



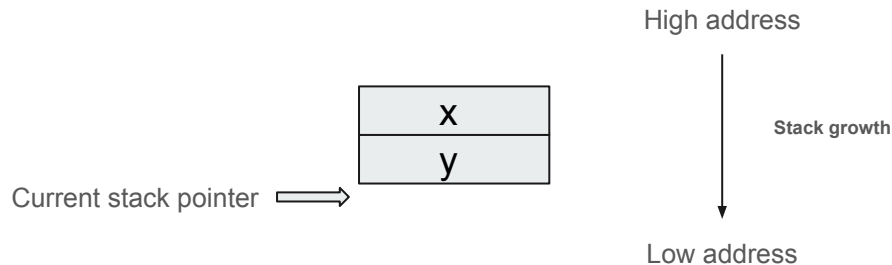
Security Vulnerabilities - Crash course

Holistic Software Security

Aravind Machiry

101: Runtime stack grows down

```
void bar() {  
    printf("Hello\n");  
}  
void foo() {  
    bar();  
    y:..  
}  
void main() {  
    foo();  
    x:..  
}
```





Stack Based Buffer Overflow



Race Condition to Memory Corruption



Temporal Vulnerabilities



References

Basics: <https://www.youtube.com/watch?v=VroEiMOJPm8>

Wargames: <https://overthewire.org/wargames/> , <https://pwnable.kr/>

Temporal vulnerabilities exploitation: <https://github.com/shellphish/how2heap>