Computer Security

2019 Exam 2 Review

Paul Krzyzanowski

Rutgers University

Fall 2019

Part 1: Malware

Question 1

version B: 6, C: 5

N-day vulnerabilities are particularly dangerous because:
(a) The affected systems have a large attack surface.
(b) Attackers have more days (N) to attack a target than with a 0-day vulnerability.
(c) The malware runs for a longer time than 0-day vulnerabilities.
(d) A larger community of attackers knows about them than they do of 0-day vulnerabilities.

- 0-day vulnerabilities: undisclosed vulnerabilities
  - Only attackers who know about them can exploit them
- N-day vulnerabilities: disclosed vulnerabilities
  - N days = time between disclosure and all systems being updated
  - Everyone knows about them, so any attacker can try to exploit them

Question 2

version B: 1, C: 6

A *Trojan* is a type of malware that:

(a) Looks and acts like legitimate software.

(b) Contains a backdoor for attacker access.

(c) Stays dormant until it gets a request from a command and control server.

(d) Attacks other systems to propagate itself.

Question 3

version B: 2, C: 1

Spear phishing differs from phishing because it:

(a) Requires a user to click on a link to download the malware.

(b) Is personalized to the victim.

(c) Is sent to a large collection of people.

(d) Contains malware within the message so the victim does not need to take any action.

Question 4

version B: 3, C: 2

Rootkits:

(a) Enable malware to run with administrative privileges.

(b) Run malware before the system boots.

(c) Hide the presence of malware in the system.

(d) Bypass standard authentication mechanisms to allow attackers to log into the system.

Question 5

version B: 4, C: 3

Anti-malware software refers to a signature as:

(a) The set of files that the malware modifies.

(b) A sequence of bytes that is unique to that specific piece of malware.

(c) The encrypted hash of the malware.

(d) The sequence of operations that a virus performs as it runs.

Question 6

version B: 5, C: 4

With *polymorphic* malware:

(a) The malware can switch between running as a worm and running as a virus.

(b) The malware modifies different files each time it runs.

(c) The payload varies based on what the malware downloads from its command and control server.

(d) The malware's code changes each time it moves to a new system.

The malware modifies itself when it propagates

- Changes code (e.g., adds NOP instructions)
- Changes packing encryption

(b) The function of the malware does not change – it does the same thing

Part 2: Cryptography

Question 7

version B: 12, C: 11

Kerckhoffs's Principle states that a cryptosystem should be secure:
(a) If the algorithm and the key are kept secret.
(b) It has been rigorously tested and no weaknesses have been found.
(c) If a unique key is used each time an encryption is required.
(d) Even if everything about it is publicly known except the key.

Question 8

version B: 7, C: 12

Polyalphabetic substitution ciphers improved upon monoalphabetic ciphers by:

(a) Being able to handle multiple languages.

(b) Reducing the size of the ciphertext by allowing a single character to represent multiple plaintext characters.

(c) Being less vulnerable to frequency analysis.

(d) Using a symmetric algorithm.

Question 9

version B: 8, C: 7

Why is the *one-time pad* almost never used?

(a) It only works on textual data rather than binary files.

(b) It is less efficient when compared to modern block ciphers.

(c) It is not as secure as modern algorithms.

(d) It requires a key that is the same length as the message.

Question 10

version B: 9, C: 8

A requirement for *perfect secrecy* is:
(a) The key must be the same length as the message.
(b) Neither the key nor the algorithm must be leaked to the adversary.
(c) A different key must be used for decryption than for encryption.
(d) Keys must be long enough to make an exhaustive search impractical.

Perfect secrecy = the ciphertext conveys no information about the content of the plaintext.

Claude Shannon proved that a system would need a key as long as the message to accomplish this (e.g., a one-time pad)

(c) This is public key cryptography

Question 11

version B: 10, C: 9

Which statement best describes the property of *confusion*?

(a) If an attacker only sees the ciphertext, it is impossible to figure out what encryption algorithm created it.

(b) Frequency analysis attacks are ineffective due to the use of multiple substitution alphabets.

(c) It is difficult to find a relationship between any part of the ciphertext with any part of the plaintext and key.

(d) Any change in the plaintext data propagates throughout the entire ciphertext.

Question 12

version B: 11, C: 10

Compared to Cipher Block Chaining, *Counter* (*CTR*) mode:

(a) Does not make the ciphertext dependent on its position in the file or data stream.

(b) Enables blocks to be encrypted in parallel.

(c) Requires fewer encryption operations.

(d) Is less secure since the plaintext is never encrypted.

CTR mode encrypts a counter value for each block & XORs the plaintext with the encrypted counter.

- There is no dependence on feedback from past blocks as with CBC

(a) The counter is incremented for each successive block, so the same plaintext will create different ciphertext based on its position

Part 3: Integrity & Key Exchange

Question 13

version B: 19, C: 18

The *Diffie-Hellman algorithm* is designed to allow:
(a) Alice to encrypt a session key for Bob.
(b) Alice and Bob to come up with a shared secret key.
(c) Alice to encrypt messages that only Bob can read.
(d) Alice to send tamper-proof and encrypted messages to Bob.

Diffie-Hellman allows two parties to derive a common key.

If desired, that key can then be used to

- (a) encrypt a session key or
- (d) send messages with a MAC and encrypt the messages

BTW – best practice is to use different keys for MAC and for encryption

Question 14

version B: 13, C: 19

A *hybrid cryptosystem*:
(a) Encrypts a symmetric session key with a public key algorithm.
(b) Uses two layers of encryption for higher security.
(c) Combines encryption with integrity.
(d) Uses a different key for each direction of communication.

A hybrid cryptosystem uses public key cryptography to encrypt a session key. After that, a symmetric cipher is used to encrypt data

Question 15

version B: 14, C: 13

Forward secrecy requires:

(a) All keys used for a session never to be reused.

(b) Sending a session key via public key cryptography.

(c) A key that is as long as the message.

(d) Pre-shared encryption keys.

Question 16

version B: 15, C: 14

A *MAC* differs from cryptographic hash functions because it:
(a) Produces a fixed-length output regardless of the message size.
(b) Incorporates a shared secret key.
(c) Can be inverted to recover the original message.
(d) Applies compression to the message.

Hash = cryptographic checksum

MAC = *hash*(key, data)

Digital signature = E_{priv}(*hash*(data))

Hashes in any form cannot recover the original message.

Question 17

version B: 16, C: 15

The *pigeonhole principle* tells us that:

(a) Hash collisions can occur.

(b) Hash collisions will never occur with a good cryptographic hash function.

(c) Hash functions are not reversible.

(d) The output of a hash is always a constant size.

N+1 pigeons cannot fit in to N holes.

An unlimited set of messages cannot be uniquely represented in 256 bits (or 160, or 512, …)

Question 18

version B: 17, C: 16

A *digital signature* differs from a MAC because it:
(a) Identifies the user who signed the message.
(b) Does not rely on hash functions.
(c) Produces a fixed-length result.
(d) Uses different keys for signing than for verification.

A digital signature uses public key cryptography to have a different signing key from a verification key.

User identification is not a core part of a digital signature & needs to be done through other means, such as sending a digital certificate.

Question 19

version B: 18, C: 17

An *X.509 digital certificate*:
(a) Secures a message with a digital signature.
(b) Contains an encrypted hash of the message to which it is attached.
(c) Associates a name with a public key.
(d) Securely stores the user's private key.

The purpose of a digital certificate:

- A tamper-proof data structure that contains a user's public key and identifying information about that user ("distinguished name").

It has nothing to do with any accompanying message

To make the structure tamper-proof, it is signed by the certificate issuer.
This is the implementation, not the purpose of a certificate

Part 4: Authentication

Question 20

version B: 25, C: 24

The *Needham-Schroeder* protocol was improved by Denning-Sacco to:
(a) Remove the need to use public key cryptography.
(b) Add the use of nonces to ensure replay attacks are not possible.
(c) Fix a vulnerability that is present if an attacker knows an old session key.
(d) Not require the use of a trusted third party.

Needham-Schroeder added the use of nonces to third-party key exchange to avoid basic replay attacks

Denning-Sacco added a timestamp to avoid replay attacks where a previous session key has been discovered.

Question 21

version B: 2, C: 3

When Alice wants to talk to Bob and receives a ticket from Kerberos, that *ticket*:
(a) Contains a session key and is encrypted for Bob.
(b) Contains a session key and is encrypted for Alice.
(c) Contains Bob's identification and is signed by Kerberos.
(d) Contains an authorization code that Alice can send to Bob.

---

ticket = *sealed envelope* = message that Alice cannot decode

Kerberos sends Alice two messages:

1. The session key encrypted for Alice
2. The session key encrypted for Bob – this is the ticket she gives to Bob

Question 22

version B: 21, C: 20

Which of the following is *NOT* an example of *two-factor authentication* (*2FA*)?

(a) Access card and face scan.

(b) Username and password.

(c) Password and SMS code.

(d) PIN and fingerprint scan.

Question 23

version B: 22, C: 21

The use of *salt* makes:

(a) It impossible to find a password from a hash with a dictionary attack.

(b) User passwords extremely difficult to guess.

(c) Stored hashed passwords from two users different even if the passwords are the same.

(d) Password transmission secure over an insecure network.

---

hash(“a5Bz!” + “monkey”) ≠ *hash*(“@$mq7” + “monkey”)

- A dictionary attack means trying chosen passwords from a dictionary rather than all combinations. How passwords are stored is irrelevant.
  - Dictionary attack ≠ precomputed hashes
- How passwords are stored has no bearing on guessing passwords

Question 24

version B: 23, C: 22

The *Time-based One-Time Password (TOTP) protocol* works because:
(a) Both sides share the same secret value.
(b) One side sends the time encrypted with the service's public key.
(c) A random sequence number ensures that the password is different each time.
(d) All messages are encrypted with a shared session key.

Time-based One-Time Passwords (TOTP):

one_time_passwd = *hash*(time_of_day, secret)

vs. Hash-based One-Time Passwords (HOTP):

one_time_passwd = *hash*(hardware_id, passcode, counter)

Question 25

version B: 24, C: 23

With Google's *reCAPTCHA*. you can simply click on a checkbox to state you are a human because:

(a) The position of the box varies slightly each time it is shown so automated software cannot predict its location.

(b) CAPTCHAs have been shown to be mostly ineffective, so checking a box is as good as typing words.

(c) Automated software cannot recognize the reCAPTCHA prompt, so only humans can check the box.

(d) The service looks at your IP address, Google cookies, and mouse movements.

Reputation management

– JavaScript code monitors mouse movement, acceleration, and precise location of clicks

– Risk analysis backend: server looks at IP address (check for known bots) &cookies (do you look like a legitimate user of Google services)

The end