Dynamically enabled defense effectiveness evaluation of a home Internet based on vulnerability analysis and attack layer measurement

Min Lei^{1,2,3} · Yu Yang^{1,2} · Nan Ma^{1,2} · Huizhong Sun^{1,2} · Chunru Zhou^{1,2} · Minyao Ma⁴

Received: 29 July 2017 / Accepted: 19 October 2017 / Published online: 2 November 2017
© The Author(s) 2017. This article is an open access publication

Abstract Smart devices in a home Internet, such as routers and cameras, suffer malicious attacks from hackers on a daily basis. Defenders should change system states dynamically to improve the system's defense ability. To quantify evaluation of defense effectiveness, this paper proposes an improved vulnerability scoring method for home Internets based on the Information Security Technology Security Vulnerability Classification Guide, which calculates a vulnerability score. A higher vulnerability score indicates weaker defense ability. This method only considers defense. In actual system attack and defense, the actions of attackers should also be considered. Therefore, a measurement method for the attack layer based on the Markov chain (MC) is proposed. This method builds a model of an attack layer that can assess whether the defender's dynamic defense is effective by calculating the factor attack layer detection probability P_d . To optimize computing process, this paper introduces stochastic Petri nets (SPN) so that the parameters of MC transition matrix are easily gained. This model also obtains the minimum time period Δt , during which the defender must change system states. If the change time period is greater than Δt , attackers increase their probability of hacking into the home Internet system.

Finally, the study concludes that if the vulnerability scores are lower after the system states are changed, Δt will become longer, meaning the home Internet system has enhanced defense ability.

Keywords Home Internet · Dynamically enabled defense · Vulnerability score · Markov chain · Attack layer

1 Introduction

With the rapid development of the home Internet, a large number of smart terminals access the Internet via routers located at home [1]. Smart devices in a home Internet, such as routers and cameras, have suffered social engineering attack and other malicious attacks from hackers everyday. Attackers use various social engineering attacks to get home Internet router username and password, such as e-mail and phishing attacks, and then attack all kinds of home Internet smart terminals, causing enormous losses. Currently, the data of home Internet stored in the cloud services exists many security problems with the rapid development of cloud

✉ Min Lei
leimin@bupt.edu.cn

Yu Yang
yangyu@bupt.edu.cn

Nan Ma
manan2012@bupt.edu.cn

Huizhong Sun
sunhuizhong@bupt.edu.cn

Chunru Zhou
zcr214@bupt.edu.cn

Minyao Ma
minyaoma2006@163.com

¹ Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China

² Guizhou Provincial Key Laboratory of Public Big Data, Guizhou University, Guiyang, Guizhou 550025, China

³ Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing 210044, China

⁴ School of Mathematics and Computer Science, Guizhou Education University, Guiyang 550018, China

computing. Researchers have proposed many solutions for cloud data storage. For example, Jian Shen et al. [2] proposed a security audit protocol to solve the problem of data security storage in cloud services. Yan Kong et al. [3] proposed a decentralized belief propagation-based method called PD-LBP to improve the efficiency of accessing the encrypted data of home Internet on the cloud. A “Greedy Depth-first Search” algorithm was proposed by Zhihua Xia et al. [4] to provide efficient multi-keyword ranked search. Dengzhi Liu et al. [5] proposed a framework for urban data sharing by exploiting the attribute-based cryptography. LiZhi Xiong et al. [6] proposed a novel reversible data hiding (RDH) scheme for encrypted digital images using integer wavelet transform, histogram shifting, and orthogonal decomposition. Jian Shen et al. [7] proposed an efficient multi-layer authentication protocol and a secure session key generation method for WBANs. To enhance the security defense ability of a home Internet, many researchers proposed dynamically enabled technology which changes system states dynamically. This paper attempts to evaluate the effectiveness of dynamically enabled technology based on vulnerability analysis and attack layer measurement.

2 Related work

2.1 Home Internet

A home Internet comprises a TV, a refrigerator, air conditioning, and other smart appliances based on the home environment [8]. It has responsibility for the interconnection and intelligent cooperation among these smart appliances.

A home Internet is composed of smart terminals, communication networks, clouds, and controller APPs. The framework of a home Internet system is shown in Fig. 1.

As Fig. 1 shows, equipment such as a TV, refrigerator, and camera acts as a service provider in a home Internet. The router is an important piece of equipment that manages network layer connectivity between a WAN and the LAN. Controller APPs control the equipment through the cloud.

2.2 Vulnerability in a home Internet

A home Internet system contains four attack layers, including smart terminals, communication networks, controller APPs, and clouds. Each input point in a home Internet system may be an attack point, and these attack points are aggregated into different attack surfaces. Multiple attack surfaces form an attack layer, as shown in Table 1.

Therefore, the number of attack points in each attack layer is equal to the sum of the number of attack points in each attack surface.

If the number of attack points is large, the attack layers and the entire system will contain additional risks. When the

vulnerability of a system exists, the method to reduce the security risk is to reduce the number of attack surfaces in each attack layer.

3 Dynamically enabled defense effectiveness evaluation based on vulnerability analysis

3.1 Concepts of a vulnerability assessment

The core concept of dynamically enabled defense technology is to change the state of the system randomly, making it difficult for an attacker to exploit accumulated and outdated system vulnerabilities directly [9]. Theoretically, there is a change in the number of vulnerabilities, and the ease of vulnerability usage before and after a home Internet system is adjusted by using dynamically enabled defense technology [10]. Additionally, only a decline in the number of vulnerabilities and an increase in the ease of vulnerability usage can positively affect the dynamic change of the system status [11]. Therefore, analyzing vulnerability distribution before and after home Internet system changes can accurately evaluate the defense effectiveness of dynamically enabled defense technology [12].

3.2 Vulnerability scoring

Based on the diversity of the vulnerability assessment results, vulnerability assessment techniques can be divided into qualitative and quantitative evaluations. Qualitative evaluation determines a threat level for vulnerabilities, such as high, medium, and low, based on vulnerability assessment factors. Quantitative evaluation determines a specific threat score for vulnerabilities based on established rating factors, for example, an integer between 0 and 10. Currently, the Information Security Technology Security Vulnerability Classification Guide [13] provides domestic-standardized vulnerability rating criteria. This paper provides improvement based on these criteria and performs a quantitative evaluation of a home Internet system.

3.2.1 Information Security Technology Security Vulnerability Classification Guide

The *Information Security Technology Security Vulnerability Classification Guide (GB/T 30279-2013)* specifies classification elements and threat degrees of information security system vulnerabilities that are applicable to information security vulnerability management organizations and information security vulnerability issuing agencies to evaluate and identify the hazard degree of information security system vulnerabilities [14]. It is also a reference for

Fig. 1 Framework of a home Internet

information security product production, technology research and development, system operations, and other organizations and institutions performing related work [15].

The criteria provide a classification method for security vulnerabilities. Users can perform a comprehensive evaluation of the damage degree of a vulnerability based on the specific deployment of an affected system and the vulnerability threat level given by the criteria [16].

In the criteria, the security vulnerability classification elements include three aspects: access vector, access complexity, and impact degree. The available values for the access vector include “local,” “adjacent,” and “remote.” In general, the damage degree of a vulnerability that can be exploited remotely is higher than one that can be exploited adjacently. The available values of access complexity include “simple” and “complex,” and the damage degree of the vulnerability that has a “simple” access complexity is higher. The available values of impact degree include “completely,” “partially,” “lightly,” and “none.” Generally, the greater the vulnerability impact degree, the higher the degree of damage.

From low to high, the security vulnerability damage degree is low, medium, high, and super. The specific hazard level is determined by the values of the three elements (access vector, access complexity, and impact degree).

In the evaluation process, the Information Security Technology Security Vulnerability Classification Guide first assigns values to access vector, access complexity, and impact degree (confidentiality, integrity, and availability). These values reflect the potential impact of the vulnerability itself. Then, based on the evaluation values of confidentiality, integrity, and availability, the impact degree is calculated.

Finally, on the basis of the evaluation values of access vector, access complexity, and impact degree, the final threat level of the vulnerability is determined. The grade assessment produced by the criteria is a quantitative assessment.

Figure 2 describes the threat level evaluation process for security vulnerabilities in the Information Security Technology Security Vulnerability Classification Guide.

3.2.2 Improved vulnerability evaluation method

Considering the home Internet system, this paper created some improvements based on the Information Security Technology Security Vulnerability Classification Guide. The improved vulnerability evaluation method is more suitable for vulnerability assessment of a home Internet system. It is a quantitative assessment method and can describe the damage degree of the vulnerability more accurately. The primary changes are as follows:

- 1) Add “physical” to the range of values for the access vector because physical paths can directly launch attacks.
- 2) Adjust the range of values of access complexity to “low,” “medium,” and “high.”
- 3) Add corresponding values to the related attributes of each vulnerability evaluation factor.
- 4) Obtain the evaluation score of the impact degree by mathematic formula.
- 5) Combine the evaluation score of each factor by using the mathematic formula to calculate the final vulnerability score.

Table 1 Security vulnerability in a home Internet system

Attack layer	Attack surface	Attack point
Smart terminals	Device storage	User name plaintext storage
		Password plaintext storage
		Insecure key storage
	Web interface	SQL injection
		XSS
		CSRF
		Weak password
	Device firmware	Violence enumeration
		Known default authentication
		Sensitive information leakage
		Backdoor account
	Network service	Firmware degradation
		Unencrypted service
		Insecure OTA firmware update
		Carrier verification deficiency
	Local data storage	Lack of integrity check
		Unencrypted data
		Encryption with a leaked key
		Lack of data integrity detection
	Hardware	Encryption with a static key
		Device forgery
Communication networks	Renewal mechanism	Verification defect
		Unencrypted update
	Authentication leakage	No-signature update
		Rewrite permitted in update location
		Malicious update
		No-verification update
		Cookie-leak attack
		Session-leak attack
	Unencrypted authentication	Unencrypted authentication between equipment and equipment
		Unencrypted authentication between equipment and terminal
Controller APPs	Unencrypted authentication between equipment and cloud	Unencrypted authentication between equipment and cloud
		Lack of dynamic authentication
		Full-trust in cloud and device
		Known default account
		Insecure data storage
Clouds	Mobile terminal	No shell
		Bad confusion
		SQL injection
	Disassembling	XSS
		CSRF
		Violence enumeration
		Weak password
	Identity authentication security	Account leakage
		Known default account
	Design defect	

The improved vulnerability evaluation method is shown in Fig. 3.

The indicators and their values based on the improved vulnerability evaluation method are shown in Tables 2, 3, and 4.

In the improved vulnerability evaluation method, the mathematic formula for calculating the score of the impact degree factor is as follows:

$$\begin{aligned} \text{Impact} = & \text{ConfImpact} \times \text{ConfImpactBias} + \text{IntegImpact} \\ & \times \text{IntegImpactBias} + \text{AvailImpact} \\ & \times \text{AvailImpactBias} \end{aligned}$$

The value ranges of the impact factors are shown in Table 5.

In the improved vulnerability evaluation method, the mathematic formula for final vulnerability score is as follows: $\text{Score} = \text{round}(10 \times \text{AccessVector} \times \text{AccessComplexity} \times \text{Impact})$.

However, in an actual home Internet system, there may be a situation in which attack points are more likely to be exploited by an attacker after dynamically enabled defense. This method, based on vulnerability analysis, only considers the strategies of the defenders. Therefore, the next section will introduce the changing behaviors of the attackers. A method

Fig. 2 Threat level evaluation process for security vulnerability

to change an attack layer is proposed to evaluate the effectiveness of dynamically enabled defense based on the Markov chain.

4 A measurement method for an attack layer based on the Markov chain

During system attack and defense, the strategies of attackers and defenders are changing dynamically. This paper proposes a measurement method for an attack layer based on the Markov chain (MC). This method is improved by introducing stochastic Petri nets (SPN) theory that can be used to evaluate the effectiveness of dynamically enabled defense.

4.1 Method description

Defenders perform dynamically enabled defense of the attack layer. Dynamically enabled defense means that the attack layer will be in a state transition with a certain probability of reaching different states. The probability of transition between each two states constitutes a state transition probability matrix. The state at a specific moment is only related to the present state; it is independent of past states. This mathematical model conforms to the Markov process condition, called a Markov chain.

The primary concept of dynamically enabled defense is to present a constantly changing attack layer to the attacker to increase the difficulty of detecting and using the attack points in the attack layer. The defense attempts to reduce the system attack surface.

Regardless of the initial state, a home Internet system will eventually reach an equilibrium state after a limited state transition. Thus, the probability that the attack layer of a system finally reaches a specific state can be determined. Additionally, the mathematical expectation of the attack layer can be calculated, which is the defense effect expected after a series of dynamic changes.

Assume that the initial state of a home Internet system is S_0 . After n state transitions, the system reaches its final stationary state. The state transition of the attack layer of the system is shown in Fig. 4.

4.2 Attack layer measurement model establishment

Based on a home Internet environment and assuming that the defender does not know the actual state of the attack layer, the transition of the attack point in the system is random.

Definition1: Assume that state S of a home Internet system is a discrete set $S = \{S_0, S_1, \dots, S_n\}$. The transition probability among the attack layers' states is denoted as $P_{t,i}$. Therefore, the transition probability matrix of system state P_t is the $(n + 1)$ -th order matrix, which can be denoted as follows:

$$P = \begin{pmatrix} P_{0,0} & \dots & P_{0,n} \\ \vdots & \ddots & \vdots \\ P_{n,0} & \dots & P_{n,n} \end{pmatrix}$$

The stationary distribution probability of the Markov chain $X = (x_1, x_1, \dots, x_n)$ can be calculated based on the equation set $\{X \cdot P = 0 \mid \sum_i x_i = 1, 1 \leq i \leq n\}$.

Attack layer detection probability P_d is proposed in this paper. It is an important indicator that can affect the mathematical expectation of the attack layer in a dynamic system. P_d is closely related to a variety of factors, such as the skill level of the attacker, the degree of familiarity with the system, the amount of computing resource, and the length of the analysis time.

Definition2: Given certain computing resources and assuming that the degree of randomization and state space is not considered, attack layer detection probability is only linearly related to the time that the attacker analyzes the system. Additionally, the system state is periodically changed. Attack layer detection probability P_d of each state to the dynamic system S is defined as follows:

$$P_d = \frac{\Delta t}{T_0}, P_d \in [0, 1],$$

where Δt is denoted as the time interval during which the system state changes. T_0 is denoted as the time period that is

Fig. 3 Improved vulnerability evaluation method

required by the attacker to research all the current attack points of the system.

Definition3: A stochastic Petri net (SPN) is a five-tuple $SPN = (P, T, F, M_0, \lambda)$, where P is a set of states, called places. T is a set of transitions. $F \subset (P \times T) \cup (T \times P)$ is a set of flow relations called arcs between places and transitions. M_0 is the initial marking. The marking of SPN is used to describe the state of SPN. λ is the array of firing rates λ

associated with the transitions. The firing rate λ , a random variable, can also be a function $\lambda(M)$ of the current marking.

In the game of system attack and defense, the strategies of attackers and defenders are changing continually. One example of the reachability graph in dynamically attack and defense is shown in Fig. 5.

This paper introduces stochastic Petri nets that are isomorphic to homogeneous Markov processes. The reachability

Table 2 Value range for access vector

Symbol	Optional value	Evaluation standards
AccessVector	Physical/local/adjacent/remote	0.7/0.8/0.9/1.0

Table 3 Value range for access complexity

Symbol	Optional value	Evaluation standards
AccessComplexity	Low/medium/high	1.0/0.9/0.8

Table 4 Value range for impact degree

Factor	Symbol	Optional value	Evaluation standards
Confidentiality	ComfImpact	None/partially/completely	0/0.7/1.0
Integrity	IntegImpact	None/partially/completely	0/0.7/1.0
Availability	AvailImpact	None/partially/completely	0/0.7/1.0

graph of a SPN can be mapped directly to a state apace of MC. It is easier to gain the parameters of MC transition probability matrix by using the reachability graph of SPN, so that the transition probability $P_{t,i}$ in stationary distribution of MC can be calculated easily.

The mathematical expectation of the state attack layer can be calculated by the equation $A^* = X^*(N^*P_d)$, where N is the total number of attack points in one attack layer. $N = n_0 + n_1 + \dots + n_i$, where n_i is the number of attack points in the i -th attack surface.

Defenders must perform appropriate dynamic defense and state transition strategy so that $A^* = X^*(N^*P_d) \leq N_0$, where N_0 is the initial number of attack points in a static system attack layer. In this manner, the attack surface of a system will decrease.

5 Case analysis

5.1 Vulnerability analysis case

In this paper, the improved vulnerability evaluation method is verified using the vulnerability of a home router as an example.

The home router is a D-link DIR-645. The following vulnerability exists in the D-link DIR-645: when fetching the value of the “password” parameter in the “POST” parameter in

an authentication script called “authentication.cgi,” the attacker can cause a buffer overflow and then obtain remote command execution rights. When “authentication.cgi” on the Web server of the router is visited, the read() function in the authentication_main() function reads the POST parameter into the stack without verifying that the content-length field in the HTTP protocol exceeds the buffer size, causing a buffer overflow.

An example of the vulnerability score using the improved vulnerability evaluation method is shown in Table 6.

The evaluation scores of the impact degree factors can be obtained by combining the scores of the impact factors and Table 5, as shown in Table 7.

Substitute the evaluation scores of the impact degree factors and the impact factors into the mathematic formula for the impact degree evaluation, as follows: Impact = $0.7 \times 0.25 + 0 \times 0.25 + 1.0 \times 0.50 = 0.675$. The evaluation score of the impact degree is 0.675.

Substitute the evaluation scores of access vector, access complexity, and impact degree into the mathematic formula for vulnerability evaluation, as follows: Score = $\text{round}(10 \times 1.0 \times 0.9 \times 0.675) = 6.08$. The final evaluation score of the vulnerability is 6.08.

Based on the dynamic characteristics of the home Internet system based on dynamically enabled defense theory, assume the D-link DIR-645 router is replaced with a DIR-818W router. However, Home Network Administration Protocol (HNAP) vulnerability (CVE-2016-6563) exists in DIR-818W, and it will possibly be used to execute remote code. The router includes a pre-authentication stack buffer overflow vulnerability which affects the HNAP SOAP protocol, accepts any string of arbitrary length of some XML parameters, and then copies them onto the stack. In the process of executing an HNAP login operation, the handling of the SOAP message generated by an incorrect format will cause a buffer overflow in the stack. The XML

Table 5 Value ranges of the impact factors

Factor	Symbol	Evaluation standards	
Confidentiality impact factor	ComfImpactBias	Normal	0.33
		Confidentiality	0.50
		Integrity	0.25
		Availability	0.25
Integrity impact factor	IntegImpactBias	Normal	0.33
		Confidentiality	0.50
		Integrity	0.25
		Availability	0.25
Availability impact factor	AvailImpactBias	Normal	0.33
		Confidentiality	0.25
		Integrity	0.25
		Availability	0.50

Fig. 4 State transition of attack layer

Fig. 5 The reachability graph of SPN in the game of attack and defense

field in the mail body of SOAP that is vulnerable includes Action, Username, LoginPassword, and Captcha.

In the improved vulnerability evaluation method, the evaluation scores of each vulnerability evaluation factor and impact factor are shown in Tables 8 and 9.

Substitute the evaluation scores of the impact degree factors and the impact factors into the mathematic formula for impact degree evaluation, as follows: $\text{Impact} = 0.7 \times 0.25 + 0 \times 0.25 + 1.0 \times 0.50 = 0.675$. The evaluation score of the impact degree is 0.675.

Substitute the evaluation score of access vector, access complexity, and impact degree into the mathematic formula for vulnerability evaluation, as follows: $\text{Score} = \text{round}(10 \times 1.0 \times 0.8 \times 0.675) = 5.40$. The final evaluation score of the vulnerability is 5.40.

According to the evaluation result, it is clearly indicated that this dynamic defense of a system is positive because the vulnerability score after the system defense is lower. It also indicates that the security risk of the system after dynamic defense becomes relatively lower.

Table 6 Evaluation score for each vulnerability evaluation factor

Symbol	Evaluation value	Score
AccessVector	Remote	1.0
AccessComplexity	Medium	0.9
ConflImpact	Partially	0.7
IntegImpact	None	0
AvailImpact	Completely	1.0

Table 7 Evaluation score of impact factors

Symbol	Score
ConflImpactBias	0.25
IntegImpactBias	0.25
AvailImpact	0.50

5.2 Attack layer measurement case

This paper takes a certain home Internet system as an example. The initial state of one attack layer can transition among five states. The reachability graph of the system is shown in Fig. 6.

P_init represents the initial place of the system. Transition t1 represents the initiation of attacks by attackers. Then, the marking will transition from P_init to P1 or P2. P_pre represents the defense strategies made by defenders. Transition t2 represents successful defenses that make the marking transition to P3. Transition t3 represents successful attacks that make the marking transition to P4. In order to realize a closed-loop system, transition t5 is added to describe the process of system from being invaded to a normal state.

The firing rate $\lambda = (2, 1, 1, 3, 2)$ is given. Therefore, a Markov chain which is isomorphic to the given SPN can be derived by replacing the transitions t_i to λ_i , which is shown in Fig. 7.

The stationary state vector $X = \{x_0, x_1, x_2, x_3, x_4\}$ can be calculated by the equation set $\{X \cdot P = 0, \sum_i x_i = 1, 1 \leq i \leq n\}$, as follows:

$$\begin{cases} 2x_0 = 2 \cdot x_4 \\ 2x_1 = 3x_2 + 2 \cdot x_0 \\ 4x_2 = x_1 \\ x_3 = x_1 + 3 \cdot x_4 \\ x_0 + x_1 + x_2 + x_3 + x_4 = 1 \end{cases}$$

The solution is $X = \{\frac{5}{43}, \frac{8}{43}, \frac{2}{43}, \frac{23}{43}, \frac{5}{43}\}$.

This paper chooses the controller APPs attack layer as an example. We assume that defenders do not know the actual state of the attack layer. The transitions of the attack points of the system are random. And the attacker cannot explore all the attack paths before the next state change.

Table 8 Evaluation score of each vulnerability evaluation factor

Symbol	Evaluation value	Score
AccessVector	Remote	1.0
AccessComplexity	Medium	0.8
ConflImpact	Partially	0.7
IntegImpact	None	0
AvailImpact	Completely	1.0

Table 9 Evaluation score of impact factors

Symbol	Score
ConfImpactBias	0.25
IntegImpactBias	0.25
AvailImpact	0.50

The controller APPs attack layer has two attack surfaces, which include five attack points, as shown in Table 1 ($N_0 = 5$). Assuming that $N_1 = 8$, $N_2 = 6$, $N_3 = 7$ and $N_4 = 4$ after a limited transition, the mathematical expectation of the attack layer is as follows:

$$A^* = \left[\frac{5}{43}N_0 \quad \frac{8}{43}N_1 \quad \frac{2}{43}N_2 \quad \frac{23}{43}N_3 \quad \frac{5}{43}N_4 \right] \cdot P_d^T$$

Defenders must perform appropriate dynamic defense and state transition strategy so that $A^* = X^*(N^*P_d) \leq N_0$; therefore,

$$\left[\frac{5}{43} \cdot 5 \quad \frac{8}{43} \cdot 8 \quad \frac{2}{43} \cdot 6 \quad \frac{23}{43} \cdot 7 \quad \frac{5}{43} \cdot 4 \right] \cdot P_d^T \leq 5$$

To simplify the calculations, assume each time attack layer detection probability $P_{d,i}$ is the same constant. Thus, $P_d^* \leq 0.762$ is used to determine whether the system's dynamically enabled defense is effective.

When $P_d \geq 0.762$, the mathematical expectation of the attack layer in a dynamic system is larger than the mathematical expectation in a static system. The home Internet system using dynamically enabled defense will not be effective in this scenario.

Fig. 6 The reachability graph of SPN of a home Internet system

	P_1	P_2	P_3	P_4	P_5
M_0	1	0	0	0	0
M_1	0	1	1	0	0
M_2	0	0	1	1	0
M_3	0	1	0	0	1
M_4	0	0	0	1	1

Fig. 7 The Markov chain of the home Internet system

Given a specific computing resource, we assume that some attackers can successfully explore all the attack points of the system within 8 h. Based on $P_d = \frac{\Delta t}{T_0}$, $P_d \in [0, 1]$, we can obtain $\frac{\Delta t}{8} \leq 0.762$. Then, the minimum time period during which the system state changes is $\Delta t = 6.096h$. Therefore, the system should perform dynamically enabled defense within 6.096 h so that the defense is effective.

6 Conclusion

Smart terminals in a home Internet suffer malicious attacks from hackers on a daily basis. Defenders should change system states dynamically to improve system defense ability. To quantify the defense ability of a home Internet, this paper proposes an improved vulnerability scoring method based on the Information Security Technology Security Vulnerability Classification Guide. Using D-link DIR-645 and D-link DIR-818W routers as an example, changing the routers decreased the vulnerability score of the home Internet system from 6.08 to 5.40. The defense ability of the home Internet system was enhanced.

During actual home Internet attack and defense, the actions of attackers should also be considered. Therefore, this paper proposes a method to measure an attack layer based on the Markov chain. This paper chooses the controller APPs attack layer as an example. This method builds a model of an attack layer that can assess whether the defenders use of dynamic defense is effective. This paper introduces stochastic Petri nets to improve this method by using the reachability graph of SPN. It is easier to gain the parameters of MC transition probability matrix with the reachability graph.

Then, by calculating the factor attack layer detection probability P_d , the model determines that when $P_d \geq 0.762$, there is no defensive effect even if defenders change the system states. This model also obtains the minimum time period $\Delta t = 6.096h$ after which the defender must

change system states. If the time period for defense is greater than Δt , attackers have a probability of hacking into a home Internet system.

Finally, this paper concludes that after defenders change the system states, the vulnerability score may become higher or lower. The minimum time period Δt of changing states will become longer if the vulnerability score is lower, meaning the home Internet system has an enhanced defense ability.

Funding information This work is supported by the National Key R&D Program of China (2017YFB0802703), National Key R&D Program of China (2016YFF0204001), the Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data (2017BDKFJJ017), the PAPD fund, the CICAET fund, the CCF-Venustech Hongyan Research Initiative (2016–009, 2017–004), and the Science and Technology Foundation Project of Guizhou Province (No. QianKeHeJiChu[2016]1115).

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

1. Yang Y et al (2017) General theory of security and a study case in internet of things. *IEEE Internet Things J* 4(2):592–600
2. Shen J, Shen J, Chen X, Huang X, Susilo W (2017) An efficient public auditing protocol with novel dynamic structure for cloud data. *IEEE Trans Inf Forensics Secur*. <https://doi.org/10.1109/TIFS.2017.2705620>
3. Kong Y, Zhang M, Ye D (2016) A belief propagation-based method for task allocation in open and dynamic cloud environments. *Knowl-Based Syst* 115:123–132
4. Xia Z, Wang X, Sun X, Wang Q (2015) A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. *IEEE Trans Parallel Distrib Syst* 27(2):340–352
5. Shen J, Liu D, Shen J, Liu Q, Sun X (2017) A secure cloud-assisted urban data sharing framework for ubiquitous-cities. *Pervasive Mobile Comput*. <https://doi.org/10.1016/j.pmcj.2017.03.013>
6. Xiong L, Xu Z, Shi Y-Q (2017) An integer wavelet transform based scheme for reversible data hiding in encrypted images. *Multidim Syst Sign Process*. <https://doi.org/10.1007/s11045-017-0497-5>
7. Shen J, Chang S, Shen J, Liu Q, Sun X (2016) A lightweight multi-layer authentication protocol for wireless body area networks. *Futur Gener Comput Syst*. <https://doi.org/10.1016/j.future.2016.11.033>
8. Verma H, Jain M, Goel K, Virkram A, Verma G (2016) Smart home system based on Internet of things, 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, pp 2073–2075
9. Babak Salamat, Todd Jackson, Gregor Wagner, et al. Runtime defense against code injection attacks using replicated execution, *IEEE Trans Dependable Secure Comput IEEE*, vol. 8, n. 4, 2011, pp. 588–601
10. Yang L, Yu Q (2016) Dynamically-enabled cyberspace defense, 1st edn. The People's Posts and Telecommunications Press (Posts & Telecom Press), Beijing, pp 214–215
11. Yang L, Hu S, Ho T-Y (2015) Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks. *Comput Aided Des (ICCAD) IEEE* 183–190
12. Nuno Antunes, Marco Vieira, Defending against Web application vulnerabilities, *Computer*, vol. 45, n. 2, 2011, pp. 66–72
13. Liu QX et al (2012) Research on key technology of vulnerability threat classification. *J Commun*
14. Srivatsa M, Liu L (2005) Vulnerabilities and security threats in structured overlay networks: a quantitative analysis, 2004 20th Annual Computer Security Applications Conference, IEEE, pp 252–261
15. Li X, Chang X, Board John A, et al (2017) A novel approach for software vulnerability classification, 2017 Annual Reliability and Maintainability Symposium (RAMS), IEEE, pp 1–7
16. Jin S, Wang Y, Cui X, et al (2009) A review of classification method for network vulnerability, 2009 I.E. International Conference on System, Man and Cybernetics (SMC), IEEE, pp 1171–1175