International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:2, No:7, 2008

New Curriculum Approach in Teaching Network Security Subjects for ICT Courses in Malaysia

Mohd Fairuz Iskandar Othman, Nazrulazhar Bahaman, Zulkiflee Muslim, and Faizal Abdollah

***Abstract*—**This paper discusses a curriculum approach that will give emphasis on practical portions of teaching network security subjects in information and communication technology courses. As we are well aware, the need to use a practice and application oriented approach in education is paramount. Research on active learning and cooperative groups have shown that students grasps more and have more tendency towards obtaining and realizing soft skills like leadership, communication and team work as opposed to the more traditional theory and exam based teaching and learning. While this teaching and learning paradigm is relatively new in Malaysia, it has been practiced widely in the West. This paper examines a certain approach whereby students learning wireless security are divided into and work in small and manageable groups where there will be 2 teams which consist of black hat and white hat teams. The former will try to find and expose vulnerabilities in a wireless network while the latter will try their best to prevent such attacks on their wireless networks using hardware, software, design and enforcement of security policy and etc. This paper will try to show that the approach taken plus the use of relevant and up to date software and hardware and with suitable environment setting will hopefully expose students to a more fruitful outcome in terms of understanding of concepts, theories and their motivation to learn.

***Keywords*—**Curriculum approach, wireless networks, wireless security.

I. Introduction

COMPUTER and network security, specifically wireless security has been a subject of much interest lately, in part because of the changes in the world we live in and the demands of people and business that require a certain standard of privacy, confidentiality and security of their online transactions and data such as online business transactions and medical records in hospitals. Academia has long realised this and has taken active steps with institutions of higher learning busy introducing subjects and courses that deal with computer and network security in general and wireless security in particular. Although this is a positive step, but often courses and subjects taught in institutions of higher learning tend to focus their attention on the theoretical aspects of computer and wireless security while forgetting that the most important aspect of learning is not just discovering 'what' but 'how' and 'why'. This paper will try to propose a new approach that will give emphasis on practical portions of teaching computer and network security subjects by taking wireless security subtopic as an example. While not disregarding the importance of theoretical knowledge, the paper hopes to show that learning by doing will leave much more impact on students as oppose to the normal way of discharging knowledge through lectures.

This work was supported in part by Universiti Teknikal Malaysia Melaka under Short Grant S249.

Authors are with Department of Computer Systems and Communication, Universiti Teknikal Malaysia Melaka, Malacca, Malaysia (e-mail: {mohdfairuz, nazrulazhar, zulkiflee, faizalabdollah}@utem.edu.my).

II. Motivation

Nowadays, we can see urgency in terms of providing security and maintaining security in business environments as well as in everyday life. To further corroborate this, IT security spending has seen a significant increase over the years, as noted by a research done by Deloitte which indicated that IT security budget saw an increase of 15% over 2006 [1]. Business nowadays simply cannot rely on the term "security through obscurity " anymore as every business needs presence on the internet where most transactions are done and valuable information and data are passed through back and forth. Wireless security is becoming a more and more important and prevalent technology nowadays as it supports both mobility and flexibility for the user. There exists an urgent need to secure wireless networks because of obvious insecurities and inherent vulnerabilities found in wireless technology. Like it or not, wireless technology is here to stay with new and emerging standards like Wimax that promises wider coverage. So, the best thing to do is to face the technology head on. In doing that, the need for technically skilled and knowledgeable IT security professionals that can handle security particularly wireless security cannot be denied. Research has shown that while companies realise the importance of security, only seven percent felt that they presently have the required skills and competencies to effectively handle existing and foreseeable security requirements [1]. So, there is indeed a significant shortage of security professionals who are both competent and skilled. Although many courses and subjects have been introduced in institutions of higher learning to address this matter, many of them still implement and use traditional teaching and learning approaches that is not suitable in a face paced and ever changing world of IT where knowledge alone cannot compensate technical skills and know how.

III. Common Approach

Before going further and detailing our proposed approach,

it is best to describe some common approaches used in teaching and learning computer science courses as outlined by [2].Traditional lecture approach is a common used approach especially used in a heavy theory based topic, for example cryptography. The method used often stems from the fact that a lot of basic and fundamental concepts must be covered. More often, this emphasis on fundamental concepts may well lead to students becoming too passive and unresponsive. The scribe approach, on the other hand, includes elements of active learning where students are responsible for taking notes during lectures and will do a presentation of what he or she understands based on his or her notes to fellow students and the instructor during or after a lecture session. It can be seen that a lot of higher institutions have begun to implement the scribe approach nowadays. The expert/mentor approach meanwhile is a fresh approach that uses guest instructors from the industry or lecturers that are well-versed and experts in their field to give lectures on specific topics. To enable this method of teaching, the university must have a good working relationship with the industry. This type of relationship can be built based on undertaking of research projects together with the industry and helping them to solve industry related problems. Both can provide working space and devices and instruments that cannot be found in the university or the industry. This approach maximizes the university's and the industry's resources as each will be able to use each other's resources when needed. This approach has been used widely in technical based universities in Australia with good results [3]. The university can benefit from this type of approach as guest lecturers from the industry will surely impart and share their experience and expertise within the context of the industry's perspective. This knowledge will indeed help shape the students' perspective of actual working scenario and conditions. Tutorial approach is often used whenever various sources of information can be obtained via sources online; an example is the use of e-learning content and online journals and papers related to the topic at hand. This type of approach gives more freedom to the students to search and obtain information while filtering the information obtained in relevance to the particular topic. Last but not least is the project approach, also a norm in institutions of higher learning. Using this approach, in the beginning of the semester, students are given a project topic to be done during the whole semester and usually ending up with the students having to do a presentation and a demo of their project.

IV. Proposed Approach / Methodology

Many literatures such as [4] state that although theory and knowledge delivered via lecture is a must, it is often the practical and technical knowledge that often distinguishes between a good graduate and an excellent and sought after graduate. The industry needs people who can work straight away without them having to spend money on retraining the graduates. It is duly expected that the graduates are already well equipped and work ready when they step out of institutions of higher learning. Realizing this, Universiti Teknikal Malaysia Melaka (UTeM) implements the practice and application oriented approach (PAO) [3]. This method inspires students to discover, query, think and propose solutions based on problems presented and theories learnt. They can simulate these problems in the lab and practical sessions, often requiring them to find the answers themselves with minimum guidance and supervision from the instructors and lecturers. Our proposed approach, while based on the PAO approach, will also include the above mentioned common approaches like the expert/mentor and tutorial approach whenever necessary. As students spend most of their time doing and attending practical sessions in labs, we believe that this is the most suitable method to be used.

Attack and defend methodology was first used by Texas A&M University [4] in teaching general computer security subjects and has seen successful implementation in institutions like Chalmers University of Technology [5] and Rochester Institute of Technology [6]. Although these methods of teaching and learning where done in graduate level classes and is used to teach general network security concepts and theories, we believe that certain portions like the wireless security subtopic can be implemented in undergraduate level classes using the attack and defend methodology. Basically, this attack/defend approach would require the students to be divided into 2 teams which are the black hat (offensive) and the white hat (defensive) teams [2]. The main goal for the offensive teams is to compromise wireless networks managed and monitored by the defensive teams. Meanwhile, the defensive team is given the task of making sure that their wireless networks are secure from any type of attacks launched by the offensive teams. Attacks can range from exploiting vulnerabilities that exists within certain standards and protocols, to the use of simple social engineering techniques. The use of social engineering techniques will feature students using their communication skills to the fullest to try to obtain useful information like usernames and passwords just by communicating with the target users. Other more simple ways of obtaining information may also include looking for notes that lay around the target's workplace or in the trash bin, to glancing over to have a better look at their network setup.

The proposed approach requires that a simple wireless network be set up by the defensive teams. Even starting from this activity, an overall view of the students' skill and competency in building and configuring the wireless network can be evaluated. The offensive teams meanwhile will be given laptops to be installed with relevant operating systems to be used in their attacks. Operating systems like Windows and a version of Slackware based Linux specially made for penetration testing called Backtrack is to be used. The next step will consist of two phases.

Phase one will start with a local site survey and traffic analysis. This is where both of the teams will get to analyse and get to know more about the wireless networks in terms of types of traffic that goes through, number of wireless nodes

and wireless access points to the source and strength of the wireless signal propagation. In short, they will already have a clear picture of the normal behaviour of the wireless network. Phase one will also require the defensive teams to deploy basic security measures such as changing the default AP password, disabling SSID broadcasting, changing the default channel, enabling WEP keys and enabling station MAC filter. After all changes have been made, attack sessions are done by the offensive teams using the latest tools that they can find. Unauthorised client access can be accomplished using software's like Netstumbler. Packet sniffing meanwhile can be accomplished using Wireshark. Packet injection and encryption attack on the other hand can be applied using the aircrack suite while Kismet can be used to detect networks that disable SSID broadcasting. Teams will be marked and graded based on how many types of offensive and defensive techniques successfully implemented and used. A basic benchmarking system will be used to make sure basic offensive and defensive methods are successfully implemented and used.

Phase two will require the defensive teams to implement the more recent and recommended security settings which include deploying and replacing WEP implementations with WPA2 or also known as the 802.11i standard. This will require the team members to deploy and configure an authentication server like FreeRADIUS or TACACS. Using these new technologies, the team must take into consideration impacts of using the new security settings and techniques on performance and whether they are interoperable with the current setup of their hardware and software. As in phase one, after all new changes have been made to the wireless networks, the offensive teams will get to try and penetrate the wall of defence created by the defensive teams by using existing methods mentioned in phase one plus the most deadly but most often forgotten method known which is social engineering. After each phase, teams will give a short presentation regarding techniques that they used to attack and to defend from threats and what appropriate actions/defences were taken.

A. Hardware Used

The latest hardware that is being used widely in the industry will be used during the whole exercise. This will include PCMCIA based network interface cards like the Proxim Orinoco gold cards. These specific cards are used as they support promiscuous mode. Promiscuous mode is a mode whereby the network interface card is able to detect wireless networks although these networks do not broadcast their SSIDs. Newer hardware that uses the USB interface connection like Airpcap by CACE Technologies will also be explored and used. Wireless APs that can support the latest standards and features like WPA2 encryption and 802.11 a/b/g standards will be used. The Proxim Orinoco gold cards will be used with computers using Linux based operating systems while the Airpcap based USB dongles will be used with computers using Windows-based operating systems. A combination of desktop and laptop based computers will be used to simulate a real world scenario where you will have static and mobile users that access the wireless network.

B. Software Used

The choice of operating system software will be based on two platforms, vendor based and open source. Vendor based operating system software to be used will be Microsoft Windows XP, Professional and Server. All variations will be tested by the students to analyze the difference in features and level of security being offered by each one. For the open source based operating system, in this case a Slackware based open source Linux live cd called Backtrack will be considered. The choice is based on its compatibility with our existing hardware and the feature set offered by Backtrack, more important than other factors such as ease of use. The latest version which is version 2 will be used. It contains more than 300 different up-to-date tools like Kismet and the aircrack suite that is commonly used by security penetration testers. Backtrack is based on a slackware Linux distro (distribution). Version 2 release supports more and newer hardware as well as providing more flexibility and modularity. The use of open source software is well in-line with the governments initiative to decrease dependency on vendor specific operating systems which incur licensing and maintenance costs. While open source software is used widely in the exercise, students will also be exposed to vendor based software that must be bought like Commview for Wifi. This software will be used on a Windows platform for comparison in terms of features, effectiveness and reliability.

C. Environment Setting

An isolated, often separate network laboratory will be used to provide a safe active learning environment [2] so that no attacks can be launched into or out from the laboratory and no sensitive data or vulnerability information is inadvertently released. An alternative method that uses virtual machines can also be explored. The use of an isolated network or virtual machines, each has their pros and cons. The availability of a fully fledged and dedicated security lab is dependent on funding. The use of virtual machines on the other hand [7] & [8] is the latest alternative to a fully fledged and often expensive laboratory setup. Virtual machines offer features such as isolation, compatibility and encapsulation. This allows instructors and students to build virtual network topologies that consist of multiple, independent operating systems, but the downside of using this method is that it is often said that the use of virtual machines seems to be more inferior in terms of real life setting and environment. Other than that, operating system images are often used together with the virtual machines as they will enable pre-installed software to be used in the labs. This is so that each session can be personalised according to what learning objective is being taught. For example, if the wireless network needs DHCP server and FTP server services to be installed, then the instructor can pre-install the operating system images with these services prior to the start of class so that lab sessions can be done more easily

and in an efficient and safe manner saving time and effort on the students from having to install the services themselves.

V. Expected Outcomes

There are several expected outcomes hoped to be achieved as a result of using this method or approach.

The attack and defend approach hopes to help students to obtain and to polish their soft skills much needed in Malaysian graduates based on reports in [9] & [10]. Soft skills which include communication and persuasion skills especially when using social engineering techniques are obtained in abundance. Meanwhile, leadership and team work skills are attained as the students will be working and operating in teams as surely there must be a team leader and team member assignment.

Students will also develop a sense of pride when they can successfully break into or defend their wireless network. This sense of pride is even elevated when knowing that it was achieved as a result of their hard work, persistence and ability to work within a time frame and a set of objectives.

The attack and defend method expects that a sense of awareness will be raised amongst students of security problems especially those related to wireless security [3]. It is hoped that they will realise that every technology has its weaknesses and vulnerabilities, and often it is up to the users of the technology to be aware and take actions to rectify and to use these technologies accordingly based on situation and circumstances. Students are also expected to be more motivated as they will be more actively involved in the entire process of the attack and defend methodology, beginning from the early stages of the wireless network setup, installation and configuration of the operating systems through to the final step of presenting their results and observations of the entire session to their peers and the instructor or lecturer.

Although it has been said that this method will be done in a controlled environment, the university can also benefit if they permit the students to do a wireless network survey of the university's wireless network implementation. This is often done within a specified set of strict guidelines so that no unintentional harm is done to the wireless network infrastructure. This will indeed help the university to strengthen its wireless network security implementation and will be considered as a social service that can be offered by the faculty students to the university.

VI. Further Work

We realize and understand that while we believe that using this method or approach is expected to be better than the other common approaches currently in used, more research and scholarly discussion must be done on certain issues pertaining to this approach.

Ethical issues have always been a centre of debate especially when we are teaching our students methods regarding security. Questions that are expected to be raised include "Are we teaching our students to be hackers?" Often the best answer used is that teaching students these methods are just the same as car manufacturers doing crash tests, often doing many destructible kinds of testing on their own cars. So, it is the exact same approach that is being used, a wireless network can only be deemed secure if there has been auditing and penetration testing done on those networks, but in a controlled manner and often done by security professionals. Cynics will say that this approach will be just like exposing our networks to our students' mercy, but to counter these allegations, often the example of a key maker is used. While key makers surely must know how to break locks to homes, rarely do we hear that those caught earn a living making keys and locks. So, the most important issue when teaching students any sort of penetration testing, are exposing them to the ethical and legal issues involved. Methods like implementing strict background checks on the students, enforcing strict guidelines and making sure they sign a certain agreement have been explored [11] & [12].

There also arise issues regarding curriculum content. Is this approach suitable in depth and breadth? [13] and [14]. Because computer security in general covers a wide range of technology, careful selection of topics and particular attention given towards presenting it to the students is vital to ensure that instructors are not lost in the details of each technology.

Other than that, hardware and software resource & funding must be taken into account, whether it is obtained internally or externally [14]. Student to instructor ratio must be adhered to, to enable successful implementation of this approach. Often it is difficult to organize practical sessions involving all students because of lack of hardware/software devices. Obtaining funding from the industry like from Cisco for networking devices and from AMP/Tyco for network cables can be ventured and looked into. The use of virtual machines where students can mimic a complete network virtually using software like VMware and Microsoft Virtual PC is a common alternative if funding is an issue.

Lastly, there must be a well number of instructors, who are always aware of the current trends and technology to instruct and monitor these sessions. It is best if these instructors are well equip with industry certified certifications offered by vendor specific companies like Microsoft, Cisco and independent based consortiums like (ISC)2 . This is so that they are always in touch with the industry's need and expectations.

VII. Conclusion

Malaysian graduates while often excel in exams; have often been labelled as lacking the most important aspect looked for by the industry, which is soft skills and competency. We have shown that computer security is a hot issue nowadays and many institutions have been introducing these subjects into their curriculum. But often than not, educators, lecturers and instructors have a hard time teaching this subject because of the content and the need to balance theoretical knowledge with skills needed by the students. Realizing this, our paper

has tried to introduce an approach called the attack and defend approach that emphasizes soft skills and competency in this subject. This approach combines aspects of active learning and cooperative group work and uses a simple subtopic of wireless network as an example of implementation. Other researchers have shown that this approach is more suitable in teaching computer security as opposed to the other methods of teaching. While many other issues still needs to be addressed, it is our hope that students going through this method will be instilled with a more complete set of soft skills and competent in implementing knowledge learnt.

REFERENCES

[1] D. T. Tohmatsu, "2007 Global Security Survey," Deloitte Touche Tohmatsu 2007.
[2] W. Yurcik and D. Doss, "Different approaches in the teaching of Information Systems Security," in Information Systems Education Conference (ISECON) Cincinnati, Ohio, 2001.
[3] I. Hassan, M. R. Ayob, M. Sulaiman, A. S. Md Tahir, and M. R. Nordin, Practice and Application Oriented Education in KUTKM: Penerbit Universiti, Kolej Universiti Teknikal Malaysia Melaka, 2005.
[4] J. M. D. Hill, C. A. Carver Jr., J. W. Humphries, and U. W. Pooch, "Using an isolated network laboratory to teach advanced networks and security," SIGCSE Bull., vol. 33, pp. 36-40, 2001.
[5] S. Lindskog, U. Lindqvist, and E. Johnsson, "IT Security research and education in synergy," in 1st World Conference on Information Security Education Stockholm, Sweden, 1999.
[6] B. Hartpence, "Teaching wireless security for results," in Proceedings of the 6th Conference on Information Technology Education Newark, NJ, USA: ACM, 2005.
[7] W. I. Bullers, S. Burd, and A. F. Seazzu, "Virtual machines - An idea whose time has returned: Application to network, security, and database courses," in Proceedings of the 37th SIGCSE Technical Symposium on Computer Science Education Houston, Texas, USA: ACM, 2006.
[8] H. J. Mattord and M. E. Whitman, "Planning, building and operating the information security and assurance laboratory," in Proceedings of the 1st annual Conference on Information Security Curriculum Development Kennesaw, Georgia: ACM, 2004.
[9] IPPTN, "Masalah pengangguran di kalangan siswazah," National Higher Education Research Institute (IPPTN), 2003, p. 10.
[10] IPPTN, "University curriculum: An evaluation on preparing graduates for employment," National Higher Education Research Institute (IPPTN), 2004, p. 22.
[11] P. Y. Logan and A. Clarkson, "Teaching students to hack: Curriculum issues in information security," in Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education St. Louis, Missouri, USA: ACM, 2005.
[12] B. Pashel, A., "Teaching students to hack: Ethical implications in teaching students to hack at the university level," in Proceedings of the 3rd annual Conference on Information Security Curriculum Development Kennesaw, Georgia: ACM, 2006.
[13] M. E. Whitman and H. J. Mattord, "Designing and teaching information security curriculum," in Proceedings of the 1st annual Conference on Information Security Curriculum Development Kennesaw, Georgia: ACM, 2004.
[14] G. Vigna, "Teaching network security through live exercises," in Security education and critical infrastructures: Kluwer Academic Publishers, 2003, pp. 3-18.