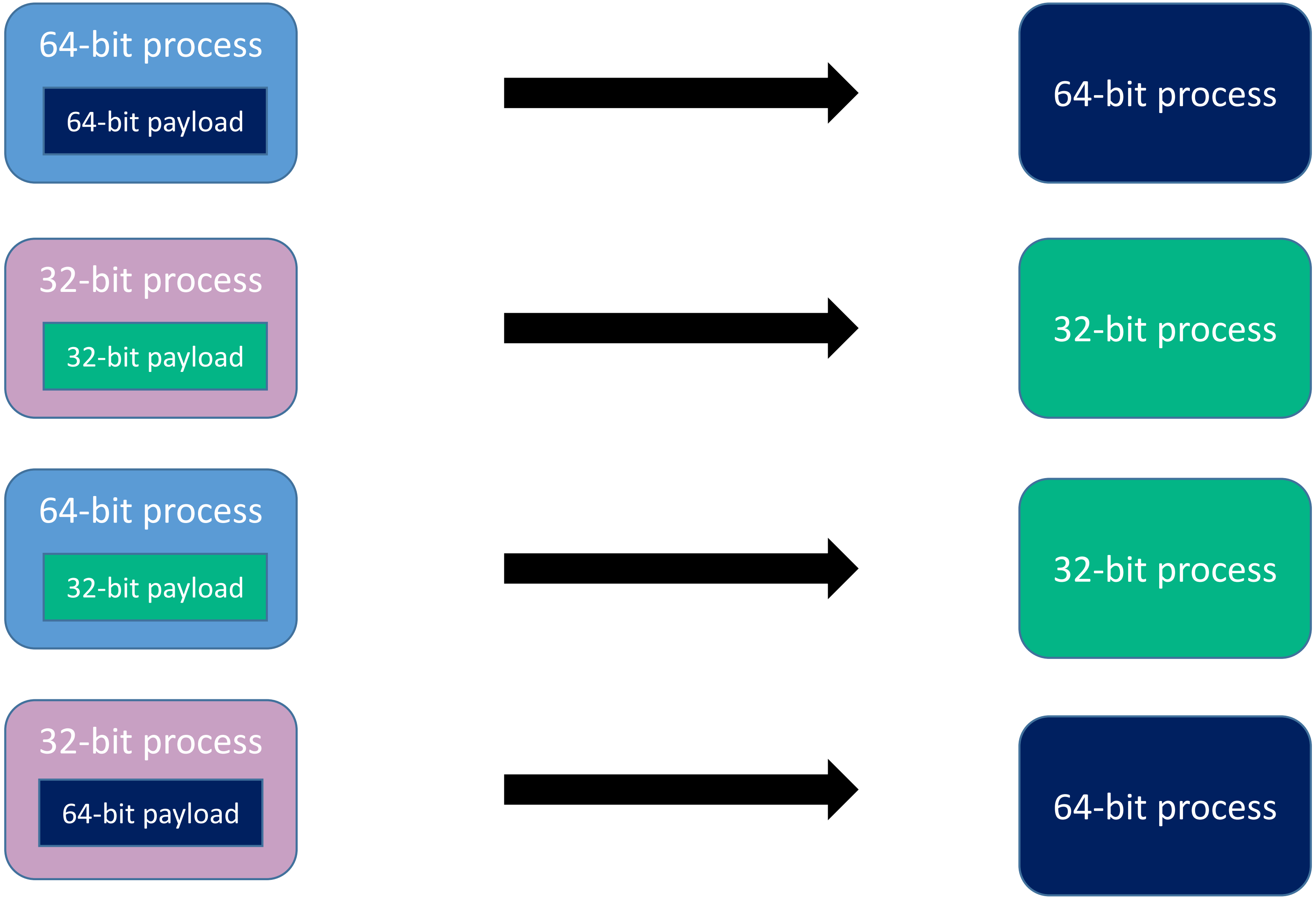
32-bit to 64-bit cross injections

How to inject 64 bit payload into 64-bit processes using 32-bit processes

Types of Cross Injections



64-bit process

64-bit payload

64-bit process

32-bit process

32-bit payload

32-bit process

64-bit process

32-bit payload

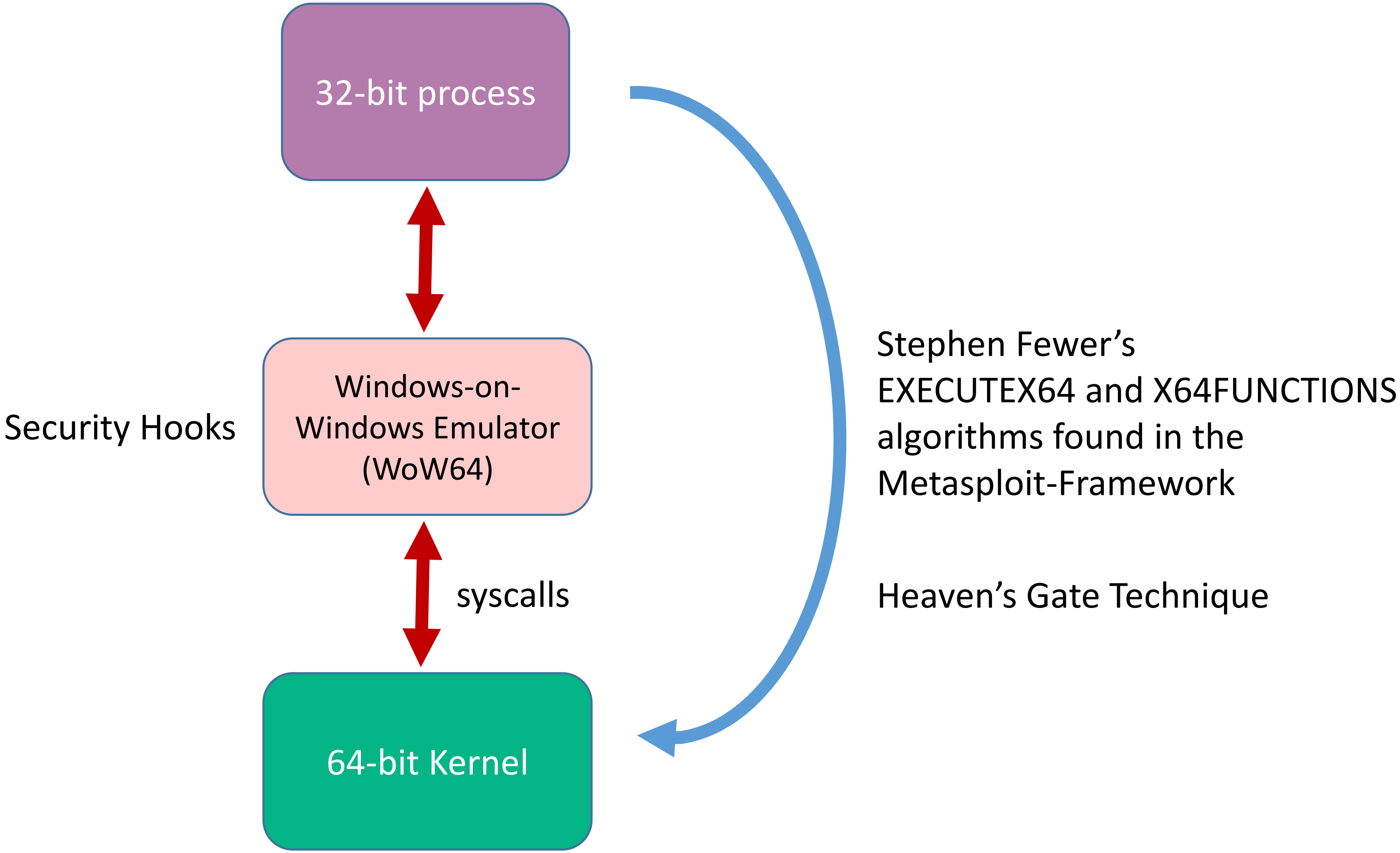
32-bit process

32-bit process

64-bit payload

64-bit process

How 32-bit applications run on 64-bit System



32-bit process

Security Hooks

Windows-on-Windows Emulator (WoW64)

syscalls

64-bit Kernel

Stephen Fewer’s EXECUTEX64 and X64FUNCTIONS algorithms found in the Metasploit-Framework

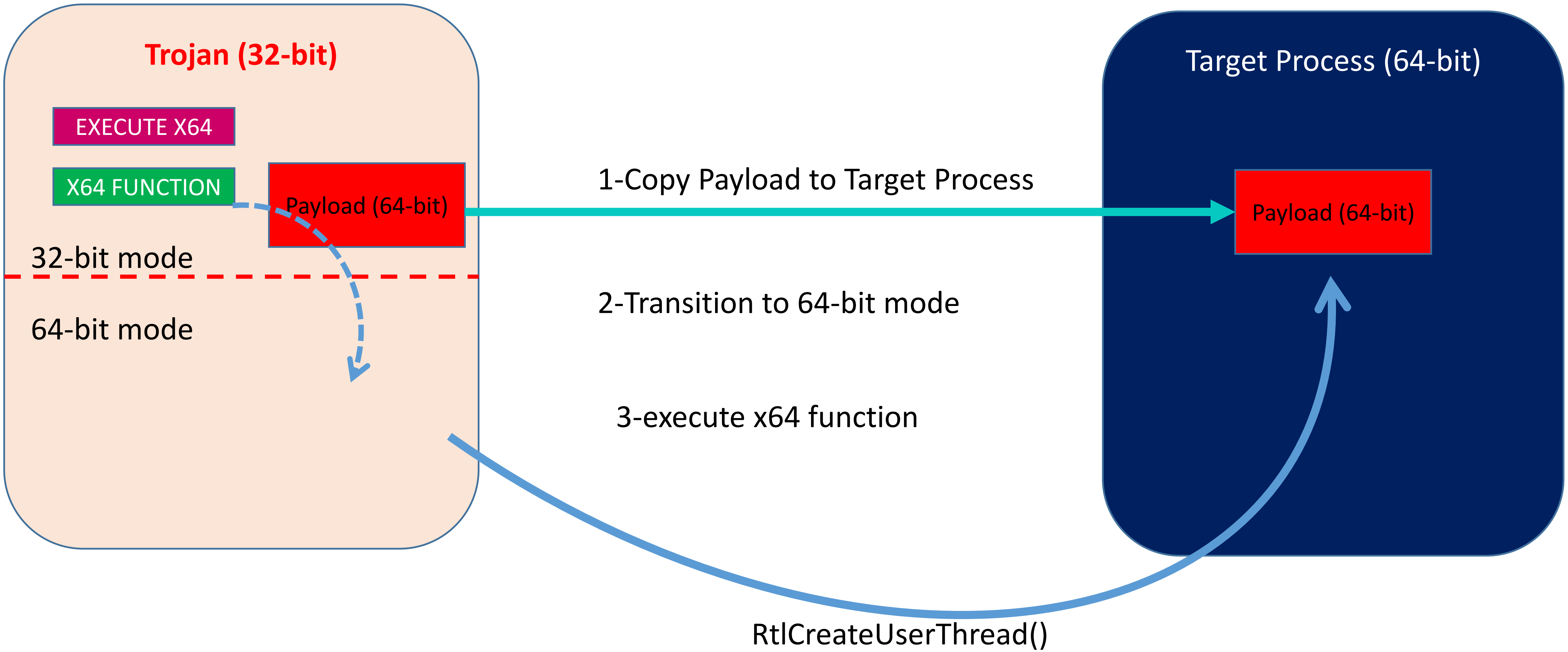
Heaven’s Gate Technique

Advantages of Heaven’s Gate Cross Injection

- Heaven’s Gate bypasses the security measures of WoW64 emulator
- AV and security hooks which depends on WoW64 is therefore evaded

Ref:
https://www.fireeye.com/blog/threat-research/2020/11/wow64-subsystem-internals-and-hooking-techniques.html
https://github.com/rapid7/metasploit-framework/blob/master/external/source/shellcode/windows/x86/src/migrate/executex64.asm

32-bit to 64-bit cross injection



Thank you