Topic: N151-067

Mayachitra, Inc.

Orthogonal Approach to Malware Detection and Classification

Cyber-security continuously evolves to establish security against ever-changing methods of attack, hackers too continuously adapt their tactics and methods to evade state-of-the art defensive security mechanisms. As this never-ending billion dollar “cat-and-mouse game” continues, it is useful to explore avenues that examine novel, orthogonal defensive strategies to counter ongoing cyber-threats. Orthogonal cyber-security protections, employ alternative strategies and multi-dimensional detection regimes, not well known to hackers, making them more difficult for hackers to detect, and evade. Mayachitra’s orthogonal cyber-security framework, MALSEE: employs a multi-tiered detection strategy; optimizes analysis times; effectively reduces scan time and the number of malware variants to be scanned; provides security against zero-day attacks; is complimentary to existing cyber-security solutions; is operating system agnostic; and derives intelligence in a fraction of the time.

Technology Category Alignment:

Machine Perception, Reasoning and Intelligence
Information Collection/Management
Synthesis/Analytics/Decision Tools
Trust Foundations
Trust Foundations

Contact:
Dr. Lakshmanan Nataraj
nataraj@mayachitra.com
(805) 453-4117
http://mayachitra.com/
SYSCOM: ONR
Contract: N68335-17-C-0048
Corporate Brochure: https://navystp.com/vtm/open_file?type=brochure&id=N68335-17-C-0048

Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
ONR Approval #43-3252-17

Topic # N151-067
Orthogonal Approach to Malware Detection and Classification
Mayachitra, Inc.

WHO

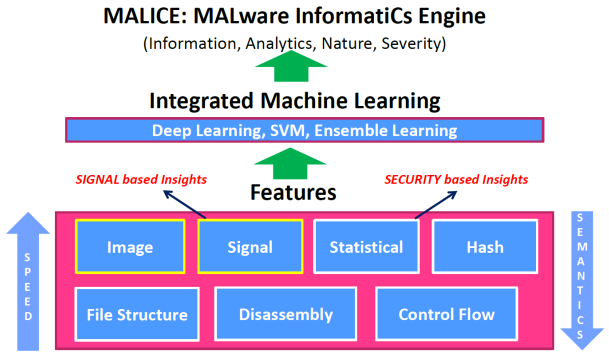
SYSCOM: ONR

Sponsoring Program: ONR Code 31 Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Division 311 Mathematics, Computer and Information Sciences (MCIS) Cyber Security and Complex Software Systems Program

Transition Target: Future Naval Capability

TPOC:
Dr. Dan Koller
daniel.koller@navy.mil

Other transition opportunities: Department of Defense (DoD) agencies, prime contractors and private commercial entities. Mayachitra's technology provides an operating system agnostic capability to detect computer viruses and malware.



WHAT

Operational Need and Improvement: While cyber security solutions constantly evolve to keep up with new attacks, hackers too change their ways and continue to evade defense mechanisms. As this never-ending billion dollar "cat and mouse game" continues, it may be useful to look at avenues that can bring in novel alternative and/or orthogonal defense approaches to counter the ongoing threats. The hope is to catch these new attacks using orthogonal methods which may not be well known to hackers, thus making it more difficult for them to evade all detection schemes. Mayachitra's proposed solution is orthogonal to other cyber security techniques. Benefits are multi-tiered: analyst time is optimized through the reduction of malware variants; the approach is complimentary to other solutions; agnostic to operating systems; and intelligence is derived in a fraction of time.

Specifications Required: Automatically detect and recognize malware at a high speed with a high level of confidence. To perform high speed malware detection on medium to high end desktop computers, it is critical to understand, evaluate, and balance performance.

Technology Developed: Mayachitra has developed a technology to automatically detect malware using non-standard approaches based on signal and image processing. The technology employs casting software executables as digital signals and images to identify whether that software is malicious or not. Mayachitra's technology is fast, compact and orthogonal to standard malware detection methods.

Warfighter Value: Reduction in malware in Warfighter computer systems.

WHEN

Contract Number: N68335-17-C-0048 **Ending on:** November 1, 2018

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Initial deployment of MALSEE tool to detect malware	Low	Average Precision	6	November 2017
Deployment of MALICE engine	Med	TRL	6	November 2018

HOW

Projected Business Model: Mayachitra's software project is planned to be deployed as a commercial tool in software-as-a-service (SaaS) platforms where customers directly purchase the application as a paid service.

Company Objectives: Maychitra's technology automatically detects and recognizes malware with a high level of confidence. It performs detection at high speeds and provides insights that are orthogonal to other cyber security regimes. The proposed business strategy partners Mayachitra with interested DoD agencies, labs, and prime contractors to mature the technology, adapt the capability to meet application-specific security needs, and to deploy the capability on tactical and support computer systems.

Potential Commercial Applications: The Navy Research Lab has shown initial interest in MALICE. Mayachitra technology also has direct applications to other DoD agencies.

Contact: Dr. Lakshmanan Nataraj, Research Scientist
nataraj@mayachitra.com (805) 453-4117