Reverse Engineering (Basic)

Andrey Ferriyan (andrey@sfc.wide.ad.jp)
ISC-SEC

7-6-2017

Outline

- Concept of RE
- Tools for basic RE
- Prepare environment
- Exercise
- CLI Main Commands
- Visual Mode
- CrackMe Exercise

RE CONCEPT

RE Concept

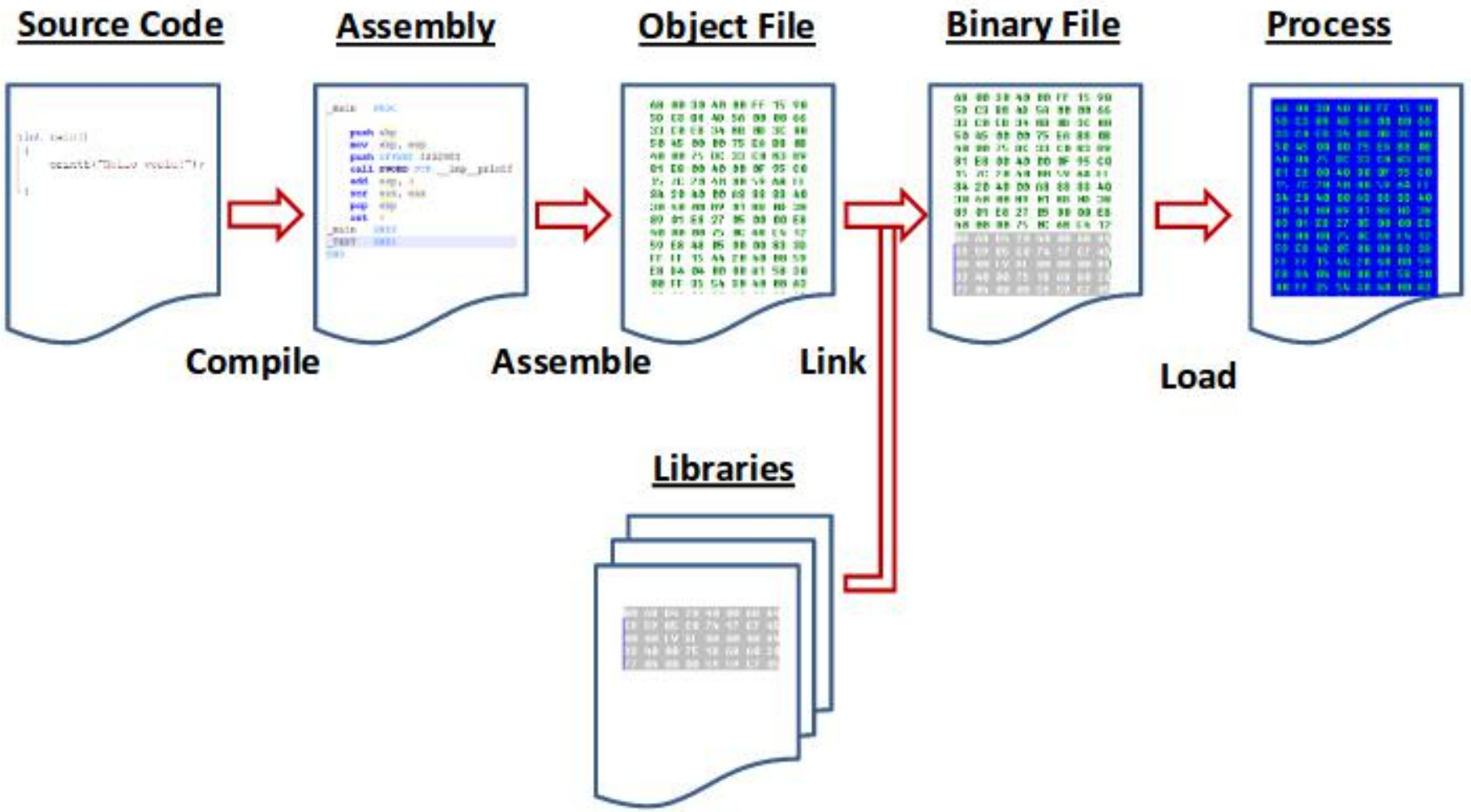

Figure 1. Compile, Assemble, Running (source: security.cs.rpi.edu)

RE Concept

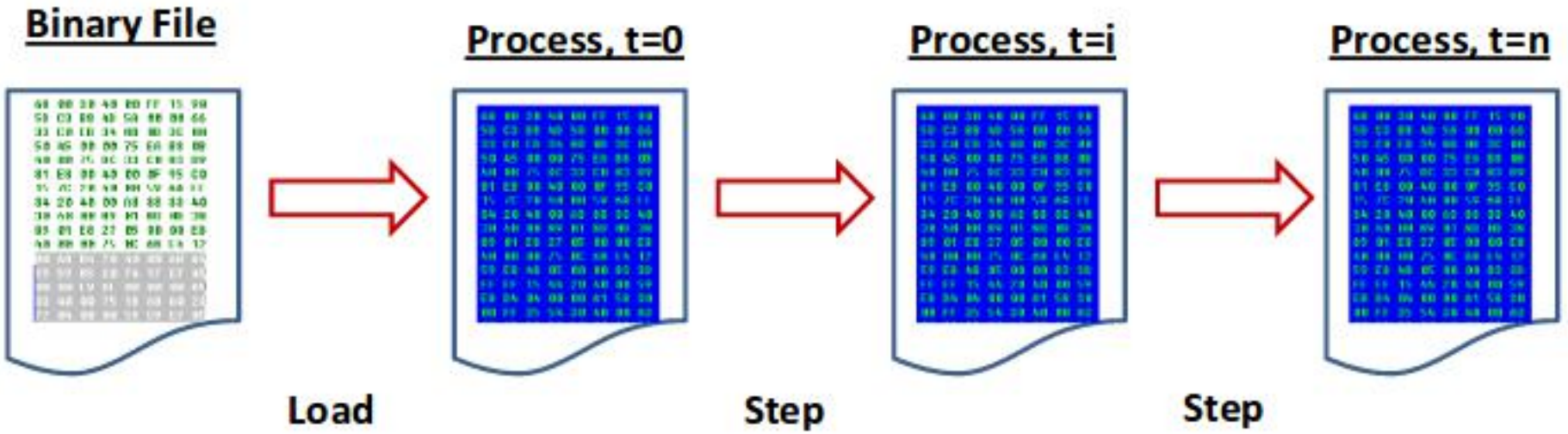

Figure 2. RE Domain (source: security.cs.rpi.edu)

RE Concept

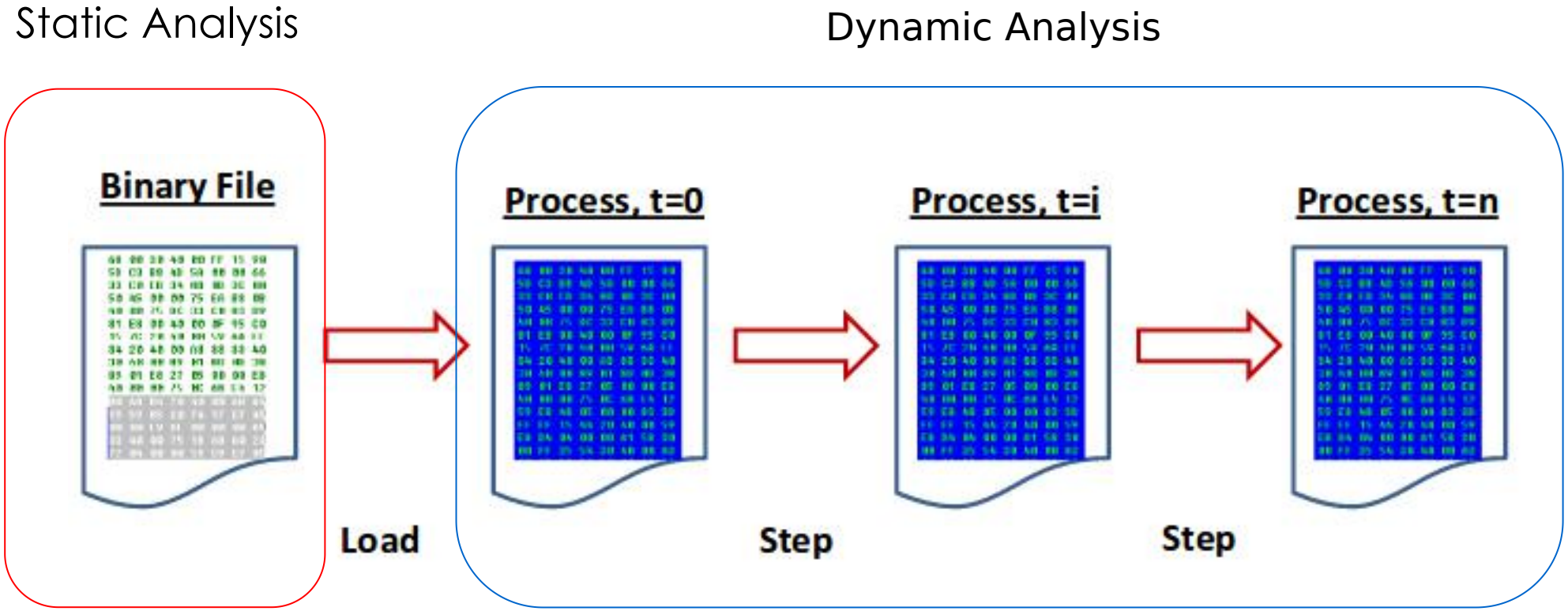

Figure 3. RE Domain (source: security.cs.rpi.edu)

Tools for Basic RE

Tools for basic RE

- radare2 (open source)
  - http://www.radare.org/r/
  - https://github.com/radare/radare2
- gdb (open source)
  - Every GNU/Linux
- IDA (closed source):
  - https://www.hex-rays.com/products/ida/index.shtml
- Binary Ninja (closed source)
  - https://binary.ninja
- Hopper (closed source)
  - https://www.hopperapp.com/

Prepare Environment

- GNU/Linux or Mac
- Installing radare2
- GNU/Linux:
  - Debian-based: sudo apt install radare2
  - Mac: brew install radare2
  - Windows: https://github.com/radare/radare2-win-installer (I'm not testing yet !)
- Use terminal

Prepare Environment

- Download the files:
  - https://andrey.web.id/re/re.tar.gz
- Extract into your folders
- Structure inside zip files
  - challenges.zip (source: security.cs.rpi.edu)
  - re

Exercise

- Enter re folder:
  - test1.c
  - test2.c
- Compile test1.c
  - gcc test1.c -o test1
  - ./test1

Exercise: Inside test1.c

```
#include <stdio.h>


int main(){
        int a = 10;
        int b = 20;
        int c = a+b;
}
```

Exercise

$ r2 test1

[0x004003e0]> aa

[0x004003e0]> pdf@sym.main

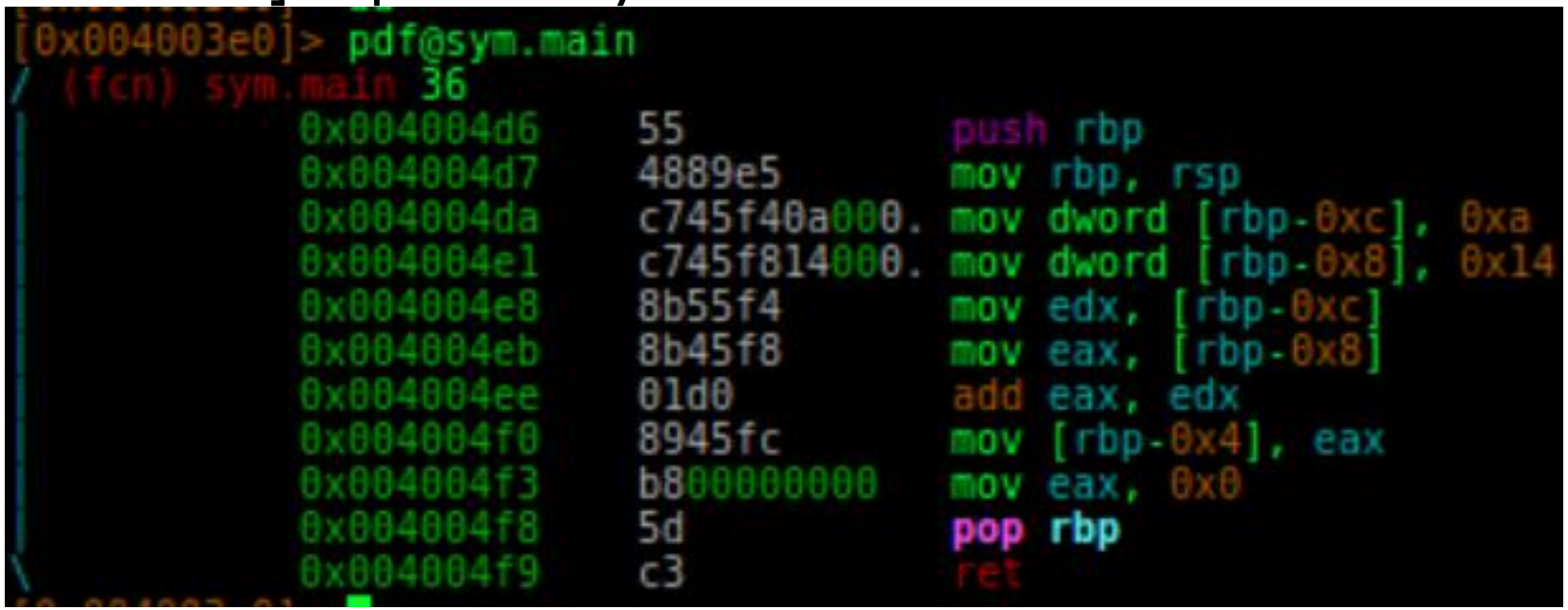

Figure 4. r2 sym.main

CLI Main Commands

Exercise: steps for RE

Radare2 contains several binary for RE

- Determine the binary file
  - PE (for windows) or ELF (GNU/Linux)
  - Practice:
    - $ rabin2 -I <filename>
    - $ rabin2 -I test1
  - Result: ?
    - some important parameters:
      - class : (ELF32 or ELF64)
      - arch
      - machine

Exercise: steps for RE

- Every character has a meaning (e.g. w=write, p=print)
- Every command is documented with **command?** (e.g. pdf?)
- r2 test1
- [0x004004c0]> aa
- [0x004003e0]> a?
- -- snippet--
- aa ; analyze all (fcns + bbs)

Exercise: steps for RE

- rax2
- rabin2
- rasm2
- radiff2
- rafind2
- rahash2
- radare2
- rarun2
- ragg2/ragg2-cc

Radare2 Visual Mode

radare2 visual mode

- r2 test2
- [0x004004c0]>V

```
[0x004004c0 336 test2]> x @ entry0
- offset -   0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0x004004c0  31ed 4989 d15e 4889 e248 83e4 f050 5449  1.I..^H..H...PTI
0x004004d0  c7c0 a006 4000 48c7 c130 0640 0048 c7c7  ....@.H..0.@.H..
0x004004e0  b605 4000 e8a7 ffff fff4 660f 1f44 0000  ..@.......f..D..
0x004004f0  b84f 1060 0055 482d 4810 6000 4883 f80e  .O.`.UH-H.`.H...
0x00400500  4889 e576 1bb8 0000 0000 4885 c074 115d  H..v......H..t.]
0x00400510  bf48 1060 00ff e066 0f1f 8400 0000 0000  .H.`...f........
0x00400520  5dc3 0f1f 4000 662e 0f1f 8400 0000 0000  ]...@.f.........
0x00400530  be48 1060 0055 4881 ee48 1060 0048 c1fe  .H.`.UH..H.`.H..
0x00400540  0348 89e5 4889 f048 c1e8 3f48 01c6 48d1  .H..H..H..?H..H.
0x00400550  fe74 15b8 0000 0000 4885 c074 0b5d bf48  .t......H..t.].H
0x00400560  1060 00ff e00f 1f00 5dc3 660f 1f44 0000  .`......].f..D..
0x00400570  803d d10a 2000 0075 1155 4889 e5e8 6eff  .=.. ..u.UH...n.
0x00400580  ffff 5dc6 05be 0a20 0001 f3c3 0f1f 4000  ..].... ......@.
0x00400590  bf20 0e60 0048 833f 0075 05eb 930f 1f00  . .`.H.?.u......
0x004005a0  b800 0000 0048 85c0 74f1 5548 89e5 ffd0  .....H..t.UH....
0x004005b0  5de9 7aff ffff 5548 89e5 4883 ec10 897d  ].z...UH..H....}
0x004005c0  fc48 8975 f083 7dfc 0274 2048 8b45 f048  .H.u..}..t H.E.H
0x004005d0  8b00 4889 c6bf b406 4000 b800 0000 00e8  ..H.....@.......
0x004005e0  9cfe ffff b800 0000 00eb 3748 8b45 f048  ..........7H.E.H
```

Crackme Exercise

CrackMe Password

```
$ ./test2
Usage : ./test2 password
$ ./test2 WhatIsThePassword
Wrong Password!
```

HOW TO CRACK THE PASSWORD ???!!!

CrackMe Password

```
$ r2 test2
[0x004004c0]> aa
[0x004004c0]> pdf@sym.main
[0x004004c0]> iz
[strings]
addr=0x004006b4 off=0x000006b4 ordinal=000 sz=20 section=.rodata string=Usagespassword
addr=0x004006c9 off=0x000006c9 ordinal=001 sz=11 section=.rodata string=HollyMolly
addr=0x004006d4 off=0x000006d4 ordinal=002 sz=20 section=.rodata string=RightPassword
addr=0x004006e8 off=0x000006e8 ordinal=003 sz=16 section=.rodata string=WrongPassword
```

NOW YOUR TURN