The Cisco Network Security Course – a critical, student based evaluation

J Gallally, N Gao, Laura, V Gogineni, D Veal, S P Maj[*]

Edith Cowan University, Perth, Western Australia

Summary
The Cisco Certified Network Academy (CCNA) is a prerequisite for the recently introduced Cisco CCNA Security course. Both the CCNA and the CCNA Security course provide: standard textbooks; on-line material and associated laboratory manuals. The CCNA is designed to provide a broad foundation of networking principles. The CCNA Security course builds upon this foundation knowledge in order to provide specialist knowledge and skills in network security. This paper is a student centric evaluation of these two awards and how well they meet their objectives.

Key words:
Network Security, CCNA, Cisco Security course.

1. Introduction

The Cisco Network Academy Program (CNAP) consists of a range of courses suitable for both novices and also practicing professionals [1], [2]. For all of these courses CNAP provides: standard textbooks, laboratory exercises, multimedia oriented training materials, simulations and assessments. The initial Cisco Certified Network Associate (CCNA) Exploration course provides both theoretical and practical instruction in network basics. According to Cisco this course, *provides a comprehensive overview of foundational to advanced networking concepts, with an emphasis on theory and practical applications.* [3]
Hence an integral aspect of CCNA is the completion of practical, 'hands-on' exercises as defined by the laboratory manual. The CCNA Exploration course consists of a subset of four inter-related courses:

1. Network fundamentals
2. Routing Protocols and Concepts
3. LAN Switching and Wireless
4. Accessing the WAN

For each of the above courses CNAP provide: recommended text book; laboratory manual; on-line, multimedia material. The network fundamentals course consists of a broad introduction to networking (table 1). The routing course builds upon this foundation in order to provide considerable detail about the principles of routing and the more popular routing protocols currently in use (table 2).

Table 1: Network fundamentals

	Network fundamentals
1	Living in a Network-centric world
2	Communicating over the network
3	Application layer functionality and protocols
4	OSI transport layer
5	OSI network layer
6	Addressing the network: IPv4
7	OSI data link layer
8	OSI physical layer
9	Ethernet
10	Planning and cabling
11	Configuring and testing

Table 2: Routing protocols and concepts

	Routing protocols and concepts
1	Introduction to Routing and packet forwarding
2	Static routing
3	Introduction to dynamic routing protocols
4	Distance vector routing protocols
5	RIP v1
6	VLSM and CIDR
7	RIP v2
8	The routing table
9	EIGRP
10	Link-state routing protocols
11	OSPF

The course LAN switching also includes a chapter on wireless based networks (table 3). This chapter includes a section on wireless security. In particular: threats to wireless security (rogue access points, man-in-the-middle attacks, denial of services); wireless security protocols (802.11i standard); authentication; encryption and controlling access to the Wireless LAN.
Accessing the WAN includes not only an introduction to Wide Area Network technologies but also network security (table 4). Topics include: basics of securing network devices; Cisco Security Device Manager (SDM)

Manuscript received June 5, 2011
Manuscript revised June 20, 2011

and Access Control Lists (ACLs). From a student perspective this material was considered to provide a good basic knowledge of networking.

Table 3: LAN switching and wireless

	LAN switching and wireless
1	LAN design
2	Basic switch concepts and configuration
3	VLANs
4	VTP
5	STP
6	Inter-VLAN routing
7	Basic wireless concepts

Table 4: Accessing the WAN

	Accessing the WAN
1	Introduction to WANs
2	PPP
3	Frame relay
4	Network security
5	ACLs
6	Teleworker services
7	IP addressing services
8	Network troubleshooting

The CCNA course is a prerequisite for the more specialized CCNA Security course.

2. CCNA Security

The CCNA Security course is designed to provide both theoretical and practical instruction in security. According to Cisco, this course, introduces the core security concepts and skills needed to install, troubleshoot, and monitor a network to maintain the integrity, confidentiality, and availability of data and devices [3]. The textbook consists of fifteen chapters with an associated nine workshop exercises defined by the student laboratory manuals. Arguably workshop exercises are designed to complement and hence reinforce learning. However the following problems were identified:

2.1 CCNA Security – Weaknesses

Problem #1 Course mapping

The main problem is the distinct lack of coherence between the standard textbook and the laboratory exercise (table 5). For some chapters there is no associated laboratory workshop exercise. This is problematic because learning that occurs whilst studying some chapters cannot be reinforced. It should be noted the majority of students express the opinion that workshops are invaluable methods of gaining a sound knowledge of a topic.

Problem #2 Wireless security

The CCNA course includes chapters on both wireless and wireless security. However the security course does not include any reference to wireless security. Arguably this is a major deficiency. It is recognized that the CCNA course provides instruction on wireless and wireless security issues the expectation is that this compulsory introductory material could be build upon by considering issues such as Wireless LAN (WLAN) controllers etc. This would thus provide a more comprehensive course of instruction.

Table 5: CCNA Security course chapter to workshop mapping

	Chapter	Laboratory workshop
1	Understanding network security principles	Researching network attacks and security audit tools
2	Developing a secure network	
3	Defending the perimeter	
4	Configuring AAA	Securing administrative access using AAA and Radius
5	Securing the router	Securing the router for administrative access
6	Securing layer 2 devices	Securing layer 2 switches
7	Implementing Endpoint security	
8	Providing SAN security	
9	Exploring secure voice solutions	
10	Using Cisco IOS firewalls to defend the network	Configuring CBAC and zone-based firewalls
11	Using Cisco IOS IPS to secure the network	Configuring an IPS
12	Designing a cryptographic solution	Exploring encryption methods
13	Implementing digital signatures	
14	Exploring PKI and Asymmetric encryption	
15	Building a site to site VNP	Configuring a site-to-site VPN
		Security policy development and implementation

Problem #3 IPv6

Some of the limitations of IPv4 were temporarily addressed by technologies such as Network Address Translation (NAT), subnetting etc. However it is recognized that the introduction of IPv6 is now required and is recognized as the only long term solution to IPv4 address exhaustion. Notably, *On January 31, 2011, the last two unreserved IANA /8 address blocks were allocated to APNIC according to RIR request procedures. This left five reserved but unallocated /8 blocks.* [4]

It is anomalous that the CCNA security, as a recently deployed course, does not refer to IPv6 and the associated security issues.

Problem #4 Security policies

The importance of security policies cannot be underestimated. However whilst workshop 9 is concerned with security policies anomalously there is no corresponding text book chapter.

Problem #.5 Host services/Cloud computing

Cloud computing is a concept that encompasses software as a service (SaaS) to the migration of the entire corporate into a virtual, remote platform with the associated potential cost benefits. However, there are concerns regarding security [5]. The CCNA security course makes no reference to cloud computing, despite its increasing importance and concerns regarding security.

Problem #6 Security Device Manager

The Cisco Security Device Manager (SDM) is a very powerful graphical user interface that considerably assists with both device configuration and management. However 'one click' solutions are also potentially problematic as extensive configurations can be generated with no real understanding of their functionality. In this situation should there be a system failure troubleshooting would be extremely difficult. Whilst the verbose Command Line Interface (CLI) is harder to use it forces some understanding of the commands being entered. It is suggested that the advantages and disadvantages of interfaces such as the SDM should be clearly annunciated.

Problem #7 Legacy systems

The CCNA security course does not address legacy secure systems and devices such as PIX firewalls. It should be recognized that many companies still deploy these older security technologies.

Problem #8 Vendor Specific

The CCNA security course is significantly vendor specific with a considerable amount of material being devoted to Cisco products such as: Cisco Security Agent, Cisco Ironport etc. It should be recognized that there are other vendor products with significant market penetration such as Checkpoint systems.

Problem #9 How secure is secure?

Whilst the course teaches how to deploy security solutions the students do not gain any measure of the resulting strength of the security measures. It is strongly recommended that the course include tools that could be used to attack and hence verify the efficacy of a secure solution.

Problem #10

Cisco Internet Operating Systems (IOSs) have both limitations and flaws. The importance of regular IOS updates and backups should be emphasized in the course material.

Problem #11 Cisco Secure Access Control Server

The Cisco Secure Access Control Server (CSACS) is a powerful and useful tool that should be included in the course material.

Problem #12 TACACS and RADIUS

A more balanced approach to TACACS and RADIUS is recommended.

Problem #13 IPSec Virtual Private Network

Virtual Private Networks (VPNs) based on the IPSec standard are a very important security tool. The material provided serves only as an introduction to this technology. The material fails to provide details about: isakmp policy scalability and redundancy; use of multiple crypto maps; backup VPN tunnels; advantages/disadvantages of the IPSec options etc.

Problem #14 Critical Infrastructure

The course fails to recognize that critical infrastructure (power supply, water treatment, manufacturing plants etc) are typically networked Supervisory Control and Data Acquisition (SCADA) systems. One definition of critical infrastructure is:

> *Those physical facilities, supply chains, information technologies and communications 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 defense and ensure national security.* [6]

This infrastructure is substantially dependent on IT systems which in turn are progressively subject to cyber attack. According to McAfee and the Centre for Strategic and International Studies (CSIS) report there are massive increases in cyber attacks and sabotage on unprepared critical infrastructure systems. Furthermore, there are now sophisticated forms of malware such as Stuxnet which is specifically designed to sabotage critical infrastructure IT systems [7]. The Cisco security course makes no reference to networked critical infrastructure. Certainly this is considered a major deficiency in the course material.

Problem #15 State Model Diagrams
It has been demonstrated that pedagogical outcomes are considerably improved if instruction is based on the State Model Diagram (SMD) representation of network devices and protocols [8-14]. This course does not make use of this teaching method.

2.2 CCNA Security - strengths

The CCNA course provides comprehensive instruction in network technology. The practical, 'hands-on' aspects are considered to be particularly useful and valuable as this enhances learning. The CCNA security course builds upon this and provides good practical experience that is especially valuable to students who have no commercial experience. The material is well structured with a good flow that gradually scaffolds knowledge. The pre-chapter tests are a good method of testing knowledge of the expected subject areas. The laboratory manuals for both courses are well structured and easy to follow. On successful completion of both courses students will have a good knowledge of networks and secure networks.

3. Conclusions

It is recognized that this new course on network security addresses a market driven need for students with these skills. The practical, 'hands-on' aspects of the course were considered to be of significant benefit and contributed to quality learning outcomes. The course coverage is broad but there are major deficiencies which is somewhat surprising given this course was only introduced last year.

References

[1] Kohli, G., et al. *Abstraction in Computer Network Education*. in *2004 American Society for Engineering Education Annual Conference & Exposition (ASEE 2004)*. 2004. Salt Lake City, Utah, USA.

[2] Murphy, G., et al. *An Examination of Vendor-Based Curricula in Higher and Further Education*. in *2004 American Society for Engineering Education Annual Conference & Exposition (ASEE 2004)*. 2004. Salt Lake City, Utah.

[3] Cisco. *Courses and Certifications*. June, 2011]; Available from: http://www.cisco.com/web/learning/netacad/course_catalog/index.html.

[4] Wikipedia. *IPv4 Address Exhaustion*. June, 2011]; Available from: http://en.wikipedia.org/wiki/IPv4_address_exhaustion#Impact_of_APNIC_RIR_exhaustion_and_LIR_exhaustion.

[5] Grayson, I. *Risks and Rewards in Cloud Computing*. 2011 June, 2011]; Available from: http://www.theaustralian.com.au/australian-it/the-hub/risks-and-rewards-in-cloud-computing/story-fn4hs56q-1225882469170.

[6] Government, A., *Critical Infrastructure Resilience Strategy*. 2010: Barton, ACT.

[7] McAfee, *In the Dark. Crucial Industries Confront Cyberattacks*. 2010, Centre for Strategic & International Studies.

[8] Maj, S.P., *State Model Diagrams for Managing Secure Networks: A New Tool for Students and Practicing Professionals.* Manuscript submitted for publication, 2007.

[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 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.

[11] 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.

[12] Maj, S.P. and B. Tran. *State Model Diagrams - a Systems Tool for Teaching Network Technologies and Network Management*. in *International Joint Conferences on Computer, Information and Systems Sciences, and Engineering*. 2006. University of Bridgeport: Springer.

[13] 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.

[14] Maj, S.P., Veal, D., *An Evaluation of State Model Diagrams for Secure Network Configuration and Management.* International Journal of Computer Science and Network Security, 2010. **10**(9): p. 66-72.

James Gallaly is currently completing his Masters in Computer and Network Security at Edith Cowan University, Australia and obtained a BSc (hons) in Business Information Technology from Bournemouth University, England. He has worked in the IT support field for a number of years, both in Australia and in England. His area of interest is network security.

Nan Gao is a student studying Computer and Network Security at Edith Cowan University. He also studied Marketing for four years in his Bachelor degree with focus on analyzing "web2.0" website' business model and how they make profit. His research interests are in network administration and security as well as user privacy protection.

Laura has completed her undergraduate degree in Jakarta, Indonesia, majoring in Accounting in 2001. She will finish her Masters in Computer and Network Security at Edith Cowan University, Australia, in July 2011. Her areas of interest are networking and wireless security.

Rama Krishna is currently studying Masters of Computers and Network Security at Edith Cowan University, Australia and holds a Degree in Bachelors of Computer Science and Engineering from Anna University, India. His areas of interest are Networks and Security.

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

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.