A Conceptual Model as an aid to student understanding of Network Security

G. Kohli, S. P. Maj, G. Murphy and D. Veal
Edith Cowan University, Perth, WA, Australia
g.kohli@ecu.edu.au

Abstract

Security is amongst the most widely discussed topics in today's world of high speed networking. Security broadly deals with problems that affect millions of computer users around the world either through the spread of viruses, or information theft from personal computers and network servers. Security issues can encompass large quantities of detailed information which can overwhelm network administrators. Security systems are traditionally often layered in a top-down manner. Abstract models could enable administrators to focus upon relevant details whilst filtering out non-essential details. Such models could also be used in a top-down fashion thus permitting the control of complexity via recursive decomposition. There are currently many security models used in industry and for teaching students about network security. These models are not only restricted to confidentiality, authentication, data integrity, non-repudiation, and access control, but also take into account physical and human aspects that can effect security. A model based upon Finite State Machines (FSM) and called a state model is proposed as an aid to device level management.

Introduction

The Internet is the driving force behind the rapid development of Computer and Networking technology. Whilst the Internet offers fast communication and ease of use, there are inherent problems. There has been a growing concern about information theft [1] and virus outbreaks on the Internet [2]. Furthermore Cisco notes with regard to corporate networks: "… *when you connect your network to the Internet, you are physically connecting your network to more than 50,000 unknown and all their users. Although such connections open the door to many useful applications and provide great opportunities for information sharing, most private networks contain information that should not be shared with outside users on the Internet*" [3]. This gives the traditional administrator little choice but to protect and monitor the security of their networks. Security is one of the key tasks required of systems administrators.

The OSI seven layer model for networking was developed by ISO (International Standard Organisation) to define standardized methods for designing internetworks and their function. Its goal is to provide standards to which all computers hardware and software vendors will adhere, so that multiplicity of interconnection and interface practices could be reduced, thus reducing the costs of designing and producing both hardware and software. It is "*A suite of protocols and*

standards sponsored by the ISO for data communications between otherwise incompatible computer systems" [4]. The ISO code 7498-2 [5] defines the following:

- Five types of security services
- Eight security mechanisms that support the above services
- Three required OSI security management methods.

The three dimensional graph put forward by ISO 7498-2 committee is shown in Figure 1.

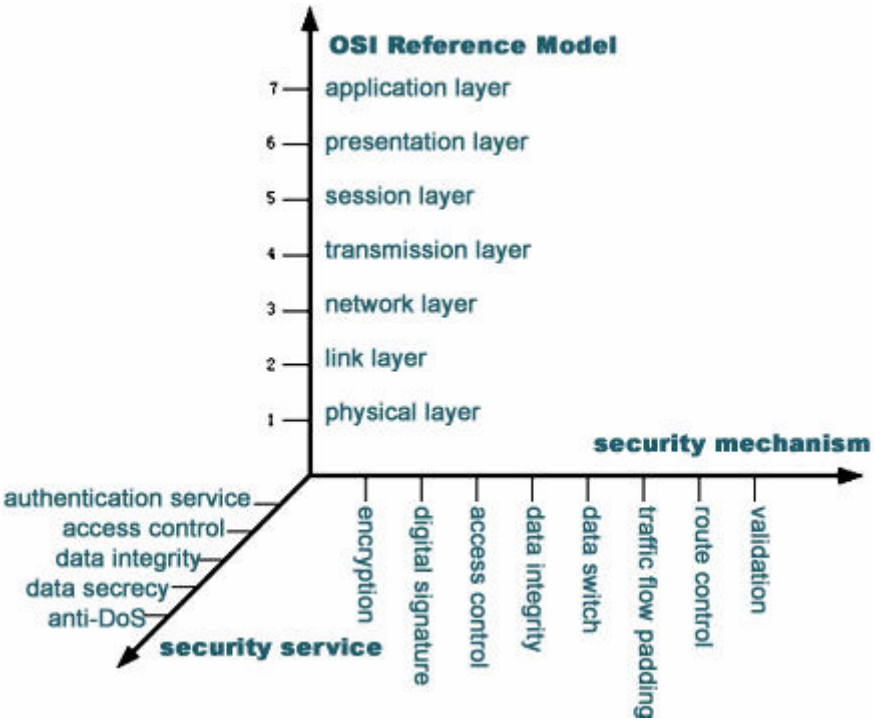

Figure 1: ISO 7498-2 3-dimentional graph [5]

There are currently many security models used in industry and for teaching students about network security [6,7]. Some of these models are based upon the OSI model [8] and the IPsec Protocol Framework [9]. IPsec, in turn, relies on existing algorithms to implement the encryption, authentication, and key exchange [10]. Other security models not based upon the OSI framework are premised upon role based models [11]. However, most of the security models developed to date are inadequate in the collaboration area [12]. Whilst these models help administrators to understand security they may fail to provide an insight into security issues relevant to networking devices, i.e. the switches and routers that actually handle security. There is a need to develop a conceptual security model which can help networking administrators gain a clearer understanding of security issues on the networks they are managing.

At the device level network security deals with protocols, and all protocols can be expressed as finite state machines (FSM) [13]. Using a FSM, protocols can be modelled to exist in one of a number of defined states. In order to address implementation-specific details there is a need to

consider protocols and the modeling of them to explain how internetworking devices e.g. (switches and routers) model security.

State Models

Models are a means of controlling detail and assisting communication. Among desirable characteristics are that any model is diagrammatic, self-documenting, and easy to use and permits hierarchical top-down decomposition to control detail. Levelling is the property in which complex systems can be progressively decomposed to provide completeness.
"*A model may be described as the body of information about a system gathered for the purpose of studying the system. It is not only an orderly collection of information, but is an orderly representation or structuring of the information. The characteristics should be representative of the characteristics of the real system* [14]. With respect to complex systems Burgess notes that "*System administration is full of intangibles; this restricts model building to those aspects of the problem which can be addresses in schematic terms. It is also sufficiently complex that it must be addressed at several different levels in an approximately hierarchical fashion* [15].

According to Cooling there are two main diagram types of diagrams: high level and low level [16]. High level diagrams show the overall system structure with its major sub-units. By contrast, low level diagrams are solution oriented and must be able to handle considerable detail. Both high and low level systems may be represented by state models. One form of state model is an FSM. According to the National Institute of Science and Technology *A finite state machine is a model of computation consisting of a set of states, a start state, an input alphabet and a transition function that maps input symbols and current states to the next state. Computation begins in the start state with an input string. It changes to new states depending on the transition function* [17].

At any given moment in time the system exists in a certain state. The set of all states is the state space. Significantly the state diagrams should show only details that are relevant to the current state. Two simple state models have been developed – one for a switch and one for a router [18]. However unlike typical state models these new models allow the introduction of progressively advanced conceptual features hence they provide scalability and complexity control [19]. Furthermore, Burgess, under a chapter heading "*Analytical Systems Administration*", notes that: "*… now days many computing systems are of comparable complexity to phenomena found in the natural world and our understanding of them is not always complete, in spite of the fact that they were designed to fulfil a specific task. In short, technology might not be completely predictable; hence there is an need for experimental verification"* [15] .

State models can be extended to model security starting with the physical layer. The physical layer is responsible for the physical communication between nodes. It is concerned with the actual encoding and transmission of data into electricity. The physical layer is critical as far security and delivery of communication data is concerned. Van Eck states the following with regards to eavesdropping on the physical layer *it is possible in some cases to obtain information on the signals used inside the equipment when the radiation is picked up and the received signals are decoded. Especially in the case of digital equipment this possibility constitutes problem,*

because remote reconstruction of signals inside the equipment may enable reconstruction of the data the equipment is processing [20]. Physical security is vital in any network [21].

Switch Security Model

Maj proposed a diagrammatic state model of a switch [19]. Each physical port is represented on the switch model (e.g. Fastethernet 0/1 or Fa0/1). At the simplest level, connectivity can be represented by internal connections between the ports within the switch. At a more complex level switches perform three main tasks: address learning; address forwarding and filtering; loop avoidance. A simple table can be incorporated into this diagram to show how a switch learns and hence maps physical MAC addresses to ports i.e. address learning. This table can be then be used to show how a switch establishes one to one connectivity (micro-segmentation) and hence performs address filtering and data forwarding. Figure 2 provides an overview of the switch state model [19]. An advantage of the switch state model is that it includes in a single diagram capture the key features of the switch along with the relevant command line outputs (CLI). The model presents information in a hierarchical manner thereby controlling complexity. Furthermore, it provides scalability by expanding the basic switch model to cater for Spanning Tree Protocol (STP) and security [22].

Layer 2 vulnerability details with MAC Address, VLAN, VTP, etc [8]. The switch state model can be modified to include security information. Various CLI outputs such as *show vlan*, *show vtp status*, etc can be used to gather the information about important security information at layer 2. Information gathered from these command can be integrated into a single state single switch security model (Figure 3). It should be noted that Figure 3 demonstrates the models.

TCP/IP	OSI	Implementation
Application	Layer7	NO
Application	Layer 6	NO
Application	Layer 5	NO
Transport	Layer 4	NO
Internetwork	Layer 3 Network	NO
Network Access	Data Link	MAC-Address-Information VLAN | MAC Address | Type | Interfaces 1 | AAAA AAAA AAAA | Dynamic | Fa0/1 2 | BBBB BBBB BBBB | Dynamic | Fa0/2 Interface table Interface | Line Protocol | Type F0/1 | Up | Trunk
Network Access	Physical Layer	Carrier detect table Inteface | Line Status Fa0/1 | up

Figure 2 Switch Model

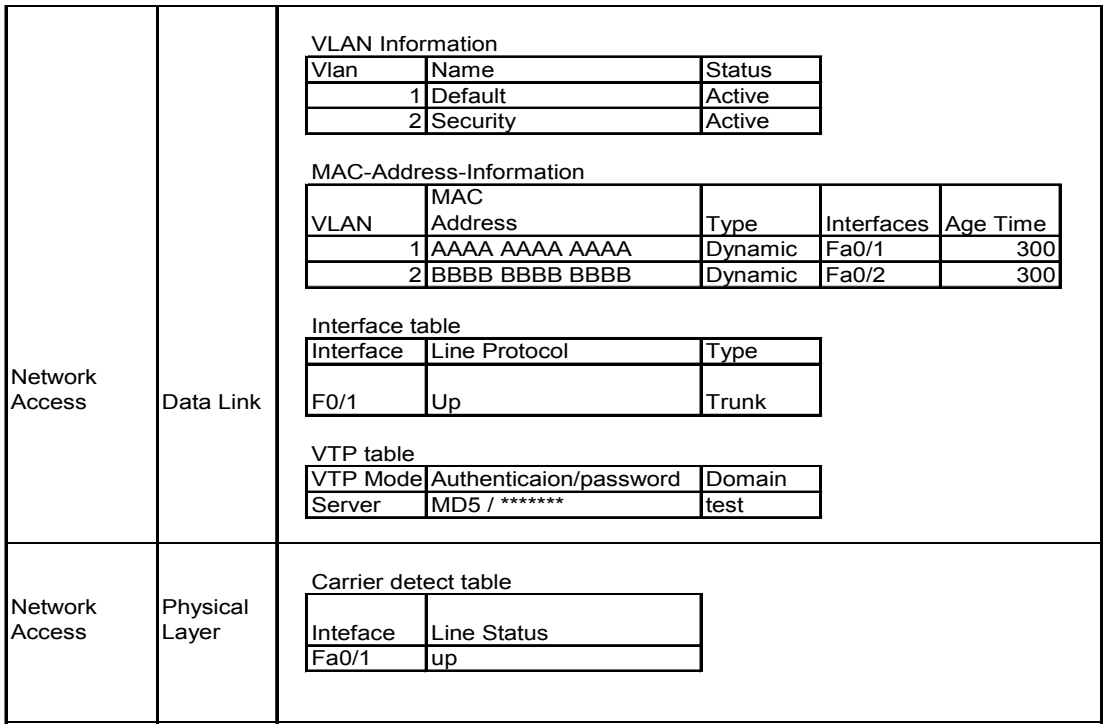

Figure 3 Switch Security Model

A Router Security Model

Similarly a router has been modelled using the ARP and routing table [18]. On a Cisco router the router commands "show arp" and "show ip route" can be used to in conjunction with the diagrams to show the state changes as networks are connected together (Figure 4).

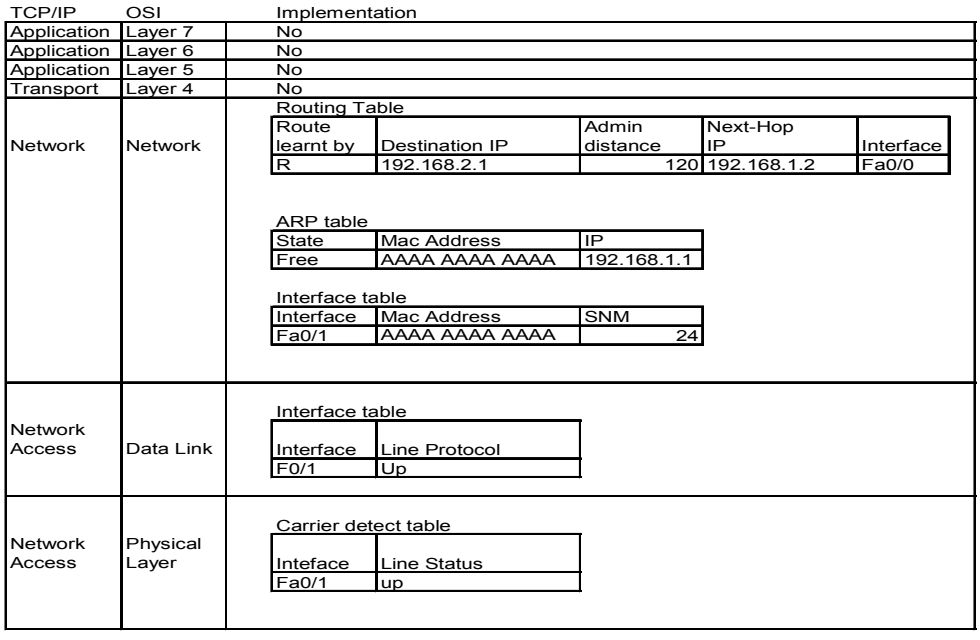

Figure 4: Simple Router Model

Again this simple router model can be further modified to monitor security at layer 3 in the seven layer OSI model. Of major concern at layer 3 are the security of routing protocol updates, and preventing certain packets (which, the authors note, may or may not include routing protocol updates) from being passed to the next router [8].

The exchange of routing protocol updates is used to ensure that all routers in an administrative area, for example a university campus or a corporate headquarters, have a common view of the administrative area, and thus can establish paths, or routes, to every network in that administrative area. Route updates are sent and received by routing protocols, and are always sent in clear text. This means that a potential hacker can use packet sniffing software, examples of which are readily available on the Internet, to intercept and capture routing updates between two routers that are connected on a broadcast, multi-access network e.g. Ethernet. However, some routing protocols will only accept updates from, or send updates to, a neighbouring router if they have a shared authentication method. Some routing protocols do not offer authentication. For example RIP v1 does not provide authentication and broadcasts routing updates from all configured ports every 30 seconds [23]. The solution to this problem can be the use of another routing protocol such as RIP v2, OSPF, or EIGRP which does provide authentication. It should also be noted that most protocols offer both simple authentication and hashed authentication. In simple authentication, passwords are sent in clear text and so can be sniffed. For this reason, simple authentication should not be used to provide security in a production environment. In hashed authentication the key and route update are used to generate a hash, and the hash and route update are then sent to the receiver. The receiver accepts the update and hash, passes the update and its own key through the hash algorithm, and then compares the output with the received hash. If the hashes do not match, the update is rejected. This ensures that a router will only accept route update information from an identified partner, and should guarantee the integrity of the update. It does not, however, guarantee that the sending router has not been misconfigured, or has not passed on data that has otherwise been incorrectly or maliciously injected into the system. As noted previously, the route updates themselves continue to be transmitted in clear text and may be intercepted, thus providing an overview of the network to a sophisticated attacker. The choice of routing protocol depends upon network design and scalability of the routing protocol [24].

It should also be noted that default operation of most routing protocols is to send updates out of all interfaces on a router, if that interfaces network is being advertised by the routing protocol. This means that even when no other router is attached to a broadcast multi access network, the router will send updates out to the network. Again, a sophisticated attacker can sniff the network, capture the updates, and reconstruct the topology from the information obtained. In Cisco routers this default behaviour is overcome by making the interface passive.

The passage of layer 3 packets, which can include routing protocol updates, through a router can be controlled by Access Control Lists (ACL), although Davies notes that ACLs can adversely affect router performance [25]. In an article entitled "The Cost of Security on Cisco Routers" it is stated that *There are significant performance penalties once you enable ACLs, especially long ones that we used in our tests, because an access list cannot always take advantage of the fastest switching technique that might otherwise be available on the router* [26].

Furthermore, dramatic performance reductions after implementing 200-line ACLs have also been noted. Bandwidth degradation can be reduced by using hardware based Private Internet Exchange (PIX) firewalls and layer 3 switches [27]. From the performance perspective, ACLs can

cause serious degradation in network performance but provide extra necessary security. Among other tasks, ACLs may be used as either a packet filter or as a route filter. When used as a packet filter, they can permit or deny transit traffic based on its source IP address, its destination IP address, its TCP or UDP source port, its TCP or UDP destination port, or any combination of these. Thus, for example, a router ACL could be used to permit a single host on a network to access the Internet, while preventing all other hosts on that network from doing the same. When used as route filter, they can be used to permit or deny transit route update traffic about a given destination network.

For the purposes of this paper, the authors are interested in security at layer 3 and how can it expressed using state models. The modified router security state model is shown in Figure 5.

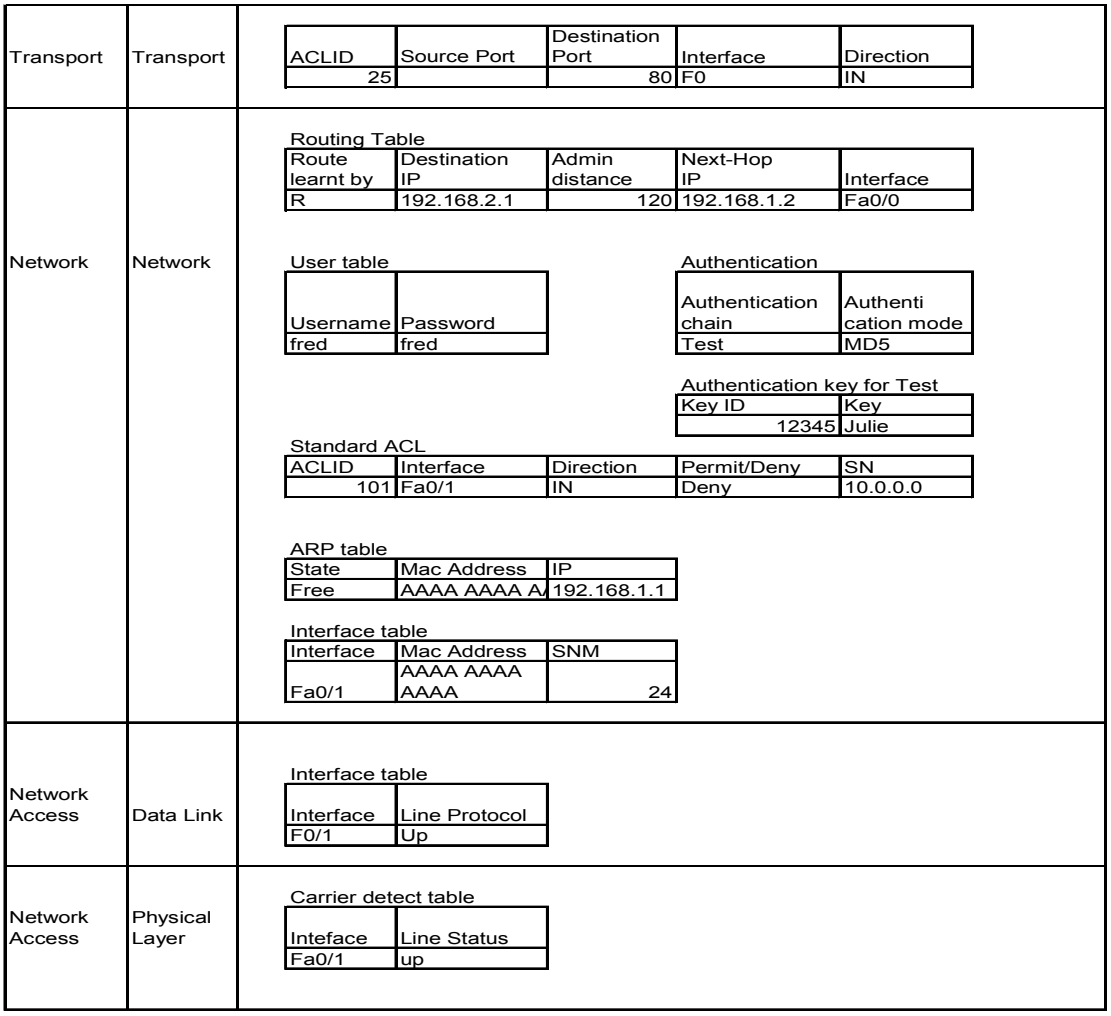

Figure 5 Router Security Model

State Model as an Aid to Teaching Networking

The diagrams were used as the pedagogical foundation of non-vendor based curriculum in networking technology and the results evaluated [22, 28]. Students on two different units were given 20 and 40 hours instruction based on the new models. The results were compared with students

from three other vendor based units who had received 100, 120 and 160 hours of instruction using the standard method of teaching based on the CLI. A networking expert was interviewed by means of a list of questions and the results recorded. The same questions were given to all groups. Despite the large difference in teaching time, the two groups taught using the new state model correctly used far more terms than the other three groups. Furthermore the answers provided by the two groups taught using the new models closely mapped the answers obtained from the expert.

Within education it is well documented that after successfully completing an examination it is not uncommon for the majority of students to demonstrate very poor retention of not only factual information but also concepts. One month after setting their examinations the students taught using the new models were again evaluated. The majority of the students clearly demonstrated that they had internalized the model. On questioning, they were able to reproduce a working model, although this was not an exact copy of the ones provided. Furthermore they demonstrated an understanding of concepts they had been taught. However further work is needed.

State models may provide advantages that network administrators may find useful. Network administrators need to search through various configuration scripts and screens output from the switch and router; this can involve huge amounts of data which can result in 'information overload'. In contrast by using the security state model all the relevant information can be trapped on the state diagram thus providing a more effective method of gleaning appropriate information. The following are some of the potential advantages of security state models:

- They provides a hierarchical view of the network;
- They make fault diagnosis easier to handle;
- A single diagram captures key security vulnerabilities; and
- Information can be hidden via abstraction.
- The uniformity and reproducibility of the model make it much easier to identify sought information.

Potential problems in the use of state models include:

The use of abstraction information could inadvertently be hidden that could prove useful in a particular situation. A limitation of the state model as developed to date is that it only captures information for the bottom four layers of the OSI model. Further work is in progress to model the security of the top three layers of the OSI model.

Conclusions

Understanding security is of crucial importance in today's world of high speed networking. As new vulnerabilities are constantly being discovered one has to provide an insight into security issues relevant to networking devices, e.g. the switches and routers that handle security. The use of a conceptual security model may help networking engineers and computer networking students gain a clearer understanding of relevant security issues on the networks that they manage or study. The use of a state model is proposed for the conceptual modeling of security on

networking devices and covers some of the key issues in networking security. Although no extensive testing has been undertaken by the authors, initial investigation suggests that these models can be of use in aiding the understanding of complex systems handling security. Furthermore, the state models provide advantages of abstraction via the use of levelling and information hiding thereby controlling complexity. This method may also provide a hierarchical perspective of networking devices which may help in fault diagnostics. Further research on state models is currently being undertaken by the authors.

Bibliography

1. Kargl, F., J. Maier, and M. Weber. Protecting web servers from distributed denial of service attacks. in *tenth international conference on World Wide Web*.. Hong Kong: ACM Press. (2001).
2. Kocher, P., et al. Security as a new dimension in embedded system design. in *41st annual conference on design automation*.. San Diego, CA, USA. (2004).
3. Systems, C., Internetworking Technologies Handbook. Cisco Press: Upper Saddle River, NJ. Chap 59 1 (1999).
4. O'Reilly Search. O'Reilly Dictionary of PC Hardware and Data Communications Terms, from http://www.oreillynet.com/search/ (2004).
5. *Security System Module*. (2004).
6. Hung, C.K. and K. Kamalakar. A secure workflow model. In *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003*. Adelaide, Australia: Australian Computer Society. (2003).
7. Dennis, A., *Networking in the Internet Age*. John Wiley & Sons, Inc: New York, NY, (2000).
8. Reed, D., *Applying* the OSI Seven Layer Network Model To Information Security. SANS Institute. 1-29. (2003).
9. Cisco, *Securing Cisco IOS Networks*, C.L. Product, Editor. 2003, Cisco Systems, Inc.
10. Systems, C., *Securing Cisco IOS Networks*. (2003).
11. Sandhu, R. *A lattice interpretation of the Chinese wall security policy*. in *Proc. 15th NIST-NCSE National Computer Security Conference.* US Govt. Printing Office. (1992).
12. Aljareh, S. and N. Rossiter. *A task-based security model to facilitate collaboration in trusted multi-agency networks*. in *Proceedings of the 2002 ACM symposium on Applied computing*. Madrid, Spain: ACM Press. (2002).
13. Halsal, F., *Data Communications, Computer Networks and Open Systems*. Harlow, England: Addison-Wesley. (1996).
14. Pooch, U.W. and J.A. Wall, Discrete event simulation: A practical approach. Boca Raton, FL: CRC Press. 293. (1993).
15. Burgess, M., Principles of Network and System Administration. John Wiley & Sons Ltd: Chichester, England. (2000).
16. Cooling, J.E., Software National Institute of Science and Technology Design for Real-Time Systems. Padstow, Cornwall: Chapman and Hall. (1991).
17. Unknown, National Inst of Science and Tech.
18. Kohli, G., et al. Abstraction in Computer Network Education: A model based approach. in *ASEE.* Salt Lake City, UT. (2004).

19. Maj, S.P. and G. Kohli, *A New State Model for Internetworks Technology.* Journal of Information Technology Education, (2004).
20. Eck, W.V., Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?
21. Beasley, J., *Networking*. Pearson Press: Upper Saddle River, NJ. (2004).
22. Maj, S.P., G. Murphy, and G. Kohli. State Models for Internetworking Technologies. in *34th ASEE/IEEE Frontiers in Education Conference*. Savannah, GA. (2004).
23. Cisco, *Cisco Networking Academy Program: Second Year Companion Guide*. 2 ed. Indianapolis IN USA: Cisco Press. (2002).
24. Grice, M., CCNP Guide to Advanced Cisco Routing. Boston MA: Thomson Course Technology. (2001).
25. Davies, P.T., Securing and Controlling Cisco Routers. Boca Raton FL: Auerbach Publications. (2002).
26. Morris, C., *White Paper:* The cost of security on Cisco Routers. (1999).
27. Bruno, A.A., *CCIE Routing and Switching*. Indianapolis IN: Cisco Press. (2003).
28. Maj, S.P., G. Kohli, and T. Fetherston. A Pedagogical evaluation of new state model diagram for teaching internetworking technologies. in *28th Australasian Computer Science Conference*. Newcastle, Australia: Australian Computer Society. (2005).

GUPREET KOHLI

Gurpreet is a PhD student at Edith Cowan University with three years of experience in Lecturing and Developing Network and Data Communication units at Edith Cowan University. Gurpreet is currently investigating web services and capacity planning of e-business sites as part of his research at ECU.

PAUL MAJ

Associate Professor S. P. MAJ is a recognized authority in the field of industrial and scientific information systems integration and management. He is the author of a text book, 'The Use of Computers in Laboratory Automation', which was commissioned by the Royal Society of Chemistry (UK). His first book, 'Language Independent Design Methodology - an introduction', was commissioned by the National Computing Centre (NCC). Dr Maj has organized, chaired and been invited to speak at many international conferences at the highest level. He has also served on many national and international committees and was on the editorial board of two international journals concerned with the advancement of science and technology. As Deputy Chairman and Treasurer of the Institute of Instrumentation and Control Australia (IICA) educational sub-committee he was responsible for successfully designing, in less than two years a new, practical degree in Instrumentation and Control to meet the needs of the process industries. This is the first degree of its kind in Australia with the first intake in 1996. It should be recognized that this was a major industry driven initiative.

DAVID VEAL

David received an honours degree in theoretical physics from the University of York in England. After completing a Post Graduate Certificate in Education from the University of Keele after which he lectured in physics at South Devon College UK for 10 years. He now lives in Western Australia where he has taught computing, mathematics and physics at high school level. He now lectures in computing science at ECU in Perth, Western Australia. His

areas of research include: Competency-based assessment techniques in computing science, modeling of computers and networks to aid student understanding, and Graphical User interfaces for the partially sighted.

GEORGE MURPHY

George has a BSc degree from the Open University UK. He is a CCNA, CCNP and is a Cisco Certified Academy Instructor (CCAI). He now lectures on the CCNP units at ECU. He also lectures on the CCNP units at eCentral TAFE in Perth Western Australia. He has previously lectured on the CCNA, CCNP, Mathematics and Control Systems units at eCentral TAFE.