SECURITY RISK ANALYSIS FOR COMPLEX SYSTEMS

Mark Branagan, Robert Dawson, Dennis Longley

Information Security Institute, QUT

Information Security Institute, QUT

Faculty of Information Technology, QUT

m.branagan@isi.qut.edu.au

GPO BOX 2434, Brisbane Q Australia 4001

Phone: (+61 7) 3864 9561

Fax: (+61 7) 3221 2384

r.dawson@isi.qut.edu.au

GPO Box 2434, Brisbane Q Australia 4001

Phone: (+61 7) 3864 9564

Fax: (+61 7) 3221 2384

d.longley@qut.edu.au

GPO Box 2434, Brisbane Q Australia 4001

Phone: (+61 7) 3864 1931

Fax: (+61 7) 3864 1801

ABSTRACT

Complex systems such as many Critical Infrastructures require new approaches in Risk Assessment and Management. In a complex system the emergent nature of much of its behaviour renders it difficult to enumerate the potential impacts of a range of scenarios. For Risk Assessment and Management a link must be made between the potential threat events and their final consequence. Given the complexity, interconnectivity, interdependency and potential geographical distribution of systems a simulation based approach offers a solution by allowing for consideration of the emergent behaviour of the system. It would, moreover, be desirable to combine an effective security documentation system with a simulation system to explore the range of system risk scenarios. This paper discusses the role of such a tool.

KEY WORDS

Risk Analysis, Simulation, Critical Infrastructure, Information Security Models, Security Documentation

SECURITY RISK ANALYSIS FOR COMPLEX SYSTEMS

1 INTRODUCTION

The last two decades have seen the exploitation of information technology advances to develop extremely complex, tightly coupled systems within the major infrastructures demanded by current society. This paper explores the problem of determining risks within such systems.

Risk analysis methodologies aim to inform management on the cost effectiveness of security systems designed to reduce system risk to acceptable levels. This proved to be an ambitious target even in the early 1970's when computers performed limited tasks in secure environments. In the current environment of complex, interdependent systems and highly insecure environments it would appear that mere risk identification is in itself a daunting task. Hence this paper does not claim to present an effective risk methodology for complex systems; it merely seeks to explore the solution space of their risk scenario identification.

The problem we are considering is that of investigating risk in complex closely coupled systems, where the individual systems are under autonomous management control. Critical Infrastructures can be considered complex systems. For example, a nation's health infrastructure which is dependent upon hospitals, medical centres, communication systems, power systems and networks, transport, health insurance and finance networks etc is one example of a complex interconnected infrastructure. Most current risk analysis methodologies take a highly macro, holistic view of the system. With closely coupled complex systems this view overlooks the detailed level where the risk resides. Moreover there is insufficient experience and data of complex systems, let alone closely coupled complex systems, to derive any such macro view of risk.

In considering security risk in critical infrastructures, it is impossible to ignore the implications of the complex nature of the systems involved. For all types of infrastructure the information systems that support their operations are vitally important. These information systems however introduce much of the system complexity, their networks increase the speed of interdependency interactions, and their ubiquity can often mask the low level extent of the coupling.

There is comparatively limited experience in the operation of current highly complex tightly coupled systems in even normal operational regimes. Experience has shown that these systems display behaviour that was unanticipated in the design process, even where a formal design process existed. Investigation of security and risk demands consideration of situations where a system is forced outside its normal operating parameters. Such investigations are complicated by the high degree of low level coupling between autonomously managed systems, and any form of experimentation would almost certainly be discouraged by the management of the systems affected.

As stated above security risk assessment is a difficult task in the best of circumstances, let alone in these scenarios. The risks arise from the system complexity, coupling and attitude of management subject to financial and operational pressure; these factors are themselves major inhibitors to the data collection and analysis necessary to gain an understanding of risk at the requisite low level. On the other hand any attempt to predict risk scenarios from macro models and historical data is negated by the limited understanding and experience of the models, and the minimal data available to cover the vast space of risk scenarios.

Simulators provide an experimental tool to explore the nature of system behaviour where experimentation on the system itself is infeasible. The simulators are specifically designed to experiment on abnormal system behaviour and therefore differ significantly from conventional training simulators, such as flight simulators, where the emphasis is on normal operations and predetermined stress situations. This paper explores the use of simulation methods to gain greater understanding and knowledge of complex system risk.

The following sections present a discussion on the nature of complex systems, followed by a discussion on the management responsibilities for systems comprising a critical infrastructure; a discussion on complex system risk is followed by sections dealing with the proposed approach. These sections commence with a discussion on the fundamental problem of acquiring and maintaining the documentation to provide the risk analysts with the necessary system information, followed by the documentation approach adopted by the authors and described in previous papers. The use of this model, and software developed for its implementation, as a basis for the suggested risk simulators, is described and followed by the authors' views on how such risk simulators could be developed and utilised.

2 NATURE OF COMPLEX SYSTEMS

2.1 Emergent Behaviour

The last couple of decades have produced highly complex human made systems. The complexity lies both in the components of the individual systems and the tight coupling between large systems made possible by advances in information technology. Humankind has traditionally dealt with complex systems, e.g. the human body, by drawing upon historical data of its macro (or large scale) behaviour, particularly its abnormal macro behaviour. No such comprehensive archive of historical data exists for the recently developed human made systems. Therefore, predicting abnormal behaviour in such systems is problematic, whilst the societal impact of such abnormal behaviour may be unacceptable.

Complex systems may be defined by the fact that the system behaviour is emergent. The macro level behaviour of the system is dependent on the interactions between its various components at a level lower than that at which the behaviour is observed. It is impossible to predict the macro level behaviour of these systems by observation of the behaviour at this macro level, particularly with the limited volume of historical data available.

Emergent phenomena can be defined as phenomena "for which the optimal means of prediction is simulation" (Darley 1994). Hence if the behaviour of a complex system is to be predicted then simulation may offer a solution.

2.2 Interdependence

Interdependence between modern systems often arises from the implementation of communication networks. There are many sources of complexity in networks, e.g. structural complexity, network evolution, connection diversity, dynamical complexity, node diversity and meta-complications (Strogatz 2001). Interdependencies between systems are a major contributing factor to increased infrastructure complexity and represent a situation in which the state of one system is influenced, sometimes mutually, by the state of another. Such interdependencies can rapidly increase the overall system complexity (Rinaldi, Peerenboom et al. 2001). Cyber interdependency, which can be defined as some dependence on information, which travels over the information infrastructure (ibid) is now a major factor in the overall system complexity.

Interdependencies thus result from coupling between systems. As complex systems and networks develop there may be minimal experience of their operation under abnormal conditions. A rapidly changing network for example may offer minimal historical experience of even normal operations to those responsible for risk in the system. System modifications can occur rapidly not only in the implementation of such systems but also in their interconnections, some of which may well be unreported

Tightly coupled complex systems are particularly problematic because system disturbances outpace diagnosis and counteraction. Normal accident theory (Perrow 1984) predated the

development of much complex systems theory but nevertheless anticipated some of these problems, e.g. even low level threats may translate to large final impacts.

There are three particular problems of risk in coupled complex systems: combination, magnification and feedback, all of which can arise if a blinkered local view of risk and threats is adopted. A local system will normally be aware of its immediate coupled neighbours; given an unusually good set of information sharing, it may be aware of the potential threat it poses to its neighbours and vice versa. This information sharing is, however, unlikely to cover all the possible combinations of security events and such combinations may present a significant magnification of risk when transmitted to distant coupled systems which, could in turn, feedback to the originating system.

2.3 Interdependence and Emergence

The preceding sections highlight the problems of gaining sufficient information to determine local macro risk from local and coupled sources. Whilst some form of interdependence between systems has existed for decades, the increased coupling introduced by information technology advances has created fresh complications and dangers, in terms of the speed of coupling and coupling at a low level of operation.

The speed of coupling effects is widely recognised as a cyber security problem, computer viruses and worms for example, can spread faster than remedial efforts. A potentially more serious problem lies with the emergent aspects of interdependency. Management may be fully aware of macro coupling impacts such as loss of supply, but lower level coupling provided by (say) a network server in a neighbouring system may not be apparent at a macro level.

3 SECURITY RISK RESPONSIBILITIES IN COMPLEX SYSTEMS

Security is largely the responsibility of local system managers but this approach has significant implications in the world of tightly coupled complex systems:

- The manager will often have insufficient to access to information on coupled systems to predict local risk scenarios
- The societal impact of an infrastructure failure arising from a local system security event may be unacceptable

3.1 Local Systems

The concept that responsibility for determining risk for an individual system can entirely divest to those directly involved with that system appears unsupportable. Particularly where a high level of interconnectedness and interdependency exists between systems. For multiple interdependent systems the risk space for any of the component systems will be dependent on the risk space for all the interdependent systems. Risk scenarios for any one of these component systems may depend on risk scenarios of coupled component systems.

It is clear that the owners of a particular system are responsible for managing risk for that system. It is less clear how a given set of owners can reasonably predict the impact their system has within the total system, if they have no authority over the information on the neighbouring systems. Moreover system security may be dependent upon systems beyond the immediate neighbours. For example Figure 1 illustrates the feedback situation where threats can be exported from a system, follow some chain through a set of systems and return as an enhanced incoming threat to the original system. This presents a difficult problem even when the coupling between systems is well identified, as discussed above (See 2.3), since coupling may occur at a level below the management radar.

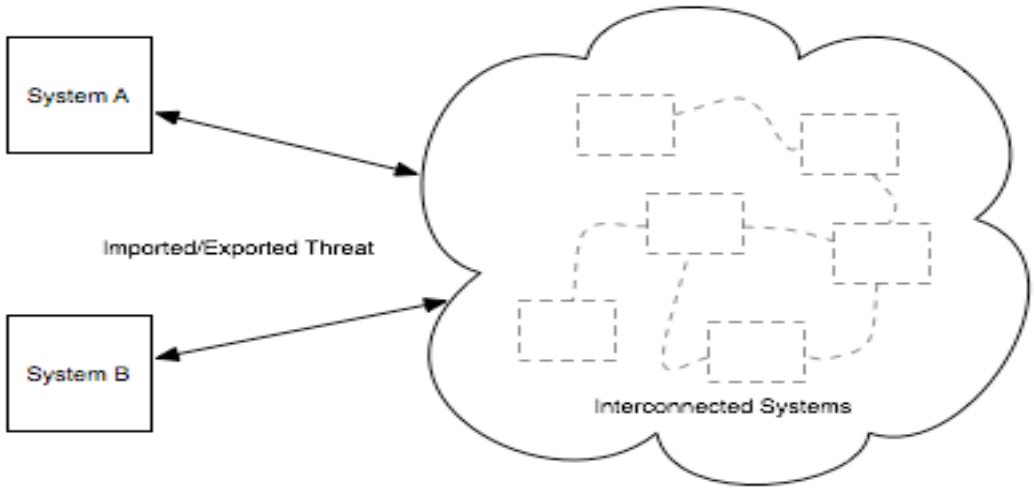

Figure 1 Imported and Exported Threats

The technical problems of information sharing are moreover minor when considered against the managerial barriers to such information flows. The owners within the interconnected infrastructure may not have the facilities to acquire and supply the required information about their systems. They will tend to be reluctant to provide information that could be considered commercially or politically sensitive, and some of the component systems may belong to commercial competitors. In any event security information is considered particularly sensitive where it may relate to subsequent liabilities.

Nevertheless such information can be vital from a security viewpoint. For example, consider malicious code creating excess traffic on a network. For a self contained system the security issues may be straightforward e.g. effective anti-virus software, but such measures can be obviated by connection to an external unprotected network. Initiatives such as the Trusted Information Sharing Network established by the Australian Federal Government (Attorneys General's Department 2005) recognise the importance of information exchange among connected infrastructures.

3.2 Overall Infrastructure Responsibilities

The previous section discussed the problems facing system managers when they have no effective means of accessing security information from the managers of coupled systems. This is just one aspect of the problem arising when critical infrastructures depend upon autonomous commercial suppliers. A more significant problem can arise if the societal impact of a total system security event is out of proportion to the impacts on the individual sub-systems. In other words, even if there is sufficient information sharing between the component systems to provide a local acceptable level of security, there is no guarantee that these levels guarantee against an unacceptable societal impact. Loss of power to a hospital may cause a minor loss of income to the power supplier, and deaths amongst hospital patients.

This is a political problem but we should nevertheless explore the potential for the provision of an overall view of the total system risks, in the light of the discussion above. The question addressed here is: can the potential solutions for risk investigations at a local level be adopted to provide a means of exploring risk for the complete infrastructure of complex coupled systems? This matter is discussed in more detail in Section 7.4.2.

4 DETERMINING SECURITY RISK IN COMPLEX SYSTEMS

4.1 Local Systems

Complex systems present a difficult set of problems for risk assessment. It has been recognised that a comprehensive knowledge of a system is required for a comprehensive risk assessment and

management process (Craft, Wyss et al. 1998; Busuttil and Warren 2004). What is less clear is how an understanding can be gained of the security interactions both within sub-systems and between coupled systems.

Whilst operational design weaknesses tend to manifest themselves during normal operations, security vulnerabilities remain hidden until some abnormal event occurs. For example the common problem of privilege escalation may only become apparent when a set of circumstances results in an auditable event. In comparatively simple systems the security event may at least be readily traced back to the vulnerability. In complex systems the security vulnerabilities may remain hidden for an extensive period. It may also prove extremely difficult to trace the security event back to the initial vulnerability after the threat manifests in a given system.

Risk assessment moreover involves a prediction of both the magnitude and likelihood of the event. As indicated above identifying vulnerability in a complex system does not readily lead to a clear indication of the nature of the potential impacts, complicating the problem of assessing these impacts. Determining likelihood is even more problematic given the diverse, long paths between the source and impact. Historical data is unlikely to provide a reliable information source to assess such probabilities and impacts, given the limited experience of such systems and the extremely large potential set of event sequences and combinations.

4.2 Infrastructure of Complex Coupled Systems

The significant problems of risk assessment in individual complex systems rise exponentially when the total system of systems is under review. The path between a security vulnerability in one system and its manifestation as a security event in another is potentially much longer. It is also likely to traverse management domains reluctant to share low-level sensitive security information. Moreover managerial sensitivity is likely to be particularly high since such data could well have serious liability implications.

The scarcity of historical data will be aggravated by wide variations in local policies on the collection and format of such data. For example, correlating security logs within an organisation is no enviable task, but is trivial compared with that of corresponding investigations involving disparate management domains.

5 ROLE OF DOCUMENTATION AND MODELS

Documentation forms an important part of any risk assessment process. The documentation provides both a description of the system under review and a record of operational / security events providing evidence of security system operations and possible inadequacies.

Some documentation types are input types. That is they provide information that is used in understanding the system. Some are output documents, i.e. they are the end result of adding security value to recorded information. For example, the information contained in an asset list may be used in creating a risk register, since it contains some information on asset value to be used in impact assessment.

The problems of developing documentation specifically directed to the needs of risk analysis has long been recognised (Baskerville 1993). Information security and risk management standards (Standards Australia 2000; Standards Australia 2001; Standards Australia 2004) form an important role as background documentation for risk managers. They do however, tend to lack guidance on the development of local system security documentation and do not highlight the problems of current highly complex systems.

The discussions in previous sections on the need to view complex systems at a detailed level render the demand for effective documentation self evident. The particular nature of security documentation in these circumstances may be listed:

- Detail – it must comprise sufficient detail to allow the risk analyst to drill down to the level at which security interactions occur. (Craft, Wyss et al. 1998).
- Form – electronic databases are more appropriate to the collection, collation and updating of large data volumes than text manuals.
- Format – local systems will inevitably be coupled to those within a separate management domain, a common format is essential for the import and export of security information between these domains.
- Cross referencing – the available data will necessarily reflect management sub systems, whilst security interaction will occurs between these subsystems, e.g. computer and building data. The documentation must facilitate ad hoc cross referencing.
- Input to software systems – risk assessment software must be able to access the documented data readily.
- Security – the sensitivity of local security data has been emphasised as a significant hurdle for information sharing between management domains. The security data for a critical infrastructure is corresponding highly sensitive and demands a high level of confidentiality and integrity protection.

6 PROPOSED MODEL AND DOCUMENTATION

A software system has been developed based upon a proposed Information Security Model (ISM) (Kwok and Longley 2004). This model used a database approach to documentation, and allied software to explore security interactions. In order to do this, the ISM uses two key concepts. First Threat Events. A threat event encodes a threat acting on some entity in the system of concern. The second major concept is a Threat Propagation. A Threat Propagation encodes the propagation of threats through the system. Presently these are a single stage, that is a Threat Event causes another Threat Event to occur.

The essential concept of this model was that detailed system data, coupled with stored generic information on the propagation of security threats, as described above could be scanned by software tools to produce threat networks (see Figure 2). Threat networks are a representation of the propagation of a series of threat events through the system for which details have been entered. Threat Networks provide a graphical representation of this propagation indicating, to the linits of the entered data, the terminating event in the system. The system model may be developed top down, with entities representing major system components, or platforms, gradually enhanced with more detail as experience of the risk scenarios develops.

A subsequent paper (Branagan and Longley 2005) considered the further use of the threat network approach to critical infrastructure security, dealing in particular with the more complex problems of multivector attacks and a loss of service in circumstances of multiple suppliers.

The significance of this work in the context of complex systems is that it demonstrates a form of documentation and risk analysis investigation meeting the Detail, Form Format, Cross Referencing and Input to Software Systems requirements for documentation discussed in Section 5

The authors propose that the ISM model and software may be extended to facilitate risk investigations of complex coupled systems. In particular the threat networks developed by scanning local system data and stored security knowledge, in the form of generic threat propagations may be extended to risk simulators. Individual local system simulators are then connected by agents to represent coupling effects.

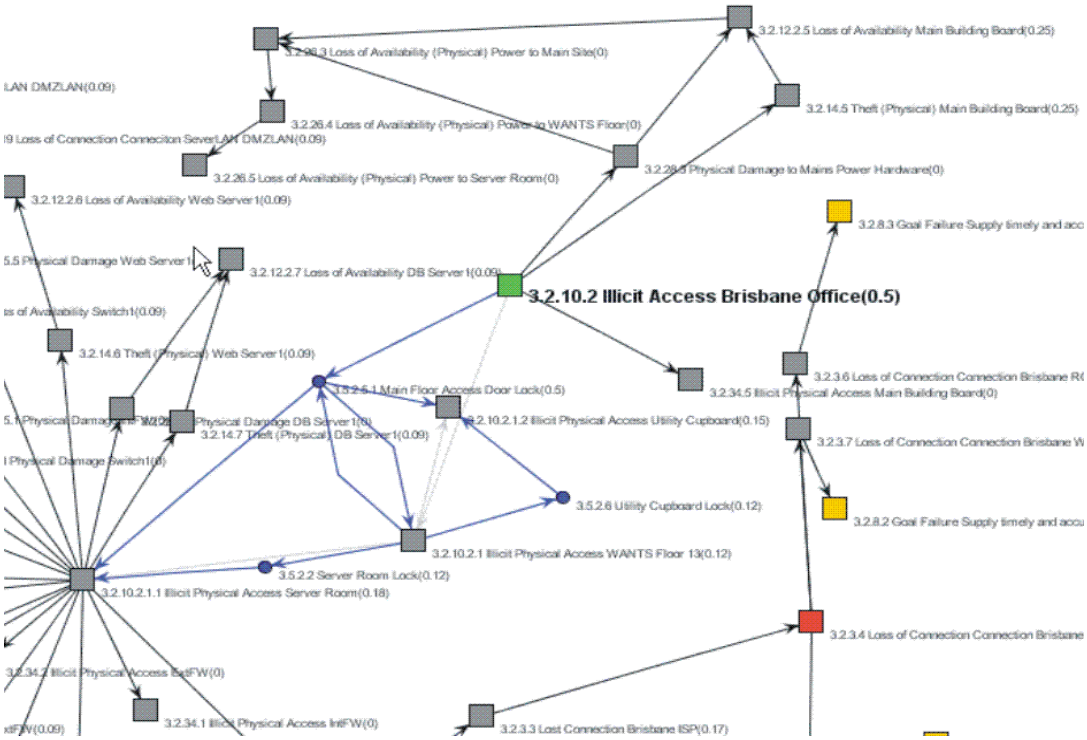

Figure 2 Sample Threat Network

Providing a model and documentation system enabling security risk practitioners to capture system information and to explore risk scenarios before drilling down to more detailed levels is one of the key qualities of the model and software. User interaction with the software helps provide guidance on further data to be collected and added.

7 RISK SIMULATORS

We currently lack detailed mathematical models to predict the behaviour of complex systems. Historical data providing adequate evidence of the macro behaviour of complex systems is also lacking. Staffing is sometimes determined by management policies favouring operational requirements at minimum cost. The consequential high employment mobility tends to limit the available pool of experience of operational, let alone abnormal system behaviour.

There is insufficient experience of risk simulators to provide a guaranteed cost effective solution to the problems of risk in complex systems. However, in the current circumstances and with an apparent lack of viable alternative approaches risk simulators do at least provide a solution space worthy of exploration.

A simulator is essentially an experimental version of a mathematical model. As such it allows the designer the opportunity to explore the behaviour of the model interactively, gain a greater insight into the system, make some decisions on the system components to be explored in more detail and refine the model and simulator. The potential of the risk simulator lies in the interactivity and refinement facilities offered.

7.1 Nature of Risk Simulators

Training simulators have been widely deployed for complex systems such as aircraft and nuclear reactors. These simulators are essentially designed for normal and well-understood abnormal situations. Their significant cost and complexity arises from the demand for accurate system behaviour over a wide range of operational circumstances.

The proposed risk simulator is directed solely to significantly abnormal behaviour and to this extent is spared a significant amount of operational detail. The approach is to model the predicted

abnormal behaviour of system components and to use the simulator to explore the interaction of these abnormal events.

The proposed paradigm for the simulation is the Threat Networks described in a previous section and papers (**Section 6, op cit**). Consequently the simulator is based around the exploration of the causal chains starting from some unavoidable threat and terminating at some unacceptable impact

There are three potential forms of threat networks for use in risk simulators:

- Probability networks
- Monte Carlo
- Dynamically developing network

Currently the models have been developed as static probability threat networks. Given the probability of one or more unavoidable threats, and that of propagation between threat events it is possible to estimate the nature and probability of consequential impacts. Moreover if some "cost" can be assigned to that impact, then the probability and cost may be combined into an expression of risk. One major advantage of the current model is that searches may be conducted backwards, i.e. from the undesirable impact to determine the range of threats associated with such an outcome.

This approach does highlight one of the abovementioned advantages of simulation. The user has an opportunity to inspect the intermediate nodes of the network, consider whether there could be missing neighbouring nodes, due to inadequacies in the model or its data, and possibly refine the model or its data. Thus the model provides not merely a predicted risk outcome but also an opportunity for the user to experiment with model itself and develop a greater insight into system risk.

The Monte Carlo approach provides a series of "deterministic" networks which may give a better insight in model behaviour by omitting low probability outcomes in some of the run outputs. In effect a node is included in the threat network by "throwing dice". At each stage a random number is generated, compared with the node probability and the result determines node inclusion in the threat network. This approach may be combined with that of the probability network to explore the range of potential risk outcomes

The dynamically developing network is a more ambitious simulator which aims to provide a time scenario of a developing major event, for risk investigation or disaster training. In this case the time delays of threat propagation, the effect of time limited resources, e.g. battery backup systems, loading and congestion effects may be portrayed.

7.2 Security and Risk Simulation

Risk simulation inevitably involves consideration of the security systems implemented to counteract the risk. Part of the rationale behind security risk assessment is gaining some insight into the effectiveness of security systems. Of particular concern are countermeasures rendered ineffective by some interaction inside the system, in other words some external or consequential threats may affect the countermeasure mechanism directly, or some component upon which it relies.

The risk simulator provides an opportunity to experiment with countermeasures and to test systems in a manner than would be quite unacceptable to operational management e.g. injecting a virus into a network. Given that small changes in a complex system may have disproportionate effects on the macro level of the system behaviour such an experimental tool may be invaluable in security design for complex systems.

7.3 Risk Simulation and Complexity

If the systems under risk investigation risk are complex, it follows that the ways in which risk in the system can be expressed will have characteristics in common with the behaviour of complex systems in general. Therefore we are exploring emergent behaviour; this may represent situations where local threat events can have disproportionate impacts on the risk space for the system as a whole.

It can thus be argued that the problems of complexity and emergent behaviour discussed above are inherent in the risk simulation of complex systems. The simulator designer will inevitably take a top down approach and then drill down as experience of interacting with the model develops. There is no guarantee that in selecting the next area to be examined, mistakes will not lead to exclusion of critical component consideration. The best that can be promised is that an effective tool, handled intelligently and methodically, will give a better outcome than ignoring the *devil in the detail*.

One approach to the drill down selection and depth problem may be to ask:

- Is it possible to identify which of the modelled components are critical from a risk viewpoint at this level of abstraction?
- What are the unacceptable security outcomes for the components so identified?
- How could these outcomes arise?

7.4 Simulation and Systems of Systems

7.4.1 Local Simulation

Closely coupled complex systems represent a major escalation in the security risk analysis effort. The technical aspects of these problems are however a minor consideration when considered against the background of the managerial constraints. The best that can be promised for the risk simulation of such coupled systems is that it lies within the solution space to be explored.

The risk simulator designer for a local system may well have the authority to seek all the relevant system risk information to produce local threat networks. However information on the threats imported from, and exported to, coupled systems require cooperation from the management of such systems to identify:

- Type and likelihood of threats emanating from those systems;
- The liability that would arise if the coupled systems were subject to threats emanating from the local system.

Even if the requisite information were provided there may well be difficulties in handling the format of the information, or gaining sufficient evidence of its provenance, i.e. evidence that it is derived from a reliable source.

A much more serious problem however arises from the neglect in magnification and feedback effects (See 2.2) on the information exchange. An assurance from a coupled neighbour that an exported threat is acceptable to that system, neglects the potential add on effects as that neighbour passes on some consequential threat to more distant neighbours.

7.4.2 Total System of Systems Simulation

At this stage let us ignore the question of ultimate responsibility for the security of large complex closely coupled systems. If a body existed with such a responsibility how could it discharge its minimal duties, i.e. explore the risk scenarios of total infrastructure? It is suggested here that a uniform approach to local system risk simulation combined with some form of simulator coupling is within the solution space.

The pre-requisite for such system of systems simulator is a common model to:

- Ensure that the risk information emanating from coupled systems is in a usable format;
- The individual models can be accredited as appropriate for the task.

The second requirement relates the provenance problem (See 7.4.1)

The advantage of risk simulation as compared with an operational simulator is apparent here. The operational simulators for highly disparate systems would experience major difficulties in meeting these requirements.

The ISM model described above has the potential to meet these requirements and as part of the work on extending the use of the model a prototype system with agents, capable of providing the coupling between system threat networks, has been developed.

8 FUTURE PROPOSALS

The ideas are presented here as a starting point to an important problem of our time: can we protect the complex, tightly coupled systems that govern our lives. The approach proposed is not a quick fix and it demands that resources be directed to gaining a better understanding of these systems.

The major question is: can we improve our understanding of these systems by a process of modelling, simulation and experimentation of complex systems to identify the areas to be explored in more detail, leading further refinement of the model. As we refine the model can we identify areas where additional data exists, e.g. security logs or real life testing is possible, e.g. building and experimenting with test subsystems, e.g. networks.

Another significant issue is that of cooperation between management of coupled systems. Is it possible to use a common model, e.g. the ISM, to model disparate systems such as power stations and hospitals and develop local simulators that can be coupled, within the constraints of security information exchange between the management?

The authors have completed a research project to build an ISM software model providing static probability threat networks and have explored a prototype risk simulator. The software can display both the security relationships of its components, the threat networks and the countermeasure systems. The next stage of development will explore the more ambitious dynamic risk simulators described above (See 7.3).

9 CONCLUSIONS

Critical infrastructures and complex systems present a major challenge to risk analysis. Their component complex tightly coupled systems conceal local threat sources that can be transmitted and magnified through the whole infrastructure, causing major damage before effective remedies can be applied. Finding these threat sources is complicated both by the system complexity and the barriers to sensitive security information data flows between autonomous managed systems. Operational and financial constraints normally render experimentation on system abnormal behaviour infeasible. Risk simulators provide a means to undertake such experimentation and assist in the risk identification task.

10 REFERENCES

Attorneys General's Department. (2005). "Trusted Information Sharing Network." Retrieved 20 April 2006, 2006, from http://www.tisn.gov.au/.

Baskerville, R. (1993). "Information systems security design methods: implications for information systems development." ACM Comput. Surv. **25**(4): 375--414.

Branagan, M. and D. Longley (2005). Developing Threat Networks for Risk Analysis of Information Systems. ISSA 2005 New Knowledge Today Conference, Sandton, ISSA.

Busuttil, T. B. and M. J. Warren (2004). CIIP-RAM - A Security Risk Analysis Methadology for Critical Information Infrastructure Protection. Security and Protection in Information Processing Systems, Toulouse, Kluwer Academic Publishers.

Craft, R., G. Wyss, et al. (1998). An Open Framework for Risk Management. 21st National Information Systems Security Conference, Crystal City, Virginia.

Darley, V. (1994). Emergent Phenomena and Complexity. Artificial life IV : proceedings of the Fourth International Workshop on the Synthesis and Simulation of Living Systems, Cambridge, Mass, MIT Press.

Kwok, L. F. and D. Longley (2004). Security Modelling for Risk Analysis. 19th IFIP International Conference on Information Security, Toulouse, Kluwer Academic Publishers Group.

Perrow, C. (1984). Normal accidents : living with high-risk technologies. New York, Basic Books.

Rinaldi, S. M., J. P. Peerenboom, et al. (2001). "Identifying, understanding, and analyzing critical infrastructure interdependencies." Control Systems Magazine, IEEE **21**(6): 11-25.

Standards Australia (2000). AS/NZS 7799.2:2000 (Previously known as 4444.2) Information security management - Specification for information security management systems. Sydney, Wellington, Standards Australia and Standards New Zealand.

Standards Australia (2001). AS/NZS ISO/IEC 17799:2001 Information Technology - Code of practice for information security management. Sydney, Wellington, Standards Australia and Standards New Zealand.

Standards Australia (2004). AS/NZS 4360:2004 Risk Management. Sydney, Wellington, Standards Australia, Standards New Zealand.

Strogatz, S. H. (2001). "Exploring Complex Networks." Nature **410**: 268-276.