

Buffer Overflow Attack

Abijith K P
Bosco Frank Paul
Krishna Pingal
K S Kurian

September 26, 2013

Overview

1 What is Buffer Overflow

2 What we are doing

3 Mark distribution

What is Buffer Overflow

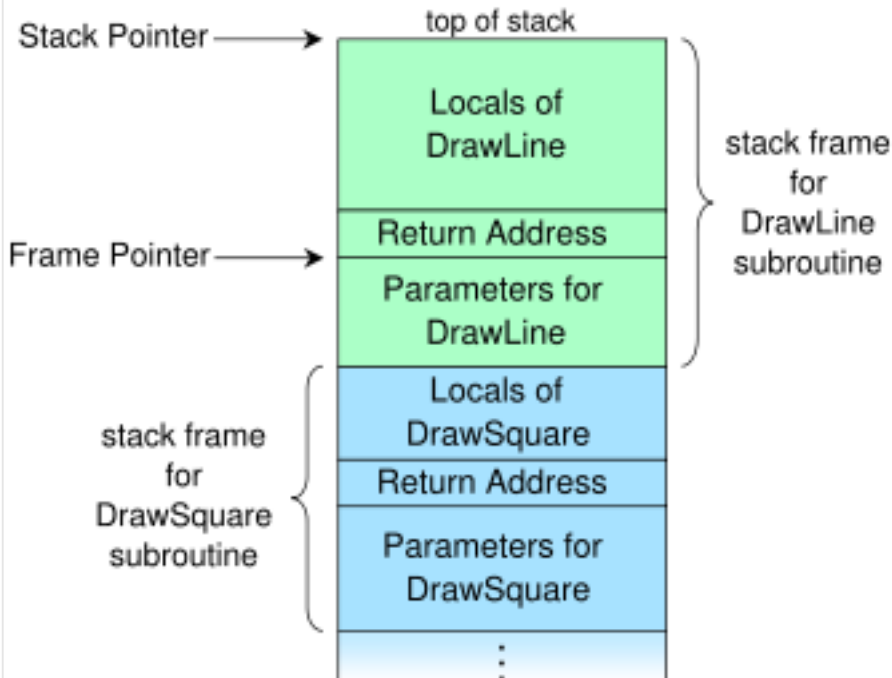
- While writing data to buffer

What is Buffer Overflow

- While writing data to buffer
- Overruns the buffer's boundary

What is Buffer Overflow

- While writing data to buffer
- Overruns the buffer's boundary
- Overwrites adjacent memory.



What we are doing

- Overwriting the return address in a stack frame: Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input filled buffer

What we are doing

- Overwriting the return address in a stack frame: Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input filled buffer
- Overwriting a local variable that is near the buffer in memory on the stack to change the behavior of the program which may benefit the attacker

Mark distribution

- Final Presentation: 30 marks

Mark distribution

- Final Presentation: 30 marks
- Team completing the task: 70 marks

Mark distribution

- Final Presentation: 30 marks
- Team completing the task: 70 marks
- Hands on demonstration: 100 marks

Mark distribution

- Final Presentation: 30 marks
- Team completing the task: 70 marks
- Hands on demonstration: 100 marks
- Total: 200 marks

Thank You