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 **20 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.

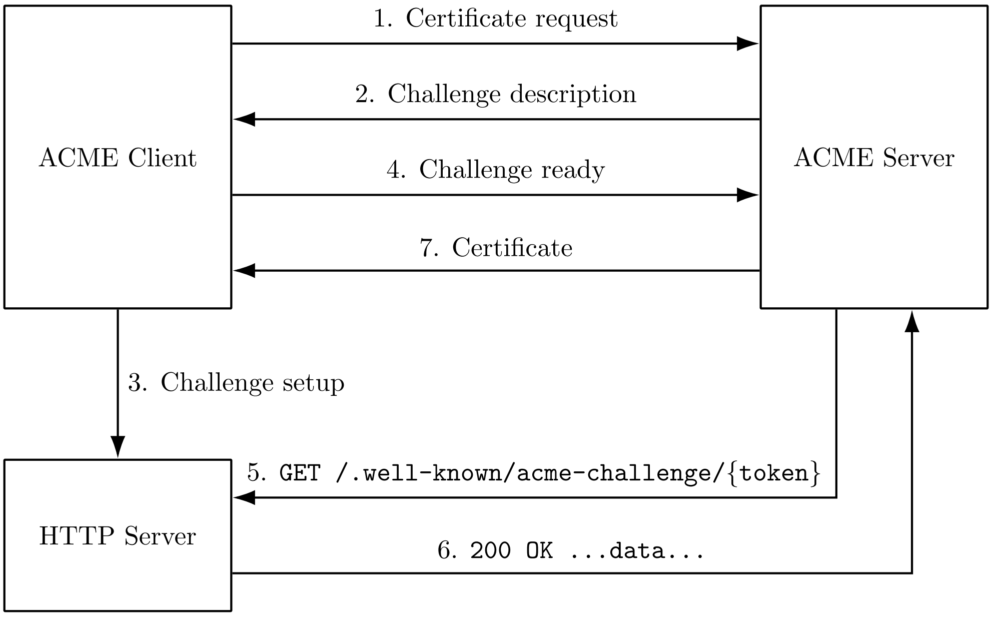


Figure 1: Schematic representation of the protocol flow of the HTTP ACME challenge. The communication between the ACME Client and ACME Server uses `HTTPS`. The GET request from the ACME Server to the HTTP Server uses `HTTP`.

(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`?

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.

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.

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.

(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.

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.

(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)*?

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.

(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.

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.

(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?

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?

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.

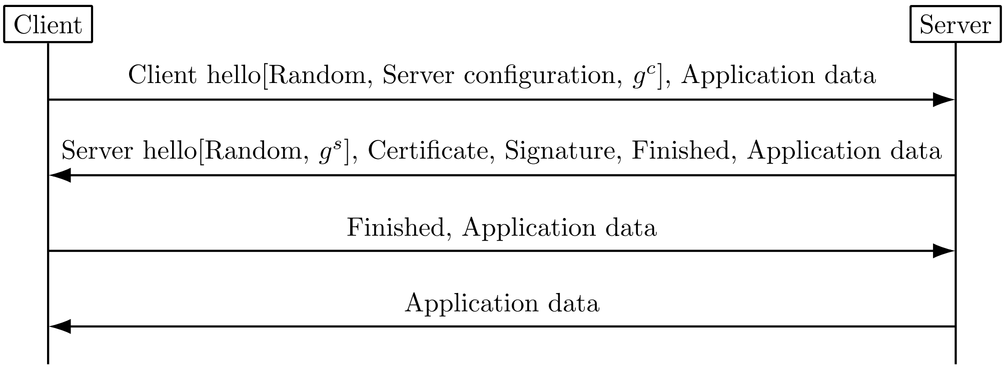
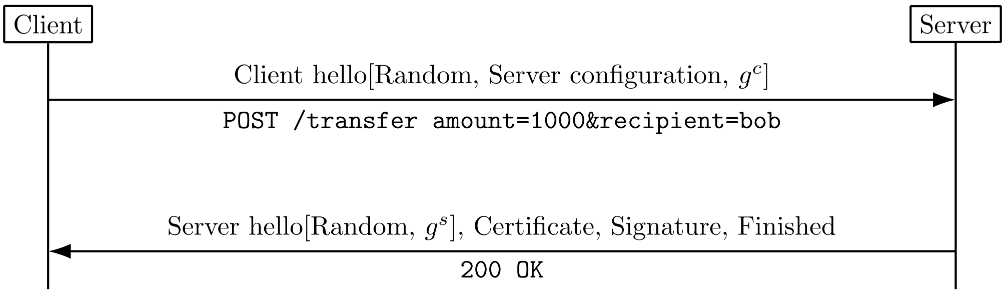

Client
Server
Client hello[Random, Server configuration, g^c], Application data
Server hello[Random, g^s], Certificate, Signature, Finished, Application data
Finished, Application data
Application data

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]
Server hello[Random, g^s], Certificate, Signature, Finished

```
POST /transfer amount=1000&recipient=bob
```

```
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.

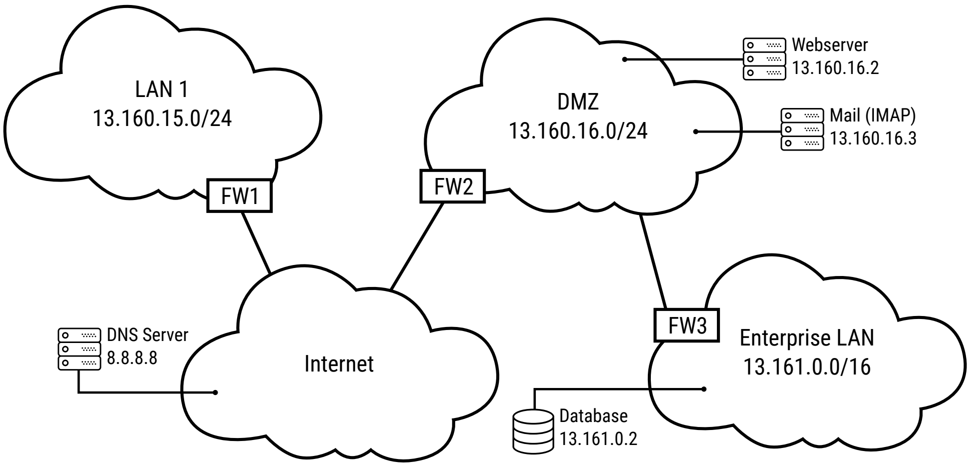


Figure 4: Network topology with 4 corporate networks with connections to the Internet. Firewalls are denoted ‘FW’.

(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).

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

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

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

(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.

(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

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

(d) (6 points) Corporate management has decided to increase security to the Enterprise LAN by adding an Intrusion Detection System (IDS) to FW4. 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.

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

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

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?

3. Blockchain (5 points)

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

(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?

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

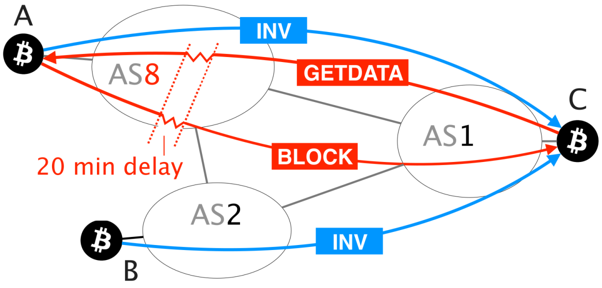


Figure 5: AS topology depicting a Bitcoin delay attack by malicious AS #8.

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.

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.

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

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

(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.

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.

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.

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.

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.

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

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.

(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.

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*?

(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.

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.

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?

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

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

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

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

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.

Extra Page

Please use this page in case you run out of space elsewhere in the exam.

Extra Page

Please use this page in case you run out of space elsewhere in the exam.

Extra Page

Please use this page in case you run out of space elsewhere in the exam.

Extra Page

Please use this page in case you run out of space elsewhere in the exam.