Malware Classification for Cyber Physical System (CPS) based on Phylogenetics

Madihah Mohd Saudi, Sazali Sukardi, Noor Azwa Azreen Abd Aziz, Azuan Ahmad, Muhammad 'Afif Husainiamer

Abstract*: Nowadays, the sectors most commonly targeted by malwares across the world are manufacturing, oil and gas, and education. Malwares such as BlackEnergy2 and Triton have the ability to cause severe, life-threatening damages to an organization and critical infrastructure systems such as oil and gas. Security researchers and practitioners are looking for efficient solutions to mitigate such malware attacks. Therefore, this paper presents a malware cyber physical system (CPS) classification to detect attacks. This classification is inspired by phylogenetics, borrowed from the biological area in terms of evolutionary relationships among biological organisms. As for the cyber security perspective, it discovers the evolution ancestry of malware genes. This malware classification approach includes malware behavior, mode of attack and connected assets in the network. It can detect numerous forms of malware attacks based on correlation. The research is beneficial for CPS developers, suppliers and contractors, government agencies which regulate and govern utility operations, and the National Cyber Security Center (NCSC) which is responsible for protecting CPS.

Keywords: Cyber Physical System (CPS); Malware Attacks; Malware Classification; Phylogenetic

I. INTRODUCTION

Cyber-attacks of Cyber Physical Systems (CPSs) via the use of epidemic intelligent malware, began in 2003 worldwide, with Middle Eastern countries being mostly targeted [1]. These malwares targeted critical infrastructure such as the nuclear, pharmaceutical, and aviation industries, and the electricity and water sectors. In 2017, Triton malware was used to attack the petrochemical plant in the Kingdom of Saudi Arabia (KSA) and caused it to shutdown to prevent an explosion [2]. Similarly, BlackEnergy2 and Indutryoyer have attacked the electrical grid system in the Ukraine, Havex has exploited the CPS of different sectors in a number of European countries for espionage purposes, and Stuxnet was used to attack Iranian nuclear facilities [3]. The chronology of the rest of the CPS malware attacks is displayed in Figure 1.

Revised Manuscript Received on September 22, 2019.

Madihah Mohd Saudi, Cyber Security & Systems Research Unit, Islamic Science Institute (ISI, Universiti Sains Islam Malaysia (USIM), Nilai, Malaysia

Sazali Sukardi, Cyber Security Malaysia, Cyberjaya, Malaysia

Noor Azwa Azreen Abd Aziz, Cyber Security Malaysia, Cyberjaya, Malaysia

Azuan Ahmad, Cyber Security & Systems Research Unit, Islamic Science Institute (ISI, Universiti Sains Islam Malaysia (USIM), Nilai, Malaysia

Muhammad 'Afif Husainiamer, Cyber Security & Systems Research Unit, Islamic Science Institute (ISI), Universiti Sains Islam Malaysia (USIM), Nilai, Malaysia

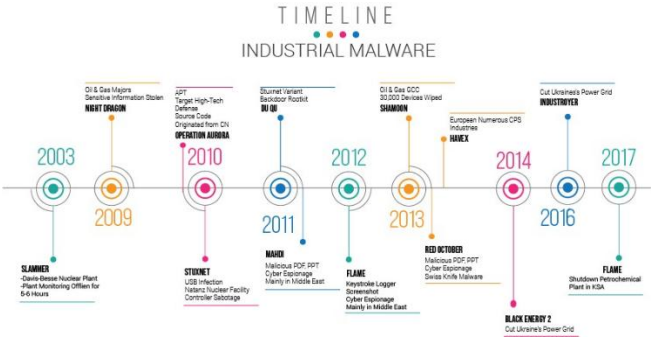

Fig. 1 Malwares Attack to CPS from 2003 until 2017

Based on the 5 main industrial control system (ICS) malwares discussed earlier, the similarities are based on command-and-control (C&C) and Remote-access-Trojan (RAT) capabilities, and these are similar in terms of botnet features. Botnet architecture and detection techniques have been studied by [4-8]. Based on existing works, it can be concluded that C&C and RAT can be conducted in a number of ways, such as via SMS, Bluetooth, website, Peer-to-peer (P2P) network or any other surveillance methods in a machine. Furthermore, the integration of advanced persistent threat (APT) into malware, and the evolution of malware, makes malware harder to detect. Each of the above discussed approaches has its own strength. Moreover, based on the existing work, most of them focus on different techniques for mobile botnet detection, but few mention malware classification, detection and response models for the CPS.

To overcome these challenges, we have developed a new malware classification formulation which considers the correlation between mode of attack, malware behaviour and devices connected to the network in the CPS. It can be used to detect past, current and future attacks, and can provide early warning alerts. As such, this classification could be used as a basis for developing a mobile malware detection model.

II. RELATED WORKS

From 1998 to 2018, only a few works such as those by [9-14] who discussed cyber-attacks with regard to CPS. CPS consists of a number of industrial control systems (ICS). These ICSs incorporate several devices such as Human Machine Interface (HMI) and Programmable Logic Controller (PLC), installed with computational software for data processing, and for providing access facilities,

connected with networks and which allows communication between humans, products and machines.

With the rise of the Internet-of-Things (IoT), these CPSs are at risk of being exposed to cyber-attacks. This is supported by work by [13]. This showed that cyber-attacks to water supply CPS could damage physical water assets and could control and decrease water supply [12]. In 2018, a work by [13] successfully introduced CIMA to prevent memory access at runtime for cyber physical systems (CPS), which is very beneficial when it comes to avoiding CPS being shut down by attackers. [15] describes the effect of side initial state information on the dynamic detection of data deception attacks against CPSs, while [16] introduces a satisfiability modulo theory approach with regard to the secure state estimation for CPSs under sensor attacks, and [17] discusses three types of cyber-attacks - denial-of-service attacks, replay attacks, and deception attacks. As for work by [18], they used a behaviour-based anomaly detection mechanism in the case of SCADA, while [19] developed a HARVEY PLC rootkit to attack power grid CPS. In addition, work by [20] used a Long Short-Term Memory Recurrent Neural Network (LSTMRNN) to detect data injection attacks on Industrial Control Systems (ICS).

Each of the works discussed above has their own techniques to mitigate CPS attacks. One of the similarities with existing works is that the problem emerges when CPSs are connected to the Internet for operational reasons. As a result, CPSs are exposed to the risk of cyber-attack. Furthermore, the fast evolvement and integration of malware incorporating APT, makes such malware harder to detect. Additionally, based on the above works, there is strong indicator that CPS will be the next target of cybercriminals in the future. Furthermore, these cyber-attacks against CPSs have caused severe harm, life-threatening damage to organizations, the shutdown of operations, risk of money loss, reduced productivity and the tarnishing of an organization's reputation.

Nonetheless, based on our analysis of the existing works, the security gaps are encountered in terms of APTs, network configurations, remote access, memory access runtime and media protection, documented policies and procedures and trained staff. They identify five (5) modes of cyber-attack against CPSs in the form of hacktivism, data theft, cybercrime, automated attacks and destructive attacks. Besides, CPS lack the ability to detect such cyber-attacks due to the non-existence of active sensors and the lack of ability to validate origin commands in the ICS. All these threats need efficient solutions. Therefore, we are proposing an intelligent malware classification based on phylogenetics to give early warning alerts with regard to CPS attacks. This classification is explained in Section IV.

There were a few works produced by [4-7] that used bio-inspired concepts to provide cybersecurity solutions. These showed the significance of bio-inspired approaches as a basis for developing new algorithms for malware detection. Table 1 displays a comparative summarization of other bio-inspired algorithms.

Table. 1 Comparison of bio-inspired algorithms

Algorithm	Concept Description	Limitations
Danger Theory (DT)	It identifies between dangerous and safe pathogens.	-Difficult to identify danger signals
Fuzzy Logic (FL)	It is a concept that possesses a degree of truth and a generalization of standard logic.	-Needs precise solutions and conditions. -Expensive, and requires extensive testing.
Genetic Algorithm (GA)	It is used in artificial intelligence and computing with the use of heuristic search methods.	-Constant optimization in response times. -Random solutions and convergence
Negative Selection Algorithm (NSA)	It is used to build an anomaly detection system based on self and non-self pattern.	-Scalability and coverage.
Phylogenetic	It is related with different organisms and taxonomic groups by using a tree diagram based on evolutionary history	Not applicable

Figure 2 is an example of the summarization of a phylogenetic diagram that assists us to understand malware evolutionary trends, extracting the crucial elements inside malware codes, and strategizing the best detection techniques.

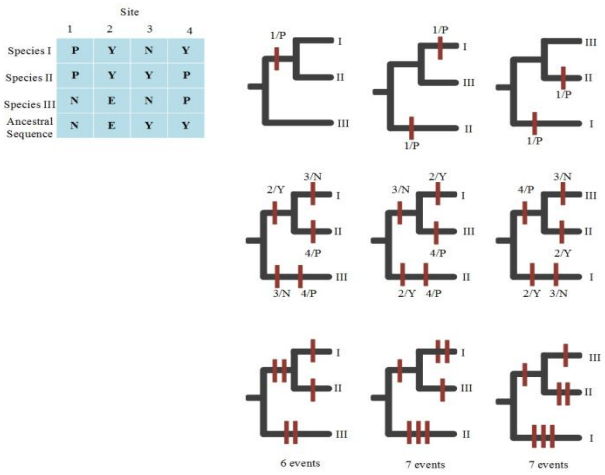

Fig. 2 Phylogenetic Diagram

III. METHODOLOGY

The research processes for this research are as summarized in Figure 3. There are 3 phases in the form of Phase 1: Reverse Code Engineering; Phase 2: Intrusion; Phase 3: ICS attacks. The main processes are: setup lab architecture, conduct continuous monitoring, conduct correlation reporting, engage in attack analytics, engage systems, and sensor improvement and upgrades. For this paper, only Triton was used to test the proposed CPS malware classifications.

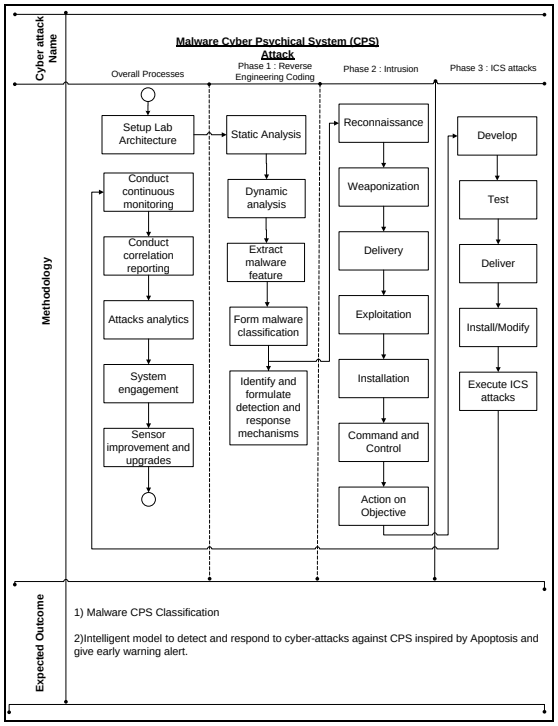

Fig. 3 Overall Research Processes

For Phase 1, reverse code engineering involves the use of hybrid analysis. This combines static and dynamic analysis. In static analysis the coding is analysed without executing it, while for dynamic analysis the coding is executed to capture its behaviour. Several works have used static analysis and others have used dynamic analysis. This depends on the researcher's objective and the depth of analysis when it comes to selecting the type of analysis to be used. For this paper, hybrid analysis is used to analyse a big dataset with better accuracy.

In terms of the lab setup architecture, we used honeynet. It is capable of monitoring threats, mimicking a real CPS-like environment which consists of several ICSs, and notifying one if a potential threat is within one's network. Furthermore, any attacks or threats from an outsider can be identified and analysed. We introduced 5 main CPS malwares in the form of Stuxnet, Havex, Black Energy 2, Industroyer and Triton. Several works such by [21-23] have used honeynet for ICS and SCADA simulation, which indicates the reliability of this architecture. Even 2 patents by [24, 25] have been made which relate to ICS honeynet. Figure 4 displays the honeynet architecture. It consists of a SCADA application server used to monitor the ICS devices, a report server to gather reports on ICS device activities, a Programmable Logic Controller (PLC) device that acts as a controller and a Human Machine interface (HMI) PC to communicate between the human user and the PLC. Table 2 displays the software and hardware used for this honeynet. The mapping of the phylogenetics with regard to mobile malware CPS is as summarised in Table 3.

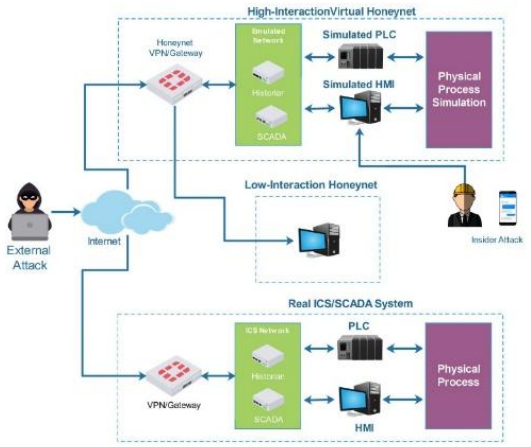

Fig. 4 Overall CPS Honeynet Architecture

Table. 2 Software and hardware Table

Name	Description
Programmable Logic Controller (PLC) device	Acts as controller
Workstation (Human Machine interface (HMI)	For data processing and modelling
Web Server (Historian Server)	Data sharing over browser and mobile devices
Database/Application Server (Report Server and SCADA server)	To store database and application / production, to gather reports of ICS device activities
Integration Server	Integration of data processing with multiple data format
Switch	Connectivity between instrument/equipment
Firewall	For Policy & Security
Security Sensor	To detect any normal and abnormal situations.
Mock SIS Control	To simulate control at ICS
Sensory management device	To monitor and communicate with sensor.

Table. 3 Mapping Phylogenetics to Mobile Malware CPS Classification

Phylogenetics	Mobile Malware
Based on evolutionary history and the relatedness of different organisms and taxonomic groups by using a tree diagram.	-Evolution ancestry of malware genes based on the integration of malware behaviour, vulnerability exploitation and connected assets in a network. -Behaviour refers to infection, payload, operating algorithm, activation and propagation. -Mode of attack is based on hacktivism, data theft, cybercrime, automated attack or destructive attack. -Connected assets refer to HMI, PC based controller, Historian, CPS apps or Engineer & Operator workstation -These three elements are mapped into a tree diagram.

IV. FINDINGS

In terms of malware classification, there are 3 main variables in the form of malware architecture, mode attack and connected asset in CPS network. These elements are correlated in the following mathematical formulations:

$$(A,T)=Z \qquad (1)$$

where $A(X + Y + V)$ (2)

$$f(A_i, T_j) = Z_{ij} \quad (3)$$

where, A represents malware classification, T represent target asset and Z is the detection model, X represents malware behaviour, Y represents mode of attack and Z represents connected assets.

$$A(X,Y,V) = X + Y + V$$

$$X = X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5$$

$$Y = Y_1 \cup Y_2 \cup Y_3 \cup Y_4 \cup Y_5$$

$$V = V_1 \cup V_2 \cup V_3 \cup V_4 \cup V_5$$

$A_i \quad X \quad Y \quad V$

. . .

. . .

. .

$A_n \quad . \quad . \quad V_n$

where:

$X1$- $X5$: Payload, infection, operating algorithm, activation and propagation

$Y1$- $Y5$: Destructive attack, automated attack, hacktivism, data theft and cybercrime.

$V1$- $V5$: PC based controller, Human machine interface (HMI), Historian, CPS apps and Engineer & Operator workstation.

Based on above formula 1 and formula 2, the correlation between the variables were formulated. The finding for mobile malware CPS as summarised in Table 4.

Table. 4 Malware CPS Classification

Malware CPS Classification	Description
Malware behavior $X = X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5$	*1) Infection*: Spread via host file - Windows computer that is connected to Safety Instrumented Systems (SIS). *2) Activation*: Self-activation. It is based on SIS controller. Whenever download process is occurred, it will inject itself into the SIS memory. *3) Payload*: Destructive. It shutdown operation and malfunction the SIS. Installed backdoor to launch attack on SIS. *4) Operating algorithm*: Terminate and Stay Resident (TSR). It injects code to modify the SIS device behaviour. *5) Propagation*: Passive monitoring.
Mode of attack ($Y1$)	Destructive attack
Connected assets ($V1$)	PC-based controller

It could be concluded that Triton consists of:

$$A(X,Y,V) = X + Y + V$$

$$= (X = X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5) + (Y1) + (V1)$$

Based on above mathematical formulation, Triton has all the elements needed for malware CPS classification and has elements for further possible exploitation by the attackers. We can also conclude that for CPS attacks, whatever CPS components are connected to PC and Internet, there is the possibility of it being exploited by attackers. Furthermore, based on the findings of this experiment, the proposed malware classification enables us to identify all the elements or weaknesses that could allow malware to infect CPSs, especially SIS. Consequently, once all these elements have been identified, it will be much easier for the introduction of a detection and removal strategy.

V. CONCLUSIONS

Based on the experiment described in this paper, it is proven that the proposed malware CPS classification could be used to identify malware attacks against vulnerable CPS. Currently, CPS cyber-attacks continue to evolve and we need effective solutions to mitigate these attacks. Malware classification is one of the input elements associated with developing a model or mechanism to detect malware CPS attacks. Our work in this paper is part of a project for malware CPS detection modelling, which will be continued in the future.

ACKNOWLEDGMENT

The authors would like to express their gratitude to Ministry of Education (MOE),Malaysia, Universiti Sains Islam Malaysia (USIM) and Cyber Security Malaysia (CSM) for the support and facilities provided. This research paper project is under grant: [FRGS/1/2019/ICT04/USIM/02/3].

REFERENCES

1. Wolfgang Schwab.(2018). The state of Industrial Cybersecurity 2018. URL: https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf
2. Nicole P. and Clifford K. (2018, March 15). A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try. Retrieved November 1, 2018 from https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html
3. Barak Perelman. (2018). Protect Your System from the Rise of ICS Malware. Cahaba Media Group. URL: https://www.pumpsandsystems.com/protect-your-system-rise-ics-malware
4. Karim, A., Shah, S. A. A., Salleh, R. Bin, Arif, M., Md Noor, R., Shamshirband, S.,Noor, R. (2015). Mobile botnet attacks – an emerging threat: Classification, review and open issues. KSII Transactions on Internet and Information Systems, 9(4), 1471–1492.
5. Lee, H., Eun Su Jeong, In Seok Kim & Dong.(2016). SafeGuard: a behavior based real-time malware detection scheme for mobile multimedia applications in android platform. Multimed Tools Appl, Springer, pp 1-21.

6. Hou, S., Saas, A., Chen, L. and Ye, Y.,(2016). Deep4MalDroid: A Deep Learning Framework for Android Malware Detection Based on Linux Kernel System Call Graphs. In Web Intelligence Workshops (WIW), IEEE/WIC/ACM International Conference on (pp.104-111). IEEE.
7. Ni, Z., Yang, M., Ling, Z., Wu, J.N. and Luo, J., (2016). Real-Time Detection of Malicious Behavior in Android Apps. In Advanced Cloud and Big Data (CBD), 2016 International Conference on (pp. 221-227). IEEE.
8. Saudi,Madihah Mohd, Muhammad Zuhair Abd Rahman,Azirah Alfaizah Mahmud,Nurlida Basir, Yum Suhaylah Yusoff,(2016). A New System Call Classification for Android Mobile Malware Surveillance Exploitation via SMS Message, Advanced Computer and Communication Engineering Technology,Lecture Notes in Electrical Engineering, Springer International Publishing Switzerland, Volume 362, pp 103-112.
9. Clark, R. M., & Deininger, R. A. (2000). Protecting the nation's critical infrastructure: The vulnerability of US water supply systems. Journal of contingencies and crisis management, 8(2), 73-80.
10. Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., & Ostfeld, A. (2017). Characterizing cyber-physical attacks on water distribution systems. Journal of Water Resources Planning and Management, 143(5), 04017009.
11. Bittau, A., Belay, A., Mashtizadeh, A., Mazi´eres, D., Boneh, D.: Hacking blind. In: Proceedings of the 2014 IEEE Symposium on Security and Privacy. SP'14 (2014) 227 – 242
12. Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., & Ostfeld, A. (2017). Characterizing cyber-physical attacks on water distribution systems. Journal of Water Resources Planning and Management, 143(5), 04017009.
13. Chekole, E.G., Chattopadhyay, S., Ochoa, M., Huaqun, G.: Enforcing full-stack memory safety in cyber-physical systems. In: Proceedings of the International Symposium on Engineering Secure Software and Systems (ESSoS'18), Springer International Publishing (2018)
14. Floyd, D.H., Shelton, J.W. and Bush, J.E., Boeing Co, 2018. Systems and methods for detecting a security breach in an aircraft network. U.S. Patent 9,938,019.
15. Chen, Y., Kar, S. and Moura, J.M., 2017. Dynamic attack detection in cyber-physical systems with side initial state information. IEEE Transactions on Automatic Control, 62(9), pp.4618-4624.
16. Shoukry, Y., Nuzzo, P., Puggelli, A., Sangiovanni-Vincentelli, A.L., Seshia, S.A. and Tabuada, P., 2017. Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach. IEEE Transactions on Automatic Control, 62(10), pp.4917-4932.
17. Ding, D., Han, Q. L., Xiang, Y., Ge, X., & Zhang, X. M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing, 275, 1674-1683.
18. Zhou, X., Xu, Z., Wang, L., Chen, K., Chen, C. and Zhang, W., 2018. Behavior Based Anomaly Detection Model in SCADA System. In MATEC Web of Conferences (Vol. 173, p. 01011). EDP Sciences.
19. Garcia, L., Brasser, F., Cintuglu, M.H., Sadeghi, A.R., Mohammed, O.A. and Zonouz, S.A., 2017, February. Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit. In NDSS.
20. Wang, W., Xie, Y., Ren, L., Zhu, X., Chang, R. and Yin, Q., 2018, May. Detection of data injection attack in industrial control system using long short term memory recurrent neural network. In 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA) (pp. 2710-2715). IEEE
21. Hyun, D., 2018. Collecting cyberattack data for industrial control systems using honeypots (Doctoral dissertation, Monterey, California: Naval Postgraduate School).
22. Mashima, D., Chen, B., Gunathilaka, P. and Tjiong, E.L., 2017, October. Towards a grid-wide, high-fidelity electrical substation honeynet. In Smart Grid Communications (SmartGridComm), 2017 IEEE International Conference on (pp. 89-95). IEEE.
23. Zhao, C. and Qin, S., 2017, December. A research for high interactive honepot based on industrial service. In Computer and Communications (ICCC), 2017 3rd IEEE International Conference on (pp. 2935-2939). IEEE.
24. Leandro Pfleger De Aguiar, Dong Wei, Shawn McGraw, High interaction non-intrusive industrial control system honeypot. WO2018044410A1, World Intellectual Property Organization, 8 March 2018.
25. Juan Asenjo, John Strohmenger, Stephen Nawalaniec, Bradford H. Hegrat, Joseph A. Harkulich, Jessica Lin Korpela, Jenifer Rydberg Wright, Rainer Hessmer, John Dyck, Edward Alan Hill, Sal Conti, Using cloud-based data for virtualization of an industrial environment. US20140336785A1, United States Patent and Trademark Office, 9 May 2013