Princeton University
COS 217: Introduction to Programming Systems
Common C Dynamic Memory Management Errors

Proper Sequence

```
int *pi;
int *newp;
...
pi = (int*)malloc(sizeof(int));
if(pi == NULL) ...
...
*pi = 5;
...
newp = (int*)realloc(pi, 2 * sizeof(int));
if(newp == NULL) ...
else pi = newp;
...
free(pi);
...
```

Memory Leak (alias Garbage Creation)

```
int *pi;
...
pi = (int*)malloc(sizeof(int));
...
*pi = 5;
...
pi = someothervalue;
...
```

Dangling Pointer (alias Dangling Reference)

```
int *pi;
...
pi = (int*)malloc(sizeof(int));
...
*pi = 5;
...
free(pi);
...
*pi = 6;
...
```

Dangling Pointer (Indirect)

```
int *pi1;
int *pi2;
...
pi1 = (int*)malloc(sizeof(int));
...
*pi1 = 5;
...
pi2 = pi1;
...
free(pi1);
...
*pi2 = 6;
...
```

Double Free

```
int *pi;
...
pi = (int*)malloc(sizeof(int));
...
*pi = 5;
...
free(pi);
...
free(pi);
...
```

Double Free (Indirect)

```
int *pi1;
int *pi2;
...
pi1 = (int*)malloc(sizeof(int));
...
*pi1 = 5;
...
pi2 = pi1;
...
free(pi1);
...
free(pi2);
...
```

Improper Expansion (fails NULL return case)

```
int *pi;
...
pi = (int*)calloc(5, sizeof(int));
...
pi = realloc(pi, 10 * sizeof(int));
...
*(pi+5) = 7;
...
free(pi);
...
```

Improper Expansion (fails relocation case)

```
int *pi;
...
pi = (int*)calloc(5, sizeof(int));
...
realloc(pi, 10 * sizeof(int));
...
*(pi+5) = 7;
...
free(pi);
...
```