International Conference on Recent Advancement in Science & Technology- 2020
(ICRAST-2020)

A Review on Malware Detection for Internet of Thongs (IoT)

[1]Shipra Singh, [2]Abhishek Saxena
Dept of Computer science
Bansal Institute of Enginnering and Technology, Lucknow, India
bhushipra14@gmail.com, abhisaxena0212@gmail.com

Abstract: Internet of Things (IoT) in military settings generally consists of a diverse range of Internet-connected devices and nodes (e.g. medical devices and wearable combat uniforms). These IoT devices and nodes are a valuable target for cyber criminals, particularly state-sponsored or nation state actors. A common attack vector is the use of malware. In this paper, we present a deep learning based method to detect Internet Of Battlefield Things (IoBT) malware via the device's Operational Code (OpCode) sequence. We transmute OpCodes into a vector space and apply a deep Eigenspace learning approach to classify malicious and benign applications. We also demonstrate the robustness of our proposed approach in malware detection and its sustainability against junk code insertion attacks. Lastly, we make available our malware sample on Github, which hopefully will benefit future research efforts (e.g. to facilitate evaluation of future malware detection approaches).

Keywords: IOT, OpCode, Eigenspace learning, Malware detection.

1. Introduction:

Junk code injection attack is a malware anti-forensic technique against OpCode inspection. As the name suggests, junk code insertion may include addition of benign OpCode sequences, which do not run in a malware or inclusion of instructions (e.g. NOP) that do not actually make any difference in malware activities. Junk code insertion technique is generally designed to obfuscate malicious OpCode sequences and reduce the 'proportion' of malicious OpCodes in a malware In our proposed approach, we use an affinity based criteria to mitigate junk OpCode injection anti-forensics technique.

Specifically, our feature selection method eliminates less instructive OpCodes to mitigate the effects of injecting junk OpCodes. To demonstrate the effectiveness of our proposed approach against code insertion attack, in an iterative manner, a specified proportion (f5%, 10%, 15%, 20%, 25%, 30%g) of all elements in each sample's generated graph were selected randomly and their value incremented by one. For example, in the 4th iteration of the evaluations, 20% of the indices in each sample's graph were chosen to increment their value by one.

In addition, in our evaluations the possibility of a repetitive element selection was included to simulate injecting an OpCode more than once. Incrementing Ei;j in the sample's generated graph is equivalent to injecting OpCodej next to the OpCodei in a sample's instruction sequence to mislead the detection algorithm. Algorithm 2 describes an iteration of junk code insertion during experiments, and this procedure should repeat for each iteration of k-fold validation. To show the robustness of our proposed approach and benchmark it against existing proposals, two congruent algorithms described in Section 1 are applied on our generated dataset using Adaboost as the classification algorithm.

A typical Internet of Things (IoT) deployment includes a wide pervasive network of (smart) Internet-connected devices, Internet-connected vehicles, embedded systems, sensors, and other devices/systems that autonomously sense, store, transfer and process collected data [1], [2], [3]. IoT devices in a civilian setting includes health [4], agriculture [5], smart city [6], and energy and transport management systems [7], [8]. IoT can also be deployed in adversarial settings such as battlefields [9]. For example in 2017, U.S. Army Research Laboratory (ARL) "established an Enterprise approach to address the challenges resulting from the Internet of Battlefield Things (IoBT) that couples multi-disciplinary internal research with extramural research and collaborative ventures.

2. Related Work:

Malware detection methods can be static or dynamic [5]. In dynamic malware detection approaches, the program is executed in a controlled environment (e.g., a virtual machine or a sandbox) to collect its behavioral attributes such as required resources, execution path, and requested privilege, in order to classify a program as malware or benign [6], [7], [8]. Static approaches (e.g., signature-based detection, byte-sequence n-gram analysis, opcode sequence identification and control flow graph traversal) statically inspect a program code to detect suspicious applications. David et al [9] proposed Deepsign to automatically detect malware using a signature generation method. The latter creates a dataset based on behaviour logs of API calls, registry entries, web searches, port accesses, etc, in a sandbox and then converts logs to a binary vector. They

used deep belief network for classification and reportedly achieved 98.6% accuracy. In another study, Pascanu et al. [1] proposed a method to model malware execution using natural language modeling. They extracted relevant features using recurrent neural network to predict the next API calls. Then, both logistic regression and multi-layer perceptions were applied as the classification module on next API call prediction and using history of past events as features. It was reported that 98.3% true positive rate and 0.1% false positive rate were achieved. Demme et al. [4] examined the feasibility of building a malware detector in IoT nodes' hardware using performance counters as a learning feature and K-Nearest Neighbor, Decision Tree and Random Forest as classifiers. The reported accuracy rate for different malware family ranges from 25% to 100%. Alam et al. [2] applied Random Forest on a dataset of Internet-connected smartphone devices to recognize malicious codes. They executed APKs in an Android emulator and recorded different features such as memory information, permission and network for classification, and evaluated their approach using different tree sizes. Their findings showed that the optimal classifier contains 40 trees, and 0.0171 of mean square root was achieved. In order to detect crypto-ransomware on Android devices as management nodes of an IoT networks, Azmoodeh et al. [3] recorded the power usage of running processes and identified distinguishable local energy consumption patterns for benign applications and ransomware. They broke down the power usage pattern into sub-samples and classified them, as well as aggregating sub-samples' labels to determine the final label. The proposed approach reportedly achieved 92.75% accuracy. The need to secure IoT backbone against malware attacks motivated Haddad Pajouh et al. [44] to propose a two-layer dimension reduction and two-tier classification module to detect malicious activities. Specifically, the authors used Principle Component Analysis and Linear Discrimination Analysis to reduce the dataset and then used Na¨ıve Bayes and K-Nearest Neighbor to classify samples. They achieved detection and false alarm rates of 84.86% and 4.86%, respectively. While OpCodes are considered an efficient feature for malware detection, there does not appear to have been any attempt to use OpCodes for IoT and IoBT malware detection. In addition, using deep learning for robust malware detection in IoT networks appears to be another understudied topic. Thus, in this paper, we seek to contribute to this gap by exploring the potential of using OpCodes as features for malware detection with deep Eigenspace learning.

E. Bertino, K.-K. R. Choo, D. Georgakopolous, and S. Nepal, 2016, The Internet of Things (IoT) is the latest Internet evolution that incorporates a diverse range of things such as sensors, actuators, and services deployed by different organizations and individuals to support a variety of applications. The information captured by IoT presents an unprecedented opportunity to solve large-scale problems in those application domains to deliver services; example applications include precision agriculture, environment monitoring, smart health, smart manufacturing, and smart cities. Like all other Internet based services in the past, IoT-based services are also being developed and deployed without security consideration. By nature, IoT devices and services are vulnerable to malicious cyber threats as they cannot be given the same protection that is received by enterprise services within an enterprise perimeter. While IoT services will play an important role in our daily life resulting in improved productivity and quality of life, the trend has also "encouraged" cyber-exploitation and evolution and diversification of malicious cyber threats. Hence, there is a need for coordinated efforts from the research community to address resulting concerns, such as those presented in this special section. Several potential research topics are also identified in this special section.

X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, 2017, Internet of Things (IoT) is an emerging technology, which makes the remote sensing and control across heterogeneous network a reality, and has good prospects in industrial applications. As an important infrastructure, Wireless Sensor Networks (WSNs) play a crucial role in industrial IoT. Due to the resource constrained feature of sensor nodes, the design of security and efficiency balanced authentication scheme for WSNs becomes a big challenge in IoT applications. First, a two-factor authentication scheme for WSNs proposed by Jiang et al. is reviewed, and the functional and security flaws of their scheme are analyzed. Then, we proposed a three-factor anonymous authentication scheme for WSNs in Internet of Things environments, where fuzzy commitment scheme is adopted to handle the user's biometric information. Analysis and comparison results show that the proposed scheme keeps computational efficiency, and also achieves more security and functional features. Compared with other related work, the proposed scheme is more suitable for Internet of Things environments.

J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, 2013, Ubiquitous sensing enabled by Wireless Sensor Network (WSN) technologies cuts across many areas of modern day living. This offers the ability to measure, infer and understand environmental indicators, from delicate ecologies and natural resources to urban environments. The proliferation of these devices in a communicating-actuating network creates the Internet of Things (IoT), wherein, sensors and actuators blend seamlessly with the environment around us, and the information is shared across platforms in order to develop a common operating picture (COP). Fuelled by the recent adaptation of a variety of enabling device technologies such as RFID tags and readers,

near field communication (NFC) devices and embedded sensor and actuator nodes, the IoT has stepped out of its infancy and is the the next revolutionary technology in transforming the Internet into a fully integrated Future Internet. As we move from www (static pages web) to web2 (social networking web) to web3 (ubiquitous computing web), the need for data-on-demand using sophisticated intuitive queries increases significantly. This paper presents a cloud centric vision for worldwide implementation of Internet of Things. The key enabling technologies and application domains that are likely to drive IoT research in the near future are discussed. A cloud implementation using Aneka, which is based on interaction of private and public clouds is presented. We conclude our IoT vision by expanding on the need for convergence of WSN, the Internet and distributed computing directed at technological research community.

F. Leu, C. Ko, I. You, K.-K. R. Choo, and C.-L. Ho, 2017, Recently, Wireless Body Sensor Networks (WBSNs) have been popularly employed to measure people's physiological parameters, particularly for disease monitoring, prevention, and treatment. In this study, we propose a smartphone-based WBSN, named Mobile Physiological Sensor System (MoPSS), which collects users' physiological data with body sensors embedded in a smart shirt. A patient's vital signs are continuously gathered and sent to a smart phone in a real-time manner. The data are then delivered to a remote healthcare cloud via WiFi. After performing necessary classification and analysis, the health information of individual patients is also stored in the cloud, from which authorized medical staffs can retrieve required data to monitor patients' health conditions so that when necessary, caregivers are able to reach the patients as soon as possible and provide required assistance. Our simulations demonstrate that the presented healthcare system provides a better solution for health management.

M. Roopaei, P. Rad, and K.-K. R. Choo, 2017, Irrigation Is Crucial For Agriculture Production To Ensure That Farmers Are Able To Meet Crop Water Demands Even In Situations Where There Is Inadequate Rainfall. However, poor irrigation scheduling and inefficient utilization of water resources are two of several ubiquitous parameters restricting production in many agricultural regions. Cultivators can use information such as light, humidity and temperature levels to modify irrigation schedules and avoid the risk of damaging crops.2 For example, soil sensors can be used to collect information on how water flows through the land and can be used to track changes in soil moisture, temperature, and levels of nitrogen and carbon. These sensors can work in conjunction with drip irrigation methods and fertigation to avoid unnecessary waste of water and fertilizer, thus, increasing fruit and leaf quality. Real-time data of weather predictions, soil conditions, crop features, etc. can support farmers in making informed decisions on which crops to plant where and when as well as when to plough, etc. This allows the monitoring, optimization, and precise control of high-yielding (wheat, corn, etc.) and sensitive crops (vineyards, tropical fruits, etc.), whether cultivated outdoors or in greenhouses. This permits farmers to help reach maximum crop production with optimal quality.

X. Li, J. Niu, S. Kumari, F. Wu, and K.-K. R. Choo, 2017, Smart city is a development tendency of future city, which improves almost all aspects of quality of urban residents' life by adopting Information and Communication Technology. In smart city, people can interact directly with the community and the infrastructure at anytime and anywhere, where GLObal MObility NETwork (GLOMONET) is an important network infrastructure for smart city. Recently, Gope and Hwang proposed an efficient authentication scheme for GLOMONET. However, we find their scheme lacks session key update and wrong password detection mechanisms, and vulnerable to denial-of-service attack. Besides, the session key can be known by HA (home agent), and perfect forward secrecy cannot be ensured. Furthermore, in their scheme, HA has to take heavy secret key management work. Based on previous work, this paper first summarizes the security and function requirements of authentication for GLOMONET in smart city environment. Later, this paper proposed a robust biometrics based three-factor authentication scheme for GLOMONET in smart city. Security features of the proposed scheme are analyzed in detail, and comparisons of our scheme with other related schemes are illustrated. Analysis and comparison results show that our scheme meets the preconcerted security requirements of authentication for GLOMONET in smart city environment, and it is robust for GLOMONET in smart city environments with higher security requirements.

D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, 2012, The term ''Internet-of-Things'' is used as an umbrella keyword for covering various aspects related to the extension of the Internet and the Web into the physical realm, by means of the widespread deployment of spatially distributed devices with embedded identification, sensing and/or actuation capabilities. Internet-of-Things envisions a future in which digital and physical entities can be linked, by means of appropriate information and communication technologies, to enable a whole new class of applications and services. In this article, we present a survey of technologies, applications and research challenges for Internetof-Things.

Kott, A. Swami, and B. J. West, 2016, The rapid emergence of Internet of Things is propelled by the logic of

two irresistible technological arguments: machine intelligence and networked communications. Things are more useful and effective when they are smarter, and even more so when they can talk to each other. Exactly the same logic applies to things that populate the world of military battles. They too can serve the human warfighters better when they possess more intelligence and more ways to coordinate their actions among themselves. We call this the Internet of Battle Things, IoBT. In some ways, IoBT is already becoming a reality1 , but 20-30 years from now it is likely to become a dominant presence in warfare. The battlefield of the future will be densely populated by a variety of entities ("things") – some intelligent and some only marginally so – performing a broad range of tasks: sensing, communicating, acting, and collaborating with each other and human warfighters2 . They will include sensors, munitions, weapons, vehicles, robots, and human-wearable devices. Their capabilities will include selectively collecting and processing information, acting as agents to support sensemaking, undertaking coordinated defensive actions, and unleashing a variety of effects on the adversary. They will do all this collaboratively, continually communicating, coordinating, negotiating and jointly planning and executing their activities. In other words, they will be the Internet of Battle Things.

C. Tankard, 2015, Internet of Things (IoT) is playing a more and more important role after its showing up, it covers from traditional equipment to general household objects such as WSNs and RFID. With the great potential of IoT, there come all kinds of challenges. This paper focuses on the security problems among all other challenges. As IoT is built on the basis of the Internet, security problems of the Internet will also show up in IoT. And as IoT contains three layers: perception layer, transportation layer and application layer, this paper will analyze the security problems of each layer separately and try to find new problems and solutions. This paper also analyzes the cross-layer heterogeneous integration issues and security issues in detail and discusses the security issues of IoT as a whole and tries to find solutions to them. In the end, this paper compares security issues between IoT and traditional network, and discusses opening security issues of IoT.

C. J. DOrazio, K. K. R. Choo, and L. T. Yang, 2017, Increasingly, big data (including sensitive and commercial-in-confidence data) is being accessible and stored on a range of Internet of Things (IoT) devices, such as our mobile devices. Therefore, any vulnerability in IoT devices, operating system or software can be exploited by cybercriminals seeking to exfiltrate our data. In this paper, we use iOS devices as case studies and highlight the potential for pairing mode in iOS devices (which allows the establishment of a trusted relationship between an iOS device and a personal computer) to be exploited for covert data exfiltration. In our three case studies, we demonstrate how an attacker could exfiltrate data from a paired iOS device by abusing a library and a command line tool distributed with iTunes. With the aim of avoiding similar attacks in the future, we present two recommendations.

M. Conti, A. Dehghantanha, K. Franke, and S. Watson, 2018, The Internet of Things (IoT) envisions pervasive, connected, and smart nodes interacting autonomously while offering all sorts of services. Wide distribution, openness and relatively high processing power of IoT objects made them an ideal target for cyber-attacks. Moreover, as many of IoT nodes are collecting and processing private information, they are becoming a goldmine of data for malicious actors. Therefore, security and specifically the ability to detect compromised nodes, together with collecting and preserving evidences of an attack or malicious activities emerge as a priority in successful deployment of IoT networks. In this paper, we first introduce existing major security and forensics challenges within IoT domain and then briefly discuss about papers published in this special issue targeting identified challenges.

3. Conclusion:

IoT, particularly IoBT, will be increasingly important in the foreseeable future. No malware detection solution will be foolproof but we can be certain of the constant race between cyber attackers and cyber defenders. Thus, it is important that we maintain persistent pressure on threat actors. In this paper, we presented an IoT and IoBT malware detection approach based on class-wise selection of Op- Codes sequence as a feature for classification task.

References:

[1] E. Bertino, K.-K. R. Choo, D. Georgakopolous, and S. Nepal, "Internet of things (iot): Smart and secure service delivery," ACM Transactions on Internet Technology, vol. 16, no. 4, p. Article No. 22, 2016.

[2] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," Journal of Network and Computer Applications, 2017.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future generation computer systems, vol. 29, no. 7, pp. 1645– 1660, 2013.

[4] F. Leu, C. Ko, I. You, K.-K. R. Choo, and C.-L. Ho, "A smartphonebased wearable sensors for monitoring real-time physiological data," Computers & Electrical Engineering, 2017.

[5] M. Roopaei, P. Rad, and K.-K. R. Choo, "Cloud of things in smart agriculture: Intelligent irrigation monitoring by thermal imaging," IEEE Cloud Computing, vol. 4, no. 1, pp. 10–15, 2017.

[6] X. Li, J. Niu, S. Kumari, F. Wu, and K.-K. R. Choo, "A robust biometrics based three-factor authentication scheme for global mobility networks in smart city," Future Generation Computer Systems, 2017.
[7] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010. [8] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.
[9] A. Kott, A. Swami, and B. J. West, "The internet of battle things," Computer, vol. 49, no. 12, pp. 70–75, 2016.
[10] C. Tankard, "The security issues of the internet of things," Computer Fraud & Security, vol. 2015, no. 9, pp. 11 – 14, 2015.
[11] C. J. DOrazio, K. K. R. Choo, and L. T. Yang, "Data exfiltration from internet of things devices: ios devices as case studies," IEEE Internet of Things Journal, vol. 4, no. 2, pp. 524–535, April 2017.
[12] S. Watson and A. Dehghantanha, "Digital forensics: the missing piece of the internet of things promise," Computer Fraud & Security, vol. 2016, no. 6, pp. 5–8, 2016.
[13] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," Future Generation Computer Systems, vol. 78, no. Part 2, pp. 544 – 546, 2018.
[14] E. Bertino and N. Islam, "Botnets and internet of things security," Computer, vol. 50, no. 2, pp. 76–79, Feb 2017.
[15] J. Gardiner and S. Nagaraja, "On the security of machine learning in malware c&c detection: A survey," ACM Computing Surveys, vol. 49, no. 3, p. Article No. 59, 2016.