College of Computing

Georgia Institute of Technology

CS 4235: Computer Security: Fall 2011

Quiz I

There are 12 questions and 8 pages in this quiz booklet (including this page). Answer each question according to the instructions given. You have **85 minutes** to answer the questions.

The last page is an easy, optional set of questions. *Rip this page off of your exam for five bonus points.* Turn it in anonymously.

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!

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 "CLOSED BOOK, CLOSED NOTES" QUIZ.
NO BOOKS, NO NOTES, NO OTHER MATERIALS, NO PHONES, NO COMPUTERS, NO LAPTOPS, NO PDAS.
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:

Do not write in the boxes below

1-5 (xx/19)	6-9 (xx/20)	10-12 (xx/11)	Bonus (5/5)	Total (xx/50)

Name:

I Warmup

1. [4 points]: Which of the following are true about the attack described in Ken Thompson's *Reflections on Trusting Trust*?

(Circle ALL that apply)

- **A.** The hacked compiler can insert arbitrary code into every program it compiles.
- **B.** The attack is only possible for compiled languages like C, but would not be possible for interpreted languages like Perl or Python.
- **C.** Inspecting the source code of the hacked compiler could reveal that the compiler was hacked.
- **D.** Inspecting the binary of the compiler could reveal that the binary was not the same as the "benign" compiler.
- **E.** All of the above.

Answer 1 The answer is: (D) ■

2. [4 points]: Which of the following are true about buffer overflows?

(Circle ALL that apply)

- **A.** Replacing `strcpy` and other memory-related functions with the corresponding functions that perform bounds checking (*e.g.*, `strncpy`) would eliminate all buffer overflow vulnerabilities.
- **B.** An operating system that allocates memory "up" on the stack instead of "down" can eliminate all buffer overflow vulnerabilities.
- **C.** A successful buffer overflow requires exact knowledge of where the return pointer is stored in memory on the stack.
- **D.** Buffer overflows require knowledge of the underlying processor architecture.
- **E.** All of the above.

Answer 2 The answer is: (A), (B), (D) ■

3. [4 points]: From the Denning paper on data security, which of the following are an example of inference control?

(Circle ALL that apply)

- **A.** Upon receiving an incorrect password for an existing username, a Web server returns "incorrect username or password".
- **B.** A database limits the number of queries that a user can issue in a given time period.

Initials:

C. A database only returns queries for a small group of authorized users.

D. An operating system prevents data from a secure database from being transferred to the Web server process.

E. All of the above.

Answer 3 The answer is: (A). ■

4. [4 points]: Which of the following can allow a worm to spread more quickly?
(Circle ALL that apply)

A. Scanning IP addresses in the same subnet as a machine that is already compromised.

B. Scanning for multiple vulnerabilities at once.

C. Scanning a list of target IP addresses in a random order from each compromised host.

D. Scanning for vulnerable hosts before launching the worm in the first place.

E. All of the above.

Answer 4 The answer is *all of the above* (E). ■

5. [4 points]: What techniques did security experts use to deconstruct/reverse engineer the Stuxnet malware?
(Circle ALL that apply)

A. Running the code in a controlled environment and observing its behavior.

B. Decompiling the code and studying the data structures in the software.

C. Running a "honeypot" to discover the geographic locations of compromised hosts.

D. All of the above.

Answer 5 The answer is: (B), (C). ■

Initials:

II Potpourri

6. [6 points]: Define the following four terms: threat, vulnerability, exploit, and attack. Explain, in the context of Stuxnet, an example of each.

(Answer legibly in the space below.)

Answer 6 ■

7. [5 points]: What is the difference between static analysis and dynamic analysis? Explain the relationship of security testing to decidability and explain why static analysis could never detect all security problems.

(Answer legibly in the space below.)

Answer 7 ■

8. [4 points]: Suppose that you were using "backscatter" attack traffic to try to estimate the size of a denial of service attack. You are monitoring backscatter traffic from a /8 IP address space, which is $1/256$ of all Inernet address space, and you see 1,000 TCP "backscatter" packet every second. How many packets per second is the denial of service attack?

Answer 8 ■

9. [5 points]: Define privilege escalation. Give an example of an attack involving privilege escalation in an automotive system (it is alright if your attack is hypothetical; it need not be one that was actually documented in the paper).

(Answer legibly in the space below.)

Answer 9 ■

III Design Question: Botnets

Emma Lerovads attended CS 4235 and has decided she can make millions selling the CS 4235 lecture notes. From the lecture on botnets, she remembers that botnets can be used to send large quantities of spam. She also remembers the how permutation scanning was used to share work across a large number of bots for vulnerability scanning and wants to apply the same idea to the work of launching the spam campaign.

10. [3 points]: From the paper *How to Own the Internet in Your Spare Time*, describe the process of permutation scanning and explain how it speeds up the process of finding vulnerable hosts.
(Answer legibly in the space below.)

Emma wants different bots to send email to a unique set of recipients, so she must somehow divide the labor across bots. To perform this load balancing, Emma decides to distribute the entire mailing list to each bot and run the following code on each bot to control which bot sends email to which victim:

```
procedure SENDEMAIL()
 comment: runs at each node
 comment: randomly permute order of email addresses in the mailing list
  Permute(mailingList);

  foreach (emailAddress) ∈ mailingList :
   comment: send the email to emailAddress
   sendMessage(emailAddress);
```

Emma notices that the above code isn't really doing exactly what she wants: although the recipients of her emails are getting the email quickly, the recipients are getting duplicate emails from each bot, because each bot is still sending email to every single email address in the list. She realizes that, instead of sending one mailing list to all of the bots, she should use what she learned about botnet command-and-control in class to distribute the workload. She re-designs her bot so that it simply takes the `sendMessage(emailAddress)` command from a centralized controller.

11. [2 points]: Describe one advantage and one disadvantage of using a single centralized controller to send the email commands to each bot.
(Answer legibly in the space below.)

Initials:

Answer 10 Distributing botnet command-and-control provides an additional amount of stealth (*i.e.*, because a single contact point can give rise to a large, anomalous traffic spike), and it also allows the botnet to potentially be more resilient by avoiding a single point of failure. On the other hand, distributing the control can make the botnet more difficult to control, since no one entity controls the botnet; additionally, ■

12. [6 points]: Describe how you would go about enumerating all of the IP addresses in the botnet for (1) a botnet where each bot executes the code above; (2) a botnet where each bot takes commands from a centralized controller.

(Answer legibly in the space below.)

Answer 11 ■

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: