# MATSUURA LAB.

## [Improving Anti-malware Technologies by Compiler Estimation]

Department of Informatics and Electronics, IIS

http://kmlab.iis.u-tokyo.ac.jp

Information Security

Information and communication engineering department

## Anti-malware Technologies Based on Machine Instruction Sequence

In the countermeasures against malware (malicious software), machine instruction sequences are susceptible to compiler variety or optimization option. That causes the decline of precision on detection or classification.

In this laboratory, we research the method to improve the precision by mitigating this ill effects based on estimation of compiler, optimization.

## Compiler Estimation Method

We propose the method to estimate compilers by stochastic model. Machine instruction sequence generated by each compilers are modeled by Hidden Markov Model and compilers are estimate by maximum likelihood estimation.

In this method, we can estimate compilers utilized to generate the malware with the precision of around 70%.

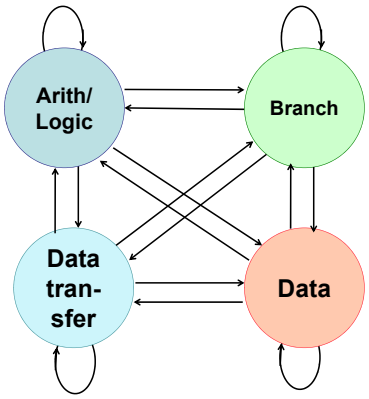


Fig.1 State transition model of machine instruction sequence

## Application to Anti-malware

We also propose the method to improve the precision of anti-malware technologies by the result of compiler estimation. For instance, fig.2 describes that classifying by compilers beforehand mitigate the ill effects of compilers. This improves the precision of malware family classification.

This research can contribute for various methods based on machine instruction sequence.

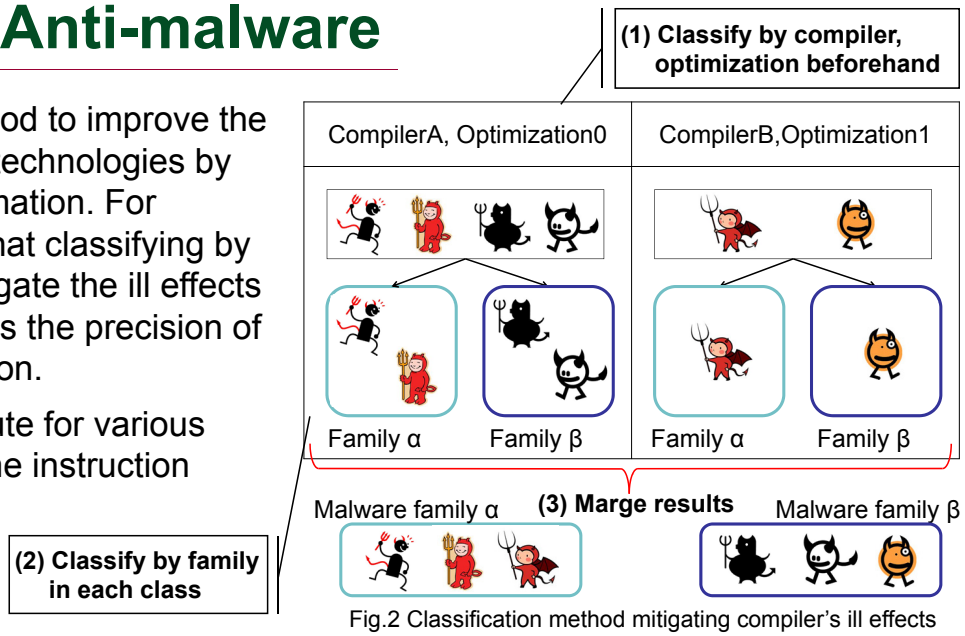


Fig.2 Classification method mitigating compiler's ill effects