CS4331/CS5332 Software Security-Exam#1-Summer2021

Name: Chen Zhang

R#:11538728

Answer the following questions shortly based on the lectures. (Every 2 points)

• Why does “the number of defects” need to be measured when defects are removed in the software development life cycle?

Answer:

Because the Defect Removal Efficiency should be measured, and based on the measurement we can decide whether to move to the next step or to stop and take corrective actions.

• Why does Agile Methods conflict with secure software lifecycle?

Answer:

The Agile Methods is designed for short requirements and fast implementation, however, Threat modeling in SSDLC is considered to be a key activity and can be challenging to perform for developers, especially in agile software development, that’s why threat modeling has not seen widespread use in agile software projects.

• Why is defective software vulnerable?

Answer:

Because most security vulnerabilities come from defects:

* Defects introduced unintentionally into software during development
* To reduce software vulnerabilities significantly
  + Reduce the overall defects
* To achieve the reduction in vulnerabilities
  + Focus on the specific types of defects

• Describe the difference between symmetric cryptosystem and asymmetric cryptosystem in terms of key(s).

Answer:

The Symmetric cryptosystem requires a single key for both encryption and decryption where the Asymmetric cryptosystem requires two keys, one to encrypt and the other one to decrypt.

• There is a speed difference between DES encryption and RSA encryption. What is the reason?

Answer:

The DES is 1000 times faster than RSA because of the key size and algorithms they use.

• Why is a public-key certificate needed?

Answer:

* How to acquire the public key of the issuer to verify the signature
* Whether or not to trust certificates signed by the issuer for this subject
* Trusted certificate authority

• Describe how Message-Digest achieves the integrity security goal.

Answer:

The integrity security goal is to protect against unauthorized changes to data and MD can guarantee this by processing a one-way encryption function, because the Hash function is easy to compute but the reverse operation is hard to do.

• What is the difference between role-based access control (RBAC) and attribute-based access control (ABAC)?

Answer:

The primary difference between RBAC and ABAC is RBAC provides access to resources or information based on user roles, while ABAC provides access rights based on user, environment, or resource attributes.

* RBAC
  + Grant access based on roles
* ABAC
  + Grant access based on attributes
    - Allows for a highly targeted approach to data security
  + To ensure an extra layer of safety that RBAC can’t provide, given that ABAC looks at many variables while establishing access

• What is a dictionary attack?

Answer:

A dictionary attack is based on trying all the strings in a pre-arranged listing, because of the following reasons:

* Infeasible to search all possible passwords to find a match
* Feasible to search all likely passwords to find a match
* Users use ordinary worlds as passwords

• Why is a non-repudiation security service needed?

Answer:

The purpose of the non-repudiation is to protect against one party in a transaction or communication activity later falsely denying that the action happened.

• What are security engineering activities in the secure software development life cycle?

Answer:

Security engineering activities include activities needed to engineer a secure solution. Examples include security requirements elicitation and definition, secure design based on design principles for security, use of static analysis tools, secure reviews and inspections, and security testing.

• Describe the difference between privacy and confidentiality.

Answer:

Confidentiality refers to personal information shared with an attorney, physician, therapist, or other individuals that generally cannot be divulged to third parties without the express consent of the client. On the other hand, [privacy](https://dictionary.findlaw.com/definition/privacy.html) refers to the freedom from intrusion into one's personal matters, and personal information.

* Privacy and confidentiality maintained
  + The clinic uses your information to treat your illness
* Privacy compromised and confidentiality maintained
  + The clinic sells your information to a marketer without agreeing with privacy disclosure
* Both privacy and confidentiality compromised
  + Your information exposed and sold on a dark web

• What is confusion in the cryptosystem?

Answer:

* Degree of prediction of what will happen to ciphertext by change in key
* Hides the relationship between ciphertext and key

• Why do not secret key systems scale well?

Answer:

Because with N parties we need to generate and distribute N\*(N-1)/2 keys

• Describe how a secret key can be exchanged between a sender and a receiver using public-key encryption.

Answer:

Suppose Alice and Bob want to exchange a shared symmetric key

* Alice and Bob have public keys for a common encryption algorithm
* Resolved authenticity for both

