



Improvement of Binary Analysis Components in Automated Malware Analysis Framework

**Keiji Takeda
KEIO UNIVERSITY**

**02/21/2017
Final Report**

DISTRIBUTION A: Distribution approved for public release.

**Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ IOA
Arlington, Virginia 22203
Air Force Materiel Command**

REPORT DOCUMENTATION PAGE			<i>Form Approved</i> OMB No. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Executive Services, Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.</p>				
1. REPORT DATE (DD-MM-YYYY) 21-02-2017		2. REPORT TYPE Final		3. DATES COVERED (From - To) 26 May 2015 to 25 Nov 2016
4. TITLE AND SUBTITLE Improvement of Binary Analysis Components in Automated Malware Analysis Framework			5a. CONTRACT NUMBER	
			5b. GRANT NUMBER FA2386-15-1-4068	
			5c. PROGRAM ELEMENT NUMBER 61102F	
6. AUTHOR(S) Keiji Takeda			5d. PROJECT NUMBER	
			5e. TASK NUMBER	
			5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) KEIO UNIVERSITY 5322, ENDO FUJISAWA, 252-8520 JP			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AOARD UNIT 45002 APO AP 96338-5002			10. SPONSOR/MONITOR'S ACRONYM(S) AFRL/AFOSR IOA	
			11. SPONSOR/MONITOR'S REPORT NUMBER(S) AFRL-AFOSR-JP-TR-2017-0018	
12. DISTRIBUTION/AVAILABILITY STATEMENT A DISTRIBUTION UNLIMITED: PB Public Release				
13. SUPPLEMENTARY NOTES				
14. ABSTRACT This research was conducted to develop components for automated system to analyze malicious software (malware) with minimum human interaction. The system autonomously analyze malware samples by analyzing malware binary program and by monitoring their behavior, then generate data for malware detection signature and for developing their counter measure.				
15. SUBJECT TERMS Malware, AOARD				
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 4
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified		
			19b. TELEPHONE NUMBER (Include area code) 315-227-7002	

Improvement of Binary Analysis
Components in Automated Malware Analysis Framework
Final Report for FA2386-15-1-4068
Keiji Takeda, Keio University
keiji@sfc.keio.ac.jp

1 Objective

This research was conducted to develop components for automated system to analyze malicious software (malware) with minimum human interaction. The system autonomously analyze malware samples by analyzing malware binary program and by monitoring their behavior, then generate data for malware detection signature and for developing their counter measure.

2 Research Outcome

Through this research project, components of a malware analysis framework which integrates both dynamic analysis and static analysis techniques have been developed. By using the developed components, a malware analyst is able to analyze malware functions while avoiding interference by the malware. The developed components analyzes malware executable by suppressing interference from malware, generates a list of C&C (Communication and Control) servers the target malware may connect, identifies code sections for encryption and decryption functions and identifies code sections for commands from the C&C servers.

The framework challenged two fundamental limitations of existing analysis platforms. The first challenge is to comprehensively extract the potential functions of malware and the second challenge is to complete the analysis in closed environment without requiring active C&C servers on the Internet. The framework conducts dynamic analysis by executing malware on a sandbox environment isolated actual computer network such as the Internet then conducts static analysis for the code sections where not executed due to self-protection mechanism of the malware. As a next step it forces to execute the portion of the code to analyze the malware automatically. The framework has process trace function by instructions, by API, and by system calls, taint analysis function and symbolic execution functions also implemented.

The framework utilizes QEMU open source machine emulator and virtualizer as base virtual machine, and utilizes modified DECAF (Dynamic Executable Code Analysis Framework) for dynamic analysis and uses Angr for static analysis and symbolic execution. The developed framework was tested with 412 malware obtained from

multiple malware data sets. The test result shows that the framework has capability to suppress analysis evasion mechanism of malware (100%), to obtain potential address list of C&C servers (approximately 5% error rate), to detect libraries used to encrypt and decrypt (100% for known APIs) and to identify command handler without having actual C&C server (approximately 90%).

The developed components enables malware analysts to observe functions of malware quickly and helps implementation of countermeasures to prevent or mitigate damage caused by malware.

3 Publication

Malware Communication Analysis using Dynamic Binary Instrumentation in Heterogeneous Analysis Environments for Stealthiness, Yuma Kurogome Keiji Takeda, IPSJ Computer Security Symposium 2015.

MEMU: Automated Extraction of Command-Dependent Behaviors from Malware Binaries, Yuma Kurogome, Keiji Takeda, The 11th International Workshop on Security 2016.

MEMU: Automated Extraction of Command-Dependent Behaviors from Malware Binaries, Yuma Kurogome, Keiji Takeda, Keio University SFC Open Research Forum 2016.

Evaluation of Economic Rationality on Information Security Measures, Keiji Takeda, IPSJ Computer Security Symposium 2016.