Dynamic Defense Architecture for the Security of the Internet of Things

Caiming Liu[1, 2], Yan Zhang [1, *], Zhonghua Li[1, 2],
Jiandong Zhang[1, 2], Hongying Qin[1, 2]
[1] School of Computer Science
Leshan Normal University
Leshan, China
[2] Key Lab of Internet Natural Language Processing of
Sichuan Provincial Education Department
Leshan Normal University
Leshan, China
[*]: Corresponding Author, zhangyan_201016@163.com

Jinquan Zeng
School of Computer Science and Engineering
University of Electronic Science and Technology
of China
Chengdu, China

***Abstract*—The security situation of the Internet of Things (IoT) is constantly changing. Traditional passive management strategies for IoT can not adapt to the complicated environment of IoT. To solve the above problem, a dynamic defense architecture for the security of IoT is proposed. It is made up of six security defense segments which include active defense, threat detection, security warning, security response, security recovery and defense assessment. The whole procedure of security defense repeats all along. The next segment provides supplements to the previous segment. IoT security threats are dealt with dynamically. According to operation results of all defense segments, the security situation of IoT is assessed, and then defense strategies for IoT are updated to make the proposed architecture adapt to the IoT environment.**

Keywords- Security of the Internet of Things; Security Defense Architecture; Security Threat; Security Defense Strategy; Defense Assessment Strategy

I. INTRODUCTION

The Internet of Things (IoT) developed rapidly[1]. It has been applied to every corner of the society. Its security problems will certainly affect all aspects of the humankind[2]. To protect IoT, existing security management methods for IoT use static security defense strategies and deploy security technologies to IoT nodes. It's a traditional security defense solution for IoT. However, along with the spreading of IoT applications, the security environment of IoT maybe changes constantly. Absolutely safe IoT doesn't exist. Only static security defense strategies and security technologies for IoT are difficult to adapt to the security situation of IoT. A theoretical model which can fit the change of the IoT environment and scientifically handle security threats against IoT is urgently needed to defend IoT[3].

IoT has a specific logic architecture[4,5]. It contains massive sense nodes and has the attributes of heterogeneity of networks, dispersity of sense nodes, uncertainty of distribution, etc. The above features make that some special vulnerabilities maybe exist in IoT[6]. It causes that traditional network security architectures[7] can not be directly used to guarantee the security of IoT. According to the logic architecture of IoT, researchers combined traditional network security technologies with IoT security and presented some theoretical models for IoT security. Falk et al [8] proposed a security architecture for multi-hop sensor networks. Their proposed architecture is designed to be used in the industrial environment. It provides IEEE 802.15.4 frame protection for hop-to-hop communication, a security manager who is used to authenticate a joining node and to establish required session keys and end-to-end protection. Sun et al [9] proposed a security framework for IoT based on 3G access and developed an achieved IoT safety demonstration system based on the 3G. Mirowski et al [10] presented an intrusion detection method for IoT according to the past access frequency of things' tags. Their method provides a complementary security defense way for the passive defense of IoT.

The security models which are mentioned in above references for IoT ensure the security of IoT to a certain ex-tent. However, they just apply some IoT security technologies to passive IoT security defense strategies. They lack dynamic feature of security defense. It causes that they do not satisfy the request of frequent change of the IoT security environment. To solve the above problem, a Dynamic Defense Architecture (DDA) for the security of IoT is proposed in this paper to realize a series of dynamic defense procedures which include active defense, threat detection, security warning, security response, security recovery and defense assessment.

In the following, in section II, dynamic defense architecture for IoT is introduced. In section III, the merits of the proposed architecture are discussed. Section IV concludes this paper.

II. THE FRAMEWORK OF DYNAMIC DEFENSE ARCHITECTURE

A. General Framework

The general framework of DDA is shown in Figure 1. The whole security defense architecture is made up of six security defense segments which include active defense, threat detection, security warning, security response, security recovery and defense assessment. The next segment provides supplements of

978-1-4673-8660-9/15 $31.00 © 2015 IEEE
DOI 10.1109/CIS.2015.100

security defense to the previous segment. Finally, the segment of defense assessment forms IoT security defense strategies which adapt to the IoT security environment.

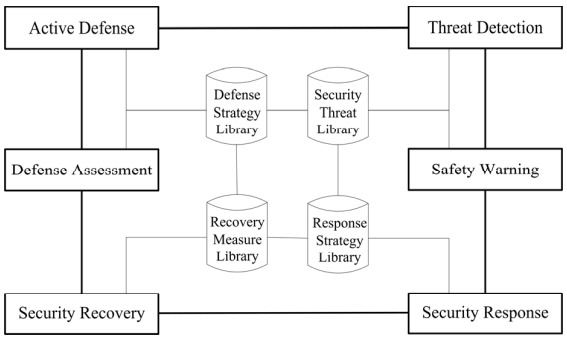

Figure 1. The General Framework of DDA.

According to the defense strategy library, the segment of active defense deploys security defense measures, recognize and handle security threats against IoT. According to the security threat library, the segment of threat detection detects security threats confronted by IoT. It detects mutated and new security threats especially. The segment of security warning adopts appropriate methods to send warning information about the detected IoT security threats. According to the response strategy library, the segment of security response responds to the detected security threats in time. It prevents or reduces the damage to IoT as far as possible. According to the recovery measure library, the segment of security recovery restores the damaged parts of IoT to the state of normal working. The segment of defense assessment analyzes security threats and their affect, reformulates inappropriate security defense strategies, and formulates new security defense strategies.

B. Active Defense

The segment of active defense is the primary part of the defense architecture for IoT security. It confronts security threats directly and prevents damages to IoT. In the proposed architecture, according to the respective security requests of sense layer, transport layer, processing layer and application layer, the security strategies such as encryption mechanism, access control, authentication mechanism, backup mechanism, etc, are deployed to IoT nodes. They deal with the security threats which can be recognized by them. However, along with the promotion of security threat technologies against IoT, active defense can not recognize all security threats. The unknown security threats are detected by the segment of threat detection. Meanwhile, on the basis of the aftereffects caused by security threats, the segment of defense assessment dynamically adjusts the security defense strategies to make DDA be appropriate to the change of the IoT environment. In other words, active defense is not changeless but dynamic.

To improve the dynamic nature of active defense, the extendible defense strategy library (DSL) is set up. In the beginning of DDA, DSL contains IoT security defense strategies which are made up of classical security services, mechanisms, plans, etc. Let the dataset of the defense strategy library be *DSL* which is shown in Eq.(1).

$$DSL = \langle \{ dID, name, mechanism, layer, service, sID, description \rangle \} \quad (1)$$

where, *dID* is the serial number of a security defense strategy, *name* is its name, *mechanism* is the security mechanism adopted by it, *layer* is the IoT layer to be defended, *service* is the IoT service to be defended, *sID* is the serial number of the security threat to be handled by the proposed model, *description* is the description information of the security defense strategy.

There are a limited number of defense strategies in *DSL*. Defense strategies are deployed to relative key nodes in IoT to satisfy the requests of every IoT layer. They change to deal with security threats according to the changes of the IoT security environment. Let the deployment operation of defense strategies be *Deploy*() which is shown in Eq. (2).

$$Deploy(DSL) = \begin{cases} NewDSL(d, layer, service), t = 0 \\ Update(d, layer, service) + \\ \quad NewDSL(d', layer, service), t > 0 \end{cases} \quad (2)$$

where, *NewDSL*() is the operation to install new security defense strategies, *Update*() is the operation to update old security defense strategies, $d, d' \in DSL$, d' is a new security defense strategy.

The segment of active defense can handle most security threats with the IoT security technologies in defense strategies. However, the security environment of IoT changes constantly. The threat technologies threatening IoT security always develop. Perfect security technologies for IoT can not recognize and deal with all security threats. The threats which can not be handled are left to the subsequent segments which make up for the damage and finally generate new defense strategies.

C. Threat Detection

The segment of threat detection detects security threats confronted by all IoT layers. These threats include physical damages, attacks, malicious codes, vulnerabilities, misuses, etc. The detection technologies adopt rule-based threat detection to recognize classical threats. Machine learning and intelligent analysis can also be applied to threat detection to adapt to the IoT security environment and discover new security threats against IoT. It is especially important to update the defense strategy library dynamically and improve the ability of threat detection.

The signatures of known security threats against IoT are used to construct the security threat library. Let the dataset of the security threat library be *STL* which is shown in Eq. (3).

$$STL = \{ \langle sID, name, layer, service, description \rangle \} \quad (3)$$

where, *sID* is the serial number of a security threat, *name* is the security threat's name, *layer* and *service* are respectively the IoT logic layer and service type which are threatened by the security threat, *description* is the description information of the security threat.

The security threat library is a dynamical library. Let the security threat library at the moment t be $STL(t)$ which is shown in Eq. (4).

$$STL(t)=\begin{cases}\{s_0,s_1,\cdots,s_n\},n\in N & t=0\\ STL(t-1)\cup STL_{new}(t) & t>0\end{cases} \tag{4}$$

where, $\{s_0,s_1,\cdots,s_n\}$ is the dataset which is collected in the beginning, N is the dataset of nature number, $STL_{new}(t)$ is the dataset of new security threats detected by threat detection technologies at the moment t, which is shown in Eq. (5).

$$STL_{new}(t)=\{s\,|\,\forall s\in Detect(t,layer,\\ ,service)\wedge s\notin STL(t-1)\} \tag{5}$$

where, *Detect*() is a method to detect security threats confronted by a specific IoT layer and service at the moment t. If the detected threats are not in *STL*, they are new. They need to be put into *STL* with Eq. (4).

The IoT security threats detected by the segment of threat detection is the basis of the next segments in DDA. After they being detected, security warning begins to work.

D. Security Warning

The segment of security warning is initiated to notice managers that security threats are detected. Common measures for security warning include logging, sending email, sending system messages, sending SMS to cell phones, voice notification, etc.

Let the dataset of security warning be W which is shown in (6).

$$W=\{\langle t,sID,frequency\rangle\} \tag{6}$$

where, t is the moment when the security threat happens, *sID* is the serial number of the detected threat, *frequency* is the frequency of occurrence of the detected threat.

When IoT security threats being detected by the threat detection, the security warning immediately updates the security warning information, which is shown in (7).

$$W(t)=\begin{cases}\phi, & t=0\\ \{w\,|\,w.t=s.t,w.sID=s.ID\wedge\forall s\in\\ \quad Detect(t,layer,service)\}, & t>0\end{cases} \tag{7}$$

Let the operation of security warning be *Warn*(). The processing procedure of security warning is shown in (8).

$$Warn(t)=\{\langle warning,type\rangle\,|\,warning=\\ Copy(W(t)),type=warning.frequency\} \tag{8}$$

where, *warning* is the message content of security warning, *Copy*() is the operation to form the message according to the dataset of security warning, *type* is the way to warn.

E. Threat Detection

After an IoT security event happens, some specific measures should be conducted to respond to it. This task is carried out by the segment of security response. The security events come from the segment of active defense or threat detection. How the segment of security response responds to security events is based on the recognized or detected security threats and their harmfulness.

The response strategy library is set up. Let the dataset of the response strategy library be *RSL* which is show in Eq. (9).

$$RSL=\{\langle rID,name,person,tool,measure,\\ sID,layer,service,description\rangle\} \tag{9}$$

where, *rID* is the serial number of a security response strategy, *name* is its name, *person* is the relative staff who settles the security threat event, *tool* represents the software or hardware tools which are adopted, *measure* represents processing methods, *sID* is the serial number of the corresponding security threat, *layer* and *service* are respectively the IoT logic layer and service type which are responded to, *description* is the description information of the security response strategy.

When new security threats against IoT are detected, new security response strategies are supplemented to prevent new security threats' damages. *RSL* is a dynamic dataset to deal with mutated and new security response strategies. Let *RSL* at the moment t be $RSL(t)$ which is shown in Eq. (10).

$$RSL(t)=\begin{cases}\{r_0,r_1,\cdots,r_n\},n\in N & t=0\\ RSL(t-1)\cup RSL_{new}(t) & t>0\end{cases} \tag{10}$$

where, $\{r_0,r_1,\cdots,r_n\}$ is the security response dataset in the beginning of the proposed architecture, which comes from typical security threats, $RSL_{new}(t)$ is the dataset of new security response strategies which are against new threats, which is shown in Eq. (11).

$$RSL_{new}(t)=\{r\,|\,r=InitR(s)\wedge\forall s\in STL_{new}(t)\} \tag{11}$$

where, *InitR*() is the operation to set up new security response strategies according to new IoT security threats.

F. Security Recovery

In the segment of security response, appropriate response strategies respond to the threats. However, they can not fix the damaged system if threats harm IoT. In the proposed architecture, the segment of security recovery is designed to fix the damaged system.

The segment of security recovery aims to restore the damaged parts of IoT to the state of normal working. The corresponding operation of security recover is based on the detected threats, the influence of the detected threats, the results of security response.

The recovery measure library is set up. Let the dataset of the recovery measure library be *RML* which is shown in Eq. (12).

$$RML=\{\langle rmID,name,tool,measure,sID,\\ rID,layer,service,description\rangle\} \tag{12}$$

where, *rmID* is the serial number of a security recovery measure, *name* is its name, *tool* represents the software or hardware tools which are used for recovery, *measure* represents

specific measures for recovery, *sID* is the serial number of the corresponding threat which causes damage to IoT, *rID* is the serial number of the corresponding security response strategy, *layer* and *service* are respectively the IoT logic layer and service type which are restored, *description* is the description information of the security recovery measure.

The recovery measure library also has dynamic nature. It is updated according to the change or generation of threats and response strategies.

G. Defense Assessment

Through analyzing the results of the segments of threat detection, security warning, security response and security recovery, the influence brought by security threats against IoT can be estimated. Security threats maybe do no harm to IoT. They also maybe cause slight damage, severe damage or destruction. It indicates that there are vulnerabilities in the active defense system for IoT security. Therefore, the defense strategy library needs to be updated.

The segment of defense assessment aims to reformulates inappropriate security defense strategies and formulates new security defense strategies. The detected threats and their influence are analyzed in this segment. Furthermore, the defense strategy library is updated and can be used to defend mutated and new security threats.

Let the dataset of the defense strategy library at the moment t be $DSL(t)$ which is shown in Eq. (13).

$$DSL(t)=\begin{cases}\{d_0,d_1,\cdots,d_n\},n\in N & t=0\\ Update\big(DSL(t-1)\big)\cup DSL_{new}(t) & t>0\end{cases} \tag{13}$$

where, *Update*() is the operation to update the old defense strategy library, which is shown in Eq. (14), DSL_{new}() is the operation to generate new security defense strategies, which is shown in Eq. (15).

$$\begin{aligned}&Update\big(DSL(t-1)\big)=\big\{d\,\big|\,d.sID=d'.sID\\&\wedge d'\in DSL(t-1)\wedge d'.sID=s.sID\wedge s\in\\&Detect\big(t-1,layer,service\big),d=Modify\big(d',\\&Evaluate_{warning}(s),Evaluate_{response}(s),\\&Evaluate_{recovery}(s)\big)\big\}\end{aligned} \tag{14}$$

where, $DSL(t\text{-}1)$ is the old defense strategy library. The operation of *Update*() updates security defense strategies according to effects of security warning, security response and security recovery. *Evaluate*() is the operation to evaluate the effects of security warning, security response and security recovery.

$$DSL_{new}(t)=\big\{d\,\big|\,d=Generate(s)\wedge\forall s\in STL_{new}(t)\big\} \tag{15}$$

where, *Generate*() is the operation to formulate new security defense strategies according to the detected security threats.

III. Conclusion

Along with the rapid expansion of IoT applications, IoT confronts more and more complicated security threats. The static defense technologies which IoT has reliance on can handle security threats to an extent in the past period of time. However, this kind of passive management strategy is not able to adapt to the IoT security environment and is difficult to handle changeful security threats. The dynamic defense architecture for IoT security proposed in this paper is separated into six dynamic and circular defense segments. The segment of active defense is not the only method to defend IoT security. All the defense segments are associated. The result data which come from all segments are used to update security defense strategies. It causes that the defense measures against security threats are active and the whole defense procedure is dynamic.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (No. 61103249), the Applied Basic Research Plans of Sichuan Province (No. 2015JY0105, 2014JY0140 and 2014JY0036), the Open Fund of Artificial Intelligence Key Laboratory of Sichuan Province (No. 2013RZJ03 and 2013RYJ04), the Scientific Research Fund of Sichuan Provincial Education Department (No. 15ZA0274, 14ZA0238, 14ZB0252 and 13TD0014), the 863 High Tech Project of China (No. 2013AA01A213), the Scientific Research Project of Leshan Normal University (No. Z1415 and Z1412) and the Leshan Science and Technology Plan (No. 13GZD051).

References

[1] A. Luigi, I. Antonio, M. Giacomo, "The Internet of Things: A survey," Computer Networks, 2010, vol. 54, pp. 2787–2805.

[2] M. T. Dlamini, M. M. Eloff, J. H. P. Eloff, "Internet of things: emerging and future scenarios from an information security perspective," Proc. of Southern Africa Telecommunication Networks and Applications Conference, August, 2009.

[3] A. Mitrokotsa, M. R. Rieback, A. S. Tanenbaum, "Classifying RFID attacks and defenses," Inf. Syst. Front, vol. 12, pp. 491–505, 2010.

[4] M. Wu, T. L. Lu, F. Y. Ling, L. Sun, H. Y. Du, "Research on the architecture of Internet of things," 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), 20-22 Aug. 2010, pp. V5-484–V5-487.

[5] J. Gubbia, R. Buyyab, S. Marusica, M. Palaniswamia, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, pp. 1645–1660, 2013.

[6] T. Kavitha, D. Sridharan, "Security Vulnerabilities In Wireless Sensor Networks: A Survey," Journal of Information Assurance and Security, pp. 31–44, 2010.

[7] S. Cheng, Z. L. Yin, "Model of Network Security based on Immune Agents," Computer Engineering and Design, vol. 24, pp. 30–32, 2003.

[8] R. Falk, H. J. Hof, "Industrial Sensor Network Security Architecture," Proc. of 2010 Fourth International Conference on Emerging Security Information Systems and Technologies, Venice, TBD, Italy, 18-25 July 2010, pp. 97–102.

[9] Y. Y. Sun, Z. H. Liu, Q. Li, L. M. Sun, "A Security Framework for Internet of Things Based on 3G Access," Journal of Computer Research and Development, vol. 47, pp. 327–332, 2010.

[10] L. Mirowski, J. Hartnett, "Deckard: A system to detect change of RFID tag ownership," International Journal of Computer Science and Network Security, vol. 7, pp. 89–98, 2007.