Buffer Overflow

What is a buffer?

- A Buffer is a temporary area for data storage. It is normal speed data storage which is mostly used for I/O operations.
- It prevents data congestion from an incoming to an outgoing port of transfer.
- It is a part of RAM and its policy is first-in, first-out.

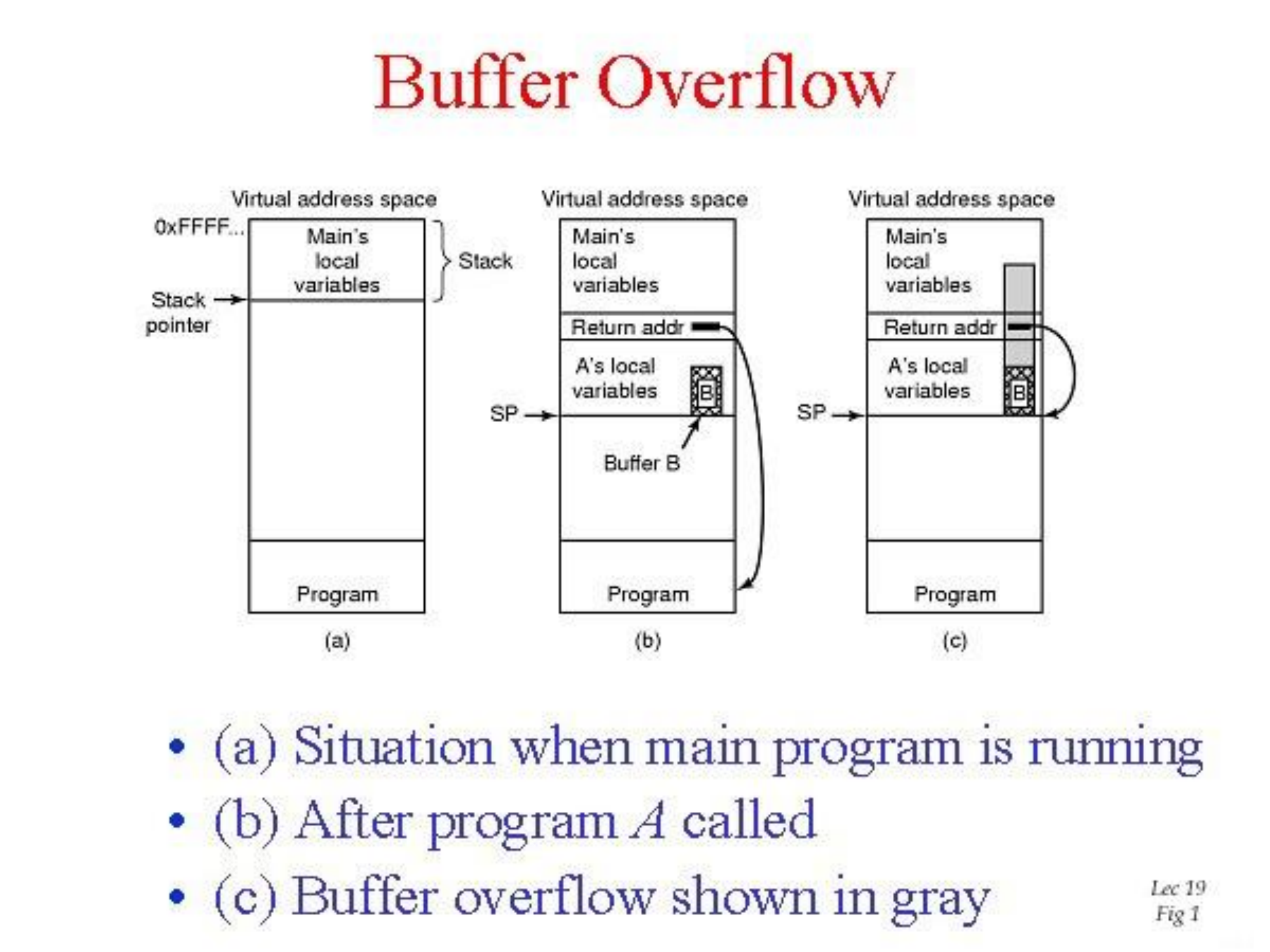
Buffer Overflow Attack

- When more data (than was originally allocated to be stored) gets placed by a program or system process, the extra data overflows. It causes some of that data to leak out into other buffers, which can corrupt or overwrite whatever data they were holding.
- In a buffer-overflow attack, the extra data sometimes holds specific instructions for actions intended by an attacker.
- Attacker would use a buffer-overflow exploit to take advantage of a program that is waiting on a user’s input.
- Buffer overflows can result in system crashes, corrupted data, user privilege escalation, or just anything an attacker can think of.

Buffer Overflow Attack

- There are two types of buffer overflows 1.Stack based and 2.Head based
- Poor programming quality controls and not including input validation checks in software leads to buffer overflow attack.
- The only countermeasures to buffer overflow attacks are to patch the software when issues are discovered and to properly code software to perform input validation checks before accepting input.

Example



Buffer Overflow

- (a) Situation when main program is running
- (b) After program *A* called
- (c) Buffer overflow shown in gray

Lec 19
Fig 1