heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Seoul National University
College of Engineering
Dept. of Computer Science and Engineering

Introduction to Social Networks

Summer University 2017
Seoul, Republic of Korea

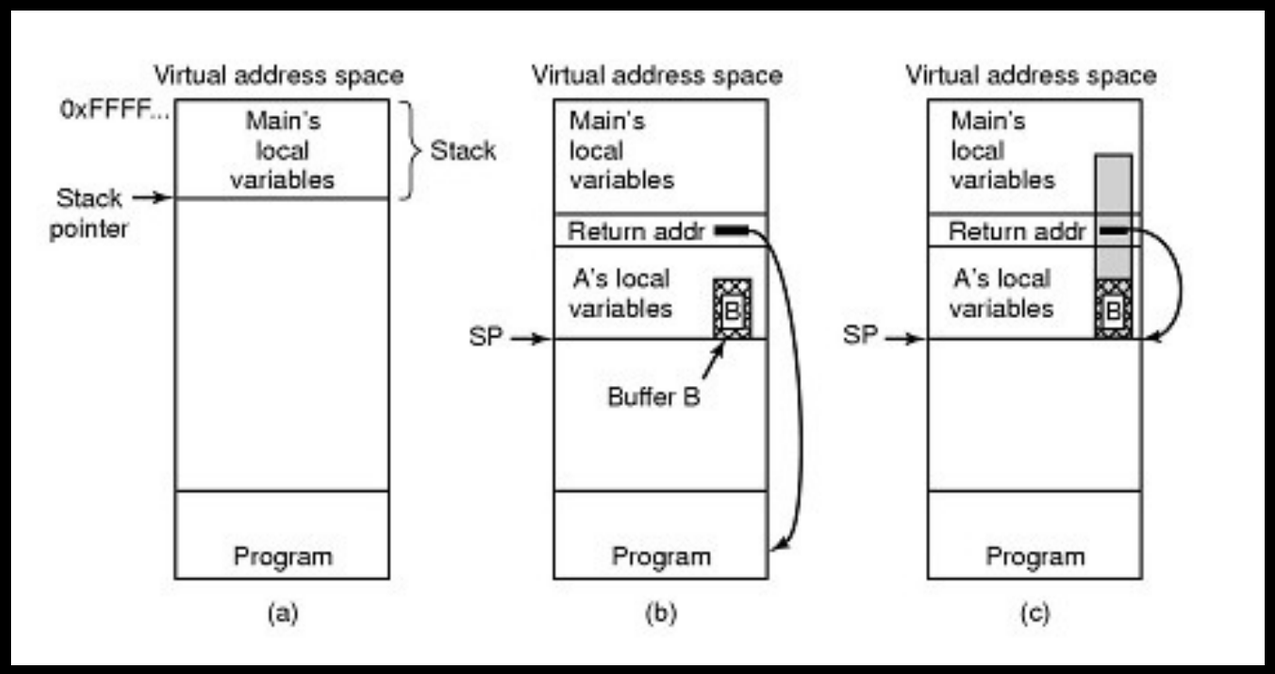
Alexandre Karlov

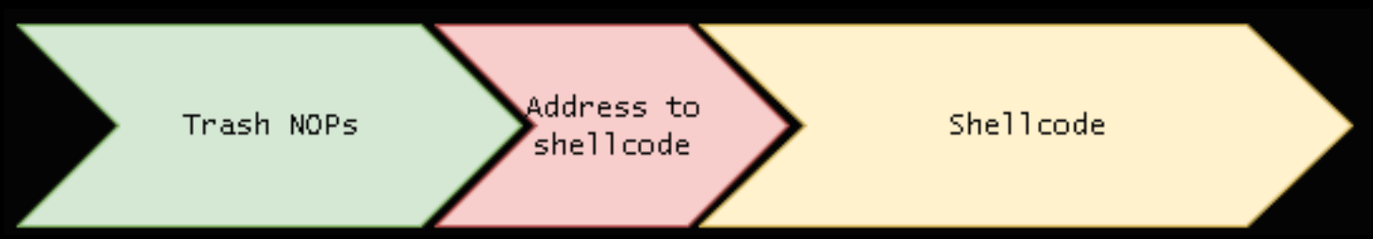
Today

- Binary exploitation and ROP
- ...

0x06 Binary Exploitation

Reminder: Basic Buffer Overflow

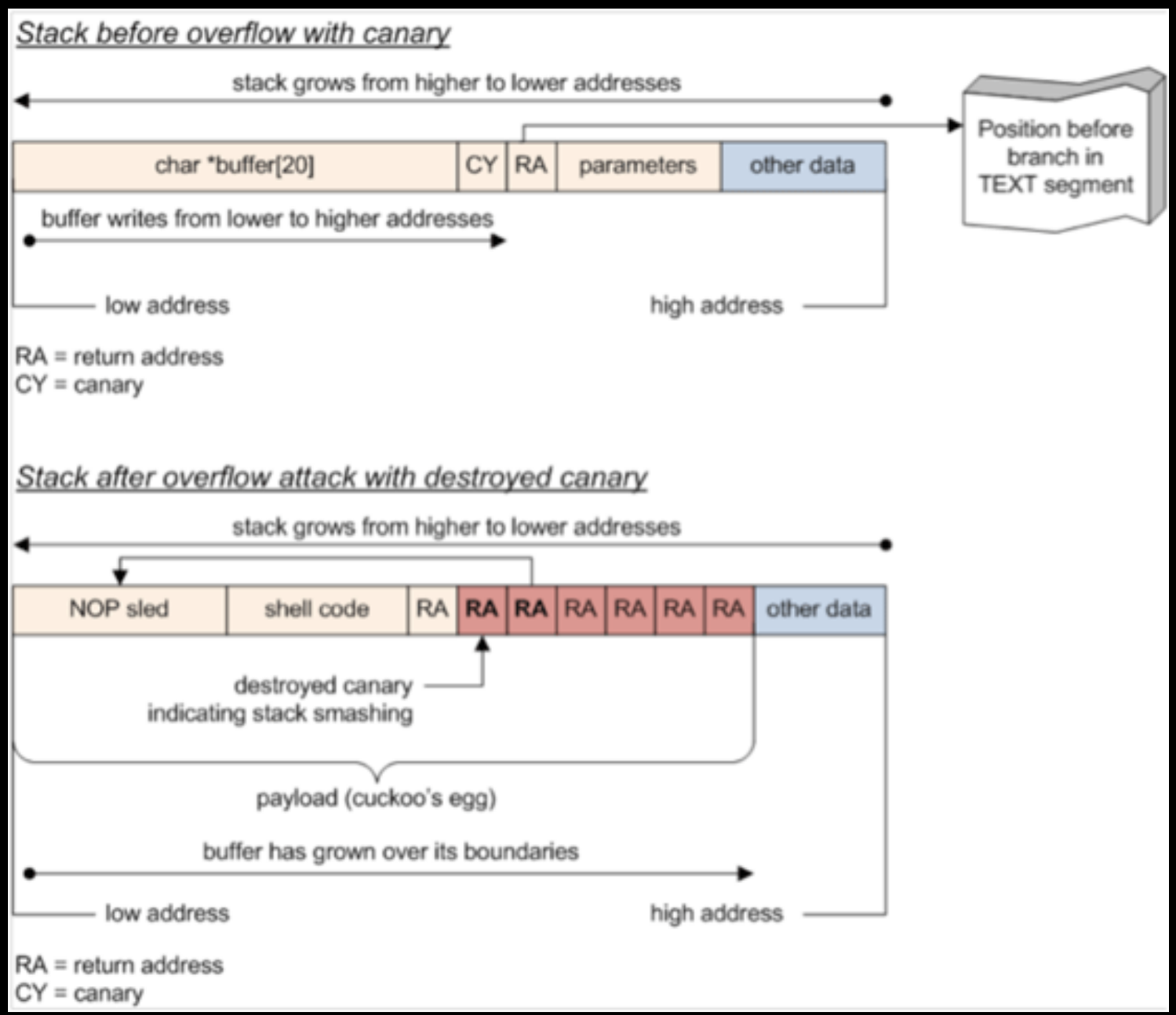




Reminder: Basic Buffer Overflow

- Assumptions:
  - Program local address space does not change
  - Executable stack
  - No stack protection
- It does not exist anymore today
  - Except some old legacy embedded systems...

Stack Protection



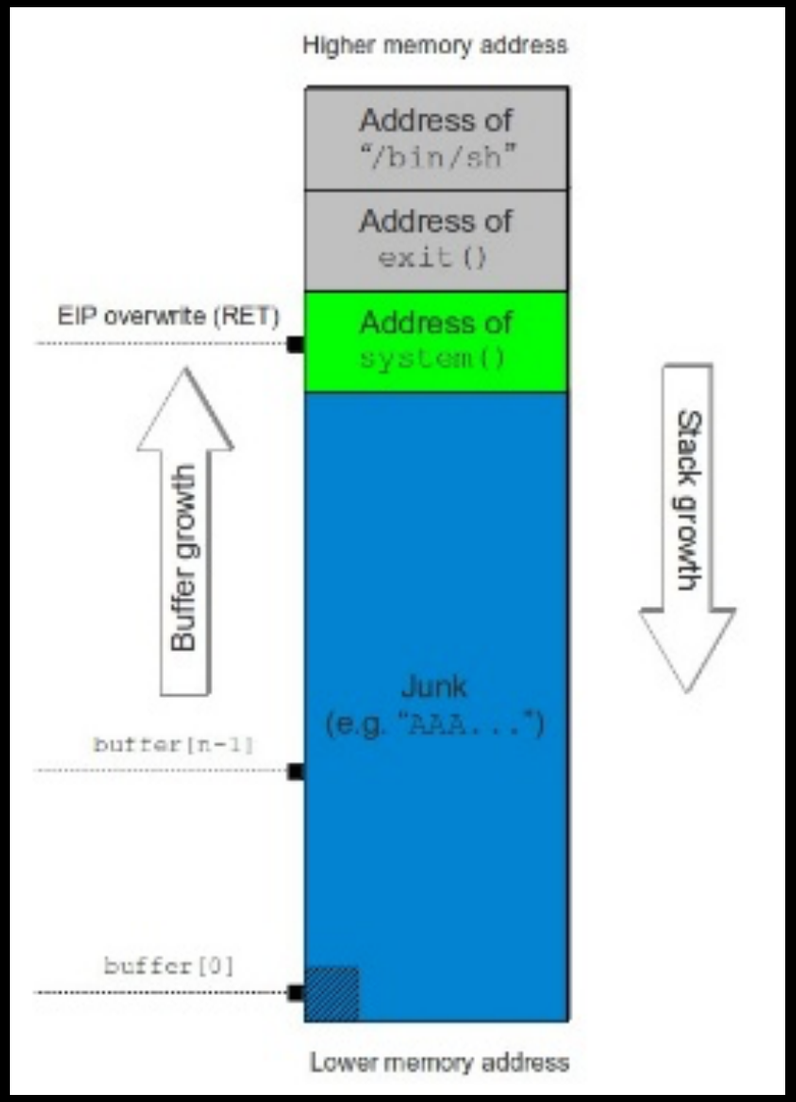
Stack Protection: bypass

- The canary is generated randomly at process start
- value written in the stack before local vars
- compiler inserts the check before ret
- But if this value:
  - is leaked
  - or is predictable
  - it's basically game over

Non-executable memory pages

- Why stack has to be executable ?
- Memory page should usually contain either code or data
  - but not mix them
- NX bit

Ret2lib

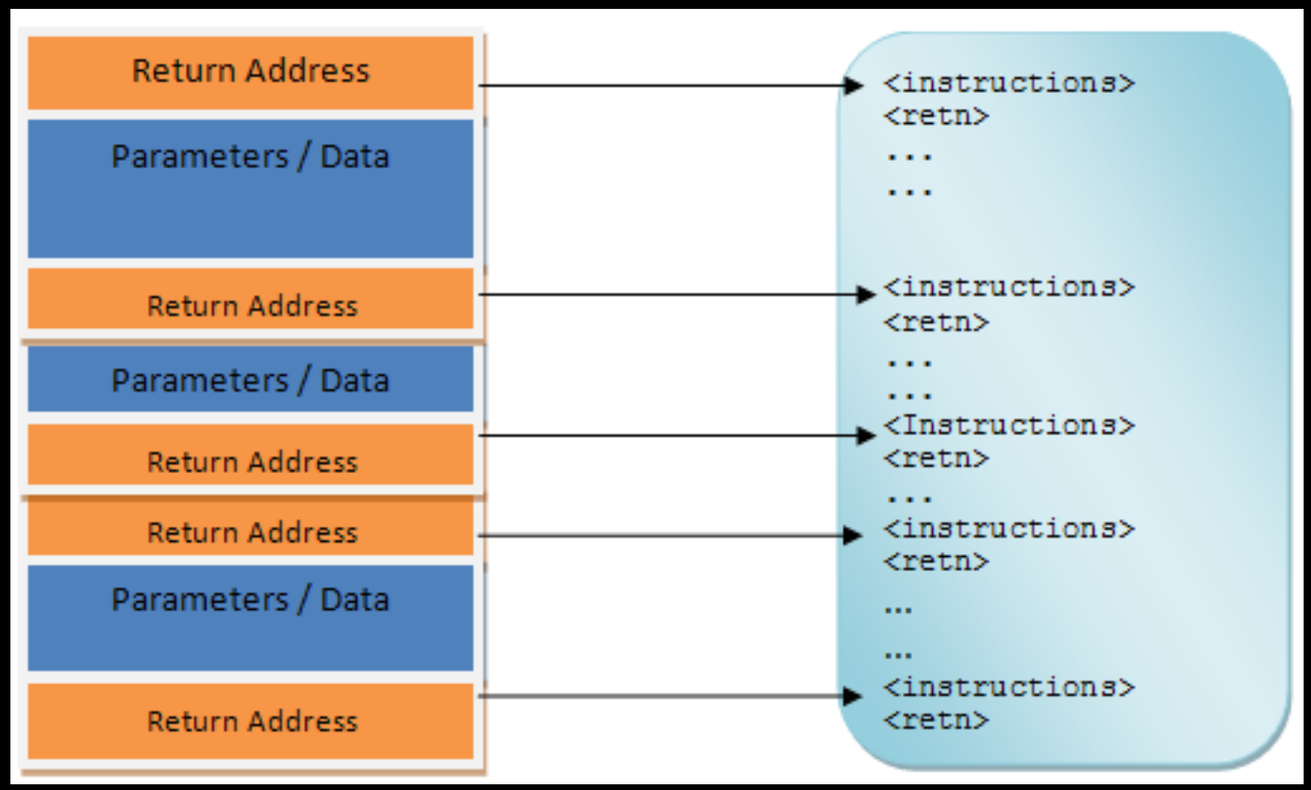


Mind the calling convention

Return-Oriented Programming

- ret2libc generalisation
- execute simple instructions already present in memory (followed by a ret)
- called Gadgets
  - pop eax ; ret
  - mov [ebx], ecx ; ret

Return-Oriented Programming



Return-Oriented Programming

- So how do you build a ROP chain ?
- Requires understanding of the underlying assembly and architecture
- Some tools to help you:
  - ropgadget, roper, ...

Return-Oriented Programming

- Some use cases:
  - redirect execution to register
  - stack-pivot (define your own fake stack)
  - set register to value
  - read memory at address
  - syscall
  - ...