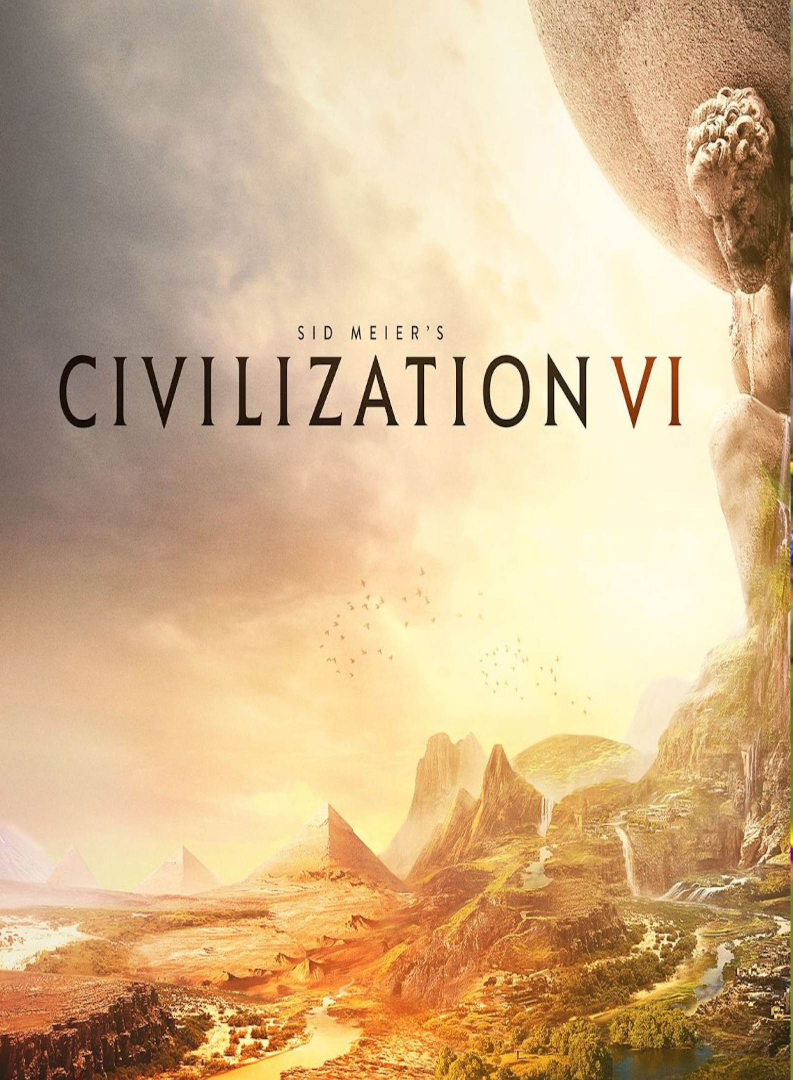
Hacking

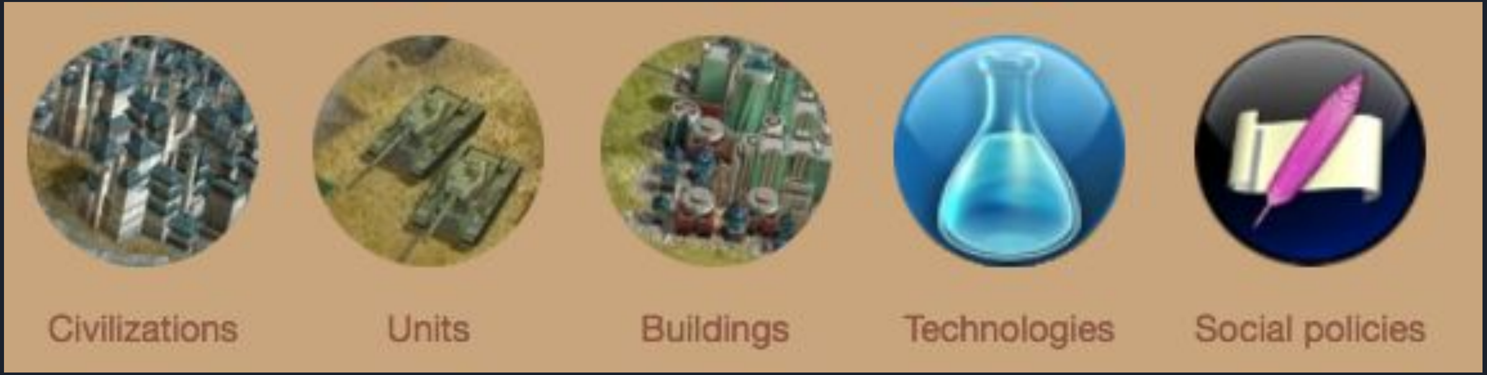
Ryan Busby

Expectations vs reality


SID MEIER'S
CIVILIZATION VI

Actions

Build, research, vote, ect.



Notable:

Diplomacy

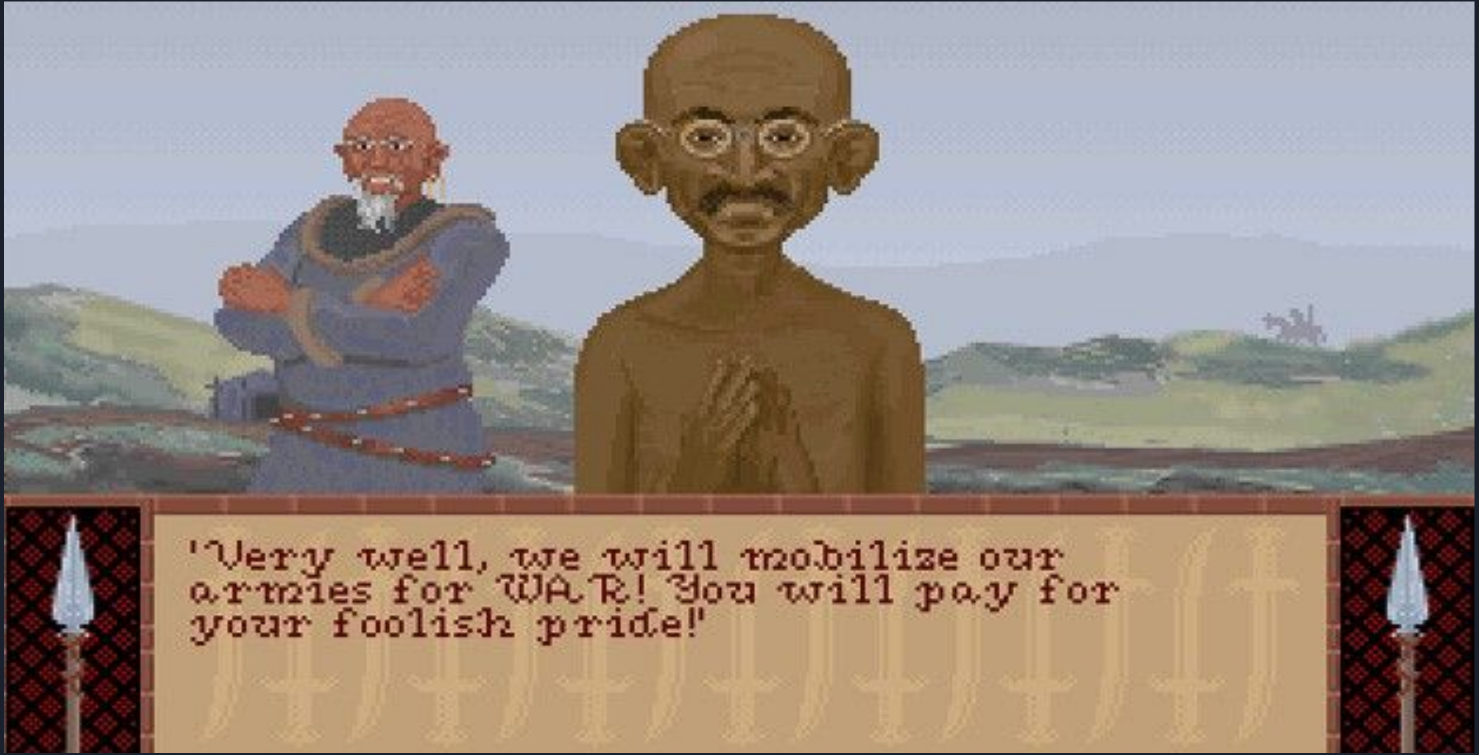
Lower threat with another target player.

Research nukes

Build nuclear missiles that can be upgraded.

PRACTICE
NONVIOLENCE

Why can’t we be friends?



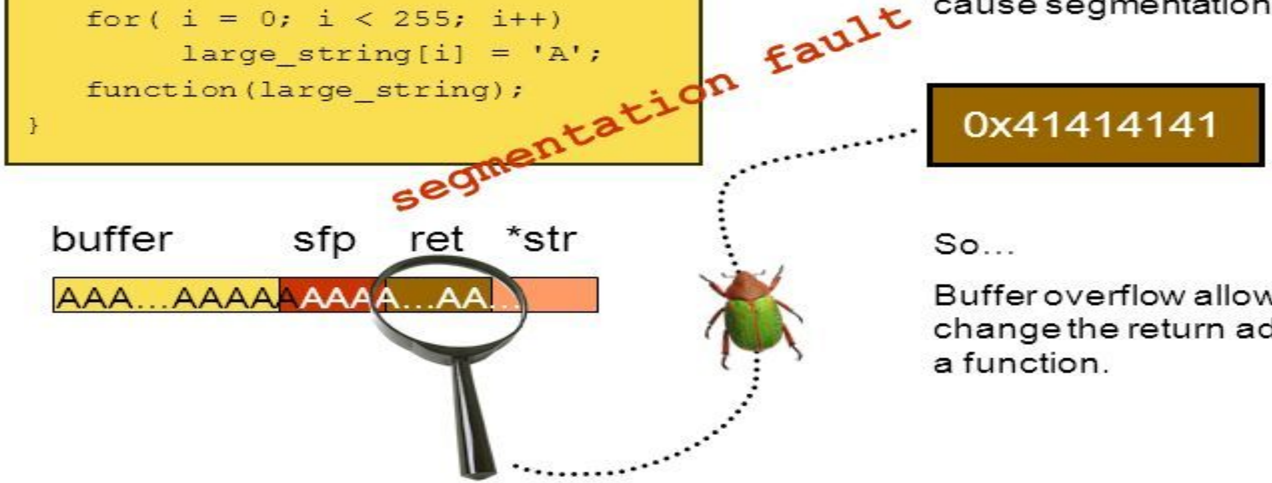
'Very well, we will mobilize our armies for WAR! You will pay for your foolish pride!"

Buffer Overflow!

```
void function(char *str) {
   char buffer[16];
   strcpy(buffer,str);
}

void main() {
   char large_string[256];
   int i;
   for( i = 0; i < 255; i++)
         large_string[i] = 'A';
   function(large_string);
}
```

- strcpy() copies the supplied string over the smaller buffer in stack without bound checking.
- 240 bytes from the end buffer are overwritten.
- The program will most likely cause segmentation Fault.



So...

Buffer overflow allows us to change the return address of a function.