CS5430: Midterm Examination (Fall 2021)

Name: _____

NetId: _____

Instructions.

- **Enter your name and NetId in the space provided on each page.**
- This examination is closed book, closed notes, and closed neighbor. The use of electronic devices (e.g., laptops, tablets, phones, calculators) is also prohibited, so please turn off these devices and remove them from sight.
- The exam is 16 pages long. Make sure your exam copy includes all pages—sometimes copy machines fail.
- You will have 65 minutes. The point breakdown for each problem is given with the problem.
- Answer each question in the space provided. Use the backs of pages as scrap for performing calculations; backs of pages will not be seen by graders.
- Assume Dolev-Yao attackers throughout.
- Some notational conventions:
  - Encryption of a message m with a key K: $\{m\}K$ or $K\text{-}Enc(m)$.
  - Digital signature of a message m with a signing key k: $\langle m \rangle k$ or $k\text{-}sign(m)$.

Name:	NetId:

Multiple Choice: Write the letter that identifies the <u>best</u> choice in the space provided at the end of each question.

1. [2 points] For a system to have been deemed *trustworthy*, it must

   A. resist attacks.

   B. authenticate requests.

   C. authorize requests.

   D. keep secrets confidential.

   E. be accompanied by an assurance argument.

   1. _____

2. [2 points] Suppose the type system for a new strongly-typed programming language $\mathcal{L}$ has been formalized using axioms and inference rules. The decision to trust any $\mathcal{L}$ program that compiles without type errors is an example of

   A. axiomatic trust.

   B. analytic trust.

   C. synthetic trust.

   D. transitive trust.

   E. language-based trust.

   2. _____

3. [2 points] The Saltzer-Schroeder *Economy of Mechanism* principle says that we should prefer

   A. mechanisms with lower impact on execution speed.

   B. mechanisms requiring smaller amounts of memory.

   C. open source mechanisms because they cost nothing.

   D. easier to understand mechanisms.

   E. mechanism requiring fewer invocations to accomplish some task.

   3. _____

Name:	NetId:

4. [2 points] An implementation of *Separation of Duty* is least likely to depend on

   A. principle of least privilege.

   B. separation of privilege.

   C. failsafe defaults.

   D. defense in depth.

   E. complete mediation.

4. _____

5. [2 points] In the usual symmetric (i.e., shared) key implementation of Kerberos: the KDC has a key K_{KDC} and each of the KDC's clients A has a key K_A. Which other principals know K_{KDC}:

   A. every other client

   B. no other client

   C. only clients that are workstations

   D. only clients that are services

5. _____

6. A web server is being developed to execute in a cloud where each processor has a TPM. For various reasons, the deployment environment does not allow `https`. So the designer has decided to use measured principals and gating functions in the implementation of the web server.

   (a) [2 points] Cookies will be used to store in a client's browser cache whatever state information is required by the server for processing that client's requests. To protect that information, the web server should use:

   A. a sealing key

   B. a quoting key

   C. the public key corresponding to some unbinding key

   D. a client-browser provided public key

   (a) _____

   (b) [2 points] If the web server must compute a response that the client's browser can authenticate, then the web server should use:

   A. a sealing key

   B. a quoting key

   C. the public key corresponding to some unbinding key

   D. a client-browser provided public key

   (b) _____

(c) [2 points] When a client's browser is submitting a request to the web server, if that request contains confidential information then the client's browser should use

A. a sealing key

B. a quoting key

C. the public key corresponding to some unbinding key

D. a client-browser provided public key

(c) _____

7. [2 points] Consider a new processor design that stores and processes numeric information as decimal digits (rather than as binary numbers). On these new processors, there are two sources for nonces.

- a *currTime* register that returns a 6 digit sequence HHMMSS giving the current time. HH is the hour (0 - 23), MM indicates minutes (0 - 60), and SS indicates seconds (0 - 60).
- a *monoIncr* register that returns a 6 digit sequence DDDDDD equal to the number of times this register has been read this week.

A designer has implemented a protocol to generate and distribute fresh session keys for sessions that are short (under 30 seconds) and that occur only between 9am and 5pm. The protocol uses the *monoIncr* register for obtaining nonces. But a summer intern you are supervising is now proposing to use the *currTime* register instead, so that keys older than 2 hours can be detected and deleted. What do you recommend?

A. Oppose it. The change could introduce a vulnerability, because the next nonce it uses would become become easier to predict,

B. Oppose it. The change could introduce a vulnerability, because nonces are not unique during a week.

C. Encourage it. The change is unlikely introduce a vulnerability and it provides better support for the Principle of Least Privilege.

7. _____

Name: NetId:

8. [2 points] We seek to implement processor names that cannot be spoofed by a virtual machine. The solution can involve having per-processor information stored in a read-only register on the processor chip. We might expect the name of such a processor to be

   A. a unique serial number.

   B. a private key.

   C. a public key.

   D. a symmetric key.

   E. a signed certificate.

8. _____

9. Recall the following definitions found in an English dictionary:

   - **extrinsic**: not part of the essential nature of someone or something; coming or operating from outside.
   - **intrinsic**: part of the essential nature of someone or something; coming or operating from inside.

   (a) [2 points] Trust is:

   A. extrinsic

   B. intrinsic

   (a) _____

   (b) [2 points] Trustworthiness is:

   A. extrinsic

   B. intrinsic

   (b) _____

   (c) [2 points] Assurance is:

   A. extrinsic

   B. intrinsic

   (c) _____

Name:	NetId:

10. [2 points] *Certificate transparency* is concerned with

A. using signing keys for which certificates are widely available.

B. having self-signed certificates.

C. having principal names that indicate certificate authorities for creating a certificate chain.

D. having certificates that are easy for humans to read.

E. detection of bogus certificates.

10. _____

Name:	NetId:

Write T in the space provided to indicate that the statement is true and write F to indicate that the statement is false.

11. [2 points] ___**F**___ An input can be a threat.

12. [2 points] ___**F**___ A program can be a threat.

13. [2 points] ___**T**___ A nation can be a threat.

14. [2 points] ___**T**___ A trusted employee can be a threat.

15. [2 points] ___**T**___ A security policy that guarantees CPU time to each user is an availability policy.

16. [2 points] ___**F**___ A security policy that limits the CPU time that a user may consume is an availability policy.

17. [2 points] ___**F**___ For a high-quality hash function $\mathcal{H}$, if $\mathcal{H}(m) = \mathcal{H}(m')$ holds then $m = m'$ holds.

18. [2 points] ___**T**___ For a high-quality hash function $\mathcal{H}$, if $m = m'$ holds then $\mathcal{H}(m) = \mathcal{H}(m')$ holds.

Name: NetId:

19. [2 points] ___**F**___ For a high-quality public-key encryption function $K\text{-}Enc(\cdot)$ and any public key K, if $m = m'$ holds then $K\text{-}Enc(m) = K\text{-}Enc(m')$ holds.

20. [2 points] ___**T**___ For a high-quality shared-key encryption function $K\text{-}Enc(\cdot)$ and any shared key K, if $m = m'$ holds then $K\text{-}Enc(m) = K\text{-}Enc(m')$ holds.

21. [2 points] ___**F**___ Decreasing the key size makes a protocol more vulnerable to Dolev-Yao attacks.

22. Assume that the following hold: A **says** P, B **says** Q, A **sfor** B, $P \Rightarrow R$, and $S \Rightarrow Q$ where $\Rightarrow$ indicates logical implication. For the following statements, given these assumptions, write T if the statement holds and write F if the statement does not hold.

    (a) [2 points] ___**F**___ A **says** B

    (b) [2 points] ___**T**___ A **says** R

    (c) [2 points] ___**T**___ B **says** R

Name:	NetId:

23. The set of beliefs for a new kind of principal "A **as** B" is defined as the intersection of A's beliefs and B's beliefs:

$$\omega(A \textbf{ as } B) \stackrel{\text{def}}{=} \omega(A) \cap \omega(B)$$

For the following statements, write T if the statement is correct and write F if the statement is not correct.

(a) [2 points] ___**T**___ (A **as** B) **sfor** A always holds.

(b) [2 points] ___**T**___ If (A **as** B) **says** S holds then A **says** S also holds.

(c) [2 points] ___**T**___ If both A **sfor** B and A **says** S hold then (A **as** B) **says** S holds.

Name:

NetId:

Write your answer in the space provided.

24. [2 points] In the space provided, describe a scenerio where a principal A **as** B (as defined above) is an ideal abstraction for formalizing the relationships in the system.

Solution: This principal would be useful for describing the execution by a server A in processing a request from a client B.

About the solution. *Many other correct answers are possible. A correct answer must give (i) a concrete example of a principal that is being described by A* **as** *B, (ii) concrete examples of principals A and B that together form A* **as** *B, and (iii) a rationale why the beliefs of A and B are combined according to the definition of beliefs for A* **as** *B.*

25. [3 points] List the elements of the Gold standard.

Solution: Authentication, Authorization, Audit.

Name: NetId:

26. You are developing an electronic lending library to control access by *patrons* to a collection of *videos*. The content of these videos ranges from harmless animation for entertaining children to subjects that typically would be viewed in private.

    The system will store

    - a collection of videos,
    - for each video V, a list Req_V that is the sequence of unfulfilled loan requests made by patrons who are still eligible to receive access to that video,
    - for each video V, a list L_V of patrons who have previously been loaned the video, along with the dates that loan period started and ended.

    Only one person should be allowed to view a given video at any time, and the total time that a patron is allowed access to any specific given video (in a single loan or a series of loans) is restricted to D days.

    (a) [4 points] Describe <u>two</u> different classes of threat, and give the goal(s) that motivate each.

    Solution:

    - Threat: Library patrons.
      Goal: Longer access to a video than allowed by above policy.
    - Threat: Outsiders.
      Goal: Learning the videos that specific patrons are viewing or have viewed.
    - Threat: Government.
      Goal: Attempting to censor content or learn which patrons are viewing specific videos.
    - Threat: Producers or people in the videos.
      Goal: Attempting to edit a video.

(b) [2 points] Give <u>two</u> important confidentiality policies:

Solution:

- No patron can view a video unless that patron is granted access.
- No patron can learn the names of the other patrons on lists Req_V or L_V for any given video V.

(c) [2 points] Give <u>two</u> important integrity policies:

Solution:

- No patron can delete or change all or excerpts of any video.
- No patron can alter the contents of list Req_V or L_V for any given video V.

Name: NetId:

27. Assuming that

- K_A is known only to A and KDC
- K_B is known only to B and KDC

the Otway-Reese protocol (below) can be used for creating a fresh key K_{AB} that is shared by principals A and B (and KDC).

1. $A \rightarrow B$: $n,\ A,\ B,\ \{r_1,\ n,\ A,\ B\}K_A$ fresh n, r_1
2. $B \rightarrow KDC$: $n,\ A,\ B,\ \{r_1,\ n,\ A,\ B\}K_A,\ \{r_2,\ n,\ A,\ B\}K_B$ fresh r_2
3. $KDC \rightarrow B$: $n,\ \{r_1,\ K_{AB}\}K_A,\ \{r_2,\ K_{AB}\}K_B$
4. $B \rightarrow A$: $n,\ \{r_1,\ K_{AB}\}K_A$

The message sent in each step includes unencrypted variables. Enter T for true and F for false in the space provided to indicate whether the unencrypted instance of the indicated variable could be deleted without causing problems.

(a) [1 point] **F** n in line 1 can be deleted.

(b) [1 point] **F** A in line 1 can be deleted.

(c) [1 point] **T** B in line 1 can be deleted.

(d) [1 point] **T** n in line 2 can be deleted.

(e) [1 point] **T** n in line 3 can be deleted.

(f) [1 point] **T** n in line 4 can be deleted.

Name: NetId:

28. [4 points] The following protocol is intended to generate and distribute a fresh session key K_{AB} to A and B. Initially: A knows K_A, B knows K_B, and S knows K_A and K_B.

1. $A \to S$: $A,\ B,\ \{r\}K_A$
2. $S \to A$: $\{r, K_{AB}\}K_A,\ \{r, K_{AB}\}K_B$ where K_{AB} is a fresh key
3. $A \to B$: $\{r, K_{AB}\}K_B$
4. $B \to A$: $\{r\}K_{AB}$
5. $A \to B$: $\{r+1\}K_{AB}$ A first checks: r agrees with value sent in 1?

The protocol is not secure—it allows an attacker T to obtain a fresh key KK_{AB} and to convince B that KK_{AB} is shared with A. Here is that attack:

1. $A \to S$: $A,\ B,\ \{r\}K_A$
2. $S \to A$: $\{r, K_{AB}\}K_A,\ \{r, K_{AB}\}K_B$ where K_{AB} is a fresh key
2.1. $T \to S$: $T,\ B,\ \{r'\}K_T$
2.2. $S \to T$: $\{r', KK_{AB}\}K_T,\ \{r', KK_{AB}\}K_B$ where KK_{AB} is a fresh key
2.3. $T \to B$: $\{r', KK_{AB}\}K_B$
~~3. $A \to B$: $\{r, K_{AB}\}K_B$~~ attacker suppressed msg
4. $B \to T$: $\{r'\}KK_{AB}$
5. $T \to B$: $\{r'+1\}KK_{AB}$

What is the smallest modification(s) to the protocol that would prevent this attack? Write your answer here:

Solution: Change message 2 by inserting "A" into the second blob and have the recipient use this information to learn which other principal is sharing K_{AB}. Then change message 3 to accomodate the new second blob.

2. $S \to A$: $\{r, K_{AB}\}K_A,\ \{r, A, K_{AB}\}K_B$ conclude A is sharing K_{AB}
3. $A \to B$: $\{r, A, K_{AB}\}K_B$

About the solution. *The corresponding change to the first blob (i.e., including "B") is not helpful for defending against the attack. The question asked for a smallest modification to prevent this attack, so that change to the first blob is not responding to the question. Finally, expanding both blobs to include "A, B" has a pleasing symmetry and allows "full sentences" to be constructed for the meaning of the blobs. But, the question asked for a smallest modification for preventing a specific attack—so this expansion is not answering the question that was asked.*

Use the space on the next page for checking that the attack is subverted with your modified protocol. The next page will not be graded.

Name:

NetId:

Use the space below for checking that the attack is subverted with your modified protocol. This work will not be graded.

Solution: Here is the attack after the protocol has been modified.

1. $A \to S$: $A,\ B,\ \{r\}K_A$
2. $S \to A$: $\{r, K_{AB}\}K_A,\ \{r, A, K_{AB}\}K_B$
2.1. $T \to S$: $T,\ B,\ \{r'\}K_T$
2.2. $S \to T$: $\{r', KK_{AB}\}K_T,\ \{r', T, KK_{AB}\}K_B$
2.3. $T \to B$: $\{r', T, KK_{AB}\}K_B$ conclude T is other principal sharing KK_{AB}

Attack detected!

Name: NetId:

29. Principal *JB* residing in USA seeks to convey a secret message to principal *VP* residing in Russia. CA's are maintained by UN, USA, and Russia. Here are some of the certificates being stored by these CA's:

CA at UN: $\langle K_{RUS}, \text{Russia}\rangle k_{UN},\ \langle K_{USA}, \text{USA}\rangle k_{UN},\ \langle K_{UK}, \text{UK}\rangle k_{UN}\ \ldots$

CA at USA: $\langle K_{JB}, \text{JB}\rangle k_{USA},\ \langle K_{FBS}, \text{FBS}\rangle k_{USA},\ \langle K_{UN}, \text{UN}\rangle k_{USA}\ \ldots$

CA at Russia: $\langle K_{VP}, \text{VP}\rangle k_{RUS},\ \langle K_{JB}, \text{JB}\rangle k_{RUS},\ \langle K_{GS}, \text{GS}\rangle k_{USA}\ \ldots$

In addition,

- every principal located within USA borders knows K_{USA} and believes that K_{USA} **sfor** USA holds;
- every principal located within Russian borders knows K_{RUS} and believes that K_{RUS} **sfor** Russia holds.

(a) [4 points] What chain of certificates should *JB* assemble from the CA's for deriving the public key for *VP*? Give that chain here:

Solution:

$$\langle K_{UN}, \text{UN}\rangle k_{USA},\ \langle K_{RUS}, \text{Russia}\rangle k_{UN},\ \langle K_{VP}, \text{VP}\rangle k_{RUS},$$

About the solution. *A sequence $C_1, C_2, \ldots$ of certificates is a chain if and only if each certificate C_i (for $i > 1$) gives a verification key (public key) for preceding certificate C_{i-1}. A chain satisfies the criteria of the problem provided (i) the verification key for the first certificate is a pubic key known to JB and (ii) the final certificate in the chain gives a verification key for VP. According to the problem statement, JB knows verification key K_{USA}, so (i) is discharged if the first certificate in the chain is signed by k_{USA}.*

(b) [2 points] Which of the following trust assumption is required?

A. VP **sfor** Russia
B. Russia **sfor** VP
C. UN **sfor** USA

(b) _____