Critical Infrastructure Protection Risk Modelling with Games Technology

Martin Masek, Adrian Boeing and William Bailey

School of Computer and Security Science, Edith Cowan University, 2 Bradford Street, 6050 Mount Lawley, Western Australia
m.masek@ecu.edu.au, a.boeing@ecu.edu.au, b.bailey@ecu.edu.au

Abstract. Threats to critical infrastructure are not passive. Trying to identify what is in fact 'critical' is proving to be very difficult as threats constantly evolve. A major benefit of simulating the infrastructure is that security tests and risk modelling can be applied before infrastructure is built or its environment modified, allowing for lower cost design alterations to minimise vulnerabilities. By using the 3D environment of an existing Game Engine we can explore several possibilities for security analysis that existing tools, due to their global view of the problem, do not allow. Providing participants with a first-person view of the situation allows for more realistic role-play, whilst the networked gaming technology allows remote experts to interact in an intuitive environment and explore, identify and assess the critical components of the infrastructure.

Keywords: Critical Infrastructure, Real-time Simulation, Risk Assessment, Games Technology.

1 Introduction

In the Australian context, critical infrastructure has been described in the National Guidelines for Protecting Critical Infrastructure from Terrorism as:

"those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security" [1].

There are several reasons why critical infrastructure can fail. However the additional risk is that caused by terrorist or criminal activity. For example, the rupture of a pipeline is a technical failure. The risk of such technical failures can be determined through standard risk engineering, where risk is measured as the probability of failure multiplied by the severity of the consequences. Such risks can be mitigated by analysing the probability of failure and building in safety margins, redundancies, and maintenance processes to lower the risk to an acceptable level.

An additional cause for failure is deliberate interference and sabotage. Although a classical probabilistic-based risk approach is at times used to determine an appropriate level of protection, its validity is questioned for such cases. Manunta [5] identifies potential shortcomings that challenge some of the assumptions behind the use of

classical risk based approaches. If a security specialist uses the probability of an attack to identify areas to defend, an attacker can utilise the same probabilities to identify areas that will not be defended. Such threats are not static and can evolve when they encounter counter-measures.

In today's security industry, there is still certainly the philosophy of protecting business interests against crime and in its purest form the "Crime Triangle" has certainly helped in identifying and assisting in the analysis of those threats. This then has to be translated in to the physical security measures we often see still in existence today, ranging from guards to access control and CCTV.

"A security consultant...is called on to...assess what types of threats or risk affect the assets to be protected, render an opinion on the probability of those threats or risks, and recommend a security or loss prevention plan to reduce the probability of those threats or risks" [6]. Often though, security was always considered as an afterthought, or a reactive approach to a negative event that has happened to an organisation.

Gibson [7] highlights that "Risk awareness in the corporate security function should be a practical discipline. Its aims should be explicit, open and objective." This approach ensures that the function is able to quantify the risk, the appropriate preventative measures and align the cost benefit to the organization against its overall strategic goals. The understanding of risk and consequence has helped the security professional to look beyond fortifying their assets or business to a more proactive and dynamic approach to risk. "The security function has traditionally been an experienced-based discipline. However security practitioners are utilizing management disciplines and theories of risk in order to compliment their experience" [7].

What is questioned here is not the "risk assessment" in itself, but it is the methods used to accomplish this assessment. Many organisations perform security risk assessments only once a year, although since September 2001, some organisations undertake reviews on a more frequent basis [7]. Manunta [5] questions the relevance of such ad hock reviews of risk, because by the time the results arrive, they tend to be outdated. The context will dictate the how quickly such results become invalid. But in the current security climate, the terrorist threat is dynamic, evolutionary, and able to adapt and learn.

2 Tools for the Analysis of Critical Infrastructure

Several tools exist for the simulation of critical infrastructure. Simulation tools provide an avenue for more frequent risk analysis using the simulation. Such tools also help bridge the gap in understanding between experts from different disciplines by determining the effect of changes to the system whilst hiding its complexity [8]. This makes each expert area accessible to the whole team, allowing the propagation of system failures and its extent to be determined. Pederson et al. [9] identified 30 simulation systems in a survey of research into critical infrastructure interdependency modelling. These simulations range in maturity from research to commercial systems and model a variety of infrastructure using various simulation types.

Most existing critical infrastructure simulations provide a simple single-user graphical visualization of the infrastructures and their interdependencies. This typically consists of a graph display, with infrastructure nodes connected by edges to show interdependencies. Some simulations are integrated with a Geographic Information Systems (GIS) application and the graph is overlaid over a top-down 2D map of the area. Such displays are useful for traditional risk-based analysis in the design and analysis of critical infrastructure systems, but not for producing a risk mindset based on local vulnerabilities that only a person on the ground would be able to identify.

A simulator that lets users take the roles of a person on the ground would allow for the enactment of realistic scenarios, allowing response times and behaviour patterns to be determined. Such a simulator, through role-play, would allow users to gain an insight into the mindset of an operative on the ground, whether it is facility architects seeking to determine how security guards might act, or response personnel playing the role of a terrorist in the simulation in order to understand how a terrorist might act. Finally, the inclusion of artificial intelligence (AI) controlled characters in the simulator would allow for the simulation of human activities. This is useful for automatic testing of the infrastructure and simulating the behaviour of large crowds, or for training personnel such as incident commanders without the need for physical personnel to take on the roles that are directed by the commander. A major benefit of simulating the infrastructure is that security tests can be applied before infrastructure is build, allowing for lower cost design alterations to minimise vulnerabilities.

By leveraging games technology there is the ability to present the “intruder” into the visual concept thus allowing for a greater assessment of the potential capability of actually inflicting damage. Many times this is a perceived threat that is not borne out by the reality of the known situation. Moreover, once a target has been identified there is the added ability to develop variations of target hardening, which can be tested prior to implementation. This has substantial cost benefits as it is not necessary to actually build in the suggested changes, in order to test them against the “intruder”.

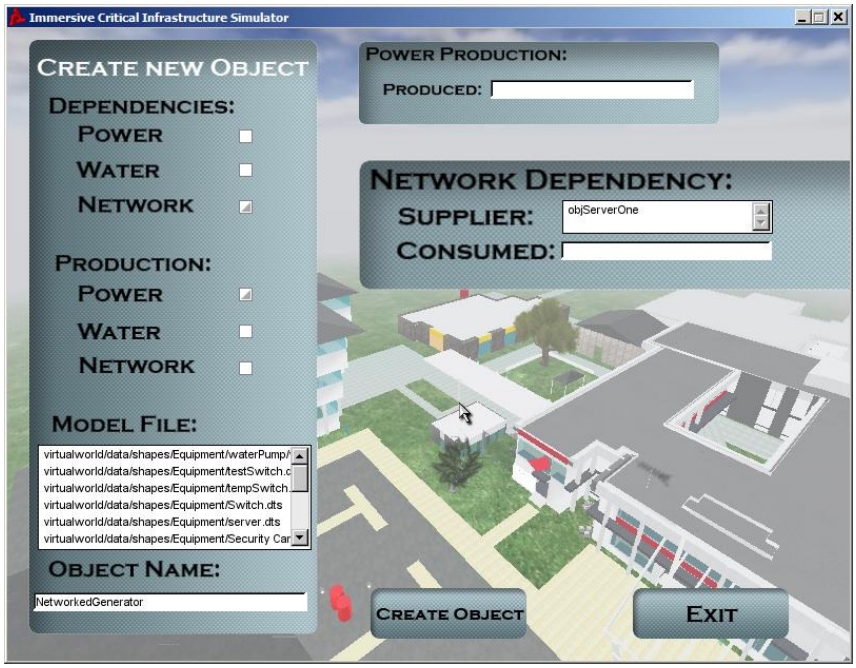

Fig. 1. Creating a networked power generator.

3 Real-time Interactive Critical Infrastructure Simulation

Our proposed solution is an interactive, high fidelity simulation tool built using existing games technology. This allows us to adapt the existing workflow typically used when producing a game to rapid scenario construction. The online nature of modern computer games gives greater opportunities for remote experts to perform security reviews and exercises.

To design and produce a virtual world for a computer game involves a large amount of iteration. An environment is designed by the positioning of obstructions to limit the player's movement, and the insertion of non-static objects such as enemy AI characters. The game is then repeatedly tested and modified in order to maximise its "effectiveness". This need for repeated modification has given rise to tools that allow for the rapid construction of worlds and scenarios, allowing designers to modify the game without an in-depth knowledge of programming. There is a similar need for rapid iterative design when seeking to design secure infrastructure, only the definition of "effectiveness" changes. A game is effective if the player is allowed to win whilst being challenged and entertained, whilst infrastructure is effectively protected if the adversaries cannot win.

Our work-in-progress, the Immersive Critical Infrastructure Simulator (ICIS), demonstrates how existing game production tools can be utilised. ICIS has been

developed using Torque Game Engine technologies from Garage Games [10]. ICIS consists of an interactive 3D world in which computer networks, along with power and water producers and consumers and their interdependencies are modelled. Various aspects of the game engine are used in a simulation run of ICIS, some can be used unchanged, whilst customisation was performed to implement some features specific to infrastructure simulation.

Fig. 2. Three objects are shown in the image, clockwise from top-left: server, power source, and computer representations in the simulator. The green colour indicates the `on' state.

3.1 Interdependency Simulation

Interdependencies between objects have been implemented using a directed acyclical graph architecture. For example, a light switch can be connected to a power source and a light associated with the light switch. The light can then be turned off by the player activating the switch, or turning off the power source. Similarly, objects can have dependencies on multiple resources. For example, a computer may rely on both the power and network infrastructures to remain operational.

In order to aid in the creation and configuration of nodes in the infrastructure network, a 2D graphical user interface has been overlayed on top of the 3D scenario. This allows objects to be created, assigned resources to generate and to consume, and a graphical representation to be assigned. Figure 1 shows an example of a new object being created, which will produce power and also depend on the computer network

infrastructure. The object can be assigned the amount of the resource that is produce, and also which nodes it is connected to in order to service its dependencies.

Infrastructure nodes are assigned a graphical representation, with colour indicating the on (green) or off (red) states. Figure 2 shows the representation of a power source, server, and computer - all in the "on" state.

3.2 Environment Creation

Coupling a critical infrastructure simulator to a 3D environment provides several possibilities for security analysis. For example, accurate views from existing and proposed security cameras can be analysed, as can views from locations where infrastructure could be observed by an attacker. These visibility studies can be performed under various simulated environmental conditions. The ability to modify environmental conditions is possible through the world editor, a tool that is a part of the game engine. Through the world editor, parameters such as the position and brightness of the sun or the effects of precipitation and dust can be interactively adjusted to achieve a desired effect. Figure 3 shows two versions of the same scene with world parameters set to simulate a rainy and dusty day.

Fig. 3. Simulating different environmental conditions.

Figure 4 shows part of the world editor for the Torque Game Engine Advanced. Objects in the world are shown in a tree hierarchy and each object's properties can be modified interactively by non-programmers, the figure showing some of the properties available for the sun. Besides setting properties, the world editor can also be used to manipulate the objects in the world, allowing aspects of the built and natural environments to be positioned, either to re-create a scene from the real world, or to create a proof-of-concept environment to be simulated.

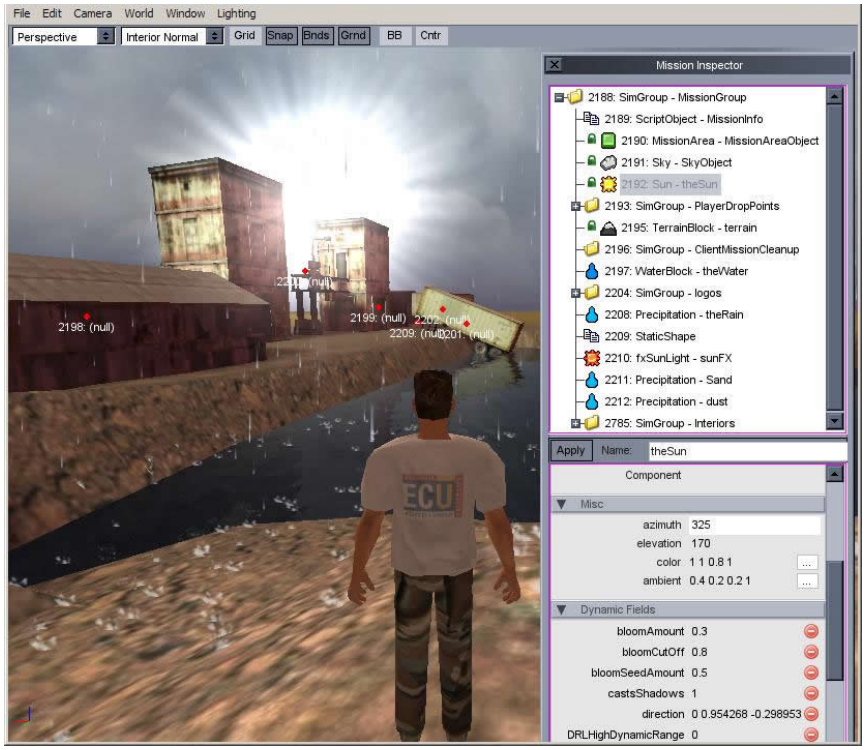

Fig. 4. The world editor allows for the interactive adjustment of the world.

The world can be viewed from several cameras, representing the view of different persons or actual cameras in the world. The top down view, much like the one in traditional “big-picture” simulators can also be gained by positioning a camera above the scene looking down, as shown in Figure 5. This kind of view can be used to gain a general overview of the scenario, and is also useful in a de-briefing situation offering a convenient perspective for re-playing a scenario that had been run previously.

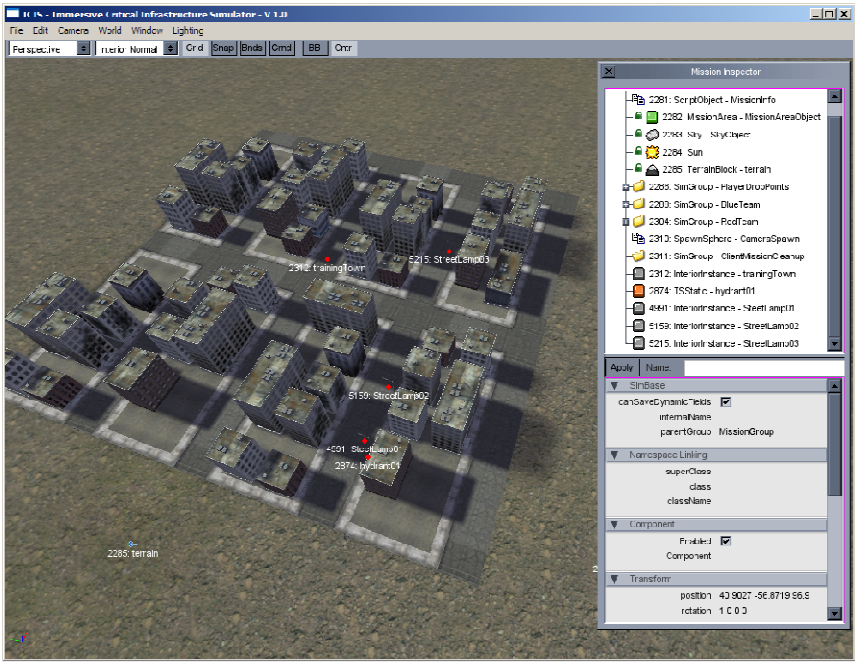

Fig. 5. A “Big-Picture” overview can be obtained using an overhead camera. This can be used by those acting in an observer role, or for re-playing missions as part of a de-briefing.

3.3 Network Architecture

Through the network facilities of the Torque Game Engine, ICIS has the ability to run place multiple users in the same environment. These users can assume a number of roles, including essential services staff and adversaries. The network architecture is based on the client-server model where a server computer runs the simulation, updating the state of the infrastructure based on its dependencies and keeping a global knowledge of the word. Each user interacts with the world through their client PC, which is mainly responsible for displaying graphics on the users monitor and transmitting the users input to the server. This architecture is quite common for game engines, as running the simulation on a central server rather than on each user's computers reduces the scope for users to subvert the simulation code to cheat. For a simulation intensive use, such architecture is useful as only the server computer needs to meet the requirements to run the simulation in real-time, whilst the client computers can be lower specification machines.

4 Discussion

Through the use of game engine tools, combined with some custom implementation of infrastructure interdependencies it was possible to devise a virtual world simulator where scenarios could be created by non-programmers, and enacted through role-play by various personnel. Through interacting with the virtual world, participants can gain an insight into the mindset of various roles by having to devise strategies first-hand to protect or attack infrastructure.

The use of such simulators offer features with various advantages. Notably, every aspect of a scenario can be logged, allowing missions to be reviewed for analysis and post-mortem purposes. The saving of mission parameters throughout the mission can allow the team to re-attempt the mission from any point in time, thus allowing them to focus on identified weaknesses. Once a point of interest in a scenario has been identified (eg. a critical breach of security), the scenario can be re-played from that point in order to determine the best protection strategy.

Whilst directed acyclic graphs are useful to model infrastructure interdependencies at a high level (in terms of supply and demand for resources), each infrastructure node in a real system is typically reliant on a complex set of processes that may be disrupted through various means. Such processes may require specific modelling methodologies to work within the directed acyclic graph system and require a detailed understanding of the infrastructure nodes. As such, the issue of validation arises.

4.1 Validation

Our current system is undergoing testing, with future work to include the implementation of more types of infrastructure interdependencies and applications targeted towards specific environments and roles. In targeting a specific environment, for example a particular oil refinery or power plant, the issue of acceptable simulation fidelity arises. This issue encompasses the following:

- Correspondence between the response of the simulation tool and the actual infrastructure under normal operating conditions.
- Correspondence under emergency/hazardous conditions.
- Physical accuracy of the 3D environment and its mechanics regarding movement in the world.
- Visual accuracy of the 3D environment.

Correspondence in terms of critical infrastructure and its interdependencies between the simulator and the real world can be validated using historical data that exists for the actual infrastructure. Whilst this data may exist in adequate quantities to validate normal operating conditions, there may be a lack of data for certain kinds of emergencies, as discussed in [11]. For simulation of such situations, historical data can be used in conjunction with extrapolation and predictive algorithms based on the physical properties of the infrastructure. As complex scenarios, such as attacks and emergencies depend on many parameters, the re-playability of the mission becomes an advantage as various possibilities can be explored.

Various means of validating visual and physical accuracy of the scenarios built environment exist. This includes comparison to plans, but also resources such as

aerial survey data. Geographic data is relatively easy to obtain, with 90 metre per point data publically available for the world through the US Geological Survey [12] (with higher resolution data available for purchase through various sources). Quite detailed layouts of various installations are also publicly available using such resources as Google Earth [13]. Whilst imagery in tools such a Google Earth may not be as precise as plans – it does offer useful validation in terms of providing a 'living' plan of the site, where architecture and usage of areas may not actually match that given in the plans. Finally, the testing of a simulator by field experts can provide useful validation in terms of visual accuracy and that of the look and feel of the simulation.

5 Conclusion

Threats to critical infrastructure are not submissive. They constantly evolve, and so too must the ability to defend against such threats. An interactive high-fidelity simulation tool greatly adds to the ability of experts to conduct multiple risk assessments often without the need to physically deploy professional security advisors to the field, providing a considerable cost saving on both time and travel.

Leveraging games technology allows simulation scenarios to be rapidly constructed at a very high fidelity and immediately tested. The networked gaming technology allows remote experts to interact in an intuitive environment and explore, identify and assess the critical components of the infrastructure. The scenario can be modified and different configurations can be examined and tested to ascertain the impact of the change on the risks to the critical infrastructure in consultation with security experts.

Furthermore, the importance of understanding of "consequence" in overall security risk mitigation becomes more obvious because of the visualisation process. Understanding consequence helps in ascertaining the cost to implement mitigation strategies relative to security and return of investment; a crucial budget aspect for companies. With that in mind the consideration of consequence in today's security environment is not only relevant but important in resource determination for the allocation of funds and prioritisation. The use of this type of technology offers a substantial improvement on the cost of conducting a series of risk assessments in the field and allows a company to have a time relative working model of their whole complex. This can be used at any time to test and improve the security measures in place at minimal cost.

References

1. Trusted Information Sharing Network for Critical Infrastructure Protection: Critical Infrastructure Protection National Strategy, Canberra: Trusted Information Sharing Network (2004).
2. Radvanovsky, R.: Critical Infrastructure: Homeland Security and Emergency Preparedness. CRC Press, Boca Raton (2006).

3. Gosch, E.: WA gas supply cut 30pc by blast at Varanus Island, The Australian (2008) (accessed on 11th February 2010), http://www.theaustralian.news.com.au/story/0,25197,23824148-5006789,00.html.
4. Sydney Morning Herald: WA faces $6.7b gas bill, Business Day, The Sydney Morning Herald (2008) (accessed on 11th February 2010), http://business.smh.com.au/business/wa-faces-67b-gas-bill-20080710-3cxn.html.
5. Manunta, G.: Risk and security: are they compatible concepts? Security Journal, 15, 43-55 (2002).
6. Thornton, W.E., McKinnon-Fowler, E., Kent, D.R.: Stalking security statistics. Security Management, 35(4), 54-59 (1991).
7. Gibson, S.D.: The case for `risk awareness', Security Journal, 16, 55-54 (2003).
8. Talend, D: Prototyping of the virtual type, ControlDesign.com (2008) (accessed on 26th August 2008), http://www.controldesign.com/articles/2008/168.html.
9. Pederson, P., Dudenhoeffer, D., Hartley, S., Permann, M.: Critical infrastructure interdependency modeling: a survey of U.S. and International research. Idaho National Laboratory Technical Report (2006).
10. Garage Games: Torque Game Engine (2010) (accessed on 11th February 2010), http://www.torquepowered.com/.
11. International Atomic Energy Agency. Application of simulation techniques for accident management training in nuclear power plants (2003).
12. USGS – The U.S. Geological Survey (2010) (accessed on 5th January 2010), http://www.usgs.gov/.
13. Google Earth, http://earth.google.com.