Design and Implementation of Ethical Values Created Curriculum Development to Improve Mobile Security

S. Ravichandran, T. J. Nagalakshmi

Abstract: Medicinal imaging has assumed a key job in the direction of MIS strategies to expand the specialists' spatial introduction and help with the distinguishing proof of basic life systems and pathology. Current intransigent perception frameworks are promising. Be that as it may, they can barely meet the necessities of high goals and continuous 3D perception of the careful scene to help the acknowledgment of anatomic structures for safe MIS techniques. In this exploration we present a by and large relevant calculation which plans to furnish specialists with constant 3D perception of complete organ misshapen utilizing 3D optical fix pictures with constrained perspectives and a solitary preoperative MRI or CT filter. The proposed calculation is stretched out to remake the inside structures of an organ by just testing on the outside surface. Reconstructing is persuaded by our exact perception that the round consonant coefficients comparing to mutilated surfaces of a given organs lie in lower dimensional subspace in an organized lexicon that can be gained from a lot of agents preparing surfaces. The proposed methodology recognizes a structured scanty portrayal of every 3D surface. This enables the method to recreate discretionary organ misshapen utilizing exceptionally restricted watched information with high exactness.

Keywords: Ethical hacking, Information security, computer Forensics, computer ethics.

I. INTRODUCTION

Data and information is being transmitted in every fraction of second all over the world by the IT users from one place to other place virtually. Most of the user's experience the improvements in technology with minimum effort by simply learning the operations. They send and receive their valuable and sensitive data through the communication devices. Like the other side of the coin, the user must understand the dangers entitled with the technology. Developers spend more time and cost for the security related issues alone. There are some ethics in transmitting the information that every user must understand and know the limits of their application. So the importance of learning not only limited to only understanding the material but also how to apply it for the secure transmission [1]. This paper focuses on the ethical issues in the usage of communication media and devices related to student perceptions. One of the promising techniques to attain the incorporation of correspondences

Framework for communications system is OFDM.[13]The proposed curriculum with the contents to be taught is also suggested by the trained instructors [5].

II. METHODOLOGY

The students in the universities are accessing the mobile devices with Wireless hot spots (Wi-Fi) to work at any time to increase their productivity. There are two modes of connectivity available: Ad hoc and Infrastructure modes. Some universities have connected their wireless devices with wired infrastructure devices instead of ad-hoc networks which are applicable only for limited users. Generally universities places their security measures such as firewalls, intrusion detection systems etc. around their wired infrastructure [6]. But they do not focus the same attention to the laptops and other mobile devices that students use while residing inside and outside of the campus.

The dangers involved with the wireless environment are discussed in the following two sections.

A. Evil Twin

The Evil Twin attack is set up by a hacker by a laptop to act as an Access Point (AP). As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites [14]. Several commercials and freeware software tools are available that can turn any laptop with a wireless card into a so-called soft AP [6]. The soft AP can broadcast AN identification beacon or Service Set symbol (SSID) that lets different computers comprehend it is offered. The hacker gives legitimate names like Reusable, Waypoint, and Free Internet Access, to fool unsuspecting users. These hot spot users connect with what seems to be a legitimate hot spot. When, it is connected the hacker can send the user to web content created to seem authentic. As the user enters passwords or creates a replacement ID with master card data, all entries square measure logged by the hacker for future abuse. If the hot spot user connected to the university network, then the hacker would have a valid user name and password to legally connect to the university system, undetected and well-armed to potentially

Revised Manuscript Received on December 11, 2019.

***** Correspondence Author

Dr. S. Ravichandran*, HOD & Prof., Computer Science Department, Annai Fathima College of Arts & Science, Madurai, India.

Ms. T. J. Nagalakshmi, Asst. Prof., Electronics and Communication Engineering Department, Saveetha School of Engineering, SIMATS, Chennai, India.

damage the university's reputation, steal critical information, and/or use the university network to launch a downstream attack.

B. Other vulnerabilities

Laptop users often do not update their system with latest anti-virus and other patches to secure the device.

Hackers know this, and they easily attack the devices for their future abuse. A Windows XP machine (in this case the target) is designed to automatically send probe frame requests whenever the Windows XP machine is powered ON.

With the use of hot spotter, the preferred network listed in the target machine's Windows XP Zero Config may be examined and used to establish network connectivity with the target machine. At this point, the [targeted] mobile device can be completely compromised by the hacker,.

III. STEPS UNIVERSITIES MUST TAKE TO ENSURE MAXIMUM SECURITY

AirDefense [6] recommends the following WLAN security practices:

- install a firewall on laptops;
- use hot spots only for Internet surfing;
- Insert passwords only into websites that include an SSL key;
- disable/remove the wireless card if you are not actively using a hot spot;
- ensure that all laptops are updated with the latest security patches;
- avoid hot spots where it is difficult to tell who's connected;
- if the hot spot is not working properly, assume your password has been compromised, and change your password at the next opportunity;
- read all pop-up windows in their entirety;
- do not use insecure applications such as non-encrypted emails or instant messaging while at hot spots; and,
- explicitly disable municipal Wi-Fi access from within the enterprise.

In addition, university IT departments should look forward to tools that automatically assist security problems. Security policies must be adopted by ensuring all WLAN user machines fully patched and have upon date virus protection in place before allowing access to the wired university infrastructure network.

To learn these protection methods the curriculum must adopt some added courses that are needed of the hour [9]. The curriculum must be built with the hacking techniques from the view of a professional hacker or a cracker. The other course must teach the protection methods to mitigate all sorts of attacks. But while teaching hacking courses, there must be some ethics to be followed strictly.

A. Importance of a IS practical courses in the curriculum

The present curriculum in the IT related fields have some basic courses on security issues namely Information Security, network Security etc. The courses are taught theoretically with minimum number of case studies. But due to the advancements in the technology and the tools that are available at minimum cost and effort, the hackers attack the devices and steal the valuable data. So the students must have a separate course that gives them the awareness and updated prevention methods to overcome these sorts of problems.

Some IT Companies have ethical hackers inside and outside their complex to entail a maximum testing on their security. University students must also have these types of courses by the trained professionals. But the course must follow some ethics related to the limits and morals adopted [2].

B. What to teach?

At the school in question general ethics instruction is distributed over several courses. There is a requirement for an ethics based liberal studies course, there is at least a week [2] of ethics coverage in a required business law course, and there are ethics modules in several other core business classes. Students in the MIS class will have completed the business law course and many of them will have completed the ethics oriented liberal studies course. Almost no students in the introductory IS course will have taken either of these courses [7]. In addition, there is approximately one week of coverage of IS ethics related topics in both the introductory IS and MIS courses. Summary results of this survey were reported to the classes and appeared to serve as a rather effective vehicle for stimulating discussion around IS ethical dilemmas.

IV. COMPUTER FORENSICS

Dardick and Lau (2005) argued that an in-depth understanding of digital forensics is needed by college students who will enter into the various fields like Information technology, business, criminal justice, law, and homeland security. McGuire and Murff (2006) discussed issues in the development of a digital forensics curriculum [5]. Gottschalk et al. (2005) offered an initial review of computer forensics programs in North America. Soe et al. (2005) discussed the deployment of computer forensics classes at undergraduate/graduate levels in a shared classroom/lab environment.

A. Minor Curriculum on computer forensics

The addition of a PC Forensics Minor is going to be begun purpose for a certification program and will probably result in the event of a PC Forensics Major Program providing. The addition of this minor can provide the scholars the chance to feature a data processor Forensics part to go with the Scientific Forensics programme offered by the faculty of Arts and Sciences. Students in Technology degree programs within the school of Business and knowledge Systems can have a chance to expand their instructional expertise into an extra specialization space compatible with corporate and government needs [3].

The benefits are,

- Students will be able to operate in a corporate environment as a security analyst [10].
- The Computer Forensics Minor will offer a start point for students in the field of Digital Forensic Investigation.
- The minor will prepare students entering the business world with basic computer investigative training.

The Students will use the latest investigative tools including computer tablet technology interest.

.

V. RESULT AND DISCUSSION

The purpose of security is to ensure protection of computer assets belongs to the business, personal, military, government and academic research institutions. The need for security has risen to another level which places the burden on the organizational entity to conduct investigations into illegal or harmful computer transmissions [5]. This presumed liability cannot be excused by a lack of prior knowledge.

Universities and organizations must actively investigate suspected illegitimate activities. The goal of the proposed minor curriculum is to expand the knowledge base of security students which could lead to internal skills for investigating network intrusions and internal security breaches [8]. The rising need in organizational security has resulted in development of this forensic minor proposal [11]. While this course of study doesn't propose to make PC rhetorical specialists, it'll actually offer students the idea to conduct internal investigations and educate them within the use of forensic computer tools.

A. Course Schedule

Required Courses in the minor level

- Computer Forensic fundamentals
- Defense and Forensics Countermeasures
- Advanced Computer Forensics
- Computer Forensics and Investigation

Elective courses in the minor level

- Management of Wireless Forensic Security
- Computer Forensics Project
- Cyber law
- Internet Forensics

B. Course Contents

The contents of the above courses are proposed below [5]:

Courses Computer Forensics Fundamentals

In this course, students learn the basic principles and ideas in laptop forensics. The topics embrace the classification of the digital evidences, the procedure of discovering and conserving evidences, varieties of laptop and web crimes, and analyses of computer crime statistics and demographics. Students additionally learn the way to go looking and retrieve info to seek out the evidences' victimization some common tools. Related legal procedures, laws, and laws are mentioned concisely.

Elective courses in the minor level

The focus of this course is on the utilization of tools to secure a network and the way the tools integrate with the various in operation systems and also the procedures necessary to protect a network through cautious events. The forensic nature of network defense is intrusion. This focus of this course is on the use of tools to secure a network and how the tools integrate with the different in operation systems and also the methodologies necessary to shield a network through defensive measures. The forensic nature of network defense is intrusion. This course prepares students for detection, investigation and systems audit procedures [13]. Since the course relies on tool usage, there'll be a relentless amendment within the course materials implementing new techniques and introducing new ideas.

Advanced Computer Forensics

This course deals with advanced and rising topics in laptop forensics. It introduces students to comprehensive analysis tools and covers how to use the tools and other applications for common forensic procedures. The course is a combination of lecture, demonstrations, and practical exercises that focus on the analysis tools (e.g., EnCase, FTK).

Computer Forensics and Investigations

Networks are transport, not storage elements. Therefore, all information should be captured and keep in real-time, or it'll be lost forever. This presents a chance for multiple forms of investigations. There square measure needs to audit logs to research traffic patterns and it applies to host yet as network traffic. This level of investigation ends up in router forensics and internet attack investigations. These types of investigation expand to email and discovery of email crimes, stenography, and mobile devices. This course covers a formal environment. Conduct forensic media investigation requirements and analysis and log file analysis to investigative reports. Student's square measure introduced to "Expert Witness" needs together with liabilities related to proof assortment and room testimony.

Internet Forensics

This course introduces students to a range of Internet-based evidences and computer code. Emphasis is placed on exploitation common media analysis tools and techniques to find and recover Internet-based proof in an exceedingly forensically sound manner. This course presents solutions to problems that may be encountered during analysis. This course examines advanced digital rhetorical information recovery topics, tools, and practices to recover information and aid investigations. Students learn ways in which to defeat information activity techniques like stenography, encryption, and passwords on protected systems. Hands on exercises that reinforce the learned techniques square measure enclosed.

Management of wireless Forensic Security

This is a course that examines wireless technologies from a rhetorical and investigatory perspective. Students learn basic communication ideas that facilitate them perceive the capabilities and limitations of varied technologies. A number of active exercises reinforce lecture material whereas providing students with first-hand data of varied vulnerabilities. Evidence collection and handling will be emphasized. Focus is placed on the volatility of proof and also the have to be compelled to secure crime scenes. Evidence handling associated chain of custody problems square measure the central thread in managing an investigation.

Computer Forensic Project

This is a scenario-based course that teaches students how to conduct detailed data analysis in a laboratory determine the specifics of a Linux-based (or other platform) intrusion. Students use tools associated analysis techniques to investigate network traffic of an interloper and correlate the findings with rhetorical proof found on a UNIX (or different platform) victim machine.

Cyberlaw

Cyberlaw may be a study of the legal (and ethical) aspects of managing technology each within the work and Net. The course focuses on problems concerning electronic commerce, technology, property, and therefore the net. Social, legal, ethical, and political issues are addressed with a global perspective.

VI. CONCLUSION

Security is the major threat that remains on the Internet and mobile environment still under investigation. The user easily adapts his new environment without any hesitation when it is reliable and fast. Many users blindly believe that their data is communicated with maximum privacy since it is authenticated via a private user name and passwords. When they experience any inconvenience in their communication, they simply change their passwords. Since Information and web technologies are prevalent, each and every user must be aware of the attacks that are made to their virtual environment. They can prevent their environment from unknown attacks only when it is identified by firewalls and other security tools. So the computer forensics knowledge must be taught basically to every user when they transmit their valuable personal and business data. The above suggested curriculum will meet the requirements to understand the ethics behind the technologies. On the other dimension, the students get opportunity to work as security analysts in universities, business organizations and other IT related fields. Once, the ethics are taught the level of security may move to have other dimensions.

ACKNOWLEDGMENT

The authors are thankful to James Morgan, Gregory Neal, Vance E. Poteat and Donna Woo providing the necessary facilities for the preparation of the paper. At last, I extend my heartfelt salutations to our beloved Parents, my Wife and to the almighty to establish this paper in successful manner.

REFERENCES

1. T. Andrew Yang, "Computer security and impact on computer science education", Consortium for Computing in Small Colleges, In *Journal of Computing Sciences in Colleges*, 16(4), Apr.2001, pp. 220-229.
2. M. Robert Davison, " Professional ethics in information systems: a personal perspective", *Communications of the Association for Information Systems*, 3(8), Apr.2000, pp.178-186.
3. James Morgan, Gregory Neal, Jo-Mae Maris, "The development of student perceptions of ethical issues in the use of IS*", Journal of Computing Sciences in Colleges*,24(1), Oct.2008, pp. 520-529.
4. Melissa Dark, NathanHarter, Linda Morales, Mario A. Garcia, "An information security ethics education model*", Journal of Computing Sciences in Colleges*, 23(6), Jun.2008, pp. 347-356.
5. Ajantha Herath and Suvineetha Herath, Rohitha Goonatilake, Susantha Herath and Jayantha Herath, "Designing computer forensics courses using case studies to enhance computer security curricula*", Journal of Computing Sciences in Colleges* ,23(1), Oct.2007, pp. 118-125.
6. DaveWassenaar, Donna Woo, and Penn Wu, *"*A certificate program in computer forensics", *Journal of Computing Sciences in Colleges*, 24(4), Apr.2009, pp.158-167.
7. Http://www.cybercrime.gov/
8. William Figg, Zehai Zhou, *"*A computer forensics minor curriculum proposal*", Journal of Computing Sciences in Colleges*, 22(4), Apr.2007, pp.32-38.
9. Http://www.ftc.gov/os/caselist/
10. Joanne Sexton, "Dangerous mobile behavior our students and university employees need to know about", *Journal of Computing Sciences in Colleges*, 23(2), Dec.2007, pp.174-18.
11. E. Vance. Poteat, "Classroom ethics: hacking and cracking", *Journal of Computing Sciences in Colleges*, 20(3), Feb.2005, pp.225-231.
12. A. Jennifer, Polack-Wahl, " *Actively learning computer ethics",* Consortium for Computing in Small Colleges, *In Journal of Computing Sciences in Colleges*, 5(15), Apr.2000, pp. 160-169.
13. R.Santhakumar, N.Amutha Prabha," Resource Allocation In Wireless Networks By Channel Estimation And Relay Assignment Using Data-Aided Techniques". *International Journal of MC Square Scientific Research Vol.9, No.3,2.017*.
14. J.Shiva Nandhini, Arun Kumar.S, Abishek.N, Meerah.G, Ashika.G" An efficient key policy attribute based encryption scheme in cloud computing" *International Journal of MC Square Scientific Research Vol.9, No.3,2.017*.

AUTHORS PROFILE

Dr. S. Ravichandran, M.C.A., M.Phil., M.Tech., ME., Ph.D., working as a HOD & Professor in Department of Computer Science at Annai Fathima College of Arts & Science, Madurai, Tamilnadu State, India. He has 21 years of teaching experiences in various Colleges. He has published 20 papers in International journals, he has presented in 15 International Conferences & presented in 19 National Conferences at various Engineering Colleges. His areas of specialization are Cloud Computing, Artificial Intelligence, Networks and Compilers.

Ms. T. J. Nagalakshmi, ME., (Ph.D.), working as a Asst. Professor in Department of Electronics and Communication Engineering at Saveetha School of Engineering, SIMATS, Chennai, Tamilnadu State, India. She has 11 years of teaching experiences in Engineering Colleges. She has published 20 papers in International journals and has presented in 5 International Conferences at various Engineering Colleges. Her areas of specialization are VLSI, Artificial Intelligence, Networks and Compilers.