Chapter 5
Data Protection in Collaborative Business Applications

Florian Kerschbaum
SAP Research CEC Karlsruhe, Germany

ABSTRACT

Collaborative business applications are an active field of research and an emerging practice in industry. This chapter will focus on data protection in B2B applications which offer a wide range of business models and architecture, since often equal partners are involved in the transactions. It will present three distinct applications, their business models, security requirements and the newest solutions for solving these problems. The three applications are collaborative benchmarking, fraud detection and supply chain management. Many of these applications will not be realized if no appropriate measure for protecting the collaborating parties’ data are taken. This chapter focuses on the strongest form of data protection. The business secrets are kept entirely secret from other parties (or at least to the degree possible). This also corresponds to the strongest form of privacy protection in many instances. The private information does not leave the producing system, (i.e., data protection), such that the information producer remains its sole owner. In case of B2B application, the sensitive data are usually business secrets, and not personally identifiable data as in privacy protection.

INTRODUCTION

Collaborative business applications are an active field of research and an emerging practice in industry. Collaborative business applications can be classified into business-to-consumer (B2C) and business-to-business (B2B) applications. Electronic B2C applications are of great interest with the advent of the Internet as an additional sales channel, but are usually restricted in their business model and architecture to classical client-server matching the buyer-seller relationship. B2B applications offer a much wider range of business models and architecture, since often equal partners are involved in the transactions. The security requirements resulting

DOI: 10.4018/978-1-60566-414-9.ch005
Data Protection in Collaborative Business Applications

from these architectures therefore also span a much broader variety than in the B2C area.

This chapter will focus on data protection in B2B applications. It will present three distinct applications, their business models, security requirements and the newest solutions for solving these problems. The three applications are collaborative benchmarking, fraud detection and supply chain management. Each application has its own business model and architecture.

In each of these applications data protection is of the utmost importance. Many of these applications will not be realized if not appropriate measure for protecting the collaborating parties’ data are taken. The involved data usually consists of business secrets whose revelation would impact the position of the company, e.g. its negotiation position or external recognition. This data is therefore associated with a risk of revelation, and the effect of data protection can be financially measured with risk analysis.

This chapter focuses on the strongest form of data protection. The business secrets are kept entirely secret from other parties (or at least to the degree possible). Each party is seen as an entity that is either entirely compromised or intact and can perform computations without being inspected. Then there is a protocol that relies on cryptographic protection run between the parties. One can show that (under certain assumptions) nothing can be inferred from the protocol except the result.

This also corresponds to the strongest form of privacy protection in many instances. The private information does not leave the producing system, i.e. data protection, such that the information producer remains its sole owner. In case of B2B application, the sensitive data are usually business secrets, and not personally identifiable data as in privacy protection. The value of business secrets can often be higher than that often irrationally low value of personal information as many studies suggest (Acquisti 2004, Cvrcek et al. 2006). Therefore the protection of data in collaborative business applications can be much better economically motivated than its counterpart privacy.

The motivation for collaboration in these business applications stems from an economic benefit that cannot be achieved by a party by itself, i.e. the motivational factor is not enhanced security, but economics. Nevertheless as mentioned before many of these applications will not be realized, if not appropriate security measures are in place. In particular this chapter is concerned with the information gain, such applications can provide and that can be an effective obstacle to the realization of the application. The economic benefit is therefore tied to the security requirements which usually stem from the business model and so data protection enables an economic benefit.

Secure Multi-Party Computation

Secure Multi-Party Computation (SMC) (Ben-Or et al. 1988, Goldreich et al. 1987, Yao 1982) allows the joint computation of a function without any party revealing its input. What seems puzzling at first can be visualized with an example (Schneier 1996).

How can a group of people calculate their average salary without anyone learning the salary of anyone else? Let there be three people: Alice, Bob and Carol. Alice starts and adds a secret random number to her salary and tells Bob the result, such that Carol cannot hear it. Bob who only knows the sum does not know anything about Alice’s salary. He then adds his salary and tells Carol the result, such that Carol cannot hear it. Bob who only knows the sum does not know anything about Alice’s salary. He then adds his salary and tells Carol the result without Alice hearing it. Carol does the same: adds her salary and tells it to Alice without Bob hearing it. Alice now remembers her secret random number and subtracts that from the result which is the sum of the three salaries. She announces the result and everybody can calculate the average by dividing by three, the number of people.

The intriguing fact about this simple protocol is that everybody learned the result, but no one else’s input. The results from (Ben-Or et al. 1988, Goldreich et al. 1987, Yao 1982) show that this