National University of Computer and Emerging Sciences, Lahore Campus

Course:	Professional Issues in IT	Course Code:	CS449
Program:	BS(Computer Science)	Semester:	Fall 2016
Duration:	2.5 hours	Total Marks:	70
Paper Date:	21-December-2016	Weight	50%
Section:	ALL	Page(s):	11
Exam:	Final		

Instruction/Notes: **You may write on the back side of the answer sheet if you find the given space not enough.**

Roll No:_____ **Section**_____

Question	1	2	3	4	5	Total
Points	15	20	7	10	18	70
Score						

Good Luck ☺

Question1: **Marks 15**

Suppose you are the CEO of a start-up company that has just shifted to Evacuee Trust Building having spent a year in FAST's incubation center. You have a team of 5 members out of which one is the Design Expert, three are Software Developers and one is Testing Expert.

Your company is signing a contract with NADRA and shall deliver a software solution in 3 months with 6 months of warranty and 1 year of free technical support. Write the contract keeping in mind the following aspects in mind: **contract management, delivery & acceptance, intellectual property rights, guarantee.** (You may not use all the clauses but must use the necessary ones making assumptions where necessary)

***Question 2*: Read the following case and perform analysis for ethical decision making using 4-step process. Marks 20**

Larry Indole was, until recently, in charge of computer security at InterGrafCorporation. InterGraf is located in Atlanta's high-tech suburbs; it is one of the three top graphics software providers in the world. Larry's job atInterGraf was to protect the company against any threats to its computer resources, especially its software and data. He had a reputation for being proactive in his work. He always tried to anticipate a problem before it happened, and provide a solution or preventive measure before any damage was done.

While Larry was still employed by InterGraf, he worked on his own computer at home on a pet project. It was an anti-virus program in which he took great pride. However, he soon realized that in order to increase the value of the program and to make it stand out from the competition, he would have to improve it to operate in a networked environment. When it came time for him to test this more powerful version of the program, he bought the extra hardware and software to create his own small linked set of computers. He dreamed of creating a start-up company that would market and upgrade his software for all users, no matter how complex.

Larry's program, which he called LIVID for Larry Indole's Virus Identifier and Destroyer had several features that made it different and more attractive. It was very easy to use. It had:

- A sophisticated graphics user interface, or GUI
- Help screens and graphics
- Procedures for backing out of any potentially hazardous activity

It could recognize and destroy both old and new viruses. It could describe a virus in detail by type; by its effect on the system; by its source; and by its structure: it could display the source code of the virus. In addition, it allows the user to isolate the virus and copy it to a diskette. As proof that LIVID could destroy any new virus, it allows the user to modify an existing virus and then set LIVID loose on this new, redesigned version. LIVID destroys the new virus every time.

Larry suggested to InterGraf that the company use this product. He mentioned to his boss Gloria Gavilan that InterGraf had its share of infections, and could improve its security greatly by using LIVID. Larry told Gloria that he was willing to let the company buy the program at a discount, as a first customer.

Gloria had many misgivings about this program. She told Larry, "It looks to me as if you've developed an extremely dangerous program. If InterGraf were to make it available on the network, it would be like leaving a kid in a candy store. InterGraf won't buy this program, 'I promise you. In fact, I'm sure the company wouldn't take it if were free of charge. It's entirely too dangerous."

Larry was shocked. He considered his program to be an unquestionable asset. How could Gloria take it upon herself to refuse it? He decided to make LIVID available on the Internet and give up his dreams of

profiting from his work. Instead, he would become a consultant on the Internet, helping people use the program. The next day, he set up a BBS (bulletin board system) that would provide the program, both in executable and source form.

When Gloria discovered what Larry had done, she immediately fired him. Larry has now been out of a job for two weeks, during which time he advertised his new program on the Internet.

Ramon Gutierrez works as systems administrator at some company in Mexico. He has followed LIVID's publicity on the Internet, and is considering the value of downloading it and using it at UCM. He approaches his boss and asks, "Should we download LIVID? I think it's a great idea. We're always infected with some virus, and our vaccine software can't seem to keep up. Also, the software we have is difficult to use. We can't disinfect our entire network at once, for example, which LIVID can do. What do you think?"

Question 3: Internet Jurisdiction.
Marks 07

Suppose a person X commits a criminal offence in country A and then moves to country B. Can country A ask that X be arrested in country B and sent back to A so that he/she can be put on trial?

Yes, if agreement between countries exist **(Extradition Treaty)** and that act is offence in both the countries

Can X be prosecuted in country B for the offence committed in country A?

- Generally No
- Yes, subject to Extraterritorial Jurisdiction claims (USA vs. Pakistan)

Question 4: Explain the five activities contributing to effective change management. **Marks 10**

1. Motivating Change
2. Creating Vision of Change
3. Developing Political Support
4. Managing the Transition of Change
5. Sustaining Momentum Effective Change Management

Question 5: Case Study – Is your passport secure? Marks 18

In August 2007, the United States began issuing electronic passports to its citizens. These passports were identical to regular U.S. passports save for the addition of a Radio Frequency Identification (RFID) chip embedded in the back cover. A RFID chip listens for a radio query and responds by transmitting its own unique ID code. The federal government pushed for the adoption of e-passports in order to automate identity verification, speed up immigration inspections, and increase border protection. Yet the information technology security industry has continuously raised concerns. Following the terrorist attacks of September 11, 2001, federal government felt that e-passports would cut down on the number of fake passports with which international criminals and terrorists could gain access to the United States and other countries. Privacy groups and the IT security community immediately raised concerns about the initiative.

RFID was designed as a means of identifying and tracking objects from a distance utilizing a scanner and a chip embedded into the object. RFID technology is widely used by libraries, museums, airports, ranches, and toll-road systems. Corporations use RFID to track inventory and manage their supply chains. Data stored on RFID chips are considerably easier to read and intercept than data imprinted onto contact chips. The chips on passport cards contain only a unique identifier that is used to query a secure government database to pull up a photo and personal information, which the border inspectors can use to verify the identity of individuals. Despite the concerns expressed, the Government Printing Office began testing e-passports in 2004.

Two potential misuses of these were demonstrated.

Firstly, in 2006 German IT security consultant demonstrated how he could clone the RFID chip in his German e-passport using a laptop, a $200 RFID reader equipped with an antenna, and an inexpensive smart card writer. The cloned chip could then be pasted onto a forged passport. The demonstration made headlines around the world. The solution found was to place a metallic material on the cover of the passport to block any attempt to read the passport until it is opened.

Secondly, mobile security company Flexilis distributed a video showing how the RFID chip in U.S. passports could be used to identify U.S. citizens among a crowd. The security professionals reasoned that e-passports could easily open up half an inch or more if placed in a handbag. In this case, the metallic covering would no longer protect the data stored on the chip. The video showed that if the e-passport was slightly open, an RFID reader could read an identifier on the chip that would be unique to U.S. passports. Terrorists or criminals could then use this information to target U.S. citizens.

1. What countermeasure you would suggest to overcome the following weakness pointed out by Flexilis.

2. List and justify very briefly three types of crimes that can be committed using the security holes in e-passport scheme.

3. Elaborate one scenario that might originate out of illegal use of e-passport. Write scenarios different from the two already provided.

4. How can e-passport more likely lead to breach of privacy than the conventional passports?

5. Are there any Intellectual Property rights violated by shifting to e-passport system? Justify.

6. As an IT expert, suggest four applicable ways by which use of e-passports can be made more effective?