Tufts University
Department of Computer Science
COMP 116: Introduction to Computer Security
Fall 2016
Practice Quiz 3. Closed Book.

Quiz 3 will cover the following topics:

- Privacy
- Static analysis
- Dynamic analysis
- Forensics
- Anti-forensics
- Malware / viruses / worms / backdoors / tini / netcat

Actual Question from Fall 2015 Quiz 3.

Consider the following working program:

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int check (char *str)
{
  char buf[16];
  int flag = 0;

  strcpy(buf, str);
  if (strcmp(buf, "blinky_the_wonder_chimp") == 0) {
    flag = 1;
  }
  return flag;
}

int main(int argc, char *argv[]) {
  if (argc < 2) {
    printf("Perhaps use your first name as an argument. :-)\n");
    return 1;
  }
  if (check(argv[1])) {
    printf("Please send me an email with the subject: I believe that I will
win!\n");
  }
  else {
    printf("%s, you are doing a heckuvajob up to this point!\n", argv[1]);
  }
  return 0;
}
```

(2 points). Pinpoint the security vulnerability or vulnerabilities in the above code.

(2 points). TRUE | FALSE (circle one). A static analysis tool will pinpoint the security vulnerability in the above code.

(2 points). How can you fix the security vulnerability in the above code?

Answers

- The use of strcpy()
- True
- Use strnpy(). More: http://stackoverflow.com/questions/1258550/why-should-you-use-strncpy-instead-of-strcpy