Research on IoT Security Defense Based on Honeypot Technology

Zhenxia Wang*, Linlin Yu
Dalian University of Science and Technology

Abstract: With the expansion of the Internet and the increase in the number of end users, mobile terminals are vulnerable to hackers, computer viruses and other dangerous attacks. Honeypot technology is a highly deceptive security protection technology, which can run in a variety of networks and terminal systems with characteristic vulnerabilities deliberately. Meanwhile, honeypot technology can induce intruders to launch attacks. Therefore, the source of the attack can be captured to realize security defenses, protecting important system terminals from infringement. Moreover, by inducing the intruder to attack the honeypot terminal, it can not only delay the time to attack the real target, but also timely monitor, collect and analyze the attack behavior to provide support for dealing with unknown threats. So, in order to solve the problems of traditional methods and apply honeypot technology to the process of unknown threat defense of mobile terminal, an intelligent defense method is proposed in the paper for mobile terminal unknown threats based on honeypot technology. The results of comparative experiments prove that the method proposed in the paper has less underreporting of unknown threats, and can fully detect the source information, which can meet the needs of mobile terminals for effective defense against unknown threats.

1. Introduction

The mobile terminal is the main presentation device for Internet content. In recent years, the rapid development of mobile terminals has made people’s lives more closely linked with mobile terminals [1]. However, due to the disadvantages of mobile terminals such as poor storage capacity and wide and complex network resources, their defense against unknown threats is weak [2]. Therefore, the study of an unknown threat defense method suitable for mobile terminals has become one of the problems that need to be solved urgently, and relevant experts and scholars have also conducted a lot of research on it.

Literature [3] designed a big data mobile terminal network information security defense method, which combines the autoregressive model and mutation operator to build the mobile terminal information autoregressive model, use the least squares method to estimate the regression coefficient, then detect the statistics of the mobile terminal information through the sliding window, calculate the value range, and defend the information outside the range. However, this method has a relatively small inspection range for external information from the mobile terminal, resulting in a low information retrieval rate. Besides, literature [4] proposed an advanced persistent threat detection and defense method for mobile terminals based on machine learning. The static detection method is used to extract the static characteristics of the mobile terminal, and the sliding window iterative algorithm is applied to capture the delayed attack characteristics. Meanwhile, boost technology will integrate multiple
classification algorithms to detect delayed attacks and implement security defenses based on the
detection results. However, this method has poor ability to capture unknown threats, leading to a high
rate of underreporting unknown threats.

Traditional mobile terminal unknown threat defense methods often fail to report, so an intelligent
defense method is proposed in the paper for mobile terminal unknown threats based on honeypot
technology to improve the defense capability of mobile terminal unknown threat intelligent defense.

2. Setting of Intrusion Detection Rules

Before performing intelligent defense against unknown threats on mobile terminals, it is necessary to
extract intrusion rules for unknown threats on mobile terminals.

Honeypot technology is first used to collect unknown threat information on mobile terminals. Since the existing honeypot technology is difficult to distinguish the types of extracted data in detail, an unsupervised clustering algorithm is applied to classify the collected data. If the intrusion behavior recorded by the honeypot is significantly different from the normal behavior, the data attribute \[b\] will be calculated and distinguished from other data. The calculation process is:

\[D = \frac{b}{F \times \varnothing}\]  

In formula (1), \(D\) represents the basic data of the unknown threat on the mobile terminal, and \(F\) refers to the data characteristic information. \(\varnothing\) is the data attribute distinguishing factor, and \(b\) is the temptation beacon of honeypot technology.

In this process, the purpose of using honeypot technology is to attract threat information into the
system in order to record the invasion process. When the intrusion behavior data is greater than the
number of normal behaviors, sort them according to how much data all the classes contain \[\text{(6)}\], and set
the proportion number. Then mark the data, and setting basis of the proportion number is:

\[G = \frac{A}{n \times g}\]  

In formula (2), \(G\) represents the proportion of mobile terminal data, and \(n\) indicates the
number of intrusion data. \(g\) is the malicious information attack potential, and \(A\) is the data ranking
factor.

Complete the setting of the proportion number according to the above process. When \(G \geq 1\), mark
the data as normal. On the contrary, when \(G \leq 1\), mark it as intrusive.

Through the above calculation, the establishment of the mobile terminal unknown threat intrusion
detection rule is completed, which provides a basis for the mobile terminal's intelligent defense against
unknown threats.

3. The Mapping of Threat Invasion Path

Based on the above-mentioned intrusion detection rules, the threat path is drawn. Among the unknown
threats of mobile terminals, threat information generally launches attacks on objects with weaknesses,
and the occurrence of threat behaviors has a certain degree of continuity \[\text{(7)}\]. Therefore, aggregate threat
information to form new threat report information, and draw threat paths based on the threat report
information. The threat path drawing steps are as follows:

step1: Aggregate threat behavior report set, and the time interval is set to threshold \(T\);
step2: Form an initial temporary queue to store threat behavior reports during the aggregation
process \[\text{(8)}\];
step3: Check whether the threat behavior report received by the server meets the threat generation
path;
step4: If no new mergeable threat report is received within time \(T\), the aggregated threat behavior
report will be output.

According to the above process, the threat path is drawn, and malicious nodes are discovered
according to the threat path. The process is as follows:

\[ S_i = \frac{\nu}{\sum_{j=1}^{\nu} g_j} \quad (3) \]

In formula (3), \( S_i \) represents the set of the number of reports submitted by nodes, and \( \nu \) refers to the threshold of malicious nodes. \( \sum_{j=1}^{\nu} g_j \) indicates the credibility of the nodes, and \( i \) is the number of nodes.

According to the above process, malicious nodes are distinguished, and interference of such reports is eliminated, so that the mobile terminal's unknown threat defense can prioritize valuable threat behaviors, thereby completing the mapping of the threat path.

### 4. Defense against Unknown Threats on Mobile Terminals

Based on the above-mentioned setting of intrusion detection rules and drawing of threat paths, intelligent defense is performed against unknown threats of mobile terminals. With the help of the honeypot technology, an intelligent defense model for unknown threats is established. The logical structure of the model is shown in Figure 1.

![Logical structure diagram of the unknown threat intelligent defense model](image)

In order to integrate the early warning effect of honeypot technology, the detection algorithm of threat degree is planned by the matching degree of threat characteristic information and intrusion rules. First, input the attribute string of the captured information feature mode, and use the following formula to output the early warning judgment result \([9-10]\). The calculation formula is as follows:

\[ F = k \times \frac{x}{l \times H} \quad (4) \]

In formula (4), \( F \) represents the information characteristic mode, \( k \) is the matching count variable, and \( l \) refers to each attribute string. \( H \) is the interval boundary threshold, and \( x \) represents the alarm information in control center.

According to the above formula, the early warning effect of the mobile terminal’s unknown threat intelligent defense model is improved. On this basis, in order to improve the security performance of the model, the concept of time is introduced \([11]\), and the model is updated to:

\[ F' = (r + m) \cdot Ft \quad (5) \]

In formula (5), \( t \) represents the protection time set by the protection security target, \( r \) refers to the time it takes to detect the attack, and \( m \) is the response time of the model after the attack is
discovered.

Under the guidance of the core module of the time concept, a security defense model is constructed through protection, detection and corresponding A. Then, honeypot technology is applied to capture the attack source, and the capture process can be described as:

$$ J = F \times \left( \frac{I \times \alpha (q + j)}{s} \right) $$

(6)

In formula (6), $I$ represents a finite state set, $q$ indicates a finite input, and $j$ is a transfer function. $s$ represents the initial state of the model, and $\alpha$ is a threat information capture factor.

According to the mobile terminal's intelligent defense requirements against unknown threats, the state of constructing an intelligent defense model based on honeypot technology is:

$$ W = (d_1 + d_2 + d_3 + d_4 + d_5) N $$

(7)

In formula (7), $d_1$ represents the initial state of the unknown threat intelligent defense model. If the mobile terminal is detected to be attacked, the defense model will switch to the $d_2$ state, and the unknown threat model will be directed and redirected. If the targeting is completed, it will be changed to $d_3$. If the targeting is not completed, then maintain current status and report status. Moreover, $d_3$ represents the status of model log recording. After the recording is completed, it will be converted to $d_4$. If the recording is not completed, the recording will continue. $d_4$ indicates the above process of extracting intrusion rules. If the extraction is completed, it will be converted to $d_5$. If not, the original state will be maintained. $d_5$ represents the above-mentioned threat path drawing state. If the attack information is recognized, the unknown attack information will be added to the $d_1$ state, and if the attack information is not recognized, the process will be repeated. $N$ refers to the technical state of the mobile terminal’s unknown threat intelligent defense model based on honeypot technology [12]. The conversion relationship of the mobile terminal’s unknown threat intelligent defense model based on honeypot technology is shown in the following figure:

![Figure 2. Schematic diagram of the conversion relationship of the unknown threat intelligent defense model](image)

In the actual use of this model, the honeypot technology is used to chase the attack source when in the $d_2$ state, and at the same time the honeypot technology is used to capture the attack source and record the attack tool and attack method in the $d_3$ state, so that the intelligent defense against unknown threats on mobile terminals based on honeypot technology can be completed. This model can not only effectively protect and transfer the attack source and target to mobile terminals, but also efficiently obtain attack information.
5. Experimental Comparison and Analysis

5.1 Experimental Method Design
In order to verify the effectiveness of the mobile terminal's intelligent defense method against unknown threats based on honeypot technology, an experimental comparison is made, which compares the performance of the big data mobile terminal network information security defense method in literature [3] and the advanced persistent threat detection and defense method of mobile terminal based on machine learning in literature [4] with the method proposed in this research. In addition, it mainly compares the number of underreporting unknown threats and the recall rate of external information in three terminal unknown threat defense methods. Among them, the number of unreported unknown threats can judge the detection capabilities of different methods against unknown threats, and the recall of external information can judge the comprehensiveness of different methods when detecting external information. The calculation process is as follows:

\[
\text{Recall ratio} = \frac{\text{The amount of foreign information detected}}{\text{Total external information}} \times 100\% \tag{8}
\]

5.2 Experimental Environment Preparation
The experimental environment is deployed in the minefield mode, and the minefield is deployed through several virtual hosts. The test environment is shown in Figure 2.

![Figure 3 Schematic diagram of the experimental environment](image)

The experimental operating system is Windows server 2003, the WEB server support is Internet Information server 6.0, and the background database supports Microsoft SQL Sever2005. Then, simulate the network deception environment. Therefore, it is necessary to simulate the network service, so that the host in the deception environment can be similar to the host in the real environment, which is achieved by using virtual reality technology. Moreover, virtual machine technology is applied to build a virtual hardware platform, and provide application operating environment technology through the platform, making the experiment more authentic.

Meanwhile, it is necessary to deploy a virtual honeypot in the experiment to scan and detect the current experimental environment and attack the preset target host. Select 10 Trojans, 10 worms, 10 viruses and 10 normal programs from the experimental host as sample programs, and use polymorphic tools to process the sample programs to obtain 130 programs, including 30 malicious programs and 60 Attack data and 40 virus data. Then, import these attack data into the above-mentioned attack host, and after successful import, the defense situation of different defense methods will be recorded in real time.
5.3 Analysis of Results
Calculating and analyzing the number of underreporting unknown threats with different defense methods, the results are shown in Table 1.

Table 1 Comparison of the number of underreported unknown threats by different methods (pieces)

| Threat object | Total/a | Literature [3] method | Literature [4] method | Method proposed in this study |
|---------------|---------|------------------------|------------------------|-------------------------------|
| Malicious program | 30      | 6                      | 5                      | 2                             |
| Attack data   | 60      | 7                      | 11                     | 3                             |
| Virus data    | 40      | 9                      | 8                      | 1                             |

Analyzing the results in Table 1, it can be seen that in the three aspects of malicious program defense, attack data defense, and virus data defense, the number of underreporting unknown threats calculated by the methods proposed in literature [3] and literature [4] is higher than the method proposed in the paper, which proves that the mobile terminal unknown threat intelligent defense method based on honeypot technology has a strong ability to detect unknown threats and can effectively recognize unknown threats.

To further verify the ability of different methods in the comprehensiveness of external detection, the experimental results are shown in Figure 4.

![Figure 4. Comparison of recall rates of external information in different methods](image)

Analyzing Figure 4, it can be seen that in the continuous iteration, only the mobile terminal unknown threat intelligent defense method based on honeypot technology which is proposed in the paper has a slow increase in the recall rate of external information, while methods proposed in literature [3] and literature [4] have irregular changes in the recall rate of external information. Meanwhile, they are all lower than the method proposed in the paper. Therefore, it can be explained that the mobile terminal unknown threat intelligent defense method based on honeypot technology can comprehensively detect external information.

Therefore, through the above experiments, it can be proved that the mobile terminal unknown threat intelligent defense method based on honeypot technology which is designed in the paper has a better defense effect than traditional defense methods, which can effectively ensure the security of mobile smart terminals.

6. Conclusion
With the expansion of the Internet and the increase in the number of end users, mobile terminals are vulnerable to hackers, computer viruses and other dangerous attacks. Traditional mobile terminal unknown threat defense methods often fail to report, so an intelligent defense method is proposed in
the paper for mobile terminal unknown threats based on honeypot technology to improve the defense capability of mobile terminal unknown threat intelligent defense. First, honeypot technology is used to collect unknown threat information on mobile terminals, and then unknown threat intrusion detection rules are set to draw the threat path. Finally, honeypot technology is combined to establish an intelligent defense model for unknown threats on mobile terminals. The experimental comparison results show that the method proposed in the paper has fewer underreports of unknown threats than traditional methods, and the detection of external information is more comprehensive.

However, when using the method proposed in the paper to conduct intelligent defense against unknown threats on mobile terminals, the entire information search process takes a long time, which reduces the defense efficiency of the method proposed in the paper to a certain extent. Therefore, in the future research phase, the method proposed in the paper will be further optimized to further improve the efficiency of defense against unknown threats.

References
[1] Wang Wei, Wang Jiajun, Wang Mingming, et al. Flooding attack defense technology for mobile ad hoc networks centered on network performance [J]. Computer Science, 2017(1): 159-166.
[2] He Yao, Huang Hai. Research on enhancing the security of IoT terminals based on non-IP+SCEF technology[J]. Telecommunications Science, 2017, 33(2):36-41.
[3] Li Longsen, Lian Yuzhu. Big data mobile terminal network information security transmission simulation[J]. Computer Simulation, 2018, 35(6):188-192.
[4] Hu Bin, Wang Chundong, Hu Siqi, et al. Research on advanced persistent threat detection technology for mobile terminals based on machine learning[J]. Computer Engineering, 2017, 43(1):241-246.
[5] Shi Leyi, Li Yang, Ma Mengfei. New progress in honeypot technology research[J]. Journal of Electronics & Information Technology, 2019, 41(02):249-259.
[6] Liu Wei, Tian Jue, Wang Jiazhou, et al. Research on Comprehensive Security Threats and Defense of Cyber-Physical Fusion System[J]. Acta Automatica Sinica, 2019, 45(01):7-26.
[7] Zhang Baoquan, Zhou Feng, Huang Zuyuan. Research on DDoS Attack Defense Based on Honeypot Technology[J]. Software, 2017, 38(6):32-37.
[8] Ji Wei, Li Bingxing, Zheng Baoyu. Distributed intelligent intrusion prevention scheme based on reputation and consensus[J]. Systems Engineering and Electronic Technology, 2018, 40(3):665-670.
[9] Fan Linna, Ma Yufeng, Huang He, et al. Research review of mobile target defense technology[J]. Journal of China Academy of Electronics, 2017, 12(2):209-214.
[10] Yin Wei, Zhou Hongjian, Xing Guoqiang. Application of honeypot encryption technology in private data protection[J]. Computer Applications, 2017, 37(12):3406-3411.
[11] Lin Yuxiang, Wang Huiting. Defense method based on dynamic changes of user address[J]. Computer Engineering and Design, 2018,39(08):25-29.
[12] Cai Chuanxi, Mei Shue, Zhong Weijun. Game Analysis of Optimal Allocation Strategy of Mimic Honeypot Deception Mechanism[J]. Chinese Journal of Management Engineering, 2018, 32(04): 115-122.