Incorporating Hacking[1] Projects in Computer and Information Security Education: an Empirical Study

Eman Alashwali

Information Security Research Group
Faculty of Computing & IT, Information Systems Department
King Abdulaziz University, Saudi Arabia

ealashwali@kau.edu.sa

Abstract. Incorporating hacking projects in information security education is controversial. However, several studies discussed the benefits of including offensive exercises (e.g. hacking) in information security courses. In this paper, we present our experiment in incorporating hacking projects in the laboratory exercises for an undergraduate-level Computer and Information Security (CIS) course at King Abdulaziz University (KAU), Saudi Arabia. We conducted a survey to measure the effectiveness of incorporating hacking projects from the students' perspective. We also questioned the ethical aspects of these projects. The results strongly suggest that hacking projects have helped the students better understanding computer and information security principles. Furthermore, the majority of the students stated that they do not intend to misuse the learned skills, mainly, for religious and ethical reasons. We also present the precautions that we took to avoid legal or ethical consequences that may be connected with these activities.

Keywords: information; security; offensive; defensive; education; Saudi Arabia; hacking; cyberattack; awareness; ethics

Biographical notes: Eman Alashwali obtained her Master degree in Information Security from University College London (UCL) in 2012, Bachelor degree in Computer Science from King Abdulaziz University (KAU) in 2004. She also holds several career certifications such as MCSA, CCNA, A+, N+, I-Net+. Eman is working in university

[1] There are different definitions for the term "Hacking". In this paper, we use the term "hacking" to refer to the exercise of exploiting a vulnerability (i.e. break the security) of a system to assess its security (ethical hacking).

teaching since 2007. She is a Lecturer in the College of Computing & IT (CCIT) at KAU, Saudi Arabia. Prior to joining the academic field, she spent three years working in IT departments in different educational organizations. She also was the first one to be selected to fill the Head position for the Labs and Technical Support Unit in the CCIT.

1 Introduction

1.1 Internet and Cyberattacks in Saudi Arabia

Internet use in Saudi Arabia is rapidly increasing. As of June 2012, the number of Internet users in Saudi Arabia had hit 13,000,000 (Internet World Stats, 2012), which means that more than half of the population (estimated at 26,939,583 by (United States Census Bureau, 2013)) use the Internet. The Internet has not only been adopted in its ordinary means but has also become a ubiquitous component of citizens' lives. A study by Google (2012) showed that 60% of the Saudi population owned smartphones, and 66% access the Internet daily using these devices. More importantly, a considerable amount of sensitive information are being transferred; 25% of these smartphone users made an online purchase using their phones (Google, 2012).

As Internet use grows, so do cyberattacks. In 2010, a report based on the Kaspersky Security Network (KSN) that recorded 327,598,028 malicious attempts to infect users' computers in various countries worldwide reported that Saudi Arabia was among the top 20 countries targeted by cyberattacks and the attacks were increasing (Securelist, 2010). In the report, Saudi Arabia ranked 13th in 2010 but had been 17th in 2009 (Securelist, 2010). More dangerously, based on several recent incidents that received public attention, cyberattacks in Saudi Arabia are targeting not only ordinary users but also government websites and extremely sensitive sectors. For instance, in 2012 an attack targeted Saudi Aramco, a government-owned company that makes more than USD 1 billion per day in revenues and was ranked the biggest energy company in the world by (Forbes, 2012). The attack targeted the country's economy by attempting to disrupt oil production, according to officials (Saudi Aramco, 2012). Fortunately, although the attack infected about 30,000 workstations, it did not affect oil production (Reuters, 2012). Another less serious attack, by a hackers group called "Saudi Anonymous" occurred in May 2013. They launched a series of attacks that targeted many Saudi government websites (see Fig. 1). In the same month, the Saudi Press Agency (SPA) (2013) officially announced that

several government websites had faced simultaneous attacks, including the Ministry of Interior portal that went down for about an hour.

Fig. 1. A screenshot of tweets by the Saudi Anonymous hackers group

1.2 Information Security Education in Saudi Arabia

As Bishop (2000) discussed in his article "Education in information security", the two main forms of information security education are: 1) academic education, which includes technical preparation for undergraduate students, and 2) public awareness.

In the Saudi Arabia case, we believe that both aspects require more attention. For example, as an illustration of technical preparation for security professionals aspect, Alzamil (2012) measured the level of security awareness from IT employees' perspective. The study surveyed 134 IT managers and employees in 41 public and private organizations in Saudi Arabia (Alzamil, 2012). The results show some misconceptions among IT employees regarding information security issues such as lack of awareness among IT employees about internal threats (Alzamil, 2012). Furthermore, the results suggest that not enough information security training is provided to IT employees (Alzamil, 2012).

Alghathbar et al. (2008) conducted a vulnerability assessment for 169 of the most popular Saudi organizations' web servers, including government, academic, and commercial organizations. The researchers found and classified 16 types of vulnerabilities that affected one or more of the servers (Alghathbar et al. 2008). The top-ranked vulnerability affected 27 servers (16% of the sample) (Alghathbar et al. 2008). This vulnerability can result in buffer overflow (Alghathbar et al. 2008), which can cause dangerous consequences such as allowing an attacker to execute an arbitrary code without the server's administrator consent. All vulnerabilities listed in the study are known vulnerabilities that can be easily discovered with free tools and avoided by updating a piece of software, installing a patch, or changing configurations, as Alghathbar et al. (2008) showed. This study reflects a lack of security awareness and education among the servers' administrators.

From the public awareness aspect, a large-scale survey by Alarifi et al. (2012) that included 462 participants measured the level of information security awareness among Saudi citizens and revealed worrisome results. The study showed a low level of awareness about some well-known security attacks. The study showed that only 25.5% of the participants were aware of identity theft, 29.7% were aware of phishing scams, and as few as 7.4% were aware of Denial of Service (DoS) attacks (Alarifi et al. 2012).

1.3 Our Motivation and Aim

Protection against security threats can never be achieved without both well-prepared security professionals and aware end users. Universities play a crucial role in preparing future professionals. Our main goal is to improve the level of understanding of computer and information security principles by incorporating hacking projects in the lab exercises of the Computer and Information Security (CIS) course offered to IS undergraduate students at King Abdulaziz University (KAU).

Incorporating offensive techniques in information security education is controversial. However, many researchers have discussed the benefits of teaching offensive techniques in information security education. Many universities worldwide include offensive techniques in their information security courses.

We believe that offensive lab exercises (e.g. hacking) are crucial to build a security mindset. The security mindset is different than the ordinary engineer mindset (Schneier, 2008). It "involves thinking about how things can be made to fail" (Schneier, 2008). The absence of the security mindset will result in insecure systems (Schneier, 2008).

However, to the best of our knowledge, we believe that such lab exercises are not widely known among Saudi universities. We are not aware of any work that has evaluated or shared their experience in incorporating offensive techniques in information security education at Saudi universities. In this paper, we evaluate the effectiveness of adding a hacking project in the lab exercises from the students' perspective, and we share our experiment and results.

1.4 Structure of the Paper

The rest of the paper is organized as follows: In section 2, we provide a brief background description. In section 3, we summarize related work. In section 4, we describe the study

methodology. In section 5, we present the results and discussion. In section 6, we conclude. In section 7, we provide examples of students' work.

2 Background

2.1 Offensive vs. Defensive Security Education Methods

Frincke (2003) defined two major philosophies in information security education: "defensive assurance" and "attack understanding". The "defensive assurance" philosophy concentrates on teaching students how to build systems that meet a security policy, design defenses that can not be broken, and prove that this has been accomplished (Frincke, 2003), in other words, "how to do things right" (Frincke, 2003). In contrast, the "attack understanding" philosophy allows students to better understand how to assess systems for weaknesses, design systems free of these weaknesses, and set up defenses against these weaknesses through hands-on learning about how attackers think (Frincke, 2003). The "attack understanding" philosophy questions "what others are currently doing wrong" (Frincke, 2003). It also incorporates learning about attack techniques and defensive techniques and allows students to verify systems' security from a practical rather than formal point of view (Frincke, 2003). Some works refer to the two philosophies as defensive and offensive.

2.2 The CIS Course in the IS Department at KAU

The CIS course at KAU is a compulsory course for undergraduate IS students (KAU, 2013). It contains 1.5 hour/week laboratory sessions supplementary to the 3 hour/week theoretical lectures in a whole semester. In general, the laboratory contains exercises that provide students with practical skills in the subject area. Covering attack-related issues is part of the course's official description: "It covers the topics of security of information and software systems including attacks and data encryption" (KAU, 2013). However, before our proposal was implemented, the available lab manual did not contain exercises that involved security attacks or offensive techniques. We proposed adding a hacking project to the lab exercises.

2.3 Saudi Arabia, a Social Background

We investigated socio-technical aspects such as the reasons that influenced our participants' decisions not to misuse the learned hacking techniques. Therefore, it is convenient to describe several characteristics of Saudi Arabian society. Saudi Arabia is one of the world's top oil-producing countries. It is a young society; about 64% of the population are under the age of 30 (Murphy, 2013). In the last decade, the government has provided unprecedented support for education. For example, in 2013, the government allocated 25% of the national budget to the education sector, about USD 54.4 billion (Ministry of Finance, 2013). The Islamic religion is very important in Saudi Arabia, for the government and the people. All of the country's decisions, educational curricula, official media content, etc., must comply with the Islamic religion. Religion is taught during all 12 years of school education as well as at universities. At KAU, for example, students in all disciplines must pass four compulsory Islamic Culture courses. In a survey by Moaddel (2006), 90% of Saudi citizens believed religion is very important in their lives.

These social characteristics data may explain some of the information or results presented in this paper. For example, the striking figures for Internet use and technology adoption described in section 1.1 might not be very surprising knowing that two-thirds of the population is under the age of 30.

3 Related Work

Mink and Greifeneder (2010) conducted an empirical study to compare the offensive and defensive methods in information security education. The comparison is based on tests results for two groups where each group received different method. The results suggest that the offensive teaching method resulted in better understanding of information security (Mink and Greifeneder, 2010). Regarding criticisms about teaching such techniques that might be misused, the authors believe that such criticism is flawed as any security technique can be used and misused (Mink and Greifeneder, 2010). Mink and Greifeneder (2010) did not present students sentiments as we do in this paper. Instead, they provide quantitative data based on tests results.

Papanikolaou et al. (2011) presented their work using the "Hackademic" tool, an open source tool equipped with deliberately vulnerable web applications that allow learners to practice hacking (Papanikolaou et al., 2011; OWASP, 2013a). The survey results showed

that 85% of the students believed that the lab exercises had helped them better understand the security issues that every exercise addressed (Papanikolaou et al., 2011).

Trabelsi and Ibrahim (2013) presented a case study that incorporated offensive techniques in lab exercises about three types of DoS attacks. The researchers measured the students' satisfaction; 85% of the students said that the lab exercises helped them better understand the theoretical concepts of DoS attacks (Trabelsi and Ibrahim, 2013). Furthermore, 86% strongly recommended the exercises to other students (Trabelsi and Ibrahim, 2013). On the other hand, about 85% of the students said that they had tried to test the learned DoS attack outside the isolated lab environment (Trabelsi and Ibrahim, 2013). The researchers also suggested tips for reducing the concerns related to offensive exercises (Trabelsi and Ibrahim, 2013).

Trabelsi and Ibrahim (2013), and Papanikolaou et al. (2011) presented students' opinions regarding offensive exercises in general. However, our work investigated what most influenced students' decision to avoid misusing the skills learned that none of the previous work questioned. Furthermore, we present the students' opinions in a more detailed 5-point Likert scale.

In addition, the author of this paper has experience as a former postgraduate student at University College London (UCL) in 2011/2012 attending two levels of computer security courses and applied cryptography course that included some offensive techniques in some exercises. In the Computer Security I course taught by Courtois (2011), students were exposed to instructor-led lab exercises provided by Giotsas (2011) to implement several known attacks (e.g., SQL injection, Man-in-the-Middle-Attack (MITM), etc.). Also, in the Computer Security II course taught by Desmedt (2012), students were required to implement a project, e.g., an attack one, either independently or in a group using a research-oriented method that included submitting a two-page paper and preparing a presentation. In applied cryptography course, there were a smart-card and RFID security lab sessions, designed and taught by Courtois (2011). In the lab sessions, students examined the security of smart cards using some offensive exercises. For example, the students tested magnetic card by "skimming" some buildings and bank cards to see how easily they can be copied and forged. Also, the students could optionally try to extract the cryptographic keys for some types of insecure cards. The author was inspired by this experience and was encouraged to transfer part of it to KAU students.

Our method was similar to Desmedt's (2012) in that it was a research-oriented method. We do not claim that this paper presents a new educational method. Many universities worldwide have adopted offensive practical exercises in information security

education. However, we believe that our paper presents results that are worth sharing for several reasons. First, we are not aware of any previous work that provided an experiment and students' feedback regarding incorporating offensive techniques in laboratory exercises in information security education among Saudi universities. Generally speaking, "hacking" is still viewed as a negative act in Saudi society. As far as we are aware, no companies or the government sector announced about rewarding white-hat hackers who report security flaws found in the companies' websites or systems. However, some companies worldwide, such as Facebook and Microsoft reward hackers who report security flaws. Second, Saudi Arabia has special social characteristics (e.g., intensive religion education) that—as we will show later—influence ethics which is an aspect that need to be considered in hacking. Therefore, our data can be useful in ethics in information security. Third, since our subjects are female students, our paper provides results in relation to women in engineering (information security in particular), a topic adopted by leading engineering associations such as IEEE Women in Engineering (WIE) (IEEE, 2014).

4 Study Description

4.1 Study Sample

The study subjects were 39 female undergraduate students from the IS department in the College of Computing and Information Technology (CCIT) at KAU who were enrolled in the CIS course in the second semester for 2012/2013. According to the biographical data obtained from this study survey, their ages ranged from 20 to 24. Regarding their programming experience, all had studied two levels of compulsory programming courses. In terms of their cultural background, all students said they had studied Islamic religion during all 12 years of education before attending the university.

4.2 *Methodology*

At the beginning of the CIS lab sessions, we provided the students with a list of eight known attacks with a brief description of each attack. The proposed topics were as follows: 1) Click-Jacking, 2) Cross-Site Scripting (XSS), 3) Cross-Site Request Forgery (CSRF), 4) SQL-Injection, 5) Smart Phones Security Risks, 6) Network Sniffing, 7) Social Engineering, and 8) Cracking Wireless Networks. In Appendix A, we provide a

brief description about each attack. We also provided the students with the hardware (e.g., switches, cables, wireless access points, etc.) if they needed.

The students were asked to arrange themselves in groups of three or four students (groups of five students could be accepted in two cases as an exception). Each group was asked to select a unique topic. Repeated topics were accepted if all the topics were taken. The groups were also given the opportunity to propose their own ideas after receiving the instructor's approval; however, no one proposed any. To meet the project requirements, the students were asked to do the following:

1. Implement a demo that demonstrates one or more examples of the attack.
2. Write a maximum four-page conference-style paper about the attack including the implementation and possible defenses against it.
3. Prepare a 10-minute presentation that summarizes the project.
4. Prepare a poster. The students could voluntarily present their posters at an annual college-level technical event called "IT Open Day" to raise awareness of security threats.
5. Prepare a detailed technical report or a video recording to provide a step-by-step description of the attack implementation.

The project represented 10% of the students' final grade for the course. During the semester, there were follow-up presentations in which each group gave a 10-minute presentation describing their progress. The paper submission had two phases: a draft submission, after which the students received feedback, and then the final submission. All groups except one implemented at least one example; however, that group presented the topic theoretically.

At the end of the course, we distributed an anonymous survey to all students enrolled. The paper-based survey evaluated several aspects of the lab including the hacking project exercise. In this paper, we analyze the project part. The survey questions format were either to rank the students' agreement on a given statement in a 5-scale Likert style (Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree), or simply a multiple choice question were the student can select one or more answer (see section 5.1 and 5.2 for more details about the project part questions) except one open question at the end of the survey for further comments. Each question was written in two languages, Arabic and English, placed in front of each other in the same survey. Participants made aware that this survey results will be used for research purposes.

4.3 Handling the Ethical and Legal Concerns in Implementing Hacking Project

When allowing students to practice hacking, there is always a concern that the learned skills may be misused either accidentally or intentionally. This concern is realistic. For example, in (Trabelsi and Ibrahim, 2013), the authors observed a considerable increase in the number of DoS attacks detected by their university's intrusion detection system each semester after students learned the DoS attack technique in the information security lab. More dangerously, as mentioned earlier, survey results showed that about 85% of the students said that they had tested the learned DoS attack outside the isolated lab environment (Trabelsi and Ibrahim, 2013). Therefore, precautions must be carefully considered.

Trabelsi and Ibrahim (2013) listed several precautions such as informing students of the legal consequences, asking students to sign a "code of conduct," and using isolated networks for offensive exercises. Similarly, in Desmedt's (2012) course, we were asked to sign a declaration that conveyed the student would perform the attack in isolated networks and not against real systems and the student would use his or her own credentials. Also, in Giotsas (2011), we implemented the attacks in virtual machines provided by (SEED project 2013; Due 2011).

In our case, to overcome the undesired consequences, we provided students with the following instructions:

1. Experiments on network security such as attacking wireless networks must be implemented in an isolated network using testing devices.
6. If the experiments need credentials, they must be self-owned or used with the account owner's permission.
7. Experiments on web security such as click-jacking, XSS, XSRF, and social engineering attacks must be implemented in a local or self-owned website. Uploading self-owned websites online for illustration must be considered with caution and must not cause harm that goes beyond the website itself.
8. Every student was required to sign a pledge that briefly conveyed these instructions. The pledge ensured the students' commitment to, understanding of, and responsibility regarding the instructions.
9. The students were made aware of Saudi Arabia's cyber-crime law via a short presentation and printed handouts. The students also signed a form acknowledging they were aware of the law.

5 Results and Discussion

All 39 participants returned the survey (37 responded in Arabic and two in English). However, the number of responses to several questions varied slightly. Most of the unanswered questions were on the back of the cover page, which seems to have been an oversight due to the survey's double-sided printing style. However, this issue did not affect the results' correctness as we computed the weighted average, and we show the sample size (N) in the tables. When we summarized the results, we combined the terms "strongly agree" and "agree" into the term "agree" and "strongly disagree" and "disagree" into the term "disagree."

5.1 The Effectiveness of Incorporating the Hacking Project

Our results strongly suggest that implementing hacking projects helped students better understand computer and information security principles; 78.38% agreed. Similarly, 78.38% of the students believed that it would be difficult for them to understand security attacks without implementing one. There was consensus that the project helped them discover new areas in information security. Furthermore, the majority recommended the project for future students and found it enjoyable. In addition, 51.29% found implementing an attack was easier than they had expected. Table 1 summarizes the students' responses to the following statements:

- **S#1:** The project implementation helped me in understanding computer and information security principles.
- **S#2:** It will be difficult for me to understand the security attacks without implementing this practically.
- **S#3:** The project helped me to discover new areas in information security that I was not aware of.
- **S#4:** The security attack project is an excellent idea and I recommend it for future students who will take this course.
- **S#5:** Learning security attacks was enjoyable.
- **S#6:** Implementing an attack was easier than I expected.

Table 1. Answers provided for evaluating the project's effectiveness, statements 1–6.

Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
S#1 (N=37)	18 (48.65%)	11 (29.73%)	6 (16.22%)	2 (5.41%)	0 (0.00%)
S#2 (N=37)	15 (40.54%)	14 (37.84%)	4 (10.81%)	4 (10.81%)	0 (0.00%)
S#3 (N=39)	22 (56.41%)	17 (43.59%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
S#4 (N=39)	20 (51.28%)	16 (41.03%)	2 (5.13%)	0 (0.00%)	1 (2.56%)
S#5 (N=39)	24 (61.54%)	11 (28.21%)	3 (7.69%)	0 (0.00%)	1 (2.56%)
S#6 (N=39)	9 (23.08%)	11 (28.21%)	5 (12.82%)	7 (17.95%)	7 (17.95%)

5.2 The Ethical Aspect

In this section of the survey, we asked whether the students intended to misuse the learned skills. Therefore, we asked the following question:

- **S#7:** After I obtained some attack skills, I may use these skills against real systems in a way that cause damage or loss to others (e.g. withdrawing money illegally or stealing passwords).

The answers show that 76.92% of the students disagreed with misusing the learned skills and 10.26% provide neutral answer. In Table 2, the responses are summarized.

Table 2. Answers to statement 7.

Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
S#7 (N=39)	3 (7.69%)	2 (5.13%)	4 (10.26%)	6 (15.38%)	24 (61.54%)

Next, we wanted to know what most influenced the students' decisions not to misuse the learned skills. Was it religion, ethics, lack of incentive, or the law? The following question was asked: **Q#8:** What is the reason that will stop you from attacking real systems to cause damage (if there is more than a reason, please, write the order in the gap based on the reason strength (No. 1 for the strongest reason, then 2 for the less strong, etc.). We provided the following choices for the question:

- **A#1:** Religious reasons (e.g. fearing God)
- **A#2:** Ethical reasons
- **A#3:** The absence of the incentive to make an attack (example of incentives: money, fame, etc.)
- **A#4:** Fearing the law
- **A#5:** Nothing can stop me
- **A#6:** Other, please specify

Generally, causing harm to others is an unacceptable act in any society. However, the reasons that drive people to refrain from causing harm to others diverge. Some people may refrain from doing so due to their own religion, ethics, etc. However, others refrain from harming others only because of an imposed law. A combination of these reasons influence many people but probably with different priorities. For example, an individual might consider religion as a stronger reason than law. Another might consider law a stronger reason followed by ethics.

Islam implies ethics that prohibit acts that cause harm to others by any means, even emotional, such as spying, which is explicitly prohibited in the Quran as stated in chapter 39 verse 12: "And do not spy or backbite each other." Hacking, includes acts that are prohibited in Islam such as stealing others' properties (e.g., passwords, data) or modifying it, spying, etc.; therefore, we expect those who comply with Islamic instructions to refrain from misusing hacking techniques against real systems due to religious reasons.

Does religion equals ethics? This philosophical question is beyond the scope of this paper. However, we must clarify why we distinguished religious reasons from ethics in the answers provided for Q#8 as reasons that will stop subjects from misusing the learned attack skills against real systems in a harmful way. We believe ethics and religion are not the same. We believe that ethics driven by religion are different from ethics that come from civilization or etiquette. To illustrate, they vary in their influence and thus one's commitment to them. As an example, ideally, Muslims believe in Judgment Day on which each person will be strictly judged (rewarded for good deeds and punished for

sins) for every single action during his or her life. They believe in eternal life (after death) that will be based on their actions in this life. These concepts may have stronger effects an individual's decision to refrain from harming others.

All our subjects stated that they studied Islamic religion during their school years and university. However, this does not imply that they are religious or abide by religious principles in their daily lives.

In this question, we allowed more than one answer, but we asked the students to rank their reasons strengths if they have more than a reason. However, a considerable number of participants did not. Therefore, we decided to count the frequency of each choice, and we ranked the most influential reasons by frequency. This question answered by 38 students. The students' answers show that religion was the most influential aspect in the students' decision to not misuse the leaned skills, which was selected by 92.11% of the students. Ethical reasons came next (81.58%), followed by the absence of an incentive to make an attack (57.89%), while fearing the law was selected by 47.37%. We understand the important role that religion plays in Saudi citizens' decisions; however, it might be surprising to find that the law ranked as the fourth reason after lack of incentive. Public attitudes toward the cybercrime law in Saudi Arabia may require further investigation. Table 3 shows the students responses.

Table 3. Summary of answers to Question 8.

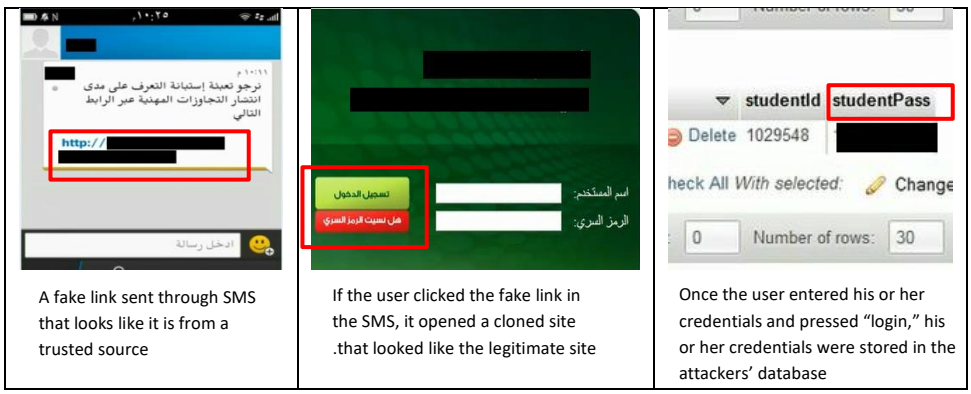
Question	**A#1**	**A#2**	**A#3**	**A#4**	**A#5**	**A#6**
Q#8 (N=38)	35 (92.11%)	31 (81.58%)	22 (57.89%)	18 (47.37%)	1 (2.63%)	2 (5.26%)

Having female-only students, this may have influence on the survey results especially in the ethical aspect (see section 5.2, S#7, and Q#8) and the easiness of performing hacking projects (see section 5.1, S#6). We will investigate the ethical aspect to some extent. We suggest that the low rate of the shown intent to misuse the learned skills by our subjects may have been influenced by the gender (in addition to the aforementioned reasons e.g. religion). This is because many studies suggest that males show higher records in "deviant behavior" than females (Ageton, 1983; Canter, 1982; Lanctôt, N. & Le Blance, 2002) in (Morris R. et al., 2009). However, cybercrimes may have different characteristics than the ordinary ones (Morris R. et al., 2009). Marcum C. et al. (2012) found that females engage in cyber-bullying 2.53 times more than males. On the other hand, Morris R. et al., (2009) found no relation between gender and the willingness in

getting involved in digital piracy. However, we can not build assumption based on the aforementioned studies. This is because the hacking projects in our study have different requirements than the cyber-bullying or digital piracy. For example, performing identity-theft or click-jacking attacks require technical background while the cyber-bullying or cyber-piracy can be done by any ordinary computer/Internet user without technical background. Our hypothesis is that females can show higher rates in the intent to or in getting involved in less technical cybercrimes for certain purposes (such as gossip or emotional harm as shown in (Marcum C. et al., 2012)) and show lower rates in the intent to getting involved in more technical cybercrimes to steal money or passwords for example. However, we are unable to confirm these hypotheses. This aspect can be further investigated but it is out of this study scope.

6 Examples of Students' Work

In this section, we provide examples of students work. The following figures (Fig. 2, Fig. 3, Fig. 4, Fig. 5 and Fig. 6) show some of the students' projects output.



A fake link sent through SMS that looks like it is from a trusted source

If the user clicked the fake link in the SMS, it opened a cloned site .that looked like the legitimate site

Once the user entered his or her credentials and pressed "login," his or her credentials were stored in the attackers' database

Fig. 2. Screenshots of SMS spoofing attack prepared by the social engineering group (Source: Social Engineering Attack: Real Life Example by (Al-Thomali et al., 2013))

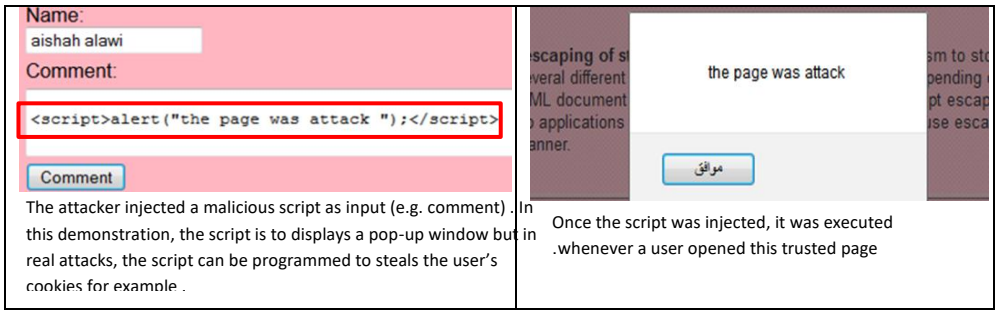


Fig. 3. A screenshot of a simple form of XSS attack (Source: Cross Site Scripting by (Alawi et al., 2013))

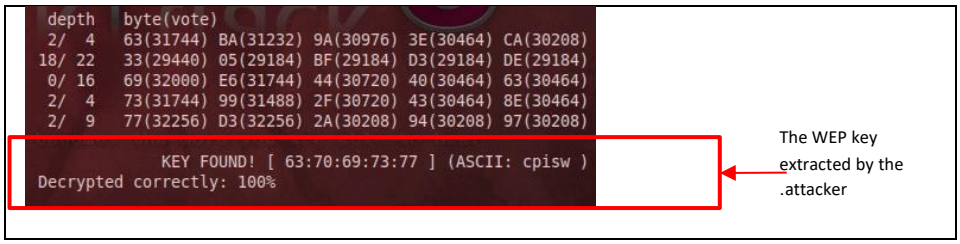


Fig. 4. A screenshot of WEP password cracking (Source: WEP and WPA Wireless Networks Cracking Using backtrack5 by (Alyousif et al., 2013))

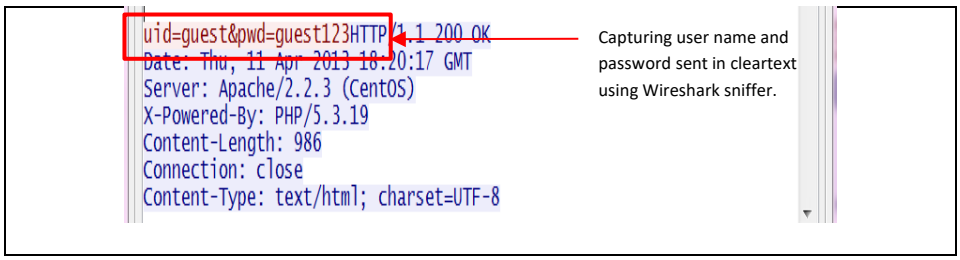


Fig. 5. A screenshot of capturing a victim's sensitive information such as user name and password (Source: Network Sniffing: Real-World Examples by (Algari et al., 2013))

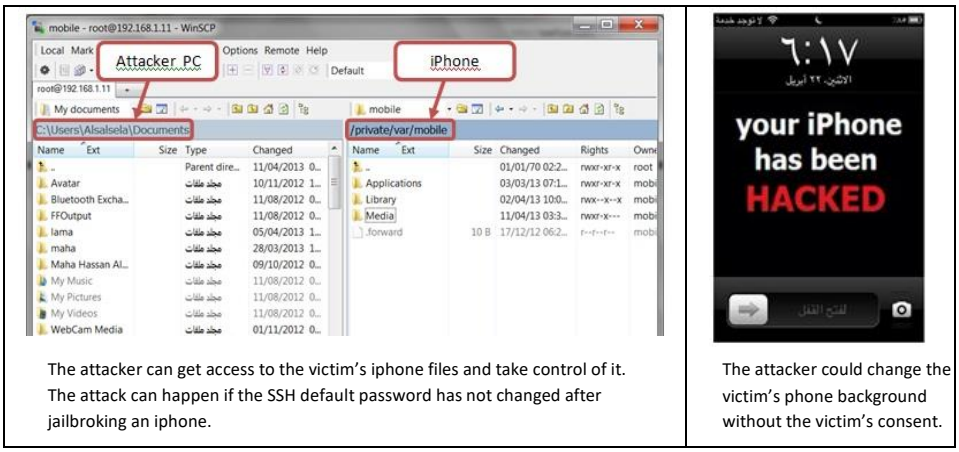


Fig. 6. A screenshot of exploiting a vulnerability in a jailbroken iphone (Source: Smart-Phones Security Risks by (Al-Zahrani et al. (2013)). The attack originally found by a Dutch hacker (see: (Foresman, 2009))

7 Conclusion and Future Work

Our results suggest that incorporating hacking projects in information security education helped students better understand computer and information security concepts. The project also helped students discover new areas in information security. Interestingly, all our subjects involved in the study were female, and the results strongly suggest that they found the project implementation enjoyable. The majority of the students said they did not intend to misuse the learned skills, mainly due to religious reasons. Fearing the law ranked the fourth reason that will stop the students from misusing the learned skills.

We made an attempt to raise awareness of real-life examples of security attacks at a college event, "IT Open Day", at which four groups voluntarily presented their posters.

The main challenge in implementing this work was performing hacking projects safely. We stress the importance of carefully taking precautions and informing students about the legal consequences to avoid any issues. It is important to follow up how the students are implementing their project to make sure they did not cross the line. We overcame ethical concerns and problems that may result from allowing students to implement such a project by taking several precautions.

In the future, we want to work on solutions that provide a safer environment and give students more freedom in learning and practicing. The use of specialized tools designed

for security training such as “Hackademic” in some projects (e.g. web/Internet security) may worth testing and considering in future work.

8 References

Ageton, S. (1983). The dynamics of female delinquency, 1976–1980. Criminology, 21, 555–584.

Al-Thomali, B., Al-Harbi, S., AL-ZahraniS (2012). Social Engineering Attack: Real Life Example. King Abdulaziz University (KAU); ‘Unpublished’

Al-Zahrani , M., Al-Harthi , M., Mutahar G. (2012). Mobile Phone Security Risk. King Abdulaziz University (KAU); ‘Unpublished’

Alarifi, A., Tootell, H., Hyland P. (2012). A study of information security awareness and practices in Saudi Arabia. In Proceedings of the 2012 International Conference on Communications and Information Technology (ICCIT), pp. 6-12.

Alawi, A., Badgale, N., Al-subhi, R. Cross Site Scripting (2012). King Abdulaziz University (KAU); ‘Unpublished’

Algari, R., Al-Harthy, S., and Al-malki, T. (2012). Network Sniffing: Real-World Examples. King Abdulaziz University (KAU); ‘Unpublished’

Alghathbar, K., Mahmud, M., Ullah, H. (2008). Most known vulnerabilities in Saudi Arabian web servers, in Proceedings of the 4th IEEE/IFIP International Conference on Internet ICI 2008, pp. 1-5

Alyousif M., A.M., Basaffar N., Alselmi A., Aljuhani G. WEP and WPA Wireless Networks Cracking Using backtrack5 (2012). King Abdulaziz University (KAU); ‘Unpublished’

Alzamil, Z. (2012). Information Security Awareness at Saudi Arabians’ Organizations: An Information Technology Employee’s Perspective. International Journal of Information Security and Privacy, 6 (3): 38–55

Bishop, M. (2002). Education in information security. IEEE Concurrency, 8 (4): 4-8

Canter, R.J. (1982). Sex differences in self-reported delinquency. *Criminology, 20*, 373–393.

Courtois N. (2011). Computer Security I Course, University College London (UCL); ‘Unpublished’

Courtois N., (2011). UCL Smart Cards and RFID Security Lab. Retrieved Jan 11 2014 from

University College London (UCL) Web site: http://www0.cs.ucl.ac.uk/staff/n.courtois/sclab.html

Desmedt, Y. (2012). Computer Security II Project. University College London (UCL); ‘Unpublished’

Du W. (2011). SEED: Hands-On Lab Exercises for Computer Security Education IEEE Security & Privacy, 9:(5) 70-73

Facuty of Computing & Infromation Technology (2013). Information System Bachelor's Core Courses. Retrieved Jan 12 2014 from King Abdulaziz University (KAU) Web site: http://computing.kau.edu.sa/pages-is41e.aspx

Forbes (2012). The World's 25 Biggest Oil Companies. Retrieved Jan 26 2013 from Forbes Web site: http://www.forbes.com/pictures/mef45ikjd/not-just-the-usual-suspects-12/

Foresman C. (2009). Dutch hacker holds jailbroken iPhones "hostage" for €5 (Updated). Retrieved Sep. 07 2013 from arstechnica Web site: http://arstechnica.com/apple/2009/11/dutch-hacker-holds-jailbroken-iphones-hostage-for-5

Frincke, D. (2003). Who watches the security educators?. IEEE Security & Privacy, 1 (3): 56-58

Giotsas, V. (2011). Computer Security I Lab Sessions. University College London (UCL); 'Unpublished'

Goldberg I. (2001). The Insecurity of 802.11. Black Hat Briefings. Retrieved Jan. 10 2014 from cypherchunks Web site: http://www.cypherpunks.ca/bh2001/mgp00001.html

Google (2012). Our Mobile Planet: Saudi Arabia. Retrieved Nov. 30 2013 from Google Web site: http://www.google.com/think/research-studies/our-mobile-planet saudi-arabia.html

Hannah, A. (2011). Linux Journal. Packet Sniffing Basics. Retrieved Jan. 09 2014 from linuxjournal Web site: http://www.linuxjournal.com/content/packet-sniffing-basics?page=0,0

Huang L., M.A., Wang H., Schechter S., and Jackson C. (2012). Clickjacking: Attacks and Defenses. In Proceedings of the 21st USENIX conference on Security symposium (Security'12), pp. 22-22

IEEE Women in Engineering (2014), IEEE. Retrieved April 12 2014 from IEEE website: http://www.ieee.org/membership_services/membership/women/index.html

Internet World Stats (2013). Saudi Arabia Internet Usage and Telecommunications Report. Retrieved Nov 30 2013 from internetworldstats Web site: http://www.internetworldstats.com/me/sa.htm

Lanctôt, N., & Le Blanc, M. (2002). Explaining deviance by adolescent females. Crime and Justice,

29, 113–202.

Marcum C., Higgins G., Freiburger, T. and Ricketts, T. (2012). Battle of the sexes: An examination of male and female cyber bullying. International Journal of Cyber Criminology (IJCC), 6 (1): 904–911

McDermott J. (2007). Social Engineering - The Weakest Link in Information Security. Retrieved Sep 07 2013 from WindowsSecurity.com Web site: http://www.windowsecurity.com/whitepapers/Network_Security/Social-Engineering-The-Weakest-Link.html

Ministry of Finance (MOF) (2013). Budget. Retrieved Dec. 01 2013 from MOF site: http://www.mof.gov.sa/english/DownloadsCenter/Pages/Budget.aspx

Mink, M., Greifeneder, R. (2010). Evaluation of the Offensive Approach in Information Security Education, in: Rannenberg, K., Varadharajan, V., Weber, C. (ed.) Security and Privacy – Silver Linings in the Cloud, Berlin Heidelberg: Springer; vol. 330, p. 203-214

Moaddel, M.(2006). THE SAUDI PUBLIC SPEAKS: RELIGION, GENDER, AND POLITICS. International Journal of Middle East Studies, 38 (1), 79-108

Morris, R., Johnson, M. and Higgins, G. (2009). The role of gender in predicting the willingness to engage in digital piracy among college students. Criminal Justice Studies: A Critical Journal of Crime, Law and Society, 22 (4), 393-404

Murphy C. (2013). The World Today 2013, Saudi Arabia Cyber-savvy youth on the rise. Retrieved Jul. 25 2013 from Chathamhouse Web site: http://www.chathamhouse.org/sites/default/files/public/The%20World%20Today/2013/AprilMay/WT0213Geopol.pdf

OWASP (2013). Clickjacking. Retrieved Jun. 27 2013 from OWASP Web site: https://www.owasp.org/index.php/Clickjacking

OWASP (2013). Cross-Site Request Forgery (CSRF). Retrieved Jan. 12 2014 from OWASP Web site: https://www.owasp.org/index.php/Cross-Site_Request_Forgery_%28CSRF%29

OWASP (2013). Cross-site Scripting (XSS). Retrieved Sep. 06 2013 from OWASP Web site: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

OWASP (2013). Hackademic Challenges Project. Retrieved Nov. 30 2013 from OWASP Web site: https://www.owasp.org/index.php/OWASP_Hackademic_Challenges_Project

OWASP (2013). SQL Injection. Retrieved Sep 06 2013 from OWASP Web site: https://www.owasp.org/index.php/SQL_Injection

Papanikolaou, A., Karakoidas, V., Vlachos, V., Venieris, A., Ilioudis, C., Zouganelis, G. (2011). A Hacker's Perspective on Educating Future Security Experts. In Proceedings of the 15th Panhellenic Conference on Informatics (PCI), pp. 68–72

Reuters (2012). UPDATE 1-Saudi Aramco says most damage from computer attack fixed. Retrieved Jun. 26 2013 from Reuters Web site: http://in.reuters.com/article/2012/08/26/saudi-aramco-hacking-idINL5E8JQ6PV20120826

Schneier, B. (2008). The Security Mindset. Retrieved Apr. 03 2014 from Schneier on Security Web site: https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html

Saudi Aramco (2012). Ministry of Interior discuss cyber-attack. Retrieved Jul. 26 2013 from Saudi Aramco Web site: http://www.saudiaramco.com/en/home/news/latest-news/2012/cyber-attack-press-conference.html

Saudi Press Agency (2013). Officials in the national center for cyber security: The ministry of interior website went down temporally due to external attacks and is backed up now (Arabic). Retrieved Dec. 02 2013 from SPA Web site: http://www.spa.gov.sa/readsinglenews.php?id=1111215&content_id=

Securelist (2010). Information Security Threats in the First Quarter of 2010. Retrieved Jun. 25 2013 from securelist Web site: http://www.securelist.com/en/analysis/204792120/Information_Security_Threats_in_the_First_Quarter_of_2010

Trabelsi, Z. and Ibrahim, W. (2013). Teaching ethical hacking in information security curriculum: A case study. In Proceedings of the 2013 IEEE Global Engineering Education Conference (EDUCON), pp. 130-137

United States Census Bureau (2013). Country Rankings. Retrieved Nov. 30 2013 from US Census Web site: http://www.census.gov/population/international/data/countryrank/rank.php

9 Appendix A

Brief descriptions of the proposed hacking projects topics are provided as follows:

9.1 Click-Jacking

A Click-Jacking attack uses multiple transparent layers to trick a user into clicking a link or a button other than what he or she sees (OWASP, 2013b). For example, the attacker places a Facebook “like” or a Twitter “follow” button on top of a different link such as “Click here for a free iPod” (OWASP, 2013b). The attacker hides the top button (the “like” button) by changing the opacity to make it invisible (OWASP, 2013b). When the user clicks the link that he or she sees (e.g., “Click here for a free iPod”), in fact, he or she clicks on the hidden button or link on the top layer (OWASP, 2013b). Click-jacking can also result in taking control of a user’s webcam, stealing a user’s private data, and compromising a user’s web surfing anonymity as shown in (Huang, 2012).

9.2 Cross-Site Scripting

A Cross-Site Scripting (XSS) attack is performed by injecting a malicious script in web applications (OWASP, 2013c). In this attack, the attacker can send malicious script through a web application to other users who trust the application (OWASP, 2013c). This can occur in web applications that generate output from the input without validation (OWASP, 2013c). For example, an attacker injects a malicious script in a link in a blog comment. The malicious script can be programmed to hijack the user’s session and steal his or her credentials stored in the cookies upon execution. When the victim user who

trusts the blog clicks the malicious link (which normally looks like an innocent link), the script is executed at the user's end, and the user's credentials are compromised.

9.3 Cross-Site Request Forgery

A Cross-Site Request Forgery (CSRF) attack works by tricking the user (through social engineering, for example) into opening a malicious page that loads a malicious code (OWASP, 2013d). Once executed, the code performs undesired requests on the user's behalf on a trusted website on which the legitimate user is currently authenticated (OWASP, 2013d). For example, the attacker transfers money if the user was logged in to his or her bank website.

9.4 SQL Injection

SQL injections occur in applications that contain SQL database(s) (OWASP, 2013e). The attack works when an attacker injects a specially crafted SQL statement in an incorrectly filtered user input field (OWASP, 2013e). The attacker can then read and modify data from the database or take administrative privileges on the database (OWASP, 2013e).

9.5 Smartphone Security Risks

Several attacks target smartphones. For example, in 2009, a Dutch hacker found vulnerability in jailbroken iPhones (Foresman, 2009). This vulnerability enables the SSH with the default root password. The attack can exploit the unchanged default root password, allowing the hacker to take control of the device and transfer or modify the user's private files (Foresman, 2009).

9.6 Network Sniffing

Network Sniffing is the process of capturing data while it is being transferred over a network (Hannah, 2011). The risk comes when a system transfers sensitive data in plain text. For example, if an attacker places a sniffer in an insecure network, he or she can steal users' credentials if they are sent in clear text (Hannah, 2011). Another type of attack that can be performed using sniffing tools is session hijacking (Hannah, 2011). In this attack, the attacker steals the user's session cookies for a certain website in which the

user is currently logged (Hannah, 2011). After capturing the cookies, the attacker can inject the cookies' values in his or her browser and open the user's URL. These attacks give the attacker control over the victims' session or credentials.

9.7 Social Engineering

In social engineering attacks, the attacker tricks users to reveal sensitive information such as their credentials by using social skills (McDermott, 2007). For example, the attacker may send an email or SMS that appears to be from a legitimate site such as a bank or a reputable organization asking the user to update his or her information through a fake link that appears to belong to the original site but in fact is a fake site that belongs to the attacker. When the user responds to the fake link, the attacker is provided with the user's credentials, and thus full control of the user's online operations (e.g., online money transfers).

9.8 Cracking Wireless Networks

Some wireless networks security protocols such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) have weaknesses. For example, WEP uses the RC4 stream cipher algorithm incorrectly (Goldberg, 2001). In stream ciphers, the key stream should not be repeated to avoid the "Two-time pad" (Goldberg, 2001). In WEP, the key stream consists of a fixed shared key and Initialization Vector (IV) (Goldberg, 2001). Hence, the key stream depends on the 24-bit IV only (Goldberg, 2001). Due to the small size of the IV, the key will be repeated after maximum 2^{24} or 16 million packets (Goldberg, 2001). Therefore, by analyzing some amount of traffic, an attacker can easily find the WEP key. Many freely available tools can perform different types of WEP and WPA attacks.