Computer Network Simulation and Network Security Auditing in a Spatial Context of an Organization

Andrzej J. Zaliwski
City University of New York, USA

zaliwskia@acm.org

Abstract

The business organizations currently functioning inside cyberspace are vulnerable to threats and forms of crimes that were unknown prior to the Internet era. New challenges for security have emerged from this situation. It has become increasingly necessary to educate a large number of professionals to be better prepared to maintain the growing number of computer networks. Also, there is a need to place strong emphasis on the security aspects of a network. These goals are impossible to realize without solving the following problems: lack of safe infrastructure, where security experiments can not compromise the organization's security; and the complexity of existing security auditing methodologies which limits the number of professionals who are able to use them. The complexity makes difficult to obtain a bird-eye view of the whole company's security system in a way similar to tactical and strategic military map. This hinders the ability to have a single complete status of an organization. This paper describes a tool that can be used to overcome the above problems.

Keywords: information system security auditing, survivability, 3D interface, network visualization

Introduction

Very often, used biological metaphors are used to describe compound organizational issues due to difficulties in explaining these issues. Business organizations can be compared to biological systems that function within an ever-changing environment. The life cycles of the organizational organisms are identified not only with manufacturing processes but also with processes involved in fulfilling customer needs.

Companies must survive among similar competitive organisms (other companies and corporate predators). Learning organizational concepts that were so popular some time ago and process improvement methodologies are really about learning the techniques of survival. The process improvement concepts typically consider environmental conditions for doing business (such as market relationships, customer demand, technological development enables innovations in products, government regulations, stock market, and competitors for doing business) and how they fit together internal organizational processes and environment challenges. Other competitors were recognized as being potential enemies to a company. The internal structures of the company are viewed as they evolve toward greater flexibility and adaptability to environmental changes.

The integration of business infrastructure around computer networks creates new threats for the business organization. There are dangers which are not coming from the same kind of corporate organisms which behave according to well defined business rules and customs so the old methods will not work in dealing with these threats. The new threats are in *micro* scale rather than *macro* scale, where competitors operate. Micro threats are like a cancer or parasites that can destroy organisms from the inside (e.g. bad guys inside a company). There are other micro scale organisms that can attack a company from the outside like insects (e.g. hackers and crackers) and bacteria or viruses (e.g. computer viruses, worms, Trojans).

The first group of threats (referred to in this paper as *macro* threats) is strictly related to day-to-day business activity and are a natural result of regular business activity of competitors, some government regulations, market fluctuations, ever-changing customer needs, technology embedded into products and services, changes in manufacturing and management processes, etc. These factors create an uncertainty when managers make business decisions because any or all of these macro threat factors can harm an organization. However problems created by macro threats are solved on a day-to-day basis using managerial practice and experience. Business competitors and government must operate within limits drawn by law, customs, and business rules. Because the rules of behavior are more clearly defined, there is less mystery about this type of threat.

The second group of threats, micro threats, is created by people who do not feel obliged to obey the law or any other rules, who often work for their own profit, for ideologies (which are sometimes stupid), or for revenge. These people often select their targets randomly. They are not a part of the business game and do not follow the common rules. The development of new telecommunication and computer technologies has created a world where more and more areas of our life are moving into cyberspace. The institutions functioning inside cyberspace have become vulnerable to new threats and new forms of crimes that were unknown before the Internet era. New challenges for security have emerged. It is becoming necessary to educate a growing number of better prepared professionals to maintain growing numbers of computer networks. Also, stronger emphasis should be placed on security aspects. These goals are impossible to realize without solving the following problems:

The ***first problem*** is that experiments with software that is related to network security such as software that tests the security of a network and experiments with different software and hardware configurations may compromise the network security of an institution. Many teaching institutions can rarely afford dedicated computer laboratories that are excluded from the university's network infrastructure and solely used for data communications and networking courses so the actual system is vulnerable during these tests.

The ***second problem*** is the complexity of existing security auditing methodologies that limit the number of professionals that are able to use these technologies. Typically risk auditing methodologies requires gathering and processing of large amount of data. A large number of forms, data from interview, access rules, descriptions of responsibility, policies and codes developed inside a company are processed with the typical auditing methodology. Dealing with this information and understanding it becomes a problem. The complexity makes it difficult to obtain a bird-eye view of the whole company's security system in a way similar to a tactical and strategic military map, both from macro and micro perspective described earlier in this paper.

The current trend is toward understanding the whole perspective of a protected system. So it is necessary to have a convenient software tool that can map an existing protected system. If organizational databases and information systems are functioning as business models of real existing organizations it is also necessary to create a kind of information system which will be an up-to-date model of all aspects of organizational security – a foundation for risk assessment or security auditing methodologies. This security model should be related to organizational structure, spatial

relationships and organizational policies and procedures. If possible, an organizational learning model should also be employed. This will allow modernizing existing organizational processes along with security needs. The ideal situation will be when all three processes: organizational process development, information system development, and security policies and practice will be aligned with each other. It is necessary to propose a compact integration model.

The next chapter contains a review of related solutions and the chapter after that one will contain a more detailed description of the proposed system.

Related Solutions

According to Mead, Ellison, Linger, Longstaff, and McHugh (2000) current software-development life-cycles are not focused on creating survivable systems and survivability issues are often relegated to separate threads of project activity, with the result that survivability is treated as an add-on property. According to Moore, Ellison, and Linger (2001) people designing information systems do not use data obtained as a result of attack or security vulnerabilities to improve their designs. System designers do not learn from documented security attacks. However survivability has become a more and more popular topic and there are several papers which draws theoretical frameworks for building survivable systems (Linger & Moore, 2001; Elison & Moore, 2001).

The existing software solutions related to parts of the system proposed in this paper can be categorized into three main groups:

1. Creation of a virtual network embedded in an existing real computer lab network

Virtual networks contain many virtual computers. There are typically two technologies able to simulate many computers with different operating systems on one machine:

a) Solutions employing open-source software: User-Mode Linux (Netkit, 2004; Spennenberg, 2004)**.** There are several similar systems that use User Mode Linux for teaching networking courses by creating a virtual network. The most important are:

- A solution proposed by McEwan (2001), which is the complicated virtual network with subnets simulated on one real machine and connected to a university network.
- Netkit (2004) (University of Roma, Italy), which is software created on User Mode Linux which makes experimentation with different network topologies possible.

b) Solutions employing commercial software: VMWare™ (Kneale & Box, 2003; Kneale, De Horta, & Box, 2004).

A characteristic example of solution based on VMware is Velnet (Kneale & Box, 2003; Kneale, De Horta, & Box, 2004). Velnet is a Virtual Learning Environment based on VMWare™ and VNC (VNC is the cross-platform software which allows remote control between different types of computers). VMWare (VMWare, 2004; VMWare White paper, 2004) encompasses multiple-hardware environments, simulating many different computers with different operating systems on one host machine. Having a virtual network among these machines is one of the VMWare functions. From the other side, VNC is used to obtain access to the console of each simulated computer via the Internet through the Remote Desktop Display. Students may control remote machines from anywhere by accessing the Internet. The virtual computers are displayed on the student's computer as a separate window. According to (Kneale et al., 2004) this system is based on a 2D based "virtual reality".

c) There are also some proprietary and rare solutions, which use specially written programming language modules (Lee, Ma, Du, & Schnepf, 1997).

2. Graphical network visualization and visualization

The majority of existing network visualization tools display information coming from the existing physical network. In most cases information is gathered by additional software installed on servers or the information is based on traffic analysis. The revealed logical or physical topology is represented as a spatial metaphor. In most cases network topology is represented as a graph structure spanning different geometric shapes (for example CAIDA: http://www.caida.org). There are many network monitoring and visualization tools that are based on the above concept.

Another interesting project is *CyberNet*. A 3D-visualizing metaphor is used to represent data coming from the real world. The solution is based on the one-way mapping of the real network into a 3D metaphor. The administrator may use a schematic building metaphor to solve problems related to geographic proximity (Abel, Gros, Santos, Loisel, & Paris, 2000). A real physical (not virtual) computer is represented as an object in 3D space. This object displays the attributes of a real computer. The real network is mapped into the virtual environment, but the system administrator cannot run programs or configure real computers by using virtual reality. This allows only one-way mapping of selected information: from a real network into a geometric 3D network model.

3. Network Design Software, Visual System and Network Administration and Management

Another group of tools (software used for network design, i.e. NetViz) may display networks under design as a set of symbols on 3D layers. This kind of software is nothing more than an advanced graphical editor. No type of network simulation is implemented in this tool.

Another example uses the popular game Doom as a network administrator interface. The Linux processes are displayed as monsters in the 3D maze. The system administrator may "shoot" unneeded processes in the same way game players would (Chao, 2001).

Examples of teaching network security ideas based on flat (2D) animation and metaphors are described in Bergstrom, Grahn, Karlstrom, Pulkkis, and Astrom (2004). Kazitow and Nelayev (1998) describes some adaptable and usable methods for teaching the concept of the virtual laboratory, however the paper is primarily focused on Chemistry.

Proposed Solution

First, as mentioned in the introduction, creating a safe environment for experimenting with security related software and network configuration will be solved by moving the network laboratory into virtual reality. After requirement gathering, the designed computer network will be built inside a "walkable" virtual building resembling real company. Using User Mode Linux all computers placed in virtual reality will behave like real computers. In this way a safe environment for teaching can be created and experiments with security related software can be conducted without compromising the security of a real network.

In modern business organizations, the computer network is created as the background for information system. However, databases were, early on, recognized as a foundation for building an information system. Computer network design is often considered separately from information system design. Some positive exceptions are described in McCabe (1998) and Oppenheimer (1999) that lean in the direction of recognizing a computer network as an important part of the information system. Methodologies presented in McCabe (1998) and Oppenheimer (1999) refer to the same phases which can be found during development of the information system. A proposed system will use a spatial representation of a company for network design (a backbone for information systems). Using this representation makes possible graphical analysis of information flows and better design of a physical structure of a network.

The proposed tool will collect information in the repository during a network design phase. This information will be used by another subsystem built upon the lowest level responsible for network design. The overall company structure together with the embedded design of a computer network will be used in later stages as a 3D map supporting the gathering of other data necessary to enable information system auditing. The organizational structure chart shows nothing about the spatial relationship (e.g. security perimeter for a given server). Potential threats could be related to possible physical access to that room as some threats depend on location. The proposed interface will shows the real physical organization of network in spatial context of an organization and location of other assets necessary for performing business operations. The auditing tool will utilize a 3D map created in the first stage.

The same graphics interface will be used for many different but related purposes: network design, testing software on a virtual network, and security auditing of a company. Lastly, the light-weight auditing methodology will be developed. Three different applications of a proposed interface are summarized in Table 1. The 3D interface will visualize data coming from three different subsystems: spatial models of a company, security auditing metadata repositories, and virtual networks.

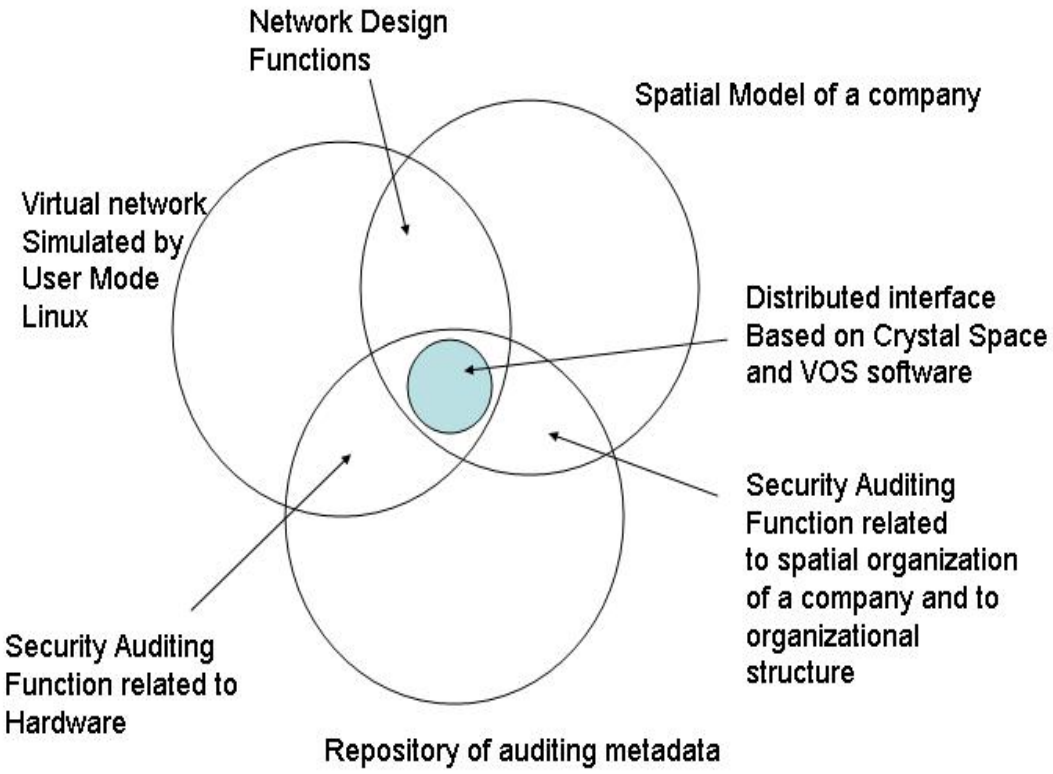


Fig.1. The architecture of a proposed system. The circles represent appropriate servers. The common parts of the circles represent functions of the 3D interface

Table 1 summarizes the different possible applications of a proposed system.

Table 1. The different levels determining uses of a proposed interface.	
A Network Design or teaching of the Network Design.	Network design takes into account a spatial structure of an organization. Information flows among different organizational entities may be represented on a 3D map and taken into account for physical network design. The interface may support network design methodologies described in McCabe (1998) and Oppenheimer (1999). These methodologies are strongly related to these that are used for information system design.
Real Network simulation, prototyping, testing or teaching security related software	Each virtual computer placed in a virtual company will behave as a real physical computer and may run any kind of software. This makes it possible to use proposed system as a prototyping tool. The virtual network also creates a safe testing environment for experiments with security software that may affect real network.
Information System security auditing	Auditing may take into account spatial aspects of a company organization and physical protection of a computer. Metadata repository and proposed simple methodology will use a 3D map of an organization together with a network embedded into it. This will create the 3D navigational structure in a form of Virtual Reality world. Each entity of this world will be associated with related metadata from the Repository.

The system proposed in this paper is based on existing open source software like User Mode Linux (for virtual network), a spatial structure built upon VOS and Crystal Space, and a repository of auditing metadata built upon open source database software. The overall distributed system will utilize three servers (Fig 1.): one for the virtual network, one for spatial structure, and one to maintain a metadata repository. The system proposed in this paper combines two promising techniques in an innovative way. The Virtual Computer Networks on one side, the Virtual Reality on the other. Virtual Computer Network is provided by User Mode Linux (UML), and virtual reality is maintained by VOS open source software based on Crystal Graphics 3D-engine. VOS (http://interreality.org/) is an infrastructure for object-oriented network communication, especially multi-user collaborative virtual environments.

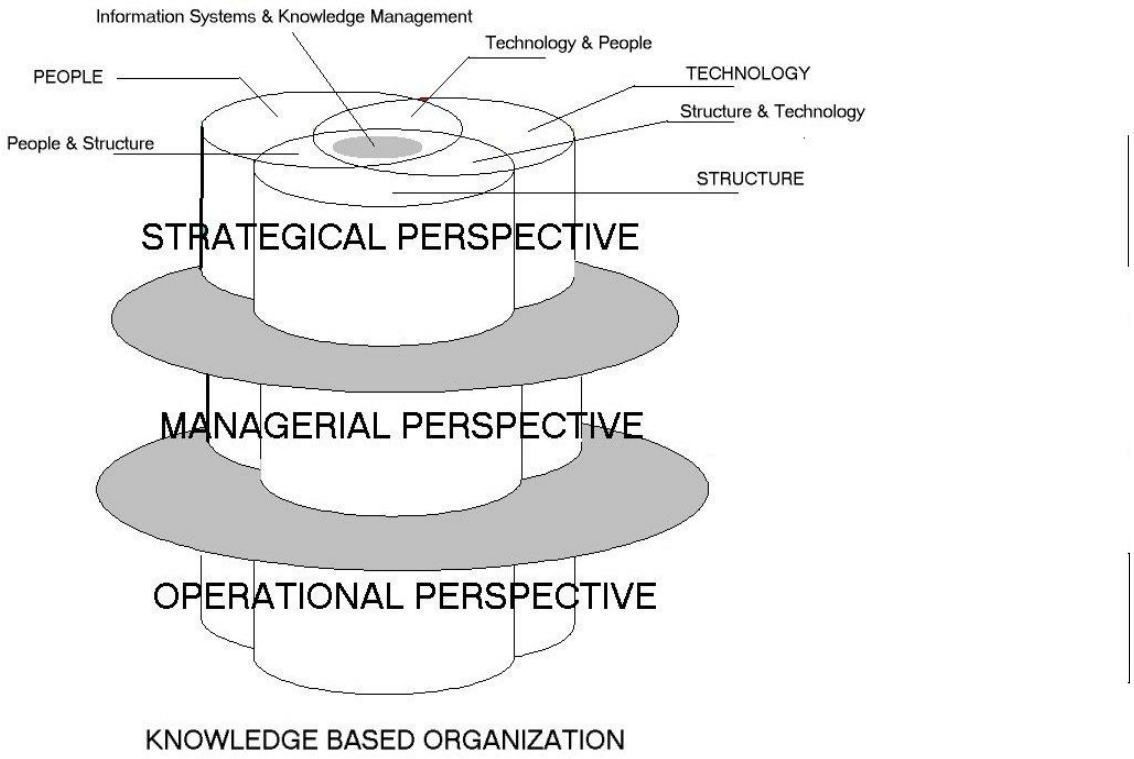
The architecture of the proposed system is described in Figure 1. One computer is used as a host for virtual machines created and maintained by *User Mode Linux* (*UML*). A second computer will be used as a server for the virtual world. Clients will communicate with the graphic server by using light-weight agents (it will be used from existing open source agent systems) instead of communication mechanisms provided by VOS. Additionally, to gather the design data and to keep metadata necessary for auditing, a third server will be provided. This third server software may work on the same machine at which spatial structure (*VOS*, *Crystal Space* 3D engine) is main-

tained. Three computers on the conceptual model of the system are used (presented in Fig. 1), but in practice using two separate computers as servers should be enough.

The interface software will be build over three existing open source application (UML, VOS, MySQL or PostgressSQL). For this project, it is necessary to create an effective communication channel between the two above mentioned software subsystems (*UML, VOS*, and repository). Creation of a virtual computer in virtual space on the graphic server should create and run related processes on the hosting *UML* server. Any change in virtual space should be reflected on a virtual network functioning on the hosting server. Additionally, all operations in virtual reality should be reflected in a repository.

Computerized support for network design methodology and for security auditing methodology

The existing information systems security auditing methodologies are often very complicated. Using these methodologies requires one to go through extensive documentation and seminars offered by companies or institutions that make these methodologies available. This limits the number of experienced professionals available to meet these needs as demands for professionals are growing. The solution may be the lightweight and easy to learn methodology affordable for small companies and teaching institutions. The general concept of this methodology is described below.



Fig, 2. The Knowledge based information security framework integrating different systems and areas of a business organization. (Zaliwski, 2003)

The auditing methodology framework (Fig. 2) will employee the knowledge management framework described by author of this paper in Zaliwski (2003). Knowledge management may be recognized as a usable integration paradigm for all information systems functioning inside a company. The knowledge management model shown in Figure 2 is comprised of three traditionally recognized organizational subsystems: *People*, *Technology*, and *Structure*. (These items are also related to the structure of the proposed interface presented in Figure 1: *Structure* (spatial and organizational structure), *Technology* (network and software comprising an information system),

People (metadata in the Repository)). The overlapping parts between these three subsystems are areas of mutual influence between information technology and organizational structure, organizational structure and social systems, and information technology and people (social aspects of an organization). Everything revolves around a knowledge management core. The central core area is the border of all the above areas, and is where the knowledge management and information systems functions take place. To achieve sustained competitive advantage (and survive as an organization), it is necessary to balance all of the above areas. Information Technology and Knowledge Management, together with all organizational subsystems, reach across all organizational levels (operational, managerial, and strategic). On each level, the mutual influence of all organizational factors should be recognized. For example on an operational level the basic protection should be recognized, access rules for personnel, security perimeter, should be established and so on. These basic items leading up to the top of the framework structure will build organizational security policies and survival strategy.

Conclusion

The project's distributed environment will combine in innovative ways several advanced techniques related to computer graphics (games and virtual environments) with computer networking and agent technology. The obtained results may be used in any distributed VRML environment. Additionally a lightweight information systems security auditing methodology is proposed as an educational alternative for sophisticated and large CERT related methodologies.

In the area of **Design:** The proposed system delivers a 3D virtual environment in which design processes may occur. The design data will be stored in a repository.

In the area of **Research**: The proposed system creates a safe *test bed* for experimentation with different network security related software.

In the area of **Teaching:** By using the described tool the following advantages over the traditional course are expected:

- Dynamic visualization of the course concepts that deal with complexity and that will improve student perception of the presented concepts.
- The material should be easier to understand and will involve teamwork due to the nature of the presentation.
- The creation of student interest, the development of imagination, and an attractive course delivery will increase effectiveness. Students may find learning with the help of a computer more interesting and challenging. The educational advantages of using games are presented by Kirriemuir (2002).
- The proposed solution may be targeted toward the delivery of network security courses. The security issue is becoming more and more important and awareness of security threats is increasing. The system proposed in this paper, along with other applications, may be used as a background for the creation of educational simulation games for computer security specialists such as those proposed by Irvine and Thompson (2003).

In all cases, the proposed system should reduce costs and the need to have an expensive specialized laboratory devoted to research or teaching topics related to network security. They also make network courses and research affordable for small budget institutions or for disabled students and researchers.

References

Abel, P., Gros, P., Santos, C.R.D., Loisel, D. & Paris, J.P. (2000). Automatic construction of dynamic 3d metaphoric worlds: An application to network management. In J. R. Erbacher, P. Chen & C. Wittenbink (Eds.), *Visual Data Exploration and Analysis VII*, volume 3960, Jan., pp 312-323.

Bergstrom, L., Grahn, K. J., Karlstrom, K., Pulkkis, G, & Astrom, P. (2004). Teaching network security in a virtual learning environment. *Journal of Information technology Education*, *3*.

Chao, D. (2001). Doom as an interface for process management. *SIGCHI'01, March 31-April 4, Seattle, WA, USA*.

Dalgarno B., & Harper B. (2003). 3D Environments for spatial learning: The importance of learning task design. *Proceedings of the 20th Annual Conference of the Australasian Society for Computers in Learning in Tertiary Education (ASCILITE), Adelaide, Australia*, 7-10 December 2003. Retrieved June 3, 2004 from http://www.ascilite.org.au

Ellison, R. J., & Moore, A. P. (2001). Architectural refinement for the design of survivable systems. *Technical Note CMU/SEI-2001-TN-008*. Carnegie Melon, Software Engineering Institute.

Irvine, C.E. and Thompson, I. (2003). Teaching Objectives of a Simulation Game for Computer Security. *Proceedings of Informing Science Conference*, *Pori, Finland*, June 24-27.

Kazitov, M.V., & Nelayev V.V. (1998). Active virtual laboratory at Internet as an effective tool for learning. *Global Congress on Engineering Education*, *Cracow, Poland*, 6-11 September 1998. Retrieved Sept, 1st, 2004 from http://thunder.prohosting.com/mvkazit/papers/usicee98/

Kirriemuir, J. (2002). Video gaming, educational and digital learning technologies. *D-Lib Magazine*. Retrieved Sept, 1st, 2004 from http://www.dlib.org/dlib/february02/kirriemuir/02kirriemuir.html

Kneale, B. & Box, I. (2003). A virtual learning environment for real-world networking. *Proceedings of the Informing Science Conference*, *Pori, Finland*, June 24-27.

Kneale, B., De Horta, A. Y., & Box, I. (2004). VELNET (Virtual Environment for Learning networking). In R. Lister & A. Young (Eds.),. *6th Australasian Computing Education Conference (ACE2004),* Dunedin, New Zealand. *Conferences in Research and Practice in Information Technology*, Vol. 30

Lee, Y-J, Ma, W-H, Du, D.H.C. & Schnepf, J. A. (1997). Creating a virtual network laboratory. *International Conference on Multimedia Computing and Systems (ICMS'97),* June 03-06, Ottawa, Ontario, CANADA, p. 642 Retrieved from http://csdl.computer.org/comp/proceedings/icmcs/1997/7819/00/78190642abs.htm

Linger, R. C., & Moore, A. P. (2001). *Foundations for survivable system development: Service traces, intrusion traces, and evaluation models*. CMU/SEI-2001-TR-029, ESC-TR-2001-029. Carnegie Melon, Software Engineering Institute

McCabe, J. D. (1998). *Practical computer network analysis and design*. San Francisco, CA: Morgan Kaufmann.

McEwan, W. (2001). Using academic research methodologies to improve the quality of teaching: A case study. In *Proceedings of the Fourteenth Annual Conference of the NACCQ*, Napier, New Zealand: pp. 83-93. Retrieved Nov. 1st, 2004 from http://user-mode-linux.sourceforge.net/case-studies.html

Mead, R. N, Ellison, R. J., Linger, R. C., Longstaff, T., & McHugh, J. (2000). *Survivable network analysis method*. Technical Report CMU/SEI-2000-TR-013, ESC-2000-TR-013. Carnegie Melon, Software Engineering Institute

Moore, A. P., Ellison, R. J., & Linger, R. C. (2001). *Attack modeling for information security and survivability.* Technical Note CMU/SEI-2001-TN-001, March 2001. Carnegie Melon, Software Engineering Institute

Netkit. (2004). The poor man system for experimenting computer networks. Retrieved from http://www.netkit.org

Oppenheimer Priscilla. (1999). *Top-DOWN NETWORK DESIGN. A systems Analysis Approach to Enterprise Network Design*. Indianapolis: Macmillan Technical Publishing.

Spennenberg, R., (2004). Emulating network using user-mode Linux. *SysAdmin, the Journal for UNIX and Linux System Administrators.* Retrieved from http://www.samag.com/print/

VMWare (2004), http://www.vmware.com

VMWare White Paper (2004) http://www.vmware.com/vinfrastructure

Zaliwski, A. (2003). Step toward information systems curriculum based on knowledge management framework. *IIAS-Transaction on Systems Research and Cybernetics*, Vol. III, No. 1. *International Journal of the International Institute for Advanced Studies in Systems Research and Cybernetics.*

Biography

Andrzej J. Zaliwski is an assistant professor of Information Systems at the College of Staten Island, City University of New York, since 2001. He received a M.Sc. in Mathematics (numerical methods and programming) at the M.C. Sklodowska University (UMCS), Lublin (Poland) in 1986 and a Ph.D. in Computer Graphics at the Academy of Mining and Metallurgy (AGH), Krakow (Poland) in 1991. From 1984 to 1990 he worked at UMCS Lublin (Poland), 1990-2000 – Computer Science Dept. of the Academy of Economics, Krakow (Poland), 2000-2001 – Computer Science Department, University College Cork (Ireland). His research interests include databases, information systems, computer networks, and knowledge management.