An Evaluation of State Model Diagrams for Secure Network Configuration and Management

S P Maj, D Veal,

Edith Cowan University, Perth, Western Australia

Summary
Dedicated firewall devices are an essential component of all secure networks. Given the importance of these devices it is therefore imperative that they are operate according to the appropriate company security policies. Regardless of the sophistication of the security devices they must be managed by people with the associated scope for human error, particularly during their configuration. PIX firewalls are typically controlled by the text based Command Line Interface (CLI) which requires considerable expertise. Whilst a Graphical User Interface (GUI) is available it is not widely used. Alternative approaches have been employed, such as network management tools, but these are arguably also problematic. These problems are exacerbated by the need to manage the integration of many different technologies (firewalls, wireless devices etc). State Model Diagrams have been successfully used for modeling a wide variety of network technologies and associated protocols. The diagrams are modular and hierarchical thereby providing top down decomposition by means of leveling. For ease of use, hyperlinks may be used for navigation within the interface. This paper demonstrates how the state model technique meets the relevant criteria for a successful Security Human Computer Interface (HCI-S) and hence may be used to manage not only firewalls but also the integration of heterogeneous technologies within a secure environment. An evaluation by twenty experienced network administrators strongly supported this approach. Results to date indicate that the State Model Diagrams may offer a vendor independent, universally applicable interface that can be used for secure device integration and management.

Key words:
Firewall, Security Device Manager, State Model Diagrams.

1. Introduction

A secure corporate network is of paramount importance, however, 'In a GCN telephone survey 39 percent of IT and systems managers said keeping their networks secure was their biggest challenge.'[1]. This problem is exacerbated by the need to rapidly respond to security threats, 'Just a few years ago, system administrators had hours or even days to respond to new threats. Now we have only minutes or sometimes seconds.' [2]

Based on company policy network devices must provide a level of security relevant to the needs of the organization. Router based packet filtering by means of Access Control Lists are relatively simple to use but do not maintain stateful information. Proxy filters typically operate on general-purpose operating systems with the associated penalties of performance overheads and increased vulnerability. Stateful packet filters combine packet and proxy filtering technologies and hence are able to keep complete session state information for each session. Each time an IP connection is established (inbound and outbound), the information is logged in a stateful session flow table. This allows individual packets to be analyzed in the context of a valid connection. Such devices include Private Internet Exchange (PIX) firewalls - high performance, dedicated (hardware and software) devices. PIX devices employ the Adaptive Security Algorithm (ASA) for stateful connection control. ASA employs the concept of relative security levels and interfaces must be configured accordingly. The PIX operating system is typically configured and managed by the text based Command Line Interface (CLI). The CLI is a very powerful tool however the output from this interface is complex and requires considerable expertise. This is problematic because, according to Bartal, 'However, firewalls are not simple appliances that can be activated "out of the box". Once a company acquires a firewall to protect its intranet, a security/systems administrator has to configure and manage the firewall to realize an appropriate security policy for the particular needs of the company. This is a crucial task … The bottom line, however, is that the security of the whole intranet depends upon the exact content of the rule-base, with no level of abstraction available. Since the syntax and semantics of the rules and their ordering depend upon the firewall product/vendor, this is akin to the dark ages of software, where programs were written in assembly language so that the programmer had to know all the idiosyncrasies of the target processor.' [3] Furthermore whilst vendor specific GUIs are available they are also problematic.

Manuscript received September 5, 2010
Manuscript revised September 20, 2010

According to Rubin cited by Wool the most important factor in firewall security is configuration. [4] This problem, according to Wool, is further exacerbated by the technical advances of firewalls. Wool continues, 'Most firewall vendors (exemplified by Cisco and Lucent) seem to be unaware of the usability issues related to direction-based filtering. These vendors simply expose the raw and confusing direction based filtering functionality to the firewall administrator. A notable exception is Check Point. In order to avoid the usability problem, Check Point chooses to keep its management interface simple, and hide the direction-based filtering functionality in such a way that most users are essentially unable to use it.' According to Wool this is highly problematic because, 'Evidence collected from detailed analyses of corporate firewalls shows that, in general, many firewalls are enforcing poorly written rule-sets, and in particular, direction-based filtering is often misguided or entirely unused'.[4]

Alternative firewall technologies exist. According to Wool, 'As we have seen, direction-based filtering is a useful tool to have in the firewall administrator's toolbox. Unfortunately, the direction-based filtering mechanism currently offered by most vendors are not very satisfactory. Most vendors force firewall administrators to deal with confusing low-level details, while Check Point essential deprives users of this capability.' [4] Wool also adds, 'However, vendors can do much better. This is demonstrated by the Rule Assignment and Direction Setting (RADIS) algorithm which was implemented within the Firmato prototype.'

In effect, this emphasizes the importance of the human factor in security. According to Shultz it is people that are responsible for configuring and managing technology leaving ample opportunity for human error and hence exposing systems to security threats. [5]

In order to address these concerns Johnston proposed criteria for a successful secure Human Computer Interface [6]. According to Johnston a security HCI (HCI-S) can be defined as, 'the part of a user interface which is responsible for establishing the common ground between a user and the security features of a system. HCI-S is human computer interaction applied in the area of computer security.'

The problems associated with security device management are further exacerbated by the need to configure, integrate and manage a wide range of heterogeneous technologies such as routers, switches and wireless devices. Van dem Akker makes the point, 'Other security breaches caused by user error can be attributed to the complexity of modern systems. Users must be able to used and clearly understand the system in order to use it effectively.' [7]

2. State Model Diagrams

Abstraction is a method for controlling complex systems and has been identified as a key process in research, development and applications work. It is listed, by the ACM/IEEE as one of twelve recurring concepts fundamental to computing,

'Levels of abstraction: the nature and use of abstraction in computing; the use of abstraction in managing complexity, structuring systems, hiding details, and capturing recurring patterns; the ability to represent an entity or system by abstractions having different levels of detail and specificity.' [8]

Models, based on abstraction, are therefore a means of controlling detail. Ideally models should be: diagrammatic, self-documenting, easy to use and allow hierarchical top-down decomposition to control detail. Leveling is the property by which complex systems can be progressively decomposed to the level that is meaningful whilst still maintaining consistent links to other levels. Network devices, including dedicated firewalls are typically configured using the command line interface (CLI). One of the problems associated with device management is that status information must often be obtained from a number of different Command Line Interface (CLI) commands, many of which are not only complex but also provide a lot of data that may not be immediately of use. Maj et al analyzed a wide range of different modeling techniques and proposed State Model Diagrams (SMDs) for modeling switches, routers and the associated protocols [9] According to Maj, 'Using the state diagrams for the internetworking devices switch and router it is possible to capture on a single diagram the information from a number of different hierarchical CLI commands.'[10]. Significantly SMDs may also be used to model different network devices and associated protocols [10]. The use of SMDs will now be illustrated. In order to determine the operation of a router key information needed includes: interface IP and MAC addresses; interface line status; interface line protocol status; ARP details and routing table entries. This information is typically obtained from four CLI commands – show interface fa0/1, show interface fa0/0, show arp and show ip route. Actual output, one such commands is as follow:

Router1#show interface fa0/1
FastEthernet0/1 is up, line protocol is up, Hardware is AmdFE, address is 000c.30e2.e501 (bia 000c.30e2.e501), Internet address is 192.168.1.1/24, MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255, Encapsulation ARPA, loopback not set, Keepalive set (10 sec), Full-duplex, 100Mb/s, 100BaseTX/FX, ARP type: ARPA, ARP Timeout 04:00:00, Last input never, output 00:00:09, output hang never, Last clearing of "show interface" counters never, Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0, Queueing strategy: fifo, Output queue: 0/40 (size/max, 5 minute input rate 0 bits/sec, 0 packets/sec, 5 minute output rate 0 bits/sec, 0 packets/sec, 0 packets input, 0 bytes, Received 0 broadcasts, 0

runts, 0 giants, 0 throttles, 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignore, 0 watchdog, 0 input packets with dribble condition detecte, 68 packets output, 8770 bytes, 0 underruns 0 output errors, 0 collisions, 2 interface resets, 0 babbles, 0 late collision, 0 deferred, 3 lost carrier, 0 no carrier, 0 output buffer failures, 0 output buffers swapped out

A single SMD can be used to represent the main data extracted from four separate CLI commands all linked to the appropriate OSI level (Figure 1). Other more complex protocols may be modeled using a single SMD by simply including and excluding tables [11]. Furthermore, using SMDs it is possible to selectively include and exclude details (i.e. hiding details and complexity) whilst maintaining the conceptual integrity by means of hierarchical leveling, 'The highest level (level 0) module is a single diagram that describes the entire system. Subsequent diagrams are expansions of this level 0 diagram and are numbered accordingly. Furthermore, all diagrams must be linked thereby allowing navigation between them.' (Maj, Kohli et al. 2004).

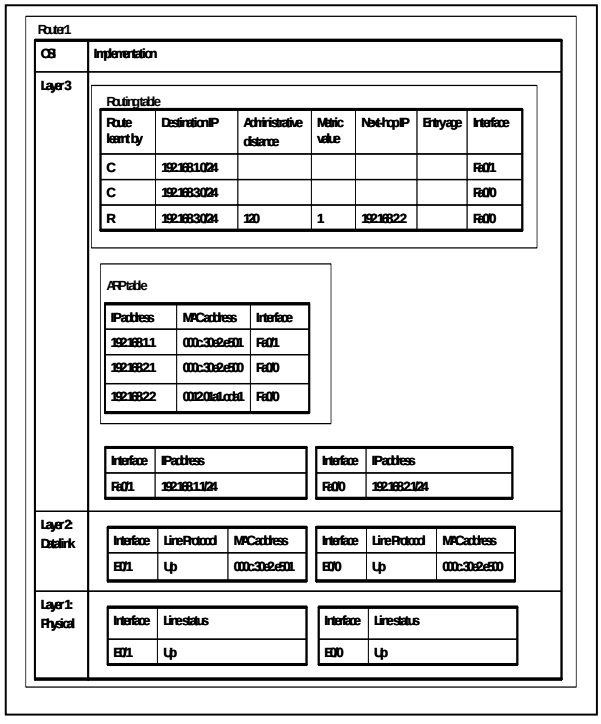

Figure 1. Router (Routing Information Protocol – RIP) State Diagram Model

In effect using SMDs it is possible by means of top-down decomposition and leveling to model a complex network as an integrated collection of units each of an amenable size. Significantly, it is possible to maintain an overview of the entire network or selectively obtaining increasing levels of detail whilst maintaining links between these different levels of complexity. [11]

The State Model Diagrams have been successfully used as the pedagogical foundation of curriculum, 'Results to date suggests that student learning based on state model diagrams demonstrates a richer conceptual understanding strongly aligned with that of an expert.' [12]

The models have also been evaluated as a technique for teaching professional network engineers. In this study by Maj a one-hour lecture on Spanning Tree Protocol using the state diagrams was given to practicing networking engineers currently undertaking part time studies towards a professional networking qualification at another institution. There was unanimous and clear support for the use of these models [12]
Work by Kohli suggests that the state model diagrams may also be used for modelling both switch and router security [13]. More complex security protocols such as Cisco Encryption Technology and IPSec have been successfully modelled using the SMD method [14]

3. PIX Firewall State Model Diagram

The above has illustrated how the State Model Diagrams can be used to control the complexity associated with the CLI for routers. The following section will demonstrate how State Model Diagrams can also be used to model PIX firewalls and hence assist in device configuration, management and systems integration. This is important because, according to Wool, 'Cisco's approach is typical of most firewall vendors; it exposes the raw and confusing direction-based filtering functionality to the firewall administrators. Other vendors that follow the same approach (with different syntactical mechanisms) include, among others, Lucent, NetScreen, and open-source tools such as ipchains and netfilter.' Wool further emphasises this point, 'This myriad of commands make the task of configuring a PIX firewall rather difficult, especially for novices. An information survey of posting to firewall mailing lists such as Firewall Wizards (1997-2003) seems to show basic configuration questions being posted much more frequently for PIX than, say, for Check Point.' [4]
For these experiments a PIX 515e with three Ethernet interfaces was used. PIX firewalls employ dedicated hardware (ensuring high performance) and use the Adaptive Security Algorithm for stateful connection control. The ASA uses the concept of security levels – by default security level 100 (Ethernet 1) being the highest and is assigned to an inside interface; security level 0 (Ethernet 0) is the lowest and is assigned to an outside interface. The PIX 515e has a third interface that can be configured according to company requirements, in this case it represents the dmz with a security level of 50.
High (inside) to low (outside) security may be enabled by two different methods – static or dynamic translation. The

515e PIX was initially configured for static address translation. The status of this operation device is determined by a number of different CLI commands that include:

PIX1(config)# show ip address
System IP Addresses:
ip address inside 192.168.100.1 255.255.255.0
ip address dmz 192.168.50.1 255.255.255.0
ip address outside 192.168.1.1 255.255.255.0
Current IP Addresses:
ip address inside 192.168.100.1 255.255.255.0
ip address dmz 192.168.50.1 255.255.255.0
ip address outside 192.168.1.1 255.255.255.0

Note, the output for interface dmz and outside not shown

PIX1(config)# show static
static (inside,outside) 192.168.1.99 192.168.100.2 netmask 255.255.255.255 0 0

PIX1(config)# show run
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
ip address outside 192.168.1.1 255.255.255.0
ip address inside 192.168.100.1 255.255.255.0
ip address dmz 192.168.50.1 255.255.255.0
static (inside,outside) 192.168.1.99 192.168.100.2 netmask 255.255.255.255 0 0

PIX1(config)# show route
inside 192.168.100.0 255.255.255.0 192.168.100.1 1 CONNECT static
dmz 192.168.50.0 255.255.255.0 192.168.50.1 1 CONNECT static
outside 192.168.1.0 255.255.255.0 192.168.1.1 1 CONNECT static

PIX1(config)# show arp
inside 192.168.100.2 0002.5573.0ad7
outside 192.168.1.2 0002.5573.0d95

PIX1(config)# show xlate
1 in use, 1 most used. Global 192.168.1.99 Local 192.168.100.2

PIX1(config)# show conn
1 in use, 1 most used. TCP out 192.168.1.2:80 in 192.168.100.2:1443 idle 0:00:28 Bytes 1253 flags UIO

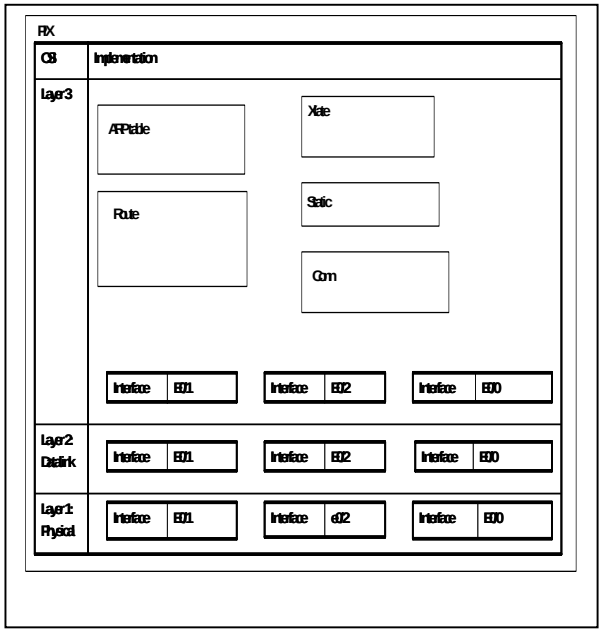

Figure 2: PIX State Model Diagram

Using this CLI output a sequence of different State Model Diagrams was designed. The level 0 diagram illustrates the tables the PIX holds and what physical interfaces are being used (Figure 2). Based on this diagram, it is then possible to determine further details, for example the MAC and IP address of each interface and its operational status i.e. are both the line status (LS) and line protocols (LP) up or down. During fault diagnosis the operational status and configuration of each interface must be checked. Using hyperlinks it is then possible to 'zoom in' on the details contained in each of the different tables (Figure 3). In order to accommodate this detail the OSI layer 1 and 2 interface details have been omitted.

Using this single diagram the user can determine the operational status of: arp, route, static translations, conn, xlate and also the security levels, IP and MAC addresses of three interfaces. Furthermore this diagrammatic representation of the CLI output allows the user to see the relationships between the different protocols. This is important in order to assist in determining if the device is correctly configured and also during fault diagnosis.

The same device was then configured for dynamic translation and the associated State Model Diagrams designed. In place of a Static Address Translation Table, dynamic addressing uses a Network Address Translation Table (NAT) and a Global table.

Again, using this diagram it is possible to 'zoom in and out' in order to obtain further technical detail. Significantly, with a minor modification, the same State Model Diagram can be used both static and dynamic PIX configurations. Preliminary work suggests that the State

model diagrams may also be applied to other firewall technologies such as Netscreen.

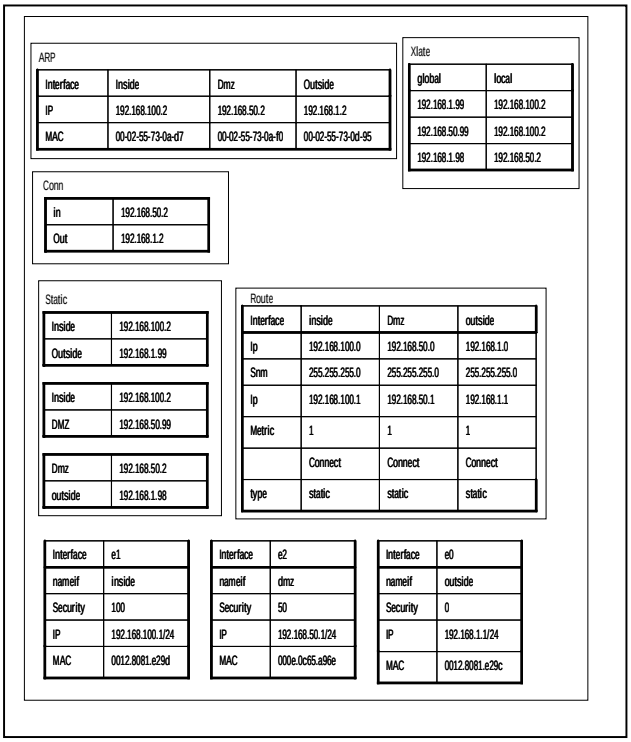

Figure 3. PIX State Model Diagram - Static Translation

4. Evaluation of State Model Diagrams

A simple LAN integrating the following technologies was implemented:

- Cisco Aironet AP1200 Wireless Access Points
- Catalyst 2950 switches
- PIX515e Firewall
- 2621xm Cisco routers (RIP)

Based on the network twenty experienced network administrators were asked to evaluate the following network management tools:

- State model diagrams (paper based only)
- Ciscoworks for Windows
- Command Line Interface (CLI)

Ciscoworks is a popular, general-purpose network management tool. The administrators were given a short introduction to the state model diagrams and provided with the opportunity to manage the network using these tools. They were then asked to complete a questionnaire to obtain details about their work experience. The questionnaire also included a number of questions most of which were based on the Likert scale (SA, A, D, SD, U) and the opportunity to provide any comments. The questions included a negative statement for evaluation.

Question 1: Does the state model provide an easy way to understand the relationship between the devices of a network?

Yes	No	Do not know
100%		

Question 2: The state model allows network administrators to have a better view of the entire network than other methods/models.

SA	A	D	SD	U
30%	65%			5%

Question 3: The state model cannot be used to manage complex networks.

SA	A	D	SD	U
	30%	60%	5%	5%

Question 4: The integration of the state model with Ciscoworks simplifies the complexity of the network.

SA	A	D	SD	U
40%	40%			20%

Question 5: The state model does NOT assist efficient network management.

SA	A	D	SD	U
		70%	30%	

Question 6: The state model assists in network security management as a tool and as a result leads to more successful network management.

SA	A	D	SD	U
20%	70%	5%		5%

Question 7: I would NOT use the state model to manage my network.

SA	A	D	SD	U
	5%	50%	40%	5%

Some typical written comments (verbatim) are as follows; note the abbreviations used are NM – Network Managements; SM – State Model Diagrams:

Network administrator 1

"Yes, state diagrams provide a clear, concise view of a network configuration which helps identify any security issues".
Network administrator 2
"Because the state model show you all the information in one go it would allow a better understanding of the network which in turn provides better security".
Network administrator 7
'State model provides clear understanding and creates a clear picture about the network. It will help to identify any bugs or faulty points in the network. I strongly believe this approach will lead to a world class product".
Network administrator 8
"Easy to understand the structure of the network and information flow through the separate interfaces which strongly helps to understand security needs".
Network administrator 10
"State model manages the network well but it does not address the security issues."
Network administrator 11
"State model is useful to efficiently manage the complexity of networks."
Network administrator 13
"State Model diagrams provide clear picture of the entire network. That will help to identify any faulty points in the network. I strongly believe this method provides an efficient network security management".
Network administrator 16
"State Model clearly shows what sort of security permissions have given to the network".
Network administrator 18
"Yes, State Model shows all information as a map rather than documentation. It is focus on the key points of the network".

Despite being only a limited study the results are consistent – the State Model Diagrams provide a unique representation that can be used to manage not only firewalls but also the integration of heterogeneous technologies within a secure environment. Only one network administrator (#10) had reservations about the State Model Diagrams.

5. State Model Diagrams as a Security Human Computer Interface (HCL-S)

A Human Computer Interface is defined by Michels, cited by Johnston, as, 'the part of a computer program responsible for establishing the common ground for a particular task (i.e. well known) user. His task is accomplished by expanding and maintaining this common ground throughout the interaction process with the application.'[6]
There are a number of well-established criteria for designing user interfaces. According to Nielson, cited by Johnston there are ten criteria necessary for a successful HCI [6]. In order to improve the integrity of secure systems Johnston proposed complementary criteria for a secure Human Computer Interface (HCI-S). Based on the results presented in this paper, the authors suggest that the State Model Diagrams of a PIX firewall substantially comply with these criteria (Table 1).

Table 1. HCI-S evaluation of PIX state model diagram

#	Criteria	Description	SMDs
1	Convey features	Interface needs to convey the available security features to the user	Diagrammatic i.e. unnecessary details hidden
2	Visibility of system status	User able to observe the security status of the internal operations	Key security status details can be highlighted
3	Learnability	Interface as non-threatening and as easy to learn as possible	Consistent interface and navigation by hyperlinks
4	Aesthetic and minimalist design	Only relevant security information should be displayed	Leveling and top down decomposition
5	Errors	Error messages to be detailed	Not implemented
6	Satisfaction	Interface aids user in having a satisfactory experience with a system	Yes, based on survey of 20 network administrators
	Trust	It is essential that the user trust the system	Significantly improves trust

6. Conclusions

State Model diagrams of a range of different technologies (switches, routers, wireless access points etc) and protocols (e.g. RIP, OSPF, STP etc) have been successfully implemented. These diagrams employ leveling and hence provide hierarchical top down decomposition thereby controlling technical detail. In effect, the diagrams integrate leveled diagrams with protocol finite state machines and the output of internetworking CLI command output. The problems associated with PIX firewall configuration and management are well documented. This paper demonstrates how these problems may be substantially addressed by modeling PIX devices using the state model diagram technique. Furthermore, based on an evaluation by twenty experienced network administrators, state model diagrams may be used to manage not only firewalls but also the integration of heterogeneous technologies within a

secure environment. Significantly, the state model diagrams appear to meet most of the criteria associated with the requirements of a secure Human Computer Interface (HCI-S). Preliminary results suggest that the state model diagrams are vendor independent however further work is needed.

Références

[1] Walker, R.W., Security, Bandwidth Occupy Network Managers, in Government Computer News, 22. 2003.

[2] King, D. A New Model for Security. 2004 [cited 2005 16th December]; Available from: http://www.comnews.com/stories/articles/0504/0504new-model-htm.

[3] Bartal, Y., et al., Firmato: A Novel Firewall Management Toolkit. ACM Transactions on Computer Systems, 2004. 22(4): p. 381-420.

[4] Wool, A., The use and usability of direction-based filtering in firewalls. Computers & Security, 2004. 23: p. 459-468.

[5] Shultz, E., The Human Factor in Security. Computers & Security, 2005. 45: p. 425-426.

[6] Johnston, J., J.H.P. Eloff, and L. Labuschagne, Security and human computer interfaces. Computers & Security, 2003. 22(8): p. 675-684.

[7] van dem Akker, T. The YGuard Access Control Model: Set-Based Access Control. in SACMAT01. 2001. Chantilly, VA.

[8] Tucker, A.B., et al., A Summary of the ACM/IEEE-CS Joint Curriculum Task Force Report, Computing Curricula 1991. Communications of the ACM, 1991. 34(6).

[9] Maj, S.P. and G. Kohli, A New State Models for Internetworks Technology. Journal of Issues in Informing Science and Information Technology, 2004. 1: p. 385-392.

[10] Maj, S.P., G. Kohli, and G. Murphy. State Models for Internetworking Technologies. in IEEE, Frontiers in Education, 34th Annual Conference. 2004. Savannah, Georgia, USA: IEEE.

[11] Maj, S.P. and D. Veal, State Model Diagrams as a Pedagogical Tool - An International Evaluation. IEEE Transactions on Education, 2007. 50(3): p. 204-207.

[12] Maj, S.P., G. Kohli, and T. Fetherston. A Pedagogical Evaluation of New State Model Diagrams for Teaching Internetwork Technologies. in 28th Australasian Computer Science Conference (ACSC2005). 2005. Newcastle, Australia: Australian Computer Society and the ACM Digital Library.

[13] Kohli, G., et al. A Conceptual Model as an aid to understanding Network Security. in 2005 American Society for Engineering Education Annual Conference & Exposition (ASEE 2005). 2005. Portland, Oregon.

[14] Nuangjamnong, C., S.P. Maj, and D. Veal. Network Security Devices and Protocols Using State Model Diagrams. in 5th Australian Information Security Management Conference. 2007. Edith Cowan University, Perth, Western Australia: School of Computer and Information Science, Edith Cowan University.

A/Prof S. P. Maj has been highly successful in linking applied research with curriculum development. In 2000 he was nominated ECU University Research Leader of the Year award He was awarded an ECU Vice-Chancellor's Excellence in Teaching Award in 2002, and again in 2009. He received a National Carrick Citation in 2006 for "the development of world class curriculum and the design and implementation of associated world-class network teaching laboratories". He is the only Australian judge for the annual IEEE International Student Competition and was the first Australian reviewer for the American National Science Foundation (NSF) Courses, Curriculum and Laboratory Improvement (CCLI) program.

Dr. David Veal is a Senior Lecturer at Edith Cowan University. He is the manager of Cisco Network Academy Program at Edith Cowan University. His research interests are in Graphical User Interface for the visually handicapped and also computer network modeling.