CS426: Computer Security **Fall 2010**

Homework #3

Due date & time: 1:30pm on November 5, 2010. Hand in at the beginning of class (preferred), or email to the TA (twykoff@purdue.edu) by the due time.

Late Policy: You have three extra days in total for all your homeworks and projects. Any portion of a day used counts as one day; that is, you have to use integer number of late days each time. If you emailed your homework to the TA by 1:30pm the day after it is due, then you have used one extra day. If you exhaust your three late days, any late homework won't be graded.

Additional Instructions: (1) The submitted homework must be typed. Using Latex is recommended, but not required.

Problem 1 (10 pts) Identify and explain the buffer-overflow vulnerabilities in the following C code snippets, and give a corrected version of the code.

1.
```
char  buf[20];
char  prefix[] = "http://";
strcpy(buf, prefix);
strncat(buf, path, sizeof(buf));
```

2.
```
char buf[32];
strncpy(buf, data, strlen(data));
```

3.
```
#define MAX_BUF  256
void BadCode(char * input)
{
    short  len;
    char  buf[MAX_BUF];
    len = strlen(input);
    if (len < MAX_BUF)
        strcpy(buf, input);
}
```

Problem 2 (5 pts) Write a C function that contains a heap-overflow vulnerability, which is caused by an integer overflow vulnerability.

Problem 3 (5 pts) Recall that a security label consists of a security level and a set of categories. Given the security levels *public*, *confidential*, and *strictly confidential*, and the categories FACULTY, STAFF, and STUDENTS. How many labels can be constructed? Which labels dominate the label (confidential, STUDENT)? More generally, how many security labels can be constructed given n security levels and m categories.

Problem 4 (10 pts) Explain the following terminologies: Trusted Computer Base, Trusted Path, discretionary access control, mandatory access control, covert channels.

Problem 5 (15 pts) Read Part IA of the "The Protection of Information in Computer Systems" by Saltzer and Schroeder. For each of the eight principles listed there, write your understanding of the principle, give an instance of where it has been applied or where it should be applied.

Problem 6 (20 pts) Read the following two articles

- Ken Thompson's "Reflections on Trusting Trust"
- David A. Wheeler's "Countering Trusting Trust through Diverse Double-Compiling"

Write a brief summary which should include: (i) How the attack described in Thompson's article work? How can it be used to compromise the security of real world systems? What are the most effective ways to defend against the attack? What have you learned.

Problem 7 Clark-Wilson (20 points) Read the Clark-Wilson paper.

- D.D. Clark and D.R. Wilson. "A Comparison of Commercial and Military Computer Security Policies".

Answer the following questions.

- How would you compare the Biba integrity models and the Clark-Wilson integrity model.
- List the two or three most significant new insights you took away from the Clark-Wilson paper and the most significant flaws or weaknesses of it (if any).

Problem 8 Common Criteria Evaluation (15 points) Read the Common Criteria evaluation report of the Green Hills Software INTEGRITY-178B Separation Kernel, and discuss your assessment of the security of the software based on the report.