Instructions

There are **65 total points**. When asked to provide your answer within a figure or table, be careful to not exceed box boundaries. Bubbles must be filled out completely: ● is correct, ✓ ⊙ ⊗ are incorrect All answers must be given within the provided circles, answer boxes, figures or tables.

1. [1 point]: Write your full name in the box to acknowledge the instructions.

Ethics

2. [4 points]: Which of the following ethics principles are described in the Belmont Report? (Select all that apply.)

◯ Do no harm

◯ Justice

◯ Informed Consent

◯ Respect for Public Policy

◯ All of the above

Case Study: Working for Frugal, an employee presents a new marketing experiment that will personalize the order of search results for retail products based on a user's *inferred* gender. (Although the company has no way of knowing for certain about the user's gender, in-lab experiments suggest that they can infer it with 95% accuracy based on the user's search history.) A demonstration of the marketing experiment shows that a search for "shoes" returns products such as stiletto heels for inferred females and running shoes for inferred males. A small pilot study within the company shows that the experiment increases shows that the experiment increases click-through rates by 10% and will ultimately boost company revenue. The employee's manager is concerned that the experiment may be unethical.

3. [4 points]: Use the principle of *beneficence* to present an argue **in favor** of the experiment.

(Answer inside the box)

4. [4 points]: Use the principle of *beneficence* to present an argue **against** the experiment.

(Answer inside the box)

5. [4 points]: Using either an example that we discussed in class, or another example of your choice explain where disregarding the "Respect for Law" principle may be justifiable.

(Answer inside the box)

6. [2 points]: To obtain approval for an experiment (e.g., from an Institutional Review Board), it is always necessary to obtain informed consent from all participants in an experiment. ◯ Yes ◯ No

Authentication

In class, and in the assignments, we talked about the use of OAuth as a mechanism to authorize to perform actions on behalf of a user.

7. [4 points]:
Which of these might be a reasonable use of OAuth? (Select all that apply.)

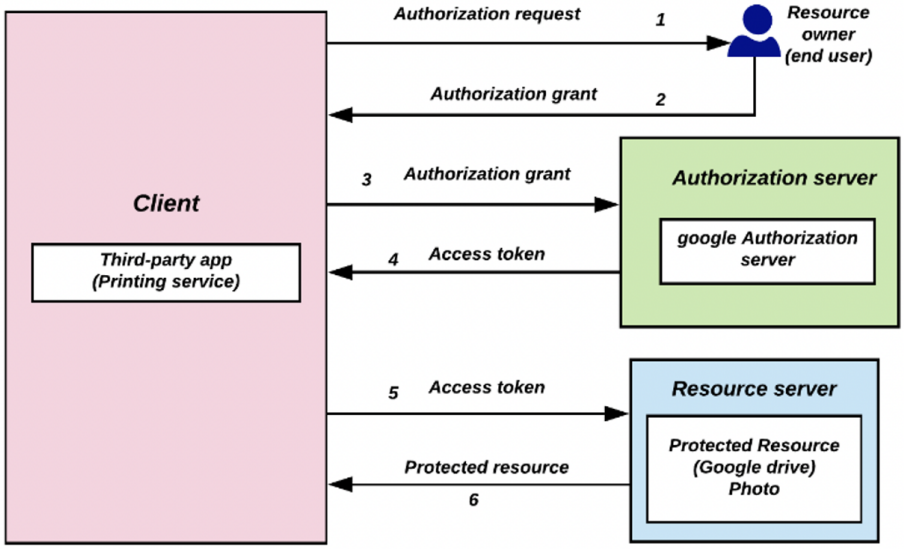
◯ Gathering information off of a private social media feed using a web scraper.

◯ Enabling users to sign in to a mobile app using their Google account.

◯ Allowing a fitness app to access a user's health data from a third-party provider.

◯ Authenticate users on a public forum without asking them.

◯ All of the above



8. [4 points]:
In the figure showing the steps of the OAuth protocol above, at which step is authorization to perform specific actions for different "scopes" (e.g., read a file, write a file) granted? (Select the best answer.)

◯ 1
◯ 2
◯ 3
◯ 4
◯ 5

Denial of Service Attacks

9. [4 points]: Which of the following is an example of amplification? (Select all that apply.)

◯ A small DNS query elicits a large DNS response.
◯ A large number of packets is sent to a single IP address.
◯ A "ping" to a broadcast address results in many reply messages.
◯ A large number of packets is sent to a single port.

10. [2 points]: Traffic from legitimate users can exacerbate the effects of a denial of service attack by adding to the overall attack traffic volume.

◯ Yes ◯ No

Public Key Infrastructure

11. [4 points]: Suppose a web server's private key is compromised (as happened with the Heartbleed attack that we discussed in class). Which of the following statements is true about the incident? (Select all that apply.)

◯ The attacker may be able to decrypt all past and future messages sent to the server.

◯ Using the private key, an attacker can impersonate clients to the server.

◯ Using the private key, an attacker can impersonate the server to clients.

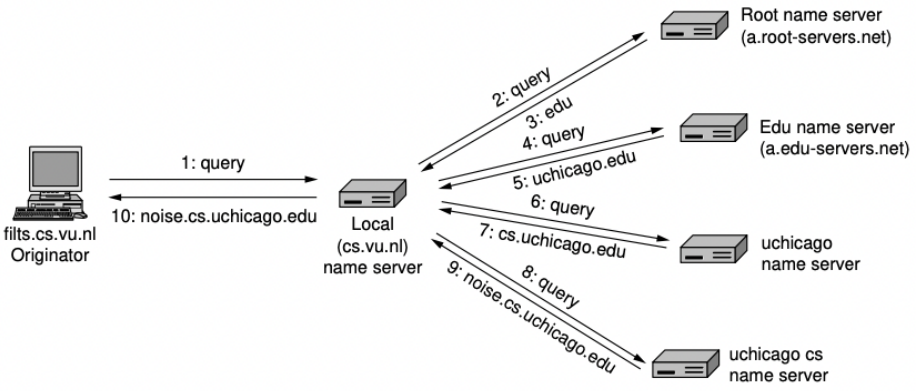
◯ The server must revoke its certificate.

◯ All of the above

12. [4 points]: Describe one possible attack scenario that could occur if a server relies on a self-signed certificate and the client chooses to accept that certificate.

(Answer inside the box)

DNS Security and Privacy



13. [4 points]: In the above figure, circle the portion of the DNS lookup process that is vulnerable to eavesdropping from an Internet service provider that encrypted DNS protects against.

14. [2 points]: When encrypted DNS is enabled in your browser, the operator of the local DNS resolver can no longer see the domain names that you are visiting.

◯ Yes ◯ No

Initials: ____

15. [4 points]: Supposing DNSSEC is widely deployed. Which of the steps in the above transaction would contain a public key for `a.edu-servers.net`? (Select the best answer.)

◯ 2
◯ 3
◯ 4
◯ 6
◯ 7

Privacy and Tracking

16. [4 points]: Which of the following attributes can enable a user to be tracked across websites, even in the absence of cookies? (Select all that apply.)

◯ Installed fonts
◯ Browser version
◯ Support for gzip compression
◯ Type of graphics card
◯ All of the above

17. [4 points]: Can the set of DNS lookups that a browser issues make it possible to determine the specific webpage (not just the website) that a user is visiting? ◯ Yes ◯ No

18. [4 points]: Why or why not?

(Answer inside the box)

Feedback

19. [1 point]: Interest (1=Boring!; 10=Amazing!): [ ] Difficulty (1=Too easy; 10=Too hard): [ ]

20. [1 point]: 1. One thing you like. 2. One suggestion for improvement:

(Answer inside the box)