CIS 751 Lecture Assignment 5

Chuck Zumbaugh

October 9, 2025

Let’s assume we have a stack that looks something like below:

Lower Addresses
EBP
EIP
Format string address
addr
Rest of input
Higher addresses

And also we have a program with the following:

```
int i = 0; // Some variable used in printf()
printf(input, &i); // Input is some user created data
```

We could then overwrite i, say with 11, using the string ”**Hello world%n**”. When executed, printf() will write the number of bytes printed (11 in this case) to the location pointed to by &i. However, we can also overwrite arbitrary stack locations provided we know the address we want to write to. When printf() encounters a format specifier it will call va_arg() and return the argument pointed to by va_list. Thus, we can specify an address to write to, and a number of format specifiers to move the va_list pointer to this address. We would need to move the pointer from somewhere in *Rest of input* to *addr* using input specifiers (ex %x). Then, when %n is encountered, it will write the number of bytes in printf() to that address.