Assignment 1: CS 63035-O01

Matthew Kirk

September 19, 2016

1 Understanding Buffer Overflow

1.1 Stack Buffer Overflow

https://en.wikipedia.org/wiki/Stack_buffer_overflow

```
#include <string.h>

void foo (char *bar)
{
   char  c[12];

   strcpy(c, bar);  // no bounds checking
}

int main (int argc, char **argv)
{
   foo(argv[1]);
}
```

1.2 Heap Buffer Overflow

https://cwe.mitre.org/data/definitions/122.html

```
#define BUFSIZE 256
int main(int argc, char **argv) {
  char *buf;
  buf = (char *)malloc(sizeof(char)*BUFSIZE);
```

```
  strcpy(buf, argv[1]);
}
```