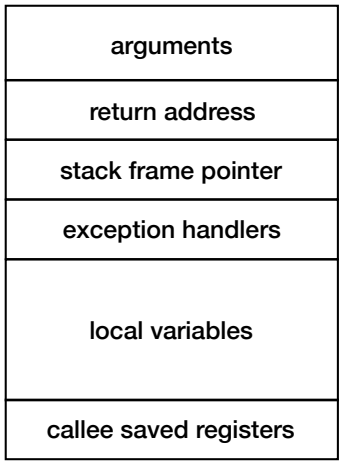
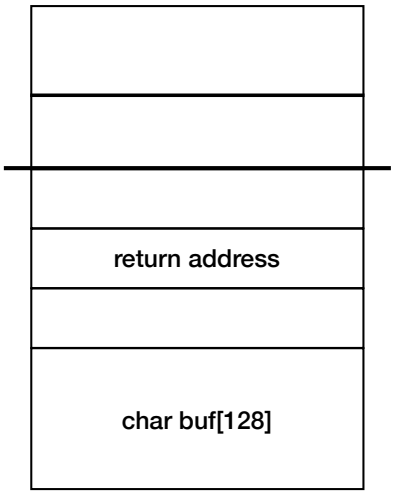
Stack Frame



A buffer overflow



Exploits can result in:

Basic problem that causes control hijacking:

"buffer overflows remain one of the top ranking vulnerabilities year over year" - 25 years of Vulnerabilities: 1988 - 2012

Some defenses:	Non-executable memory	Randomization	Canaries
1. Fix bugs			
2. Platform defenses		→	
3. Add runtime code			
What is the result of many of these defenses?	How could an attacker bypass this?		

Heartbleed (2012 - 2014)

1. What is the TLS heartbeat extension?

2. What is the bug in the heartbeat extension? How was it introduced?

3. What does this bug allow an attacker to do (what is the exploit)?

4. Can someone detect if the Heartbleed exploit has been used against them?

5. What was impacted by the Heartbleed exploit?

WannaCry ransomware (2017)

1. What did the WannaCry ransomeware attack do?

2. What exploit was used in this attack? How does it work?

3. What does this exploit allow the attacker to do?

4. Roughly how many computers were affected by this attack?

5. What "mistake" did the WannaCry ransomware make with prime numbers that was used to help stop it?