PRINCETON UNIVERSITY Department of Computer Science

Midterm

COS 432: Information Security: Fall 2016

There are 10 questions and 9 pages in this quiz booklet (including this page). **There are 200 total points.** Answer each question according to the instructions given. You have **80 minutes** to answer the questions.

If you find a question ambiguous, write down any assumptions you make. **Be neat and legible.** If we can't understand your answer, we can't give you credit!

Lifeline: For *one* part (*i.e.*, capital alphabetic letter) of any question, you can list the name of another classmate who may know the answer to the question. If that person writes the correct answer to that part of the question, you will receive full credit (*i.e.*, 10 points).

Use the empty sides of this booklet if you need scratch space. You may also use them for answers, although you shouldn't need to. *If you do use the blank sides for answers, make sure to clearly say so!*

Note: Write your name in the space below AND your initials at the bottom of each page of this booklet.

THIS IS AN "OPEN NOTES" QUIZ.
ONE TWO-SIDED LETTER-SIZED NOTE SHEET AND THE LECTURE NOTES HANDOUT IS ALLOWED.
MAKE SURE YOU'VE READ ALL THE INSTRUCTIONS ABOVE!

(1) Initial here to indicate that you've read the instructions:
(2) In the space below, write out and sign the Princeton Honor Code pledge before turning in the exam: "I pledge my honor that I have not violated the Honor Code during this examination."

Do not write in the boxes below

1-2 (xx/40)	3 (xx/30)	4-6 (xx/60)	7-8 (xx/40)	9-10 (xx/50)	Total (xx/200)

Name:

I Ethics

On Friday, October 21, 2016, a major denial of service attack was mounted using Internet of Things (IoT) devices which were infected by malware based on their reliance of default passwords. The botnet that infected these vulnerable devices was called the "Mirai" botnet, and mounted denial of service attacks against Twitter, Github, Reddit, and many other Internet sites.

Troubled by this turn of events, over the weekend, Alyssa P. Hacker took a break from COS 432 studying to develop a piece of software that:

1. Scans the Internet for all IoT devices that are vulnerable to the Mirai botnet by attempting to log into each of the vulnerable devices; and
2. If the software succeeds in logging into the vulnerable device, it changes the password to the camera's hardware address (the hardware address is something that the owner of the camera could easily discover but, after the vulnerability is closed, would be relatively more difficult for remote attackers to discover).

1. [10 points]: Explain why we need ethical reasoning guidelines such as those from the Belmont Report, as opposed to simply encoding an ethical rule or law that permits or prevents deploying this type of software.

2. [30 points]: Alyssa is considering whether to deploy her code to patch the Internet-wide vulnerability. Reason about the ethics of deploying Alyssa's patch in terms of each of the following:

A. Respect for persons

B. Beneficence

C. Justice

II PRFs and PRGs

3. [30 points]: Answer the following questions about PRFs and PRGs.

A. Let f be a function that takes a secret key of length κ and a message and outputs a result with the same length κ. Show that if κ is small (*e.g.*, $\kappa = 10$), f is not a PRF.

B. Let f be any secure PRF defined on secret keys of length κ and any message length. How can a Mallory distinguish f with a truly random function if we allow a Mallory to run even exponential number of steps (also make exponential number of queries to $f(\cdot)$)?

C. Let f be a secure PRF. Let g be $g_k(x) = f_k(x)||f_k(f_k(x))$. Is g a PRF? Show your result with an informal proof.

III Symmetric Key Cryptography

4. [30 points]: Answer the following questions regarding a communication protocol.

Alice and Bob share two secrets, k_1 and k_2, which are initially unknown to any third party. Alice wants to send a message m to Bob; she transmits the follow content:

$$c = E_{k_1}(m||H(k_2||m))$$

where E_{k_1} is the symmetric encryption function using key k_1, H is a cryptographically secure hash function (*e.g.*, SHA-1), and $||$ is the concatenation operator.

A. When Bob receives c, how does he compute and verify the original message m? Please list all the necessary steps.

B. Does this protocol provide the following properties:

(a) Confidentiality (such that no third party may retrieve m from the transmitted content c)?

(b) Integrity (such that Bob is aware of any alterations to the transmitted content c)?

(c) Non-repudiation (such that Alice cannot deny previously sent messages)?

C. In the event that the protocol above does not provide confidentiality, integrity or non-repudiation, provide a fix to the protocol to make it more secure.

5. [10 points]: Does Diffie-Hellman key exchange ensure that two parties can always exchange messages securely? If so, explain why. If not, describe a possible attack.

6. [20 points]: Alice now wants to send encrypted messages to Bob using AES. The two parties do not share any secret key, so Alice first needs to share a AES key k with Bob. We assume that the AES key is 128 bits. Alice knows Bob's 4096-bit RSA public key is (3, N), so she encrypted the key and sent $c_k = k^3 \bmod N$ to Bob.

A. Can an eavesdropper who intercepts this message learn the AES key? Explain why or why not.

B. If a vulnerability exists, propose a way to fix the problem.

IV Asymmetric Cryptography

7. [10 points]: What is one disadvantage of asymmetric compared to symmetric cryptography?

8. [30 points]: Alice wants to send a message *M* to Bob. Assume Alice and Bob have securely distributed their public keys P_A and P_B to each other. Private keys of Alice and Bob are S_A and S_B respectively. Design messages that Alice must send to meet the security requirement below.

Notation:

- $\{x\}_y$ (x is encrypted using key y)
- $A \xrightarrow{x} B$ (A sending x to B)

Example:

- $A \xrightarrow{\{M\}S_A} B$ The message *M* is encrypted with Alice's private key S_A. The encrypted message is sent to Bob.

A. Using public key cryptography, design a message that enables Bob to verify the message source, Alice, and preserves only integrity.

B. Using public key cryptography, design a message that protects only the confidentiality of the message sent from Alice to Bob.

C. Using public key cryptography, design a message that enables Bob to verify the message source, Alice, and when both integrity and confidentiality are protected.

V Public Key Infrastructure

You've recently purchased a Mest smart webcam for your dorm room that decides to communicate with a cloud-hosted server at `mest.com`. The webcam also has a client certificate that is known to the `mest.com` server.

Suppose that the webcam periodically takes a photograph, then encrypts and signs the photograph before uploading it to the Mest cloud server.

9. [30 points]: In a rush to production, Mest ships the webcam with the list of the roughly 200 trusted root certificate authorities (CAs) that are in the Firefox browser.

A. Explain why shipping the webcam with a list of so many root CAs might not be necessary in the case of a device like a webcam.

B. One of the root CAs happens to be from an organization, In-The-Clear Rootin' (ITCR), which happens to be controlled by a foreign nation-state actor. Can ITCR mount an attack on confidentiality, integrity, or both? If so, describe the attack. If not, explain why not.

C. Mest decides to revoke ITCR's root CA from all of its deployed webcams with a signed, secure software update to the webcam's firmware, which it sends to each camera over the Internet. IS the software update itself vulnerable to an attack from ITCR? Why or why not?

10. [20 points]: Your dorm room was robbed, but fortunately, you've caught the perpetrator on one of the photos from your Mest camera, and the camera uploaded the photo to `mest.com`! [1].

You log into the `mest.com` the photo to the campus police.

Before going after the perpetrator, though, they want to make sure that your photo is authentic, and actually came from the camera in your dorm room.

A. When you visit `mest.com` on your browser, you notice that `mest.com` is using a self-signed certificate for its website. In the certificate, you notice that the name of the organization is "Mest, Inc.". Can you be certain that you're visiting the website of the organization that manufactured your webcam? Why or why not?

B. Explain how the camera's *client certificate*—and an associated protocol—could link the photo to the camera in your dorm room. Be sure to list *everything that the certificate would need to contain* to help the police verify that the photo came from your camera.

[1] Suppose the photo also includes necessary metadata, like a timestamp.