SECURITY CHARACTERISTICS OF E-COLLABORATION ENVIRONMENTS

Security architectures and recommendations

Bob Hulsebosch, Ernst-Jan Goedvolk, Wil Janssen
Telematica Instituut, P.O. Box 589, 7500 AN Enschede, The Netherlands
e-mail: {Bob.Hulsebosch, Ernst-Jan.Goedvolk, Wil.Janssen}@telin.nl

Abstract: To realize a trustworthy e-collaboration business environment more is needed than ICT-security tools only. One needs to understand the characteristics of such an environment, which have an impact on the overall security. Based on this observation we suggest architectures and recommendations for ICT-security in three different e-collaboration environments.

Key words: Security, E-collaboration, Characteristics, Architectures.

1. INTRODUCTION

Over the past years, the Internet has evolved into one of the most important means of communication. Businesses thrive on the increased efficiencies, reduced costs and expanded reach of the Internet [1]. Yet the full potential of modern Internet communication is often not utilized. Especially in the communication between enterprises, a certain reluctance to move to the Internet is present. An important reason for this is the perceived lack of security and trust [2]. Despite the availability of a wide variety of new ICT-security tools and techniques more is required to address the challenges of secure e-business environments on the Internet and to increase the trust level. In order to realize a trustworthy business environment for e-collaboration one first need to understand the characteristics of such a business environment, that might have an impact on the overall security.

Three models for e-collaboration environments where small and large ICT systems have to communicate with each other are distinguished [3]:

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35691-4_52
D. Gritzalis et al. (eds.), *Security and Privacy in the Age of Uncertainty*

Bilateral model: all parties independently perform individual transactions with each other. The overall 'logical' transaction often comprises a number of bilateral transactions. The data is stored within the own domain of each party and is not accessible by others.
Decentralised model: all parties control and distribute the information/data they own/have. The data storage is within each party's own domain and each party offers services to allow controlled access to the information by others.
Centralised model: all parties make use of a central database or service provider, which is outside their domain.

In this paper, we study the different security characteristics of the three e-collaboration models. Recommendations for security architectures are given. These results were developed and validated in the Virtual Port project [4].

2. E-COLLABORATION SECURITY ASPECTS

Several aspects that typically arise in an e-collaboration environment and have an impact on the overall security can be recognized. The *autonomy* of the collaborating parties must often be respected. The differences between the autonomous actors make it difficult to impose network-wide security measures. Furthermore, in an e-collaboration environment it is important to know who is *responsible* for the physical goods and information and must take the necessary measures. If one is not made responsible for its actions, one can always deny having performed an action. Perhaps the most serious problem in managing security risks is the *absence of accepted network-wide systems that enable companies to judge the risks* embedded in their current e-business environments. Finally, one should also take into account that not all actors in the e-collaboration network have the same *level of system security*. Naturally, services like *confidentiality, integrity, authentication, authorization, non-repudiation* remain essential in each security architecture.

Bilateral e-collaboration model

This model for e-collaboration is currently applicable to most of the processes in many e-business environments. Several specific characteristics of the bilateral model concerning security can be recognized. Firstly, the *parties know each other*. Consequently, the temptation to use non-ICT channels (e.g. phone, fax) to communicate with the other party is high, since both parties know each other. Such heterogeneity of communication channels significantly reduces the level of security and complicates implementation of security measures. The absence of third parties, which are often viewed as undesired middlemen, gives a larger feeling of confidence. Secondly, a bilateral model typically *hampers chain/network-wide agreements* and use of standards. Lack of such agreements reduces the

effectiveness and efficiency of all security measures. In a bilateral environment there is *little flexibility* concerning security services, i.e. processes are optimized for both parties only. As a result, management and control of encryption keys/certificates is often done locally. The conclusion of a new bilateral agreement with another party will subsequently result in more complex key management and interoperability problems. Finally, although information is always accurate for a sending and receiving party, other parties are not aware of their information exchange and are kept in *uncertainty*. Precautionary measures are difficult to plan and as a result the overall process is delayed.

In the bilateral model, all companies must decide for themselves which security measures they use. A logical approach as to whether the content of a message needs security measures must be made by each individual party and will largely depend on the infrastructure used. Use a virtual private network (VPN) for communication integrity, end-user authentication at the application level, and access control to information. To introduce some flexibility and reliability of the authentication process, we favor a PKI in which a central party co-ordinates the management of digital certificates.

Decentral e-collaboration model

The decentralized model is growing popular because it allows more efficient working practices. Many people from within and outside the secured domain may have access to process-related information, which demands greater *discipline* and sense of *responsibility*. In a distributed system, the players are *in control* of their own data, i.e. they can decide who has access to which information. Another advantage is that the system is more *flexible/scalable*, i.e. new parties can easily join the network. On the other hand, such flexibility makes it difficult to manage access control. For each new party joining the system, all other parties have to adjust their access control lists. Accidental operations such as lock-up checks, dealing with lost keys, and access control management make the model *expensive* and *time-consuming*.

The security characteristics of distributed systems are inherently different from those of centralized systems. These differences stem from the *lack of a central authority* responsible for data handling, security, and policy enforcement. Security models for distributed systems need to take these differences into account and must scale to a large number of users. The size of distributed systems and the fact that they tend to span organizational boundaries means that they are basically characterized by several security problems [5]. Firstly, it is difficult to provide the *same level of security* to all distributed systems (components, applications, and communication links). Secondly, organizations are *responsible* for enforcing security policies over

the systems that are under their jurisdiction but used by others as well. Most organisations lack the experience and facilities to take this responsibility.

In this model, where parties have little knowledge about each other and flexibility is important, we recommend to use a VPN for secure transmission of data and for shielding of the party's own information systems. A centralized system for management of VPN server certificates is required. At the application level, each actor must be held responsible for his operations. Moreover, the actors will need to authenticate to the other party to gain access to information. This means that all parties in the decentral model must have knowledge of all actors/roles in the system. Such a knowledge system can only be based on actor/role-based certificates, which are controlled and issued by a central party. In other words, a fully functional PKI is required.

Central e-collaboration model

Today's e-business environments require a fail-safe, secure infrastructure. Availability of the data at all time is crucial and requires back-up and fail-over capabilities. Security in centralized systems depends on the ability of a trusted computing base to control access to protected resources and secure communication.

The designated key-holders guarantee that all data is placed properly and maintain close checks on loss or theft. Although reliable and proven, this is not the most *efficient* system. User profiles, roles, and rights are critical to creating a secure system and are easy to control in a central system. *Access control* to data in the central database is crucial. Therefore, roles, profiles and rights must be determined and agreed upon by all companies collaborating with the central party. Moreover, all companies must *trust* each other and the central party and must be willing to place their data in the central database. Centralization also allows for easier implementation of *standards*, which generally facilitates sharing of data across the organization.

Choosing for a central system has its advantages: it is relatively *easy* to manage authentication and access control, data will be more consistent for all parties in the network, parties can use specific information elements without having to wait until the whole (e.g. EDI) message is sent. Some disadvantages of the central system are: the *availability* of information, trust is not present, parties are not always willing to share their information, who is really in control of the data in the central database?

Based on these characteristics we propose the following security architecture for the central e-collaboration model. A central database, containing all relevant information, is easily accessed via a Web interface. The interface must be secured via an authentication check. Access to the information stored at the database is crucial. SSL is used to establish a secure connection to the Web site. A server site certificate authentication

procedure is used to enable the SSL handshake. We prefer SSL above a VPN connection because of its simplicity and ease of use.

3. CONCLUSIONS

To realize a trustworthy e-collaboration business environment more is needed than ICT security tools. One needs to understand the characteristics of such an environment that have an impact on the overall security. Typical examples of these characteristics are the (desired) autonomy of the collaborating parties and their systems, the clear definition of responsibilities and accepted risks, and the differences in computerization between the collaborating parties. Security architectures must have the ability to support these aspects. Based on three models for e-collaboration, we have presented how various parties with a different level of computerization and a variety of systems can collaborate securely. When coupling various (small) systems one should take into account the relative advantages of each model:

- Bilateral model: simple, but not scalable;
- Decentral model: robust, flexible, but highly complex;
- Central model: simple for most parties, scalable, but may conflict with the business culture.

Finally, we want to state that the current ICT systems in most e-collaboration environments are based on existing business processes. Often, little attention has been paid to the aspect of security in these business processes. As a consequence, in order to protect the ICT systems, business processes have to be redesigned taking security policies into account. Only then a suitable architecture for ICT security can be developed that tightens the trust relationships that exist in e-collaboration infrastructures. We stress that it is of importance to first have a good insight in the business processes, their critical assets and the responsibilities. Only then proper security policies can be made up and suitable security measures can be implemented.

REFERENCES

1. R. Alt, E. Fleisch, & H. Österle,, *Business networking: Shaping enterprise relationships on the Internet*, H. Österle, E. Fleisch, & R. Alt (Eds.), p. 1-13, Berlin: Springer, 2000.
2. L. Ang, C. Dubelaar & B. Lee, *To trust or not to trust?* 14th Bled Electronic Commerce of Conference, Bled, Slovenia, June 25-25, 2001.
3. Hau L. Lee & Seungin Whang, *Information Sharing in a Supply Chain*, International Journal of Technology Management, Vol. 20, p. 373-387, 2000.
4. W. Janssen & H. van Raalte (eds.). *Blueprint for a virtual port.* https://doc.telin.nl/dscgi/ds.py/Get/File-23315/, see also www.virtuelehaven.nl.
5. See also: http://www.cs.utexas.edu/users/new_directions/Papers/ken_goldman.html.