TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.6, June 2014, pp. 4639 ~ 4647
DOI: 10.11591/telkomnika.v12i6.5446

Wireless Network Risk Assessment Model and Application

JianGang Tang
Yunnan Police Officer Academy
Wuhua District, Kunming City, Yunnan Province, China, +86 13700600076
email: 65615196@qq.com

Abstract

Wireless network makes up the wired network shortcomings. With the popularity of the WiFi terminal, the security threats are constantly upgrading, and the security issues have been plaguing the legitimate user. In this paper we had analyzed the risks mechanism of WLAN for network resources, and designed an assessment model of security risk. When the incidents of network security which caused for vulnerability factors had been occurred, the model can be used to assess the consequences and impact on WLAN. The model achieves the network security early warning and control by scientific measurement and evaluation of the WLAN security risks. Wireless network security is not only with authentication, encryption, integrity testing and other technology-related, but also need intrusion detection systems, firewalls and other technology cooperation, so it's a multi-layered problem.

Keywords: *wireless network, assessment model of security risk, authentication mechanism, security policy*

1. Wireless Network Security Risk Assessment Model

1.1. The Mechanism of WLAN Security Risk Model

Establishment of a wireless network security risks Mechanism is the study of the premise of WLAN security risk assessment. Risk refers to the act or event uncertainty of the results. WLAN security risk refers to the security problems caused by WLAN system, or actual events may cause threat.

WLAN security risks constitute divided into five fields: the source of threat, the way of threat, the incentives of threat, the victims of threat and the consequences of threat. The source of threat is the initiator of the threat; The way of threat is the means of the implementation of the threat; Threat inducing factor is the weakness exploited by threats, called vulnerability or vulnerabilities; Threaten victims are threatened or target object; The consequences of the threat is due to the loss suffered as a result of the threat situation, also known hazards

The relationship between threats can be expressed as the following. One or more origins of risk, using one or more of way, damage one or more network resources, and cause information system abnormalities or crash. The source of threats uses the vulnerabilities of WLAN, threats network resources, cause a negative impact on the WLAN, As shown in Figure 1.

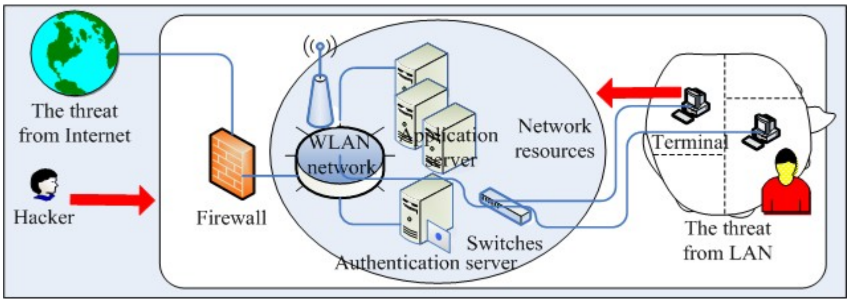


Figure 1. Network Resource Security Risks Mechanism

Received December 29, 2013; Revised March 1, 2014; Accepted March 18, 2014

1.2. Factors Considered in Risk Assessment

In the research of WLAN security risk assessment, the network resources, the threats, the vulnerabilities, the security measures, they all are the factors which have complex interrelationships, as shown in Table 1.

Table 1. The Relationship between Risk Factors and the Value of Risk Assessment

Relationship Factors of risk assessment	Risk Factors	Risk assessment values
The value of network resources	↗	↗
	↘	↘
The number of threat sources	↗	↗
	↘	↘
Vulnerability of network resources	↗	↗
	↘	↘
The cost of security measures	↗	↗
	↘	↘
The progress of security measures	↗	↗
	↘	↘
The residual risk from security measures	↗	↗
	↘	↘

1.3. The Model for Calculating the Risk Assessment

In this section, we use the problem of WLAN, and then base on the analysis of the risk factor theory above, and establish the security risk assessment model which is used to get the safety grades of WLAN, shown in Figure 2.

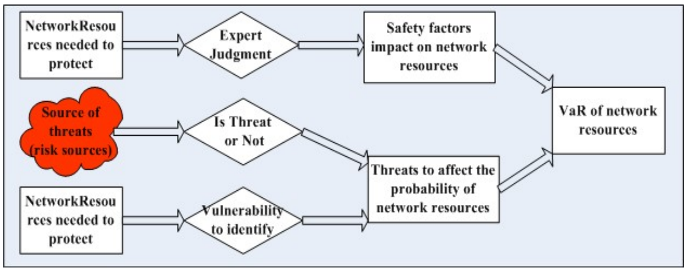

NetworkResources needed to protect
Expert Judgment
Safety factors impact on network resources
Source of threats (risk sources)
Is Threat or Not
VaR of network resources
Threats to affect the probability of network resources
NetworkResources needed to protect
Vulnerability to identify

Figure 2. Risk Assessment Model of Network Resources

It can be deduced from the model diagram, According to Figure 2:

$$R = f（\mathrm{H}, \mathrm{W}, \mathrm{T}） = f(\mathrm{I}, \mathrm{P}(\mathrm{W}, \mathrm{T})) \qquad R \in [0,1], \qquad P \in [0,1].$$

R is the risk of WLAN; N is the network resources; W is the vulnerability of network resources; T is the threat to network resources; I is the importance of the network assets; P is the probability of security incidents which will be happened.

$$I_f = 1 - I_s, \qquad P_f = 1 - P_s, \qquad I_f \in [0,1], \qquad P_f \in [0,1];$$

Subscript f indicates that the security incident did not occur; Subscript s indicates that the security incident has occurred.

The value of R is the security incidents and their impact likelihood estimation.

R=f (the importance of network resources, the probability which may be happened security issues come into being.

$$R = 1 - I_f * P_f = 1 - (1 - I_s)(1 - P_s) = I_s + P_s - I_s * P_s\,;$$

The facts that cause network security incidents are the vulnerability of network resources and the threats from WLAN. We use these two factors through a reasonable algorithm in the risk assessment model.

Definition 1. The three factors which threaten network security are from the Internet, LAN threat, and vulnerability of network resources, given a finite set of items $D = \{d_1, d_2, \cdots, d_x\}$. For example, if $x = 3$ then we deduced $D = \{d_1, d_2, d_3\}$.

Definition 2. We give different factors which threaten network a different weight, given the finite set of weight $H = \{h_1, h_2, \cdots, h_y\}$, and $y = x$. For example, if $x = 3$ then deduced $y = 3$ and $h = \{h_1, h_2, h_3\}$.

Definition 3. In the assessment of the threat level of network resources, we made an evaluation value set as $G = \{g_1, g_2, \cdots, g_q\}$, G is the set which experts evaluate the each element in set D. For example, if $q = 5$ then we deduced $H = \{g_1, g_2, g_3, g_4, g_5\}$ = {Very High, High, Medium, Low, Very Low}.

The membership degree among d_i and g_j is $K_{ij} = \sum_{i=1, j=1}^{\infty, 5} c_{ij} \Big/ \sum_{i=1}^{\infty} t_i$.

The C_{ij} is assessment level j given by the experts for the factor of i, t is the weight of factor of i.

Then the likelihood of security problems is $L_s = \prod_{i=1}^{3} \prod_{j=1}^{5} (h_i k_{ij} g_j) = HKG^T$.

The K is the membership matrix, G^T is the transposed matrix of G.

1.4. Computing the Degree of Importance of Network Resources

After the security incidents occurred, we can use the impact of network resource to assess the importance of cyber source. The importance of the conversion of assets mainly considers the three factors which are the confidentiality, integrity, availability. According to the fuzzy comprehensive evaluation method, we define the set which contains the factors of important degree for assets [1].

D' = {*Confidentiality,Integrity,Availability*} = $\{d_1', d_2', d_3'\}$

The each corresponding weight vector which assigned to different factor is varies depending on the type of evaluation system varies.

Evaluation set is $W = \{w1, w2, w3, w4, w5\}$; w1, w2, w3, w4, w5 represent the five levels of the assignment of confidentiality, integrity, assignment, assignment availability. For example, the five levels set as Very High, High, Medium, Low, and Negligible [2].

Integrated evaluation algorithm estimates the total volume of information assets, calculated as follows:

Initialize the original observation matrix X, the following is the formula:

$$S = \begin{pmatrix} s_{11} & \cdots & s_{1n} \\ \vdots & \ddots & \vdots \\ s_{m1} & \cdots & s_{mn} \end{pmatrix}$$

m is the number of samples (assess the number of experts), n is the number of variables evaluated.

Experts set each factor in U' reference to the evaluation set V, which is the valuation of information assets confidentiality, integrity, availability. Transforming the original observation matrix S, can be derived from the fuzzy subset E .

$$E=\begin{pmatrix} e_{11} & \cdots & e_{1n} \\ \vdots & \ddots & \vdots \\ e_{m1} & \cdots & e_{mn} \end{pmatrix}=\begin{pmatrix} e_{11} & e_{12} & e_{13} & e_{14} & e_{15} \\ e_{21} & e_{22} & e_{23} & e_{24} & e_{25} \\ e_{31} & e_{32} & e_{33} & e_{34} & e_{35} \end{pmatrix}$$

Then the degree of importance of network resources is $I_s = H'EW^T$.

1.5. Risk Grade Evaluation

Through calculated risk set of R we define the assessment set of V_R .

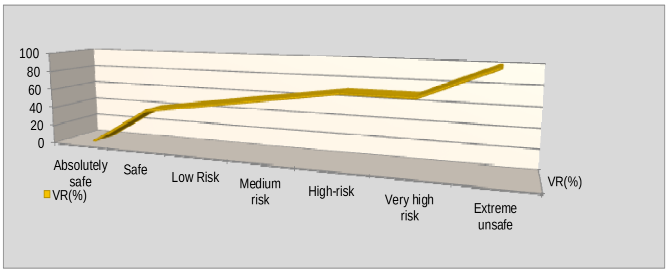


Figure 3. Network Resource Security Risks Mechanism

Generally we call that the V_R is greater than 70% of high-risk is high risk WLAN, as shown in Figure 3. It describes the implementation of safety organizations Capability Maturity is not enough. So it needs to analyze the main factors causing the larger values of R, and through the management and technical means to reduce these factors, and then assess the R again, until to reduce the risk to an acceptable degree for WLAN.

2. Wireless Network Security Risks Exist

Wireless network is faced with various ways of intrusion. To solve these problems, the client users must understand the hidden dangers of wireless network. Safety problems found are the following.

2.1. Network Devices without Security Protection

Wireless network users inexperienced not to modify the device parameters, continue to use the default settings which comes from the factory. If the wireless router is not set, hackers in the wireless network coverage can directly invade the wireless network. In addition, Windows, Android, IOS and other operating systems, which itself has zero configuration wireless network function, can automatically search for WiFi signals and automatic connection function.

2.2. WLAN Coverage too Wide

The administrator needs to be considered from a global security laid wireless network access point, so that satisfy the requirements of wireless coverage, do not beyond the scope of coverage. When design a WLAN, wireless AP should be choose according to the actual needs, if blindly select wireless AP which transmit power and antenna gain is too large, although it increases the coverage, and enhance the signal strength, but it increase the opportunities of information leakage.

2.3. Factors within the Network Terminal

Many factors endanger network security, computer virus, Trojan is the most harmful and extensive effect on the network, followed by the denial of service attack. When a terminal which had been infected with virus and Trojan connected to the network, the terminal will send a large number of invalid data or broadcast, occupied network connections, causes network congestion, and cause other users can not use the network.

2.4. The Existence of Network Monitoring Technology

Network monitoring technology was originally designed to monitor the data communication, so that the administrators convenient and efficient find network anomalies and insecurity. It's used by illegal intruders as an effective and powerful means of stealing information. Run in promiscuous mode wireless NIC can complete the network monitoring function.

2.5. The Hardware is Embedded Monitoring Module

Global network equipment manufacturers have Cisco, Motorola, SMC, IPCOM, D-Link, HuaWei, ZTE etc., Generally speaking, the manufacturers of equipment is to meet the current needs of network application and the effective realization of the network connection, ensure the stability and security of network. But for the national strategic needs, some countries in order to steal confidential information from the other countries, the government orders manufacturers to install or even embed monitoring module on its network equipment, and ordinary users cannot be aware of its existence.

2.6. Early WiFi Standard is Imperfect

Wireless network encryption methods are WEP, WPA and WPA2. Because the mechanism of wireless network security may be defective, wireless network standards need to be perfected gradually. Hackers use special technologies, tools, software to invade and endanger the safety of WLAN.

WEP (Wired Equivalent Privacy) is Wired Equivalent Privacy protocol. WEP is the originally standard protocol of 802.11b defined by wireless alliance. Because WEP uses 64 bit or 128 bit encryption key encryption algorithm RC4, a few years ago, researchers and hackers have been able to decipher the WEP standard.

WPA (WiFi Protected Access) is a wireless security protocol instead of WEP, which is mainly used in wireless network with high security level. Because it uses is still relatively weak RC4 encryption algorithm, so the illegal intruders listening enough data packet, then using high performance computing equipment, even if the WPA has TKIP protection may be cracked.

WPA certification has two kinds, one kind is to adopt 802.1x+EAP mode, the client user only need to provide certification documents, such as the account name, password and other information, certification through the RADIUS authentication server. Another way is WPA Pre-Shared Key (WPA-PSK) mode, it dose not equip with a professional authentication server .WPA-PSK is mainly used for the application which contains a small number of users.

WPA2 is the second generation of WPA. It's the security solutions WiFi Alliance launched a revised based on the latest IEEE 802.11i standard. WPA2 uses AES encryption follows the (U.S.) National Institute of Standards and Technology (NIST) FIPS140-2 and 802.1x authentication.

3. Wireless Network Intrusion Process Analysis

WPA encryption system has no flaws can be exploited currently, so can not gain the password by collecting sufficient data packet and analyzing encryption algorithms. The only way to crack WPA passwords is to use a dictionary to attack. However, some of the equipment can be cracked by using WPS encryption security vulnerabilities, and therefore it can be invaded.

3.1 Crack WEP Encryption

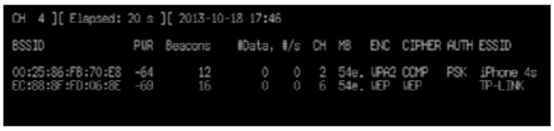
802.11 had defined the WEP algorithm for data encryption process, as shown in Figure 4.

Figure 4. WEP Encryption Process

IV is initialization vector, PASSWORD is the encryption password of the AP, KSA=IV+ PASSWORD, DATA is not encrypted data, CRC-32 is the integrity check value, PRGA=RC4 (KSA),gain ENCRYPTED DATA by XOR, IV+ENCRYPTED DATA is sent out through WiFi.

Upon receiving the decryption process of terminal, it adopts the method to generate the same encryption and decryption key, then make the ciphertext and decryption key XOR and calculated a new CRC-R, If the encryption key and decryption key is the same and CRC-R equals the original CRC32, it indicates the receiver had already got the original plaintext, conversely decryption failed.

WEP encryption invasion process is as follows: Firstly, need to obtain the target network information by scanning WiFi, as the Figure 5 shows. Then grab IVs packet, when access to enough number of packet data, you can obtain the WEP encrypted password, as the Figure 6 shows.

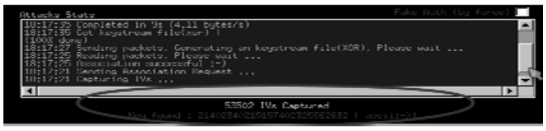


```
CH  4 ][ Elapsed: 20 s ][ 2013-10-18 17:46

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:25:86:F8:70:E8  -64       12        0    0   2  54e. WPA2 CCMP   PSK  iPhone 4s
EC:88:8F:F0:06:8E  -69       16        0    0   6  54e. WEP  WEP         TP-LINK
```

Figure 5. Scanning WEP



```
18:17:35 Completed in 9s (4.11 bytes/s)
18:17:35 Got keystream file(xor) !
(100% done)
18:17:27 Sending packets. Generating an keystream file(XOR). Please wait ...
18:17:25 Reading packets. Please wait ...
18:17:25 Association successful :-)
18:17:21 Sending Association Request ...
18:17:21 Capturing IVs ...

53502 IVs Captured
Key found : 214023402151574023255E2632 ( ascii:->)
```

Figure 6. Get the WiFi Password

3.2 Crack WPA Encryption

Crack WPA-PSK need to get a handshake packet called 4-way-handshake, as shown in Figure 7. WPA-PSK security system is a secure encryption mechanism. At present only the probable way uses password dictionary to attack. In the security system of WPA-PSK joined the unspoken rule against them. Because the packet of 4-way-handshake contains contact information and passwords, so hackers rely on this information and use password dictionary to attack wireless network. The main data transfers by 4-way handshake are the following: SSID, AP_MAC, STATION_MAC, Snonce, Anonce, 802.1x data and MIC. We all know that MIC and password which only has a relationship. By pdkdf2_SHA1, SHA1_PRF, HMAC_MD5 algorithm finally generates MIC-1, when a password is found in the dictionary which MIC-1 is equal to the MIC, then the hacker had found the password.

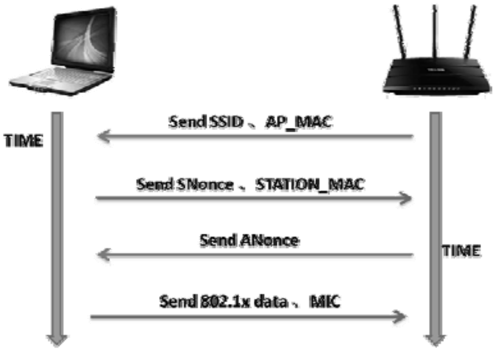


Figure 7. 4-way Handshake

3.3. Crack WiFi with a Password Dictionary

This method is suitable for all types of encryption network, for example the WEP encryption, the WPA encryption, the WPA2 encryption. Its principle is through the known string one by one to verify the password dictionary which the hacker made, to determine whether the password is correct to the target wireless network. Password dictionary has the following three kinds of categories.

Weak password dictionary is likely to be found and cracked by hackers. The strong password had been exposed. Social engineering password which has a relationship with the individual information, such as the birthday of client, cell phone numbers, etc.

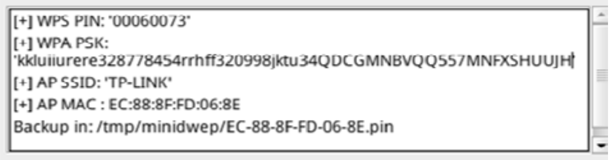
3.4. Use the Vulnerabilities of WPS

WPS (WiFi Protected Setup) is the Wi-Fi alliance certification program, is not a new safety performance, the purpose is to simplify the wireless LAN configuration. By the end of 2011, security researcher Stefan Viehbock had published the WPS exists security flaws in his blog, and many manufacturers have this problem for wireless devices. This defect causes the PIN of WPS become more likely to be found by trying each PIN Method.

Mainly three reasons WPS can be cracked. The first, PIN code is the only requirement for network equipment to acquire access, and do not need the other way of identifying. The second, WPS PIN code of the Eighth digits is a checksum, so the hackers only need simply to calculate the first 7 digits. The third, Viehbock found when PIN authentication connection failed, wireless AP will send a message called EAP-NACK back to the client, the attacker will be able to determine the PIN front or back part is correct through the response information, therefore, the hackers need only find a 4 digit PIN and a 3 digit PIN from the 7 digit PIN, that is the possibility only has 10000 and1000 times [3]. In the actual crack attempt, Only a maximum of test 11000 times, an average of about 5500 times to crack WPS.

WPS encryption wireless network intrusion process is as follows:

First step is to scan and obtain the target AP information. Then input the parameter of reaver command, began to exhaustive PIN code. When this PIN and AP wireless PIN code is consistent to the target device, WPA/PWA2 encrypted password, complete crack, the results are shown in Figure 8.



```
[+] WPS PIN: '00060073'
[+] WPA PSK:
'kkluiiurere328778454rrhff320998jktu34QDCGMNBVQQ557MNFXSHUUJH
[+] AP SSID: 'TP-LINK'
[+] AP MAC : EC:88:8F:FD:06:8E
Backup in: /tmp/minidwep/EC-88-8F-FD-06-8E.pin
```

Figure 8. Obtain WPA/WPA2 Passwords

4. Wireless Network Security Problems Coping Strategies

Because the wireless communication mode determines as long as it is in the wireless network signal coverage data communication within a region are likely to be listening, steal or modify, and the application of wireless network is a serious threat. In order to ensure the security of wireless communication, the necessary safety strategy shall be adopted.

4.1. Disable the DHCP Server [4]

When the clients access to the wireless network, wireless router will automatically assign an IP address to the client, such as the IP address, subnet mask, DNS and gateway information, this put the wireless router be exposed, therefore, in this way should through assign static IP address to the user to avoid this situation. In order to improve the network security performance, disable the wireless router DHCP service to avoid the leakage of the related parameters of DHCP server network configuration.

4.2. Using Physical Address (MAC) Filtering

Each wireless client adapter has a unique 48-bit physical address (MAC), in order to achieve the goal that only allow legitimate users NIC access AP, the network administrators can set up in AP MAC address filtering table. Its efficiency will decrease with the increase in the number of terminal. since illegal users through the network listener can get valid MAC address table, and NIC's MAC address is also not difficult to modify[5],so that the Illegal users can misappropriation legitimate user's MAC , therefore, MAC address filtering is not very effective authentication methods.

4.3. Use Network Communications Encryption Technology

Whether the wireless router or wireless AP, its settings are provided wireless encryption options. When a wireless network encryption, the client must use the correct password before access the WiFi. Wireless network devices typically provide the encryption settings are WEP, WPA/WPA2 and WPA-PSK/WPA2-PSK several models, because the of congenital defects of WEP encryption method which exists in the design, WEP password or communication is very easy to be illegally obtained, so it is necessary to adopt a higher security level encryption to protect the communication.

4.4. Use Firewalls, Intrusion Detection Systems

Because there did not set the necessary security policy in the process of building a wireless network, so the users will be very unsafe in the course of using the network. In order to protect the security of local data, it is needed using the software and hardware firewalls and intrusion detection systems, etc, to achieve the purpose of network intrusion defense.

4.5. Set High Intensity Login Password

The users must change the default administrator name, login password of the wireless router, wireless AP. Password must use the Combination of uppercase and lowercase letters and numbers, and change them regularly.

4.6. Hide or Turn Off SSID Broadcast

SSID (Service Set Identifier) is the name of a LAN. A WLAN can be divided into several subnets which required different authentication, so the computers only with the same SSID can communicate with each other, unauthorized users can not access this network. Usually the wireless equipment of the same manufacturer has a same or similar SSID name. Hackers used to try all known SSID name to connect the network, It is possible to establish data communication link, and threat to other users in the WLAN. Wireless devices need to modify its SSID identifies and recommended to close the SSID broadcasting to prevent illegal users through SSID to direct the search to the target network.

4.7. Solutions for WPS Vulnerability

There is not a good solution to resolve WPS vulnerabilities at present. Most wireless routers do not limit the times of wrong password input, they are naked and exposed to attacks by hackers. In order to avoid being attacked from hackers, people need to timely close WPS, but most people probably don't realize it is serious. Before the network password has not been attacked and found, the suggestion is immediately disable WPS on still in use WPS wireless encryption equipment, and use the more secure WPA2 encryption methods, and also disable Universal Plug and Play function.

4.8. Timely Upgrade the Software of Equipment

Wireless network devices usually have security configuration options, the network administrator can set according to their own needs. Even low-end SOHO (Small Office Home Office) wireless router now, also provides "software update" function. In order to make wireless networks more secure, the network administrators need to upgrade the system software of network equipment regularly

4.9. Using Next Generation 802.11i Wireless Networking Standard

In order to further enhance the security of wireless network and ensure the compatibility between different manufacturers of wireless security technology, the IEEE802.11 working group developed a new safety standards of IEEE802.11i, it can provide security protection of government level [6]. It completely solves the security problems of IEEE 802.11, The IEEE802.11i standard to solve the security flaws of 802.11, increases the technology includes identity authentication, integrity verification, data encryption, key negotiation. Theoretically speaking, this protocol can solve the security problem of wireless network, and applicable to all wireless network deployment

5. Summary

Using wireless technology to replace the wired medium wireless network in the area of network construction and data transmission, wireless network has obvious advantages in practicality, convenience etc, on the other hand, security threats are always go hand in hand. Authentication, encryption, integrity detection and other related aspects of wireless network security, also needs IDS, firewall technology, it is a multi-level problems. We need to use the technology and standard WiFi Alliance launched to enhance the wireless network security management, in order to design a wireless network with high security. In the use of wireless network, it need the network administrator use of all kinds of security technology effectively, also the users needs to strengthen the prevention consciousness and awareness of network security of their own.

References

[1] Wu-yuan Jiang, Zhou-jun Yang. The Phase-type Risk Model Perturbed by Diffusion under a Threshold Dividend Strategy. *Acta Mathematicae Applicatae Sinica (English Series*). 2013; 01; 216-224.

[2] Xie Jie-hua, Zou Wei, Wang De-hui. On the Expected Present Value of Total Dividends in a Risk Model with Potentially Delayed Claims. *Communications in Mathematical Research*. 2013; 10; 192-202.

[3] JunTan Fang, ZhiQiang Xu, ChunMin Ye. Wi-Fi WPS Security Analysis. *Netinfo Security*. 2013; 01: 84-85.

[4] Zhang Xiao-ming. Research of security Strategy in Wireless Network. *Journal of Taiyuan University.* 2013; 14; 135-137.

[5] JianHui Lai. Study on the construction and security of wireless network. *China New Telecommunications.* 2013; 10; 80.

[6] LiMin Zhang. Security technology of wireless network. *Fujian Computer.* 2009.