REVERSINGLABS

Što je novo u svijetu reversinga?

Tomislav Zubčić, CIS FER 2018.

Prethodna predavanja

- Branko Spasojević, Čudesan svijet reverznog inženjerstva, 2013. [1]
- Robert Perica, (un)packeri – alati za zaštitu ili napad, 2014. [2]
- Žad Deljkić, Natjecanja u informacijskoj sigurnosti, 2017. [3]

Sadržaj

- Debuggeri i disassembleri
- Decompileri
- Metode za zaštitu
- Biblioteke i razvoj vlastitih alata
- Dynamic binary instrumentation
- Solveri i symbolic/concolic execution
- Deobfuskacija koda
- Analiza formata koji ne sadrže nativni kod

Debuggeri/disassembleri

- OllyDbg
- x64dbg
- Hopper
- Radare2
- IDA Pro
- Binary Ninja

Decompileri

- Snowman
- RetDec
- Hopper
- Hex-Rays
- JEB

Metode za zaštitu

- Pakiranje/kriptiranje izvršnih datoteka
- Detekcija debuggera
- Obfuskacija koda
- Virtualne mašine

Biblioteke

- Disasembleri
- Asembleri
- Emulacija koda

Biblioteke - disasembleri

- Bea Engine
- Intel XED
- Capstone engine
- Zydis

Biblioteke - asembleri

- Xbyak
- AsmJit / AsmTK
- Keystone engine

Biblioteke – emulacija koda

- libx86emu
- Unicorn engine

Dynamic Binary Instrumentation

- Analiza ponašanja aplikacija tokom izvršavanja
- Ubacivanje koda za instrumentizaciju
- Detaljna kontrola nad izvršavanjem aplikacije
- Vi birate koji dijelovi koda vas zanimaju

Dynamic Binary Instrumentation

- Intel PIN
- DynamoRIO
- Frida

Solveri

- Alati za rješavanje logičkih formula
- Podrška za razne teorije
- Postavljanje uvjeta

Solveri

```
x = BitVec('x', 32)
y = BitVec('y', 32)
z = BitVec('z', 32)

s = Solver()
s.add(x != 0, y != 0, z != 0, x + y > 70000, z > x, z % 3 == 1, y % 193 == 145)

c = s.check()
print c

if c == sat:
    print s.model()
```

Solveri

- Weak crypto
- Statička analiza koda
- Ranjivosti u aplikacijama
- Deobfuskacija koda

Solveri

- Weak crypto
  - Petya ransomware
  - Bazirano na Salsa20
  - Implementirano pomoću Z3 solvera [4][5]
  - ‘16-bit Salsa10’
  - Dekripcijski ključ pronađen za 0.02s

Symbolic i Concolic execution

- Analiza programa koristeći simboličke varijable
- Analiza uvjetnih skokova
- Concolic: CONCrete + symbOLIC
- Solveri za generiranje novih inputa

Deobfuskacija koda

- Kompajlerski alati/metode
  - npr: Peephole optimization
- Opaque predicates
- Duplikacija koda
- Junk code

Opaque predicates

```
xor eax, eax
jz label
```

```
xor eax, eax
jo label
```

```
xor eax, ebx
jz label
```

Opaque predicates

```
and eax, 0x3fffffff
and ebx, 0x3fffffff
xor ecx, edx
xor edx, edi
add eax, ebx
jo label
```

Opaque predicates

```
and eax, 0x3fffffff
and ebx, 0x3fffffff
xor ecx, edx
xor edx, edi
add eax, ebx
jo label
```

Opaque predicates

and eax, 0x3fffffff

and ebx, 0x3fffffff

xor ecx, edx

xor edx, edi

add eax, ebx

jo label

Opaque predicates

and eax, 0x3fffffff

and ebx, 0x3fffffff

xor ecx, edx

xor edx, edi

add eax, ebx

jo label

Opaque predicates

and eax, 0x3fffffff

and ebx, 0x3fffffff

xor ecx, edx

xor edx, edi

add eax, ebx

jo label

Opaque predicates

and eax, 0x3fffffff

and ebx, 0x3fffffff

xor ecx, edx

xor edx, edi

add eax, ebx

jo label

Opaque predicates

and eax, 0x3ffffff

and ebx, 0x3ffffff

xor ecx, edx

xor edx, edi

add eax, ebx

jo label

Opaque predicates

```
 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
&00111111111111111111111111111111111
 -----------------------------------
```

Opaque predicates

```
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
&0011111111111111111111111111111111
  ------------------------------------
  00xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Opaque predicates

```
  00xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
+00yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
  --------------------------------
```

Opaque predicates

```
  00xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
+00yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
  --------------------------------
  0zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
```

Formati bez nativnog koda

- .NET (C#/VB.NET)
- Visual Basic
- PDF
- OLE / Microsoft Office dokumenti
- Android aplikacije
- Java CLASS

?

Reference

- [1] https://www.youtube.com/watch?v=Ch8dzu91pJs
- [2] https://www.youtube.com/watch?v=ycLjVyA_2UM
- [3] https://www.youtube.com/watch?v=HHo8AyEyoTY
- [4] http://pastebin.com/Zc16DfL1
- [5] https://reddit.com/r/ReverseEngineering/comments/4ecrgm