Unit - 8
Risks and Liabilities of Computer-Based Systems

- Software risks
- Safety and the engineers
- Implications of software complexity
- Risk assessment and management

Software risks

- Software risk encompasses the probability of occurrence for uncertain events and their potential for loss within an organization.
- Risk management has become an important component of software development as organizations continue to implement more applications across a multiple technology, multi-tiered environment.
- Typically, software risk is viewed as a combination of robustness, performance efficiency, security and transactional risk propagated throughout the system.
- Various risks related to software are:

1. Injection

- It is a code injection technique in which the data is injected through the input fields of the software.
- The way to protect from this is to enforce input type and length, ensure special characters are escaped, validate all input fields and use and input validation whitelist, and avoid dynamic queries or commands.

2. Weak Authentication and Session Management

- This is when attacks take advantage of improper authentication or session management practices and can lead to revealing sensitive information like passwords.
- This is why user management and authentication are important. You should perform user and role validation on all actions and use secure session cookie flags.

3. Cross Site Scripting (XSS)

- XSS is a technique that enables attackers to inject client-side scripts to the web pages.
- An unwanted script can lead to compromised credentials and sessions or redirection to malicious sites. To mitigate this, you should sanitize input.

4. Insecure Direct Object References

- It’s scary when files are exposed. Insecure direct object references lead to unauthorized data access. The most common that most people have heard of is called Local File Inclusion. This is where a secure file shows up on the front end of a web page.
- You can ensure access control checks when using direct object references and use reference maps instead of direct references.

5. Security Misconfiguration

- If security configuration is outdated, or not set up properly this can lead to unintended access to data or application functions.

6. Sensitive Data Exposure

- This is caused by improper encryption of sensitive data like payment credentials or personal information. This can lead to fraud or a company being victim.
- To fix this you should encrypt data and avoid storing sensitive data.

7. Unvalidated Redirects and Forwards

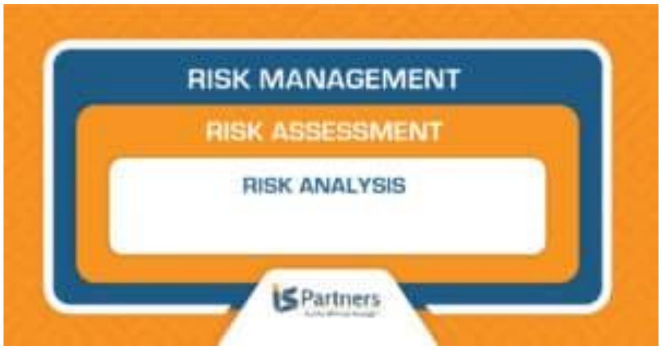
- If site gets hacked, the hackers can redirect users visiting that site to malicious sites. Also, it can trick us to think the malicious site is our site. So, we should avoid redirects and forwards altogether.

Safety and the engineers

Implications of software complexity

- Early prediction of software quality is important for better software planning and controlling.
- In early development phases, design complexity metrics are considered as useful indicators of software testing effort and some quality attributes.
- Although many studies investigate the relationship between design complexity and cost and quality, it is unclear what we have learned beyond the scope of individual studies.
- With increasing demands on software functions, software systems become more and more complex.
- This complexity is one of the broadest factors affecting software development productivity.
- Assessing the impact of software complexity on development productivity helps to provide effective strategies for development process and project management.
- To produce reliable software, its complexity must be controlled by suitably decomposing the software system into smaller subsystems.
- A software complexity metric is developed that includes both the internal and external complexity of a module.
- This allows analysis of a software system during its development and provides a guide to system decomposition.

Risk assessment and management



- Risk assessment helps us identify and categorize risks. Plus, it provides an outline for potential consequences.
- Performing a risk assessment involves processes and technologies that help identify, evaluate and report on any risk-related concern.
- Risk assessment is a “key component” of the risk management process and is primarily focused on the identification and analysis phases of risk management.
- If we take the example of a security risk assessment, it involves the following steps:
    - Identify the critical assets and sensitive data,
    - Build a risk profile for each asset,
    - Determine cybersecurity risks for each asset,
    - Mapping how critical assets are linked,
    - Prioritize which assets to address in case of a security threat,
    - Continually monitor risks, threats, and vulnerabilities.

- Risk management involves the identification, analysis, evaluation, and prioritization of current and potential risks.
- This allows you to address loss exposures, monitor risk control and financial resources in order to minimize possible adverse effects of potential loss.
- Further, a solid risk management strategy gives you the ability to maximize the realization of available opportunities to avoid risk.