SYMBOLIC EXECUTION AND BUG HUNTING

Chong-Kuan Chen 陳仲寬 @ DSNSLab NCTU

https://www.facebook.com/Bletchley13

Twitter: @bletchley13

Bletchley13@gmail.com

WHOAMI

- 陳仲寬(Bletchley)
  - 交通大學網路安全實驗室博士生
    - Sandbox: https://github.com/GlacierW/MBA
    - Malware, Vulnerability, Virtual Machine, Machine Learning
  - BambooFox(前)領隊/交大網路安全策進會顧問
    - CTF, CTF and more CTFs
    - Rank 31 in ctftime 2016
    - NCTU PT Team -> discover about 40 bugs in NCTU
    - Synology bug bounty -> 7 new bugs
  - HackerCollege Member
    - http://hackercollege.nctu.edu.tw/
  - HITCON.KB Editor
  - ….

AGENDA

- 10:00 – 10:20 Environment Setting
- 10:20 - 11:00 Introduction to Symbolic Execution
- 11:10 – 11:30 Introduction to Z3 SMT
- 11:30 – 12:15 Binary Instrument with Pin
- 13:15 – 14:00 Triton: The Concolic Execution Engine(1)
- 14:10 - 15:00 Triton: The Concolic Execution Engine(2)
- 15:10 – 16:00 Angr: Symbolic Execution Binary Analysis(1)
- 16:10 - 16:40 Angr: Symbolic Execution Binary Analysis(2)
- 16:40 – 17:00 Other Symbolic Execution Application

ABOUT THIS WORKSHOP

- Understand symbolic execution and it’s application
- Write some code and play with symbolic execution engine
- Share your code and your idea
  - 共筆
    - https://hackmd.io/GYFgJgzA7ApgjAVgLSwIYiSYMMCMAcIuSqCADAMa5gJRzBn5A===
    - https://hackmd.io/MYFgTAnAHADAjCAtMA7BArIkAzAzNxAQ2FykSnWwFMA2FAEyjEJgiA==
    - https://hackmd.io/AwDgrAxgJgzAbAMwLQEMUBYDsT0FMFSoTABGSUC6YAnFAIwnoh0pA===
- After today’s workshop, we will implement 2 small tools
  - Triton – Traversal code coverage and check bugs
  - Angr – Find path and Check bugs

ENVIRONMENT

1. The VM image in VMDK
   - Contain everything
     - Angr and Triton Docker

2. Docker image
   1. Angr official docker: angr/angr
   2. My Triton+pin+z3 docker: bletchley/triton

3. Data
   1. VXCON In the USB