

Data Flow Security Analysis for System-of-Systems in a Public Security Incident

Bo Zhou, Abdullahi Arabo, Oliver Drew, David Llewellyn-Jones, Madjid Merabti, Qi Shi
School of Computing and Mathematical Sciences
Liverpool John Moores University
Email: {B.Zhou, A.Arabo}@ljmu.ac.uk,
O.J.Drew@2007.ljmu.ac.uk, {D.Llewellyn-Jones,
M.Merabti, Q.Shi}@ljmu.ac.uk

Adrian Waller, Rachel Craddock, Glyn Jones,
Arnold K. L. Yau
Thales Research and Technology (UK) Limited
Worton Drive, Reading, UK
Email: {adrian.waller, rachel.craddock, glyn.jones,
arnold.yau}@thalesgroup.com

Abstract—In any system-of-systems there is the potential for interactions between systems to occur that affect the security of the overall system. This paper presents a scenario that highlights such potential problems. This scenario considers cooperation and interactions between organisations and systems that might occur in the context of a major public security incident involving multiple emergency services such as police, fire and ambulance services. Based on this we present a modelling tool able to highlight potential access violations that might occur through the transfer of data between multiple organisations, and suggest ways that vulnerabilities highlighted by the tool can be mitigated. Using the example scenario, we suggest how security and operational effectiveness can be achieved by applying safeguards to those areas that are vulnerable, while allowing the free flow of data between organisations where this is shown to be safe.

I. INTRODUCTION

We aim to develop a practical method to measure the security properties of a composed system. In many situations, various entities or organisations need to work together in order to provide a joint service or accomplish a complex task. These entities, i.e. the components in the composed system, could range from personal appliances in a small home network to government organisations involved in a massive event. For example, in a business meeting, representatives from different companies may form an ad-hoc network to allow exchange of business reports. In a military operation, multinational troops may need to share information about activities or opposing forces and along with Non-Governmental Organisations (NGOs) cooperate to achieve their shared objectives. Additionally, with the continuous development of computing and communication technologies, people's experience of both is growing ever closer to the notion of ubiquitous computing. We can expect to see this kind of cooperation between system components occurring both more widely and more casually as time progresses.

As dynamic, heterogeneous, interoperating systems become more widespread, one of the most important and difficult challenges is to measure the security properties of the composed systems [1]. Because the components belong to different systems and organisations, they have various requirements on information security. When composing them together, security policies are often inconsistent [2]. For example, one organisation may have a stricter security policy than others by enforcing a stronger encryption algorithm on external interfaces. A flaw in one system may

result in severe consequences to the entire composed system. There are lots of possibilities and aspects involved in security, and component composition only makes it more complicated [3].

This paper is primarily intended to set out a secure component composition scenario with a particular focus on response to potential emergency incidents that require inter-organisational co-operation. The scenario, along with its related threats and initial ideas about potential solutions are set out. An appropriate set of security tools has been devised, incorporating a number of novel techniques, especially in allowing security vulnerabilities to be highlighted in an immediate visual manner that can then be acted upon in real-world situations. This is reinforced by our scenario, which has been developed into a concrete, practical model. Although the scenario we develop here is relatively straightforward due to space limitations, we believe it highlights appropriate composition security tools that would apply in more complex scenarios, and application of these tools to provide a solution.

The remainder of the text is split into the following sections. In the next section, a brief survey of background material is presented. Section III presents our security analysis and what the modelling process is trying to achieve. In Section IV the process of modelling data access and flow between organisations is described. We present our scenario in Section V followed by the proof of concept modelling tool in Section VI. Finally we conclude and discuss future work in Section VII.

II. BACKGROUND

In previous work, researchers studying Secure Component Composition mainly focused on establishing the most appropriate model with the potential to formulate a property through some form of model-based analysis. Some examples include Non-interference [4] and Composable Assurance [5]. Non-interference can be considered as the 'original' composition property; it tries to describe the flow of information through a system. More specifically, it attempts to determine the situation in which sensitive data does not flow to an unauthorised level through a system, in order to ascertain whether secrecy in the system is being maintained. This is particularly important in relation to the discovery of covert channels in a system where data secrecy is paramount. Composable Assurance is also a composition property, although it takes a more generalised form

compared to non-interference, and indeed most other composition properties. Such properties can be characterised as satisfying the requirement of separability, whereby the security of a system is decided by analysing each component separately [5]. Composable Assurance on the other hand takes a different approach by considering both the properties of individual components and the interactions between components. Thus by knowing the security properties of individual components and the manner in which they interact, we can easily deduce the security properties of the composed system.

Although a considerable number of publications tackle the subject [6-9], this is done almost universally from a theoretical standpoint. Very little academic work can be found that attempts to apply the properties in any practical sense. This perhaps stems from the lack of a suitable practical formulation. Some work with a more practical focus has grown out of the interest in service-oriented and distributed computing technologies [10-12]. Our own previous work has resulted in the development of an effective analysis tool called MATTS (the Mobile Agent Topology Test System) to test and demonstrate the process of secure component composition [13].

However, these previous results have concentrated on interactions between individual systems with strictly defined properties. In a crisis situation, systems tend to be managed in larger, more ad-hoc federations. For example, the London Emergency Services Liaison Panel (LESLP) 'Major Incident Procedure Manual' [14] defines co-ordinated procedures agreed by the emergency services for use in response to a major incident. According to these procedures services will form into *Gold*, *Silver* and *Bronze* units, associated with *strategic*, *tactical* and *operational* functions respectively. These units may be comprised of multiple individuals and systems that cut across different emergency services. Units operate both independently and co-operatively, and the potential composition issues involved are considerable.

The issue of controlling data flow within such environments, and between organisations more generally is not itself new. However no single system has been able to provide a complete solution and a number of different approaches that attempt to resolve issues such as inter-organisational access control have been proposed. A common approach is through the use of logical domains, within which different access policies can be established [15-17]. Whilst providing a practical method of interoperation between organisations, these do not tackle the issue of data flow across domains and how to manage it. More flexible systems have been proposed to accommodate for example Web Services [18] and mobile agent systems [19]. Increasing attention in the areas of virtual organisations and inter-organisational workflow management have also resulted in more complex access control mechanisms for use between multiple organisations [20-22]. These allow for finer-grained control of access in a way that tackles differences between organisations, however they assume a uniform system layered on top of existing access control mechanisms (or mediating between them). A technology called OBSCURE™ developed by TRT (UK)

takes the approach of tying access control to data, rather than tying access control to systems, using encryption containers that protect data from unauthorised access [23]. While this provides a solution particularly appropriate for control of data flow in extraordinary and ad-hoc collaborations such as those described here, it provides a complete new access solution for all participating organisations, rather than dealing with the management of existing deployments.

We know of no similar approach for tackling the issue of modelling potential incompatibilities between differing access control mechanisms to determine potential data leakage or security issues. Some work has considered formal modelling of access control interactions, but largely in the areas of Role-Based Access Control (RBAC) role conflicts [19, 24] or vulnerabilities in access control protocols [25]. These are generally not appropriate in dynamic contexts and are specific to particular access mechanisms.

In contrast to these, our system is founded on the modelling of networks where problems may be dependent on the network structure, rather than being intrinsic flaws in the way individual access control mechanisms are applied. While in this paper we do focus on particular access control mechanisms, one of the principal aims of the work has been to allow flexibility, and as future work we intend to extend the system to highlight where the use of different access control mechanisms across different organisations may themselves be the source of vulnerabilities (or just as important: where they may not).

III. SECURITY ANALYSIS MODEL

Enforcing appropriate access safeguards is not just important from a security standpoint within an organisation; it can also be a legal requirement. Under EU Data Protection legislation [26], individually identifiable data collected by an organisation must also be protected¹. Safeguards must be in place to ensure it is only used for designated purposes, and can only be passed on to other organisations given certain criteria have been met. In a crisis situation, data being transferred may include medical information, credit card details or police records, and in these cases enforcing adequate safeguards is likely to be especially important. Yet at the same time, allowing data to be accessed unimpeded may be crucial from the perspective of effective response.

In such scenarios a variety of difficulties present themselves.

- The security systems and policies across organisations may be inconsistent, making it difficult to adequately protect data using existing access control configurations [27]. An example might be where one organisation focuses on security using the Bell-LaPadula model, and another on integrity using the Biba model.

¹ It should be noted that data processing relating to public safety, defence, State security and the enforcement of criminal law are not addressed by this legislation.

- Not all data channels between organisations can be controlled using technological or unassailable means. For example, many security breaches occur through physical transfers of data or word-of-mouth, which can be difficult to control [28].
- Networks and the flow of data between organisations rarely remain static, especially in crisis situations. Changes to data flows mid-operation can have a serious and unexpected effect on inter-organisation security characteristics [29].
- Any restrictions imposed for security reasons may have a consequent effect preventing data from going to where it's needed. Balance is always required in order to ensure security doesn't have a negative impact on operational effectiveness [29].

In order to mitigate such difficulties, we propose a system to model organisations and the data that flows between them.

The basis of the model is that nodes representing organisations can be placed in a virtual environment, properties assigned to these nodes and data flows of various types assigned between them. The resulting system and interactions can then be automatically analysed, either after the system has been configured or dynamically as communication links are assigned between the organisations. The modelling tool incorporates a scripting technique to allow various properties to be analysed in a flexible manner.

In the case where we wish to ensure data is transferred only to appropriate organisations, access criteria can be assigned to pieces of data within the model, along with the properties of organisations that may have access to the data. Organisations that may gain access through network transfers can be determined, and potential 'weak spots' in the system can be automatically identified. We will discuss what we mean by this more precisely later in this paper. Since data flows can be user-assigned, channels which may exist other than computer network links can also be included, such as those that may occur due to manual transfers where this is known to be a possibility. Moreover, changes to the network topology can be dynamically re-evaluated to highlight any changes to potential risk areas prior to making any changes to real structures.

In addition to describing the analysis process, we will also consider methods of re-structuring that can be used to mitigate dangerous or potentially risky interactions that may lead to data compromise.

IV. MODELLING INTER-ORGANISATIONAL DATA ACCESS

In order to understand data flow between organisations and potential access issues, we first present a rudimentary model of access control between organisations.

Consider a situation involving a set A of n organisations, where $A = \{a_1, a_2, \dots, a_n\}$. These organisations might be emergency services, hospitals, companies, volunteer groups and so on. For the purposes of the model, we assume that an organisation may be split into sub-units. Consequently the police may for example be represented by more than one element from A .

In our simplified model, we assume that all members of an organisation have access to data within that organisation. In general this assumption is too conservative; in fact access control procedures are likely to be in place within an organisation as well. However, as we will see later, in a crisis situation this may not be the case. Moreover, many commonly applied access control procedures can be modelled by splitting an organisation into multiple sub-units each unit having access to different data resources.

Consider some organisation a_i and piece of data d . The organisation a_i forms part of a network made up of elements of A . Let $A' \subseteq A$ be all organisations downstream from a_i ; that is, all organisations reachable in the network from a_i .

Let

$$r: D \rightarrow P$$

represent the access rules that map a piece of data to the people entitled to access it, and

$$m: A \rightarrow P$$

represent the mapping of an organisation to its members.

Then the general form of access policy we aim to ensure is that

$$r(d)^c \cap \bigcup_{a \in A'} m(a) = \emptyset,$$

where X^c represents the complement of the set X .

Using naïve set theory, this is equivalent to saying that

$$\bigcup_{a \in A'} m(a) \subseteq r(d).$$

In other words, all of the people with access to the nodes downstream from a_i , are within the set of users entitled to access the data d . This may seem a relatively straightforward requirement, but can be surprisingly important in a distributed environment.

We'll consider a specific case of this, where each piece of data is assigned a sensitivity level between 0 and 10 (with 0 being most sensitive), and each organisation is assigned an access level from 0 to 10 (with 0 being greatest access). In this case, every member of an organisation is authorised to access data of that level or higher. So, suppose a user u has authorisation level $\alpha(u)$ and a piece of data d has sensitivity level $\sigma(d)$, then u can access d iff $\alpha(u) \leq \sigma(d)$.

We can derive this scheme from the general case by stating that, for a piece of data d with sensitivity level $\sigma(d)$, we define

$$r(d) = \{p \in P: \sigma(p) \leq \sigma(d)\}$$

and for an organisation a with authorisation level $\alpha(a)$ we define

$$m(a) \subseteq \{p \in P: \alpha(p) \leq \alpha(a)\}.$$

Given the above definitions, we note that

$$r(d)^c = \{p \in P: \sigma(p) > \sigma(d)\},$$

and so using these interpretations, our earlier access rule becomes

$$r(d)^c \cap \bigcup_{a \in A'} m(a) = \emptyset$$

which we can guarantee if

$$\{p \in P: \sigma(p) > \sigma(d)\} \cap \bigcup_{a \in A'} \{p \in P: \alpha(p) \leq \alpha(a)\} = \emptyset,$$

which is equivalent to saying that

$$\alpha(a) \leq \sigma(d) \text{ for all } a \in A'.$$

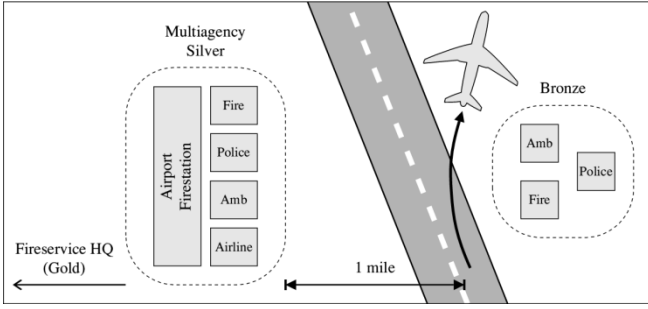


Figure 1. Post-incident scenario.

In other words, every downstream node has an authorisation level less than or equal to the sensitivity level of the data d (recall that a lower number represents greater access). We use this as a rule for the sake of demonstration; in reality a more complex rule is likely to be applied using the tool.

To understand this better, the following section considers an example of how these access rules may be applied and incorporated into our modelling tool in practice.

V. SCENARIO

In our example scenario we assume an incident has occurred in which a passenger plane has veered off the runway at a major international airport.

In the post-incident scenario, fire, ambulance and police units have arrived at the scene and set up their individual Bronze command units. Located approximately a mile away at the airport fire station, a multi-agency Silver command unit has been set up with representatives from the fire, police and ambulance services, as well as from the airline company involved in the incident. This Silver command would then report to the Gold command located at the regional police force HQ, however we will omit this aspect for the sake of clarity.

A rough representation of this scenario can be seen in Figure 1. The Bronze fire, police and ambulance services are collecting data about the incident at the scene. Within each control unit data is shared without restriction, as would be normal in such a situation. A data flow diagram of the situation would therefore look something along the lines of that shown in Figure 2. In this figure the authorisation level is shown below the node as a number between 0 and 10, where 0 is the highest authorisation level and 10 the lowest, and the node label is shown above the node. The details of each organisation are as shown in Table 1.

We assume we're only interested in the data stored by the Police on nodes a_1 and a_5 in our example, hence for the sake of simplicity there is no need to assign data sensitivity levels to nodes $a_2 - a_4$, $a_6 - a_7$.

With no connection between nodes a_3 and a_4 , the topology is split into two groups: $a_1 - a_3$ (Bronze) and $a_4 - a_7$ (Silver). Within these groups the data can flow freely between organisations without causing a violation of the policy rules. We can see this since all of the nodes downstream from a_1 that may receive the data with sensitivity level 6 all have authorisation level of 6 or above. Similarly all those downstream from a_5 have authorisation level of 8 or above.

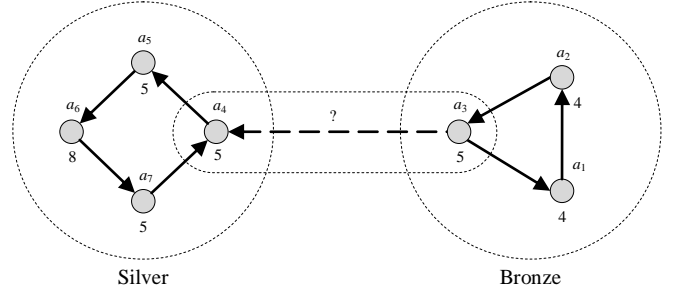


Figure 2. Multiple organisations communicating at different security levels.

Now consider a possible data link between the two fire service units a_3 and a_4 . If we were to look at the connection purely from the perspective of these two nodes in isolation, as would be the case with a simple negotiated connection, there would not on the face of it be any problem: both organisations have authorisation level 5 and can safely pass data between one another.

However, if we take a holistic view, with data flowing into a_3 from other nodes, adding the link may allow the police level 6 data from node a_1 to be transmitted to the airline node a_6 , which has only level 8 authorisation. Such data might represent investigation data the police are accumulating that might relate to a criminal investigation, and which it may be important that the airline not be given access to. A more complex overview analysis considering more than just each pair-wise connection individually must therefore be applied.

VI. MODELLING SYSTEM

In order to highlight such vulnerabilities, we have developed a system that allows the creation of topologies such as that shown in Figure 2, after which an analysis can automatically highlight potentially problematic areas. Figure 3 shows a screenshot of the system configured with the example topology. Each of the markers in the screenshot represents one of the organisations from Table 1 with Table 2 explaining the symbols used for these markers. When creating the link between nodes a_3 and a_4 the network is analysed and the potential vulnerability is highlighted by generating a report and indicating the source and destination nodes that cause the problem.

TABLE 1. NODE DETAILS.

Label	Organisation	Authorisation level	Data sensitivity level
a_1	Police	4	6
a_2	Ambulance	4	n/a
a_3	Fire Service	5	n/a
a_4	Fire Service	5	n/a
a_5	Police	5	8
a_6	Airline	8	n/a
a_7	Ambulance	5	n/a

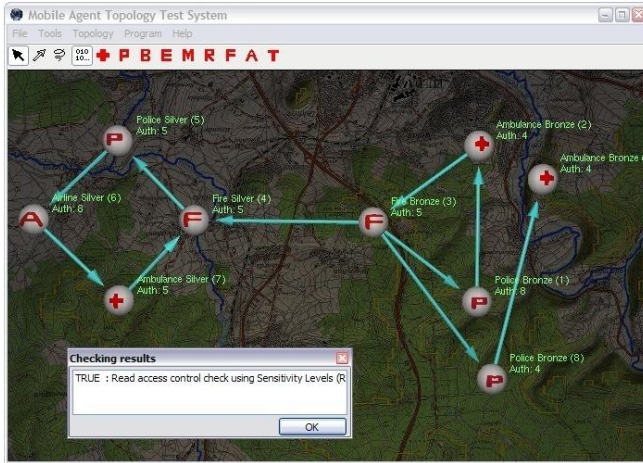


Figure 6. The adjusted network.

When we run our adjusted network through the modelling tool, we find it successfully passes the analysis as shown in Figure 6, where no organisations are highlighted as being vulnerable and the result indicates that the network is safe. This suggests there are no immediate vulnerabilities relating to data flow in the system.

B. Extensible Solution

The above demonstrates a simple use for our modelling tool in highlighting particular vulnerabilities related to data flow between multiple organisations. As an automated system, more complex scenarios can be tested easily, immediately identifying problems that might be missed through manual checks in a large network. The analysis process itself is also reprogrammable using an XML scripting technique. In addition to the access control properties above, we have also applied the technique to boundary property analysis, information filtering and covert channel discovery. We believe it may be usefully applied to other scenarios which we also hope to tackle in the future.

VII. CONCLUSIONS AND FUTURE WORK

The interaction between different organisations sending data between them can result in violations of access control policies. This possibility arises unless rights metadata is coupled tightly with the data itself, interacting organisations have closely compatible access control mechanisms and policies, and all organisations in a system take care to consider how data may be transferred beyond its immediate destination.

Even in time-rich situations, a secure system can be hard to achieve. However, in crisis situations involving dynamic interactions between multiple public and commercial organisations, the difficulty of providing adequate protection is substantially increased. Moreover, in such situations the need to ensure suitable safeguards are in place that do not hinder the ability of data to flow unimpeded to those organisations where it's needed is especially acute.

We have presented a modelling environment that can incorporate dynamic updates based on real network changes

and which is able to highlight vulnerable areas of an inter-organisation data network. The intention has been to show how such a tool can be used as a guide to centre attention on the areas that are of most importance, allowing adequate safeguards to be put in place. We demonstrated our approach and the implementation of our tool using the example of a hypothetical crisis situation; we also suggested ways to mitigate potential risks through the rearrangement of the network structure.

At present only a small collection of data flow related vulnerabilities can be highlighted using our tool, and in our example we used a somewhat simplistic set of data access policies. In future work we intend to consider a wider variety of policies, ideally incorporating real systems commonly used within organisations for the purposes of security. In the longer term, we hope to assess the effectiveness of the tool in allowing better control of data flow between organisations using real-world case studies.

While the work remains at a relatively early stage of development, we know of no other tools available for assessing real-world inter-organisation data flows in this way. Moreover, we believe our current implementation provides a good base to build on, allowing the application of useful techniques that go beyond security and operational effectiveness improvements in crisis situations.

REFERENCES

- [1] J. McLean, "Trustworthy software: why we need it, why we don't have it, how we can get it," in 30th Annual International Computer Software and Applications Conference COMPSAC 2006, Chicago, IL, USA, 17-21 September 2006.
- [2] A. Samuel, A. Ghafoor, and E. Bertino, "Context-aware adaptation of access-control policies," *IEEE Internet Computing*, vol. 12(1), pp. 51-4, January 2008.
- [3] L. Gong and X. Qian, "The complexity and composability of secure interoperation," in Proceedings of 1994 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, 16-18 May 1994.
- [4] P. Ryan, C. Mellon, J. McLean, J. Millen, and V. Gligor, "Non-interference, who needs it?," in 14th IEEE Computer Security Foundations Workshop (CSFW-14), Cape Breton, NS, 11-13 June 2001.
- [5] Q. Shi and N. Zhang, "An effective model for composition of secure systems," *Journal of Systems and Software*, vol. 43(3), pp. 233-44, November 1998.
- [6] R. Focardi and S. Rossi, "Information flow security in dynamic contexts," *Journal of Computer Security*, vol. 14(1), pp. 65-110, 2006.
- [7] J. Jurjens, "Composability of secrecy," in Information Assurance in Computer Networks. Methods, Models and Architectures for Network Security. International Workshop MMM-ACNS 2001, St. Petersburg, Russia, 21-23 May 2001.
- [8] H. Mantel, H. Sudbrock, and T. Krausser, "Combining different proof techniques for verifying information flow security," in 16th International Symposium on Logic-Based Program Synthesis and Transformation, LOPSTR 2006, Venice, Italy, 12-14 July 2006.
- [9] S. Tini, "Rule formats for compositional non-interference properties," *Journal of Logic and Algebraic Programming*, vol. 60-61, pp. 353-400, July 2004.
- [10] J. Buford, R. Kumar, and G. Perkins, "Composition trust bindings in pervasive computing service composition," in Proceedings. Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshop-PerCom Workshop 2006, Pisa, Italy, 13-17 March 2006.
- [11] I. Djordjevic, T. Dimitrakos, N. Romano, D. Mac Randal, and P. Ritovato, "Dynamic security perimeters for inter-enterprise service integration," *Future Generation Computer Systems*, vol. 23(4), pp. 633-657, May 2007.

- [12] M. Kolberg, E. Magill, D. Marples, and S. Tsang, "Feature interactions in services for Internet personal appliances," in 2002 International Conference on Communications (ICC 2002), New York, NY, 28 April-2 May 2002.
- [13] M. Merabti, Q. Shi, B. Askwith, and D. Llewellyn-Jones, "Secure Component Composition for Personal Ubiquitous Computing: Project Summary," Liverpool John Moores University, Liverpool December 2005.
- [14] LESLP, Major Incident Procedure Manual Manual, 7 ed: The Stationary Office, 2007.
- [15] D. Estrin, "Inter-organization networks: implications of access control requirements for interconnection protocols," in ACM SIGCOMM '86 Symposium on Communications Architectures and Protocols Computer Communication Review, Stowe, VT, USA, 5-7 August 1986.
- [16] D. C. Robinson and M. S. Sloman, "Domain-based access control for distributed computing systems," *Software Engineering Journal*, vol. 3(5), pp. 161-70, September 1988.
- [17] H. Hu, D. Chen, and C. Huang, "Securing role-based distributed collaboration system," in 2004 IEEE International Conference on Systems, Man and Cybernetics, SMC 2004, The Hague, Netherlands, 10-13 October 2004.
- [18] D. Zhang and J. Xu, "Securing instance-level interactions in web services," in 2005 International Symposium on Autonomous Decentralized Systems, ISADS 2005, Chengdu, Jiuzhaigou, China, 4-8 April 2005.
- [19] A. Omicini, A. Ricci, and M. Viroli, "An algebraic approach for modelling organisation, roles and contexts in MAS," *Applicable Algebra in Engineering, Communications and Computing*, vol. 16(2-3), pp. 151-178, August 2005.
- [20] P. Robinson, Y. Karabulut, and J. Haller, "Dynamic virtual organization management for service oriented enterprise applications," in 2005 International Conference on Collaborative Computing: Networking, Applications and Worksharing, San Jose, CA, United States, 19-21 December 2005.
- [21] M. H. Kang, J. S. Park, and J. N. Froscher, "Access control mechanisms for inter-organizational workflow," in Proceedings of the sixth ACM Symposium on Access Control Models and Technologies (SACMAT 2001), Chantilly, VA, United States, 3-4 May 2001.
- [22] N. Oikonomidis, S. Tcaciuc, and C. Ruland, "Provision of secure policy enforcement between small and medium governmental organizations," in Second International Conference on Trust, Privacy and Security in Digital Business, TrustBus 2005, Copenhagen, Denmark, 22-26 August 2005.
- [23] A. Waller, J. Lewis, R. Craddock, and G. Jones, "Secure Situation Awareness using Web Based Mashups," in The Navigation Conference and Exhibition (NAV 07), Royal Institute of Navigation, London, UK, 30 October-1 November 2007.
- [24] A. Schaad, V. Lotz, and K. Sohr, "A model-checking approach to analysing organisational controls in a loan origination process," in 11th ACM Symposium on Access Control Models and Technologies, SACMAT 2006, Lake Tahoe, CA, United States, 7-9 June 2006.
- [25] H. R. Shahriari and R. Jalili, "Modeling of network security-related behaviours using NVML," in Proceedings of INMIC 2004. 8th International Multitopic Conference, Lahore, Pakistan, 24-26 December 2004.
- [26] "Directive 95/46/EC of the European Parliament and of the Council," *Official Journal of the European Communities* 23 November 1995.
- [27] O. J. Tilak, R. R. Raje, and Z. Xukai, "Composing access control policies of distributed components," in 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, DASC 2006, Indianapolis, IN, United States, 29 September-1 October 2006.
- [28] M. White, B. Jennings, V. Osmani, and S. van der Meer, "Context driven, user-centric access control for smart spaces," in IEE Seminar on Intelligent Building Environments, Colchester, UK, 28 June 2005.
- [29] C. E. Phillips Jr., S. A. Demurjian, and T. C. Ting, "Information sharing and security in dynamic coalitions," in Proceedings of Seventh ACM Symposium on Access Control Models and Technologies: SACMAT 2002, Monterey, CA, United States, 3-4 June 2002.