Modelling E-business Security Requirements: Developer and Client Expectations

Michael N Johnstone
Donald C McDermid
John R Venable*

School of Computer and Information Science
Edith Cowan University
*School of Information Systems
Curtin University of Technology
Perth, Western Australia
Email: {m.johnstone, d.mcdermid}@ecu.edu.au
venablej@cbs.curtin.edu.au

Abstract

User perceptions of e-business systems' security are, at best, that such systems are not as secure as more traditional ways of doing business. As security is now considered to be so crucial to e-Business success, the question of how security requirements are identified and how users can become involved in identifying security requirements for their organisation has become all the more important. This paper describes some of the results of an interpretive study into requirements elicitation using the business rules diagram (BRD) method. An interpretive analysis focusing on security provides some understanding of how users can contribute to the process of security requirements specification. In the study, users became active users of the BRD method and diagram in many requirements engineering areas, including security. A model of cognition is proposed that explains the behaviour that resulted during the study. The model posits two distinct modes of reasoning, formal and informal, and shows how movement occurs between the modes as roles and expectations change over time.

Keywords:

Electronic Business, Security, Requirements Modelling, Requirements Elicitation

Introduction

The adoption of the Internet for e-business is hindered by the reticence of some consumers to take part in transactions due to a perceived lack of security. These concerns are also evident in businesses anxious to ensure that the integrity of their transactions is maintained. A global survey by Ernst & Young (2001) found that 66% of the firms surveyed consider the lack of security or privacy to be the biggest inhibitor to furthering their e-business goals.

A major issue for the design and implementation of web-based systems is how to deal with the issue of maintaining transaction integrity whilst operating in a stateless environment. However, this issue need not be a concern during requirements elicitation and engineering.

Another issue for web-based systems development is how to specify web-based security requirements in a manner that both involves users and allows them to be comfortable with the process and tools used. The authors are particularly interested in the prospects for the use of tools and methods (especially diagrams) as a communication mechanism between systems analysts and users. Diagrams are a central part of many IS development (ISD) methodologies. However, we believe that the way diagrams are actually used is an area that has not been investigated in sufficient detail.

From our perspective, it is useful to have a method that integrates security with other aspects of requirements. The Business Rules Diagram (BRD) developed by McDermid (1998) is a state-based requirements elicitation and engineering method that can be used to engineer the requirements of all functional aspects of a system, including its security mechanisms.

The results of the study reported in this paper attempt to address the above issues by exploring and conceptualising how system developers and their clients model e-business processes. The interpretive research described in this paper studied the shared use of the BRD (McDermid, 1998) by end-users and analysts in eliciting and modelling the requirements for a subscription-based e-journal publishing system. As part of this effort, the security-oriented concerns and elicitation and modelling behaviours of end-users became apparent and are reported in this paper.

The study reported here focused on the BRD in particular. It is not intended to compare the BRD with other approaches, which requires a different form of study. While space limitations prevent a detailed discussion, Johnstone and McDermid (2001) compared the BRD method with the UML at the analysis level (in terms of the SDLC), with the result that each method has strengths in different areas and neither method is ontologically complete.

While focused on the BRD, with this paper we also propose more detailed theory about the use of diagrams in order to improve requirements specification in general and e-business security requirements specification in particular. We provide some evidence of the validity of the theories espoused for the BRD, but other studies will be needed to investigate whether the theory applies to other methods.

The Role of Diagrams in Systems Development

There is a range of web design methods described in the literature, for example RMM (Isakowitz *et al.*, 1995), OOHDM (Schwabe and Rossi, 1995) and the Scenario-based approach of Lee *et al.* (1999). These methods, however, focus on the design of EC systems and not on requirements elicitation.

During requirements elicitation and engineering, diagrams serve two main roles. Diagrams provide a vehicle for external processing (communication) and they facilitate reasoning or internal processing (through mental models). The use of mental models is well documented e.g. consider the well-known metaphor of Johnson-Laird (1983, p10) described thus: "*human beings understand the world by constructing working models of it in their minds. Since these models are incomplete, they are simpler than the entities that they represent. In consequence, models contain elements that are merely imitations of reality - there is no working model of how their counterparts in the world operate, but only procedures that mimic their behavior.*"

As communication mechanisms, diagrams document claims about some situation that the diagrams model, which are then used for various purposes by the receiver of the diagrammatic information. In Information Systems Design, a diagrammatic model can describe to clients what an analyst has learned and act as a vehicle for feedback about the validity or correctness of that learning. The client is then expected to confirm or disconfirm the validity of the diagrams. Diagrams are also used to communicate the results of work in one phase of the system development life cycle to others who do further work in later phases e.g. an entity-relationship diagram may be passed on from an analyst to a database designer. The different uses and users of diagrams in Information Systems Design present problems in the design of diagramming techniques, as described by Moody *et al.* (1995).

Larkin and Simon (1987, p98) present several reasons for the superiority of diagrams over other forms of representation, namely that diagrams can group together all information that is used together; diagrams typically use location to group information and diagrams automatically support a large number of perceptual inferences. It is this last point that is of most interest in this research.

Diagrams and systems of diagrams combined with other model representations are used to facilitate reasoning about requirements during ISD. Commonly, they are checked for consistency and completeness, i.e. uncovering inconsistencies and gaps in requirements elicited from users. Systems analysts usually perform these tasks (Bostrom and Thomas, 1983). However, reasoning with diagrams is not limited to systems analysts. It has been proposed that users may also use diagrams to reason about systems as an aid to discovering and documenting requirements (DeMarco, 1978). This requires either the development of notations that are so intuitive that only brief explanation is necessary – or training of users in how to make use of the diagrams.

Research Aims

The research in this study was part of an action research programme designed to enhance and evaluate the Business Rules Diagram (BRD) method (McDermid, 1998). The work described here reinterprets data collected during a study reported in Johnstone *et al*. (2000), which was originally conceived to investigate the qualities of BRDs including analysis of e-business systems.

The development of the BRD method is consonant with the re-emergence of business process modelling as a tool for understanding the functions within organisations. That, coupled with the necessity to maintain state information in today's web-based transactions, suggests that process-oriented techniques (such as the BRD) may be useful in modelling e-business systems.

Summary of the BRD Method

A recent approach used to capture business rules is that of McDermid (1998). This approach, called the Business Rules Diagram (BRD) method, utilises a state-based model which has a notation similar to, but more powerful than, flowcharts. The BRD is used for eliciting and analysing the requirements for an information system to support a notional human activity system (Checkland, 1981). As an information systems development approach, the BRD method is positioned between the use case approach of Jacobson *et al*. (1992) and more complex object models. The steps used in the method to create a complete BRD are defined as:

- identify candidate business rules;
- identify candidate events and signals;
- identify candidate objects;

- construct Object Life Histories (OLHs);
- construct User Business Rule Diagram (UBRD);
- construct Business Rules Diagrams; and
- construct Event Specification Tables (ESTs).

A business rule, as defined by McDermid (1998), contains five explicit constructs, these being states, events, conditions, signals and blobs (see, for example, figure 1). Connected combinations of these constructs make up a User Business Rule Diagram (UBRD). States (circles) reflect the status of a system or one of its components. For example, a visitor to an electronic journal web site might traverse the states visiting, subscribed and unsubscribed. Events (rectangles) are actions carried out internally by the organisation. Conditions (diamonds) define the criteria by which objects of interest in the business move from one state to the next as events take place and are sometimes known as "if-then rules" in other systems. Signals (arrows) either enter or leave the human activity system. Signals that enter the system typically initiate activity within the system and are called triggers (see T5 on figure 1). Signals that leave the system serve to inform those outside the system boundary about what has occurred inside the system and are called messages (see M11 on figure 1). The last construct is the Harel blob (Harel 1988), which encapsulates other constructs and is used to model selection or simultaneous action. The use of the blob construct in the full BRD distinguishes the BRD from the UBRD (a precursor diagram).

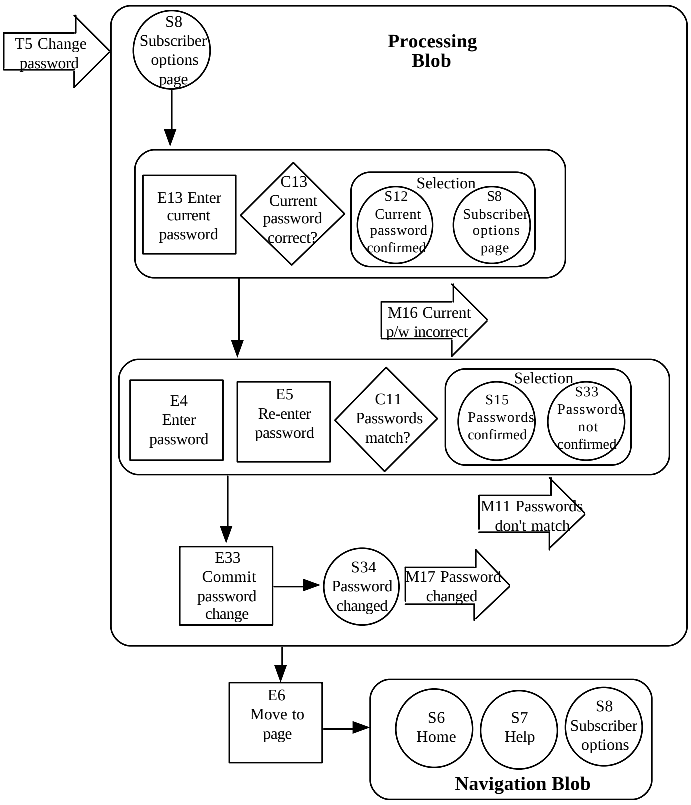
T5 Change password
S8 Subscriber options page
Processing Blob
E13 Enter current password
C13 Current password correct?
Selection
S12 Current password confirmed
S8 Subscriber options page
M16 Current p/w incorrect
E4 Enter password
E5 Re-enter password
C11 Passwords match?
Selection
S15 Passwords confirmed
S33 Passwords not confirmed
M11 Passwords don't match
E33 Commit password change
S34 Password changed
M17 Password changed
E6 Move to page
S6 Home
S7 Help
S8 Subscriber options
Navigation Blob

Figure 1: Business Rules Diagram for "Change Password" Use Case.

Research Context

This study describes a project involving the development of a business to consumer (B2C) subscription-based electronic commerce system for a business group in a large Australasian University. The domain was that of electronic publishing. A small project team was established comprising a group of two clients and a trained business analyst (one of the researchers) acting as the group facilitator. The researcher was skilled in the use of the method. The first client (henceforth referred to as "Client F") was a web site developer with experience in paper-based publishing but no training in any formal (structured) systems development method. The second client (Client G) was an academic with a strong interest in web site development but no training (formal or informal) in systems development methods.

Both clients were taught the notation and stages of the BRD method and then attempted to model the problem situation, aided by the researcher/analyst/facilitator. The group generated 84 business rules across twelve functional areas covering many aspects of journal publication (both traditional paper-based and electronic). The web site provides a way for non-subscribers to browse abstracts and journal tables of contents and allows them the option of subscribing via credit card across the Internet or other, more conventional means. The site also gives subscribers on-line access to full articles as well as the opportunity to provide an on-line commentary on selected articles.

The process of the entire action research study is depicted in figure 2. The ISD activities studied are shown with ovals. The researcher activities are shown with rectangles. Softboxes (rounded rectangles) show the evidence collected.

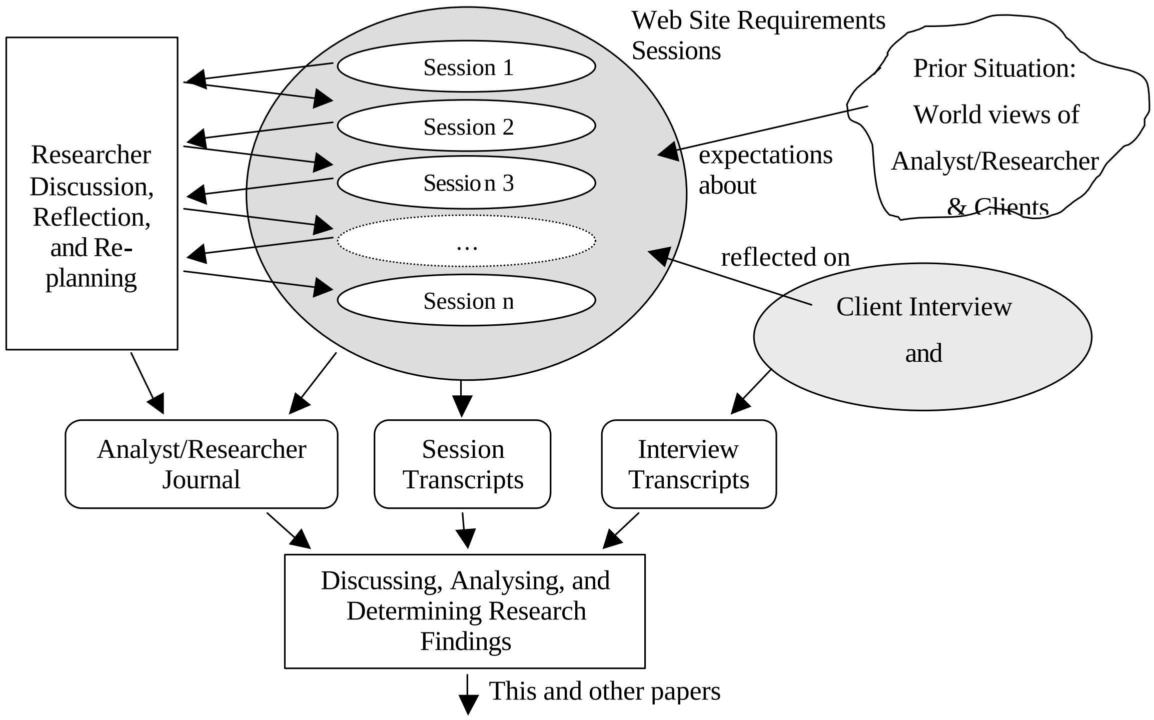
Web Site Requirements Sessions
Session 1
Session 2
Session 3
…
Session n
Researcher Discussion, Reflection, and Re-planning
Prior Situation: World views of Analyst/Researcher & Clients
expectations about
reflected on
Client Interview and
Analyst/Researcher Journal
Session Transcripts
Interview Transcripts
Discussing, Analysing, and Determining Research Findings
This and other papers

Figure 2: The research process, evidence collected, and researchers' analysis during this study

Analysis of the Evidence

In this section we discuss themes that emerged from analysing the evidence. To support each theme, relevant excerpts from interview transcripts are provided together with comments on those responses. They are discussed under themes entitled:

- Ability to define detailed security requirements;
- Reasoning about new security requirements;
- Recognition of the benefits of diagrams over text;
- Ownership of models; and
- Re-alignment of client-analyst roles.

Collectively, these themes represent an emerging perspective on client-analyst interaction during specification using diagrams. The headings are organised in such a manner as to show growing development or sophistication in the way that clients look at the process. The first two themes deal with the ability of the diagramming technique to support the e-business security specification process.

Ability to define detailed security requirements

The following is an excerpt in which Client F confirms that the method assisted him in modelling the detailed behaviour of the system. Figure 3 is an example of one of the diagrams referred to in these excerpts.

> (Client F) I've only had some work on the sidelines of e-commerce developments through [another firm] but was not primarily involved in either systems creation or the planning. I was more involved in ensuring that current and future plans met with international and local government criteria.
>
> I found it [the BRD method] sensible and it broke down what happens in a system into a number of parts and it standardises ways of interaction within the system so it is easy to understand the specific events in a system and how things change so it seemed logical and flexible enough to use.

At another point in the interview Client F is quite explicit in explaining how he used the method to reason about the complexities of the “rules” of the system, particularly being able to recognise redundant behaviour as well as extract common behaviour.

One interesting aspect of the first excerpt is in understanding the initial mindset or world view that the user has of user-analyst interaction. It is clear here that the user had a initial view that the user is expected to specify the requirements at a high level of abstraction (e.g. by specifying that something has to “happen” on the website without supplying all details) and that further it is expected that the analyst will be able to pick this up, and fill in the gaps as it were. Towards the end of the first excerpt it becomes clear that the user has begun to rethink that viewpoint – in other words to acknowledge that the user is needed to supply more detail in requirements.

Reasoning about new security requirements

The above excerpt was a response to questions about whether the diagram helped in defining the detail of requirements. In themselves, the questions do not specifically ask if the diagram supports the user in *reasoning* about the specification as opposed to describing or defining the specification. The other participant, Client G, said:

> (Client G) Oh, I mean, the flow diagram really brought out that, OK, you could actually model the person in your own mind - "OK, I've done this, I've done this, I've done this. Yeah, I...what do I do now?" It brought up questions that said "OK, if I'm the user and I go through this process, what am I missing?". I could easily follow it with the diagram whereas in my site I would put the stuff up, then I would find out as a user, as I tried to use it "hey there is something wrong here". So I'd have to go back and re-change the whole thing - does that make sense? I think that it allowed me to see the sights in more detail and probably in a better flow system than I would if I'd just done my normal method of just trying it out.

From the perspective of a researcher interested in how diagrams and techniques support the development process, it is observed that here there were shifts in thinking from formal ("the flow diagram really brought out…") to informal ("you could actually model the person in your own mind…") to formal modes ("I could easily follow it with the diagram…"), an observation which will be generalised in figure 4 later. The other client exhibited similar shifts in thinking.

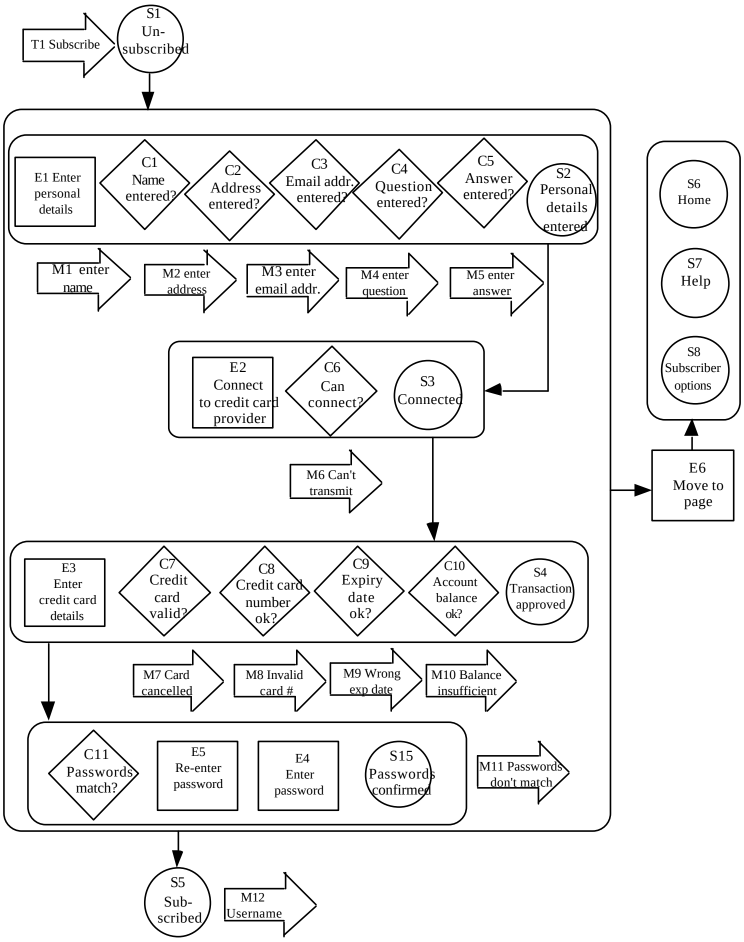

Figure 3: Business Rules Diagram Modelling the "Subscribe" Use Case.

The preceding excerpts were responses to questions regarding the BRD method and how it aided the mechanics of specification. The next few excerpts discuss themes of a more reflective nature that emerged from the interviews.

Recognition of the benefits of diagrams over text

There is a considerable body of literature that expounds the benefits of diagrams as reasoning tools over text-based (or other) representations. Not surprisingly in this context, several comments were made by both clients in regard to this view as a means of articulating specifications. The comments actually arose in answers to other questions i.e. questions not specific to comparing diagrams to text as a specification medium.

> (Client F)… and so using the diagrams kind of enables people who are planning a site like we have been to weed out the kind of wishy-washy talk about "you'll be able to do this and you'll be able to do that". It really forces you to think in a very structured and coherent way, which is what you need to do to create a structured and coherent site.
>
> (Client G) It surfaced some of the underlying requirements that hadn't really been considered. So it surfaced those requirements and allowed them to sort of … "hey , we've got a gap here. what's the problem. bring it out and see it" ...and also the linking of those diagrams because they go into different depths so it also allowed you to...you've got one diagram and from that another box that goes into another diagram and I found that quite useful 'cause you could then sort of follow the flow and that also fits in with what I used to do when I was strategic planning something - you'd do the flow diagram and then you'd have a box with a whole complex thing and that would be the next level so I was quite comfortable with that.

A point to note about the above excerpts is that the experience of this study encouraged the clients to reflect upon the relative strengths and weaknesses of text and diagrams as alternatives for specification. The fact that they chose to bring these observations up in response to other questions strengthens the "value" of their responses and is indicative of the level of cognitive reflection (formal/informal) i.e. that they are beginning to critique alternative types of specification techniques.

Ownership of models

During one of the modelling sessions, client G took the marker pen from the analyst and drew his own BRD on the whiteboard. This is indicative of both the level of confidence in and the ownership of the BRD method exhibited by the clients. During the structured interview session, the analyst asked Client G about this behaviour.

> (Client G) Yes, If Client F has a suggestion, then if he wants to describe it or he can do it, so give them pens and get them to do it.

As more diagrams were developed, the clients elected to omit the use case dialogue step and chose to draw the diagrams directly. The clients also began to model abnormal behaviour directly. At this stage the clients were able to take full control of the diagram and used it to reason about the logic of web site navigation. The clients also used the diagram to analyse the expected interactions between a user and the system as well as using it to check the logic and validity of the business rules themselves to some extent, although this cross-checking was a role they generally deferred to the analyst.

The fact that the clients were gaining ownership of the models and indeed of the process is significant in terms of understanding the degree to which this study was succeeding in its aims of providing a viable diagramming technique with which to specify requirements. It demonstrated that the approach was "working" as far as the clients were concerned and also that the declared semantics of the diagram (being able to support reasoning etc.) appeared to be correct.

Re-alignment of client-analyst roles

As the ownership of the modelling process was transferred from the analyst to the group, the rate of progress increased markedly. At this stage the clients were not interested in the precise syntax of the BRD method and clearly saw that role as being the domain of the analyst as indicated by:

> (Client G) I know you are the facilitator type thing, but maybe it would be better if you let them get it down and then go back and start doing the detail and change it as necessary…So rather than you do it and then talk about what you've just done, that little bit, let us get it all down, then you back and facilitate the changes.

Here, questions are raised about user and analyst expectations in terms of what roles are acceptable in a given situation. In attempting to measure the degree of sophistication that the clients had achieved since the beginning of the study, clearly a shift emerges in the active/passive relationship between client and analyst and also the level of participation.

Theoretical Explanations

In the previous section, we identified and discussed several themes, which acted to illustrate how the expectations, roles, and behaviours of the analyst and clients related to, and changed with, each other. We now propose a simple model of analyst/client interaction to explain the link between the formal and informal aspects of shared understanding.

We suggest that the model in figure 4 represents the process by which the analyst/researcher and the clients jointly attempted to perceive, discuss, and agree upon a satisfactory shared interpretation of the previously unstructured business problem and choose a solution, using the mechanism of a (semi-)formal diagram or model. At the outset, both the analyst/researcher and the clients brought in their worldviews and expectations of how the process ought to take place. The process itself used the mechanism of a diagramming method (the BRD), to achieve a more detailed, precise, correct, and shared understanding of requirements. This was arrived at through various forms of formal and informal communication. In order to achieve a shared context, the analyst taught the modelling method to the clients. This enabled both parties to establish common referents for the problem under consideration. This is evidence of formal (rational) knowledge transfer. Informal (intuitive) knowledge transfer also occurred between the analyst/researcher and the clients (as well as between the clients themselves). This initially took the form of natural language statements. Gradually, assertions about the business problem began to take the form of more formal statements using the BRD. However, this doesn't totally supplant the less formal communications, as natural language statements are always needed that refer to the formalisms (BRD in this case) and establish the formal language's correspondence to the business situation. Over time, a shared understanding is built using the formal diagram and, when familiar enough, its capabilities for supporting reasoning lead to its adoption and usage in the conversation about requirements.

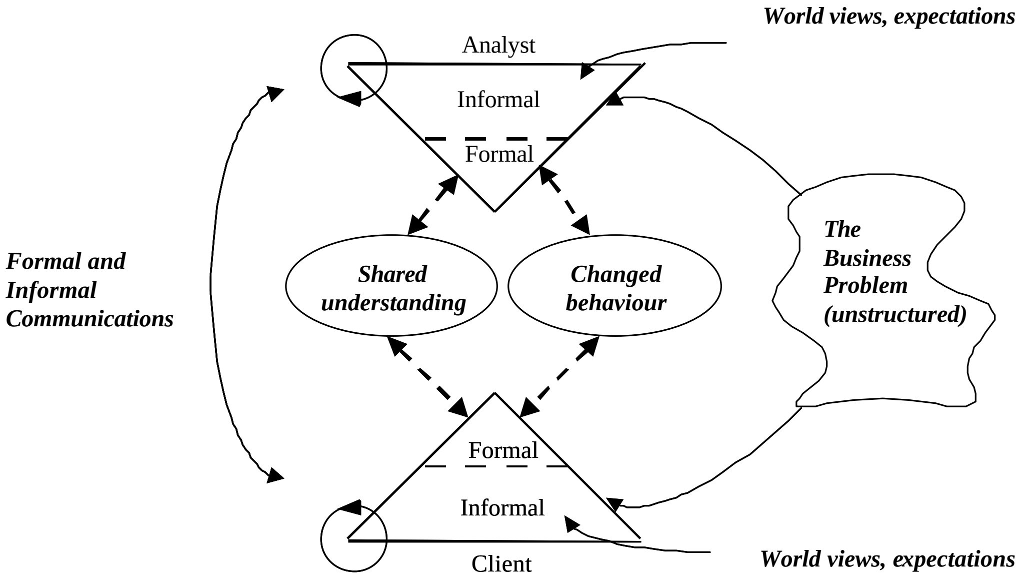

Figure 4: A Model of the Analyst/Client Interaction.

Conclusions and Future Research

It is acknowledged that the scale of this study was very small, consisting of a single analyst and two clients, thus it is not easily generalisable. However, in terms of action research, the reflective stage following the study provided insight into the nature of the complex relationships that form during system development. At present, the conceptual model is perhaps too general, and therefore several other studies in different domains are underway which will provide further cases and will act to prove or disprove the utility of the model. These new studies will also address concerns of generalisability. The BRD method is also being extended in these studies to cover further phases of the SDLC.

We have presented an analysis of the nature of analyst/client interaction within the context of defining requirements for an e-business electronic journal application using a particular systems development method, the BRD method. We have identified a number of aspects of the interaction in terms of web site security that may not have surfaced with a design-oriented development method, such as those commonly used in the development of web-based systems. We have also suggested new and extended existing theory that provides generalised explanations of the findings.

At the beginning of the study, the various actors had expectations about the process. The analyst/researcher had his expectations about how the tasks would proceed, what roles the others would play, and how the technology (the BRD method) would be employed. The clients also had their own expectations. To some extent these expectations were set by the organisation. These expectations were then negotiated into ways of working with the diagrams that evolved over time. In some cases, this resulted in changed behaviour as was evidenced by the clients taking control of some tasks. At the same time, the diagram itself evolved as the BRD method was modified. This then caused further re-negotiations. Thus, over time, the expectations of people, their changing roles of the tasks within the BRD method, and the diagram itself were negotiated and re-negotiated. In addition to, but concomitant with this, we believe we observed a shift in the way that users perceived the requirements elicitation process from a relatively simplistic and naïve position in which the role of users was essentially one of providing requirements information, to a more sophisticated and mature position in which it is recognised that requirements are often unclear, uncertain and problematic and that sharing, negotiation and compromise through modelling is a more productive and effective requirements elicitation process.

We strongly suggest that further qualitative, interpretive, and detailed research is needed on the BRD and other diagrammatic techniques and methods to further explore their use in practice as a means for improving their use and design – particularly with respect to the increasingly critical domain of e-business security requirements specification. Across-method research is also needed before we can generalise the findings of this research to other diagrammatic methods.

References

Bostrom, R. P., and Thomas, R. D. (1983). 'Achieving excellence in communications: a key to developing complete, accurate, and shared requirements'. *Communications of the ACM.* 11, pp1-13.

Checkland, P. (1981) *Systems Thinking, Systems Practice.* John Wiley & Sons.

DeMarco, T. (1978). *Structured Analysis and System Specification*. Englewood Cliffs, New Jersey: Prentice-Hall.

Ernst & Young (2001). Information Security Survey 2001.

Harel, D. (1988). On Visual Formalisms, *Communications of the ACM,* 31(5), pp. 514-530.

Isakowitz, T., Stohr, E. A., and Balasubranamian, P. (1995). 'RMM: A Methodology for Structured Hypermedia Design'. *Communications of the ACM, 38*(8), pp34-44.

Jacobson, I., Christerson, M., Jonsson, P., and Övergaard. G. (1992). *Object-Oriented Software Engineering*. Reading, MA: Addison-Wesley.

Johnson-Laird, P. N. (1983). *Mental Models*. Cambridge, Massachusetts: Harvard University Press.

Johnstone, M.N., McDermid, D.C. and Venable, J.R. (2000) Teaching an New Dog Old Tricks: Modelling Electronic Commerce with Business Rules, in Gable, G. and Vitale, M. (eds), *Proceedings of the 11th Australasian Conference on Information Systems*. Brisbane, Queensland.

Johnstone, M.N., and McDermid, D.C. (2001) Using Ontological Ideas to Facilitate the Comparison of Requirements Elicitation Methods, in Finnie, G., Cecez-Kecmanovic, D. and Lo, B. (eds), *Proceedings of the 12th Australasian Conference on Information Systems*. Coffs Harbour, NSW.

Larkin, J. and Simon, H. A. (1987) Why a diagram is (sometimes) worth ten thousand words. *Cognitive Science*, 11, pp. 65-99.

Lee, H., Lee, C., and Yoo, C. (1999). 'A Scenario-based Object-oriented Hypermedia Design Methodology'. *Information & Management, 36*, pp121-38.

McDermid, D. C. (1998) *The Development of the Business Rules Diagram*, PhD thesis, Curtin University of Technology.

Moody, D., Simsion, G., Shanks, G., Olson, N., and Venable, J. (1995) Stakeholder Perspectives in Conceptual Modelling, *Proceedings of the 6th Australasian Conference on Information Systems*, Curtin University, Perth, Western Australia, 26-29 September 1995, pp. 187-205.

Schwabe, D., and Rossi, G. (1995). 'The Object-Oriented Hypermedia Design Model'. *Communications of the ACM, 38(8),* pp45-46.