CS625 Professional Practices Final Term (Week 9-16)

Software engineering II (Virtual University of Pakistan)

CS625 Professional Practices

FINAL TERM (WEEK 9-16)

(VURANK)

Introduction to Software Safety
Liability & Practice:

- We will explore areas of legal liability and mechanisms for regulating potentially hazardous activities as well as the factors which should be taken into account for safety related applications
- Nowadays, computer-controlled systems are to be found in a wide range of diverse applications such as:-
    - Industry: Manufacturing systems, robots etc.
    - Medicine: Intensive care monitoring, radiotherapy etc.
    - Transport: Railway signaling systems, aircraft, space shuttle etc.
    - Military and defense applications

Regulatory Issues:

Standards:
Use of appropriate standards is both a familiar and traditional technique for regulating hazardous activities and attempting to ensure the safety of a product

Certification and licensing:
Certification requires that either the product or the practitioner conforms to some specified standard whereas licensing means that the product cannot go on the market at all, or the practitioner operate, unless the product is licensed or the practitioner in possession of the requisite license

Professional codes of practice:
Professional and trade associations should devise codes of practice to govern their members

Regulation by law:
The law may exert a regulatory effect either directly or by requiring compliance with other forms of regulation such as standards and licensing because of fears of litigation if safety standards are breached

Legal Liability:

Introduction
System designers and software engineers may have legal responsibilities under statutes such as the Health and Safety

Product liability and the Consumer Protection Act 1987
Product liability is the area of law in which manufacturers, distributors, suppliers and retailers are held responsible for any injuries products cause.

Regardless of any contractual limitations of liability, if a product or any of its component parts are defective its manufacturer may be liable for damage under the Consumer Protection Act (CPA) or the common law of negligence

Negligence
The manufacturer or system designer has failed to take due care in the construction or design of the system, and this lack of care has resulted in failure leading to the injury

Competence, training and experience:

- Competence means "knowledge and the ability to apply that knowledge"
- There is an understood assumption that all those engaged in the design and development of safety system software are competent to perform the necessary tasks
- Factors such as training and relevant experience are also considered important traits for a competent software engineer

Factors affecting system safety:

- Hazard analysis
- Requirements and specification
- System Reliability and safety
- Design
- Testing and debugging
- Safety integrity analysis and risk assessment
- Documentation

(END OF WEEK 9)

(WEEK # 10)

Computer Misuse & Criminal Law:

Introduction:

The media and popular computing press abound with tales of multi-million pound computer frauds and of the dangers to commercial companies, governmental data banks, financial institutions and national security from the activities of computer hackers

Computing and criminal activity:

- Modern business process is done through utilizing computer software and hardware, i.e. some form of computer system is used in it.
- There has been a sharp rise in the number of crimes involving computing; and the Internet has undoubtedly created new security risks

Categories of misuse:

Under the study of the English criminal law, the Law Commission highlighted a number of categories of misuse of computers

- Computer fraud
- Unauthorized obtaining of information from a computer
    - Computer hacking
    - Eavesdropping on a computer
    - Making unauthorized use of computers for personal benefit
- Unauthorized alteration or destruction of information stored on a computer
- Denying access to an authorized user
- The unauthorized removal of information stored on a computer

Computer Fraud:

- The Law Commission defined computer fraud as conduct which involves the manipulation of a computer or internet, by whatever method, in order dishonestly to obtain money, property, or some other advantage of value, or to cause loss
- Computer fraud is further divided into three categories
  - **Input frauds**

    E.g. intentionally entering false data or amending data into the computer
  - **Output frauds**

    Output fraud involves stealing or misusing system output
  - **Program frauds**

    Program fraud involves the dishonest alteration of a computer program

Obtaining unauthorized access to a computer:

- The second form of misuse identified by the Law Commission was unauthorized obtaining of information from a computer. It is sub-divided as:
- **Computer hacking:**

  Accessing a computer without the authorization of the owner. In this case the person accesses the computer secretly for stealing information, data or manipulation of data for diverse purposes
- **Eavesdropping**

  Literal meaning listening or spying secretly
- **Unauthorized use of a computer for personal benefit**

  Using computer's authorized information for personal benefits. In this case, the person misusing the computer is usually employee or authorized user of the company

---

(END OF WEEK NO #10)

(WEEK # 11)

Regulation and control of personal information: data protection, defamation and related issues:

Introduction:

- We can not deny the dramatic impact which increasing computerization has had on the storage, processing, retention and release of information and data.
- Computerization has revolutionized the handling and processing of information to such an extent that the data itself has now become a commodity which possesses commercial value and can be traded on the market in the same way as any other commodity
- The value to businesses is also enhanced by the fact that how easily and safely data can be transferred around the globe

Data Protection and Privacy:

- Data protection refers to how your personal information is used by the organization or being an organization, how you would make sure to protect data of your customers, employees etc
- Privacy refers to the privilege provided to an individual by law or by the organizational policy where the individual can keep the information secret to or from a specific group

The impact of the Internet:

- The original challenge of data protection law was to provide a suitable mechanism for dealing with the perceived threat to individual privacy of large centralized data banks
- The development of global information networks has changed and intensified the character of the privacy protection problem
- The question which is inevitably being asked is whether the original formulation of data protection law is capable of controlling the amorphous decentralized activities which occur through the medium of the Internet and World Wide Web

Factors affecting the regulation of data processing:

- There is by no means a straightforward answer to this question, complicated as the issues are by rapidly advancing technology, the global nature of the activities to be regulated and the variety of possible regulatory approaches to be found in the various legal traditions within the world
- Formidable problems of policy and implementation are presented by the attempt to regulate systems and practices that are technologically advanced, widely professional issues in software engineering dispersed, rapidly changing and employed by powerful economic and government interests

Convergence of Data Protection Practices:

- It is an observed fact that, at the level of international agreements and national legislation, the requirements imposed by this particular type of technology have resulted in a convergence of the rules made to ensure good data management
- An example in this respect is the emergence of data protection principles or fair use guidelines which have created a harmonizing effect on national legislation on data protection

Defamation and Protection of Reputation:

- Even without the cover of anonymity, the various methods available for the dissemination of information on computer networks provide fertile ground for the propagation of information about others
- What redress is available for those who feel that untrue and unwarranted statements have been circulated about them
- Publication of such material might attract an action for defamation. Such actions are not uncommon against newspapers and other sections of the media
- Although there may be some differences of degree and substance, most jurisdictions provide some form of remedy for injury to a person's integrity or reputation

---

(END OF WEEK NO #11)

(WEEK # 12)

Introduction to hacking:

The process of attempting to gain or successfully gaining, unauthorized access to computer resources is called hacking.

OR

The process of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose.

Who is hacker?

- A computer hacker is someone who develops, changes or attempts to circumvent computer security hardware or software.
- Intelligent, having advance knowledge of hardware and software.
- Can either happen for negative (criminal) or positive reasons.
- Criminal hackers develop computer malware or spyware to gain access to confidential information.

Types of hacking:

- Website Hacking
- Net Hacking
- Password Hacking
- Software Hacking
- Ethical Hacking
- Email Hacking
- Computer Hacking

Website Hacking:

- Hacking a website means taking control from the website owner to a person who hacks the website.

Net Hacking:

- Gathering information about the domain
- IP address (Address of your computer in the internet)
- Port (It is logical port on your computer which hacker can use to enter in the system)

Password Hacking:

- Password Hacking or Password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- **Brute force** (Hackers try out all the combination of all keyboard letters)
- **Dictionary based** (Hackers use predefine passwords. It is unsuccessful method)

Software Hacking:

- In that hackers changes the look & execution way of that software. For example change the demo version into the full version of that software.
- Modifying existing features of the software.

Ethical Hacking:

- The process in which a person hacks to find weakness in a system and then usually patches them.
- Can be used to recover lost information where the computer password has been lost.
- To test security of the system.
- Also called white hat computer hacking.

Email Hacking:

- Email hacking is unauthorized access to an email account or email correspondence.

Computer Hacking:

- Computer Hacking is when files on computer are viewed, created, edited or deleted without authorization.

What should do after hacked?

- Shut down /Turn off the system
- Separate the system from network
- Restore the system with backup Or reinstall all programs
- Connect the system to the network
- Good to call the police

Tools of Hacking:

Scanners

A program that automatically detects security weakness in remote host

Telnet

It is terminal emulation program that allows us to connect to remote system

FTP

FTP is one type of protocol but some time it is used as hacking tool, port 21 for the ftp. For connecting ftp we need some ftp s/w known as ftp client. For connecting ftp server you have to hammer that server.

Computer Security Ethics:

- Being ethical is not necessarily following one's feelings; "feelings frequently deviate from what is ethical".
- Ethics is not confined to religion nor is the same as religion. Also being ethical is not solely following the law
- Example: "If a person conceives of engineering activity as only making money, then one's definition of practical ethics, one's actions and values will, be guided by this basic philosophical position. "

Ethical Hackers:

- Performs most of the same activities but with owner's permission such as penetration tests.
- Penetration test means Legal attempt to break into a company's network to find its weakest link Tester only reports findings

Penetration-Testing Methodologies:

- **White box model**

  Tester is told everything about the network topology and technology and is authorized to interview IT personnel as well. Makes the job easier for him

- **Black box model**

  Company staff does not know about the test. Tester is not given detail about the network so the burden is on the tester to find out the details. The test determines if the security personnel are able to detect an attack.

- **Gray box model**

  This mode of test is combination of both white and black box models. The company provides the tester with partial information about the network.

Hackers Code of Conduct:

Hacker creed (Steven Levy's "Hackers: Heroes of Computer Revolution" - 1984):

- Access to computers should be unlimited and total.
- Always yield to the Hands-On Imperative
- All information should be free.
- Mistrust authority -- promote decentralization.
- Hackers should be judged by their hacking.
- You can create art and beauty on a computer.
- Computers can change your life for the better.

New Code of Ethics (90s) - Steven Mizrach :

- Above all else, do no harm"
- Protect Privacy
- "Waste not, want not."
- Exceed Limitations
- The Communicational Imperative
- Leave No Traces
- Share!
- Self Defense
- Hacking Helps Security
- Trust, but Test!

Certified Ethical Hackers:

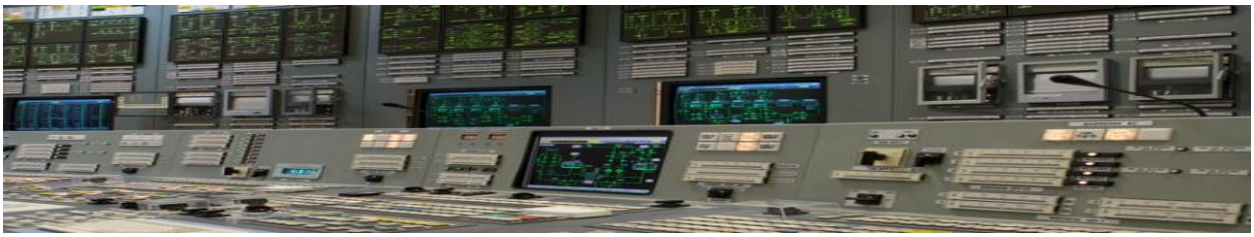
- ❑ Developed by the International Council of Electronic Commerce Consultants (EC-Council)
- ❑ Based on 21 domains (subject areas)
- ❑ Web site: www.eccouncil.org
- ❑ Red team: Composed of people with varied skills
- ❑ Conducts penetration tests

(END OF WEEK NO #12)

(WEEK # 13)

Information Security Practices:

Introduction:

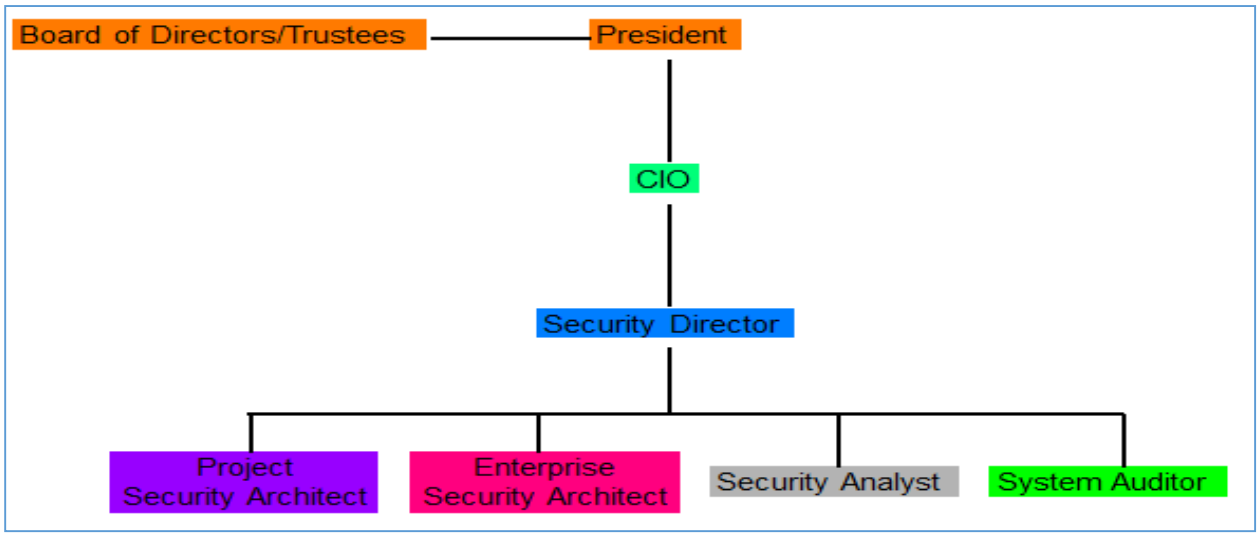


- **Information security,** sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical)

The CIA: Information Security Principles:

- The CIA principle
  - Confidentiality
  - Integrity
  - Availability

Information Security Organizational Structure:



Information Classification:

- **Information Classification**
- Government classifications
- Private Sector classifications
  - Criteria

(END OF WEEK NO #13)

(WEEK # 14)

Risk Management:

- ❑ Introduction
- ❑ Overview of Risk management
- ❑ Risk identification
- ❑ Risk assessment
- ❑ Risk control strategies

Overview of Risk Management:

Risk is

The **likelihood** of the occurrence of a vulnerability

Multiplied by

The **value** of the information asset

Minus

The percentage of risk mitigated by **current controls**

Plus

The **uncertainty** of current knowledge of the vulnerability

Risk Management is identifying, evaluating, and mitigating risk to an organization

A systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking

- It's a cyclical, continuous process
- Need to know what you have
- Need to know what threats are likely
- Need to know how and how well it is protected
- Need to know where the gaps are

Risk Identification:

- ❑ Assets
- ❑ Threats
    - Threat-sources: man-made, natural
- ❑ Vulnerabilities
    - Weakness
- ❑ Controls
    - Safeguard

Risk Assessment:

- ❑ Assessing Potential Loss
- ❑ Percentage of Risk Mitigated by Current Controls
    - Uncertainty
- ❑ Risk Determination
- ❑ Likelihood and Consequences

Risk Control Strategies:

- ❑ **Identify Possible Controls**
    - For each threat and its associated vulnerabilities that have residual risk, create a preliminary list of control ideas. Three general categories of controls exist:
    - Policies
    - Programs
    - Technical controls

Examples:

Level	Descriptor	Example of Description
1	Insignificant	No injuries, low financial loss
2	Minor	First aid treatment, onsite release immediately contained, medium financial loss
3	Moderate	Medical treatment required, onsite release contained with outside assistance, high financial loss
4	Major	Extensive injuries, loss of production capability, offsite release with no detrimental effects, major financial loss
5	Catastrophic	Death, toxic release offsite with detrimental effect, huge financial loss

Level	Descriptor	Description
A	Almost certain	Is expected to occur in most circumstances
B	Likely	Will probably occur in most circumstances
C	Possible	Might occur at some time
D	Unlikely	Could occur at some time
E	Rare	May occur only in exceptional circumstances

(END OF WEEK NO #14)

(WEEK # 15)

Social Networking & Ethics:

- ❑ **Introduction**
- ❑ **The Good, the Bad and the Ugly**
- ❑ **How to Protect yourself**
- ❑ **How to protect your children**

Introduction to Social Networking & Ethics:

Def:

When a computer network connects people or organizations, it is a social network. Just as a computer network is a set of machines connected by a set of cables, a social network is a set of people (or organizations or other social entities) connected by a set of social relationships, such as friendship, coworking or information exchange.

National Cyber Alert System:

- ❑ **Web 2.0**
  - Facebook & Myspace - Free-access social networking websites
  - Twitter – "micro" blog – 140 characters or less
  - Blog – shared on-line journal
  - Video Sharing Sites – YouTube, Flikr
  - Podcast – audio broadcast that can be downloaded

The Good, the Bad and the Ugly:

- ❑ **Example**

The case of a person asking for emergency money while impersonating a Facebook user to her friends

http://eliasbizannes.com/blog/2009/01/phishing-for-fraud-on-facebook/

Also the British MI6 chief that was exposed by his wife's Facebook pictures: http://www.dailymail.co.uk/news/article-1197562/MI6-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html

How to Protect Your Self:

- ❑ Keep private information private
- ❑ Do not post address, ssn, phone number, financial info, your schedule, full birth date
- ❑ Be careful not to display information used to answer security questions (e.g., favorite pet, mother's maiden name)
- ❑ Use caution when you click links
- ❑ Be careful about installing extras on your site
- ❑ Be wary of unknown friends (strangers)
- ❑ Google yourself
- ❑ Don't blindly connect
- ❑ Trust your gut instinct
- ❑ Use and maintain anti-virus software
- ❑ Use strong passwords
- ❑ Don't use the same password for a social networking site and for your email
- ❑ Remember - social networking sites are a public resource – like a billboard in cyberspace
- ❑ Evaluate sites privacy settings
- ❑ Lock down your profile information to people you accepts as a friend. That way no one can read your personal information unless they are an approved friend
- ❑ Be skeptical

How to Protect Your Children:

- ❑ **"**It's 10 p.m., do you know where your children are?"
  - "And who they are talking to online?"
  - Age limits on some social networking sites
  - Facebook and MySpace open to people 13 and older
  - Twitter open to all

(END OF WEEK NO #15)

(WEEK # 16)

Moral, Social and Ethical issues associated with Internet:

- ❑ Introduction
- ❑ Moral Issues
- ❑ Ethical Issues
- ❑ Advantages and Disadvantages of Internet
- ❑ Owner Ship of the internet

Introduction:

Def: The Use of internet by individuals and organizations has raised a number of issues that need to be considered.

- ❑ Setting up websites containing incorrect information. People may rely on and use this information thinking it is correct
- ❑ Bullying via email, text message, chat
- ❑ Inappropriate websites with illicit material
- ❑ Using e-mail to give bad news when explaining face to face would have been better
- ❑ Spreading rumors using the Internet

Moral Issues:

- ❑ Plagiarism
- ❑ Sending spam. People waste time deleting spam if the spam filter allows it through
- ❑ Companies monitoring staff use of the internet and e-mail
- ❑ Using someone's wireless internet connection without permission
- ❑ Using photo editing software to distort reality

Ethical Issues:

The Internet has a lot of illicit materials. The availability
of offensive, illegal or unethical material on the Internet

- Privacy issues
- Gambling addiction
- Obsity
- Addiction to computer games
- Widens the gaps between the haves and have nots (e.g. between rich and poor countries and individuals)
- Organizations moving call centers abroad. The same service can be provided cheaply using the internet and internet phone links
- Growth of e-commerce may mean shops have to close, leaving some city centers looking desolate Social Issues Many countries in the world that are not democratic; they do not allow the free passage of info to or from other countries. They control on what their people can and cannot view.
- Don’t use the same password for a social networking site and for your email

Advantages and Disadvantages of Internet:

The internet has both positive and negative effects on the users. Effects on communities

- **Advantages:**
  - Blogs & chats for communities to discuss local issues - Housebound members of the community are less isolated as people contact them to check everything is ok
  - Employment opportunities
- Local citizens advice websites can be set up to deal with the problems they have There are laws covering the production and distribution of this material BUT, the material is perfectly legal in other countries, so we can't really stop it.
  There is a special software that's able to filter out this material but we're not completely that sure.
  It doesn't have to be illicit content to be offensive; an image of a pack of hounds attacking a fox maybe offensive to animal lovers but not for the hunt

- **Disadvantages:**
  - Lack of social interaction - social networking, computer games etc.
  - Local shops shutting - more orders for goods are placed using the internet so local shops close FIN

Ownership and Control of the Internet:

- Internet is for everybody and no one actually owns it
  o Governments have started to control what can be seen on it
  o The lack of policing of the internet means that information is not checked to make sure that it is accurate

---

(END OF WEEK NO #16)