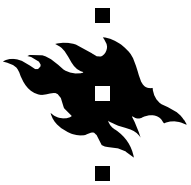
DEPARTMENT OF COMPUTER SCIENCE
SERIES OF PUBLICATIONS C
REPORT C-2010-56

Safeguarding against new privacy threats in inter-enterprise collaboration environments

Pirjo Moen, Sini Ruohomaa, Lea Viljanen, Lea Kutvonen



UNIVERSITY OF HELSINKI
FINLAND

Contact information

Postal address:
Department of Computer Science
P.O.Box 68 (Gustaf Hällströmin katu 2b)
FIN-00014 University of Helsinki
Finland

Email address: postmaster@cs.Helsinki.FI (Internet)

URL: http://www.cs.Helsinki.FI/

Telephone: +358 9 1911

Telefax: +358 9 191 51120

Computing Reviews (1998) classification: C.2.4, H.5.3, K.4.4, K.6.5
Helsinki 2010
Helsingin yliopisto, tietojenkäsittelytieteen laitos

DEPARTMENT OF COMPUTER SCIENCE
SERIES OF PUBLICATIONS C
REPORT C-2010-56

Safeguarding against new privacy threats in inter-enterprise collaboration environments

Pirjo Moen, Sini Ruohomaa, Lea Viljanen, Lea Kutvonen

UNIVERSITY OF HELSINKI
FINLAND

Safeguarding against new privacy threats in inter-enterprise collaboration environments

Pirjo Moen, Sini Ruohomaa, Lea Viljanen, Lea Kutvonen

Department of Computer Science
P.O. Box 26, FIN-00014 University of Helsinki, Finland
firstname.lastname@cs.helsinki.fi

Technical report, Series of Publications C, Report C-2010-56
Helsinki, December 2010, iii + 15 pages

Abstract

Inter-enterprise collaboration has become essential for the success of enterprises. As competition increasingly takes place between supply chains and networks of enterprises, there is a strategic business need to participate in multiple collaborations simultaneously. Collaborations based on an open market of autonomous actors set special requirements for computing facilities supporting the setup and management of these business networks of enterprises. Currently, the safeguards against privacy threats in collaborations crossing organizational borders are both insufficient and incompatible to the open market. A broader understanding is needed of the architecture of defense structures, and privacy threats must be detected not only on the level of a private person or enterprise, but on the community and ecosystem levels as well. Control measures must be automated wherever possible in order to keep the cost and effort of collaboration management reasonable. This article contributes to the understanding of the modern inter-enterprise collaboration environment and privacy threats in it, and presents the automated control measures required to ensure that actors in inter-enterprise collaborations behave correctly to preserve privacy.

Computing Reviews (1998) categories and subject descriptors:
C.2.4 Computer-communication Networks: Distributed Systems
H.5.3 Information Interfaces and Presentation: Group and Organization Interfaces
K.4.4 Computers and Society: Electronic Commerce
K.6.5 Management of Computing and Information Systems: Security and Protection

General terms:
Design, Management, Security

Additional key words and phrases:
Privacy, Inter-enterprise Collaboration, Threats, Trust, eContract Control

Contents

Chapter 1

Introduction

Inter-enteprise collaboration involves a group of enterprises working together for a joint goal. Each enteprise offers a specific service, such as transporting goods, managing customer payments, or order handling. These services fulfil roles in a business network, with a predefined joint process and goals. The collaboration is regulated by a shared contract.

As competition increasingly takes place between supply chains and networks of enterprises, service providers have a strategic business need to participate in multiple collaborations simultaneously. They expect to easily compose new collaborations from services in the open service market, and need to manage these constructs while respecting both regulation and the autonomy of collaboration partners. Control measures must be automated wherever possible, in order to keep the cost and effort of collaboration management reasonable.

Collaborations based on an open market of autonomous service providers set special requirements for computing facilities supporting the setup and management of these business networks of enterprises. New threats emerge in the fields of data security and enterprise-level privacy.

We define privacy as *the claim of individuals, groups, or institutions to determine for themselves, when, how, and to what extent information about them is communicated to others* [35]. In other words, the subject of privacy can either be a person, a group of people, or a formal organization under which people and groups cooperate. In the inter-enterprise collaboration context, privacy appears on four levels: private people, the enterprise, the collaboration, and the entire service ecosystem.

Cross-organizational privacy-enhancing technologies and standards are sorely needed, as partnering makes more and more data being shared between organizations [20]. Many proposed solutions for collaborations are based on a closed set of strategic partners who are "already known", and rely on forming a single domain of trust [36, 18, 24]. Gaining membership in the trusted virtual breeding environment is no real guarantee that the enterprise partner will behave well and follow shared norms in the future. The research challenge of security and privacy management is far from solved from the data management viewpoint; solutions are needed for policy definition and enforcement, monitoring and the negotiation of joint policies, such as contracts [14].

We aim to fill this gap with the friendly combination of distrust and punishment. We focus on data security and privacy threats emerging from misbehaving collaborators, monitoring their requests and continuously weighing the risks of the collaboration against the benefits gained from it. We also propose a combination of technical, social and legal sanctioning when breaches of contract or policy are detected.

Our contribution is threefold: first, we contribute to the understanding of the modern inter-enterprise collaboration environment and defense structures in it; second, we identify new threats to assets such as data and metadata, and new domains of threats created by collaboration that must

be addressed; and third, we present automated control measures to ensure that actors in inter-enterprise collaborations behave correctly to ensure data security and privacy beyond our means to directly control the enterprise partners.

Chapter 2 provides a condensed overview of the ecosystem for inter-enterprise collaboration, supported by the Pilarcos architecture. Chapter 3 discusses the findings of our threat analysis, and Chapter 4 presents countermeasures specifically against partner misbehaviour. Finally, Chapter 5 concludes with some environmental requirements for the future.

Chapter 2

Ecosystem for inter-enterprise collaboration

The Pilarcos architecture views inter-enterprise collaboration as a loosely-coupled, dynamic constellation of business services. The constellation is governed by an eContract that captures the business network model describing the roles and interactions of the collaboration, the member services, and policies governing the joint behaviour [15, 17].

The Pilarcos architecture provides a middleware layer with common services for a breeding environment of new collaborations, and local, enterprise-system services for accessing trusted agents for managing the entire lifecycle of a collaboration. These services are supported by repositories of public and private information. Multiple collaborations in different phases of their lifecycle can run simultaneously within this open service ecosystem. An overview of the open service ecosystem is depicted in Fig. 2.1.

The management services include 1) service discovery and selection, 2) eContract establishment, 3) monitoring, and 4) experience reporting. They provide support for the four phases of the collaboration: establishment, agreement, enactment and control, and evaluation. Unlike many existing proposals [36, 18, 24, 21], collaboration management in the open service ecosystem does not rely on centralized control of the entire collaboration: participants remain autonomous and independent of the initiator of the business network. In addition, some of the management support needed can be offered as services by specialized third parties rather than requiring one ultimately trusted actor to rule over everything.

Service discovery and selection services support the collaboration establishment phase. It is based on public business process models describing the collaborations, and public service offers made by service providers [15, 29]. Business network models capture the best practices of a given field, and they are built from formally defined service types. The task of producing these models and types naturally falls to consortia and standardization bodies.

Automated eContract establishment supports the agreement phase of the collaboration [15]. The business process model and the proposed service offers to populate the roles in it are processed by an automated contract negotiation infrastructure, which is controlled locally by each collaboration partner. Contracts are based on templates specific to the collaboration model, and the terms of service provision given in service offers form the basis of negotiations. The negotiated eContract includes a model of the business process of the collaboration as well as the finalized terms of service in the form of accepted service offers.

Monitoring supports the enactment and control phase of the collaboration in particular [16]. It is done by each collaborator to protect local resources, keep track of the progress of the collabo-

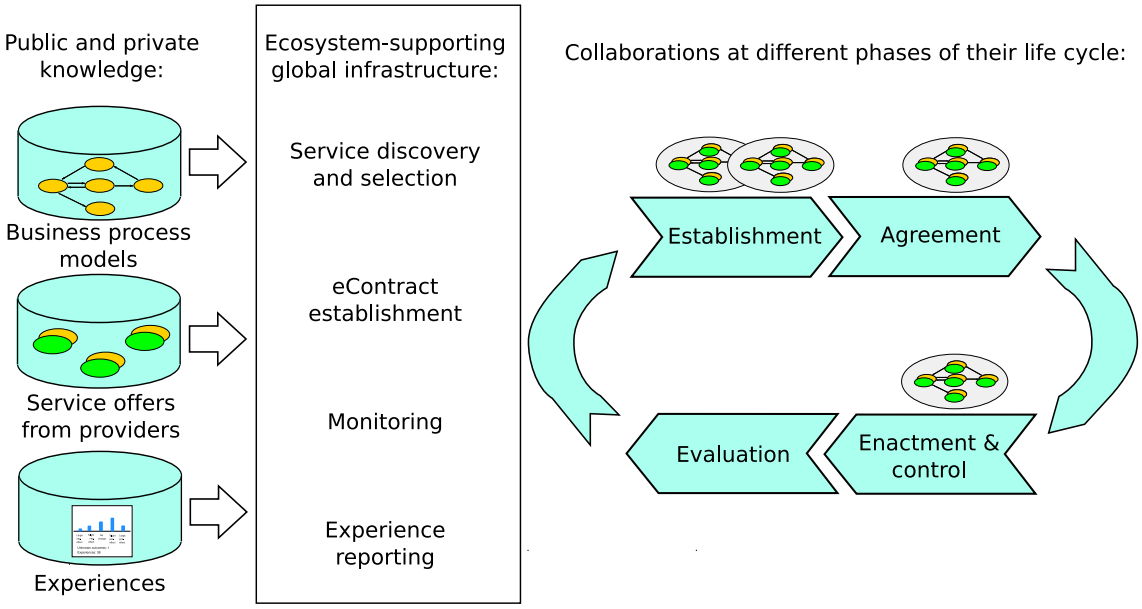


Figure 2.1: An overview of the open service ecosystem.

ration, and to ensure that partners follow the collaboration model.

Experience reporting mainly supports the evaluation phase of the collaboration, although it also connects to the monitoring service during the enactment of the collaboration [28, 27]. Experience reporting forms the core of social control in the open service ecosystem. As contract violations are detected by monitors, they are published to other actors as well: it is important to create a direct reputation impact to privacy and data security violations in order to limit the damage that misbehaving actors can achieve in other collaborations.

Chapter 3

Threats

Collaboration with partners, some previously known and some unknown, exposes the enterprise to security and privacy threats. Threats are targeted towards assets that are either concrete and intangible, such as money, data, contracts, the good reputation of the enterprise and its ability to remain autonomous and independent of any single dictating partner. The importance of intangible assets increases in a collaborative setting. While partial efforts in filling the gaps between single system and enterprise level security exist, for example in the form of message context protection [33], a thorough analysis of general threats, risks and possible countermeasures in the inter-enterprise collaboration context has not been previously done [6].

3.1 Threat analysis for inter-enterprise collaboration

We have performed a threat analysis of inter-enterprise collaboration with the open service ecosystem in focus, in order to find threats arising from the structure of the ecosystem that should be safeguarded against. To ensure a sufficiently broad threat analysis for the generic collaboration context, we applied the formal threat tree method [2], dividing the target system into views of *actors* (member services in a collaboration, members of the community, the possibly external client receiving the collaborative service, public and private parts of the collaboration management middleware, and others) and the *assets* of the community, the enterprises in it and other involved parties. After compiling lists of what threats each actor can cause towards another actor's assets for all selected categories, we classified them and selected specific types of threats for further analysis in the next section.

As threats and risks arise from multiple levels in inter-enterprise collaboration, it is no longer sufficient to think of the security of the single technical service:

- On the service ecosystem level, e.g. the metainformation acting as the basis of collaborations is at stake.
- On the collaboration level, e.g. reaching the shared goal may be threatened by participants not fulfilling their tasks.
- On the enterprise level, e.g. local policy or contract violations need to be protected against, and the fulfilment of business objectives of the single member enterprise are at stake. These are reflected on all the services provided by the enterprise.
- On the level of private people, data security and privacy issues are numerous enough to even have given rise to multiple taxonomies [32, 4].

The existing solutions for mitigating privacy and security threats to enterprise data must be extended to protect the metadata around inter-enterprise collaboration as well: for example, while the open-ended service offers can be more or less public, the negotiated terms of service provision in the eContract are already more sensitive information. Experience information is particularly important to protect from distortion, as it not only affects the targeted service, but also inhibits the other actors' ability to assess its behaviour, reducing the power of social control [32].

3.2 Threats arising from the structure of the ecosystem

We will now discuss a set of threats that are independent of the specific type of collaboration at hand, but rather arise from the structure of the open service ecosystem. These include threats incurred by modelling, false offers of service provision, committing resources to harmful collaborations, and partner misbehaviour, such as contract violations. We will present the central countermeasures briefly; a deeper analysis is provided in the next section on three of them: automated decision-making, monitoring, and reaction to detected breaches.

As business network models and service offers are a focal element for the ecosystem, special care must be taken with the management of model repositories. Inter-enterprise collaborations are defined through business network models, defining the roles and interactions in the collaboration, service types, defining the outward behaviour of the service, and service offers, defining the terms of providing a service of a given service type.

Many threats to privacy and data security in collaborations arise from structural problems in business network models and the interoperation of formal service types. Together, these models define the interactions between services in the collaboration. For example, if the collaboration model sets a demand for sharing information in a way that violates local policy, there are no safeguards deployable at the collaboration enactment time that can allow the collaboration to continue.

Avoiding these threats sets requirements to collaboration modelling, as they are the keystone of ensuring collaboration-level security. The model repositories store these public models and distribute them for the purpose of initiating new collaborations. They should perform validation analysis and consistency checking on new models before accepting them. When breaches to local privacy policies are detected, they should serve as feedback to the improvement of the models. In addition, service offers must be verified to match their service type before being accepted into the public service offer repository, and the sources of the offers must be traceable.

Service offers convey a commitment to provide a service of the given type, with a given, public set of terms. The central content of a service offer involves setting parameters or negotiable parameter ranges for providing the service, and the final values are set during negotiations. For example, the announced price of service provision may be a broad range depending on other negotiable parameters in the offer, while after negotiations the price is set to a single value which is no longer publicized outside the collaboration. In the meanwhile, a parameter indicating that the service supports a specific protocol version can remain both fixed and public.

Service offers can contain false information. Fake offers can be used to enter into negotiations and discover the terms that competitors would be willing accept for offering their service. In order to safeguard against this kind of misinformation, service offers must be traceable to whoever submitted them to the repository, and negative experience reports should be sent out by the other negotiators to incur a reputation cost to the source of false offers.

A more general threat arises from automation: the enterprise may enter into collaborations that at odds with its local policies or even put the enterprise assets at risk due to unreliable partners. The central countermeasure is to set decision-making points, i.e. policy enforcement, before join-

ing a collaboration, and during its enactment at relevant resource commitment points within the collaboration. Routine decisions with clear outcomes can be made automatically, while borderline and unclear cases must be left to a human user.

Partner misbehaviour is the source of a multitude of threats. Causes for misbehaviour are numerous: besides the partner being downright malicious, their service can be buggy, poorly designed or subverted by an outside attacker, participating in multiple collaborations may leave them with conflicts of interest either between collaborations or between a collaboration and local policy, and in the end they may well wish to optimize their resource use by simply bending the contract a little. These are all familiar problems from the brick-and-mortar enterprise tradition, and they will follow us into the ecosystem of modern inter-enterprise collaborations as well.

As partner behaviour can change, the decision-making mentioned above must be based on up-to-date experience information to take this into account. Sharing experiences globally within the ecosystem allows enterprises to learn from each others' mistakes and strengthens the sanctions from misbehaviour: not only does a contract violation affect the ongoing collaboration, but future collaborations with other partners as well [26].

Chapter 4

Countermeasures against misbehaving partners

The guiding principle of operating in the open market is to be ready to enter into new collaborations in order to reap the gains from them, but to be vigilant bordering on distrustful at the same time to avoid the pitfalls. When misbehaviour is detected, however, a corrective reaction is needed that repairs what damage is possible and ensures that the problem does not repeat itself. We present three central countermeasures against threats involving the misbehaviour of collaboration partners: automated decision-making to protect enterprise assets, monitoring to detect misbehaviour, and sanctioning to encourage cooperative behaviour in the future.

4.1 Automated decisions to protect enterprise assets

During the negotiations in the agreement phase of the collaboration and at relevant points during its enactment, each participant makes local decisions on whether to first join the collaboration in the first place, and later on whether they wish to continue in it. These decisions are based on private policy, and a combination of private information about e.g. local valuations as well as experience information that is globally shared in the ecosystem. The goal is to evaluate whether the benefits of participation outweigh the risks; particularly the latter evaluation can change during the collaboration based on new experience information. Borderline and unclear cases cannot be determined by automation; they are instead forwarded to a human user. This distinction is guided by a metapolicy defining what kind of situations can be considered routine, with clear outcomes [27].

The decisions are made to protect the assets of the enterprise. In our model, we have defined assets more broadly than a single monetary dimension would allow, particularly in order to better support policies directed towards protecting intangible assets, such as the privacy of data and metadata.

A decision weighs the benefits of the collaboration against the risks. Both are represented as effects that the considered commitment has on assets. Benefits include the completion of the task of the collaboration and fulfilment of the enterprise's goals in it, return of investment, strategical gain of a new partner or strengthening market share. Of these, only the return of investment can easily be measured in monetary terms. In addition, any contractual penalties from refusing service during the collaboration to e.g. a misbehaving partner must be considered as a part of the decision. Avoiding contracts that are too binding in this sense is an important way to protect the autonomy of the enterprise.

Risks include not completing the task, loss of money and other committed resources, loss of

reputation in the eyes of customers or other partners, or loss of privacy, autonomy (in the form of overly strict contracts or being bound to a single partner) or security (if the collaboration model enforces poor security practices). Risks are represented both as an impact of the described threat happening, and the probability of this outcome. The probabilities are extracted from experience information.

Further details on the information model and algorithms for decision-making are presented in earlier work [28, 27].

4.2 Monitoring to detect misbehaviour

Monitoring is the responsibility of each participant; there are no all-seeing trusted third parties present in the open service ecosystem. This also means that unless the business network model explicitly support it, no single service has complete overview of what goes on in the collaboration. For example, if a specific collaboration type requires a notary to act as a witness to specific activities, it must be incorporated as a role in the business process model itself, and a suitable service provider found to act as the witness.

Monitors control traffic both in and out of the technical service application, which is capable of varying behaviour. The service provision policy set in the collaboration eContract is enforced by the monitor, as well as more persistent enterprise policies such as a privacy policy for handling sensitive data. If the eContract policies are found to be at odds with local policy, the latter overrides the shared policy.

In terms of the eContract, misbehaviour is defined straightforwardly as anything deviating from the business process set in the business network model that the eContract stores. Contract-abiding but "suspicious" behaviour, however, is more difficult to capture; anomaly detection approaches suffer from false alarms and therefore would be best used under human supervision [34].

The monitor operates in three modes: proactive, active and passive. Proactive monitoring blocks messages from passing until the analysis is complete. For example determining whether the service request is authorized in the eContract, as well as the automated decision-making discussed in Section 4.1, are both incorporated into a proactive monitoring module. Active monitoring does not block messages, but operates in real time and may produce side effects, such as alerts: for example, negative experience reports can be produced immediately when misbehaviour is detected, while positive reports generally wait until the successful end of a collaboration or a well-defined part of it. Passive monitoring is used for later analysis that no longer depends on time. It can be used to for example plot service usage patterns over longer periods.

Monitoring is based on simple rules produced from higher-level policies. For monitoring that takes place in real time, and blocks the message exchanges between services during analysis, performance is a real concern. We have considered this both in choosing the decision algorithms and information models used [27], and in simulation experiments on the monitor infrastructure itself to ensure the feasibility of this solution.

Based on the results of our threat analysis, we have reimplemented the Pilarcos monitoring system to be more modular, allowing new rules to be plugged in to a processing tree of interdependent checks. This makes it more straightforward to transform policies with different goals and from different levels — the business level, community level and service level — into monitoring rules. We have found that there is an overall need to bring business concepts, which form the language of the policy-setters, closer to the technical concepts, which form the language of automated policy enforcement.

Ensuring that communication between services is done only through contractually authorized

partners considerably reduces outsiders' means to attack the information passed between them. The business services cannot be completely firewalled in on any level, as they must be able to form these pairwise authorizations freely during collaboration establishment. However, monitors limit access to the actual technical service application during the enactment of the collaboration. While this safeguards the service against external attackers, the threat of misuse remains within authorized peers. The threat can, in the end, only be mitigated through the counterthreat of legal and social sanctions, including being shut off from further collaborations.

4.3 Sanctioning to encourage cooperative behaviour

When a breach is detected, a sanctioning system must be activated. Sanctions can be divided into three categories: technical access control, legal sanctions and social pressure. The regular automated decision-making provides a way to immediately revoke access to a service in case a partner misbehaves. This safeguards against further damage, but does nothing to the damage already done.

Contract violations are penalized by law, which generally provides sufficiently harsh monetary penalties but operates very slowly and, in the meanwhile, does not protect other organizations from unwittingly collaborating with the miscreant. Technical countermeasures and legal sanctions must therefore be complemented by social pressure.

Social pressure can be implemented as a form of service reputation based on the experience reports that are constantly shared among actors in the service ecosystem. Uncooperative behaviour is punished by a drop in reputation, which discourages other actors from collaborating with the misbehaving actor.

A reputation system is a form of a sanctioning. Sanctioning institutions have been demonstrated to carry a clear competitive advantage in the long run [9]. In the absence of centralized control, punishment is altruistic: it is carried out by peers who do it at a cost to themselves and no direct benefit. In human behaviour, this cost is balanced out by reputational benefits, which make just punishers be seen as more trustworthy [3].

Supporting altruistic punishment allows collaborative societies to scale up in size and time. It is essential that sanctions are not only limited to those who misbehave, but also those who spread misinformation in the form of forged experiences [8].

In order for the social pressure from reputation to have any effect, persistent digital identities are needed for the services [26]. On the other hand, strong identity management is already necessary to enter into legally binding contracts. As creating a legal entity capable of signing contracts carries more cost than generating a simple fake service, this also protects against experience distortion by a group of generated drone services [7].

Chapter 5

Conclusion

In the recent years, privacy has become an important issue in many areas of computer science, and a need for supporting it in networked environments has also become very actual [20]. Privacy aspects for individuals in particular are well present in OECD work [22, 23] as well as EU directive level [30].

Several privacy-related architectures have been proposed. These include the use of a mediator [19], enhancing the privacy of web services [12], or different approaches for managing and enforcing privacy policies [5, 1, 31]. Some of these architectures have also been implemented as prototypes (e.g., Privacy Injector [5]), or even as commercial products (e.g., the IBM Tivoli Privacy Manager for e-business —Tivoli software [13], HP Select Access [10] and HP Select Identity [11]. However, none of these architectures as such is suitable for controlling privacy in the inter-enterprise collaboration, as they either assume the collaborations to be closed and to form a single domain of trust, or concentrate on protecting only intra-enterprise privacy.

Our contribution has been to identify the new levels of privacy and data security threats emerging from modern inter-enterprise collaboration, and presenting countermeasures for threats particularly poorly addressed in the past: those caused by partner misbehaviour. These countermeasures are threefold: automated decisions, monitoring and corrective measures when breaches are detected, particularly experience reporting.

The sharing and use of experience information introduces social control into inter-enterprise collaboration in the open service ecosystem. Shared experiences form a computational equivalent of reputation: those who are caught misbehaving suffer damage to their reputation, while those who correctly report this misbehaviour gain positive reputation. The reputation damage, in turn, warns off other actors to not collaborate with the misbehaver, which limits the overall damage they can cause. In the long run, misbehaviour must also be sanctioned by law in order to provide a final deterrent. This requires a new level of legal support for inter-enterprise collaboration, in two categories.

First, legislation must be modified to support computational agents making legally binding contractual commitments. It is technically fully feasible to automate contract negotiations based on contract templates, where the terms of service provision are adjusted to fit all members of the proposed collaboration. This automation is useless, however, if the resulting contracts are not legally valid due to having been finalized and enacted by agents. The combination of standardization and legislation should eliminate any need of manual pairwise signing of pre-contracts between all potential partners in the market.

Second, legal support is also needed for the partially as well as fully automated exchange of experience information on these agents. As these experiences form a reputation for services, even valid negative experience reports cause an opening for defamation charges, vengeful business

tactics and even retaliatory negative reports [25].

In order to support straightforward and usable monitoring rules, it is important that the message exchanges between services incorporate sufficient information to see what is happening. As the monitor is not a part of the technical service application but hooks into the messaging interface, it cannot observe the internal state of the service application directly. This should be taken into consideration when building the business network models and service types that define the message exchanges.

As enterprise collaborators can reside in different jurisdictions, legal recourse becomes more problematic when compared to more geographically limited collaborations. However, this is not a new problem introduced by open service ecosystems, and international collaboration has already become a reality for many enterprises. Increased support from local legislation and international agreements will reduce the setup costs and risks of international collaboration, but some level of location awareness will have to remain as a part of services provided on the Internet as well.

Bibliography

[1] ALLISON, D., EL YAMANY, H., AND CAPRETZ, M. A. M. Metamodel for privacy policies within SOA. In *Proceedings of SESS'09* (Vancouver, Canada, 2009).

[2] AMOROSO, E. G. *Fundamentals of Computer Security Technology*. Prentice-Hall International, Inc., 1994.

[3] BARCLAY, P. Reputational benefits for altruistic punishment. *Evolution and Human Behaviour 27* (Sept. 2006), 325–244.

[4] BARKER, K., ASKARI, M., BANERJEE, M., GHAZINOUR, K., MACKAS, B., MAJEDI, M., PUN, S., AND WILLIAMS, A. Data privacy taxonomy. In *Dataspace: The Final Frontier* (Birmingham, United Kingdom, July 2009), vol. 5588 of *LNCS*, Springer, pp. 42–54.

[5] BERGHE, C. V., AND SCHUNTER, M. Privacy injector - automated privacy enforcement through aspects. In *Proceedings of 6th Workshop on Privacy Enhancing Technologies (PET 2006)* (2006), Springer, pp. 99–117.

[6] DESMET, L., JACOBS, B., PIESSENS, F., AND JOOSEN, W. Threat modelling for web services based web applications. In *Communications and Multimedia Security* (2004), vol. 175 of *IFIP*, Springer, pp. 161–174.

[7] DOUCEUR, J. R. The sybil attack. In *Electronic Proceedings of the 1st International Workshop on Peer-to-Peer systems (IPTPS'02)* (MIT Faculty Club, Cambridge, MA, USA, Mar. 2002).

[8] FEHR, E., AND FISCHBACHER, U. The nature of human altruism. *Nature 425* (Oct. 2003).

[9] GÜREK, Ö., IRLENBUSCH, B., AND ROCKENBACH, B. The competitive advantage of sanctioning institutions. *Science 312* (2006).

[10] HP. Openview select access - overview and features. http://www.openview.hp.com/products/select, 2005.

[11] HP. Openview select identity - overview and features. http://www.openview.hp.com/products/slctid/index.html, 2005.

[12] HUNG, P. C., CHIU, D. K., FUNG, W. W., CHEUNG, W. K., WONG, R., CHOI, S. P., KAFEZA, E., KWOK, J., PUN, J. C., AND CHENG, V. S. End-to-end privacy control in service outsourcing of human intensive processes: A multi-layered web service integration approach. *Information Systems Frontiers 9*, 1 (2007), 85–101.

[13] IBM. Tivoli privacy manger for e-business. http://www-306.ibm.com/software/tivoli/products/privacy-mgr-e-bus/, 2005.

[14] JEFFERY, K. G. The internet of things: the death of traditional database? In *Proceedings of the 1st International Workshop on Database Architectures for the Internet of Things (DAIT)* (Birmingham, UK, 2009).

[15] KUTVONEN, L., METSO, J., AND RUOHOMAA, S. From trading to eCommunity management: Responding to social and contractual challenges. *Information Systems Frontiers (ISF) - Special Issue on Enterprise Services Computing: Evolution and Challenges 9*, 2–3 (July 2007), 181–194.

[16] KUTVONEN, L., METSO, J., AND RUOKOLAINEN, T. Inter-enterprise collaboration management in dynamic business networks. In *On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE: OTM Confederated International Conferences, CoopIS, DOA, and ODBASE* (Agia Napa, Cyprus, Nov. 2005), vol. 3760 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 593–611.

[17] KUTVONEN, L., RUOKOLAINEN, T., AND METSO, J. Interoperability middleware for federated business services in web-Pilarcos. *International Journal of Enterprise Information Systems, Special issue on Interoperability of Enterprise Systems and Applications 3*, 1 (Jan. 2007), 1–21.

[18] MEHANDIEV, N., Ed. *Dynamic Business Process Formation for Instant Virtual Enterprises*. Springer, 2010. To appear in March 2010.

[19] MITRA, P., PAN, C.-C., LIU, P., AND ATLURI, V. Privacy-preserving semantic interoperation and access control of heterogeneous databases. In *Proceedings of the 2006 ACM Symposium on Information, computer and communications security (ASIACCS'06)* (New York, NY, USA, 2006), ACM, pp. 66–77.

[20] NELSON, M. R., SCHUNTER, M., MCCULLOUGH, M. R., AND BLISS, J. S. Trust and on demand: Enabling privacy, security, transparency, and accountability in distributed systems. In *Proceedings of the 33rd Research Conference on Communication, Information and Internet Policy (TPRC'05)* (Arlington, VA, USA, 2005).

[21] NORMAN, T. J., PREECE, A. D., CHALMERS, S., JENNINGS, N. R., LUCK, M., DANG, V. D., NGUYEN, T. D., DEORA, V., SHAO, J., GRAY, W. A., AND FIDDIAN, N. J. Agent-based formation of virtual organisations. *Knowledge-based systems 17*, 2–4 (Apr. 2004), 103–111.

[22] OECD. The guidelines on the protection of privacy and transborder flows of personal data, September 1980.

[23] OECD, WORKING PARTY ON INFORMATION SECURITY AND PRIVACY. Privacy online: policy and practical guidance. Tech. Rep. DSTI/ICCP/REG(2002)3/FINAL, OECD, 2003.

[24] RABELO, R. J., GUSMEROLI, S., ARANA, C., AND NAGELLEN, T. The ECOLEAD ICT infrastructure for collaborative networked organizations. In *Network-Centric Collaboration and Supporting Frameworks* (2006), vol. 224, Springer, pp. 451–460.

[25] RESNICK, P., AND ZECKHAUSER, R. Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system. In *The Economics of the Internet and E-Commerce* (2002), vol. 11 of *Advances in Applied Microeconomics*, Elsevier Science, Amsterdam, pp. 127–157.

[26] RESNICK, P., ZECKHAUSER, R., FRIEDMAN, E., AND KUWABARA, K. Reputation systems. *Communications of the ACM 43*, 12 (Dec. 2000), 45–48.

[27] RUOHOMAA, S., AND KUTVONEN, L. Making multi-dimensional trust decisions on inter-enterprise collaborations. In *Proceedings of the Third International Conference on Availability, Security and Reliability (ARES 2008)* (Barcelona, Spain, Mar. 2008), IEEE Computer Society, pp. 873–880.

[28] RUOHOMAA, S., VILJANEN, L., AND KUTVONEN, L. Guarding enterprise collaborations with trust decisions—the TuBE approach. In *Interoperability for Enterprise Software and Applications. Proceedings of the Workshops and the Doctoral Symposium of the Second IFAC/IFIP I-ESA International Conference: EI2N, WSI, IS-TSPQ 2006* (Mar. 2006), ISTE Ltd, pp. 237–248.

[29] RUOKOLAINEN, T., AND KUTVONEN, L. Service Typing in Collaborative Systems. In *Enterprise Interoperability: New Challenges and Approaches* (Apr. 2007), G. Doumeingts, J. Müller, G. Morel, and B. Vallespir, Eds., Springer, pp. 343–354.

[30] SAFEGUARDING EUROPEAN UNION. Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995.

[31] SCHUNTER, M., AND WAIDNER, M. Simplified privacy controls for aggregated services — suspend and resume of personal data. In *Proceedings of the 7th Workshop on Privacy Enhancing Technologies (PET)* (Ottawa, Canada, 2007).

[32] SOLOVE, D. J. A taxonomy of privacy. *University of Pennsylvania Law Review 154*, 3 (Jan. 2006). GWU Law School Public Law Research Paper No. 129.

[33] VAN DEN HEUVEL, W.-J., LEUNE, K., AND PAPAZOGLOU, M. P. EFSOC: A layered framework for developing secure interactions between web-services. *Distributed and Parallel Databases 18*, 2 (2005), 115–145.

[34] VILJANEN, L. A survey on application level intrusion detection. Tech. rep., University of Helsinki, Department of Computer Science, 2005.

[35] WESTIN, A. F. *Privacy and freedom*. Atheneum, New York, 1967.

[36] WILSON, M., ET AL. The TrustCoM approach to enforcing agreements between interoperating enterprises. In *Interoperability for Enterprise Software and Applications Conference (I-ESA 2006)* (Bordeaux, France, Mar. 2006), Springer-Verlag.