Final Exam

Network Security Autumn 2019

6 February 2020

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 **15 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. The exam has **100 points**.
- 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.
- 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	7	8	9	Total
Points:	16	3	7	17	11	14	11	13	8	100
Score:										

1. Securing SMTP (16 points)

You are hired as a system administrator by a new tech startup that plans to provide a mail service. Your first order of business is to set up a Simple Mail Transfer Protocol (SMTP) server that allows your users to submit new messages.

SMTP is a simple, text based, protocol. A transcript of a user submitting an email to an SMTP server is given below.

```
S: 220 smtp.server.com Ready     // The server indicates that it is
                                    ready to receive a message
C: EHLO client.example.com       // The client identifies itself and
                                    requests the server's abilities
S: 250 smtp.server.com
S: 250 STARTTLS                  // The server advertises
                                    that it supports STARTTLS (see below)
S: 250 AUTH PLAIN                // The server advertises
                                    that it supports user authentication
C: AUTH PLAIN                    // The client requests to authenticate itself
S: 334                           // The server accepts the request
C: dGVzdAB0ZXN0ADEyMzQ=          // The client sends the base64-encoded
                                    username and password
S: 235 2.7.0 Auth. success       // The server accepts the credentials
C: MAIL FROM:bob@example.com     // The client starts sending the mail
C: .... [truncated] ...
```

Two mechanisms can be used to secure an SMTP session. These two mechanism are usually referred to as `Implicit TLS` and `STARTTLS` and work as follows:

- `Implicit TLS` works similar to HTTPS: the SMTP server listens on a separate, TLS-enabled, port and the entire SMTP session is wrapped in TLS.
- `STARTTLS` reuses the standard SMTP port. It allows servers to advertise that they are TLS capable as shown in the transcript above. When communicating with a TLS-capable server, a TLS-capable client can issue the `STARTTLS` command after the client EHLO (Extended Hello). Once the `STARTTLS` command is issued, the client and server will initiate a TLS session which will be used for the remainder of the SMTP exchange.

We will now compare the security of `Implicit TLS` and `STARTTLS`. You may assume that there are no known vulnerabilities in the TLS protocol and implementation.

(a) (4 points) Eve is a passive network level attacker. That is, she can only eavesdrop on the communication between the SMTP client and server.

i. (2 points) Can Eve compromise the confidentiality of an SMTP connection secured by `Implicit TLS`? If yes, how? If no, why not?

ii. (2 points) Can Eve compromise the confidentiality of an SMTP connection when both client and server are configured to negotiate `STARTTLS`? If yes, how? If no, why not?

(b) (6 points) Mallory is an active network level attacker. She has all the capabilities of Eve, but can also drop, modify, reroute and inject packets.

i. (3 points) Can Mallory compromise the confidentiality of an SMTP connection secured by `Implicit TLS`? If yes, how? If no, why not?

ii. (3 points) Can Mallory compromise the confidentiality of an SMTP connection when both client and server are configured to negotiate `STARTTLS`? If yes, how? If no, why not?

(c) (6 points) Because the `STARTTLS` command was not part of the original SMTP specification, old clients might not support it. To prevent clients from sending sensitive data over a clear-text channel, SMTP servers supporting `STARTTLS` can enforce the use of TLS by issuing the error "`530 5.7.0 Must issue a STARTTLS command first`" and then closing the connection when the client does not try to negotiate TLS.

i. (3 points) Is this a foolproof mechanism against passive attackers like Eve? Why (not)? Remember that not all SMTP clients will correctly implement the specification.

ii. (3 points) What would happen if `Implicit TLS` is used? Does the situation change (from a security perspective)? If so, is it improved or worsened? Why?

2. TLS 1.3 (3 points)

TLS 1.3 does not provide replay protection for 0-RTT data.

(a) (3 points) Which of the following mechanisms are sufficient methods to mitigate replay attacks when using TLS 1.3? You may assume that you only have one server.

true false
□ □ Only allowing the use of cipher suites which offer perfect forward secrecy (PFS).

true false
□ □ Verifying that the timestamp in the `ClientHello` message lays less than one RTT in the past.

true false
□ □ Verifying that the timestamp in the `ClientHello` message lays less than two RTTs in the past.

true false
□ □ Keeping track of the nonce value in the `ClientHello`, and ensuring that each nonce is used only once.

true false
□ □ Serving a fully static website.

true false
□ □ Disabling 0-RTT on the server.

3. Certificates and Trust (7 points)

(a) (3 points) Online Certificate Status Protocol (OCSP) stapling allows web servers to pre-fetch OCSP responses and attach ("staple") them to their HTTPS responses. Name two major issues with standard OCSP that are resolved by OCSP stapling.

(b) (4 points) Explain the main difference between the trust model used in DNSSEC and that (typically) used by HTTPS and give a disadvantage of each approach.

4. Probabilistic Counting (17 points)

As part of the network monitoring in the core of a large backbone ISP, you would like to estimate the number of flows on all the routers. Due to the limited storage capacity, you decide to use *probabilistic counting* to obtain an estimate:

Each router hashes the flow tuple of each packet, interpretes the result as a value in the interval $[0, 1)$, and keeps track of the smallest $k = 16$ values (you can assume for this problem that the number of flows, n, is much larger than k).

(a) (2 points) What properties (in addition to being efficiently computable) does a hash function need to have in order to be usable for probabilistic counting?

(b) (2 points) Assume that you have chosen an appropriate hash function, what is the expected value of the kth smallest hash value x_k as a function of the number of flows n? (You can assume $n \gg 1$.)

(c) (2 points) As a hash function, your boss suggests to use the efficient and widely implemented MD5 algorithm. Why is this a bad idea? What could an attacker do to compromise the system?

(d) (3 points) Can an adversary cause a significant *underestimation* of the number of flows (assuming he only contributes a small share to the total number of flows)? If yes, how can he achieve this? If not, why is it not possible?

(e) (3 points) Can an adversary cause a significant *overestimation* of the number of flows (assuming he only contributes a small share to the total number of flows)? If yes, how can he achieve this? If not, why is it not possible?

(f) (2 points) If you absolutely have to use MD5, how could you modify the computation such that it can be used for probabilistic counting?

(g) (3 points) Remember that the variance of the kth smallest value is approximately $\frac{k}{n^2}$ (for large n). What can you conclude about the precision of the estimation when using x_{16} compared to x_1? Which result is more precise and by which factor?

5. VPNs and Anonymous Communication (11 points)

In 2013, Eldo Kim, a student at Harvard University, sent a bomb threat during the exam session in order to delay one of his exams. He was connected to the university's wireless network; wanting to remain anonymous, he used Tor to send the threat email.

We will use this incident to illustrate important concepts of anonymous communication.

(a) (3 points) Even though he was using Tor correctly and sent the email via an anonymous email server, Eldo Kim was very quickly identified as the most likely culprit by the police. He was arrested and confessed to sending the threat email (even though the police did not have hard evidence).

Explain the concept of an *anonymity set* and use this to explain why the student was immediately identified as the culprit.

(b) (2 points) Explain how it is possible for the police and university to identify Tor users based on their network traffic.

For the remainder of this question, let us assume that the student wanted to remain anonymous for less illegal purposes, e.g., for anonymously reporting illegal activity, etc.

(c) (3 points) Name and explain at least two ways in which a Tor user intending to send an anonymous email can achieve better anonymity compared to Eldo Kim.

(d) (3 points) Using Tor can itself make someone look suspicious. One of your friends thus suggests to simply use a VPN instead. How do you respond, i.e., how do the anonymity guarantees of VPNs compare to Tor? (Name at least two differences.)

6. DNS Security (14 points)

(a) (6 points) For every attack on DNS below, state whether the deployment of DNSSEC would make the attack less effective, equally effective or more effective. Moreover, justify your answer. Only answers that are correctly justified will be awarded points.

i. (1½ points) Reflection/Amplification Attack

ii. (1½ points) Botnet control over DNS

iii. (1½ points) DNS Spoofing

iv. (1½ points) Stefan Frei's TTL Attack

Background: *Before your lecturer Dr. Stefan Frei had to transfer the domains schweiz.ch, suisse.ch and swizzera.ch to the Swiss state, he set the TTL on the old DNS records, which were still pointing to his servers, to 136 years. This information was cached by DNS servers around the world, some of which were still serving the information for weeks after the transfer.*

(b) (3 points) While DNSSEC provides authentication, the communication with a DNSSEC-enabled server is not encrypted and thus not confidential. This lack of confidentiality leads to a range of privacy issues, especially Internet usage monitoring of customers by their ISP.

Given that public keys (DNSKEY records) are already present on a DNS server for verifying record signatures, a privacy-sensitive colleague of yours suggests to use these public keys also to achieve confidentiality.

Your colleague proposes to use TLS with the DNSKEY as the server's public key. After key agreement, the user's DNS request would then be communicated over the TLS-secured connection.

Would this DNSSEC-assisted DNS-over-TLS be a good protocol to enhance DNS privacy? Explain why/why not.

(c) (5 points) The following two questions relate to DNS root name servers, the basic footing of the global DNS infrastructure.

i. (3 points) Name three reasons why root name servers are replicated across the globe.

ii. (2 points) A recent proposal suggests to eliminate DNS root servers altogether and distribute the data that would be on those root servers (i.e., the root zone file) to recursive resolvers.
This proposal has a security benefit for DNS (not DNSSEC). What is the security benefit of this proposal for DNS?

7. Intrusion Detection (11 points)

You are the network engineer of an important stock exchange receiving transactions over the Internet. Since the users of the stock exchange engage in high-frequency trading with large volumes, low latency and high availability are important requirements. However, this stock exchange is also an attractive attack target, thus skilled cybercriminals are constantly attempting to break in and shut down the stock exchange.

(a) (9 points) Given this threat scenario, you have to evaluate different IDS architectures. Name one advantage and disadvantage (each with justification) of each architecture presented below.

i. (3 points) Single signature-based IDS

ii. (3 points) Single sandbox-based IDS

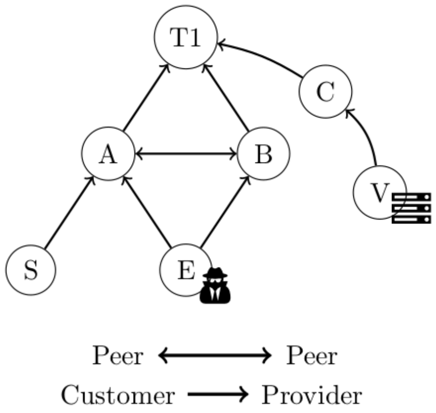
iii. (3 points) Conditional Sequence of IDSs: Signature-based IDS that forwards suspicious traffic to a sandbox-based IDS and bypasses the sandbox-based IDS for unsuspicious traffic

(b) (2 points) While discussing the IDS architecture, you learn that most transactions for the stock exchange come from a handful of trusted stock exchanges and banks.

What kind of IDS solution does this fact enable?

8. BGP Hijacking (13 points)

Consider the inter-domain topology in the Figure. AS E is compromised, and operated by a malicious entity. Assume the standard BGP forwarding rules apply. A refresher of BGP routing is provided in the following.



BGP routing reference
BGP route propagation and forwarding follows business relationships:

1. the announcement for a prefix coming from a customer is propagated to all customers, peers and providers;
2. the announcement for a prefix coming from a provider or a peer is only propagated to customers.

Additionally, if the announcement for two paths to the same prefix are received, they are ranked by their preference. The announcement for the path with the highest preference is then propagated. Preferences are computed in the following way:

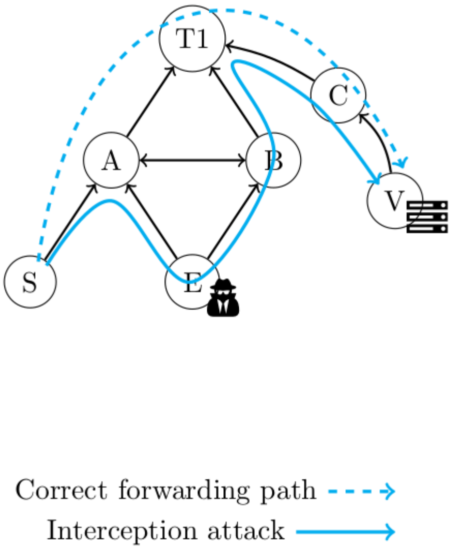
1. forwarding to customers is preferred to forwarding to peers. Forwarding to peers is preferred to forwarding to providers (customers > peers > providers);
2. to break ties, the number of hops in the path is used. Shortest paths have higher preference;
3. further ties are broken using local preferences, that depend on the AS.

(a) (2 points) **Attack A:** The compromised AS E wants to attract all traffic destined to the victim AS V, and originating from ASes A, B and S. The address block announced by AS V is `10.0.0.0/16`. What is the simplest announcement that AS E can make to achieve this goal?

(b) (3 points) **Attack B:** What can you say about the forwarding policy of the Tier-1 AS $T1$? The malicious AS E now wants to attract all traffic destined to a specific server in AS V. The address of the server is `10.0.1.1`. How can AS E modify the announcement from **Attack A** to make sure to attract all the traffic *originating from* AS $T1$ and *destined to* the server?

(c) (3 points) Is origin authentication sufficient to prevent **Attack A**? What about **Attack B**?

This particular type of hijacking is called a *redirection* attack: the hijacked traffic terminates in AS E, and never reaches the correct destination (AS V). The malicious operator, however, now wants to perform an *interception* attack on AS S. The goal is to capture **all the traffic originating from** AS S to the address block `10.0.0.0/16` in AS V, while still being able to forward this traffic through AS B, as in the following figure:



(d) (3 points) Name one use case for redirection attacks, and one for interception attacks.

(e) (2 points) **Attack C:** AS E tries to achieve the interception attack (as in the Figure) by announcing the hijacked prefix only to AS A. AS E is hoping that AS B will use the correct announcement originating in AS V, and received from AS $T1$. Will this work? Why/why not?

9. SCION and Hijacking (8 points)

In the following, consider the SCION Internet architecture *without extensions.*

(a) (2 points) SCION addresses differ from IP addresses. Specifically, which are the parts that compose a SCION address?

(b) (2 points) How is path discovery secured in SCION?

(c) (2 points) How does SCION prevent hijacking attacks from an off-path attacker? (hint: use your answers from the previous 2 questions)

(d) (2 points) On-path attackers can always intercept or drop traffic. What other mechanism provided in SCION can mitigate the effect of an on-path attacker?

Extra Page

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