A Novel Approach on Teaching Network Security for ICT Courses

Mohd Najwan Md Khambari, Mohd Fairuz Iskandar Othman, Mohammad Radzi Motsidi, Mohd Faizal Abdollah
Fakulti Teknologi Maklumat dan Komunikasi
Universiti Teknikal Malaysia Melaka
Melaka, Malaysia.
najwan_ra, mohdfairuz, radzi, faizalabdollah@utem.edu.my

Abstract— **This paper discusses a curriculum approach that will give emphasis on practical sessions 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 [1]. Research on active learning and cooperative groups showed that students grasps and have more tendency towards obtaining and realizing soft skills like leadership, communication and team work as opposed to learning using the traditional theory and exam based method. While this teaching and learning paradigm is relatively new in Malaysia, it has been practiced widely in the West. This paper examines a particular approach whereby students learning wireless security are divided into small manageable groups consisting of black hat and white hat team. The former will try to find and expose vulnerabilities in a wireless network while the latter will try to prevent such attacks on their wireless networks using hardware, software, design and enforcement of security policy and etc. This paper will try to demonstrate whether this approach will result in a more fruitful outcome in terms of students concept and theory understandings and motivation to learn.**

Keywords-wireless; networks; security; education; NS-2; wireless networks simulation;

I. INTRODUCTION

Computer and wireless network security has been a subject of much interest lately. In part, this is because of the changing world and the demands of people and business that require a certain standard of privacy, confidentiality and security when conducting their online transactions. Similarly, such concerns involved the treatment of data such as online business transactions and medical records in hospitals. Academia has long realised this and has taken active steps by introducing courses that deal with computer and network security in general and wireless security in particular. However, courses and subjects taught in institutions of higher learning tend to focus on the theoretical aspects of computer and wireless security, forgetting that the most important aspect of learning is not just discovering 'what' but also 'how' and 'why'. This paper will propose a new approach that will emphasize on practical methods 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 hands on learning will have greater impact on students compared to the normal way of discharging knowledge through lectures.

II. MOTIVATION

Currently, there is urgency in providing 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. A research done by Deloitte Touche Tohmatsu indicated that IT security budget saw an increase of 15% over the total spending in 2006 [2]. Business nowadays simply cannot rely on the term security through obscurity anymore as every business needs their presence on the Internet. This is where most transactions are done and valuable information are passed back and forth. Wireless security is becoming a more important and prevalent as it provides both mobility and flexibility for users. There is indeed an urgent need to secure wireless networks because of obvious insecurities and inherent vulnerabilities found in wireless technology [2].

Like it or not, wireless technology is here to stay with new and emerging standards such as Wimax that promises wider coverage. Therefore, it has been argued that to counter the threats is to face the technology head on. In doing that, the need for technically skilled and knowledgeable IT security professionals who can handle security particularly wireless security cannot be denied. Research such as [2] has shown that while companies realize the importance of security, only 7% felt that they presently have the required skills and competencies to effectively handle existing and foreseeable security requirements. 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 in Malaysia to address this matter, many of them still implement the traditional teaching and learning approaches that are not suitable in a fast paced and ever changing world of IT. Knowledge alone cannot compensate for technical skills and know-how.

III. COMMON APPROACH

Before presenting our proposed approach, it is best to describe some of the common approaches used in teaching and learning computer science as outlined by [3].

Firstly is the traditional lecture approach. It is a common method used especially in theory laden topics, 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.

On the other hand, the scribe approach includes elements of active learning where students are responsible for taking notes during lectures and will do a presentation based on their understandings during or after a lecture session. It can be seen that a significant number of higher institutions have begun to implement the scribe approach.

Meanwhile, the expert/mentor approach is the current method that uses guest instructors from the industry or lecturers who are well-versed and experts in their field. They will give lectures on specific topics. To enable this method of teaching, the university must have a good working relationship with the industry. The relationship can be built based on the university-industry joint research projects to help them solve industry related problems. Both parties 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 [1]. The university can benefit from this type of approach as guest lecturers from the industry could impart and share their experience and expertise within the context of the industry's perspective. This knowledge will indeed help shape the students' perspectives of actual working scenario and conditions.

The tutorial approach is often used whenever various information can be obtained via online sources. 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 relevant to particular topics.

Finally is the project approach which is also a norm in institutions of higher learning. At the beginning of the semester, students are given a project topic to be researched for the whole of the semester. This project is concluded by having students to present their findings and do hands on demonstration of their projects.

IV. Proposed Approach/ Methodology

Many scholars such as [4] stated 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, 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) [1]. 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 students 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 participating in practical sessions in labs, we believe that this is the most suitable method to be used.

Attack and defend methodology was first introduced by Texas A&M University [4] for the general computer security subjects. It has also been successfully implemented in institutions like Chalmers University of Technology [5] and Rochester Institute of Technology [6]. Although this method of teaching and learning were used in graduate level classes and are used to teach general network security concepts and theories, we believe that certain parts such as the wireless security subtopic can be implemented in undergraduate level classes.

Basically, this attack and defend approach would require the students to be divided into 2 teams. Each team are assigned either the Black Hat (offensive) or the White Hat (defensive) teams [3]. The main goal for the offensive teams is to compromise the security of 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 or to glance over to have a better look at their network setup.

The proposed approach requires that a simple wireless network be set up. In order to familiarize the students with the wireless networks and the background process, they are first introduced to a basic simulation setup in Network Simulator 2 (NS-2). During the introduction, the students will be exposed to the different types of traffic flow, basic architecture of the NS-2 simulator, agents in NS-2 that pump traffic and packets throughout the networks, applications that determines the types of the protocols to be used and so on. Those elements in the simulator reflect the real wireless network environment. Then, students are required to develop their own network scenario, both on ad-hoc and infrastructure mode of wireless networks using NS-2 and the Network Animator (NAM) that comes with the NS-2 to visualize the network. Both the infrastructure and ad-hoc mode can be visualized as Fig. 1 and Fig. 2 below.

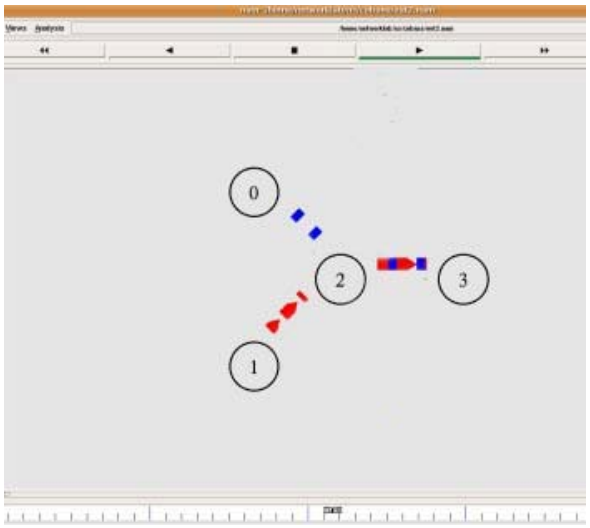

Figure 1. Example of an Infrastructure Mode in Wireless networks.

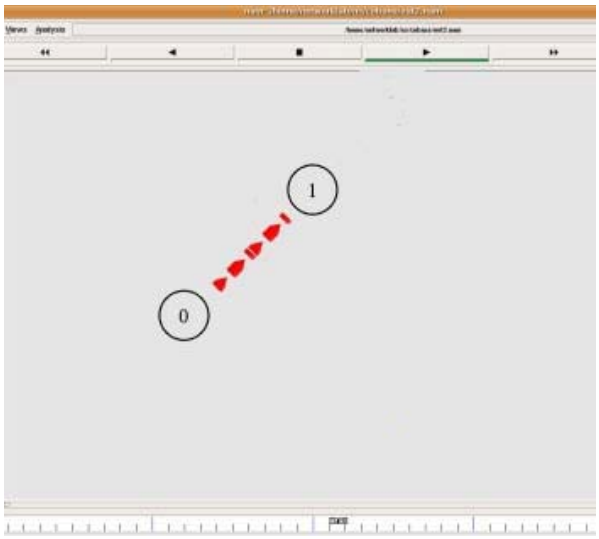

Figure 2. Example of an Ad-hoc Mode in Wireless networks

Even starting from this activity, an overall view of the students' skill and competency in building and configuring the wireless network can be evaluated.

After familiarizing the students with the wireless network environment, the practical or hands-on session will be done. The offensive teams 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 will be used. The next step will consist of two phases.

Phase I will start with a local site survey and traffic analysis. The defensive teams are required 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. 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. After all changes have been made by the defensive team, 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, which is the activity of capturing and analyzing the contents of the packets can be accomplished using Wireshark. Packet injection (generating bogus packets and inserting them into the network) and encryption attack (guessing of the keys used to encrypt the message) on the other hand can be applied using the aircrack suite. Meanwhile Kismet can be used to detect networks that disable SSID broadcasting. Teams will be graded based on the number of offensive and defensive techniques successfully implemented. A basic benchmarking system will be used to make sure that the basic offensive and defensive methods are successful.

Phase II will require the defensive teams to implement the more recent and recommended security settings. This includes 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 the 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. After all new changes have been made to the wireless networks, the offensive teams will get to penetrate the wall of defence created by the defensive teams by using existing methods mentioned in Phase I. This also includes the most deadly but forgotten method known as social engineering. It is the art of obtaining useful information just by way of interacting with the victim. 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.

V. 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 such as the Proxim Orinoco Gold. These specific cards are used because 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. 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. Meanwhile, wireless APs that can support the latest standards and features like WPA2 encryption and 802.11 a/b/g standards will be used. 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 who access the wireless network.

VI. SOFTWARE USED

For the hands-on session, the choice of operating system software will be based on two platforms, vendor based and open source. In this case, the vendor based operating system softwares used are Microsoft Windows XP Professional Microsoft Waindows Server. All variations will be tested by the students to analyze the differences in features and level of security being offered by each one. Meanwhile, for the open source based operating system, Linux Slackware Live CD will be used. The choice is based on its compatibility with our existing hardware and the features set offered by Backtrack. The latest version which is version 3 will be used. It contains more than 300 different up-to-date tools like Kismet and the aircrack suite that are commonly used by security penetration testers. Version 3 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 Malaysia government's 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.

Meanwhile, Network Simulator 2 (NS-2) will be used as the tool to simulate the wireless network environments. It is an event driven simulator that has been developed at the University of California, Berkeley that simulates a variety of Internet Protocol (IP) networks [7]. It implements network protocols such as TCP and UDP, traffic source behaviour such as FTP, Telnet, Web and Constant Bit Rate (CBR). Besides that, NS-2 is also capable of simulating router queue management mechanism such as Drop Tail besides supporting routing algorithms such as Djikstra. NS-2 has a specific support for mobile ad-hoc networks. NS-2 extends the usage of the node to support wireless nodes called MobileMS. The mobility features include node movement, periodic position updates and maintaining topology boundary. Some of the main factors of selecting NS-2 is that it is an open-source based network simulator which means the software can be downloaded, installed and modified for free, without requiring any fee or license which is very cost effective. Besides that, NS-2 is developed by a community based group. This means, there are numerous newsletters and support groups available across the Internet. Therefore there are many additional contributed codes and new features that are brought by many people. Meanwhile, a study was carried out by [8] to compare simulator performance, specifically for NS-2 and GloMoSim with testbed implementation. It shows that the performance results from the simulation tools of NS-2 are much closer to testbed results as compared to Glomosim. Another research was also carried out by [9] where findings showed that 43.8% proceeding papers of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc) from the year 2000 to 2005 used NS-2 as the tool to simulate networks. It is the biggest percentage compared to other simulators (10% uses GloMoSim, 6.3% uses Qualnet, 6.3% uses OPNET, 3.8% uses MATLAB and 2.5% uses CSIM). Therefore using NS-2 as the simulation tool is very significant.

VII. ENVIRONMENT SETTING

An isolated, often separate network laboratory will be used to provide a safe active learning environment [3]. This is to ensure that no attacks can be launched into or out from the laboratory and no sensitive, vulnerability information is inadvertently released. An alternative method that uses virtual machines can also be explored. The availability of a fully fledged and dedicated security lab is dependent on funding. On the other hand, the use of virtual machines [10] and [11] are 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. 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 personalized 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. However, the downside of using this method is that the use of virtual machines seems to be more inferior in terms of real life setting and environment.

VIII. EXPECTED OUTCOME

There are several expected outcomes hoped to be achieved as a result of using this approach. The attack and defend approach hopes to help students to obtain and to polish their soft skills which are much needed by Malaysian graduates based on reports in [12] and [13]. The soft skills which include communication and persuasion skills can be nurtured during the social engineering techniques. Meanwhile, leadership and team work skills can also be attained because the students will be operating in teams which involve 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 specific time frame within a set of objectives.

The attack and defend method expects that a sense of awareness will be raised amongst students about security problems especially those related to wireless security [1]. It is hoped that they will realise that every technology has its weaknesses and vulnerabilities. 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 allow the students to do a 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 the implementation of its wireless network security implementation and it will be a significant social service that can be offered by the faculty's students to the university.

IX. FURTHER WORK

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

Ethical issues have always been a centre of debate especially when we are teaching our students methods on security. Questions that are expected to be raised include "Are we teaching our students to be hackers?" Often the best answer given 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, albeit in a controlled manner, by security professionals. Cynics will say that this approach could expose our networks to our students' mercy, but to counter these allegations, the example of a key maker is often used. While key makers surely must know how to break the locks to homes, rarely do we hear that those caught actually 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 [14][15].

There are also issues regarding curriculum content [11][16]. Is this approach suitable in depth and breadth? Due to the fact that 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 [16]. Student to instructor ratio must be adhered in order to enable successful implementation of this approach. Often it is difficult to organize practical sessions involving all students because of the lack of hardware/software devices. Obtaining funding from the industry like Cisco for networking devices and 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 sufficient 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 equiped with industry certified certifications offered by vendor specific companies like Microsoft, Cisco and independent based consortiums like $(ISC)^2$. This is to ensure that they are always in touch with the industry's needs and expectations.

X. CONCLUSION

Malaysian graduates, while often excel in examinations, have often been labelled as lacking the most important aspects needed by the industry. These are the soft skills and the competency value. We have shown that computer security is a hot issue nowadays and many institutions have been introducing these subjects into their curriculum. However, educators, lecturers and instructors have hard time teaching this subject because of the content and the need to balance theoretical knowledge with practical and hands on skills. Realizing this, our paper has tried to introduce an approach called the attack and defend approach that emphasizes soft skills and competency in the teaching of 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 needed to be addressed, it is our hope that students learning through this method will be instilled with a more complete set of soft skills and competent in implementing knowledge learnt.

REFERENCES

[1] I. Hassan, M. R. Ayob, M. Sulaiman, A. S. Md Tahir, & M. R. Nordin, Practice and Application Oriented Education in KUTKM: Penerbit Universiti, Kolej Universiti Teknikal Malaysia Melaka, 2005.

[2] D. T. Tohmatsu, "2007 Global Security Survey: Deloitte Touche Tohmatsu "

[3] W. Yurcik, & D. Doss. "Different approaches in the teaching of Information Systems Security," Information Systems Education Conference (ISECON) 2001.

[4] J. M. D. Hill, C. A. Carver Jr., J. W. Humphries, & U. W. Pooch. Using an isolated network laboratory to teach advanced networks and security, 2001. SIGCSE Bull., 33(1), 36-40.

[5] S. Lindskog, U. Lindqvist, & E. Johnsson. "IT Security research and education in synergy," 1st World Conference on Information Security Education, 1999.

[6] B. Hartpence. "Teaching wireless security for results," Proceedings of the 6th Conference on Information Technology Education, 2005.

[7] NS-2, (2007). The ns Manual. Available at: http://nsnam.isi.edu/nsnam/index.php/User_Information

[8] F. Haq, & T. Kunz. "Simulation vs Emulation: Evaluating Mobile Ad Hoc Network Routing Protocols," Proceedings of the International Workshop on Wireless Ad-hoc Networks 2005(IWWAN'05), 2005.

[9] S. Kurkowski, T. Camp & M. Colagrosso, “MANET simulation studies: the incredibles,” ACM SIGMOBILE Mobile Computing and Communications Review Archive. vol. 9, 2005.

[10] W. I. Bullers, S. Burd, & A. F. Seazzu, “Virtual machines - An idea whose time has returned: Application to network, security, and database courses,” Proceedings of the 37th SIGCSE Technical Symposium on Computer Science Education, 2006.

[11] H. J. Mattord, & M. E. Whitman, “Planning, building and operating the information security and assurance laboratory,” Proceedings of the 1st annual Conference on Information Security Curriculum Development, 2004.

[12] IPPTN. Masalah pengangguran di kalangan siswazah. National Higher Education Research Institute (IPPTN), 2003.

[13] IPPTN. University curriculum: An evaluation on preparing graduates for employment. National Higher Education Research Institute (IPPTN), 2004.

[14] P. Y. Logan, & A. Clarkson, “Teaching students to hack: Curriculum issues in information security,” Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education, 2005.

[15] B. A. Pashel, “Teaching students to hack: Ethical implications in teaching students to hack at the university level,” Proceedings of the 3rd annual Conference on Information Security Curriculum Development, 2006

[16] G. Vigna, Teaching network security through live exercises. In Security education and critical infrastructures, 2003, Kluwer Academic Publishers, pp. 3-18.