ICT Virtual Organization of ASEAN Institutes and NICT
ASEAN IVO Forum 2016
Call for Presentations

Submission and Registration Form

Please enter the relevant information in the fields below, giving an appropriate explanation when necessary. You may add supplemental pages and supporting data. If necessary, you may be asked to provide additional documents.

I. Title—
Proposed Framework for Root Kit Analysis and Cyber Forensics for Cyber Security

II. Author(s)—Full name (First name family name):
(If you are already planning a project, please include the names of all team members)

1. Dr. Mie Mie Su Thwin
2. Ms. Cho Cho San
3. Mr. Tin Maung Maung
4. Mr. Naing Linn Htun

III. Organization(s):
(If you are already planning a project, please include the institutions of all team members)
Cyber Security Research Lab,
University of Computer Studies (Yangon), Myanmar

IV. Topic selection:
(Select one from the topics listed in "Call for Presentations")
Cyber-Security and its applications
Monitoring/Detection Systems

IV. Abstract:
(Describe the purpose, background, objectives, content, plans for connected projects, expected results/outcomes, etc.)

Cyber security is becoming universal problem and affecting entire mankind directly or indirectly. It has become an every national top most priority to ensure a safe and healthy environment in cyber space. To define the domain of the science of cyber security, let's focus on the most salient artifact within cyber security-malicious software. Therefore the propose system concentrates on the malware that infect the

user-level and kernel-level components of the operating system. Among them, we especially focus on the samples that used the user level or kernel hooking techniques and that have the hidden functionalities such as rootkit, Trojan and worm. Firstly, we collect the samples and analyze these samples in Virtual box on Window-7 guest OS and host is Ubuntu. And to combine the features for the accurate categorization, the Cuckoo sandbox will also be used in our proposed system for detection accuracy. Then features extraction and selection will be performed in our proposed system. Finally we will cluster these samples based on their infection techniques using data mining algorithms.

Nowadays, people are committed the cybercrimes by using the technology and electronic devices such as computer, mobile phones, USB flash drive and so on. Investigators collect the data to get evidence from cybercrimes. These evidence data are essential for investigators to contest a legal suit. So, we also want to propose a forensic framework for Cyber Security Lab. This framework will support and cover to collect evidence data in different forensic fields. We will use some freeware tools, ultimate tools and our own tools in this framework.

This document provides a high level framework of the overall solution delivery model that we propose to provide Forensic and Malware Analysis Framework, together with the specific benefits that will accrue to Cyber Security Research Lab in UCSY.

The proposed system includes the following objectives:

- To design and implement the Forensics and Malware Analysis Environment
- To propose the malware detection framework
- To extract and categorize the malware dominant features
- To collect evidence from the crime scene
- To propose the Forensic Framework for Cyber Crime Investigation System

The proposed system will provide the valuable dataset from the experiment of malware analysis. The

proposed system aims to detect the compromised system by using the resulted dataset. The proposed system may help the system administrator for future malicious samples detection framework. The proposed system produces the forensic suite framework, detail analysis algorithm and malware detection system as a result.

V. Speaker information:

Full name: Ms. Cho Cho San
Institute: University of Computer Studeis (Yangon)
Address: Zewaka Hostel, Hlaing Campus, Yangon.
Telephone: +95943198800
E-mail: chochosan@ucsy.edu.mm

VI. Support for speaker—circle or underline any that you wish to request:

- Round trip fare at discount economy class
- Accommodation