IJCSI International Journal of Computer Science Issues, Volume 13, Issue 6, November 2016
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org https://doi.org/10.20943/01201606.129135

Information Security Issues and Threats in Saudi Arabia: A Research Survey

Ahmed Alzahrani[1], and Khalid Alomar[2]

[1] Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University Jeddah, 21589, Saudi Arabia

[2] Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University Jeddah, 21589, Saudi Arabia

Abstract

The purpose of this paper is to examine the information security awareness (ISA) among undergraduate students in Saudi Arabia, using online survey. The survey attracted 2325 respondents 828 male, and 1,497 female. The results reveal that the most significant information security awareness problems are found to lie in the areas of "Cloud storage security awareness," "Social networking security awareness" and "Wireless network security awareness." This paper contributes to the literature by identifying key findings and recommendations regarding information security attitudes, behaviors, and tools used by students along with suggestions for improving information security awareness at institutions of higher education. In this paper, we will show the need for security education, training, and awareness programs in universities in the Middle East by presenting results of various information security issues and threats in Kingdom of Saudi Arabia among students.

Keywords: *Information Security, Information Security awareness, Cloud storage, Social networks.*

1. Introduction

The number of Internet users in Saudi Arabia continues to rise rapidly, reaching about 22.4 million for the end of second quarter of 2016, with a population penetration of 70.4 % [1]. Besides, the total number of mobile broadband subscriptions continued to increase and reached around 26.6 million by the end of the second quarter of 2016, representing a population penetration rate of 83.5 %. This growth has attracted different sectors such as government, health, and education to provide their services online. On the other hand, it permits abusers to use new techniques to misuse or destroy information [2].

To overcome these threats, it is essential to have good information security practices, and must be an appropriate level of Information Security Awareness (ISA). ISA has become one of the strongest lines of defense against information threats; it has been confirmed that a high-level of ISA can reduce users' errors, and maximize the efficiency of security techniques and procedures [3].

2. Cyber-attacks in Saudi Arabia

Cyber-attacks is growing in Saudi Arabia due to the rise in digital devices (computers, tablets, and smartphones), lack of information security awareness among Internet users terrorism, politics, and an increase of cyber-crime groups. Although, Saudi organizations are continuing management challenge to protect computer systems and their information against cyber-crimes [4]. However, Kaspersky Lab reported that the highest numbers of web threat incidents were found in Saudi Arabia and some other countries [5]. For instance, a joint study of information security of businesses conducted by Kaspersky Lab and B2B International in 2015 among over 5,500 IT specialists from 26 countries around the world, including Saudi Arabia. They found that 40% of companies in the Kingdom of Saudi Arabia have been affected by internal information security incidents, and the largest single cause of confidential data losses are employees [6]. Media sometimes report incidents of online fraud, attempts to hack social network accounts and websites being shut down or deface. For example, In October 2012, Saudi Arabian Oil Company computer network was compromised, and the virus was inserted into the network via a USB flash drive [7]. The attack destroyed data and erased hard drives of computers. Moreover, in 2015, Kaspersky Lab has discovered Desert Falcons which are Arabic cyber espionage targeting Middle East countries and the primary focus of its activity performs to be in Saudi Arabia. They used a phishing attack via e-mails and social networks to send the malicious payload. Kaspersky

Lab experts found more than 3,000 victims in 50 plus countries, with more than one million files stolen [8].

Furthermore, The Official Website of King Saud University (KSU) got hacked by some unknown hacker. A Database of 812 Users hacked and dumped on the Internet [9]. To decrease the risks of both Human malicious and human non-malicious threats, it is needed to increase the level of ISA within the organization or to the general public. In the organizations, Information security policies and procedures should be clearly classified and regularly tested for integrity; thereby the general public also will be aware of information security threats. Overall, there is a lack of academic and professional literature about (ISA) in Saudi Arabia. One study has been conducted the level or causes of ISA among the Saudi general public [3]. In the previous study, 462 participants are in two groups: information security issues, and preferences for information dissemination. It has confirmed that ISA in Saudi Arabia is low due to highly-censored, patriarchal and tribal nature of Saudi culture. Another study focuses on analyzing the state of the information security awareness at some of the Saudi's organizations. The results of that study show that most of the information technology employees at the surveyed organizations have some misconceptions about information security practices and not aware of the internal information security threats. The authors recommended that organizations need to consider the information security awareness programs within their public relations and training programs [10]. It is [10] focused only on organizations security awareness, ignored the general public and did not study the level of ISA in Saudi Arabia. The first goal of this paper, we will examine the level of ISA in Saudi Arabia based on the following security threats and issues that some do not cover in the previous study [3] such as wireless network security awareness, social networking security awareness and cloud storage security awareness.

3. Methodology

This study seeks to gather and analyze data from a sample of the Saudis to examine the level of (ISA). The survey questions type was semi-closed ended, hence bring together the benefits of closed-ended and open-ended questions. The survey is in the Arabic language because the participants are all from Saudi Arabia. The study was subjected to pilot testing by 50 participants. Pilot test participants believed that asking Saudis irrelevant questions will result in giving random answers or getting frustrated and close the survey. So, pilot test participants strongly recommended making all questions optional and use skip logic which is automatically sent respondents to a future question based on the answer choice they choose in the survey. Survey was used to upload all survey questions and the survey link distributed to social media, popular Saudi educational and business websites. The total number of responses in this study was 2325 from students, employed and unemployed. The responses were from different education level and different age rate.

4. Results

Because of skip logic function and also questions were optional, the number of responses for each question was different. In addition, we found that the rate of non-response was around 25%. However, there were still over 1700 respondents for every question. Responses are in five awareness sections: general information security issues, password security, wireless network security, social networking security and cloud storage security.

4.1 General information security issues

Figure 1 shows that 91.68% of respondents never received any awareness training courses. Only 8.32% of respondents attended some courses like digital crimes, IT security system and introduction to cyber security. So, there is a lack of security awareness training in Saudi, and this is a major security risk.

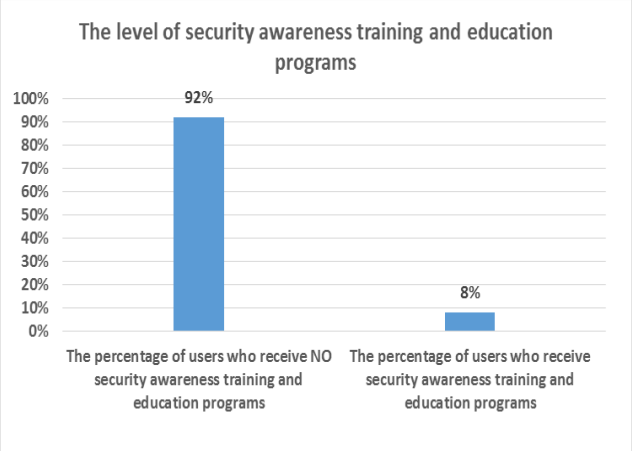

Figure 1: The level of security awareness training and education programs.

Table 1 shows the respondent's responses to the question," which type of protection software they used?" 74.59% of participants use only antivirus software. Nevertheless, most Saudis are not aware of other possible threats. Only 12.32% of respondents use anti-phishing software, 11.87% use anti-spam, and 16.58% of Saudis respondents have no knowledge about protection software at all. Thus, this may cause malware, Spyware, and hacking. Another question

was asked, what is the source of protection software they use? 86.97% of respondents use software's official website, but 14.60% of respondents uses different sources to download illegal protection software. Downloading from a non-trustworthy source means downloading malware, tracking, Trojans, cross-site scripting (XSS), and viruses that damage the computers and steal user privacy.

Table 1: Protection software

What type of protection software you used?(N= 1972)	
Anti-Virus	74.59% (1471)
Phishing-Anti	12.32% (243)
Firewall	41.28% (814)
Spam-Anti	11.87% (234)
Spyware-Anti	18.86% (372)
I do not know	16.58% (327)

One of the major properties of software updates is the security patch upgrades. Users must keep the protection software up to date to control threats like viruses or Trojans. An attacker can use the old version of protection software vulnerabilities to steal sensitive user data and banking account info. So users need to know that, it is not enough to install protection software to protect their devices without keep it up to date.

Table 2 shows that 59.28% of respondents use automatic updates. 7.61% of respondents update annually and 18.51% do not even update the protection software. Therefore, this shows that, the little awareness of the need of updates software. The last question was if respondents use Virtual Private Network (VPN) to encrypt the internet connection. Only 21.04% of respondents use the VPN connection. Unfortunately, only 43.51% of respondents have no knowledge about VPN and 35.45% do not use it. Indeed, most Saudis use free access points which are available at restaurants, hotels or airports. An attacker can position himself between the user and the connection point. Accordingly, attackers can get access to important user emails, credit card information or even distribute malware. So there is a surprising lack of care for the use of VPN.

Table 2: Protection software update

How often do you update the protection software? (T=1972)		
	Count (T)	Percentage
Automatically	1,169	59.28%
Weekly	96	4.87%
Monthly	192	9.74%
Annually	150	7.61%
Never	365	18.51%

4.2 Password security issues

A password is a secret series of letters, numbers, and symbols that enable a user to access a file, computer, or program. However, passwords are no longer considered to be a strong defense against hackers or vandals [11]. Usually, users create weak passwords that compromise security due to human memory. Users cannot memorize long and complex passwords and cannot remember passwords for diff erent accounts. Indeed, there are several types of attacks that can be used to detect a password. This section will outline some of the password issues in Saudi Arabia, such as using the same password for all accounts, sharing passwords with others and choosing a secure password. Participants were asked if they use the same password for all accounts. The study found that 40% of respondents use the same password. When users use the same password for their email, bank account, or credit cards and once it has been compromised, the hackers will be able to gain access to other accounts and steal user information. In contrast, 60% of respondents do not use the same password for all accounts, but that does not mean Saudis are aware enough. They need to learn more about password awareness to avoid hacker attacks. Another question was if respondents share the password with others. Of 2325 Saudi respondents, 9% of respondents indicated that they share their password with others and 38% share their password in case of need. The sum of these two percentages is 47 %. So, users still need more to be educated in this part. In fact, sharing passwords with others let information to be easily compromised. In contrast, 53% of respondents do not share their password. 56.11% of respondents indicated that they use a mix of alphabetic, numeric characters, upper/ lower case, and symbols to create a secure password. 24.87% of respondents use their personal information that can be easily guessed like birthdays, telephone number or names of family members to create the password.

This information can be found easily on social networking websites or by social engineering. 6.11% of respondents use the different method to create the password like car

plate number, perfume name, student ID odd or even numbers and 9.06% of participants use only numbers. Thus, Hackers can use free tools and special techniques for guessing or cracking passwords. As a result, Saudis are still unaware of the value of strong passwords. However, having a secure password is not enough to protect users' information from unauthorized access.

Table 3 shows the respondent's responses to the question,"How often do you change your passwords?" Passwords should regularly be changed to prevent users from sharing passwords with others. Unfortunately, 51.29% of respondents have never changed their passwords. Consequently, this is the main security risk for Saudi Arabia. The another question was asked if respondents use login passwords to secure their devices. The study found that 58.78% of respondents used passwords to login into their devices but 41.22% do not. Lack of login password awareness may cause DoS attacks. The last question was asked if respondents save their password on a browser. 34.52% of respondents save their password on the browser. Thus, users who have access to the computer can log into accounts and take the passwords. Also, some viruses and malware can steal user's passwords or banking information. In contrast, 65.48% of respondents do not save their password in a browser.

Table 3: Password Change.

How often do you change your password? (T=1903)		
Response	Count (T)	Percentage
Never	976	51.29%
More than a year	310	16.29%
Annually	183	9.62%
Every six month	155	8.15%
Every three month	144	7.57%
Monthly	100	5.25%
weekly	35	1.84%

4.3 Wireless Network Security issues

The wireless access point is configured with factory default settings. In most cases, users don't read the access point manual or do not even know about it, to change the default login username and password. In this section, the first question asked if respondents changed the default password of the administrator account, which gives access to the access point management software. Only 40.23% of 2325 respondents indicated that they change the default password. A further 59.77% of respondents never change the default username and password. As a result, default login can be easily guessed and give an attacker access to the wireless access point to change all settings including the wireless password. So, there is a surprising lack of care for access point factory default settings. The second question asked if respondents use wireless encryption. The study found that 13.43% of respondents used WEP encryption method which makes easy for the attacker to break the encryption key with freely available tools and 41.43% do not use encryption. The sum of these two percentages is 54.86%. Hence, this shows the lack of awareness among some users and an attacker can easily steal the user's critical data, such as private files, emails, and bank account information. In addition, an attacker can use the access point to hide the identity to perform attacks against others or downloaded copyrighted content. On the other hand, only 45.14% of respondents use WPA/WPA2. The third question asked if respondents keep the wireless device firmware up to date. Periodically, the manufacturer provides the latest firmware version for their products on their website. The study found that only 31.89% of 2325 respondents keep the wireless device firmware up to date. Indeed, the main benefits of updating wireless device firmware are patch security holes and increase the device performance. In contrast, 38.57% of respondents do not upgrade the firmware, and 29.54% have no knowledge about firmware. So there is a lack of care for wireless device firmware. Consequently, this makes them more likely to firmware attacks.

4.4 Social networking security issues

Figure 2 shows that, in 2015, WhatsApp and Facebook are the most popular social networks in Saudi with 27, 25 percent penetration rate, respectively, 35 percent of the total population were active social media users. Despite the fact, social networks allow users to keep in touch with friends and family; there are security issues to be disturbed about. The first question asked if respondents share their personal details like mobile number, email address, birthday or home address on social networks. The study found that 28.08% of 1.638 respondents share their personal information which others might use for nefarious purposes. Nevertheless, 71.92% of respondents do not share their information. Social networking creates a risk of sharing information that will be damaging to the user himself. Sharing personal information online provides criminals with clues to guess user passwords. Thus, Saudi still needs more training to avoid sharing their personal details in social networks and change their behavior to get them to think securely before posting. Also, the respondents asked if they change the social networking privacy. 66.91% of 1600 respondents changed the privacy settings, and 33.09% do not change. Thus, Saudi still needs more awareness to understand how to use the privacy features to avoid identity theft. Also, the study found that 51.04% of 1681 respondents do not trust third party

applications in social networks. While 10.56% of 173 respondents do trust third party applications and 38.40% of respondents, do not use it. Some Companies are using quiz applications on social network sites to access user information like addresses and phone numbers. The databases of these applications will rise and become targets for hackers. Indeed, more use of third applications equals to larger security risk. Other questions asked if respondents use identity verification to protect their accounts. Amazingly, 67.58% of respondents use the verification code for better protection against phishing with user password and phone. The main advantage of using the identity verification method is that a higher level of security is added to user accounts. On the other hand, 11.05% of respondents have no knowledge about the identity verification method and 21.37% of respondents never use it. Last questions asked if respondents check the link before clicking on social networks. 50.92% of 1638 respondents check the links, to protect their accounts from spams, phishing or malicious content. However, 49.08% of respondents never pay any attention to the links in social networks. As a result, social network users in Saudi could be in danger of identity theft. Most social media are carrying malware threats which are links to videos or pictures, once the user clicks on them will take him to a malicious website.

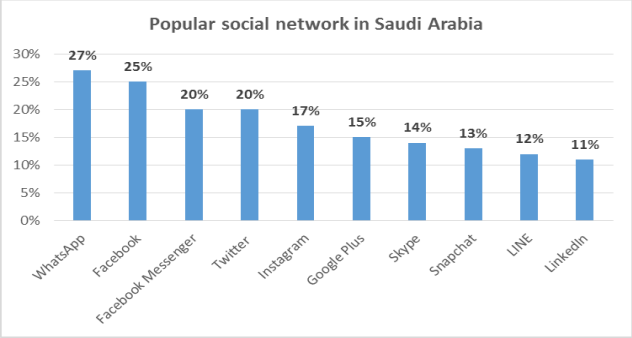

Figure 2: Popular social networks in Saudi Arabia as of 4th quarter 2015.

4.5 Cloud storage security issues

This study found that 50.40% of 1633 respondents use cloud storage to store their documents and photos. However, they do not ensure that the company has a good reputation and solid security policies. For instance, where will the data be stored and how is it protected, technically or physically to prevent unauthorized entry. Saudis just trust the cloud storage company to store their cloud data. 49.60% of respondents never use cloud storage and have no knowledge about online storage. Furthermore, we found that 97.99% of 798 respondents do not encrypt their files that stored online. Also, Saudi user does not care about reading the terms of service to make sure that, data encrypted when stored in the cloud. On the other hand, only 2.01% of respondents use two applications to encrypt and decrypt the files that are BoxCryptor and TrueCrypt. The user can use encryption tools to protect the privacy of the data that stored online. So, the files remain safe even if hackers manage to steal user passwords. Also, the study found that amazingly 61.56% of 492 respondents backup their cloud data while 33.35% do not. Users should back up their cloud data regularly to prevent against data loss. Cloud file sharing provides end users with the ability to access files from any location. We found that 80.83% of 798 respondents do not share their files online. However, 19.17 % of respondents share their files with friends and colleagues. Cloud file sharing methodology including privacy and security are showed in Table 4. The user should set a password for shared files to ensure that only collaborators with the password can access shared files. However, only 40.27% set a password to access shared files. As a result, cloud storage account could be at risk and password can be exposed by malware or phishing. Also, 65.10% of respondents know that how to set shared files permissions (Read/Write/Delete) to avoid losing them. As a result, File owner can set up shared permission-based folders around members needs and allow them to access that file from anywhere securely. Furthermore, only 27.52% of 41 respondents know that if the service provider has access to data. Saudis are still ignoring the security policies and privacy about the service providers. 18.12% of 27 respondents give access control to members to invite anyone. Thus, the user account will be hacked, and data will be lost. Also, only 39.60% of respondents know that how to unshare a shared file at any time and ensure that editors or viewers in that file do not have the ability to unshare it. So, the file will be permanently deleted from member accounts, and it can't be recovered.

Table 4: Files sharing methodology on the cloud

User methodology for sharing files on the cloud (T=149)		
	Percentage	Count (c)
Set password to access shared files.	40.27%	60
Users know files permissions concepts.	65.10%	97
Users know that if service providers have access to cloud data.	27.52%	41
Users who have access to shared file can give access to anyone.	18.12%	27
The user knows that how to cancel access for any user.	39.60%	59
The user can determine who change or delete shared files.	35.57%	53

5. The overall level of Information Security Awareness

Figure 4 shows the overall level of ISA in Saudi for each section in this study. The percentage of general information security awareness is 35% due to lack of security awareness training. While cloud services market is growing rapidly, the level of cloud storage security awareness is (44%). However, to reduce the incidence and severity of cyber security threats, we suggested security awareness training and education guidelines that will help to increase the level of ISA among users in Saudi Arabia.

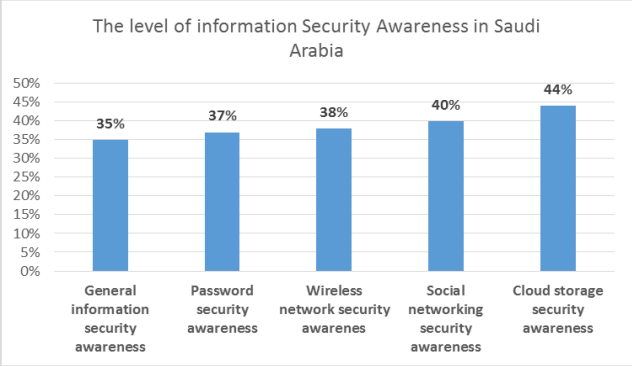

Figure 3: The overall level of information security awareness in Saudi.

6. Security Awareness training and education guidelines

As hackers or vandals are constantly identifying new methods of attack, security awareness training is the best method to defense against security threats. Indeed, an uneducated or poorly trained user increases the risk of loss and disclosure of vital data. However, security awareness training is not a simple task to be achieved. In this section, we have involved seven groups to help increase the security awareness among users in Saudi Arabia. We suggest some of the recommendations below:

- Schools and universities should provide students, staff, and employees with the knowledge and tools needed to protect them from cyber threats; thereby schools and universities data will be protected too. They should offer security awareness campaigns such as seminar, lectures and integrate information security awareness topics into their computer courses. Moreover, they should provide web-based training for better understanding and utilize security best practices.
- In 2007, the anti-cyber-crime law was issued in Saudi Arabia [12], universities should educate their students about the new anti-cyber-crime law.
- Universities should provide security awareness program that includes web-based training, onsite or both. The training should include the importance of information security, user responsibilities, threats, vulnerabilities, mobile device security, could computing security awareness and social media awareness. Also, they should include awareness campaign such as, posters, short animated videos and emailing both of information security threats news and security best practices to users. Assessments conducted to measure the level of security awareness among the employees- clients, security awareness campaign and training, incident investigations, evaluations and independent evaluations of a company's IT infrastructure.
- Universities need to develop awareness campaign in collaboration with all government sectors, and popular media to increase awareness and education of information security risks, threats, vulnerabilities and responsibilities of information protection. This could be online or onsite training or a combination of both.
- There are many resources that can help user for independent information security awareness training by reading books, newspaper or websites. As new information security threats appear continuously, the reading should be done regularly.

7 Conclusion

The purpose of the current study was to highlight the security issues and threats in Saudi Arabia. The most obvious finding to emerge from this study is that there is a lack of awareness of basic information security among Saudi students. The second significant finding was that with respect to training and awareness surprisingly the score was very low (92% have never taken any type of security training). The results of this study suggest that Saudi universities should educate their students about the anti-cyber-crime law, along with three significant information security awareness problems found in this study. Considerably more work will need to be done to determine how knowledge levels can be improved among students by adopting suitable awareness enhancing programs. Further research might determine how the problem areas identified in this study can be approved through best practices.

References

[1] M. o. C. a. I. Technology. (2015, 3/1/2016). 21 million Internet users in Saudi. Available: http://www.mcit.gov.sa/En/aboutmcit/sectordevelopment/pages/sectorindices.aspx
[2] R. Bragg, M. Rhodes-Ousley, and K. Strassberg, Network security: the complete reference: McGraw-Hill/Osborne New York, 2004.
[3] A. Alarifi, H. Tootell, and P. Hyland, "A study of information security awareness and practices in Saudi Arabia," in Communications and Information Technology (ICCIT), 2012 International Conference on, 2012, pp. 6-12.
[4] B. M. E. Elnaim, "Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future," in Information and Knowledge Management, 2013, pp. 14-19.
[5] T. C. MEA. (2015, 25/1/2016). Highest numbers of web threat incidents reported in Qatar, UAE, Turkey and Saudi Arabia. Available: http://techchannelmea.com/security/highest-numbers-web-threat-incidents-reported-qatar-uae-turkey-and-saudi-arabia
[6] K. Lab. (2016, 15/1/2016). 40% of Companies in the Kingdom of Saudi Arabia Affected By Internal Information Security Incidents. Available: http://me.kaspersky.com/en/about/news/virus/2016/Forty-per-cent-of-Companies-in-the-Kingdom-of-Saudi-Arabia-Affected-By-Internal-Information-Security-Incidents
[7] K. Lab. (2012, 25/1/2016). Code in Aramco Cyber Attack Indicates Lone Perpetrator. Available: http://usa.kaspersky.com/about-us/press-center/in-the-news/code-aramco-cyber-attack-indicates-lone-perpetrator
[8] K. Lab. (2015, 3/2/2016). Hunting Desert Falcons –the First Known Arabic Cyber Espionage Group Attacking Thousands of Victims Globally. Available: http://www.kaspersky.com/about/news/virus/2015/hunting-desert-falcons
[9] M. Kumar, "Saudi Arabia's King Saud University Database Hacked," ed: The Hacker News, 2012.
[10] Z. A. Alzamil, "Information Security Awareness at Saudi Arabians' Organizations: An Information Technology Employee's Perspective," International Journal of Information Security and Privacy (IJISP), vol. 6, pp. 38-55, 2012.
[11] M. Ciampa, Security Awareness: Applying Practical Security in Your World: Cengage Learning, 2013.
[12] C. a. I. T. Commission, "Anti-Cyber Crime Law," ed, 2007.

First Author Obtained his Bachelor degree from Computer Science in 2006, Faculty of Science, King Abdulaziz University, Jeddah, Saudi Arabia. Obtained his Master degree from Computer Science (Security in Computing) in 2011, School of Computer Science and Information Technology, the University of Melbourne property of Technology, Melbourne, Australia. He is currently a Lecturer at Faculty of Computing and Information Technology, Jeddah, Saudi Arabia. His main research interests are in the information security, Networking, and Software Engineering.

Khalid Alomar obtained his Ph.D. in Software Engineering in 2010 from the University of Bradford (United Kingdom). He is currently an associate professor at Faculty of Computing and Information Technology, King Abdulaziz University (Saudi Arabia). His main research interests are in the area of Human Computer Interaction, Data mining, and intelligent systems. He is currently the vice dean of the technical affairs at the Deanship of e-learning and Distance Education at King Abdulaziz University (Saudi Arabia).