State-of-the-Art in System-of-Systems Security for Crisis Management

Kashif Kifayat, David Llewellyn-Jones, Abdullahi Arabo, Oliver Drew, Madjid Merabti, Qi Shi
Liverpool John Moores University
Email: {K.Kifayat, 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
Thales Research and Technology (UK) Limited
Worton Drive, Reading, UK
Email: {adrian.waller, rachel.craddock, glyn.jones}@thalesgroup.com

Abstract— **Natural or man-made crises and disasters often bring large scale financial, environmental and human losses and can result in widespread damage to the information infrastructure. This affects the responding agencies' ability to communicate, with restrictions on the sharing of information making it difficult for them to provide emergency services to the population. Emergency ad hoc communication networks and systems can be established for use by the responding agencies, but these need to maintain an acceptable level of security. This paper discusses how to intelligently construct such an ad hoc network from existing assured systems, and how to ensure that the resultant composite system, or System-of-Systems (SOS), achieves a satisfactory level of information assurance. The paper also highlights possible threats and vulnerabilities to information and recommends possible solutions using SOS Security during crisis response to ensure that all organisations can securely and efficiently perform operational tasks during a crisis.**

Keywords- System-of-Systems Security; Information Assurance; Crisis Management; Asset Protection

I. Introduction

A crisis or disaster is a tragedy of a natural or man-made hazard that negatively affects society or the environment [1]. Such events range from localised crises, disasters affecting large areas of a nation, up to catastrophes affecting multiple nations. History has recorded huge financial and human losses after such events. For example, an earthquake in Pakistan in 2005 killed 100,000 people and caused $5 billion of estimated financial loss; Hurricane Katrina in 2005 killed over 1604 people in New Orleans, USA, and with an estimated financial loss of $25-$100 billion [2]. Irrespective of the scale of the event, it is typical for multiple agencies to be involved in the response. For the response to be effective, good communications and information sharing are required between these agencies, however, a consequence of the event is usually the loss of an effective information infrastructure, due to damage, overload, or deliberate action (deliberate actions may intentionally affect the infrastructure capability, e.g. denial of service attacks, or may accidentally affect the infrastructure capability, e.g. excessive security). The result of such a loss means that critical information and communication systems might consequently become unavailable, especially if significant parts of the communication systems of cities or countries are affected. It is therefore important to ensure that the agencies involved in the response are able to establish effective communication networks at short notice, in difficult environments.

Dynamic ad hoc communication networks and systems can be established between the responding agencies, although such communication technology is not widely used at the current time, with deployments being mainly for research purposes [3]. In the crisis management application, it is likely that a System-of-Systems (SOS) approach will be adopted to produce such a network, since each agency will have its own communications networks and systems, and ideally it should be a simple matter to rapidly connect these separate systems together in an assured way. However, in reality things are never this simple, for a variety of reasons:

- Assurance currently takes time to establish, and there are many interrelated security issues which could create delay or loss of critical information. In crisis management, delays have large consequences.
- Crisis management includes the need to use whatever is available at the time, the high likelihood that the situation will change rapidly, and the unpredictable and unforeseen way in which changes will occur.
- Security and assurance are essential to protect sensitive data and privacy, but in crisis response, any restrictions imposed for security reasons may have the effect of preventing information from going where it's needed. Balance is therefore required in order to ensure security doesn't have a negative impact on operational effectiveness [4].
- SOS Security and Assurance involves not only ensuring that each component system is secure and assured (this can be established prior to a crisis occurring), but also ensuring that the composed system is secure and assured (the composed system is only created once the crisis response is in progress, and the exact composition may not have been known in advance). Composed systems typically possess undesirable emergent properties, so composition assurance of the resultant system is therefore required.

Therefore, SOS Security, whereby security properties are considered based on the composed system rather than just components in isolation, should be an essential part of the crisis management process in order to allow secure communication without incurring delays.

Here, SOS Security Composition is a key issue, which refers to the process of combining distinct systems or components with different security properties to form a whole new secure system for a specific task. The focus of this paper is on the composition assurance layer, and on how composition can be performed intelligently to achieve a known and acceptable level of assurance using the proposed tools and techniques described in the following sections. Use of these tools and techniques means that constructing the composed system is not simply a case of putting together whatever is available and hoping for the best. Instead, by composing the system intelligently, a balance between the security assurance needs and the crisis management functional requirements can be achieved. Building on known and assured properties of individual components allows the establishment of known and assured properties of potential combinations. The most appropriate combination can then be chosen and its configuration improved to get the best result. Note that the issues discussed above are not restricted to SOS Assurance or to the crisis management application. Similar issues arise in more general systems engineering, especially where the system needs to be designed for diverse, and potentially changing, functional and security requirements. Therefore the tools and techniques referred to in this paper should be applicable much more generally.

The remainder of the paper is split into the following sections. In the next section, a brief survey of background material is presented. Section III describes the importance of SOS Security and our project work. Section IV presents the research challenges in crisis management in the context of SOS Security. Finally we conclude and discuss future work in Section V.

II. Related Work

Previous work in secure component composition has 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 [5] and Composable Assurance [6]. 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 [6]. Composable Assurance, on the other hand, takes a different approach by considering both the properties of individual components and the interactions between components. In the case of security properties that satisfy the requirements of Composable Assurance, if we know the properties of the 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 [7-10], 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 [11]. 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, and which we will consider in greater detail shortly [12].

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 [13-15]. While 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 this, for example technologies such as OBSCURE® developed by TRT (UK). This 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 [16]. This provides a solution particularly appropriate for control of data flow in extraordinary and ad hoc collaborations such as those described here, however, its focus is on providing a completely new access solution for all participating organisations, rather than dealing with the management of existing deployments [17].

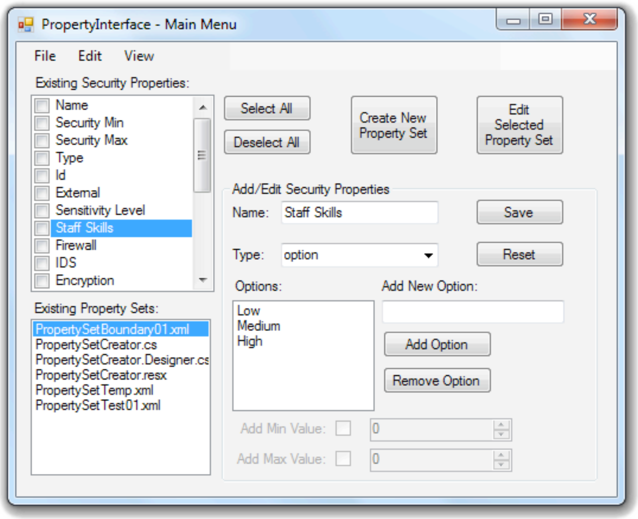
III. System–of-Systems Modelling and Analysis Tools

There is a great need for software tools able to create different possible scenarios, establish communication networks between different organisations, assign security properties to organisations (systems) and analyse the security of different systems using their security properties. All dynamic properties and the nature of the crisis should be added to such software to realistically analyse and identify possible security issues. This could help emergency service departments to understand the identified problems and to pre-plan in order to avoid any damage caused by them.

Developing a software tool which can help to design a crisis scenario with different departments (systems) to develop a communication network, allow them to be connected in any manner, and allow unconstrained changes in their position presents a number of challenges. In particular, it is important that such software should be able to analyse the security properties and communication links of all the nodes in the scenario and identify possible threats and vulnerabilities.

In order to test various crisis management scenarios, and apply SOS Security techniques within these scenarios, we developed the MATTS suite of software tools. MATTS consists of two main applications: a composition client and a MATTS server. The client-side software can represent any organisation that could participate in the crisis management process. We consider these organisations (police, fire service, medical, etc.) to be equipped with communication devices such as PDAs, smart phones or laptops. Furthermore, each of these clients has a set of security properties and policies established according to the security needs of their respective organisations. The security properties (e.g. which firewall device is running; what encryption algorithm is being used; the sensitivity level of the device *etc.*) of organisations can differ from one to another. To tackle this, we have developed a property interface tool (as shown in Figure 1) that allows node properties to be defined and saved in a simple XML format. Using the interface in Figure 1, the user is able to select security properties (on the left portion of the interface) or even create a new property set, as well as loading properties from existing property set files (as shown in the lower left hand corner of the interface). These files can then be automatically transferred between nodes to help identify the level of security in a specific scenario.

The security policy describes the process of how, when and with whom information can be shared, and under which conditions and what the appropriate actions are when discovering threats or vulnerabilities. Technically the security properties of every organisation are stored in a policy XML file. These policy files and the data flow topology are used to determine the overall security status.



Existing Security Properties:

- ☐ Name
- ☐ Security Min
- ☐ Security Max
- ☐ Type
- ☐ Id
- ☐ External
- ☐ Sensitivity Level
- ☐ Staff Skills
- ☐ Firewall
- ☐ IDS
- ☐ Encryption

Existing Property Sets:

- PropertySetBoundary01.xml
- PropertySetCreator.cs
- PropertySetCreator.Designer.cs
- PropertySetCreator.resx
- PropertySetTemp.xml
- PropertySetTest01.xml

Add/Edit Security Properties

Name: Staff Skills

Type: option

Options:

- Low
- Medium
- High

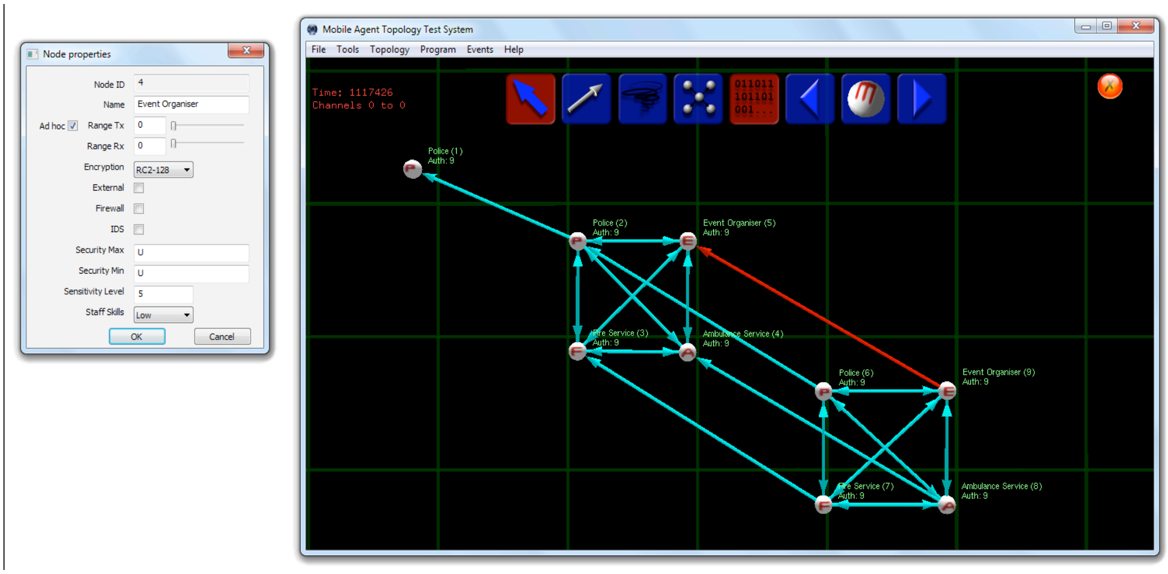
Add New Option:

Add Min Value: ☐ 0

Add Max Value: ☐ 0

Figure 1: Property Interface for defining node properties.

The main analysis runs on the server, once all knowledge about client nodes properties, connectivity (links with neighbouring nodes) and integration details has been transferred in XML files from the clients. As mentioned in the introduction, all this information is necessary during composition analysis. The process of transferring this data begins as soon as the client has connected to the network. The interface for this server-side software is shown in Figure 2. The figure shows nodes from various interconnected organisations. In the upper right corner of the interface the 'X' indicates a security problem has been identified in the network that involves multiple nodes simultaneously. This provides a notification, but we are currently working on systems to provide richer feedback to the user (e.g., highlighting the affected nodes) The dialogue on the left in Figure 2 shows how the user can modify the properties of a node in order to manage the model. This also provides a means of resolving security issues by making suitable changes to node properties (e.g., by increasing staff skills assigned to the node). The analysis is directed by an XML script file which describes the process to be followed for each property tested against. The MATTS tools are able to interpret this script and follow the process, ultimately resulting in a verification or refutation of the property as it applies to the configuration of the services. Assuming a suitable script file is being adhered to; the most important information needed by MATTS to undertake its analysis is an overview of the dependencies or links between the components of a system.



Node properties

Node ID: 4
Name: Event Organiser
Ad hoc ☑ Range Tx: 0
Range Rx: 0
Encryption: RC2-128
External ☐
Firewall ☐
IDS ☐
Security Max: U
Security Min: U
Sensitivity Level: 5
Staff Skills: Low

```
Time: 1117426
Channels 0 to 0
```

Figure 2: Network established at server using different client organisations.

During the analysis, it often transpires that additional information is needed to complete the analysis and provide an accurate result. This is because composition results invariably depend on both the composition structure and the specific properties of individual services. These latter properties may be queried at any time during the analysis.

The result of the composition analysis stage identifies whether the security property being tested for is satisfied or not. The proposed tool gives freedom to the user to model all possible scenarios using different numbers of nodes with different security properties, and to run different vulnerability tests on the modelled scenarios. We have successfully tested "Data Flow Security" and "Boundary Check" vulnerabilities using MATTS and some interesting lessons have been learnt. Further detail can be found in [17][22]. Our aim is for the operator to be able to make use of the results from the tool and lessons learned from the secure composition analysis to design a system that will be secure. Rather than just showing the user what security problems could occur during composition in a modelled scenario, we believe the proposed tool can guide the user to a better and more efficient solution for secure systems composition.

Other examples of security properties that we have considered include whether a particular configuration is liable to trigger a buffer overrun vulnerability, or whether it is liable to cause an access violation. Such further properties may be tested by creating additional scripts, and the results are important for interoperability security, since they can tell us whether a particular configuration of services will be safe to deploy and use. At present, the system can be used as a 'warning' indicator, to tell whether potential security vulnerabilities are present in a system. In future development we hope to produce a 'pro-active' version that not only establishes possible problems, but also provides dynamic solutions, e.g. through the generation of intermediary services that marshal data safely between otherwise potentially vulnerable services. Next we present some examples to show how MATTS is able to check for security weaknesses.

In our example scenario we assume a major incident has occurred at an event that involves all of the major emergency services and that the Bronze-Silver-Gold command structure developed by the UK Metropolitan Police [17] is being used. This provides a cross-service command structure tied to the location of security personnel, whereby Bronze and Silver command centres are set up on-site for direct and strategic actions respectively, with overall control and monitoring of events at a Gold command centre located away from the incident. This structure, which can be seen reflected in Figure 2, has relevance from a security perspective, since different command units will require access to different information resources. In the post-incident scenario, fire, ambulance and police units have arrived at the scene and set up their individual Bronze command units, with representation from the event organiser involved in the incident. Located nearby at a local fire station, a multi-agency Silver command unit has been set up with representatives from the fire, police and ambulance services, as well as the event organiser. This Silver command would then report to the Gold command located at the regional police force headquarters.

The Bronze fire, police and ambulance services collect data about the incident at the scene. Within each control unit data is shared without restriction, as would be normal in such a situation.

Using MATTS, networks can be tested prior to deployment in order to highlight any vulnerable areas. Should a problem be discovered, procedures can be implemented to mitigate it. Additionally, the system can be set to reflect real network structures, changing dynamically as the network changes and highlighting problems in real time as it does so. In this example it might be deemed acceptable for the emergency services at the scene to liaise with the event organiser, and for them to liaise similarly within the Silver command unit, based on the reasoning that the emergency services have processes in place to ensure that sensitive information isn't provided to the event organiser without suitable authorisation. However, similar safeguards may not be in place for data that is passed directly between the representatives of the event organiser at the scene, and the event organiser at the Silver command unit. For example, the event organiser at the scene may not have procedures in place for labelling data appropriately. Using a suitable policy reflecting this requirement, the software might therefore identify the connection between the event organiser at the scene and their representative at the Silver command unit as being problematic, since it presents a potential means of 'laundering' the authorisation metadata from sensitive information. Figure 2 indicates how this might be flagged up, through highlighting of the problematic link.

This example shows the benefits of such an analysis tool able to identify problems in this way, especially given that it can be very hard to predict how the events in a crisis will unfold. Using MATTS we can model different types of scenario, including those which evolve dynamically, in order to find security vulnerabilities during actual operation in a crisis management situation. We believe the tool is likely to be useful for emergency services and crisis management organisations to understand all possible threats and vulnerabilities in an effective way. However, research in this area is new and requires considerable further work. In the next section we describe some of the remaining research challenges.

IV. Research Challanges

In crisis management operations an emergency ad hoc network may be established to share information between emergency service organisations to enable them to provide basic services. However, an ad hoc or other form of communication network could face many security and non-security challenges impacting on its ability to provide good, safe and reliable information at any time. In this section we describe some of the issues and challenges which could be faced during a crisis.

A. Data Availability

During crisis management operation, data availability could be disturbed using denial-of-service attacks, or excessive security may prevent or severely limit information flow between systems. Both cases could result from an inability to assess the assurance in a composed system correctly and may result in the lack of precise and timely information, leading to a change in the outcome of an ongoing crisis to be worse than might otherwise be the case. In other words, it can result in an inability to carry out some of the main crisis management steps of the pre-incident, post-incident and post-occurrence phases [18].

The process whereby a lack of, or unavailability, of data diverts the crisis towards a worst-case scenario is referred to as an information crisis [19]. This can also happen due to limited resources. Therefore it is crucial that all possible means (security and non-security) are used to prevent an information crisis from occurring. In emergency cases data availability is highly important; for example during a flood scenario we could imagine the case where somebody is suffering from a serious health condition and needs urgent medical help. Any delay during communications, incorrect data exchange or unavailability of data could risk lives. Therefore all security and non-security risks should be considered in order to provide a high level of data availability. All of the worst cases in different scenarios with respect to data availability should be considered.

Tools like MATTS are needed with the capability to check the entire network and available resources. Any sign of where potential communication breakage could happen or risk of where data could be lost should be identified, and also possible solutions or alternatives suggested in order to increase information availability.

B. False Information Hazards

In different types of scenario, false information hazards can occur. Any possible action on false information could result in wasted resources. For example, in a given scenario an adversary could join the network as a representative of an organisation and send false emergency alerts to gather other nodes to that location, in order to help an adversary in achieving their objective. For example this could be used as a means to aid robberies or launch possible attacks on weak points of a network.

C. Data Protection in Crisis Management

According to US and UK law (Privacy Act 1974 [20] and Data Protection Act 1998 [21] respectively) information must be protected during crisis management. During a crisis (small or large-scale) the management of different types of organisations could be involved which share different types of information. For example, in our scenario from earlier, individuals' personal information is likely to be collected and shared between different organisation categories. It is important to ensure that personal data is secure, accurate and available, and that it is covered by data protection principles that must be applied to personal information as follows [21]. Personal data must be:

1. Fairly and lawfully processed.
2. Obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Adequate, relevant and not excessive.
4. Accurate and up to date.
5. Not kept for longer than is necessary.
6. Processed in line with your rights.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Not transferred to other countries without adequate protection.

Possible risks should be identified which might violate data protection law. During the crisis management process, communication devices will collect information and therefore all of the above principles should be satisfied. These principles can form part of a security policy. In relation to our scenario, without due care there could be a high risk of violation of the Data Protection Act.

D. Asset Protection

In crisis management operation, scenario information is an important asset and plays a very important role. As discussed, information security is the fundamental requirement which is based on three well known components: Confidentiality, Integrity and Availability (CIA). Besides security requirements there are other important elements which play an important role to gather real-time scenario information such as personnel, hardware (laptop, mobile phone, etc.), software, communication networks and data. Interestingly all these elements are integrated, and dysfunction of any elements could cause serious loss or damage to an enterprise, institution or individual. For example, physical damage to personnel or a communication device may stop communication with the rest of the network, which could block the important information. Such information might be critical and directly help in saving lives.

All organisations involved in crisis management should identify assets, their importance and possible related risks in different scenarios. Possible precautions should be defined in order to prevent any damage to these assets. For example, in cases where personnel are unable to handle or accurately operate their devices (PDA, laptop, mobile, etc.) due to medical conditions, devices should automatically change their security policies and take appropriate action, informing the relevant organisation of the change.

E. Confidentiality and Authentication

During crisis management it is important to maintain confidentiality of different types of information. Information that might be widely shared within the network, but which may nonetheless be sensitive, could include details about how many and which organisations are involved in the crisis management; how many nodes are participating inside a network; where nodes are operating (i.e. their geographical locations) and so on. If such details became available, they might help adversaries to plan different types of attack or achieve some specific objectives. As discussed earlier, during the crisis management process the communication network is dynamic (ad hoc) and nodes from different organisations frequently join and leave the network. Furthermore, a large amount of sensitive information is shared between the various organisations. Therefore all new nodes should be accurately authenticated in order to reduce the risk of possible attack.

V. Conclusion

In this paper we have described the importance of information technology and SOS Security during crisis management operations. We described SOS analysis and our software tool which is aimed at identifying possible threats and vulnerabilities in crisis management networks. To aid our understanding we have drawn on a scenario to demonstrate this work. We also highlighted some security related issues which could have a strong impact on operational activities. Finally, we presented issues and research challenges (data availability, privacy and asset protection) in SOS Security during crisis management.

Acknowledgement: These results form part of a project co-funded by Thales Research and Technology (UK) Ltd. and the School of Computing and Mathematical Sciences at Liverpool John Moores University. Part of the work has been funded through the EU 7th FP Funded Aniketos Project (Project reference: 257930).

References

[1] E. L. Quarantelli, "Where We Have Been and Where We Might Go," in *What Is A Disaster*, E. L. Quarantelli, Ed. London: Routledge, 1998, pp. 146-159.

[2] C. Wattegama, "ICT for Disaster Management," United Nations Development Programme-Asia-Pacific Development Information Programme 2007.

[3] N. Glombitza, M. Lipphardt, H. Hellbruck, and S. Fischer, "FRED - An application for a real-life large scale multihop ad hoc network," presented at 5th Annual Conference on Wireless on Demand Network Systems and Services (WONS 2008), Garmisch-Partenkirchen, Germany, 2008.

[4] C. E. Phillips, S. A. Demurjian, and T. C. Ting, "Information sharing and security in dynamic coalitions," presented at Proceedings of Seventh ACM Symposium on Access Control Models and Technologies: SACMAT, Monterey, CA, United States, 2002.

[5] P. Ryan, C. Mellon, J. McLean, J. Millen, and V. Gligor, "Non-interference, who needs it?," presented at 4th IEEE Computer Security Foundations Workshop (CSFW-14), Cape Brenton, NS, 2001.

[6] Q. Shi and N. Zhang, "An effective model for composition of secure systems," *Journal of Systems and Software*, vol. 43, pp. 233-244, 1998.

[7] H. Mantel, H. Sudbrock, and T. Krausser, "Combining different proof techniques for verifying information flow security," presented at 16th International Symposium on Logic-Based

Program Synthesis and Transformation, LOPSTR, Venice, Italy, 2006.

[8] R. Focardi and S. Rossi, "Information flow security in dynamic contexts," *Journal of Computer Security*, vol. 14, pp. 65-110, 2006.

[9] J. Jurjens, "Composability of secrecy," presented at Information Assurance in Computer Networks. Methods, Models and Architectures for Network Security. International Workshop MMM-ACNS, St. Petersburg, Russia, 2001.

[10] S. Tini, "Rule formats for compositional non-interference properties," *Journal of Logic and Algebraic Programming*, vol. 60-61, pp. 353-400, 2004.

[11] J. Buford, R. Kumar, and G. Perkins, "Composition trust bindings in pervasive computing service composition," presented at Proceedings. Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshop-PerCom Workshop, Pisa, Italy, 2006.

[12] 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.

[13] H. Hu, D. Chen, and C. Huang, "Securing role-based distributed collaboration system," presented at IEEE International Conference on Systems, Man and Cybernetics, SMC, The Hague, Netherlands, 2004.

[14] D. Estrin, "Inter-organization networks: implications of access control requirements for interconnection protocols," presented at ACM SIGCOMM '86 Symposium on Communications Architectures and Protocols Computer Communication Review, Stowe, VT, USA, 1986.

[15] D. C. Robinson and M. S. Sloman, "Domain-based access control for distributed computing systems," *Software Engineering Journal*, vol. 3, pp. 161-70, 1988.

[16] A. Waller, J. Lewis, R. Craddock, and G. Jones, "Secure Situation Awareness using Web Based Mashups," presented at The Navigation Conference and Exhibition (NAV 07), Royal Institute of Navigation,, London, UK, 2007.

[17] B. Zhou, A. Arabo, O. Drew, D. Llewellyn-Jones, M. Merabti, Q. Shi, A. Waller, R. Craddock, G. Jones, and K. L. Y. Arnold, "Data Flow Security Analysis for System-of-Systems in a Public Security Incident," presented at The 3rd Conference on Advances in Computer Security and Forensics (ACSF 2008), Liverpool, UK, 2008.

[18] R. J. Craddock, "Crisis Management Models and Timelines," Thales Research and Technology (UK), White Paper TRT060601 22 June 2006. 2006.

[19] E. Aarhold and O. Berg, "Information Grid in Support of Crisis Management," ADA467178, Jun 2002 2002.

[20] "The Privacy Act of 1974", U.S.C. 552a, http://www.justice.gov/opcl/privstat.htm (November 2010)

[21] "The Data Protection Principles", Schedule 1 of the Data Protection Act 1998, http://www.legislation.gov.uk/ukpga/1998/29/contents (November 2010).

[22] B. Zhou, O. Drew, A. Arabo, D. Llewellyn-Jones, K. Kifayat, M. Merabti, Q. Shi, R. Craddock, A. Waller, G. Jones, "System-of-Systems Boundary Check in a Public Event Scenario", 5th International Conference on Systems of Systems Engineering (SoSE 2010),Loughborough, UK, 22-24 June 2010. Winner of the Conference Best Paper Award.