*College of Computing*

Georgia Institute of Technology

## CS 6262: Network Security: Spring 2009

# Quiz I

There are 13 questions and 10 pages in this quiz booklet (including this page). Answer each question according to the instructions given. You have **85 minutes** to answer the questions.

If you find a question ambiguous, write down any assumptions you make. **Be neat and legible.** If I can't understand your answer, I can't give you credit! There are three pretty challenging questions (clearly marked); you may want to look through the whole quiz and save those for last.

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

**THIS IS AN "OPEN NOTES, OPEN PAPERS" QUIZ.**
**LAPTOPS ARE ALLOWS, BUT NETWORKING IS NOT.**
**NO ENCRYPTED WIRELESS TRAFFIC.**
**MAKE SURE YOU'VE READ ALL THE INSTRUCTIONS ABOVE!**

**Initial here to indicate that (1) you've read the instructions and (2) you agree to abide by the Georgia Tech Honor Code:**
The last page has easy bonus questions, which you can answer outside of the allotted time. Rip the last page off of your quiz for some bonus points and turn it in (anonymously if you like). You won't get the points if you don't tear off the page (this is to make certain you've read this far!).

*Do not write in the boxes below*

| 1-5 (xx/20) | 6-11 (xx/24) | 12-13 (xx/14) | Bonus (xx/7) | Total (xx/65) |
|---|---|---|---|---|
| | | | | |

**Name:**

# I Warmup

1. **[4 points]:** Which of the following is true about substitution ciphers?
**(Circle ALL that apply)**

**A.** Encrypting plaintext with a sequence of multiple substitution ciphers can help create a more uniform distribution of ciphertext symbols.

**B.** Given ciphertext encrypted with a Vigenere cipher, knowledge of the length of the key could help an attacker recover the plaintext.

**C.** When used correctly, a one-time pad produces ciphertext that bears no statistical relationship to the original plaintext.

**D.** The original Caesar cipher only has 26 possible keys.

**E.** None of the above.

2. **[4 points]:** Which of the following is true about TCP SYN flood attacks?
**(Circle ALL that apply)**

**A.** TCP SYN packets used as part of a SYN flood attack cannot use spoofed source IP addresses.

**B.** TCP SYN cookies prevent a server from needing to maintain "half open" TCP connections when a TCP SYN arrives.

**C.** TCP SYN cookies protect the server against all resource exhaustion attacks.

**D.** Knowledge of the timestamp that the server uses to create the TCP SYN cookie helps an attacker forge the third part of a three-way handshake.

**E.** None of the above

3. **[4 points]:** Which of the following is true about public keys?
**(Circle ALL that apply)**

**A.** In the self-certifying file system, directories are named by the hash of a public key; this process alleviates the need for any key distribution mechanism.

**B.** For public key cryptography algorithms, the encryption operation is equivalent to the signing operation.

**C.** Public key encryption can be used to establish a shared (symmetric) session key.

**D.** The RSA public key encryption algorithm is based on the hardness of the discrete logarithm problem.

**E.** None of the above.

**4. [4 points]:** Recall the "design suggestions" from the *How to 0wn the Internet in Your Spare Time* paper. Which of the following are true about the design suggestions mentioned in that paper (and about malware spreading, in general)?

**(Circle ALL that apply)**

**A.** Permutation scanning helps ensure that different compromised hosts scan different parts of the IP address space for vulnerable hosts.

**B.** Hit-list scanning may help reduce the overall time for the worm to reach the point where it has infected all vulnerable hosts.

**C.** Many worms increase their overall scanning rate by seeding the random number generator for scanning IP addresses using the the infected host's local time.

**D.** The Slammer worm spread quickly partially because its payload was delivered via UDP.

**E.** None of the above

**5. [4 points]:** Which of the following weaknesses of ATM security were discussed in the paper *Why Cryptosystems Fail*?

**(Circle ALL that apply)**

**A.** Taking bank slips with account numbers out of trash bins.

**B.** Calling bank customers by telephone asking for bank account numbers.

**C.** Building a vending machine to harvest bank numbers and PINs.

**D.** Changing the bank account number on the magnetic strip of the card.

**E.** None of the above

# II Potpourri

**6. [4 points]:** Consider Georgia Tech's BuzzCard system, which only lets certain people into the Klaus Computing Building on nights and weekends. The system involves both *authentication* and *authorization*.

**A.** Explain the token used for authentication, describe a possible weakness to the authentication system, and propose one other authentication mechanism.

**B.** Define authorization. Speculate on how the BuzzCard system performs authorization. (Any plausible explanation that *could* work will receive credit.)

**(Answer legibly in the space below.)**

**7. [4 points]:** Ben Bitdiddle asks you to design a network protocol such that two network hosts, Alice and Bob, who have knowledge of each other's public keys can sign every packet between the two parties.

**A.** Explain why Alice and Bob can't simply sign each packet with their respective private keys.

**B.** Draw a message exchange below that shows how Alice and Bob can establish a shared secret key, and show how that shared secret key can be used to affix a compact ($< 200$ bits), efficient signature to each packet. (Your scheme does not need to be robust against man-in-the-middle attacks.)

**8. [6 points]:** Various network protocols often begin with the same (or a small set of) initialization messages. For example, HTTP messages often with a `GET` request after the initial TCP three-way handshake. Also, Web pages often serve largely the same content to multiple parties.

**A.** Explain how knowledge of the initial protocol messages could help an attacker recover the encryption key for a secure HTTP session.

**B.** Explain how knowledge about the Web page a user was visiting could help an eavesdropper determine the content that a user was downloading.

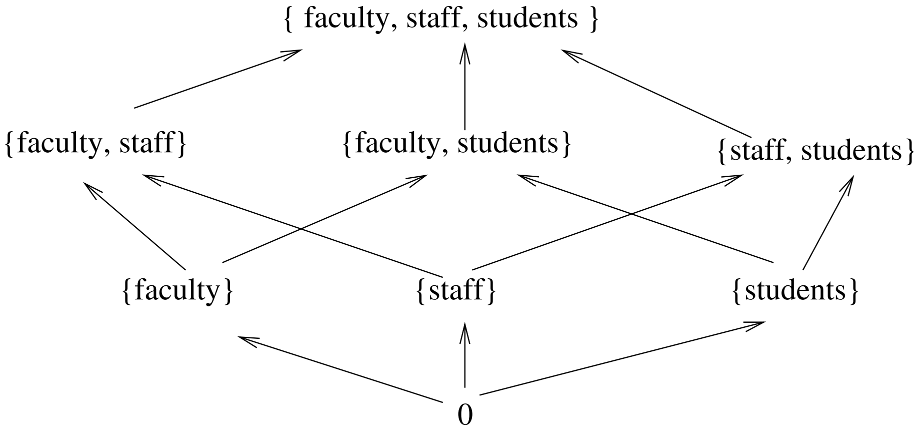
**(Answer legibly in the space below.)**

**9. [2 points]:** Recall from Problem Set 1, you performed a brute-force dictionary attack against an encrypted password file. The password file included a "salt" for each user. Explain what a salt is, how it is used, and how it makes a brute-force dictionary attack against the password file more difficult for an attacker.

**(Answer legibly in the space below.)**

**10. [4 points]:** Consider the lattice below.

**(Answer legibly in the space below.)**



A file, `payroll.txt`, might have payroll data about students, faculty, and staff.

**A.** What security class should that file have?

**B.** In the lattice model above, can a program with classification "staff" read such a file? Why or why not?

**C.** Faculty may need to read access to student payroll, but may have no need to access staff or faculty payroll information. Suggest how the payroll file might be divided into multiple files, and how security classes might be assigned, to permit this access granularity.

**Initials:**

**11. [4 points]:** Consider the PlayFair cipher below, which has “Network Security” as the key.

| | | | | |
|---|---|---|---|---|
| N | E | T | W | O |
| R | K | S | C | U |
| I | Y | A | B | D |
| F | G | H | J | L |
| M | P | V | X | Z |

**A.** Produce the ciphertext corresponding to the plaintext “Encryption is easy”.

**B.** Produce the plaintext corresponding to the ciphertext “BSI EUD TGSI NP”

**Initials:**

# III Design Question: Web Authentication

George Burdell needs some help designing a Web authentication system for his new e-Commerce Web site. He decides to allow his Web site to use more sophisticated client authentication schemes. In this problem, you will evaluate various client authentication mechanisms.

**12. [6 points]:** George's first idea is to give a client a sequence-number-based session identifier when it successfully authenticates, as follows:

```
// secret, not exposed outside of program
unsigned long globalSessionID = 34215;

void success() {
 char redirectURL[256];
 if (authenticated[user]==1) {
   sprintf(redirectURL, "http://burdellbooks.com/%s&sid=%lu", path,
                             globalSessionID) ;
   /* redirect user to redirectURL */
  ...
  }
}
```

assume that `authenticated[user]` becomes 1 after a user successfully logs in.

**A.** Explain how the above scheme is vulnerable to a brute-force guessing attack. Explain how you might change how the session identifier is generated to defend against a brute-force attack.

**B.** Explain how the above scheme is vulnerable to a replay attack. Extend the design of the session identifier to defend against replay attacks.

**13. [8 points]:** George decides instead to place an HTTP cookie on the client that is applies the `crypt()` function, as follows:

```
char* genCookie(char *username) {
  char input[20];
  char cookie[13];

  sprintf(input, "%s%s", username, "secret");
  sprintf(cookie, "%s", crypt(input, "CS"));
  return cookie;
}
```

**A.** How is the above code vulnerable to a buffer overflow?

**B.** Note that `crypt()` truncates inputs that are longer than eight characters. Explain how you might use a chosen plaintext attack to mint authenticators for long usernames.

**C.** *Hard.* Suppose that, as an attacker, you did not know the server secret salt "secret", but that you could use the server as an oracle to produce cookies for arbitrary usernames. Devise an attack to recover the secret. (There are both exponential and linear time attacks. Full credit for the linear-time attack.)

# IV Bonus: Anonymous Course Feedback

**This page is anonymous.** Rip this off from your exam, and turn it in separately if you like. You'll get five points for simply ripping off the last page of the exam, but I'd prefer if you fill it out and hand it in in a separate stack.

What are the things you like most about the course so far? Anything is fair game here (topics, course structure, board technique, etc.).

What are the things you like least about the course so far? Again, anything is fair game.

What topics would you like to see covered?

**Initials:**