CS 136 Midterm Spring, 2018

1. Which of these issues enables both the Cold Boot attack and the Rowhammer attack?

a. Poor programming practices
b. Improper choice of operating system security policy
c. Inadequate models of hardware behavior
d. Fundamental aspects of Internet design

2. What is the purpose of an *own* right for an access control list?

a. It gives the processor all access rights to the controlled object
b. It allows the processor to change the list
c. It stands for Other Write Null, and allows truncation of a file
d. It allows the posessor to create a new group with a subset of the access permissions he possesses for the object

3. What is the difference between masquerading and delegation access requests?

a. Delegation request explicitly indicated the party being delegated to
b. Masquerading requests are commonly used to provide role based access control
c. Delegation requests cannot be performed across a network
d. Masquerading requests can be detected with ingress filtering

4. What does the principle of attenuation of privilege mean?

a. Over time, privilege in a system grows progressively more limited
b. The finer the granularity of data that access control can be applied to, the harder the access control system is to set properly
c. Security is best if one limits the access privileges of all subjects to the minimum required for them to perform proper actions
d. Subjects cannot increase their rights to access an object nor grant rights they do not possess to someone else

5. What is write-down?

a. Intentional reclassification of sensitive information to allow less privileged subjects to work with it
b. Saving passwords in a password vault
c. Removal of a subject from an access control list
d. Tagging an object for special care in performing access control

6. What party controls access to a piece of information in originator controlled access control systems?

a. The party that owns the object that contains the information
b. A party specified by name in an associated access control list
c. The party that first created the information
d. The party owning the system that implements the policy

7. What is the purpose of the Kerberos system?

a. To prevent DDoS attacks
b. To detect attempts at buffer overflows
c. To distribute authenticated keys in a distributed system

d. To prevent booting of a false version of an operating system

8. What does crossover error rate indicate?

a. The probability that a bit flip of an encrypted message will corrupt future blocks of encrypted data, given use of a particular mode
b. The point at which the false positive and false negative curves for a biometric intersect
c. The speed with which a heap-based buffer overflow attack will successfully compromise an application
d. The likelihood that a bug in a program will allow a remote user to compromise the system

9. Which of the following is NOT an advantage of providing full disk encryption in hardware vs. in the operating system?

a. Hardware full disk encryption will protect the disk even if it is stolen and examined on another machine
b. Hardware full disk encryption is faster
c. Hardware full disk encryption have less performance impact on user processes
d. Hardware full disk encryption does not require the operating system to protect the key

10. What is the purpose of a proactive password checker?

a. To assist hackers in dictionary attacks
b. To rapidly check passwords provided by users trying to log in
c. To salt passwords
d. To ensure users do not choose weak passwords

11. Which of the following is an advantage a DDoS attacker gains by using IP spoofing?

a. The attacker can more easily generate a large quantity of traffic
b. It's harder for a defensive system to add capacity to meet the size of the attack
c. It's harder for the defender to filter packets
d. The attacker can more easily perform a SYN flood attack

12. Which of the following is an advantage of Diffie Hellman key exchange?

a. Participants can share a symmetric key using only an unencrypted channel
b. It can be used to share a key among an arbitrary number of users
c. It authenticates the participants in the key exchange
d. It does not require pre-agreement on anything to exchange a key

13. For which of the following types of cipher is cryptanalysis by index of coincidence likely to be helpful?

a. A pure transposition cipher
b. A pure substitution cipher
c. A one-time pad
d. An elliptic curve cipher

14. In the Needham Schroeder key exchange protocol, why does Alice believe she is not being subjected to a replay attack?

a. A message she receives from Trent contains the encrypted identity of Bob
b. A message she received from Bob contains a nonce encrypted with the new session key
c. A message she received from Bob contains information encrypted by Trent that includes the session key
d. A message she receives from Trent contains the encrypted nonce she chose

15. If an attacker obtains a site’s salted and encrypted password file, what attack is he likely to perform?

    a. A brute force attack
    b. An off-line dictionary attack
    c. A social engineering attack
    d. A SQL injection attack

16. What type of attack does address space layout randomization (known in Windows as ASLR) address?

    a. Buffer overflows
    b. Dictionary attacks on passwords
    c. SQL injection attacks
    d. DDoS attacks

17. What is the purpose of padding in network defense?

    a. To conceal characteristics of users’ traffic
    b. To provide greater integrity for messages
    c. To prevent IP spoofing
    d. To combat DDoS attacks

18. Why is DES no longer recommended for serious use?

    a. The details of its implementation have become publicly known
    b. There is a known method of quickly cracking the cipher
    c. Evidence shows the NSA has a back door allowing simple breaking of the cipher
    d. The key is too short

19. Which characteristic must a third party site (i.e., non-compromised site) have to be useful in performing a reflection attack?

    a. It must accept requests from anywhere on the Internet
    b. It must be a DNS server
    c. It must not have ingress and egress filtering enabled at its ISP
    d. It must provide services based on TCP

20. If my firewall uses source address filtering to drop some packets going from my edge network to the Internet, which of the following packers can’t it safely drop?

    a. Packets using possibly spoofed addresses of my own edge network
    b. Packets using unallocated addresses
    c. Packets using possibly spoofed addresses of some remote autonomous system
    d. Packets using private network addresses

21. What issue causes users of RSA to keep increasing key length as time goes by?

    a. Newly discovered vulnerabilities in the algorithm
    b. Increased ease of brute force attacks on the key due to increased processing power
    c. Increased ease of factoring large numbers due to increased processing power
    d. Tendency of long-used keys to be divulged

22. What is the main purpose of multifactor authentication?

    a. To slow down attackers trying to compromise a system
    b. To provide authentication in key exchange protocols
    c. To ensure complete mediation in a computer system
    d. To compensate for security vulnerabilities in each of the factors

23. What security benefit is made possible by gathering entropy in a computer system?

a. Selection of better cryptographic keys

b. Detection of buffer overflows

c. Defense against DDoS attacks

d. Prevention of cold boot attacks

24. What does use of a Linear Feedback Shift Register (LFSR) to generate a key try to simulate?

a. Use of a one time pad

b. Diffie Hellman key exchange

c. Generation of an elliptic curve public/private key pair

d. Performing a known-plaintext attack on a cipher

25. What is the purpose of including a clock value in computation of a SYN cookie?

a. To ensure authentication of the SYN message

b. To prevent replay of ACK messages

c. To prevent use of spoofed source IP addresses

d. To prevent replay of SYN messages

CS 136 Midterm Spring, 2009

1. In asymmetric cryptography, which of the following MUST be true:

a. Different keys are used for encryption and decryption

b. Different algorithms are used for encryption and decryption

c. Cryptographic operations are one-way, and not reversible

d. Encryption takes much longer than decryption

2. Which of the following is NOT a common use of public key cryptography?

a. Digital signatures

b. Key distribution

c. Protection of real time streaming data

d. Certificates

3. Crossover error rate refers to:

a. The point at which cryptography cannot keep up with speed of data creation

b. The intersection between false positive and false negative curves for a biometric authentication measurement

c. The measurement used in differential cryptanalysis to determine the next plaintext to offer to a cipher

d. The data rate achievable by a covert channel

4. Full disk encryption protects against which of the following threats:

a. Buffer overflows

b. Covert channels

c. Compromises of the operating system

d. Loss of data when computers are stolen

5. Social engineering refers to:

[✓ a.] Attackers fooling human users into revealing information

b. Proper design of security solutions for usability

c. Improvements in user training and education to reduce security risks

d. Methods of designing web-of-trust applications to match real world social structures

6. The *-property of the Bell-La Padula security policy prevents the following from happening improperly:

a. Unprivileged subjects from reading sensitive objects

b. Transfer of privileges from one subject to another

c. Alteration of a critical object by an unprivileged subject

[✓ d.] Write-down by a privileged subject

7. The Microsoft Vista operating system contains a mandatory access policy. Which of these is its purpose?

[✓ a.] Maintaining integrity of files when a user runs untrusted executables

b. Maintaining secrecy of files between users in a server system

c. Implementing the Chinese Wall policy

d. Allowing access only to authenticated users

8. Encapsulation mechanisms allow a system to achieve which of these security goals?

a. Allowing access only to authenticated users

b. Maintaining integrity of critical data

[✓ c.] Implementing the principle of least privilege for executables

d. Improving protection of cryptographic keys

9. Why do conflicts in access control lists occur?

a. Because users disagree on when access should be granted

[✓ b.] Because a principal matches multiple entries in the access control list

c. Because users are not properly authenticated

d. Because a principal’s access privileges change over time

10. Which of the following is true of man-in-the-middle attacks?

a. They cannot be performed if one uses public key cryptography

b. They require the attacker to have pre-recorded some legitimate messages for use in the attack

[✓ c.] They require the ability to intercept communications between legitimate parties

d. They can only be performed with the active involvement of a human attacker

11. Which of the following pairs of desirable properties in a cipher will be hard to achieve simultaneously?

a. Freedom from complexity and low error propagation

b. Good diffusion and good confusion

[✓ c.] Good diffusion and low error propagation

d. Good confusion and freedom from complexity

12. If one uses a cipherblock chaining (CBC) cryptographic code, which of the following is true?

a. A single bit flip error in the first block will corrupt decryption of that block only

[✓ b.] A single bit flip error in the first block will corrupt decryption of the first and second block

c. A single bit flip error in the first block will corrupt decryption of the first, second, and third blocks

d. A single bit flip error in the first block will corrupt decryption of all blocks of the transmission

13. Which of the following statements is true about using symmetric cryptography to provide authentication of the creator of a piece of information?

a. It cannot be done
b. It cannot be used for authentication of information stored for a long period of time
c. Untrusted third parties can directly check the authentication
d. It requires use of a trusted third party

14. If a particular cipher used by party A to encrypt a packet sent to party B has been cracked by brute force, which of the following is true?

a. The cracker can now easily read all messages encrypted with that cipher by all parties using it
b. The attacker has only gained access to the information encrypted in the particular packet he cracked
c. Communications between party C and party D using the same cipher are likely to be just as secure as before the crack
d. The particular key used by A and B must never again be chosen by anyone using that cipher

15. Which of the following issues is NOT critical to the secure use of public key cryptography?

a. Key length
b. Authentication of the owner of a particular public key
c. Inability of anyone to derive a private key given a matching public key
d. Ensuring that only desired communication partners learn one's public key

16. Alice and Bob each have their own public/private asymmetric cryptographic key pair. Alice knows Bob's public key and Bob knows Alice's public key. Neither knows each other's private key. Alice encrypts a message to Bob with her private key and transmits it to him. What does Bob know, based on this cryptography, when he receives and decrypts this message?

a. The message could only have been created by Alice
b. The message has been kept secret from everyone except himself and Alice
c. Alice meant this message only for Bob
d. None of the above

17. In a cryptographic protocol, what is the purpose of a nonce?

a. To ensure that each run of the protocol is new and fresh
b. To handle situations where clock synchronization is hard to obtain
c. To verify that a trusted arbitrator has responded with a key for the desired communication partner
d. To defeat brute force attacks on the session key

18. Choosing good passwords depends on a number of factors, including the set of characters one chooses from and the number of characters in the password. Assuming 8 character passwords, if you go from passwords chosen randomly using only the English lower case letters a-z, to passwords that include both the lower and upper case English letters, how many more passwords are possible?

a. Twice as many
b. 256 times as many

c. 128 times as many
d. 26 times as many

19. Which statement best describes the standard operating system approach to protecting data in RAM?

a. Use hardware protection to limit what pages can be named
b. Use standard access control mechanisms to handle access requests
c. Encrypt data on data pages
d. Detect illegal accesses and log them

20. Which of these describes a fundamental difference between the Unix/Linux setuid/setgid mechanism and role-based access control?

a. One of them allows controlled expansion of a human user's privileges, while the other doesn't
b. One of them requires careful setting of access permissions if it is to be used safely, while the other doesn't
c. One of them allows specification of only a limited number of identities, while the other allows specification of an arbitrary number
d. One of them is explicitly tied to use of particular executables, while the other isn't

21. Originator controlled access control policies (also known as ORCON or ORGCON) are usually technically difficult to implement in computer systems. Why?

Because the entity that can provide actual access control isn't the entity that originated the policy. It's especially hard in distributed systems, since the supposedly controlled data may move away from systems that can be trusted to follow the originator's policy.

22. How could you use the Chinese Wall model to achieve the desirable goal of separation of duties for a critical task requiring multiple steps?

Each step in the task should be assigned to the same Conflict of Interest class. Once a subject has performed one of the tasks, the Chinese wall policy will prevent him from performing any of the others, since they're in the same COI class.

23. Which would be easier to implement in hardware, DES or RSA? Why?

DES is easier, because it makes use of simple arithmetic and logical operations that are easy to implement in hardware. RSA uses exponentiation, which is not easy to implement in hardware.

24. One method of revoking a capability is to require a generation number to be provided with the capability when presented for use. To revoke the capability, one increments the required generation number at the capability checking mechanism, providing the new number to those who should still have access, and not providing it to those who should have access revoked. What is problematic about this approach in a distributed capability system where multiple authorities run the different machines?

The other authorities might be untrustworthy, in which case they might provide the number to subjects who should have had their access revoked. Even if the capability is protected cryptographically, unless it's tied to the particular subject, the untrustworthy remote system might give a copy to the wrong party.

25. One approach to automatically generating passwords for people to use us to create random, but pronounceable, passwords by combining phonemes. What are the advantages and disadvantages of this approach?

The advantage is that a password not in any actual dictionary might be used, while still being relatively easy to remember. The disadvantage is that brute force attacks need only test all legal combinations of phonemes, not all legal combinations of letters, making the attack a lot easier.

CS 136 Midterm Winter, 2017

1. Chip and Pin is one form of two-factor authentication. What types of factors does it use?
   a. Something you have and something you are
   b. Something you are and something you know
   c. Two different types of something you have
   d. Something you know and something you have

2. Assuming random choices of passwords in each case, which of the following will be most resistant to brute force attacks?
   a. 8 character passwords, upper and lower case alpha characters only
   b. 10 character passwords, lower case alpha characters only
   c. 8 character passwords, lower case and numeric characters only
   d. 6 character passwords, upper case, lower case, numeric characters only

3. What is the purpose of a shadow password file?
   a. To prevent non-privileged users from accessing some password-related information
   b. To permit storage of passwords in encrypted forms
   c. To deceive attackers into trying to crack fake passwords
   d. To allow the system to send users plaintext versions of passwords they have forgotten

4. What is the confinement problem as defined by Lampson?
   a. Ensuring that untrusted code cannot access confidential information
   b. Preventing a server from leaking confidential information
   c. Ensuring that a cipher has proper quantities of confusion
   d. Ensuring that malicious code cannot propagate from one node to another

5. What is a covert channel?
   a. A type of VPN
   b. A method of securely distributing a cryptographic key
   c. A channel that uses shared resources as a path of communication
   d. A channel that uses one time pads to protect communications

6. Which of the following is an example of applying the principle of separation of privilege?
   a. Running newly download code in a sandbox that does not have access permission to most system resources
   b. In a setuid root program, relinquishing superuser status as soon as possible
   c. Prohibiting single sign-on to a sensitive system
   d. In a system using the Bell-La Padula model, requiring more than one user to approve write-down

7. Which of the following operations could not be performed by a filtering firewall?
   a. Preventing HTTP traffic from being delivered to a local machine that does not run a web server

b. Stopping ping floods
c. Ensuring that all packets delivered to a VPN server have the address of a known partner VPN server
d. Dropping email messages sent by unknown parties

8. Which of the following messages should not be put into a log?
a. A message indicating that a program used OS features to escalate its privileges
b. A message indicating that a packet was delivered to a closed port on the receiving machine
c. A message indicating the user ID and password for failed login attempts
d. A message indicating that a program attempted to open a file for which it did not have proper access permissions

9. Which of the following is true of the Biba security policy?
a. Subjects cannot write objects with lower clearance levels
b. Subjects cannot read objects with lower integrity levels
c. Subjects cannot write objects with lower integrity levels
d. Subject cannot read objects with higher clearance levels

10. What is mandatory about mandatory access control policies?
a. The system requires the policy to be followed based on the choices of the owners of data items
b. The system does not allow individual users to prevent access to their data
c. The system requires the policy to be followed regardless of the wishes of users
d. The policy must be applied to all data items in the system

11. Which of the following operations is easy to perform in a capability-based access control system?
a. Taking access permissions away from a user
b. Determining the entire set of subjects that can access an object
c. Determining the entire set of objects a subject can access
d. Ensuring proper access control when subjects and objects are located in different nodes of a network

12. Which desirable security property is most closely related to the use of a reference monitor?
a. Complete mediation
b. Least privilege
c. Fail-safe defaults
d. Economy

13. Which of the following is a strong mixing function?
a. SHA-1
b. A one-time pad using XOR to encrypt
c. A polyalphabetic substitution cipher
d. A triple columnar transposition cipher

14. Which of the following is the best example of an interchange key?
a. A public key contained in a X.509 certificate
b. The key established by a Diffie-Hellman key exchange
c. The key used to perform full disk encryption
d. A session key set up by the Needham-Schroeder protocol

15. What security problem is addressed by certificate pinning?

a. Creation of false certificates by legitimate certificate authorities
b. Certificate revocation
c. Handling updates to expired certificates
d. Improper copying of certificates

16. What type of attack does data execution prevention (known in Windows as DEP) address?

a. SYN floods
b. Brute force password guessing
c. Return oriented programming attacks
d. Buffer overflows

17. Which of the following statements is true of key use for different styles of network encryption applied to applications like web browsing?

a. It can only use end-to-end encryption
b. It can use either end-to-end encryption or link level encryption, but not both
c. It may use both end-to-end and link level encryption
d. It can only use link level encryption

18. Which of the following is true of IPSec?

a. It only works with IPv4
b. It can be used to ensure message integrity
c. It includes procedures for key distribution
d. Its transport mode encrypts an entire IP packet

19. What is a reflection attack?

a. A method of attack-back, in which a defender sends attack packets to the site that attacked him
b. A DDoS attack in which the attacker sends spoofed packets to legitimate sites, which respond to the target site
c. An attack that results in the duplication of a virtual machine, allowing the attacker to replay its behavior
d. An attack on a pseudo-random generator that causes it to reuse old seeds

20. If my firewall uses source address filtering to drop some packets coming into my edge network from the Internet, which of the following packets can’t it safely drop?

a. Packets using spoofed addresses of my own edge network
b. Packets using loopback addresses
c. Packets using spoofed addresses of some remote autonomous system
d. Packets using private network addresses

21. What is a reverse firewall?

a. A firewall configured to specify only the packets that should be let through, rather than those that should be dropped
b. A firewall used to control access to a secondary network connection
c. A firewall used to trace attackers rather than filter their packets
d. A firewall that filters outgoing packets

22. Which of the following is not an element of a cryptographic mode?

a. A cipher
b. A key

c. A key distribution mechanism
d. A form of feedback

23. In the field of computer security, what is meant by non-repudiation?
    a. An inability to revoke a capability or certificate
    b. An inability to change a system's trust in another system
    c. An inability to distinguish false positives from false negatives
    d. An inability to deny one's past actions
24. What important security property does Diffie-Hellman key exchange provide?
    a. Authentication of participating parties
    b. Secrecy when using an insecure channel
    c. Immunity from man-in-the-middle attacks
    d. Immunity from replay attacks
25. Which of the following is a reasonable concern about security properties of data in a page frame on a modern general purpose operating system?
    a. Will an arbitrary process be able to read the data in a page frame allocated to my process?
    b. Will a malicious process be able to prevent me from accessing data in my page frame?
    c. Will the data in the page frame be cleaned before the page frame is given to another process?
    d. Will a malicious process be able to prevent me from swapping the data in my page frame to disk?
26. Why is length an important property of an initialization vector?

    In the past, security protocols like WEP have been exploited due to using a short initialization vector. Longer initialization vectors are better because they make the initial encryptions performed by a stream cipher less predictable.
27. Why do capabilities used in a distributed system typically need to be cryptographic?

    Since capabilities used in a distributed system are transmitted over the network, they need to be cryptographic so that malicious users cannot spoof bit patterns that look like a valid capability. Users are not checked against an access control list, so capabilities better be valid since there is no other last line of defense.
28. Why did users of non-Miscrosoft operating systems have a concern about the SecureBoot element of the UEFI?

    SecureBoot in UEFI only allows certain versions of certain operating systems to boot by keeping a list of valid OS signatures. Linux users were concerned that they would not be able to install Linux on new UEFI hardware because they did not think Microsoft would include Linux OS signatures in SecureBoot.
29. Why does full disk encryption fail to provide protection against a compromised operating system on the machine hosting the file system?

    The OS is still able to decrypt files when they are read and encrypt files when they are written, because it has the key in a secure location. The OS is in complete control. Therefore, if the OS is compromised, an attacker could make the OS do whatever they please, including reading encrypted data since this is a valid action of the OS.
30. What is the purpose of an IPSec security association?

IPSec security associations are used in order to pick the type of encryption used during the communication of the secure on way channel.

CS 136 Midterm Winter, 2021

1. Let P be the set of all states of a system, R be the set of states a particular security mechanism allows the system enter, and Q be the set of all secure states in the system as defined by the system's security policy. If there is a state r that is a member of P and R, and r is not a member of Q, which of the following describes the security mechanism?

   a. The security mechanism is secure
   b. The security mechanism matches the security policy
   c. The security mechanism is narrow
   d. The security mechanism is broad
   e. The security mechanism is precise

2. What is the purpose of a shadow password file?

   a. To prevent non-privileged users from accessing some password-related information
   b. To allow the use of salting in password storage
   c. To allow the system to send users plaintext versions of passwords they have forgotten
   d. To permit storage of passwords in encrypted forms
   e. To deceive attackers into trying to crack fake passwords

3. Which of the following is an example of a covert channel?

   a. Sending data between two machines encrypted with the receiver's public key
   b. A tamper-resistant hardware link between two computers that is only usable by the computers' trusted processes
   c. Sending data between two machines encrypted with the sender's private key
   d. Diffie-Hellman key exchange
   e. Sending information between two processes by adjusting the time slice behavior of the sender

4. For a commercial system trying to provide separation of function, which of the following is likely to be true?

   a. Different security mechanisms will be used in each part of the system
   b. The system will use the Bell-LaPadula security model
   c. Strong barriers will be placed between users working for different clients who are competitors
   d. Critical security functions will require at least two different users to take action
   e. New software will not be developed on production systems

5. Which of the following is the best example of transitive trust?

   a. Using cipher block chaining to protect a data transmission containing multiple packets
   b. Using virtual memory techniques to prevent a process from accessing another process' memory
   c. TPM used by the OS to sign the validity of a particular version of an application
   d. The Biba integrity security model
   e. Using nonces to defeat a replay attack

6. Which of the following is the best example of a phishing attack?

a. Using a buffer overflow to take over a web server

b. A forged email saying that you need use a particular web site to reset your password

c. Leaving a flash drive infected with malware lying in a parking lot

d. Performing a man-in-the-middle attack on Internet commerce

e. An email message trying to sell you a product you don't want

7. Which of the following is the best example of fail safe design?

a. A reverse firewall that only permits outgoing packets to a set of trusted IP addresses

b. Data execution prevention

c. Exclusively using open source libraries in one's software products

d. Using timestamps in a cryptographic protocol

e. SYN cookies

8. Which of the following is an important element of PGP?

a. Use of symmetric cryptography for authentication

b. Reliance on a limited set of well known signing authorities

c. Freedom from chains of trust

d. Embedding trust information in a digital signature

e. Protection against denial of service attacks

9. Which of the following approaches would be helpful in detecting that a piece of ciphertext was encrypted using only permutation techniques?

a. Attacking the random number generator used to create the key

b. The Kasiski method

c. The Index of coincidence method

d. Finding repeated patterns of symbols in the cipher text

e. Examining the frequency distributions of the encrypted data

10. What kind of security system does a type flaw attack typically operate against?

a. A system for defending against DDoS attacks

b. A randomization method for key selection

c. An ASLR system combating buffer overflows

d. A capability-based access control system

e. A cryptographic protocol

11. What aspect of TCP does a SYN flood attack try to misuse?

a. Interfaces between TCP and IP

b. Limited size of open connection tables at a server

c. TCP's use of sequence numbers

d. TCP slow start

e. TCP's exponential backoff feature

12. What kind of attack does padding typical help defeat?

a. An attack on Diffie-Hellman key exchange

b. A replay attack

c. A DDoS attack

d. A traffic analysis attack

e. A man-in-the-middle attack

13. Deep packet inspection is likely to be used in which of the following defenses?

a. An ingress filtering system

b. An onion routing system

c. A filtering gateway

d. A proxy gateway

e. A SYN cookie system

14. Which of the following approaches helps a security protocol avoid the suppress-replay attack when timestamps are used in the protocol?

a. Including multiple timestamps in all messages

b. Using asymmetric cryptography in the protocol

c. Using symmetric cryptography in the protocol

d. Ensuring all parties in the protocol are authenticated

e. Always using timestamps from a single clock

15. Why have modern GPUs caused problems with the use of passwords for authentication?

a. They make dictionary attacks easier

b. They make password salting impossible

c. GPUs cannot authenticate users via passwords

d. They can intercept and divulge passwords when they are created

e. They limit possible choices of passwords

16. Node A is sending a large quantity of data to node B over the network. They are encrypting the data with AES, using ECB mode. A network error flips one bit in the encrypted version of block N. Which blocks will be improperly deciphered at B due to the bit flip?

a. Block N-1, block N, and block N+1

b. All blocks in the same packet as block N

c. Block N and block N+1

d. Block N and all subsequent blocks

e. Block N

17. Which of the following changes to the basic Chinese Wall policy does the aggressive Chinese Wall policy add?

a. Adding integrity controls to confidentiality controls

b. Ability to apply the model in a distributed environment

c. A generalization of the conflict of interest classes

d. More precise inspection of operations on objects controlled by the policy

e. Applicability to system objects, in addition to user level objects

18. In the context of computer security, what is OCTAVE?

a. A framework to self-assess security of a system

b. A DDoS defense tool

c. An access control policy

d. A mechanism for reporting security flaws in software

e. A firewall

19. Your company backs up its critical data on tapes, which are stored in a remote facility. Which of the following is the best technology to protect the data on the backup tapes?

a. DES

b. AES

c. RSA

d. SHA 256
e. Elliptic curve cryptography

20. Which of the following is an advantage polyalphabetic substitution ciphers have over monoalphabetic substitution ciphers?

a. Polyalphabetic ciphers make frequency analysis harder
b. Polyalphabetic ciphers offer better diffusion properties
c. Polyalphabetic ciphers are safe against use of index of coincidence cryptanalytic methods
d. Polyalphabetic ciphers offer better perfect forward secrecy
e. Polyalphabetic ciphers use simpler key creation methods

21. In the context of use of cryptography, what is meant by a round?

a. The period after which a new key must be established
b. The period over which feedback is applied in use of a cryptographic mode
c. One of several repeated operations as part of a cipher
d. An exchange of messages in a cryptographic protocol
e. The steps in negotiating the cipher and other properties of an encrypted session

22. In the context of computer security, what is the difference between a weakness and a vulnerability?

a. A weakness is a more serious security problem than a vulnerability
b. There is no meaningful difference between these terms
c. A weakness is a system flaw with no security implications, while a vulnerability is a flaw with security implications
d. A weakness is a vulnerability that can be exploited
e. A vulnerability is a weakness that can be exploited

23. Which of the following is true of identity-based encryption?

a. The only secrets required by such a system are the secret keys
b. It uses symmetric cryptography
c. It does not require trusted third parties
d. It can provide key escrow services
e. It can be based on RSA

24. Which of the following operations is easy to perform in a capability-based access control system?

a. Determining the entire set of subjects that can access an object
b. Taking access permissions away from a user in a distributed system
c. Determining the entire set of objects that a subject can access
d. Ensuring proper access control when subjects and objects are located in different nodes of a network
e. Changing a remote user's ability to access a local resource

25. Which of the following is true of IPSec?

a. It includes procedures for key distribution
b. It can only be used to provide message confidentiality
c. It only works with IPv4
d. Its transport mode encrypts only the payload of an IP packet
e. It can be used to provide availability

CS 136 Sample Midterm Exam

1. Which of the following best describes how a process' authentication is most commonly performed in a typical operating system?

    a. Processes are not authenticated unless their application software requires it
    b. Processes must provide a password upon creation
    c. The process inherits the identity of the parent process
    d. Processes receive an identity associated with the executable they are running

2. Nonces, initialization vectors, and password salts, at a high conceptual level, provide the same characteristic benefit to a security system. Which of the below best describes that benefit?

    a. They simplify the problem of key distribution
    b. They ensure that the encrypted versions of two pieces of information are different
    c. They permit multi-factor authentication
    d. They improve diffusion in cryptography

3. Why are asymmetric ciphers more useful for authentication than symmetric ciphers?

    a. They are harder to break
    b. They provide faster authentication
    c. They allow parties to create cryptographic proof of identity that can be easily checked
    d. They provide both secrecy and authentication in a single cryptographic operation

4. Which of the following is typically an example of link level encryption?

    a. IPSec
    b. WPA2
    c. SSL
    d. VPNs

5. Which of the following best describes the relationship between security policies and security mechanisms?

    a. Security policies implement security mechanisms
    b. Security mechanisms implement security policies
    c. Security policies are a type of security mechanism
    d. Security mechanisms are a type of security policy

6. Which should change more frequently, a session key or an interchange key?

    a. A session key
    b. An interchange key
    c. Both should change at the same rate
    d. Neither should change

7. Which of the following is a disadvantage of the volume encryptor approach to encrypted file systems?

    a. It requires hashing a possibly weak password to obtain the encryption key
    b. It is not transparent to the user during ordinary operation
    c. Its cryptography is performed in a possibly untrusted user level process
    d. It does not offer fine-grained encryption at the file or directory level

8. Which of the following is a passive threat?
   a. A man-in-the-middle attack on an Internet connection
   b. A SQL injection attack
   c. A phishing attack
   [✓ d.] Eavesdropping on an unencrypted wireless network

9. Which of the following is a disadvantage of the Bell LaPadula security model?
   a. It does not provably achieve its stated purpose
   b. It does not allow mandatory access control
   c. It does not address secrecy of information
   [✓ d.] It makes it difficult to share necessary information among subjects with different security clearances

10. The Linux file access control model is a form of what access control method?
   [✓ a.] An ACL
   b. Role based access control
   c. Capabilities
   d. An access control matrix

11. What is the confinement problem?
   [✓ a.] Preventing a server from leaking confidential information
   b. Dividing a network into disjoint segments for security purposes
   c. Preventing details of key generation from becoming known to attackers
   d. Ensuring that all data that should pass through a VPN does so

12. Which of the following is a direct benefit of using a password vault?
   a. It reduces the risk of single sign-on
   [✓ b.] It allows the user to select longer and more complex passwords
   c. It makes the user immune to a dictionary attack
   d. It prevents phishing attacks from succeeding

13. Which of the following kinds of cryptanalytic attacks is most likely to require physical access to the device performing the cryptography?
   a. A known plaintext attack
   b. Differential cryptanalysis
   [✓ c.] A timing attack
   d. A chosen plaintext attack

14. Which of the following problems do we need to worry about most if we use a certificate hierarchy for authentication?
   a. IP spoofing
   b. Covert channels
   [✓ c.] Transitive trust
   d. Replay attacks

15. Which of the following security mechanisms has trouble with revocation?
   a. Firewalls
   b. Data execution prevention
   [✓ c.] Capabilities
   d. Honeypots

16. What kind of cryptographic algorithm is a one time pad, of the form described in class?

a. A monoalphabetic substitution cipher
b. A polyalphabetic substitution cipher
c. A single permutation cipher
d. A multiple permutation cipher

17. Which of the following is not an element of a cryptographic mode?

a. A key
b. Feedback
c. Authentication
d. A cipher

18. If a secure communication system exhibits the property of perfect forward secrecy, what benefit does it gain?

a. Decrypting one packet encrypted with a particular key will not help an attack decrypt other packets encrypted with that key
b. Proper use of entropy in the system is ensured
c. Authentication of communicating parties is provided
d. Divulging one session key will not help an attacker learn other session keys

19. What is cross-over error rate?

a. The speed at which a DDoS defense system discovers which packets should be dropped to mitigate the attack
b. A description of the effectiveness of a biometric authentication mechanism
c. The rate at which a covert channel can transmit data
d. A description of how far an error propagates in an encrypted data stream using a particular mode

20. Which of the following is true of password salts?

a. They can be stored in plaintext form without reducing their benefit
b. They need to be changed frequently to remain effective
c. Users must take special care to choose their password salts
d. The password salt should be derived from the password via a one-way cryptographic hashing function

21. Which of the following is true of authentication devices based on cryptographic challenge/response?

a. The challenge is chosen from a small set of pre-defined personal questions
b. Only asymmetric cryptography can be used
c. Such devices ensure proper authentication even if they are stolen, without any further authentication required
d. The cryptography should be performed on the device, rather than a computer the device is plugged into

22. Which of the following security guarantees does a typical paged virtual memory system attempt to provide to a process?

a. No other process can read the data in its pages
b. The page frames used by the process cannot be taken away by another process
c. No covert channel can be used to transmit data in the process’ pages to another process
d. Buffer overflows cannot corrupt memory outside of the page frame where they occur

23. Which form of cryptography is likely to have the most problems preventing repudiation?

a. A symmetric cipher
b. An asymmetric cipher
c. A block cipher
d. A stream cipher

24. When is it easiest to perform source address filtering?

a. As traffic enters a tier 1 autonomous system
b. On arrival at scrubbing sites where traffic is diverted from its usual path
c. On arrival at the destination machine
d. As traffic leaves a local network and enters the Internet

25. Which of the following is an example of failing to provide complete mediation?

a. Single sign on
b. Use of DES
c. Failure to salt passwords
d. Lack of true randomness in key generation

CS 136 Final Spring, 2009

1. In symmetric cryptography, which of the following MUST be true:

a. Encryption and decryption take the same amount of time
b. Different algorithms are used for encryption and decryption
c. Cryptographic operations are one-way, and not reversible
d. The same key is used for encryption and decryption

2. If one uses electronic codebook (ECB) cryptographic mode to transmit a series of related blocks of data, which of the following is true?

a. A single bit flip error in the first block will corrupt decryption of that block only
b. A single bit flip error in the first block will corrupt decryption of the first and second block
c. A single bit flip error in the first block will corrupt decryption of the first, second, and third blocks
d. A single bit flip error in the first block will corrupt decryption of all blocks of the transmission

3. Which of the following statements is true about using asymmetric cryptography to provide authentication of the creator of a piece of information?

a. It cannot be done
b. It cannot be used for authentication of information stored for a long period of time
c. Untrusted third parties can directly check the authentication
d. It requires on-line use of a trusted party

4. Alice and Bob share a symmetric cryptographic key that is known by nobody else, and both Alice and Bob know that. Alice encrypts a message to Bob with the shared key and transmits it to him. Which of the following does Bob NOT know, based on this cryptography, when he receives and decrypts this message, given that he knows someone other than himself created the message?

a. The message could only have been created by Alice
b. The encrypted message is unreadable by anyone except himself and Alice
c. Both of the above
d. None of the above

5. Personal Identification Numbers (PINs) are essentially passwords used as a second form of authentication for ATM cards and similar situations. A typical PIN is 4 characters long, and only uses the numerals from 0-9 in each position. But many of the keyboards used to enter PINs have two extra keys, often with a different symbol on each, such as a telephone pad's common inclusion of a * and # key. If PINs can also include either of these symbols, as well as the numerals, in each position, how many more PINs would be possible than with just the numerals?

a. Around twice as many
b. Around 20% more
c. Around four times as many
d. Around 16 times as many

6. A SYN flood exhausts what resource at its target?

a. Ability of the machine's network card to handle incoming packets
b. Entries in the process table
c. Entries in the TCP connection table
d. Processing power

7. Which of the following has NOT been a factor in making it hard to defend against distributed denial of service attacks?

a. Ability of attackers to spoof their IP addresses
b. Number of compromised machines available to perform attacks
c. Ability of attackers to use arbitrary packets in the attack
d. Inability of intrusion detection systems to detect such attacks

8. Which of the following is true of the use of link level encryption in a multihop network?

a. It ensures that only the original sender and ultimate receiver can view the data in unencrypted form
b. It requires fewer encryption and decryption operations than end-to-end encryption
c. It can vary cryptographic algorithm strength to match individual components of the overall network path
d. It is how a typical virtual private network (VPN) manages security across the Internet

9. Which of the following is NOT true of an IPSec Security Association (SA)?

a. It describes a duplex connection
b. It users a particular set of cryptographic algorithms to protect the data it is related to
c. It describes a connection between precisely two end points
d. Its properties must be stored in databases at the parties making use of it

10. If you were implementing Tor-style onion routing using IPSec to provide all necessary cryptographic services, which of the following statements would be true?

a. You would only need to use IPSec's authentication features
b. ESP in transport mode would be a good match for your needs
c. ESP in tunnel mode would be a good match for your needs

d. You would want to avoid using IPSec Security Parameter Indices (SPIs) to prevent tracing of the packets

11. Source address filtering can be used either on packets coming into or going out of an edge network. Which of the following is true for a typical edge network?

a. The same set of packets can be properly filtered in either direction
b. More different source addresses can be filtered on packets leaving the edge network and going into the Internet than packets coming from the Internet going into the the edge network
c. More different source addresses can be filtered on packets coming from the Internet going into the edge network than packets leaving the edge network and going into the Internet
d. If you perform filtering in one of the two directions, you must not perform it in the other or you will interrupt proper follow of packets

12. Which of the following is true of firewalls?

a. An application gateway firewall will probably need more processing power than a filtering gateway firewall
b. If you use an application gateway firewall, you will not need to update it regularly
c. If you install a reverse firewall, you will have no need for a filtering firewall
d. Transparency is an undesirable property for a firewall

13. In a normal multi-firewall configuration, which of the following is true of the DMZ?

a. It contains any machines you keep outside your outermost firewall
b. It is the area inside your innermost firewall
c. It is between your outermost firewall and innermost firewall
d. It contains portable machines that have not yet been validated to allow them any network access

14. Which of the following is true of virtual private networks?

a. They use cryptography to provide a similar security effect as a direct protected network link
b. Their main purpose is to guarantee quality of service in the face of denial of service attacks
c. They are primarily used to allow secure communications within a honeypot that is emulating multiple machines on one real machine
d. They require use of TPM technology at all endpoint machines to achieve their goals

15. In the context of network security, what is backscatter?

a. Damage done to legitimate traffic when a denial of service defense drops traffic coming from some source
b. Evidence of IP spoofing obtained by watching traffic arriving at unallocated IP addresses
c. A method of obtaining entropy to create cryptographic keys to be used by IPSec
d. A method botnet controllers use to communicate within the botnet

16. Which of the following is not an important failure mode for an intrusion detection system?

a. False positives
b. Subversion errors
c. False negatives
d. Synchronization errors

17. Which of the following is true of anomaly detection based on intrusion detection systems?
    a. They can only detect problems they are already aware of
    b. They may be susceptible to training attacks
    c. They are the basis of most commercial intrusion detection systems available today
    d. They are only usedable for network-based intrusion detection, not host-based intrusion detection

18. One dimension along which computer viruses are classified is what kind of computer resource they infect. Which of the following is not a virus classification of this kind?
    a. Polymorphic viruses
    b. TSR viruses
    c. Multipartite viruses
    d. Macro viruses

19. Which of the following is NOT a reason why it is hard for defenders to deal with botnets?
    a. Legal issues
    b. Difficulty of finding and analyzing copies of the botnet code
    c. Scale
    d. Difficulty in tracing the controlling user of the botnet

20. What is the main purpose of a rootkit?
    a. To obtain and maintain complete control of a compromised computer
    b. To spread to other machines
    c. To steal private information
    d. To fool users into running malicious executables on their machines

21. The term TOCTOU is relevant to which kind of program security flaw?
    a. Buffer overflows
    b. Misplaced trust
    c. Race conditions
    d. Variable initialization

22. Experts in secure C/C++ programming recommend that you do not use *scanf()* function. Why?
    a. It fails to ensure that its cryptographic key is chosen properly
    b. It is often susceptible to buffer overflows
    c. It is likely to cause improper synchronization between its first and second parameters
    d. It tends to cause race conditions

23. Which of the following is most likely to cause a security problem in the use of a random number generator?
    a. Use of a pseudorandom number generator
    b. Generating a random number based on variations in hardware performance
    c. Using a cryptographic hash to generate a random number
    d. Generating a random number based on user input

24. Which of the following was NOT a reason for the ultimate failure of the Orange Book approach to security ratings?
    a. Slow time to market of rated products
    b. Lack of confidence that the ratings actually meant systems were suitability secure
    c. Lack of universal trust in the parties performing the security evaluations

    d. Too much generality in the security models it covered

25. What is the primary purpose of an attack tree?
    a. Tracing spoofed packets through the Internet
    b. Ensuring proper input validation
    c. Describing improper behavior for misuse detection methods of intrusion detection systems
    d. Threat modeling
26. Which of the following is the fundamental result of Cohen's theoretical analysis of virus detection?
    a. Detecting an arbitrary virus in an arbitrary program is undecidable
    b. The number of tests one must perform to detect a set of virus
    c. The rate of infection of a computer virus in a particular environment is a logarithmically increasing function
    d. The path of a virus' infection through a set of programs is Hamiltonian
27. What is a trusted computing base (TCB)?
    a. A Common Criteria term describing the system being evaluated
    b. Special hardware that can provide remote attestations about the software running on a machine
    c. The set of protection mechanisms within a computing system that are responsible for enforcing a security policy
    d. A formally verified operating system kernel that ensures access controls are properly handled
28. In a typical case of cross-site scripting, which party is attacking which party?
    a. A client is attacking a server
    b. A client is attacking another client
    c. A server is attacking a client
    d. A server is attacking another server
29. What of the following is NOT true of Tor-style onion routing?
    a. Data is encrypted multiple times
    b. The packet takes the most direct path from the source to the destination
    c. Each intermediate router does not know if the next hop is the final destination
    d. Proper key management is critical to the goals of the system
30. Which of the following is NOT an important issue for using capabilities for access control?
    a. Preventing improper copying of capabilities
    b. Handling revocation
    c. Figuring out a given subject's security domain
    d. Identifying all subjects that can access a resource
31. Is an intrusion prevention system more like a honeypot or a firewall? Why?

    One can argue this question either way, and the main point is to do so intelligently. It's like a firewall because it's protective, it frequently relies on what amounts to signature matching, and it typically examines most or all input. It's like a honeypot because it needs fairly deep understanding of what's going on, it doesn't reject attack inputs, and (depending on type) may need to be stateful.

32. What does the quality of its random number generator have to do with the ability of a worm to spread quickly?

> A worm with a good random number generator will visit each IP address once before it visits any address twice, allowing the fastest possible spread.

33. Cryptography can be used for many things. For example, it could be used to encrypt data to be archived on a tape for many years, or it could be used to protect a critical message being sent across the Internet. Are the issues of key selection the same or different for these two cases?

> Keys used for permanent storage will never (or, at most, rarely) be changed. Keys used for message transit will be used once and discarded. One might argue the permanent storage key must be of higher quality. However, if the message remains critical forever, then, again, the key must never be learned.

34. Recent proof-pf-concept experiments have shown that malware can potentially infect firmware in peripheral devices. What changes will this observation require in procedures for cleaning up infected machines?

> If malware can infect peripherals, then cleaning a machine requires cleaning all infectable peripherals. One can't simple use a clean boot disk.

35. Why is error handling an important issue for writing secure code?

> Error handling is important in writing secure code because attackers will force your error handling code to be exercised, looking for a flaw. Since such code is rarely tested and used, it is more likely to contain such a flaw, so special care is necessary with it.