Solutions: Final Exam

Network Security Autumn 2018

7 February 2019

Surname, Given Names (*e.g.*, Turing, Alan Mathison): ____________________

Student Identification Number (*e.g.*, 15-123-456): ____________________

Student Signature: ____________________

Rules and guidelines:

- Place your identification card on your desk. An assistant will check your identity during the exam.
- Once the exam starts, make sure you have received **all** pages of the exam. The exam should have **21 pages total**, including a page for extra space. **Do not** separate the exam sheets.
- Do not forget to fill in your **name, student identification number and signature** on this page.
- You **must** answer questions using **black or blue ink**. Illegible answers may not get any credit.
- The use of notes, textbooks or other written materials is **not** allowed. You are allowed to use a **scientific calculator** during the exam. Any other device that provides communication or document storage capabilities is **not** allowed (this includes smart watches).
- You have **120 minutes** to complete this exam.
- You should write answers that are **clear and concise**. Generally, you do not need to completely fill the space provided for solutions.
- You are **not** required to score all points to get the maximum grade.
- When answering questions, always **explain your reasoning**. If a question asks, for instance, whether A is more secure than B, a plain "yes" or "no" answer will not be awarded any points.
- For questions during the exam, **raise your hand** and an assistant will come to answer your question.
- If you need extra space to answer a question, use the page provided at the back of the exam.
- At the end of the exam, please **remain seated** while we collect the exams. You may hand in your exam before the end, except in the last 10 minutes of the exam. Please **hand in all exam sheets**: if any sheet is missing, the examination will be marked with grade 1.0 and counts as failed.

Question:	1	2	3	4	5	6	Total
Points:	21	17	5	14	15	8	80
Score:							

1. PKI and TLS (21 points)

During your master thesis in the system security group, you designed a new cryptocoin. Your design is so promising that you decide to create a spinoff to bring your coin to market, and as a tribute to your favorite course at ETH, you decide to call your company *NetSecCoin.*

One of the first things you do, is to setup an online wallet system. For this you register the domain `netsec.coin`, on which you set up a web server.

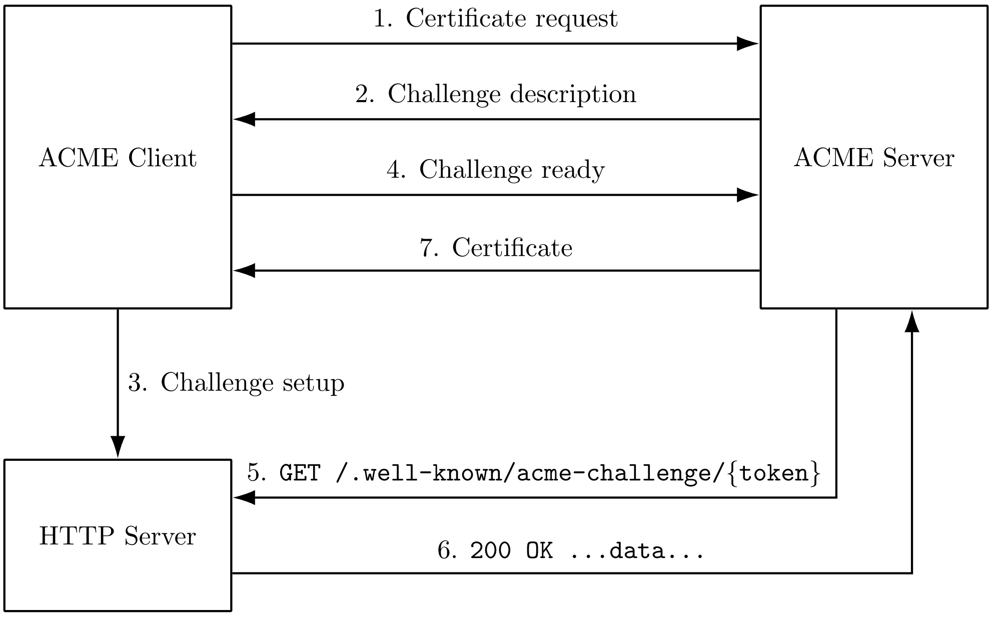

Figure 1: Schematic representation of the protocol flow of the HTTP ACME challenge. The communication between the ACME Client and ACME Server uses `HTTPS`. The GET request from the ACME Server to the HTTP Server uses `HTTP`.

(a) (9 points) You want to a acquire a certificate for `netsec.coin`. You decide to use a free Let's Encrypt *Domain Validation (DV)* certificate. Let's Encrypt certificates are issued using *Automated Certificate Management Environment (ACME)*. In summary, ACME works as follows: the client sends a certificate request to an ACME server (operated by the CA), which responds with a challenge that the client has to complete to prove that it has control over the domain for which it requests the certificate. Once the ACME server has verified that the client executed the challenge correctly, it will issue the certificate to the client.

The current ACME specification draft specifies —among others, the `HTTP` challenge, in which the domain has to serve a file with specific content at the following URL: `http://{domain}/.well-known/acme-challenge/{token}`, where the value of the token is determined by the ACME server. The protocol flow when using this challenge is shown in Figure 1.

i. (1 point) What is the reason that step 5 and 6 in Figure 1 use `HTTP` rather than `HTTPS`?

Solution: Because the server does not have a certificate— yet, `HTTPS` can not be used yet. OR: Arguing that using a cert (e.g. self signed) at this point would not add any security. **Grading Scheme:** =1 point for reason

ii. (2 points) Eve is a passive network level attacker. That is, she can *only* eavesdrop on the communication. Can she exploit the HTTP challenge to obtain a certificate and corresponding private key for `netsec.coin`? If yes, describe an attack. If no, argue why not.

Solution: No, the HTTP Challenge is secure against passive network level adversaries. The token and file content do not reveal any information about the web server's private key. **Grading Scheme:**

- +.5 points for No,
- +.5 Points for cert is sent over `HTTPS`
- +.5 points for challenge useless to attacker
- =2 points if all previous mentioned
- =2 points for mentioning private key never leaves client
- -.5 points if said that cert can be eavesdropped on

iii. (3 points) Mallory is an active network level attacker. She has all the capabilities of Eve, but can also drop, modify, reroute and inject packets. Can she exploit the HTTP challenge to obtain a certificate and corresponding private key for `netsec.coin`? If yes, describe an attack. If no, argue why not.

Solution: Yes, for example consider the following attack:

1. M requests a certificate for `netsec.coin`.
2. M receives the challenge from the ACME server.
3. M informs the ACME server that the challenge is ready.
4. M intercepts the GET request from the ACME server to `netsec.coin`.
5. M responds with the challenge to the ACME server.
6. M receives the certificate from the ACME server.

Grading Scheme:

- +.5 point for yes
- +1.5 points MiTM / spoofing of HTTP server
- +1 point for running ACME client
  OR +.5 points for MiTM ACME server
- =3 points for running ACME client + spoofing web server

iv. (3 points) Besides a certificate for `netsec.coin`, you also request certificates for `secret.netsec.coin`, `internal.netsec.coin` and `blog.netsec.coin`. The former two subdomains are for private use within your company only, the latter is a public blog. Let's Encrypt automatically records all certificates it creates in a *Certificate Transparency (CT)* log. Explain how this can be problematic, and name one way that you can work around this issue.

Solution: Recording these certificates in a public CT log leaks information about the existence of those domains. This information can be used by attackers.
Possible solutions:

- use a wildcard (`*.netsec.coin`) certificate.

- use a self signed certificate, and manually add it to all the computers in the company.
- set up an “internal CA”
- use a CA that does not enforce CT.
- Properly secure the internal servers (e.g. FW / client authentication)

Grading Scheme:

- +1 point for pointing out log is public & leaks info
- +2 points for good solution
- +1 point for self signed certs, but not mentioning that they must be added to all company computers.

(b) (3 points) When you configure your web server, you have to configure the `HTTP` server (on port 80) and the `HTTPS` server (on port 443) separately. In order to be user friendly, you enable both the `HTTP` and `HTTPS` server.

i. (1 point) Initially, you configure the `HTTPS` server to serve the wallet system. You configure the `HTTP` server to respond to all requests with a `HTTP 301 Moved Permanently` status code which redirects the client to the `HTTPS` server. Is this a good idea? Motivate your answer.

Solution: Yes, this is a good idea. It transparently forces all clients to use `HTTPS`.
Note: Many students answered that this was *not* a good idea, as it would open the door for MiTM attacks on the initial `HTTP` request. It is true that the `HTTP` request can be MiTM'ed. However, not running a `HTTP` server would not solve this, as the request would still be sent, and the attacker could intercept it and respond to it.
However: A valid argument would be that data (path, parameters, ...) in the initial request could be leaked by doing the `HTTP` request, and that not running the `HTTP` server would mean that the TCP session would never be opened, and thus the request would never be made. We gave points for this reasoning too. (as a side note, an active attacker could still pretend to be the `HTTP` server, open a TCP connection with the victim and receive the `HTTP` request.)
Grading Scheme: =1 point if yes AND a good reason

ii. (2 points) The next day, you get a call from your friend who works at *MicroCorp*. He tells you that his company intercepts and scans all `HTTPS` connections (they do this by installing a custom root certificate on all company-owned computers), and that he therefore would rather use `HTTP` to browse your website. He suggests to let the `HTTP` and `HTTPS` server *both* serve the wallet system, so that users can choose between `HTTP` and `HTTPS` themselves. Is this a good idea? Motivate your answer.

Solution: This is a bad idea, your friend is an idiot.
Possible reasons why this is a bad idea:

- Using `HTTP` would not prevent his company from eavesdropping on his connection.
- There is no good reason to use `HTTP` instead of `HTTPS`, it thus makes more sense to force users to use `HTTPS`.
- Users should not be expected to be educated enough to decide when they do not want to use `HTTPS`.
- Users might browse the website over `HTTP` without being aware that `HTTPS` is also available.

Grading Scheme:

- +.5 points if no
- +1.5 points for reason
- -1 point for clear false statements
- =1 point if reason given is that "downgrade attacks" are made possible

,

(c) (2 points) Assume that you did not follow your friends advice. You notice that the framework you use for your wallet application shows you the following warning:

> The "Strict-Transport-Security" HTTP header is not set to at least "15552000" seconds. For enhanced security, it is recommended to enable HSTS as described in the security tips.

i. (1 point) What is *HTTP Strict Transport Security (HSTS)*?

Solution: HSTS is a security mechanism that allows a website to declare (in a `HTTP` header) that clients should only connect to it using `HTTPS`. Note that it does not 'force' the client to use `HTTPS`, which many of you wrote (but we gave points for it anyway).
Grading Scheme:

- =1 point if mentioned that it instructs clients to only use `HTTPS`
- =.5 points if claimed that server 'rejects' `HTTP` connections

ii. (1 point) As your web server is already configured to redirect all `HTTP` traffic to `HTTPS`, is there still an advantage to using HSTS? Motivate your answer.

Solution: Yes, it can help prevent TLS-stripping man-in-the-middle attacks. **Grading Scheme:** =1 point for yes and mention of prevented attack

(d) (2 points) You notice that the default TLS cipher suites used by your web server are outdated, and you want to manually specify which suites to use. For each of the following cipher suites, indicate wether they provide the stated properties. (For each cipher suite: 1 point if all correct, 0 points if one or more wrong.)

i. (1 point) *RSA with a signing only key* with *256-bit AES in Galois/Counter Mode (GCM)* (GCM is an *authenticated encryption with associated data (AEAD)* encryption algorithm.).

√ **Secure against passive attackers.**

√ **Secure against active attackers.**

√ **Offers perfect forward secrecy.**

□ Has contributory key agreement.

Solution: Because fixed RSA with a signing only key is used, there is no contributory key agreement. 256-bit AES-GCM is secure, and provides both secrecy and authenticity. **Grading Scheme:** =1 point if *all* correct

ii. (1 point) *Ephemeral Diffie-Hellman* with *40-bit DES* encryption and a *384-bit SHA-2* based MAC algorithm.

□ Secure against passive attackers.

□ Secure against active attackers.

√ **Offers perfect forward secrecy.**

√ **Has contributory key agreement.**

Solution: 40-bit DES is very insecure, and therefore the protocol is neither secure against active or passive attackers. However, when the server's long term key is leaked, this does not reveal the session keys (each 40-bit session key must be individually cracked), therefore this cipher suite does offer PFS. **Grading Scheme:** =1 point if *all* correct

(e) (5 points) In order to improve user experience, you decide to also enable TLS 1.3 with 0-RTT session resumption. As a reminder, a TLS 1.3 handshake with 0-RTT data is shown in Figure 2.

i. (1 point) What do the g^c and g^s in the handshake represent?

Solution: g^c and g^s are the client's and server's DH parameters. **Grading Scheme:**

- =1 point for DH parameters.
- =.5 points for 'public keys'
- =1 point for explaining how DH works

ii. (2 points) Can g^c and g^s be left out of the handshake? If not, why not? And if yes, what impact does that have?

Solution: Yes, g^c and g^s are optional. When they are not sent (and thus no DH handshake takes place), the session has no PFS. **Grading Scheme:**

- +.5 point for yes
- +1.5 point for no PFS
- -1 point for clearly false statements

iii. (2 points) In order to save memory on your servers, you decide to close each TCP session after 1 second of inactivity. Effectively, this means that for each user request, you have to reopen the TCP session. Because you use 0-RTT session resumption, this does not result in increased latency. For example, a request to transfer funds from one account to another now looks as in Figure 3. Is this secure? Motivate your answer.

Solution: No, this is not secure. 0-RTT data is not replay protected, and therefore should only be used for idempotent requests. **Grading Scheme:** +.5 point for not secure, +1.5 points for no replay protection

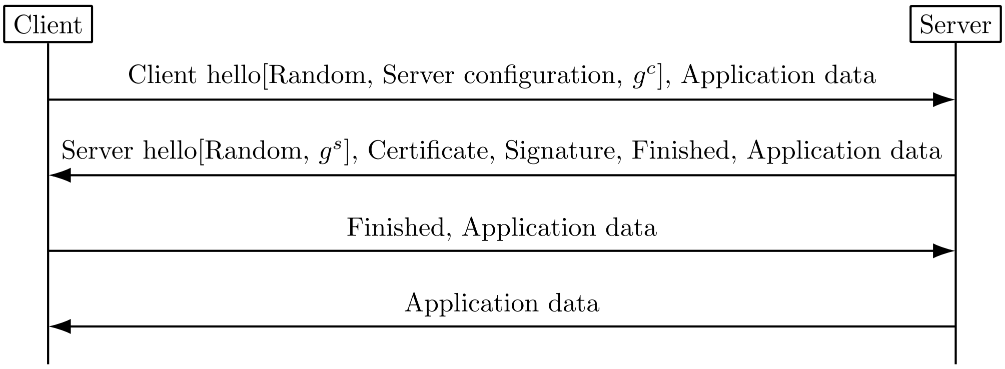
Client
Server
Client hello[Random, Server configuration, g^c], Application data
Server hello[Random, g^s], Certificate, Signature, Finished, Application data
Finished, Application data
Application data

Figure 2: Schematic representation of a TLS 1.3 handshake with session resumption and 0-RTT data.

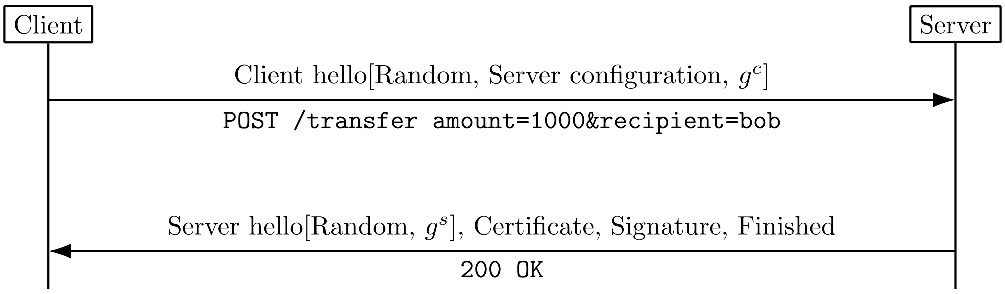
Client
Server
Client hello[Random, Server configuration, g^c]
POST /transfer amount=1000&recipient=bob
Server hello[Random, g^s], Certificate, Signature, Finished
200 OK

Figure 3: Schematic representation of the interaction between the client and server to transfer 1000 PRC. Application data is shown bellow the arrows.

2. Firewalls & Intrusion Detection Systems (17 points)

Consider the network topology shown in Figure 4 with 4 network segments connected to the Internet, and depicting a DNS server on the public Internet as well as mail, web and database servers on the corporate networks. Answer the following questions.

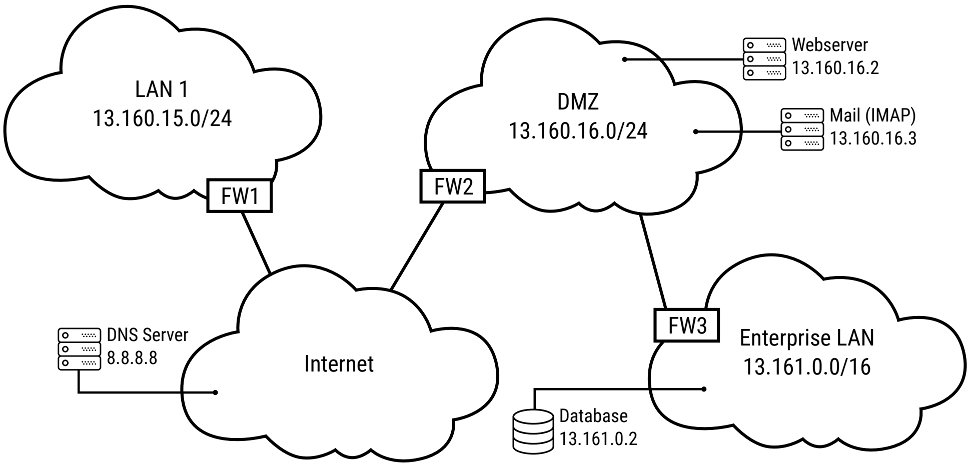

Figure 4: Network topology with 4 corporate networks with connections to the Internet. Firewalls are denoted 'FW'.

(a) (2 points) Consider the stateless firewall rules shown below, for a (host) firewall located on the web-server in Figure 4. The ACK column indicates that the rule matches when the ACK flag of TCP packets is set.

	Direction	Src. Addr.	Src. Port	Dest. Addr.	Dest. Port	Protocol	ACK	Action
1	Ingress	Any	> 1023	13.160.16.2	22	TCP	Any	Allow
2	Ingress	Any	> 1023	13.160.16.2	80	TCP	Any	Allow
3	Egress	13.160.16.2	80	Any	> 1023	TCP	Yes	Allow
4	Either	Any	Any	Any	Any	Any	Any	Reject
5	Egress	13.160.16.2	22	Any	> 1023	TCP	Yes	Allow

For each of the following statements answer **true** if the rules would permit the **webserver** to perform the following operations, and false otherwise. Consider only the host firewall. Each correct answer gives 0.5 points. Each incorrect answer removes 0.5 points. No answer gives 0 points. You will receive a minimum of 0 points on this question (that is, if your total for this question is negative, you will receive zero points instead).

true false
□ ☒ Perform a DNS query (port 53).

Solution: No UDP traffic is permitted.

true false
□ ☒ Establish an SSH session (port 22).

Solution: The SYN/ACK from the remote host is blocked as rule 5 follows the default reject rule.

true false
☒ □ Receive and respond to requests via HTTP.

Solution: Rules 2 and 3 allow for this.

true	false	
□	☒	Ping a host located in LAN 1.

Solution: Ping is handled by ICMP packets which are not permitted.

(b) (3 points) What is the difference between 'drop' and 'reject' in denying access to a packet? Describe one advantage of each over the other.

Solution: Drop silently drops the packet whereas reject sends an ICMP error message (or RST for TCP if the firewall is TCP aware) **(1 point)**. Reject is more transparent and can help with debugging connectivity issues **(1 point)**, but drop provides less information to adversaries which are gathering information about the network **(1 point)**.

1 point can also be awarded for a bandwidth argument for drop given the load of a DDoS attack, in the typical case, the bandwidth and processing overhead to send an ICMP packet is trivial.

Note that drop does not prevent scanning altogether, but it may increase the scan time of naïve scanners and provides ambiguity as to whether a UDP port is open or filtered by a firewall.

-0.25 points for claiming that reject sends back only an RST message, as this does not apply to most protocols.

(c) (6 points) You are tasked with designing the firewall policy for the network presented in Figure 4. The firewalls enumerated in the diagram, FW 1 through 3, are *stateful firewalls*. Connection states in the firewall can be one of the following:

- *N* for new - the packet is initiating a new connection or is otherwise associated with a connection which has not seen packets in both directions
- *E* for established - the packet is associated with a connection which has seen packets in both directions
- *N,E* - the rule applies to both of the above.

Consider the following set of requirements for the network traffic. For each requirement, fill in a suitable **ingress** policy which satisfies it. All rules are by default **ingress, TCP** and **allow** and the default ingress action is **reject**. The first one is done for you as an example. *Again, please provide only the **ingress** policies.*

i. Every host should be able to query the web server (ports 80 & 443).

FW	Source Address	Src. Port	Destination Address	Dest. Port	State
1	13.160.16.2	80, 443	13.160.15.0/24	> 1023	E
3	13.160.16.2	80, 443	13.161.0.0/16	> 1023	E
2	Any	> 1023	13.160.16.2	80, 433	N, E

ii. (3 points) Hosts in LAN 1 and the Enterprise LAN should be able to establish communication with the IMAP server over TLS (port 993). Additionally, the mail server should be able to receive mail on port 25 from the Internet.

FW	Source Address	Src. Port	Destination Address	Dest. Port	State
1	13.160.16.3	993	13.160.15.0/24	> 1023	E
3	13.160.16.3	993	13.161.0.0/16	> 1023	E
2	13.160.15.0/24	> 1023	13.160.16.3	993	N, E
2	Any	25	13.160.16.3	25	N, E

iii. (3 points) Hosts in LAN 1 and the webserver should be able to establish communication with the database server (port 66).

FW	Source Address	Src. Port	Destination Address	Dest. Port	State
1	13.161.0.2	66	13.160.15.0/24	Any	E
2, 3	13.160.15.0/24	Any	13.161.0.2	66	N, E
3	13.160.16.2	Any	13.161.0.2	66	N, E

Solution: **-0.5 points** are subtracted up to a maximum of **-1 points** for overly permissive rules (O.P.). This applies when a valid rule is overly permissive, or all solution rules are present and additional rules are provided.

-0.25 points are subtracted for incorrect ports and states. Additionally, in cases where it was clear that the student may have misinterpreted the 'FW' column, **-0.25 points** may be subtracted for invalid 'FW' values on otherwise possible solutions.

(d) (6 points) Corporate management has decided to increase security to the Enterprise LAN by adding an Intrusion Detection System (IDS) to FW3. They have been presented with two options, IDS-A and IDS-B. IDS-A relies predominantly on signatures whilst IDS-B utilises a combination of machine learning and sandboxing.

i. (2 points) Contrast (differentiate between) a reactive and proactive IDS and classify the above as either reactive or proactive.

Solution: A reactive IDS can only detect known attacks whereas a proactive IDS can additionally detect yet unknown attacks **(1 point)**. IDS-A is reactive **(0.5 points)** and IDS-B is proactive **(0.5 points)**.

ii. (1 point) Which IDS would have a lower impact on performance and why?

Solution: IDS-A would have a lower impact on performance as signature matching is significantly faster than sandboxing **(1 point)**.

iii. (1 point) Define *false-positives* and *false-negatives* as they relate to IDSs.

Solution: A false positive occurs when the IDS classifies benign traffic as an intrusion **(0.5 points)** and a false negative when it fails to classify an intrusion as such **(0.5 points)**
-0.25 points if the answer defines FP & FN in terms of IPSes.

iv. (2 points) For a given exploit, IDS-B has false positive of 1% and a false negative of 2% whereas IDS-A has a false postive of 3% and a false negative of 0%. Which IDS would you recommend and why, given that the organization is not in a critical infrastructure sector?

Solution: IDS-B **(0.5 points)** could be recommended on the basis that it has lower false positives which would result in less human time required to inspect 3x as many false alarms **(1.5 points)**. **0 points** for justifications which confuse IDSes and IPSes. Note that given the likelihood of a given exploit in comparison to even single user traffic volumes, the additional work for to check each alert far outweighs the benefit of a 2% increased accuracy in identification.

3. Blockchain (5 points)

(a) (1 point) What is the primary advantage of Proof of Stake over Proof of Work in blockchains?

> **Solution:** Proof of Stake selects the consensus leader, who extends the Blockchain, probabilistically thus avoiding the resource intensive computation in Proof of Work which may be considered a waste of resources **(1 point)**.

(b) (2 points) A 0-confirmation transaction in Bitcoin is a transaction which is considered confirmed by a merchant despite not yet being appended to the blockchain. Typically the merchant would only wait a number of seconds in an attempt to spot any attempts at double spending.

What benefit do 0-confirmation transactions offer and why would they considered a dangerous practice?

> **Solution:** 0-confirmation transactions allow the merchant to serve the purchase more quickly than when waiting for the transaction to be n-blocks deep on the Blockchain **(1 point)**. Unfortunately as consensus is based on agreeing on the longest chain, it is still possible that the transaction many not make it into the longest chain and would be revered **(1 point)**.

(c) (2 points) Consider the AS-level topology shown in Figure 5 displaying a Bitcoin *delay attack* on node C in the Bitcoin network.

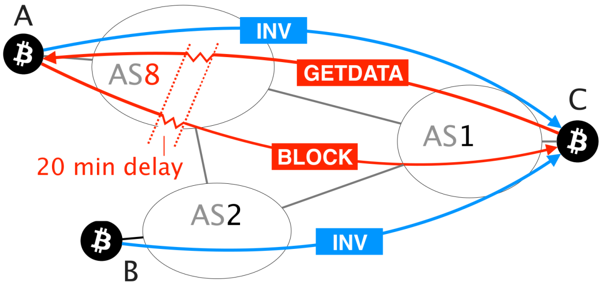

Figure 5: AS topology depicting a Bitcoin delay attack by malicious AS #8.

The adversary, AS8, intercepts a `GETDATA` message for a transaction block from node C to A and modifies it to request a different block. On receiving the older block, C ignores it and continues to wait for up to 20 minutes for the requested block to be delivered, before disconnecting and requesting the block from B. Shortly before the 20 minutes has elapsed, AS8 triggers its delivery by modifying another `GETDATA` block from C to A to request the missing block, thereby keeping the connection alive.

Consider the case where C is a merchant which uses 0-confirmation transactions with a wait period of 10-seconds. Describe how the delay attack mentioned above could be used to launch a double spending attack on the merchant.

> **Solution:** An adversary could make a purchase with their Bitcoin and delay C's receiving the block containing that transaction. While delayed, the adversary could then spend this Bitcoin with C who would authorize the transaction before receiving the block detailing the already spent coin **(2 points)**
>
> Note that after spending at the merchant the transaction will be propagated throughout the network and will reside in the mempool of a majority of the nodes after about 10 seconds. Attempting to then spend a second time with another node will only then be possible if the transaction is eventually not added to the longest chain.

4. Anonymous Communication (14 points)

(a) (6 points) **Adversarial scenarios for Tor.** Alice is a privacy-enthusiast and runs most of her computer's traffic over the Tor network. In particular, all her web-browsing traffic uses sessions running within a *single* Tor circuit. She has identified an entry guard (G) and an exit node (E) which she thinks she can trust and uses for all her traffic. However, she sometimes wonders how bad it would be if G and/or E were actually malicious or compromised...

For the following three scenarios that violate Alice's trust assumptions, describe what information the adversary could gain, and whether it could be sufficient to deanonymize some/all of Alice's traffic. If deanonymization is possible, briefly describe how and under what circumstances.

i. (2 points) The entry guard (G) is compromised.

> **Solution:** The adversary knows Alice's identity and can observe all of her traffic patterns **(1 point for either)**. The adversary may be able to deanonymize some web traffic by performing a website fingerprinting attack **(1 point)**, especially if that is the only traffic traversing the relay at the time **(1 point)**.
> **Grading:** Maximum 2 points. Very unlikely/inefficient attacks (e.g., assuming that Alice is the only Tor user at some point) only get **0.5 points**. Deduct **0.5–1 points** for traffic analysis attacks that are outside the usual Tor threat model (e.g., the adversary is a GPA), depending on how well it is motivated.

ii. (2 points) The exit node (E) is compromised.

> **Solution:** The exit node knows all the websites Alice visits and hosts she contacts, and knows that they originate from a single entity because the same circuit is used for all traffic; the adversary can even read the content if HTTP or similar is used **(0.5 points for one, 1 point for $\geq$two)**. If Alice were to reveal her identity at a higher layer (e.g., by connecting to her own website that nobody else visits) then *all* her traffic would be deanonymized **(1 point)**.
> **Grading:** Deduct **0.5–1 points** for traffic analysis attacks that are outside the usual Tor threat model (e.g., the adversary is a GPA), depending on how well it is motivated.

iii. (2 points) Both entry guard (G) and exit node (E) are compromised.

> **Solution:** In this case, besides the attacks mentioned above, G and E can work together to deanonymize *all* of Alice's traffic **(1 point)** by performing a (passive/active) *traffic analysis attack* or an *intersection/statistical disclosure attack* **(1 point)**.
> **Grading:** Deduct **1 point** for (explicitly) considering only the case of a compromised middle node.

(b) (8 points) **Botnet CnC over Tor.** You are the proud owner of a large botnet, and so far you have been managing it in the traditional way, using the typical layered command and control (CnC) architecture, and DNS fast flux to recover from take-downs of the domains used for CnC. However, recently you have been looking into switching to a new system based on *Tor hidden services.* The idea is to create a hidden service and use it for CnC, leveraging the inherent take-down resilience of hidden service directories (the Tor relays that store the lists of introduction points for hidden services). All bots would directly connect to your hidden service over Tor, and the hidden service itself would run directly on the servers in your basement.

i. (2.5 points) How would the new system fare in terms of your *anonymity* (with respect to law enforcement) compared to the system you are currently using? Motivate your answer.

> **Solution:** Your anonymity would be similar or worse in the new system **(0.5 points)**, because with traditional CnC you also have multiple layers of indirection, like using Tor, and additionally in the traditional system the list of indirection points (a subset of

the list of bots) is not well known, can change continuously as more bots are infected, and are with higher likelihood not under the control of law enforcement **(2 points)**.

Grading: The following alternative answers are awarded partial points:

- **1 point** Traffic coming from the house is recognizable by law enforcement (this is not the main issue, and law enf. still needs to somehow get the warrant).
- **1 point** DNS info needs to be updated, which leads to an additional deanonymization channel (there are ways to do anonymous registrations, and this does not address the main issue).
- **1 point** In Tor anonymity is better because of the other flows helping to hide your traffic (bots in a botnet also exchange other traffic with other machines, and Tor relays are more likely to be compromised).

ii. (2 points) How would the new system fare in terms of *management effort* compared to the system you are currently using? Motivate your answer.

Solution: The management effort is lower **(0.5 points)** since using Tor all the layered architecture for CnC in the traditional system is replaced by Tor relays, and the management of these is not the responsibility of the botnet owner anymore. Also, the overhead of having to frequently register new domains is removed **(1.5 points for either)**.

Grading: Saying that effort is needed to manage the basement server and keep the available, since there are no intermediate layers to fall back upon, gets **1 point** (one needs machines from which to manage the botnet anyway, and there are other significant downsides that this answer ignores).

iii. (2 points) How would the new system fare in terms of *performance*, intended on one hand as (**1**) time for a bot to connect to CnC, and on the other hand as (**2**) time for you to send an instruction to a connected bot from your basement servers, compared to the system you are currently using? Motivate your answer.

Solution: For (**1**), performance would be worse, because the bot needs to establish the Tor circuit which takes significant time (due to telescopic setup and per-hop asymmetric crypto), compared to the bot just directly connecting to one of the servers on the most external layer of the CnC architecture **(1 point)**.

For (**2**), it depends on how many layers there are in your CnC architecture, and how performant the bots are compared to the Tor relays **(1 point)**, though in general the traditional approach has the potential to be better.

Grading: The following alternative answers are awarded points:

- **1 point** Centralization may be a performance issue if the setup is not sufficiently scalable, since all connections are coming to a central point (the servers could be provisioned to handle the load, and multiple HS names could be used).
- **0–0.5 points** The new system is worse because it requires circuits and multiple layers (incorrect assumption that no layers are used in the traditional architecture).
- **0.5 points** For **(1)**, performance might be better because the bots do not need to look up many domains (this only happens for a new bot that doesn't have state, and it only takes a few DNS requests, which can be issued in parallel).

iv. (1.5 points) How would the new system fare in terms of *identifiability* of the bots (how easy it is for the owner of a host to detect that the host is infected) compared to the system you are currently using? Motivate your answer.

Solution: It would become much easier to identify bots in the Tor-based system, because it is a type of traffic that is otherwise basically never used (except when the host owner is using the Tor browser, or some other anonymity-based software, which is rarely the case) **(1.5 points)**.

Grading: The following alternative answers are awarded partial points:

- **0.5–1 points** Detection is more difficult because in the old case there are recognizable DNS queries (Tor has many highly recognizable features as well, while DNS is commonly used by many different applications).
- **0.5 points** The owner can detect Tor based on the power consumption of the bot (this is very hard to do in almost all circumstances, and doesn't work in cases where the bot is a normal host, only for low-end IoT devices.

5. DNS and DNSSEC (15 points)

(a) (6 points) **CIA for DNS and DNSSEC.** The CIA triad identifies three fundamental security properties: *confidentiality*, *integrity* (with respect to adversarial manipulation), and *availability.*

i. (2 points) For each property of the CIA triad, say whether DNS (protocol and/or infrastructure) contains measures towards achieving that property, and if it does, briefly state what those measures are.

> **Solution:** Confidentiality is not provided **(0.5 points)**, queries and responses are sent in cleartext. Integrity is also not provided **(0.5 points)**, no MAC or signature is used, so queries and responses can be modified by an on-path adversary. Availability is provided **(0.5 points)** through the hierarchical architecture of DNS, and the redundancy in the root and TLDs **(0.5 points for either)**.

ii. (2 points) Briefly explain how DNSSEC improves on DNS in terms of the CIA properties.

> **Solution:** DNSSEC adds integrity **(0.5 points)** by introducing record signatures and new public key and delegation records which allow a resolver to verify the record based on a chain of signatures up to a trust root (the root KSK) **(1.5 points** for knowing the important elements of DNS, **1 point** for knowing about signed records**, 0.5 points** for more vague answers**)**. Deduct **0.5–1** for stating that confidentiality is added.

iii. (2 points) Assume we were to redesign DNS from scratch, both protocol and architecture (with our new DNS having the same role in the Internet ecosystem as the current DNS). Rank the priority (from highest to lowest) that the CIA properties would have in our new design, motivating your choice.

> **Solution:** The most important property for a vital component such as DNS always has to be availability, since it needs to be able to sustain very large volumes of traffic (whether malicious or not), and if it were to fail, almost the entire Internet would be paralyzed **(1 point)**. Integrity is also important to counter attacks, but today's DNS is a good example of how the system can work well even without (strong) integrity measures **0.5 points**. Confidentiality of the DNS data is not a concern in most cases; privacy of users is a concern, but in most scenarios an adversary who sees cleartext queries also sees subsequent connections, which reveal (almost) the same amount of information**(0.5 points)**.
> **Grading:** The order is not that important as long as the motivations provided are solid and the order is argued. Deduct **0.5 points** for not arguing the order. No points for tautologies/vague answers such as "confidentiality is important because it gives us privacy", or "we want integrity to be secure."

(b) (4 points) **DNS over HTTPS (DOH).** A working group of the IETF is currently standardizing the use of DNS over HTTPS (DOH). It is meant to be used mainly between stub resolvers (clients) and recursive resolvers. The client would open a TLS connection to the resolver, and then send the query and obtain the response over HTTPS (possibly with a different format for encoding queries and responses than in DNS).

i. (3 points) For each one of the CIA properties (see Question 5.a), name either an advantage *or* a disadvantage of using DOH in terms of that property.

> **Solution:** DOH provides confidentiality **(0.5 points)** prevents an network adversary between the stub and the recursive resolver from learning what queries a client makes **0.5 points**.
> DOH provides integrity **(0.5 points)** w.r.t. a local adversary (but not w.r.t. a compromised resolver, or other adversary located beyond the recursive resolver) **(0.5 points)**.

DOH can also affect availability: TLS is complex and may fail due to certificate errors, so if no DNS fallback is possible availability is negatively affected **(1 point)**. *Alternative*: TLS requires more resources, and is therefore more vulnerable to DoS (state exhaustion) attacks **(1 point)**. *Alternative*: in some networks, middleboxes could mess with UDP or protocols other than the very common HTTPS protocol, so DOH could help **(1 point)**.
Grading: For availability, the following gets only **0.5 points**: saying that no source spoofing is possible, which prevents reflection-based amplification attacks (it is typically still possible to leverage authoritative NSes).

ii. (1 point) A company decides to make DOH to the company's recursive resolver mandatory for all the devices in its intranet, blocking DNS. From the company's perspective, why is this beneficial *for security*?

Solution: It is beneficial both for integrity and confidentiality: for the former, it prevents hijacking attacks, and for the latter, it prevents eavesdropping **(0.5 points)**. In both cases, the threat model is that of a malicious insider, e.g., a disgruntled employee or a compromised host **(0.5 points)**.

(c) (5 points) **DOH and DNSSEC.** *(Related to previous question.)* Assume now that also authoritative name servers begin to support DNS over HTTPS (DOH), allowing recursive resolvers (and also clients) to connect to them via DOH to do DNS lookups over HTTPS.

i. (2 points) Assume that all authoritative name servers support DOH: does this have a significant *performance overhead* for the name servers compared to them just supporting the usual DNS and DNSSEC? Motivate your answer.

Solution: DOH has two main performance drawbacks: first, it requires multiple round-trips to perform the TCP and TLS handshakes, second, it requires the use of online asymmetric cryptography, which DNSSEC is designed to avoid **(2 points for either)**.
Grading: The following alternative answers are awarded partial points:

- **0.5 points** if only symmetric cryptography is mentioned, **+0.5** if it's explained in detail, saying that the setup can be amortized over multiple sessions.
- **0.5 points** for mentioning only TCP or state overhead (TLS is more important, state does not necessarily impact performance, and DNSSEC also often uses TCP).
- **1 point** for stating only that a TLS session has to be opened (too vague, unclear where the overhead actually comes from).
- **1 point** for stating that the overhead is negligible as long as connections are kept open (this does not apply to 2nd level domains that are not accessed frequently).

ii. (3 points) Assume that, despite any possible performance problem, all authoritative name servers decide to support DOH: would DNSSEC become completely superfluous? Motivate your answer.

Solution: Grading: The following answers are awarded points (cumulative):

- **2 points** Unless DOH is used directly from client to authorities—the client does full recursive lookup—there is no protection against a malicious recursive resolver.
- **2 points** The many root of trust of the TLS PKI are a problem, as it is more likely that one is compromised, and DNSSEC further provides the guarantee of a unique view of the namespace.
- **2 points** DOH does not allow transferability of authenticity proofs, meaning that caching by untrusted entities is not possible. DNSSEC provides this and offers accountability.
- A hacked authority server could be made to serve fake records **(1 point)** which is not possible in DNSSEC if the record signing is done offline/not on that server **(1 point)**. (Same applies to hosted DNS scenario.)

- **1.5 points** DNSSEC is backwards compatible, good if not all clients switch at once.
- **1 point** A malicious authority could reply with records for which it is not autoritative (could be prevented if recursion is done properly).
- **1 point** DNSSEC is useful because would be faster.
- **0.5 points** Unifying the roots of trust of DNSSEC and HTTPS could be undesirable (no security in depth).

6. SCION (8 points)

(a) (3 points) **Comparing to BGP.** Answer the following questions that compare SCION and BGP.

i. (1 point) One key property of BGP is that ASes can perform traffic engineering to some degree by manipulating BGP announcements. In SCION, how do ASes control how packets are routed?

Solution: ASes can choose to which customers and peers to forward which beacons, but in the end it is the sources that determine the final path.
Grading Scheme:

- +.5 points for choosing which beacons to forward
- +.5 points for source has final say

ii. (1 point) BGP may suffer from temporary unavailability during route convergence. How does SCION avoid such a problem?

Solution:

- Separation between routing and forwarding plane OR
- Forwarding state is carried in the packet and it is put into the packet by the source. It is not affected by routing updates and it does not change en route.

Grading Scheme: 1 point for good reason.

iii. (1 point) Describe an advantage of SCION routers compared to BGP routers.

Solution:

- SCION routers do not require TCAM, which are expensive and consume a lot of energy.
- SCION routers are faster, because MAC calculation is faster than table lookup.
- SCION routers are not vulnerable to path hijacking attacks.

Grading Scheme:

- =1 point for advantages that are directly related to the *router*.
- =0.5 points for simply stating that the routers are “simpler” without a reason why.

(b) (5 points) **DRKey and SCMP.**

i. (1 point) SCMP stands for secure ICMP in SCION. What security property does SCMP aim to provide?

Solution:
Source authentication of ICMP messages. **Grading Scheme:** Binary, no points for “integrity”

ii. (4 points) Assume Host **H** in AS **A** sends an SCMP message, and AS **C** that receives this message wants to authenticate this message. Describe how DRKey can be used for this purpose.

Solution:

1. First-level Key Exchange: AS **C** has its local secret SV_C. It uses SV_C to generate the first level key $K_{C \to A} = PRF_{SV_C}(\text{“}A\text{”})$. AS **C** securely sends $K_{C \to A}$ to AS **A**, e.g., encrypts using the private key of AS **C**.
2. Second-level Key Exchange: AS **A** generates a second-level key for **H** that can be used for source authentication by AS **C**, i.e., $K^{SCMP}_{C \to A:H} = PRF_{K_{C \to A}}(\text{“H | SCMP”})$ and gives it to host **H**.
3. Host **H** authenticates its ICMP message using $K^{SCMP}_{C \to A:H}$.
4. AS **C** dynamically recreates $K^{SCMP}_{C \to A:H}$ by retrieving the first-level key that it generated in Step 1 and computing the second-level key that AS **A** computed.
5. Finally it verifies the authenticity of the message.

Grading Scheme:

- +1 for explaining first level key derivation
- +1 for explaining second level key derivation
- +1 for using SCMP specific key
- +1 for explaining first level key sharing
- -1 when explicitly saying that DRKeys are for public key crypto
  (No minus points for confusing signature / MAC)
- Both directions of key derivation have received full marks (i.e. $K_{C \to A}$ and $K_{A \to C}$)