Name:_____

CS 600.443 Final Exam

This exam is closed book and closed notes. **You are required to do this completely on your own without any help from anybody else.** Feel free to write on the back of any page to continue an answer, and indicate (over) when doing so.

Part I. Multiple choice: circle one choice (2 points each)

1. Which one of the following is NOT a basic property used in authentication
    a. Something you have
    b. Something you ate
    c. Something you are
    d. Something you know
2. The Microsoft Passport scheme
    a. Is totally secure
    b. Uses persistent cookies as long-term authentication tokens
    c. Is designed to find buffer overflow attacks
    d. Was designed in conjunction with the United States INS.
3. Which of the following is an example of Network Layer security
    a. SSL/TLS
    b. WEP
    c. IPsec
    d. SSH
4. The main problem with WEP is that
    a. The underlying cipher, RC4 is totally insecure
    b. The particular implementation of RC4 was flawed
    c. The designers should have used RC4 but they didn't
    d. Actually, the problems with WEP have nothing to do with RC4
5. In the privacy lingo, the term "Access" means
    a. You get to know what data is collected about you
    b. You get to control what data is collected about you
    c. You get to control who can see data that is collected about you
    d. That somebody has hidden your private information
6. The Iplog program sends bogus responses to nmap queries. This is useful because
    a. Somebody might be trying to scan the ports on your network.
    b. It satisfies the protocol queries, so the contract can be completed.
    c. It serves as a fingerprint scrubber against faulty multi-purpose agents
    d. It prevents attacks against the incremental IP protocol as defined by the IETF
7. Which of the following was not a problem that the Morris Worm exploited:
    a. A bug in the central library server
    b. People pick plenty poor passwords
    c. A bug in the sendmail program in debug mode
    d. A bug in the fingerd server
8. Which of the following is a DDOS tool:
    a. IPsec
    b. Trinoo
    c. VPN
    d. AFLP

9. A firewall filters packets
    a. Based on transport layer port numbers
    b. Based on network layer addresses
    c. Possibly based on previous state
    d. All of the above

10. Which of the following implementations of IPsec is the least secure:
    a. AH with ESP in tunnel mode
    b. AH with ESP in transport mode
    c. AH without ESP in either mode
    d. ESP without AH in either mode

    (2 points) Justify your choice:

Part II. True/Fale: circle T for True or F for False (2 points each)

T F 1. The PATRIOT II bill text accidentally leaked out.
T F 2. A Non-Disclosure agreement is a good way to protect a trade secret if you have to share it with someone.
T F 3. The Freedom of Information Act enables citizens to obtain many government records that were previously kept secret.
T F 4. According to the CyberSecurity Enhancement Act ISPs can voluntarily share information with no warrant during an emergency.
T F 5. Browsers always automatically reveal user's e-mail addresses to web servers.
T F 6. Cookies can be used to launch denial of service attacks.
T F 7. The primary legitimate use for cookies is to link multiple browsing sessions together.
T F 8. Cookies were designed to enable single singon by the original architects of the web.
T F 9. Web bugs only work on SSL protected pages.
T F 10. Doubleclick collects browsing patterns of users across multiple web sites using embedded images in web pages.
T F 11. X.10 cameras use an analog 2.4 Ghz signal, so it is hard to encrypt the content.
T F 12. Mixes use public key cryptography.
T F 13. Crowds uses public key cryptography.
T F 14. Publius uses public key crytpgoraphy.

Part III. Short answer. (use the back if necessary) (4 points each)

1. Explain how a non e-mail based computer virus/worm can copy itself from computer to computer.

2. What is the difference between a block cipher and a stream cipher? When would it be more appropriate to use each one?

3. Describe the role that zombies play in distributed denial of service attacks.

4. What are two differences between trademarks and patents?

5. Explain how cookies and Referer headers can be used to track web movements.

6. Give three reasons why voting in public elections over the Internet is not a good idea from the point of view of security.

7. The FBI's CARNIVORE system described by Ari Schwartz in class has been criticized as a privacy invading technology. Explain how security problems with the system could lead to even more serious privacy compromise.

8. Explain how the first and last mix in a Chaum mix network can collaborate to break anonymity.

9. What is the fundamental difference in the way messages are routed in Crowds versus in Mixes?

10. (Choice of two problems. Answer either one, but not both) Explain why the solution to the embedded image problem in Crowds (timing attack) introduces performance problems.

OR

Explain why static paths were needed in Crowds and the purpose of "join commits".

11. In Publius, content is published by encrypting it with a key, secret sharing the key, and storing shares with the encrypted content. Describe a modified publishing algorithm for Publius that does not require encryption, but which yields the same security and censorship resistance properties as the one in Publius.

Part IV. Long answer. (20 points) use front and back of this sheet and the next, if necessary

You have decided to set up a fancy home network. You have several housemates, Alice, Bob, and Charlie who live with you, and they each have a computer. You don't really trust them very much. You would like to run a web server out of the house. Your high-speed connection comes from an ISP called Comcast, and you would like the ability to have a laptop in the house on a wireless network. You are very worried about attacks from the outside world into your home network. It is also important for you to be able to access any outside machine from the inside.

1. Diagram your home network, showing every computer, firewall, router, server, etc
2. List the firewall rules that you would implement between your house and the ISP
3. List the firewall rules that you would implement inside your house. Specify where the firewalls are and the filtering rules that would go with each firewall.
4. If a virus infects Bob's machine, what are the risks to your computer? How does your architecture reduce those risks?
5. If you wanted to some day put all of the machines on the wireless network, how would the architecture change?