FP-International Journal of Computer Science Research (IJCSR)
Volume 2, Issue 2, Pages 64-67, June 2015

MPN: Monitoring the Proximity of Malware Propagation in Wireless Sensor Network

Nataraj.J
M.Tech, SITE School
VIT University Vellore-632014
natarajlogin@gmail.com

Prof. KamalaKannan .J
SITE School VIT University
Vellore- 632014
jkamalakannan@vit.ac.in

ABSTRACT
Malware infection is one of the weaknesses of computer system through software. This may happen when the software react irrelevant action based on user's process. Malware attempts to proliferate in communication system without regard to the state of infected system: It is one of the ways to prevent the malware infection that can only say that systems are patched to eliminate that exploit. In prior system, they used dynamic malware scam framework to reduce the propagation activity in single system. But it couldn't suitable to eliminate the propagation in multi-environment system. The proposed system, by analysis of appearance and disappearance of malware types can dynamically predict the malware samples which are classified by behavioral profiles correlated with timelines. To simulate the result of vulnerable time period can used to analyze the propagation of malware in communication medium.

Keywords
Malwares patch time, vulnerability resolutions, and malware emergency.

1. Introduction

Recent advances in sensor networks research have shown that an attacker can exploit different mechanisms of sensor nodes and spread malicious code throughout the whole network without physical contact. Such a method is to exploit memory related vulnerabilities, like buffer overflows [2, 3], to launch a worm attack. Since all sensor nodes execute the same program image, finding such vulnerability can lead to the construction of self-propagating packets that inject malicious code to their victims and transfer execution to that code. If the malware is constructed such as it resends itself to the neighbors of the node by repeating the same process, the attacker can compromise the whole network rapidly and take complete control of it [1, 4]. While this attack is extremely dangerous, there has been very little research in this area. Our work target sensor devices following the von Neumann architecture. In the saturations and data are stored in the same memory space, allowing the attacker to transfer execution control where the mal-packet is stored. This allows the injection and execution of arbitrary code that did not exist previously in the mote's memory.

However, achieving that in sensor devices following the von Neumann architecture has some interesting parameters. First, since code injection attacks are based on changing the flow of control in a program, this may lead the sensor to restart itself or go into an unstable state, where further execution of the attack code is canceled. Furthermore, sensor nodes characteristics and constraints limit the capabilities of an attacker, who may want to send large blocks of code that exceed the allowed packet size. Thus, in order to send a meaningful piece of code, one has to break it down and send it through multiple packets. We should also stress that the whole attack code must reside in a contiguous memory region so it can be executed. Therefore, the attacker must perform a "multistage buffer-overflow attack", where she can manipulate an arbitrary address pointer and modify the data it points to.

2. Literature Survey

Vengali Sagar, V. Ravi Kumar [1] declare different mobile cloud services get into mobile cloud infrastructure and to discuss the security threats that might be chance through the usage of many service scenarios. Then, we explore architecture and methodology for abnormal behavior detection through the observation of host and network data. To check our methodology, we inserted malicious programs into our mobile cloud test be and utilized a machine learning algorithm to find out from those programs the abnormal behavior that arise

Sancheng Peng, Shui Yu, and Aimin Yang [2] described mobile malware evolution since 2004, and then list the classes of mobile malware and their infection vectors. At the end of the first part, we enumerate the possible damage caused by smart phone malware. In the second part, we focus on smart phone malware propagation modeling. In order to understand the propagation behavior of smart phone malware, we recall generic epidemic models as a foundation for further exploration. We then extensively survey the smart phone malware propagation models

Yi Yang, 1,2 Sencun Zhu, and 1 Guohong Cao [3] the notorious buffer overflow vulnerability that has caused numerous Internet worm attacks could also be exploited to attack sensor networks. We call the malicious code

that exploits buffer-overflow vulnerability in a sensor program sensor worm. Clearly, sensor worm will be a serious threat, if not the most dangerous one, when an attacker could simply send a single packet to compromise the entire sensor network.

Bo Sun Guanhua Yan ; Yang Xiao[4] wireless sensor networks suffer from growing security concerns posed by worms because of sensor networks' low physical security, lack of resilience and robustness of underlying operating systems, and the ever increased complexity of deployed applications. In this paper, we study worm propagation in 802.15.4 based wireless sensor networks. First we present a baseline worm model in the context of wireless sensor networks. Then we describe a preliminary study of the impact of various protocol parameters and network scenarios on worm propagation dynamics.

Thanassis Giannetsos, Neeli R. Prasad described the malicious code is defined as software designed to execute attacks on software systems. This work demonstrates the possibility of executing malware on wireless sensor nodes that are based on the von Neumann architecture. This is achieved by exploiting a buffer overflow vulnerability to smash the call stack, intrude a remote node over the radio channel and, eventually, completely take control of it. Then we show how the malware can be crafted to become a self-replicating worm that broadcasts itself and propagates over the network hop-by-hop, infecting all the nodes.

Wang XiaoMing[1*], HE ZaoBo[1], ZHAO XueQing[1], LIN Chuang[2], PAN Yi[3], CAI ZhiPeng[3] proposed to track the malware propagation over a time on WSN using spatial distribution behavior methodology. The malware threats propagate while users access the E-mail and instant messing through the wireless sensor network. An infected node replicates the copies of malware over the WSN. The dynamic behavior of malware propagation can be controlled by the spatial monitoring system. The simulation result showed tracking of sensor node performance, speed and packet transmission.

3. Proposed system

User can access data through communication nodes from wireless sensor network to succeed their operation. During this process, irrelevant files entered to the system without have an authorization certification. It occupied more memory space in each node in the wireless sensor system. It degraded the system performance and less capability to handle data transmission. It may affect the node density and packet data transmission. Based on the analysis, monitor the malware propagation activity over the wireless sensor nodes. The malware propagation can be controlled by two ways of behavior analysis. The tracking system of malware behavior can be filtered and mapped with behavior pattern.

The sensor nodes have efficient capability to handle the heterogeneous behavior and highly restricted for vulnerable nodes. The malware propagation is tracked from the WSN and split out the malware binaries. The malware binaries can synchronize with common behavioral prototype. Then analyze the behavior model for the malware propagation in the wireless sensor nodes. The behavior pattern is embedded to the clustered nodes. These clustered nodes are grouped as cluster using K-Means Algorithm [2]. The collection of data transmission through each sensor node has monitored their behavior activities. The homogeneous clustered nodes are easily handled the malware and its propagation. Analyze of this framework, can control the propagation of malware in WSN.

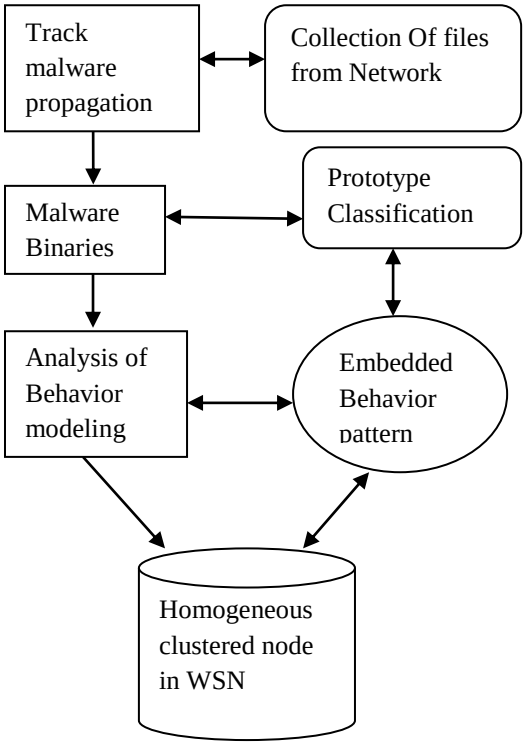

Fig1. Monitoring of homogeneous WSN

3.1. Clustering sensor nodes

Filtering the propagation activity of malware as static and dynamic behavior and it can be formed in the clustered nodes in wireless sensor network. The classification of malware binaries based on the behavior analysis of malware activity. It formed as clustered nodes based on the track of homogeneous behavior of malware.

Using K-means algorithm, cluster the malware propagated files which is in the similar behavior. Let Z be the dataset and binaries feature $U=\{u_1,u_2,u_3,..u_n\}$. The centroids A producing the cluster $x=\{x1,x2,..x_n\}$

Step 1: Let the values to M centroids a1, a2, a3…a_n, normally N random entities X←{}.
Step 2: Then assume each entity Z_i in the dataset to its closest centroid A_n, generating
the clustering node X' = {X'$_1$, X'2,…X'$_n$}
Step 3: Update all the centroids of the clustered nodes to the centre of their relevant clusters.
Step 4: If X! = X' then X← X' and also go to the step 2.
Step 5: In an Output side of the clustering nodes X= {X_1, X_2,…Xn} and the centroids of the cluster C = {C1,C2,…Cn}

The K-means algorithm repeatedly diminish the sum of the squared error over K clusters, So here its show the K-Means criterion in E

$$W(S,C) = \sum_{N=1}^{n} \sum_{j \varepsilon Xn} d(b_i, a_n) \quad ...(1)$$

Where d ($bi_,$ a_n) is the function which calculate distance between the entities and the centroids A_k. The clustering nodes in the wireless sensor network depends on the initial centroids have given to this algorithm.
The malware binaries nodes in the WSN form the homogeneous cluster.

4. Result Analysis

The dynamic behavior of malware activity is monitored by using malware behavior modeling in wireless sensor network. It can monitor the malware activity continuously. Generally malware propagation in the user system activities as follow: File infection, password brute force, energy holes and so on in the WSN. By analyze the prior research; we conclude the percentage of malware activity found in WSN during user activities.

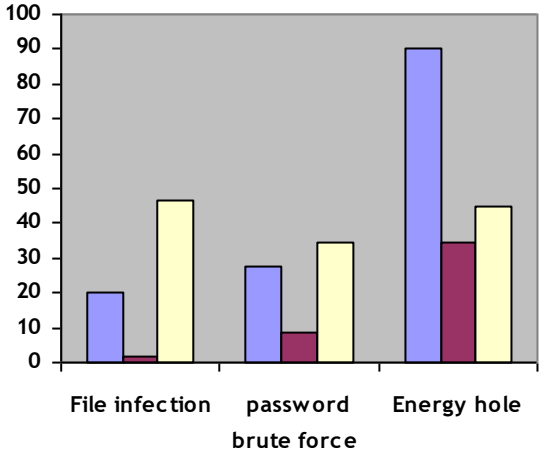

Fig.2. Simulation result of malware propagation activity.

Based on the simulation result, can known that the malware propagation has less activity to react in WSN. The fast propagation malware like conficker, welchia, gamescom and so on are difficult to eliminate from Microsoft operating system. After recognize the feasibility study, we proposed the model of dynamic behavior profile to form the clustered nodes in the WSN and can extract the highly reactive malware and their affected nodes based on behavior pattern. Then use pattern matching to filter the malware and its propagation from the wireless sensor network. Finally get free from vulnerabilities and get reliable user accessibility. So we access the behavioral profile of each malware activity.

Wireless sensor nodes are protected from malware downadue using varies prior research work are there. But even couldn't reduce malware activity in the WSN. In this paper can analyze behavior of malware activity. Then monitor the malware propagation in the sensor nodes and observe the behavior of malware binaries. The simulation result shows the comparison of prior research work with the behavior model.

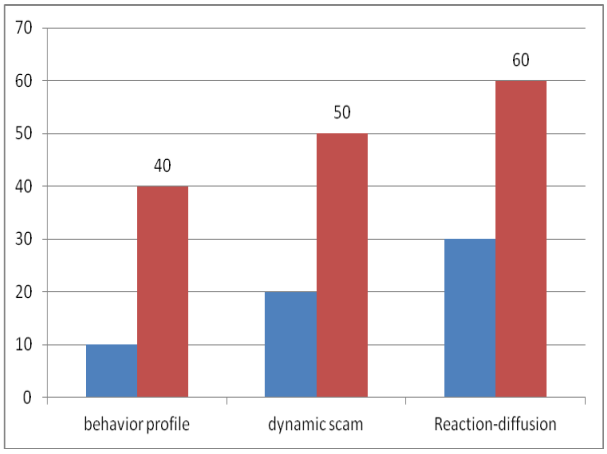

Fig 3. Efficient handling process of Malware propagation in the WSN

The above graph explain an efficient handling of malware activity in the wireless sensor network. The dynamic scam in the spatial distribution of malware found in the wireless sensor network can handle the activity of downadue. It can migrate and damage the file frequently. It has less efficient to handle the propagation knoc.

5. Conclusion

Malware propagation vector is the infect user authorised file and violate the security map. The dynamic behavior can be monitored and made it as cluster using K-means algorithm. The centroids of the cluster can map the behavioral pattern of malware

propagation in the wireless sensor network. The simulation result showed an effectiveness of the behavioral profile of malware activity. In future, to implement the behavior profile for heterogeneous malware binaries to avoid completely from the user's system.

6. REFERENCE

[1] Peng, Wei, et al. "Behavioral Malware Detection in Delay Tolerant Networks."Parallel and Distributed Systems, IEEE Transactions on 25.1 (2014)

[2] Mohaisen, Aziz, Omar Alrawi, and M. Larson. AMAL: Highfidelity, behavior-based automated malware analysis and classification. Verisign Labs, Tech. Rep, 2013

[3] A Survey Sancheng Peng ; Shui Yu ; Aimin Yang" Smartphone Malware and Its Propagation Modeling" Surveys & Tutorials, IEEE Volume: 16 , Issue: 2 DOI: 10.1109/SURV.2013.070813.00214 Publication Year: 2014 , Page(s): 925 – 941

[4] Bo Sun ; Guanhua Yan ; Yang Xiao "Worm Propagation Dynamics in Wireless Sensor Networks", 2008. ICC '08. IEEE International Conference on DOI: 10.1109/ICC.2008.298 Publication Year: 2008 , Page(s): 1541 – 1545

[5] WANG XiaoMing1*, HE ZaoBo1, ZHAO XueQing1, LIN Chuang2, PAN Yi3, CAI ZhiPeng" Reaction-diffusion modeling of malware propagation in mobile wireless sensor networks" SCIENCE CHINA Information Sciences 2013, Vol. 56 Issue: 092303(18) DOI: 10.1007/s11432-013-4977-4.

[6] F. Li, Y. Yang, and J. Wu, "CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-Based Mobile Networks," Proc.IEEE INFOCOM, 2010.