Security Engineering, Final Exam (Maximum points: 35) **Date: April 24, 2015**

Name:_____

EmailID:_____

Part I

Part I has 10 multiple choice questions. Each question has exactly one correct answer. Each correct answer would be awarded 2 points. There are no negative points for incorrect answers.

1. You are to design an authentication and authorization system to authenticate users who join in the IIITD network and grant them various privileges – e.g. accessing the web, accessing ERP site, accessing various folders that contain internal official documents etc. What do you think are some of the key security mechanism the system should employ
    a. Mandatory Access Controls (MAC) and Role Based Access Controls (RBAC) to delegate various roles and privileges to different users.
    b. Discretionary access controls to make sure that a user cannot access files and resource he shouldn't.
    c. (a) along with authentication schemes such Kerberos (for domain authentication)

2. Which of the following makes it hard to execute Return Oriented Programming (ROP) based attacks:
    a. Canaries and stack smashing protections (SSPs).
    b. Address Space Layout Randomization (ASLR).
    c. Write (xor) Execute (W^X) bit.
    d. Static code checking.

    Option:_____

3. Which of the following statements is true about the heap (used in any ordinary program).
    a. Programs that don't use the malloc() (or any related routines) do not have a heap.
    b. You can never execute code off the heap. Buffer overflow only works for code residing in the stack.
    c. Memory allocated on the heap, for a process, is not de-allocated when the process terminates.
    d. The vulnerability of malloc(), that arises from the unchecked input corrupting the internal data structures that are used to manage chunks and manipulate the pointers, could be detected using mediated input.

    Option:_____

4. Perfect forward secrecy Transport Layer Security (TLS) ensures perfect forward secrecy by:
    a. Relying on RSA encryption.

b. Server certificates.
c. Separation between long-term master secret and short-term session keys.
d. None of the above.

Option:_____

5. The real advantage of using HMAC compared other ordinary hash algorithms such as SHA256 or MD5 is:
    a. The length of the hash output.
    b. It is considered to be more collision resistant compared to SHA256 and MD5
    c. Not only is it useful to check integrity but also authenticity of the messages because the hash generation involves using the key.
    d. It is faster to compute HMAC compared to SHA256 or MD5

    Option:_____

6. Which of the following do you think is a good source of random numbers:
    a. /dev/random file which listens for noises from device drivers etc. to generate random numbers.
    b. C rand() function that returns a random value in between $0 – 2^{16}$.
    c. C srand() function that generates a random value based on a seed. These random values are repeatable by using the same seed repeatedly.
    d. None of the above.

    Option:_____

7. OTPs are believed to provide “Perfect Secrecy” because:
    a. They are secretly shared between the communicating parties.
    b. They are hard to be guessed by the attacker who looks at messages corresponding to different sessions.
    c. Each OTP is used exactly once.
    d. None of the above.

    Option:_____

8. PGP (Pretty Good Privacy) (or its modern implementation Gnu Privacy Guard), differs from PKI in the following ways.
    a. PGP cannot be used for authentication. It can be only used for encryption.
    b. Both PGP and PKI involve some form of centralized attestation of messages to authenticate the identity of the original sender.
    c. PKI involves the use of centralized attestation while PGP does not.
    d. PGP is more like Kerberos than PKI.

    Option:_____

9. The basic issue with disk encryption, particularly relevant to security, is as follows:
    a. Encryption of the entire disk/partition is slow.
    b. Disk encryption algorithms generally involve stream ciphers like RC4 which are believed to be weak.
    c. Disk encryption algorithms generally don't involve long keys and are thus not resistant to brute force attacks.
    d. By default, the key being same, there is no way to store the randomization information for each sector of the disk. This can result in chosen plaintext attack (making the process semantically less secure).

    Option:_____

10. Assume you are to encrypt a file that is to be sent to a friend over an insecure medium. Which method do you think is the best way to protect the file in such a way that the friend can: a) ensure that no one knows the contents of the file b) ensure that no one has modified the contents c) ensure who has sent the file. What do you think is the BEST way to achieve the above:
    a. Use GPG to encrypt the file using some pre-shared secret and generate a hash of the file using SHA1. Thereafter send the encrypted file along with the hash.
    b. Use openSSL to achieve (a), instead of GPG, because it is considered more secure against replay attacks and also ensures perfect forward secrecy.
    c. Using GPG generate a public private key pair for yourself. Ask your friend to do the same. Thereafter encrypt the file using the friend's public key and send to him the file. Only your friend would be able to decrypt it. You could also hash the contents of the file and encrypt it with your own private key and send it along with the encrypted file.
    d. Using GPG generate a public private key pair for yourself. Ask your friend to do the same. Thereafter encrypt the file using your own private key and send to him the file. Your friend would be able to decrypt it. You could also hash the contents of the file and encrypt it with your friend's private key and send it along with the encrypted file.
    e. None of the above.

    Option:_____

Part II

There are three questions in Part II. Question 1 is worth 10 points. Question 2 and 3 are worth 5 points each. Please describe the solutions to each part. You may make whatever assumptions you think are necessary. You may use the available blank spaces.

1. Assume that you have a job as the systems analyst the State Transport Authority. You have been assigned to design the new smart card based drivers license. The license should have, apart from the owner' personal information (like name, DOB, address etc.), should also have information such as non-forgeable ID, expiry date, kind of vehicles he or she is allowed to operate and information such as violation of rules. The smart card based license could be validated even in the physical absence of the owner (for example if it is lost). Describe the design of the system – particularly what kind of information should the card store, how can it be validated and how can it be made unforgeable.

2. Sketch the design of an OTP based replay-resistant authentication scheme that relies on pre-shared secrets/passphrases. Describe in detail the steps of the process. Describe some attacks towards which the system is resilient.

3. Consider the original Kerberos protocol. It uses pre-shared long term keys of all users to generate short term session keys that have fixed timeouts associated with them. The system is generally used to authenticate users in a network where the underlying medium in insecure. Design a public-private key pair based system that can be used for the same purpose. It must be resilient to replay and MITM attacks. Describe using two attacks that validate the claim that such a system is indeed resilient to such attacks.