Stack layout
Data-modifying attack
Code-running attack
Stack frames of the calling procedure, the caller's caller, and so forth
Return address
Other values
Input buffer
Other values
Free space
Stack frame of the procedure processing the input
Stack frames of the calling procedure, the caller's caller, and so forth
Return address
Overwritten values
Very long input that exceeds the buffer size
Other values
Free space
Stack frames of the calling procedure, the caller's caller, and so forth
Address of attack code
Overwritten values
Attack code
Other values
Free space
(a)
(b)
(c)