CS 444/544 Spring 2017 Midterm

Name:_____

Circle the section of the class you are registered for: 444 544

This test is closed book, closed notes, closed neighbor, and closed everything else except for a pen or pencil. If you are logged into any lab computer or other computer that is connected to the Internet or using any devices such as a cell phone, kindle, or calculator during the exam you will receive a 0 on the exam and I may take further action pursuant to University policy about cheating.

Write all answers on the front or back of this sheet, you will tear off this page and only turn in this page. You can keep the rest of the pages, but don't share them with anyone. None of these are meant to be trick questions, if the question seems simple it probably is. If it's not clear which selection you marked, I'll mark it as incorrect.

For questions 1 through 10 (10 points each) circle the correct answer (A, B, C, or D) below:

1. A B C D
2. A B C D
3. A B C D
4. A B C D
5. A B C D
6. A B C D
7. A B C D
8. A B C D
9. A B C D
10. A B C D

This page intentionally left blank (except for this bit about it intentionally being left blank and all the levels of self reference that follow from that).

DON'T CIRCLE ANSWERS HERE, CIRCLE THEM ON THE ANSWER SHEET.

1. If you were to use Wireshark to illegally record the network traffic of someone you share a network with (a neighbor, a roommate, a classmate, *etc.*) and then read their private communications, which of these laws is the most applicable (*i.e.*, which are you likely to be convicted of)?:

A. The Computer Fraud and Abuse Act

B. The Electronic Communications Privacy Act

C. The Cybersecurity Enhancement Act of 2002

D. The Access Device Statute

This amended the Wiretap Act and Stored Communications Act.

2. During a horizontal port scan, nmap sends SYN packets to port 80 on a whole /24 subnetwork of machines. Five of those machines respond with a SYN/ACK, and the rest (248-ish if you exclude unusable IPs) respond with a RST or ICMP error or don't respond at all. Which of these statements would be the most reasonable conclusion?:

A. Five of the machines have port 80 open, *i.e.*, are listening on port 80

B. Five of the machines are filtered on port 80

C. Those five machines have low TTLs

D. The scan is a stealth scan

This is the most basic operation of nmap.

3. Which of these would you be most likely to use if you controlled a router in the core of the Internet and wanted to spy on all traffic that went through your router?:

A. The tuple of source and destination IP addresses

B. RSA

C. A port mirror

D. Diffie-Hellman

We talked about port mirrors during the networking part of the class.

4. For the SSL/TLS system where certificates are signed by certificate authorities and used for authentication, what cryptographic algorithm is likely to be used for the signatures?:

A. Diffie-Hellman

B. AES

C. The Zodiac cipher

D. RSA

B and C are not asymmetric, A can only be used for key exchanges.

5. Which of these is **NOT** a technique that is typically used by attackers for Network Intrusion Detection System evasion? (Assume that the NIDS is fail-open):

A. Limiting TTLs so packets don't reach the destination

B. Exploiting ambiguities in the way different operating systems put together overlapping IP fragments

C. Denial of Service

D. Port mirrors

Port mirrors are a hardware device, not an evasion technique.

6. Suppose I crack a simple substitution cipher (where each letter is replaced uniquely by another letter) by using frequency analysis and assuming the plaintext is in English, although I don't know what the plaintext is. What type of attack have I most likely carried out?:

A. Ciphertext only

B. Known plaintext

C. Chosen plaintext

D. Chosen ciphertext

You don't know the plaintext, and you're not changing/choosing it or the ciphertext.

7. During a Diffie-Hellman key exchange between Alice and Bob, with Eve as the eavesdropper, who knows Alice's private key at the end of the key exchange? Assume the simplest possible scheme with no forward secrecy.

A. Alice only

B. Alice and Bob

C. Alice, Bob, and Eve

D. Nobody, not even Alice

This is a basic tenet of asymmetric cryptography.

8. Imagine a padding oracle chosen ciphertext attack like what you did for Lab 2, but instead of the padding oracle being based on the malleability of CBC block chaining mode it is instead based on the malleability of RSA. As a poorly designed form of key exchange by an app, an AES key is randomly generated by the client and then encrypted using the server's public RSA key, then sent to the server where it is decrypted. Without knowing the details of the attack, which of the following would you **NOT** expect to be true of the attack?:

A. It involves sending slightly modified ciphertexts to the server

B. The attacker learns information based on the server's responses

C. The attacker needs to know the server's private key to carry out the attack

D. The attacker can modify the plaintext of the RSA by themselves only doing operations on the ciphertext

The point of an oracle attack is that you don't need the key because the oracle has the key.

9. Which of the following things can typically happen while carrying out a CBC padding oracle attack?:

A. The server can decrypt parts of the original padding and think that they're part of a message

B. The attacker can recover the AES key used for encryption

C. The attacker can recover the AES key used for decryption

D. The attacker can use the CBC padding oracle to factor extremely large products of primes (on the order of 2048 bits**)**

You probably saw this happening (or imagined it happening in the server) in your Lab 2 debugging.

For question 10, answer the undergraduate version if you are registered for 444 and the graduate version if you are registered for 544.

Undergraduate (444) version of question 10: If you're reverse engineering an Android app and you see "srand(currenttimeinmilliseconds); key = rand()" being used to generate an AES key for encrypting messages, what attack would you most likely use to exploit this?:

A. A number sieve to factor two large primes

B. A brute force attack based on the time a message was recorded

C. The malleability properties of RSA

D. Differential cryptanalysis

This is the QQ Browser example we talked about.

<u>Graduate (544) version of question 10:</u> When you generate a PGP public/private key pair in Linux using standard utilities, you have to add entropy to the Linux entropy pool (*i.e.*, /dev/random) for the process to complete. What is the best way of doing that?:

A. Randomly hitting keys on the keyboard and moving the mouse around

B. Calculating the totient for a product of two primes

C. Performing RSA encryption using your previous public key

D. Blowing air into the little paper clip hole in the CD-ROM

Interestingly, all of these will add entropy in the sense that they may affect, e.g., a hard drive timing, but only A will directly add entropy in a significant way from the perspective of the Linux kernel.