirements, protection mechanisms, open questions) for CIS in the next sections.

3 SECURITY REQUIREMENTS

In previous work (Dagorn, 2009), we proposed an innovative taxonomy of CIS based on the task-technology fit theory, which distinguishes between five main tasks supported by the CIS (document exchange, integration of information flows, standard business transactions, online or standard resource sharing, online transactions) and associated technology (Electronic Document Management - EDM-, integrative, standard or Web technology). This stucture is kept in this section to analyze the security requirements of the CIS identified. In this section as well as in the next one, we assume that two organizations A and B cooperate using a CIS.

3.1 Security Requirements for the CIS Identified

3.1.1 CIS Based on EDM Technology

XML Document Systems. A and B cooperate by exchanging XML messages or documents. The exchange network can be private or public. To ensure security, Ekelhart et al. (2008) recommend to:

- Secure the partners A and B in matter of access to the common network in order to authorize XML messages only
- If critical/confidential data is exchanged, secure data in transit
- If a public network such as the Internet is used, implement secure exchange protocols.

Workflow Document Systems. A cooperates with B by respectively connecting to the workflow application to edit, modify, create, view, delete a document. To ensure security, Wainer et al. (2003), Mortgage Banking (2008) recommend to:

- Secure A and B
- Secure the workflow application
- If another application is used to exchange files, secure this application
- Secure the server access hosting the workflow application
- If a Web interface is used, secure the Web site
- If a database is used, secure the database
- If critical/confidential data is exchanged, secure data in transit
- If a public network is used, implement secure exchange protocols.

3.1.2 CIS Based on Integrative Technology

Electronic Data Interchange (EDI) Systems. A and B cooperate by exchanging messages called transactions. Those are transmitted either through a private or a public network such as the Internet. From the security viewpoint, the EDI system itself is not intrusive (since A does not access directly B's data or applications). Narayanan et al. (2009) recommend to:

- Secure A and B in matter of access to the common network in order to authorize EDI messages only
- Secure the EDI application
- If critical/confidential data is exchanged, secure data in transit
- If a public network is used, implement secure exchange protocols.

Enterprise Application Integration (EAI) Systems. A cooperates with B using EAI-interfaced information systems. To ensure security, Izza (2009) recommends to:

- Secure A and B
- Secure A and B's interfaced applications
- Secure the server where the operations are performed as well as its access
- If a database is used, secure the database
- If critical/confidential data is exchanged, secure data in transit
- If a public network is used, implement secure exchange protocols.

3.1.3 CIS Based on Standard Technology

Proprietary Applications. A and B cooperate in a client-server mode. If B wants to access data from A, the client application must be installed by B to enable the connection to A's server. To ensure security, Wortman (2008) recommends to:

- Secure A and B
- Secure the proprietary application (in general, made by the provider)
- If a database is used, secure the database
- If critical/confidential data is exchanged, secure data in transit
- If a public network is used, implement secure exchange protocols.

Enterprise Resource Planning (ERP) Systems. A cooperates with B by allowing their respective ERP applications to exchange information through a public or private network. To ensure security, Allen (2008) recommends to:

- Secure A and B;
- Secure A and B's ERP applications
- Secure the server access that hosts the ERP system
- If a database is used, secure the database
- If critical/confidential data is exchanged, secure data in transit
- If a public network is used, implement secure exchange protocols.

3.1.4 CIS Based on Standard or Web Technology

Groupware. A cooperates with B using a groupware. Since all cooperation situations cannot be analyzed here, only generic guidelines (best practices) to ensure security are proposed (Briguet, 2009; Menold, 2009):

- Secure A and B
- If applications are used to exchange files, secure these applications
- If a Web architecture is used, secure the Web site and its access
- If the organizations need to connect to a server to put files to be shared, secure access to this server
- If a database is used, secure the database
- If critical/confidential data is exchanged, secure data in transit
- If a public network is used, implement secure exchange protocols.

Grid/Cloud Computing. A and B are elements of the grid/cloud. Cooperation data is shared across the grid/cloud. To ensure security, Demchenko et al. (2008), Mansfield-Devine (2008), Smith et al. (2009) recommend to:

- Secure A and B
- Secure the grid/cloud application
- Secure the server where the operations are performed as well as its access
- Secure the database
- If critical/confidential data is exchanged, secure data in transit
- If a public network is used, implement secure exchange protocols.

Workflow Transactional Systems. A cooperates with B using a workflow system, which manages the correct sequence of the tasks achieved by A and B, and performs automated processes. Various tasks can be achieved, from the use of specific applications to the generation of files or messages in a predefined format (XML, EDI, etc.), or even the update of a database. To ensure security, Cao et al. (2009) recommend to:

- Secure A and B
- Secure the server access that hosts the workflow application
- If another application is used to exchange files, secure this application
- If a database is used, secure the database
- If critical/confidential data is exchanged, secure data in transit
- If a public network is used, implement secure exchange protocols.

3.1.5 CIS Based on Web Technology

Web Applications. A and B use the same Web application to cooperate; they access it through an authentication system. To ensure security, Whittaker and Andrews (2006), Waters (2009) recommend to:

- Secure A and B
- Secure the Web application
- Secure the Web server and its access
- If a database is shared, secure the database
- If critical/confidential data is exchanged, secure data in transit
- Implement secure exchange protocols.

Online Markets. The CIS is a Web site, which partners (customer, seller) connect to. It stores cooperation data and uses applications and/or databases to manage it. To ensure security, Malik and Bouguettaya (2005), Khosrow (2008), Lin and Liu (2009), Tsung-Yi et al. (2009) recommend to:

- Secure the invoked applications
- Secure access to the Web server of the site
- Secure the Web Site
- Secure the back-office database(s)
- Secure data in transit
- Implement secure exchange protocols.

Table 1. Security requirements for the twelve CIS identified in the taxonomy.

Techno-logical environ.	CIS	Secure A and B	Secure applica-tion	Secure server access	Secure Web site or server	Secure database	Secure data during transfer	Secure exchange protocols
EDM-based	XML document system	×					× if critical	× if public network
	Workflow document system	×	×	×	×	× if used	× if critical	× if public network
Inte-grative	EDI	×	×				× if critical	× if public network
	EAI	×	×	×	×	× if used	× if critical	× if public network
Stan-dard	Proprietary application	×	×			× if used	× if critical	× if public network
	ERP	×	×	×		× if used	× if critical	× if public network
Stan-dard or Web	Groupware	×	×	× if used	× if used	× if used	× if critical	× if public network
	Grid/cloud computing	×	×	×	×	×	× if critical	× if public network
	Workflow transactional system	×	× if used	×		× if used	× if critical	× if public network
Web	**Web application**	×	×	×	×	× **if used**	× **if critical**	×
	Online markets		×	×	×	×	× **if critical**	×
	XML-based Web services	×	×	×	×	×	× **if critical**	×

Web Services. A and B cooperate by invoking services on the Web (regardless of the platform type). To ensure security, Cook et al. (2006), Whittaker and Andrews (2006), Periorellis (2007) recommend to:

- Secure A and B
- Security the invoked applications
- Secure access to the Web server hosting the services
- Secure the Web site
- Secure the back-office database
- If critical/confidential data is exchanged, secure data in transit
- Implement secure exchange protocols.

3.2 Synthesis

The main security requirements related to the CIS identified are summarized in Table 1. The table shows that CIS operating in heterogeneous environments have generally higher security requirements than CIS operating in homogeneous environments. The most attention should be paid to CIS developed with Web technology (in the lowest part of the table). The security techniques usually implemented to meet these requirements are discussed in the following section.

4 SECURITY PROTECTIONS

To prevent or counter security attacks on traditional information systems, many hardware devices and software may be deployed by the organizations, for instance the use of a firewall, a demilitarized zone (DMZ), a proxy, an antivirus solution or an intrusion detection/prevention system (IDS/IPS). Some additional techniques like cryptography, biometry or steganography can be employed complementarily. Many generic books on computer security are available (e.g., Anderson, 2001; Cheswick et al., 2003; Lehtinen, 2006), and the reader may refer to them for more details on the mentioned mechanisms. Thus, only the (logical) techniques meeting the security requirements identified in previous section are developed here.

4.1 Usual Security Techniques

Securing A and B. The following techniques may be implemented:

- Deploy a firewall to filter network traffic to the server (block telnet/ftp access)
- Implement a routing policy between the partners (e.g., route the network traffic from the partner to the DMZ and not to the local area network -LAN)
- Implement authentication mechanisms based on a trust relationship between Windows domains
- Install a leased line dedicated to cooperation operations between the organizations (always preferable than using the Internet network).

Securing the Application. This may be enabled by:

- Developing the application with secure coding techniques (Howard and LeBlanc, 2001; Graff and Van Wyk, 2003)
- Authenticating users when the application is launched (credentials).

Securing the Server Access. The following techniques may be implemented:

- Restrict the server access to certain users (authentication)
- Administrate user rights (group management, read/write/execute permission)
- Deploy a public key infrastructure (PKI).

Securing the Web Site or Server. This may be achieved in particular through:

- Restricting the server access to certain users (authentication)
- Setting security parameters for the HTTP server (disallow directory traversal, disable scripts where possible, etc.)
- Restricting the services provided by the server (disable ftp/telnet services, etc.)
- Deploying a firewall to filter network traffic to the server (allow only HTTP traffic for port 80, etc.)
- Implementing a DMZ to install the server.

Securing the Database. The following techniques may be employed:

- Implement authentication mechanisms
- Manage user rights to access data based on user groups
- Encrypt data.

Securing Data in Transit. This may be achieved by the use of cryptographic and network management techniques like:

- Data encryption
- Use of IPSec (protocol suite intended to secure IP communications by adding authentication and/or encryption layers for each IP packet; IPSec includes protocols to create cryptographic keys)
- Streaming of content available only to holders of a valid group key (e.g., multicast video streaming).

Implementing Secure Exchange Protocols. According to the type of exchange, it is recommended to:

- Use secure versions of protocols (e.g., HTTPS based on SSL, which provides security features to the HTTP protocol)
- Use SSL, SET, 3D Secure (Visa) or SPA/UCAF (Mastercard) for electronic commerce
- Use IPSec for the encryption of IP data packets.

4.2 Limitations and Issues to Solve

The security techniques developed in this section are, for most, individually well mastered today. However, they are generic, do not take into account the specificities of CIS, and are usually implemented as needed without a cooperation rationale. Hence, security vulnerabilities may persist in the organization's trust architecture. Since it is not relevant to create security techniques and tools specific to CIS, but assuming that future information systems will inevitably go towards greater openness and interoperability (Fenoulière, 2004), we recommend integrating some of these security techniques in a framework specific to CIS in order to adapt their features to an inter-organizational cooperation context.

5 CONCLUSIONS AND FUTURE WORK

Taking into account the latest technological developments and issues in the area of CIS, our research shows in particular that most inter-organizational cooperative activities take place today via the Web, and that this practice raises major security issues for the CIS. Therefore, security issues were emphasized by analyzing the security requirements of each CIS identified, and highlighting the limitations of the security techniques usually implemented to address these issues.

A questionnaire survey conducted with ten leading French companies of the sectors of industry, research, banking and insurance, engaged in one or more inter-organizational cooperation processes, confirmed the trend of Web cooperation, the growing issue of Web security, as well as the recent efforts of the organizations to manage their security (through technical protections, security policies that mainly conform to ISO standards, security budget, etc.). It also confirmed our assumption that more security techniques should be implemented when the technological environment of the CIS is heterogeneous (Dagorn, 2008). Finally, the security requirements and techniques proposed in this paper were validated for each CIS by the concerned organizations.

To complete this research, our ongoing work in this area consists in establishing a security model for CIS, and deriving a security framework for CIS including some of the security techniques described in Section 4.

REFERENCES

Allen, V., 2008. ERP Security Tools. In *Internal Auditor*, Vol. 65 Issue 1, p25-27.

Anderson, R., 2001. *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons. http://www.cl.cam.ac.uk/~rja14/book.html.

Apostolou, D., Mentzas, G., Klein, B., Abecker, A., Maass, W., 2008. Interorganizational knowledge exchanges. In *IEEE Intelligent Systems*, Vol. 23 Issue 4, p65-74.

Bharadwaj, S., Bharadwaj, A., Bendoly, E., 2007. The performance effects of complementarities between information systems, marketing, manufacturing, and supply chain processes. In *Information Systems Research*, Vol. 18 Issue 4, p437-453.

Briguet, C., 2009. Building a Secure Collaborative Infrastructure. In *ECN: Electronic Component News*, Vol. 53 Issue 2, p27-29.

Cao, J., Chen, J., Zhao, H., Li, M., 2009. A policy-based authorization model for workflow-enabled dynamic process management. In *Journal of Network & Computer Applications*, Vol. 32 Issue 2, p412-422.

Cheswick, W.R., Bellovin, S.M., Rubin, A.D., 2003. *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley Professional. 2nd edition.

Chi, L., Holsapple, C.W., Srinivasan, C., 2007. Competitive dynamics in electronic networks: a model and the case of interorganizational systems. In *International Journal of Electronic Commerce*, Vol. 11 Issue 3, p37-49.

Cook, N., Robinson, P., Shrivastava, S.K., 2006. Design and Implementation of Web Services Middleware to Support Fair Non-Repudiable Interactions. In *International Journal of Cooperative Information Systems*, Vol. 15 Issue 4, p565-597.

Dagorn, N., 2008. Politiques en matière de sécurité des systèmes d'information inter-organisationnels: une enquête dans dix grandes entreprises. In *Systèmes d'Information et Management*, Vol. 13 Issue 2, p97-125.

Dagorn, N., 2009. Sécurité des systèmes d'information coopératifs. *PhD Dissertation*, Nancy-Université, September (to appear).

Demchenko, Y., Mulmo, O., Gommans, L., de Laat, C., Wan, A., 2008. Dynamic security context management in Grid-based applications. In *Future Generation Computer Systems*, Vol. 24 Issue 5, p434-441.

Ekelhart, A., Fenz, S., Goluch, G., Steinkellner, M., Weippl, E., 2008. XML security: A comparative literature review. In *Journal of Systems & Software*, Vol. 81 Issue 10, p1715-1724.

Fenoulière, P., 2004. *Vers une informatique ouverte : enjeux et infrastructures*, Hermes Science Publications. Paris.

Graff, M.G., Van Wyk, K.R., 2003. *Secure Coding: Principles and Practices*, O'Reilly Media.

Howard, M., LeBlanc, D., 2001. *Writing Secure Code*, Microsoft Press.

Izza, S., 2009. Integration of industrial information systems: from syntactic to semantic integration approaches. In *Enterprise Information Systems*, Vol. 3 Issue 1, p1-57.

Khosrow, M., 2008. *Web Technologies for Commerce and Services Online*, Information Science Reference. Hershey, PA.

Lehtinen, R., 2006. *Computer Security Basics*, O'Reilly Media. Sebastopol, CA, 2nd edition.

Lin, S.-J., Liu, D.-C., 2009. An incentive-based electronic payment scheme for digital content transactions over the Internet. In *Journal of Network & Computer Applications*, Vol. 32 Issue 3, p589-598.

Malik, Z., Bouguettaya, A., 2005. Preserving trade secrets between competitors in b2b interactions. In *International Journal of Cooperative Information Systems*, Vol.14 Issue 2-3, p265-297.

Mansfield-Devine, S., 2008. Danger in the clouds. In *Network Security*, Vol. 2008 Issue 12, p9-11.

Menold, N., 2009. How to Use Information Technology for Cooperative Work: Development of Shared Technological Frames. In *Computer Supported Cooperative Work (CSCW)*, Vol. 18 Issue 1, p47-81.

Mortgage Banking, 2008. Elements of a Successful Platform. In *Mortgage Banking*, Vol. 69 Issue 3, p71.

Narayanan, S., Marucheck, A.S., Handfield, R.B, 2009. Electronic Data Interchange: Research Review and Future Directions. In *Decision Sciences*, Vol. 40 Issue 1, p121-163.

Periorellis, P., 2007. *Securing Web Services: Practical Usage of Standards and Specifications*, Information Science Reference. Hershey, PA.

Saeed, K.A., Malhotra, M.K., Grover, V., 2005. Examining the impact of interorganizational systems on process efficiency and sourcing leverage in buyer-supplier dyads. In *Decision Sciences*, Vol. 36 Issue 3, p365-396.

Smith, M., Schmidt, M., Fallenbeck, N., Dörnemann, T., Schridde, C., Freisleben, B., 2009. Secure on-demand grid computing. In *Future Generation Computer Systems*, Vol. 25 Issue 3, p315-325.

Straub, D., Rai, A., Klein, R., 2004. Measuring firm performance at the network level: a nomology of the business impact of digital supply networks. In *Journal of Management Information Systems*, Vol. 21 Issue 1, p83-114.

Tsung-Yi, C., Yuh-Min, C., Chin-Bin, W., Hui-Chuan, C., 2009. Flexible authorisation in dynamic e-business environments using an organisation structure-based access control model. In *International Journal of Computer Integrated Manufacturing*, Vol. 22 Issue 3, p225-244.

Wainer, J., Barthelmess, P., Kumar, A., 2003. W-RBAC: A workflow security model incorporating controlled overriding of constraints. In *International Journal on Cooperative Information Systems*, Vol. 12 Issue 4, p455-485.

Waters, J.K., 2009. Target: the web. In *THE Journal*, Vol. 36 Issue 2, p34-40.

Whittaker, J., Andrews, M., 2006. *How to Break Web Software: Functional And Security Testing of Web Applications And Web Services*, Addison-Wesley Educational Publishers Inc.

Wortman, J., 2008. Seven Deadly Sins of IT Due Diligence. In *Buyouts*, Vol. 21 Issue 5, p44-46.