International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 24th Feb 2018. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-02

Title: A NEW STATEGIE FOR MOVING TARGET DEFENCE BY USING BIO-INSPIRED TECHNIQUES

Volume 08, Issue 02, Pages: 57–63.

Paper Authors

MS.K.SANDHYA RANI, A.LAKSHMI SOUJANYA

Vignan's Lara Institute of Technology & Science

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A NEW STATEGIE FOR MOVING TARGET DEFENCE BY USING BIO-INSPIRED TECHNIQUES

MS.K.SANDHYA RANI[1], A.LAKSHMI SOUJANYA[2]

Assistant Professor[1], Department of M.C.A ,Vignan's Lara Institute of Technology & Science

M.C.A Student[2],Department of M.C.A ,Vignan's Lara Institute of Technology & Science

Abstract:

This project has created (in collaboration with another DOEfunded project1) the first scalable, real-world prototype of the Digital Ants Framework (DAF)[11] and integrated five technologies into this flexible, decentralized framework: (1) Ant-Based Cyber Defense (ABCD), (2) Behavioral Indicators, (3) Bioinformatic Classification, (4) Moving-Target Reconfiguration, and (5) Ambient Collaboration. The DAF can be used operationally to decentralize many such data intensive applications that normally rely on collection of large amounts of data in a central repository.ABCD is a hierarchical organization of human and software agents that relies on swarm intelligence and decentralized communication to defend large, complex cyber infrastructures from attack. Behavioral Indicators enable defenders to identify previously unknown problems before there are signatures for them by examining the behaviors of systems in a decentralized approach that enables machine-to-machine comparison automatically and in a scalable fashion. Bioinformatic Classification provides a means of inexact matching borrowed from proteomics that makes it harder for attackers to reuse old attacks. The Moving-Target Reconfiguration technology provides the basis for defenders to reconfigure systems automatically, increasing diversity between systems and simultaneously reducing vulnerabilities. Finally, Ambient Collaboration was a minor focus of this work that enables collaboration among human analysts without conscious collaboration e↵ort. Together, these technologies, distributed via the DAF, will help secure large cyber infrastructures that support our society. This report presents an operational scenario involving a corporate espionage situation and applies the proposed defense as a scalable and efficient solution for electric smart grid defense, communications security, industrial control security, and information technology cyber security. We present a brief summary of the most applicable literature and list the unique contributions of our work including: (i) a novel movement and pheromone model for randomly moving agents, (ii) a set of behavioral indicator data sources and sensors, (iii) a decentralized method of bioinformatics classification of malicious binaries, (iv) a way to distributively change configurations of machines in a moving target environment, (v) a method of ambient collaboration, and (vi) a number of publications. We conclude the report with a description of our demonstrations that show the efficacy of the DAF in dynamic moving-target reconfiguration of systems and the scalability of the DAF to realistic enterprise scales. In the appendices, we recapitulate the project milestones and deliverables, expand the operational scenario, and discuss

in detail the DAF architecture. The accompanying CDROM contains reports, deliverables, papers, videos, software, and other information on the Digital Ants and the related technologies developed by this work

Introduction

This research concentrates on achieving a Moving-Target cyber defense against complex-adaptive adversaries throughvthe application of bio-inspired research technologies. The Moving-Target problems will focus on two research tasks:

(i) Digital Ants as Moving-Target research: using mobile agents (based on digital social ants metaphor developedvat PNNL) in combination with distributed genetic algorithms to provide a robust moving target environment, and

(ii) Cyber economics: shifting the burden of complexity/costs back to the attacker via a biology-based classification of cyber entities approach that shifts the burden of complexity onto the attacker, making it harder to hide malicious artifacts. The digital ants technique will make our network a moving target in cyberspace, thus requiring increased sophistication (complexity/costs) on the part of would-be attackers. This work concentrates on designing and developing a trustworthy cyberspace–a system of defenses that operate in an environment that is presumed to be compromised.High-level description The Bio-Inspired Approaches to Moving-Target Defense Strategies project has incorporated a number of bio-inspired cyber defensive technologies within the elastic framework of the Digital Ants. Digital Ants is a hierarchical organization of human and software agents that relies on swarm intelligence and decentralized communication to defend large and complex cyber infrastructures from attack. This project has invented or adapted five technologies and decentralized them via the Digital Ants Framework (DAF).

Existing system:

Autograph [16] is a distributed system for automatically generating signatures of Internet worms via coordinated sensors that examine byte sequences within TCP packets. Autograph depends on the ability to heuristically identify worm-like patterns in network traffic and employs a “tattler” to share these signatures with other sensors. Unlike CID, Autograph does not incorporate other kinds of rationality, provides no basis for trust among signature-sharing sensors, and does not use feedback to benefit from the false positives it generates. CRIM [6] is a cooperative module designed for the MIRADOR distributed intrusion detection system (IDS) that clusters, merges, and correlates IDS alerts. CRIM’s correlation attempts to reduce administrator burden by composing sets of related “elementary” attacks into compact attack scenarios that mirror the plans and intentions of the attacker. While CRIM would save human workload, unlike CID, it requires the human to work closely with the software to correlate alerts in to an attack plan. CRIM shares data that could make it useful in an infrastructure, but does not use swarm intelligence, nor does it make efficient use

of false positives. Cossack [19] employs a distributed set of "watchdog" systems deployed at the boundaries of large networks or Autonomous System to detect and control DDoS attacks. While this is a decentralized system that would enable multiple organizations to cooperate in a cyber defense at the large network level, it does not use mobile agents at the individual host level nor does it allow for emergent cooperative sensor behavior. Cossack does not involve humans at all, thus it is useful primarily for high-speed malware such as worms. Similarly, Nojiri, et al. [18] describes a system that is designed to thwart worm attacks. This system uses decentralized mobile agents for detection and reaction and is designed for emergent features. Essentially Nojiri's system is a "white worm" designed to propagate among "friends" to defeat malicious worm spread. Nojiri presents no mechanism for controlling spread of the worm, and no indication of human involvement.

Proposed system

This effort has advanced the Systems Behavior Research group's Cyber Security research program to secure digital infrastructures by developing a dynamic means to adaptively defend complex cyber systems. The eventual result will be trustworthy enclaves in cyberspace that will have observable security metrics and be modeled so that abnormalities are readily identified and acted on. In this section, we briefly discuss potential operational outcomes for the digital ants framework and for each of the component applications of this work. Operational Scenario The operational scenario revolves around a corporate espionage situation where the target corporation is defending its enterprise-computing infrastructure from cyber attack through a variety of attack vectors. We pay particular attention to the need for detecting malicious capacity of executable code and compromised computing elements. We assume that humans will always have a role in the decision making process, but that we can enable them to make rapid, well-informed decisions through delocalized sensing coupled with transparent (i.e. no penalty for false positives) secondary responses. The scenario describes both defender and threat capabilities showing how the technologies advanced by this work will enable a resilient cyber defense. Operationally,this will enable analytics to scale far beyond current limitations while not suffering from the bandwidth or computational limitations of centralized analysis. What must be traded in is a central overview of the entire problem space, with humans being able to participate in the analysis at the lowest levels. Arguably, this cannot be done even now since centralized decision-making, even when supported by visual or automated analytics, cannot keep pace with the volume and velocity of relevant cyber information. Instead, the DAF provides a means for accomplishing efective analytics at the edge, making it possible once again to keep up with the growth of networks and processing.Operationally, this means that humans will be in the right loop, at a level where they can influence the system appropriately, not "down in the weeds" looking at individual data items. Decentralized analysis will enable analysis

to scale without requiring humans to be hired to scale with the size of the data and networks.Behavioral Indicators While malicious software can vary greatly in form, it nearly always produces unintended side effects on the systems it colonizes. By examining the behaviors of systems rather than the files on the systems, behavioral indicators enable defenders to identify previously unknown problems before there are signatures for them.By decentralizing this behavioral analysis, our work shows how system behaviors can be compared with one another automatically and in a scalable fashion.

Modules:

Agents

The Sergeant, Sentinel, and Sensor are all agents. There is an AbstractAgent class from which all of the agents derive. It contains a single abstract method execute that is where subclasses can customize the behavior of each type of agent.

AbstractAgent::execute is the main 'run loop' of each agent. In the case of the Sentinel and the Sergeant, this is executed as part of the external initialization of those classes. For the Sensor, it is executed by the Sentinel. There are two scripts used for development to start the Sergeant and Sentinel: start sergeant.py and start sentinel.py,respectively. These each take the XML configuration file as a parameter.

Sergeant

The Sergeant is responsible for creating the network of Sentinels, creating and dispatching Sensors to the network and as a central logging location. An XML configuration file is loaded by the Sergeant that specifies the Sentinels (by IP address and port) and their neighbors. The file also contains the Sensor specifications.The Sergeant has no default behavior, but this can be specified in a subclass. There is currently a development Sergeant subclass that sends a single Sensor of each type to a random Sentinel.

Sentinel

The Sentinel is responsible for managing an interface to data sources for Sensors to read, as well as receiving and executing Sensors. The Sentinel also packages and transmits (migrates) Sensors to its neighbors.The Sentinel has an XML configuration file that specifies its ID (synonymous with the IP port) as well as its data sources. Upon startup the XML file is read and the data sources are instantiated and stored in a list by the name of the data source. The Sensor has a method, 'inspect data' that the Sensors call. The method takes two parameters:the name of the data source and an optional parameter to pass to the data source. The Sentinel invokes the get value method on the data source, passing the optional parameter and returns the value to the Sensor.When a Sentinel receives a new Sensor it is added to an execution queue. If there are Sensors to execute it will run the execute method of the Sensor and then sleep for a configurable amount of time.The Sentinel has no default behavior besides managing Sensors and data sources. However subclasses of the Sentinel class can do any type of processing they like.Data Sources Data sources are the means by which a Sentinel can provide data to a Sensor. Each data source is a subclass of Abstract Datsource which simply has an abstract method get value which takes a parameter. The implementation can store

values, make calls to the operating system, or do anything that the user deems necessary.

Sensor

Sensors inherit from AbstractSensor which has an abstract method execute. The base class provides initialization to assign a unique ID to each Sensor (this is one reason that Sensors are created at the Sergeant). In addition the base class provides a memorize method that allows the Sensors to maintain a limited memory (default is 5). [[This should be broken into a subclass, as not all Sensors will need this.]] Each Sensor contains a reference to the Sentinel instance that it is currently visiting. This reference is managed by the Sentinel when a Sensor is received and unpackaged. The Sensor uses this reference to communicate with the Sentinel, e.g., to move to a new Sentinel or to query a data source.

Logging

The framework has a mechanism for centralizing all logging at the Sergeant level. AbstractSensor has a log method which takes a level and a message. This method calls into the AbstractSentinel log method which then writes the message to the Sentinel's logger. This logger uses a DatagramHandler which allows it to send its messages to a server. For the Sentinel, the DatagramHandler points to the Sergeant who writes messages it receives to its logger.Currently the Sergeant's logger writes to a stream logger, but this will be changed to a file handler. The logging.conf file is used to setup the framework's logging. This determines the default log level, format of messages, etc. Additionally, the Sergeant's configuration file has a "loggingPort" attribute which is used to setup the server which listens for log messages. This port is handed to the Sentinel when it joins an enclave in order to setup its DatagramHandler to point to the Sergeant.

Conclusion:

We conclude the report with a description of our demonstrations that show the efficacy of the DAF in dynamic moving-target reconfiguration of systems and the scalability of the DAF to realistic enterprise scales. In the appendices, we recapitulate the project milestones and deliverables, expand the operational scenario, and discuss in detail the DAF architecture. The accompanying CDROM contains reports, deliverables, papers, videos, software, and other information on the Digital Ants and the related technologies developed by this work. In this work, we have shown how these component applications may be decentralized and may perform analysis at the edge. Operationally, this will enable analytics to scale far beyond current limitations while not suffering from the bandwidth or computational limitations of centralized analysis. This effort has advanced the Systems Behavior group's Cyber Security research program to secure digital infrastructures by developing a dynamic means to adaptively defend complex cyber systems. We hope that this work will benefit both our client's efforts in system behavior modeling and cyber security to the overall benefit of the nation.

References

[1] Bruce J, GA Fink, "Shopping for Danger: E-commerce techniques applied to collaboration in cyber security," in Proceedings of VisualCol 2012 workshop.

[2] Carvalho, M. 2009. A distributed reinforcement learning approach to mission survivability in tactical MANETs. In Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies (CSIIRW '09), Frederick Sheldon, Greg Peterson, Axel Krings, Robert Abercrombie, and Ali Mili (Eds.). ACM, New York, NY, USA.

[3] Crenshaw, A., Programmable HID USB Keystroke Dongle: Using the Teensy as a pen testing device. Available at: http://www.irongeek.com/i.php?page=security/programmable-hid-usb-keystroke-dongle. Last viewed:5 July 2011.

[4] Crouse M, GA Fink, JL White, EW Fulp, KS Berenhaut, and JN Haack. 2011. "Using Swarming Agents for Scalable Security in Large Network Environments." Invited paper in Proceedings of the 54th IEEE International Midwest Symposium on Circuits and Systems.

[5] Crouse M and EW Fulp, "A Moving-Target Environment for Computer Configurations Using Genetic Algorithms," In Proceedings of the 4th Symposium on Configuration Analytics and Automation, 31 Oct 2011.

[6] Cuppens F and A Miege (2002). Alert correlation in a cooperative intrusion detection framework. In Proceedings of the 2002 IEEE Symposium on Security and Privacy

[7] Fink GA, CS Oehmen, JN Haack, AD McKinnon, EW Fulp, and MB Crouse, "Bio-Inspired Enterprise Security,"Self-Adaptive and Self-Organizing Systems (SASO), 2011 Fifth IEEE International Conference on, pp.212-213,3-7 Oct. 2011

[8] Golovanov, S. and Soumenkov, TDL4 Top Bot I. http://www.securelist.com/en/analysis/204792180/TDL4_ Top_Bot. Last viewed: 5 July 2011.

[9] Goodin, D., Hackers pierce network with jerry-rigged mouse: Mission Impossible meets Logitech. Posted in Enterprise Security, 27 June 2011. Available at: http://www.theregister.co.uk/2011/06/27/mission_ impossible_mouse_attack/. Last viewed 5 July 2011.

[10] Greitzer FL, and RE Hohimer. 2011. "Modeling Human Behavior to Anticipate Insider Attacks." Journal of Strategic Security 4(2):25-48. doi:10.5038/1944-0472.4.2.2

[11] Haack JN, GA Fink, WM Maiden, AD McKinnon, SJ Templeton, and EW Fulp, "Ant-Based Cyber Security," in Proceedings of the 8th International Conference on Information Technology: New Generations. IEEE Computer
Society, 2011.

[12] Dabek, F., R Cox, F Kaashoek, and R Morris, 2004. "Vivaldi: a decentralized network coordinate system,"SIGCOMM Comput. Commun. Rev. 34:4, pp. 15–26, ACM, New York, NY, USA.

[13] Hohimer RE, FL Greitzer, CF Noonan, and JD Strasburg. 2011. "CHAMPION: Intelligent Hierarchical Reasoning Agents for Enhanced Decision Support." In Proceedings of the Sixth International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS 2011), November 16-17, 2011, Fairfax, Virginia, vol.808, ed. PCG Costa and KB

Laskey, pp. 36-43. CEUR Workshop Proceedings, Aachen, Germany.

[14] Hui PSY, J Bruce, A Endert, GA Fink, ML Gregory, DM Best, and LR McGrath, "Towards Efficient Collaborationin Cyber Security" in Proceedings of the 2010 International Workshop on Collaboration in Security(COLSEC 2010), PNNL-SA-70532