CSE5380 **Assignment 1 (Crypto)** **Due Thursday, Sept 17, 2020**
InfoSec 1 **Worth 100 points** **at 11:59 PM**

All questions are worth **1 point** unless otherwise stated.

Submit your answers as a simple list like:

1) a
2) b
etc.

Multiple Choice, Part 1: Answers to these questions can be found in the assigned parts of Ch. 1 and in the assigned paper by Landwehr which can be found at http://www.landwehr.org/2001-ijis-landwehr-computer.pdf.

1. What is an example of a moderate impact loss of confidentiality?
   a. Student enrollment information is exposed.
   b. Entries in an online discussion forum are falsified.
   c. Access to an online telephone directory is blocked.
   d. A personal health record is exposed.

2. Which of these systems has a high availability requirement (just choose the best answer)?
   a. A university Website
   b. A system to process financial transactions
   c. An online telephone directory
   d. Anti-virus software running on a PC

3. Why do attackers have a significant advantage over defenders?
   a. Security mechanisms are complex and it is not obvious that such measures are needed.
   b. Computer security has complex requirements that are hard to describe.
   c. The attacker only needs to find one hole; defenders must attempt to close all holes.
   d. Finding successful attacks is straightforward exercise once the system is understood.

4. If our main concern is confidentiality of data from a hostile country's hackers, we should be most concerned about what type of attack?
   a. Active insider attack
   b. Passive insider attack
   c. Active outsider attack
   d. Passive outsider attack

5. Which of these involves backup systems?
   a. Prevention
   b. Detection
   c. Response
   d. Recovery

6. What is the first step in devising security services and mechanisms?
   a. Developing a security policy
   b. Deciding between prevention and detection/reaction
   c. Designing assurance metrics
   d. Locking down unnecessary services

7. Which of these is NOT a part of what needs to be considered when developing a security policy?
    a. The value of the assets being protected
    b. The effect on ease of use of the system of various decisions
    c. The degree to which the security system implementation meets its specifications
    d. The cost of failure and recovery

8. Why is security a "weak-link" property?
    a. One weakness in the system leads to more weaknesses later.
    b. The security of the whole system is only as good as the security of each (exposed) part.
    c. The link between typical users and the system security goals is weak.
    d. Weak links in a defense can be overcome with stronger links through security design.

9. In which application area is integrity typically valued higher than confidentiality?
    a. Military documents
    b. Financial transactions
    c. Health care records
    d. Video rental records

10. Why is it difficult to simply ban the use of mobile code in a strictly controlled environment (e.g. military)?
    a. Mobile code makes Flash animations possible.
    b. Mobile code runs more efficiently than static code.
    c. Virus scanners use mobile code to distribute and install patches.
    d. Virus scanners would fail to detect the use of mobile code, making enforcement hard.

11. A misconfigured rule enforced by a firewall is an example of which of these?
    a. Risk
    b. Threat
    c. Attack
    d. Vulnerability

12. What is the BEST reason to be concerned about the insider threat?
    a. Insiders can plant malware on the system.
    b. Insiders have some degree of authorized access to the system.
    c. Insiders like disgruntled employees have greater motivation to cause harm.
    d. Insiders are harder to prosecute than external hackers.

13. What is the main advantage of risk management over risk avoidance?
    a. It leads to greater focus on defending against more dangerous threats.
    b. It leads to removal of a greater number of vulnerabilities from the system.
    c. It leads to defending against a larger variety of threats.
    d. It is more effective against insider threats.

14. Manufacturers setting a strong password on wireless routers is an example of which security property?
    a. Least privilege
    b. Accountability
    c. Default security
    d. Minimize the variety, size, and complexity of trusted components (KISS)

15. Authentication, authorization, and audit (AAA) are all part of which security property?
    a. Least privilege
    b. Accountability
    c. Default security
    d. Minimize the variety, size, and complexity of trusted components (KISS)

16. Which security principle dictates that you should use multiple, diverse, and complementary defense mechanisms?
    a. Least privilege
    b. Accountability
    c. Defense in Depth
    d. Minimize the variety, size, and complexity of trusted components (KISS)

17. Keeping the trusted code base very small in trusted computing is an example of which security property?
    a. Least privilege
    b. Default Security
    c. Defense in Depth
    d. Minimize the variety, size, and complexity of trusted components (KISS)

18. What is the computer equivalent to a fenced area?
    a. Domain
    b. Password
    c. Encryption algorithm
    d. Intrusion detection system

19. If a database application provides authorization checks for accessing data, what is the importance of file system authorization checks on the DB file?
    a. It is faster than the authorization checks.
    b. It allows for logging of the file accesses for later auditing.
    c. It ensures that the principle of least privilege is maintained.
    d. It prevents the user from simply reading the DB file directly.

20. Which of these is the best example of why administration of systems is so important to security?
    a. Administrators have more privilege than other users.
    b. Administrators are responsible for password creation.
    c. The bulk of attacks can be blocked by a properly administered firewall.
    d. The bulk of attacks are against vulnerabilities for which there are patches available.

Multiple Choice, Part 2: Answers to these questions can be found in the assigned parts of Ch. 2 and in the Wikipedia article on key size (https://en.wikipedia.org/wiki/Key_size).

21. Which of these is NOT a requirement for secure use of symmetric encryption?
    a. Sender and receiver keep the key secure
    b. Hiding the details of the encryption algorithm from the attacker
    c. Sender and receiver have obtained the secret key in a secure fashion
    d. Keys are long and random enough to prevent brute force attacks

22. Why is the DES algorithm considered unacceptable today?
    a. It is too slow.
    b. It is vulnerable to brute force.
    c. It is vulnerable to cryptanalysis.
    d. It is vulnerable to rainbow tables.

23. What type of plaintext is hardest to perform brute force on (starting from the ciphertext)?
    a. English text
    b. Chinese text
    c. A Windows 7 executable
    d. A compressed spreadsheet of numerical data

24. How much more security do you get against brute force when you go from a 64-bit key to an 80-bit key?
    a. 25% more
    b. 16 times as much
    c. $16^2 = 256$ times as much
    d. $2^{16} = 65{,}536$ times as much

25. Why do people use 3DES?
    a. AES is not yet a federal standard.
    b. It is three times as secure as DES.
    c. It is almost three times faster than DES.
    d. It retains the security of DES against cryptanalysis.

26. How long would it take to break 128-bit AES assuming 106 (1 million) decryptions per microsecond on average? (note: 1018 is a quintillion, or "billion billion". So if computers sped up a billion times, ...)
    a. 5.4×10^{18} seconds
    b. 5.4×10^{18} days
    c. 5.4×10^{18} years
    d. 5.4×10^{18} millennia

27. Which of these statements is true?
    a. Public key encryption is commonly used to share secret keys.
    b. Public key encryption is likely to supplant symmetric key encryption in the next decade.
    c. Public key encryption is more secure against brute force than symmetric key encryption.
    d. Public key encryption is more secure against cryptanalysis than symmetric key encryption.

28. Encryption of a plaintext using one's private key is _____.
    a. insecure, because anyone with the public key can decrypt it
    b. useful for providing authentication but not confidentiality
    c. useful for providing confidentiality but not authentication
    d. useful for providing both authentication and confidentiality

29. Which of these is the best for encrypting secret keys when speed is critical?
    a. RSA
    b. Diffie-Hellman
    c. DSS
    d. ECC

30. A secure hash function has which of these properties?
    a. It is impossible to undo the hash to find original input X.
    b. It is computationally infeasible to compute the hash of X.
    c. It is impossible to find inputs X and Y with the same hash value.
    d. It is computationally infeasible to find inputs X and Y with the same hash value.

31. Which of these is considered a secure cryptographic hash function?
    a. MD5
    b. SHA (the Secure Hash Algorithm)
    c. SHA-384
    d. SHA-1024

32. A brute force attacks on a hash function with n-bit outputs requires about how many hash operations?
    a. 2^n
    b. $(2^n)^{1/2}$ (the square root of 2^n)
    c. n
    d. n^2

33. What property does Alice's signature on a message NOT provide?
    a. Authentication: The message came from Alice.
    b. Non-repudiation: The receiver can prove that Alice signed it.
    c. Data integrity: The message has not been altered since it left Alice.
    d. Confidentiality: The message has not been read by anyone except Alice.

34. When checking the digital signature of Bob's message, how is a hash function used?
    a. It is used to hash the input to the encryption function.
    b. It is used to hash the output of the decryption function.
    c. It is used to hash Bob's public key before decryption; the key is long otherwise.
    d. It is used to hash the message; the hash is compared with the decrypted hash value.

35. What is the purpose of a certificate?
    a. To encrypt the secret key
    b. To keep the private key secret
    c. To prove that an identity and a public key are linked
    d. To prove that a certificate authority trusts a given user

36. Which of these crypto tools does a certificate NOT need?
    a. Hashing
    b. Symmetric key encryption
    c. Decryption using the public key
    d. Encryption using the private key

37. For a bank website, what kind of checking of identity should the certificate authority do (ideally)?
    a. Go to the bank's website to validate their information.
    b. Make a phone call to the head of the bank's Website division.
    c. Go to a bank branch in person and get bank details from a manager.
    d. Go to the bank headquarters and verify details in person with the CEO and the top Website people.

38. What is the advantage of a digital envelope over encrypting the message with the public key?
    a. The digital envelope method uses less bandwidth.
    b. Public key encryption is less secure than symmetric key encryption.
    c. Public key encryption is slow, so it saves computation time in most cases.
    d. Public key encryption can only be made to work on small amounts of data at a time.

39. Creating a digital envelope includes which of these steps?
    a. Encrypt the symmetric key with the sender's public key.
    b. Encrypt the symmetric key with the receiver's public key.
    c. Encrypt the sender's private key with the receiver's public key.
    d. Encrypt the receiver's private key with the sender's public key.

40. Random numbers for cryptography should have which of these features?
    a. Uniform distribution, Independence, and Unbreakability
    b. Uniform distribution, Independence, and Unpredictability
    c. Non-uniform distribution, Independence, and Unbreakability
    d. Non-uniform distribution, Independence, and Unpredictability