Buffer overflow discussion

Buffer overflow often come from innocent programmer oversights or failures to document and check for excessive data. Also its a condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. That is the condition attackers exploit to crash a system or to insert specially crafted code that allows them to gain control of the system. Attacks can be perpetuated through; first, identification of a buffer overflow vulnerability that can be triggered using externally sourced data under the attackers control or understanding of how that buffer will be stored in the process memory and hence the potential for corrupting adjacent memory locations and potentially altering the flow of execution of the program.