Name: _____
Unity ID: _____

MIDTERM Exam – Fall 2016
CSC 515-001 – Software Security

Please read and sign the honor pledge below. Thank you in advance for your efforts to uphold our commitment to honesty and integrity.

I certify by my signature that I have neither given nor received unauthorized aid on this exam.

_____
Signature

Instructions:

1. Print your name and Unity ID at top of this page.
2. Print your name on the remaining pages.
3. Sign the honor pledge.
4. If you have any questions, raise your hand, and someone will assist you.
5. The test is 75 minutes long. You must stop writing immediately at that time.
6. If you feel a detail is missing, then state that as an assumption on your exam for the relevant question.

You may tear off these pages and we will staple them back on when you turn in your exam.

Circle the appropriate answer or answers for each of the following multiple choice questions:

1. What is a hash function is typically used for?
    a. Protecting the confidentiality of usernames
    b. Protecting the integrity of usernames
    c. Protecting the confidentiality of passwords
    d. Protecting the integrity of passwords
2. What is the prisoner's dilemma meant to illustrate?
    a. It is better to always think selfishly
    b. It is better to cooperate with others
    c. There is always a good cop and a bad cop
    d. It is better to confess
3. From a security perspective, which of the following is the best error message?
    a. com.ncsu.login.exception: Invalid credentials
    b. Invalid password supplied three times
    c. Invalid username or password: Please call 1-800-XXX-XXXX for help
    d. Username is valid but invalid password entered. Try again!
4. While inspecting OpenMRS, you see a stack trace on the screen in response to bad data that you submitted. This is a violation of which principle of secure design?
    a. Principle of least privilege
    b. Compartmentalization
    c. Fail and Recover Securely
    d. Defense in Depth
5. Which of the following attack strings may be used to exploit an **insecure direct object reference** vulnerability? (More than one may apply)
    a. ' or 1 = 1; --
    b. ../../../etc/passwd
    c. %PATH%/apache/bin/passwd
    d. <script>window.close()</script>
    e. All of these
    f. None of These
6. An attacker wants to lure a victim to malicious content on a website. A request is automatically sent to the vulnerable site which includes victim's credentials. This attack is:
    a. Cross Site Scripting
    b. Cross Site Forgery
    c. Broken Authentication
    d. Phishing
7. Cross-site scripting attacks seek to violate which of the following?
    a. Password management policy
    b. Server configuration policy
    c. Minimum access control policy
    d. Same origin policy

8. Which of the following are true about passwords? More than one may apply.
    a. Password expiration policies frequently frustrate users, who then tend to choose weak passwords and use the same few passwords for many accounts
    b. People are better at remembering passphrases as passwords than pronounceable passwords
    c. It is easier to crack new passwords if old passwords had been cracked before
9. Which of the following statements are true? More than one may apply.
    a. Throttling is a process of limiting the number of login requests to a system
    b. Filtering is a process of limiting the number of login requests to a system
    c. Throttling can be used to mitigate DOS attacks
    d. Filtering can be used to mitigate DOS attacks
10. Which of the following would be considered indications of a larger attack surface? More than one may apply.
    a. Features off by default
    b. Open network connections
    c. Larger code
    d. Authenticated access
11. What access control model is suitable for highly sensitive military information?
    a. Role Based Access Control
    b. Mandatory Access Control
    c. Discretionary Access Control
12. ISPs should make sure that messages being sent to their networks are coming from known IP addresses. This technique mitigates which security risk:
    a. Input injection
    b. Distributed denial of service
    c. Spear phishing
    d. Unvalidated redirects
13. What is the best location for storing a session ID?
    a. URLs
    b. Form variables
    c. Persistent cookies
    d. Non-persistent cookies

The following statements are either True or False; indicate your choice.

14. Limited memory, lower computing power, and decreased functionality makes mobile devices a difficult attack target.

15. Digital signatures aid in non-repudiation and in protecting the integrity of material downloaded from the Internet.

16. In an Attack Tree, if a parent node has only OR-type children nodes, then the cost of the parent node is sum of the costs of the children nodes.

17. An HttpOnly cookie can be accessed by client-side JavaScript.

18. Excessive data logging can hinder a system administrator's ability to detect anomalies.

19. Of implementation bugs, design flaws, and trust problems, trust problems are the hardest to deal with in system design.

20. A certificate Authority (CA) is responsible for signing public keys.

21. (5 points) Discuss a defense in depth strategy for (1) preventing; and (2) testing for cross site scripting vulnerabilities.

The following questions utilize the domain of an automotive assistance system, such as GM OnStar[1].

The system relies on mobile phone voice and data communication as well as location information using GPS technology. The system has the following capabilities:

1. Drivers and passengers can push a button to activate an audio interface to contact service representatives for emergency services.
2. Monthly, the system will remotely conduct vehicle diagnostics (engine & transmission system, emissions system, airbag system, stability control system, antilock braking system, tire pressure) and report results to the owner via email. Through the audio interface in the car, anyone in the car can also request a service representative execute vehicle diagnostics. These on-demand diagnostic results are sent to the owner via email.
3. Through the audio interface in the car, drivers and passengers may request turn-by-turn directions through the audio interface. The service representative initiates the car receiving directions similar to those provided by an in-car navigator system (such as Garmin or TomTom).
4. Equipped vehicles with an active subscription will also automatically contact representatives in the event of a collision.
5. The Stolen Vehicle Tracking system can be used to provide the police with the vehicle's exact location, speed, and direction of movement.
6. The Stolen Vehicle Slowdown system allows OnStar to remotely slow down the stolen vehicle. The service is also expected to help reduce the risk of property damage, serious injuries or fatalities resulting from high-speed pursuits of stolen vehicles.
7. The Remote Ignition Block can be used to remotely deactivate the ignition so when the stolen vehicle is shut off, it cannot be restarted.
8. All Stolen Vehicle Assistance services (Stolen Vehicle Tracking, Stolen Vehicle Slowdown and Remote Ignition Block) can be requested by the OnStar subscriber, but OnStar will not activate them until confirming with the police that the vehicle has been reported as stolen.
9. Drivers can make and receive calls in the car through Hands-Free Calling and can use voice-activated calling to place calls.

---

[1] Information presented on this page has been obtained from a most reliable source: Wikipedia (http://en.wikipedia.org/wiki/OnStar#Overview) as well as various pages linked from http://www.onstar.com

22. (9 points) Name 3 possible malicious user types of this system; and what would they be motivated to do and why?

23. (16 points) Create a combined use and abuse case diagram for the automotive assistance system. The diagram should contain all users and functionality listed in the description. The diagram should include all of the malicious user types from the last question and should show relationships between the use cases and the abuse cases. The attacks must be against functionality listed in the description. Please indicate the number of the feature(s) your attacks are against.

24. (15 points) Choose one attack in your use/misuse/abuse case diagram. Develop an attack tree with a projected cost for each attack scheme. These costs are **estimates;** however, we're looking for the logic underneath your estimates. Explain your logic and your choice of attack the team should be most concerned about.

25. (15 points) Choose the least cost attack in your attack tree diagram. Develop a defense/protection tree with a projected cost for each protection. These costs are **estimates** but we're looking for the logic underneath your estimates. Explain your logic and your choice of defense the team should focus on first.