FUTURE COMPUTING 2017

The Ninth International Conference on Future Computational Technologies and Applications

ISBN: 978-1-61208-530-2

February 19 - 23, 2017

Athens, Greece

FUTURE COMPUTING 2017 Editors

Carla Merkle Westphall, Federal University of Santa Catarina, Brazil

Woomin Hwang, National Security Research Institute, South Korea

Kendall E. Nygard, North Dakota State University - Fargo, USA

home

top

<<

>>

FUTURE COMPUTING 2017

Forward

The Ninth International Conference on Future Computational Technologies and Applications (FUTURE COMPUTING 2017), held between February 19-23, 2017 in Athens, Greece, continued a series of events targeting advanced computational paradigms and their applications. The target was to cover (i) the advanced research on computational techniques that apply the newest human-like decisions, and (ii) applications on various domains. The new development led to special computational facets on mechanism-oriented computing, large-scale computing and technology-oriented computing. They are largely expected to play an important role in cloud systems, on-demand services, autonomic systems, and pervasive applications and services.

The conference had the following tracks:

- Computational intelligence strategies
- Security and Privacy in Computing Environments
- Computing technologies

We take here the opportunity to warmly thank all the members of the FUTURE COMPUTING 2017 technical program committee, as well as all the reviewers. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors that dedicated much of their time and effort to contribute to FUTURE COMPUTING 2017. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

Also, this event could not have been a reality without the support of many individuals, organizations and sponsors. We also gratefully thank the members of the FUTURE COMPUTING 2017 organizing committee for their help in handling the logistics and for their work that made this professional meeting a success.

We hope that FUTURE COMPUTING 2017 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress in the area of future computational technologies and applications. We also hope that Athens, Greece provided a pleasant environment during the conference and everyone saved some time to enjoy the charm of the city.

FUTURE COMPUTING 2017 Committee

FUTURE COMPUTING 2017 Steering Committee
Cristina Seceleanu, Mälardalen University, Sweden
Hiroyuki Sato, The University of Tokyo, Japan
Kendall E. Nygard, North Dakota State University - Fargo, USA
Alex Wijesinha, Towson University, USA

home
top
<<
>>

Albert Zomaya, University of Sydney, Australia
Sergio Ilarri, University of Zaragoza, Spain
Dan Tamir, Texas State University, USA
Wail Mardini, Jordan University of Science and Technology, Jordan

FUTURE COMPUTING 2017 Industry/Research Advisory Committee
Francesc Guim, Intel Corporation, Spain
Yasushi Kambayashi, Nippon Institute of Technology, Japan
Jay Lofstead, Sandia National Laboratories, USA

home
top
<<
>>

FUTURE COMPUTING 2 / SEPYCE: Security and Privacy in Computing Environments

Towards Software-Defined Malware Analysis with a Deep Introspection

Sang-Hoon Choi
SysCore Lab.
Sejong University
csh0052@gmail.com

Woomin Hwang Ph.D.
National Security
Research Institute
csh0052@gmail.com

Ki-Woong Park Ph.D. †
Dept. Computer and Information
Security, Sejong University
woongbak@sejong.ac.kr

† Corresponding Author (Ki-Woong Park, woongbak@sejong.ac.kr)
This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (2016R1A4A1011761) and by the Ministry of Education (2015H1C1A1035859).

Contents

Introduction

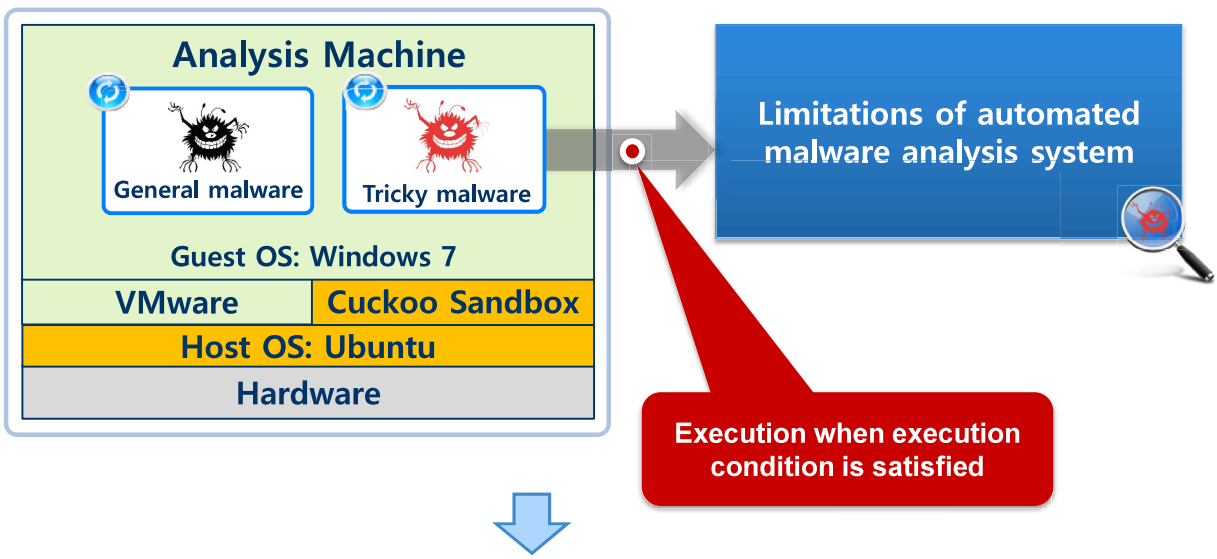
❖ Research background

- AV-TEST Labs: Number of malware infections as of November 28, 2016
  → About 6 billion malware infections
- Much time and manpower needed to analyze large numbers of malware
  → Limitations of malicious code analysis
- Automating malware analysis is critical for a large numbers of malware analysis
  - Cuckoo sandbox: Malware analysis system based on open source platform

Introduction

❖ Motivation 1/2

- Malwares that works only when every execution condition are satisfied
  → **Malware with Tricky Execution Conditions**

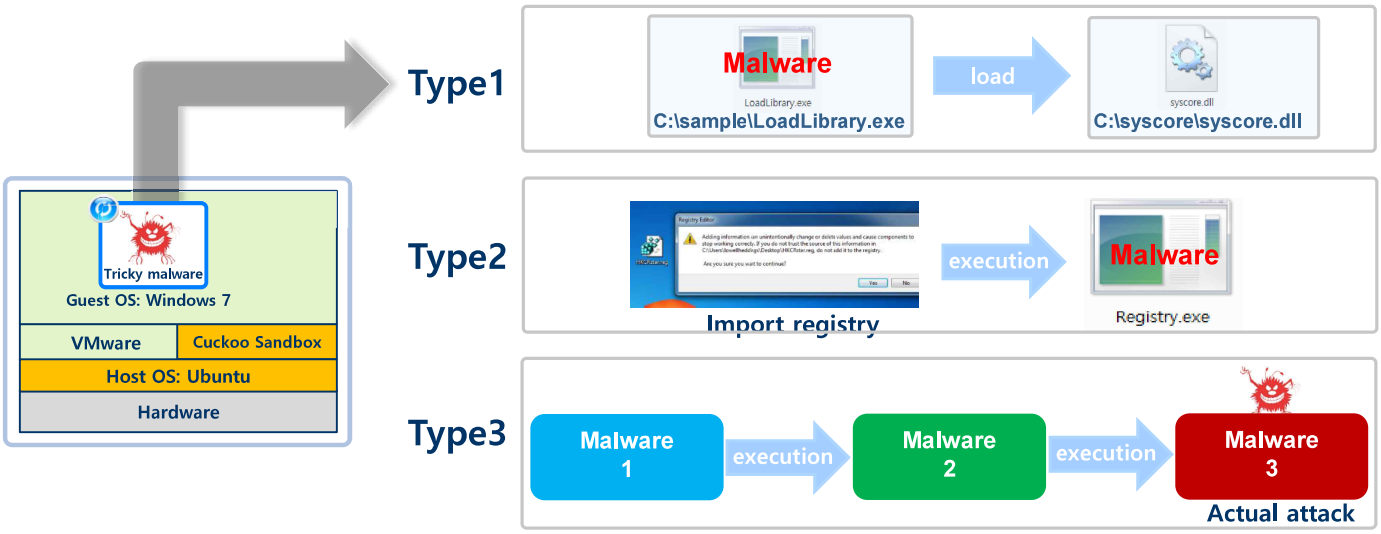


Software-Defined Malware Analysis with a Deep Introspection
✓ **(Customized Cuckoo Sandbox + Accelerated Memory Dump)**

Introduction

❖ Malware with Tricky Execution Conditions

- **Type1:** Specific file is located on a different path
- **Type2:** Registry file must be imported before the malware is executed
- **Type3:** Actual attack occurs only after multiple malwares are executed in a step-by-step manner



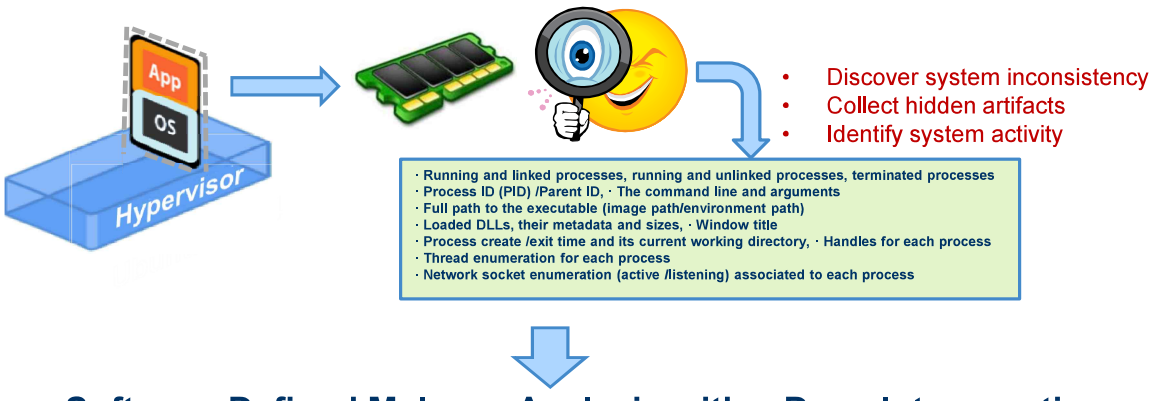
Introduction

❖ Motivation 2/2

- Memory dump image may be critical clue in malware analysis

→ **But, memory dump leads to <u>user-obstructive latency</u>**

- Dealing with encrypted or obfuscated malware
- Finding what's been hidden [processes, files, registry, and even network connections, drivers]
- Finding information about processes that have since exited

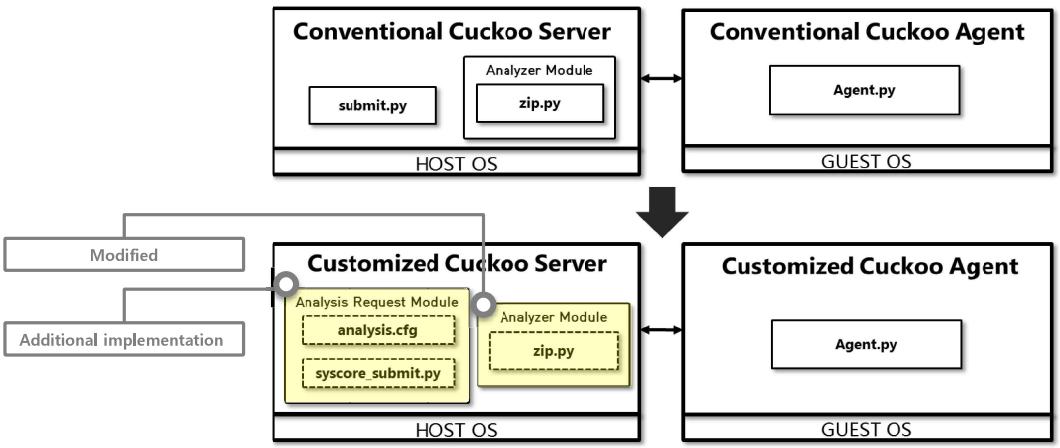


Software-Defined Malware Analysis with a Deep Introspection
(Customized Cuckoo Sandbox + Accelerated Memory Dump) ✓

Design and Implementation (Customization of Cuckoo Sandbox)

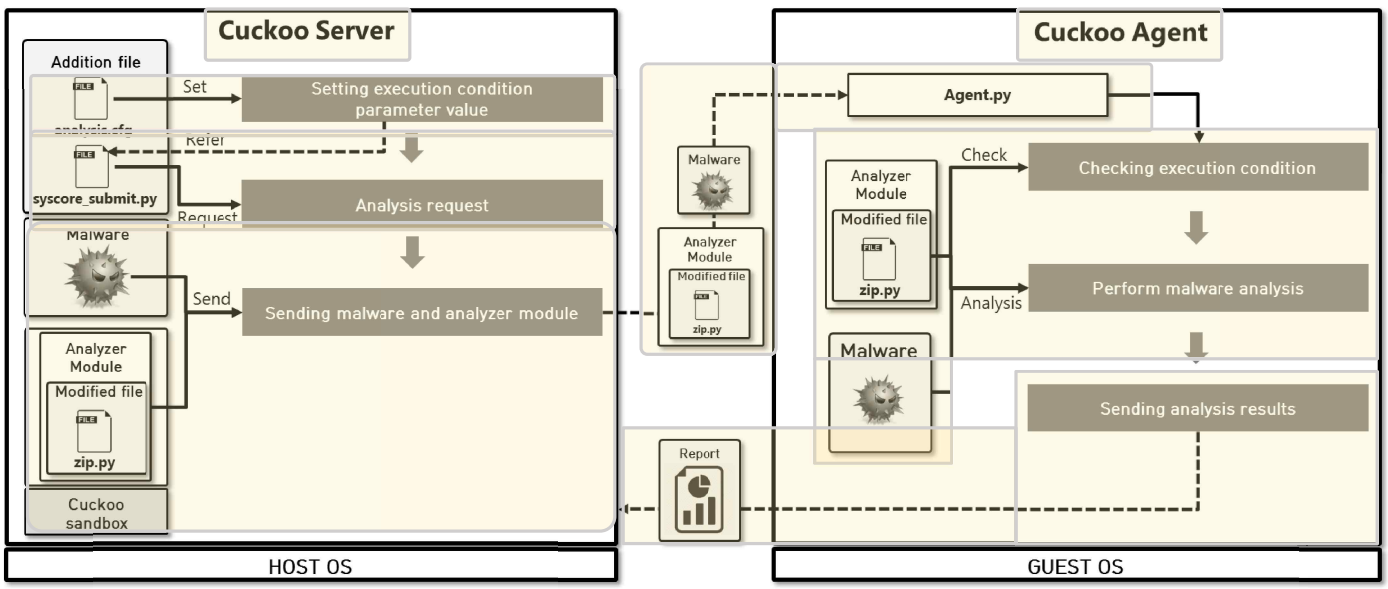
❖ Towards Software-Defined Cuckoo Sandbox

- Analysis request module(Additional implementation)
  - analysis.cfg: Set the parameter value of tricky execution condition
  - syscore_submit.py: Request malware analysis with tricky execution condition by referring to analysis.cfg and zip.py
- Analyzer Module of Cuckoo Sandbox(Modified)
  - zip.py: Built-in functions for malware analysis with tricky execution conditions



Design and Implementation (Customization of Cuckoo Sandbox)

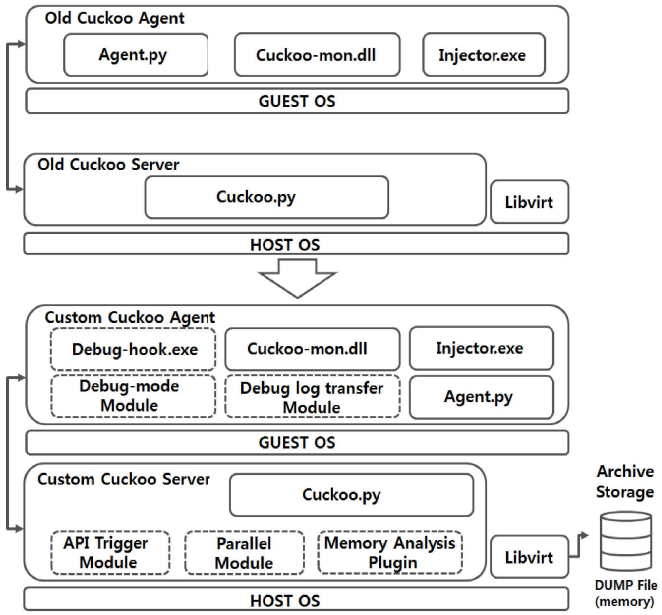
❖ Analysis Process of Customized Cuckoo Sandbox

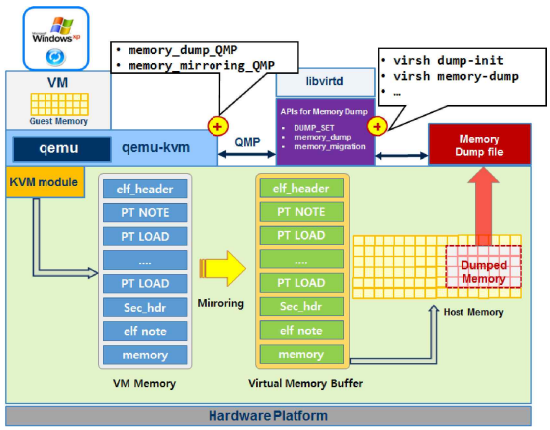


Design and Implementation (Accelerated Memory Dump)

❖ Modified Cuckoo Sandbox for Accelerating Memory Dump

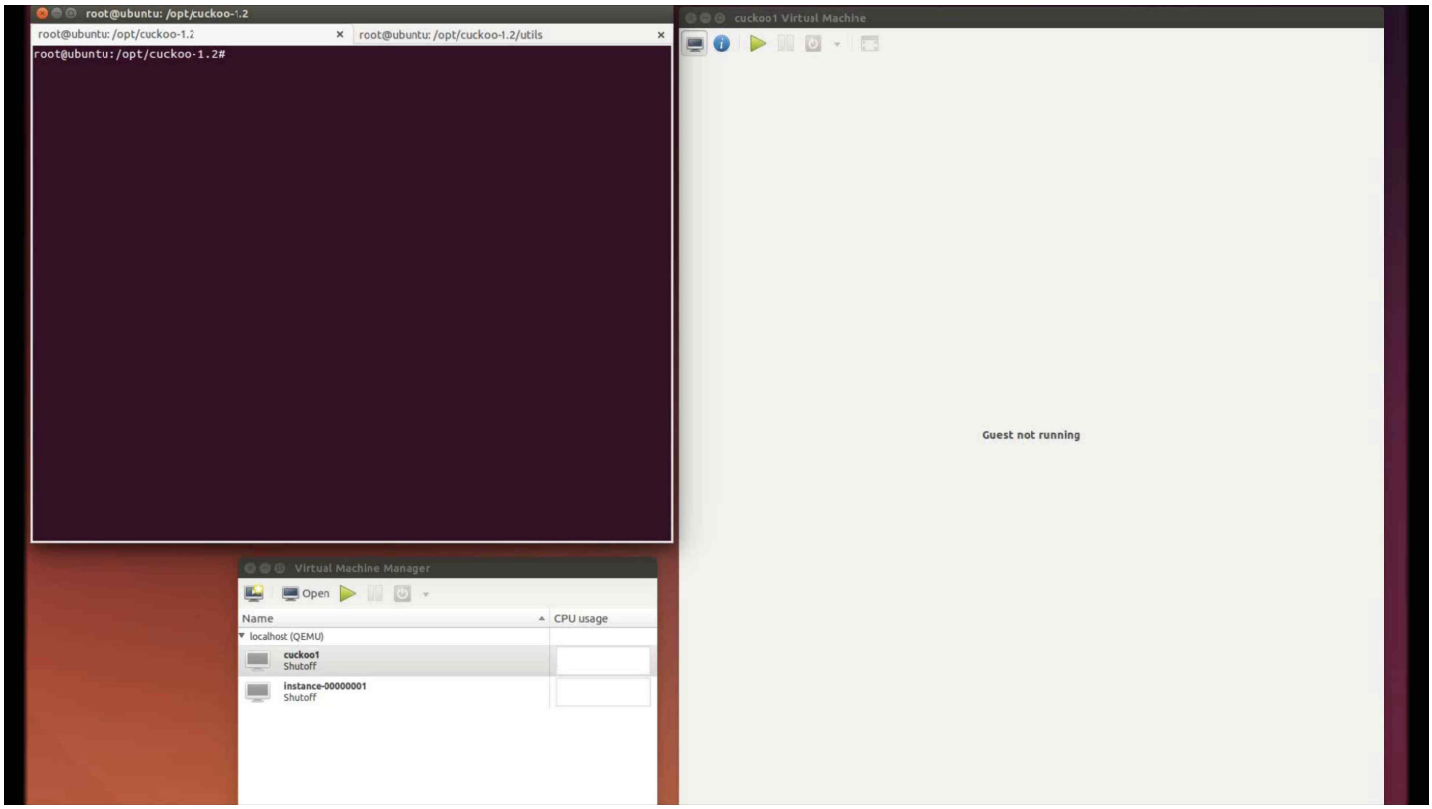
- APIs for boosting up memory dump are integrated into the hypervisor (KVM)





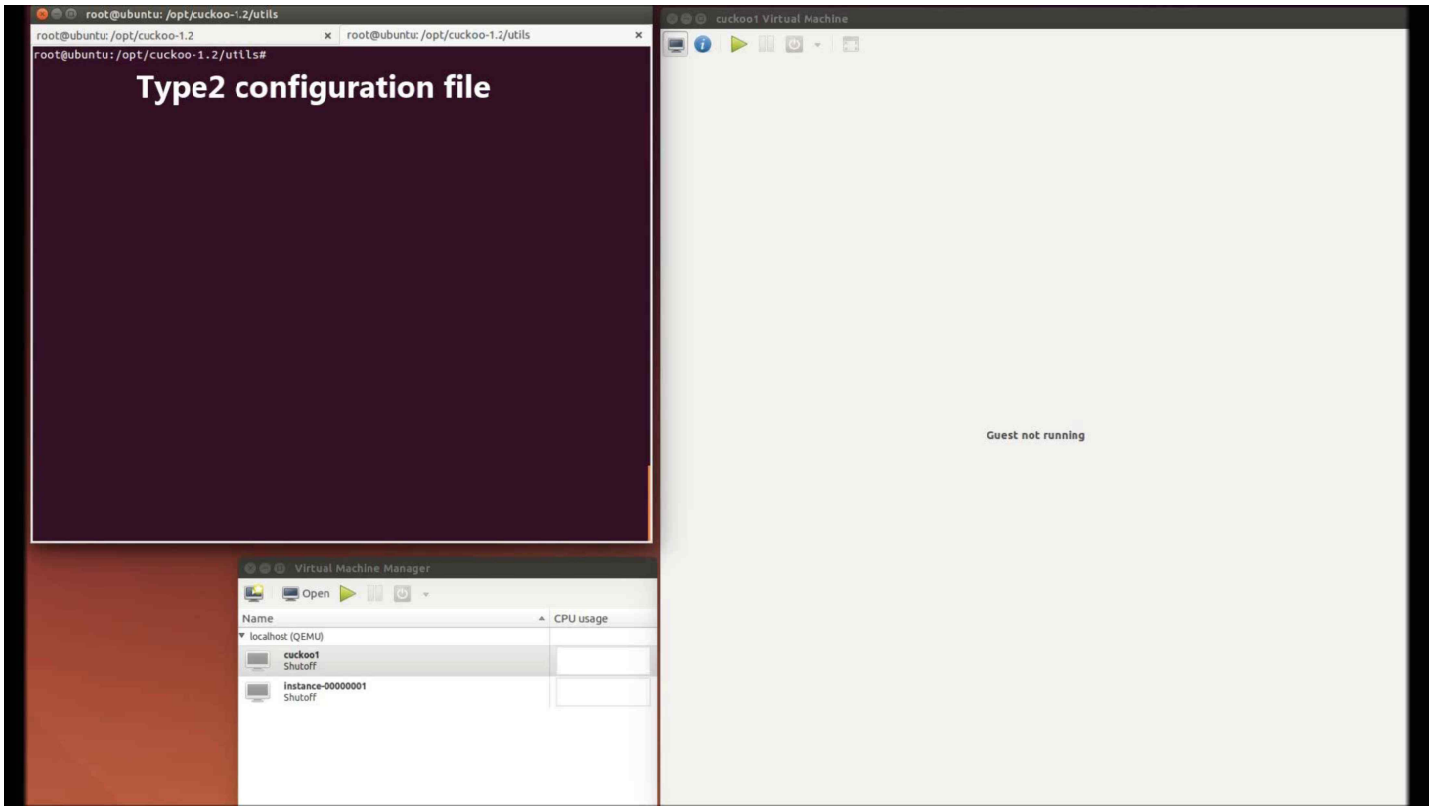
Demo: Type1

❖ Type1: Specific file is located on a different path



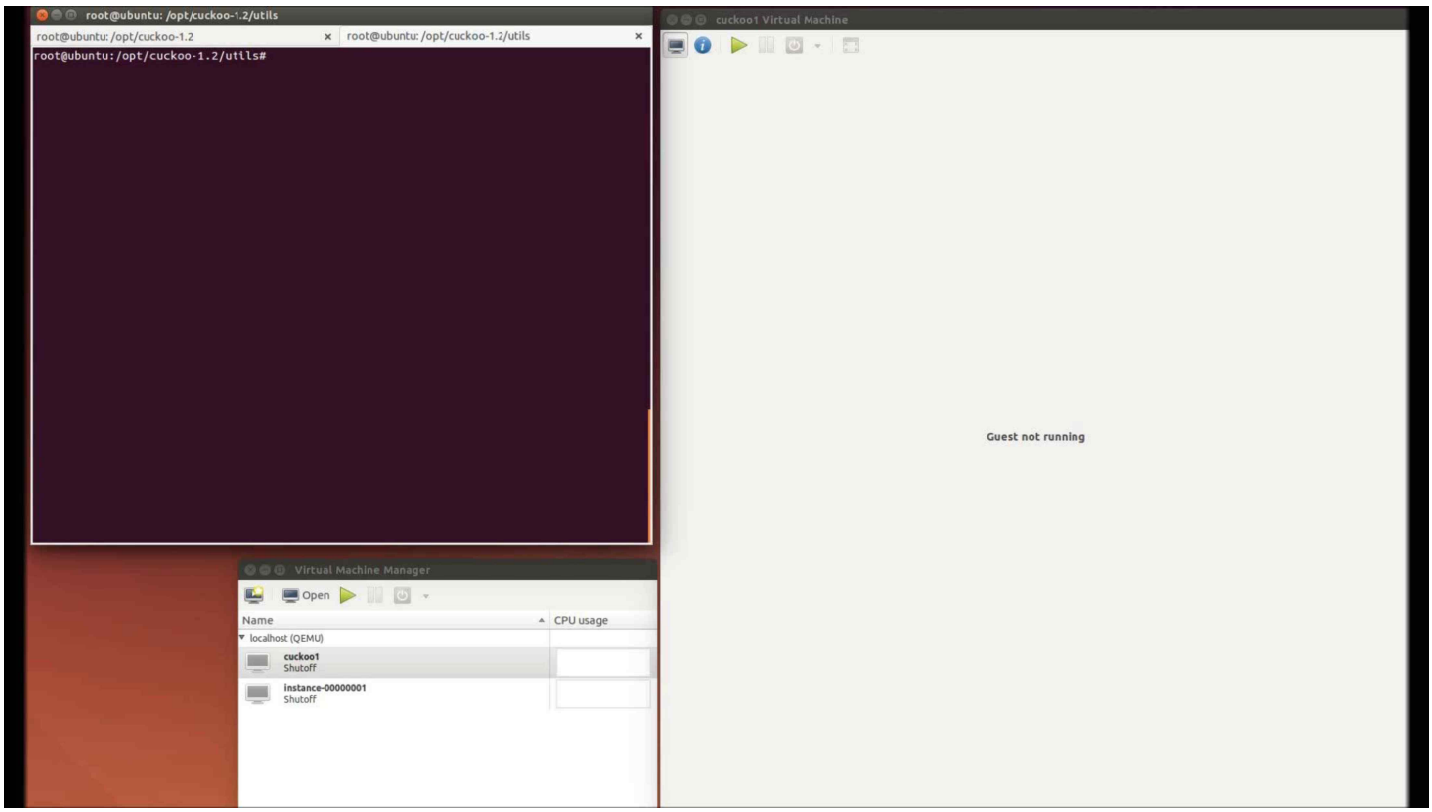
Demo: Type2

❖ Type2: Execute Malware after importing registry



Demo: Type3

❖ Type3: Actual Attack after Step-by-Step Execution



Conclusion

Towards Software-Defined Cuckoo Sandbox

- We present our effort to **customize Cuckoo Sandbox for enabling analysis of malware with tricky execution conditions**.
- As a result, this **allows analysis of malware with various execution conditions**, in a software-defined manner
- Further work will perform a various experiments and profiling for advanced malware dynamic analysis engines based on Cuckoo Sandbox

Accelerated Memory Dump

- We developed an API Trigger-based memory dump module to extract hidden information from sample-malware in memory.
- Existing Cuckoo Sandbox was modified to implement the API Trigger-based memory dump technology.
- We modify the hooking method that existing that Cuckoo Sandbox uses API triggering.

Q & A

Thank you.