Quiz 2 Answer Key

ECE 4112 / ECE 6612 / CS 4262 / CNS 6262
Spring 2025

True/False Questions

Grading Rubric:

- 2pts if correct

1. With BGP, routes to a subnet are selected primarily based on economic/financial factors (e.g., cost), with other factors such as shorter AS paths or lower latencies being secondary factors.
    a. **True. Cost is the main factor for BGP routes.**
2. If two ASes have a peering relationship, they will route each other's traffic for free, for certain routes as agreed upon when establishing the peering relationship.
    a. **True. This is exactly the definition of a peering relationship.**
3. Route Origin Validation (ROV) implemented on all routers would provide integrity over the entire AS-PATH for all routes in BGP advertisements/announcements.
    a. **False. ROV only provides integrity over the originating AS.**
4. TCP sequence numbers start at 0.
    a. **False. They are randomly chosen initial values to prevent easy prediction.**
5. TCP requires a 4-way handshake to establish a connection.
    a. **False. TCP requires a 3-way handshake (SYN, SYN+ACK, ACK).**
6. Let's say Eve knows Alice has a TCP connection with Bob, and wants to inject data into the TCP stream. To do so, Eve would at least need to know the IP addresses, ports, and sequence numbers used in the TCP connection by Alice and Bob.
    a. **True. Then Eve can spoof a valid-looking TCP packet, with the right address and port to get to Alice/Bob's TCP connection, and the right sequence numbers for them to accept the packet as part of the TCP stream.**
7. DNSSEC provides integrity, authenticity, and confidentiality.
    a. **False. DNSSEC doesn't provide confidentiality.**
8. Without DNS bailiwick checking, the gatech.edu authoritative name server could do a DNS cache poisoning attack and set the cached A record for uga.edu at a recursive resolver.
    a. **True, this is the example we showed in class (except for mit.edu NS setting the facebook.com record).**
9. An attacker wishes to spoof a UDP response packet. To do so, the attacker only has to guess the UDP identification number correctly.
    a. **False. UDP does not have an ID number.**
10. The defense against the Kaminsky Blind Spoofing DNS attack is to randomize both the source and destination ports used for DNS requests, in addition to the DNS ID value.

    a. **False. The defense is randomizing the source port (in addition to the DNS ID #). The destination port needs to be known, since it's the port used by the server (which needs to listen for DNS requests on a known specific port).**

11. Compared to TLS 1.2, TLS 1.3 reduces the number of round trips required for the TLS handshake.
    a. **True. That was the design advantage of TLS 1.3 over TLS 1.2.**
12. TLS uses asymmetric cryptography for key exchange and symmetric cryptography for the rest of the connection's data transmission.
    a. **True. TLS first uses RSA/DH key exchange to select symmetric crypto keys, then uses those symmetric keys for everything else.**
13. TLS 1.2 and TLS 1.3 both support RSA and Diffie-Hellman key exchange.
    a. **False. TLS 1.3 removes RSA as a key exchange option, as it doesn't offer perfect forward secrecy.**

Multiple Choice Questions

Grading Rubric:

- 4 pts if fully correct
- 2 point if some choices are correct, but did not get all correct choices (or chose incorrect choices)
- Only incorrect choices got 0 pts

1. Let's say a router wants to route to IP address 18.0.0.1, and has the following entries in its routing table (e.g., the routes it has previously learned and selected via BGP). Which route would be picked for 18.0.0.1?
    a. Subnet = 18.0.0.0/8 ; AS-PATH = A,B ; Cost = 20
    b. Subnet = 18.0.0.0/10 ; AS-PATH = A,C ; Cost = 20
    c. Subnet = 18.0.0.0/18 ; AS-PATH = A,C,D ; Cost = 25
    d. Subnet = 18.0.0.0/24 ; AS-PATH = A,C,E ; Cost = 25

With routing to a specific IP, we'll use the longest prefix match. The routing table already has the "best" route to a specific subnet, so we find the most specific subnet to that IP.

2. Which of the following are true about TLS? (Select all that apply)
    a. SSL is the newest version of TLS
    b. TLS is an application-layer protocol
    c. TLS 1.2 has a 3-way handshake
    d. TLS uses 4 symmetric cryptographic keys (2 for encryption, 2 for integrity)

A is wrong as SSL is the old version of TLS, now deprecated. B is true as TLS is indeed application-layer as it sits above the network layer. C is wrong as TLS 1.2 has a 4-way handshake; TCP has a 3-way handshake. D is correct, as TLS generates one encryption and one integrity key for the client, and one encryption and one integrity key for the server (so 4 keys total).

3. Your browser connects successfully to google.com over HTTPS. Given this successful connection, which of the following individual attacks/attackers could not have affected the security of your connection with google.com? Assume that google.com's private key has not been compromised. (Select all that apply)
    a. **Hijacking the BGP routes to google.com's IP address**
    b. A compromised certificate authority (CA) mis-issuing a certificate for google.com to a malicious entity
    c. **Spoofing DNS responses for google.com's IP address**
    d. **A malicious Wifi router/access point**

If you connected to google.com successfully over HTTPS, that means you have successfully validated google.com's TLS certificate (and google.com's server demonstrates ownership of the associated private key). Thus, you have authenticated that you are connected to google.com's server, so any attacks that attempt to redirect you to an attacker's server or MITM your TLS connection would fail (answers a, c, and d). However, if a compromised CA issues a wrong cert for google.com, your trust assumptions are no longer valid and it's possible you're actually connected with the attacker server using the mis-issued google.com cert.

4. Which properties does TLS provide for end-to-end communication? (Select all that apply)
    a. **Confidentiality**
    b. **Integrity**
    c. Availability
    d. **Authentication**
    e. None of the above

TLS provides confidentiality through encryption, integrity through MACs, and authentication through certs/public keys/signatures. It does not protect against availability attacks (like DoS).
NOTE: I saw a few responses that indicated not D (authentication), b/c TLS as described in class provides authentication of the server but not the client. Technically TLS can allow for client certificates, so bidirectional authentication (although not often used), but we didn't discuss this in class. So I've decided to allow A+B for full credit too.

5. With BGP, say that AS1 is a paying customer of AS2. Which of the following would be true of their BGP advertisements, based on financial incentives? (Select all that apply)
    a. **AS2 will advertise to AS1 that it can route to other neighboring ASes**
    b. **AS2 will advertise to other neighboring ASes that it can route to AS1**
    c. AS1 will advertise to all neighboring ASes that it can route to AS2
    d. AS1 will advertise to AS2 that it can route to other neighboring ASes

Since AS1 is a paying customer of AS2, AS1 needs to pay AS2 for any traffic it sends and receives through AS2. So AS2 will be incentivized to advertise routes that send traffic to AS1 (b) and routes that take traffic from AS1 (a). AS1 will avoid trying to route traffic to AS2 and avoid taking traffic from AS2 (so not options c and d, respectively).

6. Which of the following are reasons that BGPSEC may not be widely adopted yet? (Select all that apply)
    a. BGP operators don't understand how BGPSEC works
    b. Computational overhead due to the cryptographic operations
    c. Limited benefits with only partial deployment
    d. ROV is a strictly more secure solution

B and C were discussed in class. A is generally not true (and not discussed in class). D is also not true as ROV covers a different issue compared to BGPSEC (route origin vs whole AS Path validation).

7. Which of the following domains are within the bailiwick of the gatech.edu name server? (Select all that apply)
    a. amazon.gatech.edu
    b. www.cc.gatech.edu
    c. georgiatech.edu
    d. gatech.com

Options a and b are subdomains of gatech.edu, so within its name server's bailiwick.

8. Which of the following statements are true about DNSSEC? (Select all that apply)
    a. Key-signing keys (KSKs) are used to generate all DNSSEC signatures
    b. Given the same DNS query, DNSSEC responses are bigger than regular DNS responses
    c. DNSSEC records cannot be cached
    d. With DNSSEC, every name server (whether the root, TLD, or authoritative) will include a signature (an RRSIG record) for every DNS record it provides to a DNS client

B is true due to the key/signature data. A is false because KSKs only sign other key records. ZSKs sign other DNS records. C is false as DNSSEC records can be cached, a core DNSSEC property.
Finally, D is false because only the authoritative NS returns a signature for the final answer record. Intermediate NSes do not provide RRSIGs on DNS records, such as those telling the client what NS to use next (e.g., root tells the client to go to the .com NS, that record is not accompanied with another RRSIG record, as discussed in class; only the DS record has an accompanying RRSIG).

(However since D was a common selection, I believe there was some ambiguity with this option, so I will give 3/4pts if B+D are selected.)

9. Which of the following methods allow TLS clients to detect that a certificate has been explicitly revoked by a certificate authority? (Select all that apply)
    a. Certificate expirations
    b. Certificate Revocation Lists (CRLs)
    c. Online Certificate Status Protocol (OCSP)
    d. DNS Bailiwick Checking

OCSP and CRLs are CA mechanisms for revocation. Certificate expirations aren't revocations, and DNS bailiwick checking doesn't have to do with TLS at all.

10. Let's say you are on the Georgia Tech WiFi network, and your DNS client is using DNS-over-TLS (DOT) with the public Google DNS recursive resolver (8.8.8.8). Which of the following entities can observe the domains that your DNS client is querying?
    a. Google's DNS recursive resolver (8.8.8.8)
    b. DNS authoritative name servers
    c. Georgia Tech's WiFi router
    d. Georgia Tech's local DNS recursive resolver

NOTE: We forgot to put "Select all that apply" so if you select one of the correct values, we will give full credit.

The DOT connection, since it uses TLS, means that entities on the path between the client and Google's DNS recursive resolver cannot see the DNS traffic (so that eliminates c). The local DNS recursive resolver wouldn't receive the DNS queries to start with, so not d. But the Google recursive resolver naturally sees the requests (as it needs to resolve it) as does the authoritative name servers, so a and b are true.

Fill-in-the-Blank Questions

1. A browser just sent a web server a TCP data packet with a sequence number of 1500, an acknowledgement number of 2000, and a data payload of 30 bytes. The server responds to that packet with a TCP data packet containing a 10-byte payload. What are the sequence and acknowledgement numbers in the server's TCP packet? (Assume no packet loss/drops in this connection.)
Answer:
Seq #: 2000
Ack #: 1530

The server response's seq # will be the ack # from the client request (since the ack # indicates the next seq # that the client expects to receive from the server), so seq # = 2000.

The server response's ack # will be the index of the next expected data byte from the client. Recall that the seq # itself is indicating the index of the first byte of the packet. So here, the client request's seq # is 1500, indicating the first byte of the client's packet is at index 1500. The data payload is 30 bytes, so the last payload byte is at index 1529. That leaves the server response's ack # as 1530, as the index of the next expected data byte from the client.

Grading Rubric:

- **3pts each for correct answer**
- **2 pts if off by just 1 for an answer**
- **1 pts each for incorrect answer**
- **0 pts for no answer**

Long(er) Answer Questions

7 points each

1. A BGP router supports BGPSEC, and receives a route to subnet X with AS-PATH A->B->C. That route has BGPSEC signatures for the A->B and B->C hops in the route that verify successfully (i.e., the full AS-PATH is verified with BGPSEC). Can the router be confident that this is a legitimate route to subnet X? Answer yes or no, and explain why in detail.

No. BGPSEC by itself just validates that the path is legitimately composed of announced routes (e.g., A truly did hear from B that there's a route to X through C, and likewise B did hear from C that it has a route to X). However, it does not validate the route origins, that C really can announce routes to X. This is the purpose of ROV/RPKI.
Grading Rubric: Key aspects are 1) mentioning the need for origin validation, and 2) BGPSEC doesn't provide origin validation (it provides only path validation, although this doesn't need to be explicitly mentioned).

- **2 pts for effort (wrong answer/explanation)**
- **3 pts for a correct answer with a missing or incorrect explanation.**
- **5 pts for a correct answer with a generic/incomplete explanation (e.g., saying BGPSEC doesn't protect such situations without explaining why).**
- **6 pts for a correct answer and specifying one of the two key aspects**
- **7 pts for a complete answer specifying both key aspects**

  <u>Alternative Answer:</u> No, BGPSEC by itself only guarantees path validation, but it cannot prevent route leaks. A route leak occurs when an intermediate AS incorrectly propagates a route it received from one of its neighbor ASes to another AS when it shouldn't. This violates routing policies or business

agreements, making the advertised route illegal. It could be possible this route is not legitimate in the sense that it was a leaked route.
Here, simply saying route leak is 5pts (generic/incomplete), and full credit requires explaining the route leaks scenario leading to this route not being legitimate.

2. You and Eve are in the same coffee shop, both on their open WiFi network (within WiFi range of each other). She can also see your screen, and notices that you just opened *https://youtube.com* in your browser. Eve would like to prevent you from watching Youtube videos (probably because it's distracting to her), and wishes that she could somehow terminate your Youtube HTTPS connection. Can Eve disrupt your browser's connection with Youtube? If yes, explain in detail what Eve would do for her attack. If not, explain how the Youtube HTTPS connection prevents Eve from doing so.

Yes, Eve can try to close your TCP connection by spoofing a TCP RST packet. Eve can easily do so correctly since she can sniff your TCP traffic (being within WiFi range on an open network), so she can see your TCP header parameters, including the addresses, ports, and sequence numbers. Despite the connection being over HTTPS (so TLS), TLS doesn't protect against TCP-level attacks like RST injections.

Grading Rubric: Key aspects are discussing that 1) Eve can do a TCP RST injection attack (or a FIN + subsequent ACK attack), or describe such an attack, and 2) Eve can sniff your TCP traffic so easily observe your header information (or mention seeing the sequence numbers and ports).

- **2 pts for effort (wrong answer but provided an explanation)**
- **3 pts for correct answer but missing/incorrect explanation**
- **5 pts for correct answer with generic/incomplete explanation (e.g., briefly saying Eve can reset the TCP connection without explaining how)**
- **6 pts for correct answer with partially correct explanation, mentioning one of the two key aspects**
- **7 pts for correct answer with a fully correct explanation with both aspects**

3. Your browser connects to https://gatech.edu using TLS 1.2, using the Diffie-Hellman key exchange. Mallory is a MITM attacker who can observe and potentially tamper with your TLS 1.2 traffic (including the handshake). Let's say that Mallory changes the Diffie-Hellman key exchange message sent by the browser to gatech.edu (so not gatech.edu's half of the DH key exchange).

Will your browser and gatech.edu successfully set up a TLS connection?
If yes, will Mallory be able to observe the plaintext web traffic? Explain why or why not.
If not, why won't the TLS connection be set up successfully?

No, the TLS connection won't be set up correctly. If Mallory changes the browser's DH key exchange message, your browser and the server will compute different symmetric keys. Then, during the last phase of the TLS 1.2 handshake where both sides exchange

MACs of the TLS handshake dialog, the MACs won't validate correctly because both sides will have generated different MAC integrity keys and the dialogs will also be different.
Note, the browser's DH key exchange does not have a signature (only the server does, since the server's public key is known from the TLS certificate). So answers mentioning signature detection, or earlier detection than the dialog check, won't receive full credit.

Grading Rubric: Key aspect is discussing the MAC dialog checks failing.

- **2 pts for effort (wrong answer but provided an explanation)**
- **3 pts for correct answer but missing/incorrect explanation (including mentioning a signature verification of the browser's DH key exchange message).**
- **5 pts for correct answer with generic/incomplete explanation (e.g., briefly saying TLS protects against this without discussing specifically why)**
- **6 pts for correct answer with partially correct explanation (e.g., detailed discussion without specifically mentioning the MAC dialog checks)**
- **7 pts for correct answer with a fully correct explanation**

4. Let's say that the root and .edu name servers support DNSSEC, as does the gatech.edu authoritative name server. So normally, all DNS records from the gatech.edu authoritative name server should be fully verifiable with DNSSEC.

One day, Mallory is able to compromise the .edu name server, including the cryptographic keys that the .edu name server uses for DNSSEC.

Afterwards, your DNS client iteratively queries for ece.gatech.edu using DNSSEC, and gets a final answer that fully validates in DNSSEC. Can you trust that this final answer is correct? If yes, explain how DNSSEC ensures this final answer is correct. If not, explain in detail how Mallory can control the final answer while still fully passing DNSSEC validation.

No. Mallory, having compromised the .edu NS, can cause your client to go to a malicious authoritative NS, rather than the real gatech.edu authoritative NS. Mallory can still pass all DNSSEC checks because the now-compromised .edu NS can generate the right DS and RRSIG values for the malicious authoritative NS (e.g., the DS can have the hash of the malicious authoritative NS's key, and Mallory can sign that using the compromised .edu NS private key). All the remaining DNS records (including DNSSEC records, such as keys and signatures) from the malicious authoritative NS are purely within Mallory's control, and she can generate and sign the records under her control correctly (as .edu NS has already validated its key).

If someone explicitly assumed that by ".edu's cryptographic keys" they meant only public keys within DNSSEC then we'll accept as fully correct answers of yes, where the explanation is about how Mallory cannot create DNS records with valid RRSIGs w/o the private keys.

Grading Rubric:
For the no answer, aspects of the explanation are that 1) the .edu NS can respond with a different authoritative NS than the real one (the real one is not under Mallory's control), 2) the .edu NS can update its DNSSEC records to match those of the malicious/different authoritative NS
For the yes answer, full credit requires both 1) the lack of access to the private key and 2) the inability to generate valid RRSIGs to be mentioned.

- **2 pts for effort (wrong answer/explanation)**
- **3 pts for a correct answer with a missing or incorrect explanation.**
- **5 pts for a correct answer with a generic/incomplete explanation (e.g., saying that once the .edu NS is compromised, nothing is secure; more explanation is needed here).**
- **6 pts for a correct answer and specifying one of the two key aspects**
- **7 pts for a complete answer specifying both key aspects**