TELKOMNIKA, Vol. 11, No. 8, August 2013, pp. 4832~4840
e-ISSN: 2087-278X

Wi-Fi Protocol Vulnerability Discovery based on Fuzzy Testing

Kunhua Zhu*[1], Guohong Zhu[2]
[1]School of Information Engineering Henan Institute of Science and Technology
Xinxiang 453003, Henan, China
[2]College of Computer and Information Engineering Henan Normal University
Xinxiang 453002, Henan, China
*Corresponding author, e-mail: zwkh100@163.com

Abstract

To detect the wireless network equipment whether there is protocol vulnerability, using the method of modular design and implementation of a new suitable for Wi-Fi protocol vulnerability discovery fuzzy test framework. It can be independent of its transmission medium, produce deformity packet and implementation of the attack on the target system. The author firstly describes the wireless network protocol vulnerability discovery and fuzzy test in this paper, then focused on the test frame technical scheme, detailed technical realization and so on, and its application are analyzed. In the experimental stage the fuzzy test is applied to a wireless networks gateway, the test results show that the fuzzy test framework can be well applied to the wireless network equipment agreement loophole mining work.

Keywords*: Wi-Fi protocol, fuzzy testing, vulnerability discovery*

Copyright © 2013 Universitas Ahmad Dahlan. All rights reserved.

1. Introduction

With the wide application of wireless network, wireless network protocol security problem is becoming more and more attracted people's attention. Wi-Fi is wireless network protocol IEEE 802.11b's nickname, is a short-range wireless transmission technology, can support Internet access radio signal in the hundreds of feet range. With the development of technology, now the IEEE 802.11 standard has been collectively referred to as Wi-Fi. Since the emergence of its technology in 1999, Wi-Fi is widely used in many areas, is developing very rapidly, and greatly changed the way of people's life and working. At present, Wi-Fi is used in the Bluetooth headset, radio, printer, camera, notebook; even being used in the manufacture of mosquito net, drug delivery in vitro, do wireless glasses, mobile devices over the past two years also uses a lot of intelligent operating system, and has the function of Wi-Fi, billions of dollars each year the market. However, the Wi-Fi of the new protocol and new application is seldom considered in terms of security, there is much vulnerability, and Wi-Fi protocol continues to expand, the more the number of the relevant agreement, the agreement is more complex, it is the invasion and spread of hackers and virus creates convenient conditions. Compared with the traditional wired network, from a security point of view, the wireless network is always with new different attacks of network and terminal threat, therefore, a threat on Wi-Fi safety testing and vulnerability discovery is of great significance.

At present the international Wi-Fi safety testing and vulnerability discovery work is still in its initial stage. In 2006, two senior researchers from Secure Works, Johnny Cache and David Mayor [1,2] leased the first 802.11 wireless driving loopholes in the United States the world Black Hat, through this vulnerability they successfully broke into a Mac Book [3, 4] the same year, a student named Seng Ooh Toh form Georgia Institute of Technology, found a leak in 802.11 wireless network card in the firmware in the completion of a project, To found from the access point send test response data frames if the Service Set ID length Set to 0 can cause some wireless card stop response [5, 6].

In succession after more researchers do the relevant work: In 2006, senior lecturer Chris Eagle from California the Naval Postgraduate School by combining Fuzzing and manual analysis, found the Broad Com 's wireless device driver vulnerabilities; In 2007, a researcher, Laurent BUTTI, from network and service security laboratory of Orange Labs France Telecom

Received April 4, 2013; Revised May 27, 2013; Accepted June 6, 2013

Network made a report-Wi-Fi Advanced Fuzzing in 2007 Black Hat Europe, presented his results, who used Scaly and Meta Spoilt fuzzy test on Wi-Fi, found a lot of bugs:

Similar basic just to improve the existing testing framework foreign, and Wi-Fi applications has been quite extensive [7], and a growing number of consumer electronics products support wireless connectivity. At present Wi-Fi protocol continues to expand, the complexity increase will inevitably bring more bugs, which should attract more attention to the excavation work on the Wi-Fi security detection and vulnerability.

Fuzzy test is a kind of based on defect injected automation software testing technology, the target software a large injection of half valid data, monitoring program of the abnormal condition to find software potential security vulnerabilities [8, 9].Using fuzzy test method is not ensuring that will find all the program errors, but through this tentative fuzzy test to find out mistakes must be due to some measured code cause. As far as possible in order to improve the efficiency, we need to optimize fuzzy unit test scheme. Fuzzy test has two key operations: Produce deformity data and observe whether the application abnormal. But two operations have the following questions [8]:

(1) At present, the theory does not appear the way which can be mature and optimization of the generation deformity data. Many of the established method operability is not strong [9]; For example, If fuzzy device based on exhaustive way to produce all sorts of possible deformity protocol data combination, is whether produce data of time, or to be measured target response testing time will rise dramatically, which makes the test effort and inefficient; If fuzzy device based on random way produce deformity data, then even if found the problem, and also it is difficult to accurate positioning problem.

(2) Need to have a monitor to observe whether the application abnormal. But it use what method to determine the response of the measured target is abnormal, the anomaly is a found holes. Network protocol fuzzy device only to solve above two problems can have good effect in practical application[10].

This paper will focus on research is a wireless network protocol for 802.11 vulnerability discovery fuzzy test framework, the framework using optimizes the data generation method, in order to improve the efficiency and effect of fuzzy test.

2. Network Protocol Fuzzy Tester

Test object of Network protocol fuzzy is mainly the product of all kinds of network in the network protocol analysis module, the purpose is to test the existence of vulnerability in the program of assembly, parsing network protocols. The idea is that communication can be made between fuzzy controller and the object measured target, to measure target application send variation or contain errors of fuzzy value, and monitoring target application to the discovery of the error.

According to whether network protocol adjacent digital packet content is related or not, we can put the agreement is divided into no state agreement and state agreement. No state agreement is refers to the network protocol between adjacent packet no context relevance, such as have multiple ICMP Request, each a separate Request. A state of the protocol is refers to between adjacent packets with context relevance. Such as RTSP (real time streaming protocol) agreement to terminate the session initial session there will be a series of related state changes, and the system may be introduced in a particular state will existence of loopholes. According to the agreement without state, fuzzy unit each input as an independent module; the state agreement, fuzzy device according to the state of the agreement to perform testing mechanism.

Using network protocol fuzzy device for fuzzy test, firstly, we need to study codes and standards of various agreement, in order to create a reasonable test data. At present, there are two plans of the most common network protocol fuzzy test: Plan 1 is the client and the server test mode, namely fuzzy device and the measured object being two end of testing process respectively. As shown in Figure 1 showed. At this time, the fuzzy device can serve as a client role, used to test the server program, such as the security of the Web service program. At the same time, fuzzy device can also act as the service role, used to test the safety of client program, such as fuzzy device can be DHCP (dynamic host dynamic host configuration protocol) server, used for testing the DHCP client safety.

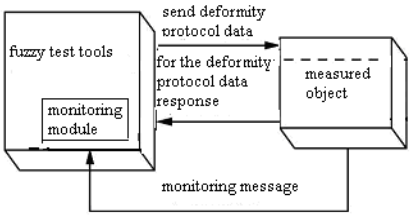

Figure 1. Network Protocol Fuzzy Test Plan 1

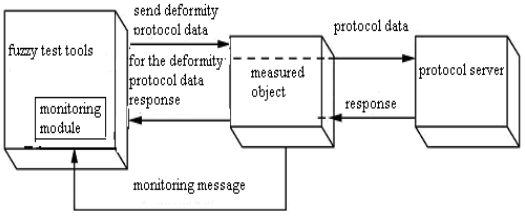

Figure 2. Network Protocol Fuzzy Test Plan 2

Plan 2 Network protocol fuzzy test plan is to test the equipment in the middle of the deployment of the network, such as the firewall, router, security gateway, etc. It was shown in Figure 2. Fuzzy device structure data to be sent to the protocol server process, the measured object being between the fuzzy apparatus and Protocol server to its play reorganization and analysis function, and once the restructuring and analytical process error, may cause the measured object appear abnormal state. Fuzzy apparatus of the monitoring module used to tested object of abnormal state for the collection, analysis, and ultimately positioning holes in. Through this method can find vulnerabilities of the measured objects in the process of network protocol processing.

3. For Wireless Network Protocol Wi-Fi Fuzzy Test Scheme

Below we will from the framework design, detailed technical implementation, fuzzy test process, and the defects of the packet formation and monitoring and so on several aspects expound wireless network protocol 802.11 vulnerability discovery fuzzy test framework.

3.1. IEEE 802.11 the Concept of the Agreement

The frame structure of the MAC layer and physical layer is defined as shown in Figure 3, the relationship between news and service defined by IEEE 802.11 is shown in Figure 4.

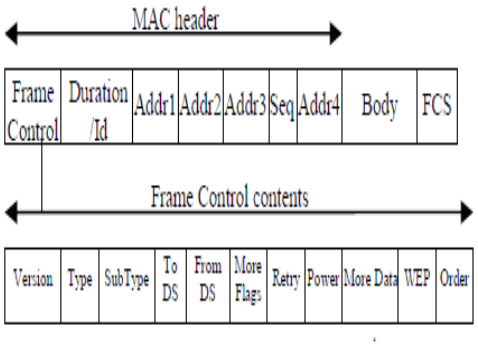

Figure 3. Generic Wi-Fi MAC Frame Former

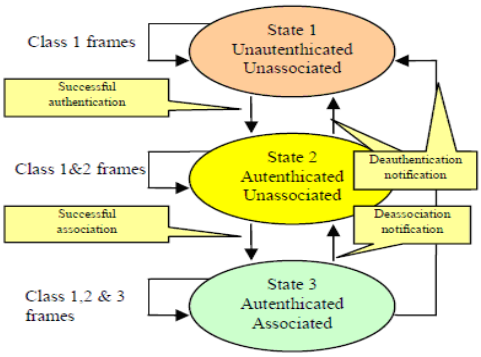

Figure 4. The relationship between IEEE 802.11 messages and the services

3.2. Wireless Network Protocol Fuzzy Controller Design Framework

Wireless network protocol fuzzy controller test object is mainly to the wireless connection device drivers bug location so as to achieve the purpose of eliminating these problems. We designed a new fuzzy test framework, which can produce deformity packet and implementation of the attack on the target system, and is independent of its transmission medium. The fuzzy testing framework consists of nine modules, as shown in Figure 5.

(6)Monitor: monitoring the state of an object is being tested. Mainly responsible for collecting and analyzing the response of the target equipment state, in turn, judgment target equipment whether there are abnormal situation. For example, if the response that destination

device returns is not in conformity with the RFC (request for comments), shows that abnormal in equipment. There are exceptional, monitor will report to attack controller.

(7) Measured unit: Optional components in the test unit monitoring program and the transmitter can exchange the status of the unit under test, to detect whether the attack was successful which is conducive to decide what should be implemented next attack.

(8) Access point: access point of optional component transfer device is used to generate and exchange legal packets what between access point and measured unit, which can observe in attack and real access point transfer the right data at the same time the behavior of the system.

(9) Holes confirm and analysis: Once you determine measured target exists fault, it is necessary to determine whether the Bug found can return, and after return successfully, you have to make further judgment whether the Bug can be used.

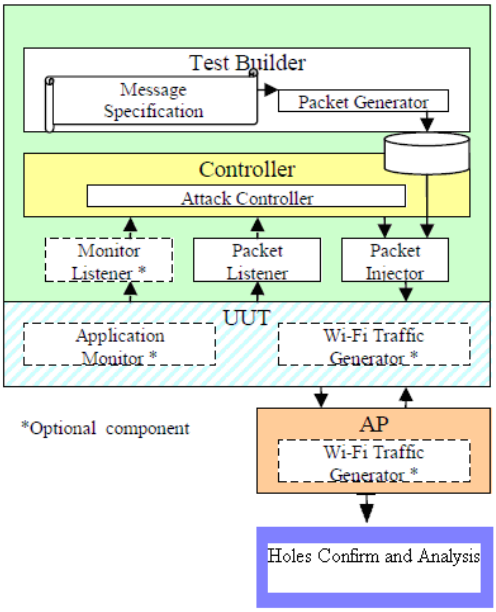

Figure 5. The Frame Structure of Wireless Network Protocol Fuzzy Controller

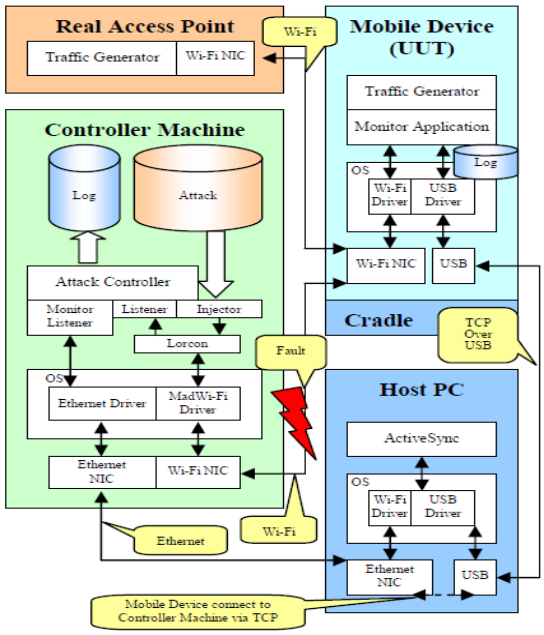

Figure 6. The Composition of the Test Equipment

3.3. Test Equipment Detailed Technical Realization

Test equipment is made up of four parts, as shown in Figure 6 shows.

(1) Controller: Controller formation contains the malformed data Wi-Fi packet (such as the cross-border value and repeat label), and through the Wi-Fi interface sent it to the measured unit, each data packets are sent several times to ensure that the measured unit can receive. At the same time, the controller monitoring test of the data and the collection of data stored in the hard disk for later analysis.

(2) Measured unit: measured unit is a Wi-Fi destination device. It runs a monitoring program can regularly connected to the controller of the monitor, and inform the current detected access point list and any existing link state.

(3) Host computer: Measured unit and host through the USB interface get connection, the host running Windows XP and Microsoft sync software, which can allow measured unit and host through the TCP protocol making communication on the USB, and host and controller is through the TCP protocol getting connection in LAN, thus, control program of measured in a unit need not take up Wi-Fi media and attack the controller interaction.

(4) The real access point: The real access point is installed in Windows XP on a ready access point application, it can make the measured unit experience Wi-Fi agreement of each

state, so as to ensure that controller coding complexity can be controlled, so specific data frame can be injection in each state.

3.4. The Implementation Process of Fuzzy Test

Use this framework implement fuzzy test process is as follows:

(1) Determine the target object

The task of this phase is to determine the measured object, to define the test range, usually need to consider the following questions: type of measured target, Such as measured goal is client or server program, is the application layer protocol or the network layer protocol, etc; The history of measured target whether appeared holes, and where the reasons for these vulnerabilities.

(2) Editing strategy

According to the characteristics of target, add new or modify existing data generation strategy. For example, to test the processing power of a network device Http (hyper text transfer protocol) protocol, Http protocol version can be edited, Method, Request-Header et al option data generation strategy. After you have finished editing strategy issued to the core engine.

(3) Generate fuzzy test data

The core engine uses a variation and modifies the default and other ways to generate malformed data. For example, the fields of network sniffer capture network packets to variation or modify, a particular field of network packets can be set terminator and invalid string operation and so on.

(4) Perform tests and monitoring

To perform testing is the process of running a particular test strategy. Data contract can choose the number of concurrent processes in the process, the order of the contract. Also start monitor to monitor the operation of the target.

(5) Holes confirm and analysis

Once you determine measured target exists fault, it is necessary to determine whether the Bug found can return, and after return successfully, you have to make further judgment whether the Bug can be used. The most commonly used means to reproduce the failure is the replay detection, which is packet replay tools will dump network packets to replay.

3.5. Data Formation and Abnormal Monitoring

First of all, this framework using optimization grouping method try to solve the deformity data to create inefficient. In order to clarify the data structure method, first make a concept, anomaly elements, Piece of data in this definition are used to excite the unexpected behavior of the measured target. A test case can contain one or more abnormal factors. Abnormal factors often damage protocol specification, but in some cases, its value is not illegal, this is to consider whether appropriate when testing the protocol implementation. The following the 802.11a protocol as an example to illustrate the process of the construction of the test data. It can be considered an 802.11a protocol test data is an Wi-Fi packet consists of fields, each field may be constituted by abnormal elements can also be constituted by the normal elements, namely a Wi-Fi packets can contain one or more abnormal factors. To achieve the purpose of the test, a test data should contain an abnormal factor, at least.

For instance, in the fuzzy test framework, Fuzz () function provide can provide the following means random generation any frame, even if you did not provide its value.

(1) In a beacon, whether to random fuzzy IE

frame=Dot11(proto=0,FCfield=0,ID=0,addr1=DST,addr2=BSSID,addr3=BSSID,SC=0,addr4=None)/Dot11Beacon(beacon interval=100,cap="ESS")/Dot11Elt()

(2) Whether to random fuzzy SSID beacon

frame=Dot11(proto=0,FCfield=0,ID=0,addr1=DST,addr2=BSSID,addr3=BSSID,SC=0,addr4=None)/Dot11Beacon(beacon interval=100,cap="ESS")/Dot11Elt(ID=0)

(3) Whether to random fuzzy 802.11 packets

Frame=Dot11 (addr1=DST, addr2=BSSID, addr3=BSSID, addr4=None)

The composition of the test cases was shown in Figure 7 shows.

The test data is a collection of a very large space, and the measured network equipment protocol defects is unknown. To test the entire collection, will consume a lot of time, so it is necessary to optimize the grouping of test data, to find a representative set of use cases.

Optimize the packet can be divided into known vulnerability, specify the value, particular option random values, and all data collection. Among them, one of the most important data generated is based on the characteristic of known exploits variation method, because loophole program that appeared in the history often still has weak point. Known vulnerabilities can be obtained from CNNVD, CVE (common vu-inerrability and exposures), CERT/CC (Computer Exigency Response Team Coordination Center) or Sequoia, etc, so that we can quickly find agreement in which there are security flaw, used as a deformity data generated reference.

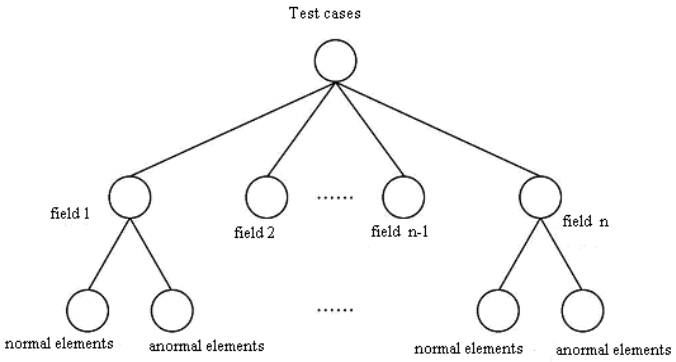

Figure 7. Test Data Component Diagram

3.6. An Example of Using the Fuzzy Test Framework Found a Bug Program

For example, using the fuzzy test method, bugs are found in a specific WPA tester, the content is as follows:

IE browser payload must have a valid WPA (OUI + Type + Edition),

Located in the holes of the code: net80211/ieee80211_wireless.c

It is defined in giwscan_cb () static buffer, as shown in Figure 8 shows:

```
#if WIRELESS_EXT > 14
        char buf[64 * 2 + 30];
    #endif

  #ifdef IWEVGENIE
  memset(&iwe, 0, sizeof(iwe));
  memcpy(buf, se->se_wpa_ie, se->se_wpa_ie[1] + 2);
  iwe.cmd = IWEVGENIE;
  iwe.u.data.length = se->se_wpa_ie[1] + 2;      butter overflow
#elsestatic const char wpa_leader[] = "wpa_ie=";
memset(&iwe, 0, sizeof(iwe));              encode_ie () vulnerable
iwe.cmd = IWEVCUSTOM;
iwe.u.data.length      =      encode_ie(buf,      sizeof(buf), se->se_wpa_ie,
se->se_wpa_ie[1] + 2,
wpa_leader, sizeof(wpa_leader) -1);
#endif
```

Figure 8. Defined in giwscan_cb () Static Buffer

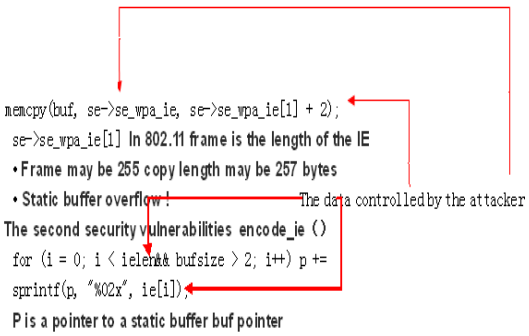

Figure 9. Security Bug Code

RSN and WME information element are the same code. The first security bug, as shown in Figure 9 shows:

Ielen is IE802.11 frame length, may be 257, if give it is not the appropriate value, static buffer will overflow.

These bugs are triggered due to a SIOCGIWSCAN, only abnormal 802.11 frame vulnerable code attack holes, SIOSIWSCAN will be triggered. If you scan the driver may analytic those abnormal 802.11 frame, but any other applications using wireless tool API will trigger bug.

3.7. This Framework Attempts to Use Reconnaissance Package to Monitor the Target Object

In the fuzzy test process, the most common target monitoring methods including simple observation analysis, reconnaissance bag recognition method, debugger tracking method, dynamic binary insert method, etc. In this framework using reconnaissance bag recognition method, namely to measure target to send a group of malformation test data, then into a normal/reconnaissance bag 0, through the analysis of the measured target for reconnaissance packet data response to monitor the operation of the measured target state.

Because of the measured object holes caused by system response set itself exists unpredictability, in this framework design process will monitor as a fuzzy controller is a program module, monitor in the following conditions appear when the object to be measured stress analysis to determine whether there are vulnerability :

(1) The response of the measured object does not accord with a standard or norms. For example, the measured object is a Web server, the fuzzy after sending a group of malformations test data is sent to the measured target host the a/Http Get0 request reconnaissance package, and recognized in the malformed packet before sending the next group received response, to determine whether the measured target system has malformed packets under abnormal. By default, the Web server should be according to the request to return to Http status code, see Table 1.

Table 1. HTTP Status Code

Status Code	Description
100 Continue	The client should continue to send the request
…	…
200 OK	Request has been successfully, response header that request desired, or the data body will be returned with this response
…	…
400 Bad Request	Contains a syntax error, the request can not be understood by the server
500 Internal Server Error…	The servers encounter an unexpected condition, ledding that it cannot complete the request processing…

If the response of the measured object reconnaissance package does not comply with the provisions of RFC, you can focus on analysis.

(2) Through the Syslog (recording system log mode), SNMP (simple net work management protocol) etc, detection measured object appeared in software and hardware of a serious disorder, such as system crash, restart, process, dead or output segment error, etc.

Need to mention is that through an automatic method to realize fuzzy test process monitoring is not mature, monitor process need some manual operation to fit.

4. Application Analysis

The following use of the fuzzy control framework to achieve the automatic detection of the Bug, test environment map can be found in Figure 10.

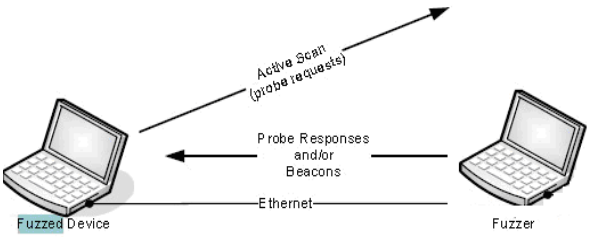

Figure 10. Bug Automatic Detection

In Windows, the key bug will trigger a BSOD (bluescreen crash). A script at any time to run on Fuzzing station ie ping Fuzzed-processing station, and sends a SIGINT, the victim can not respond. Figure fuzzer displays the last test --- triggered bug.

In Linux, bug will trigger dump kernel log (system log), there is a script run in the Fuzzed station, in the kernel message grep {oops | can not handle | assertion | panic} failure may have missed the non-function a wireless devices. A script at any time to listen to the radio probe request and send SIGINT and have no more probe request.

Fuzzy test process:

(1) Structure fuzzy test packets. According to the above description of the optimization of the test data, according to the known vulnerabilities y, specify a value of Y, specific options random value y, all data packet sequence, structure data packet.

Through the retrieval of the Wi-Fi protocol related historical vulnerability, we can find the related flaw of Wi-Fi protocol appears in the Wi-Fi protocol driver(such as CVE-2006-6651, CVE-2006-6332, CVE-2006-6125, CVE-2006-6059, CVE-2006-6055, CVE-2006-5972, CVE-2006-5882, CVE-2006-5710, CVE-2006-3992, CVE-2006-3509, CVE-2006-3508, etc.), Wi-Fi malicious allow remote attackers to cause denial-of-service command parsing overflow, malicious remote attacker could execute arbitrary code with the unknown vector by the Multiple SSID the INA Cisco vendor tag 802.11 management framework, based on the stack overflow, etc. During the test, the framework focusing on Wi-Fi protocol command options data variability, such as cross-border value and repeat labels, in the Wi-Fi agreement related field fill some illegal character.

(2) Perform tests. Send a test packet in accordance with the order of the optimized data, all the historical vulnerabilities packet to send all other packet to be sent in accordance with the generated sequence, open the log function measured security gateway, and capture the replay of the interactive process.

(3) Monitoring found that the problem. Send reconnaissance package in the testing process, monitoring the measured object, each sending 10 abnormal packet, and then send a normal RTSP request. At the same time with the network sniffer, target system log function and resource management functions to monitor them. Tests found that measured security gateway appeared many system is down machine and restart phenomenon.

(4) Reproduction. According to the fuzzy test system design requirements, once found measured target failure, you need to save network communication process, used in the replay detection. During the test process, the fuzzy unit captures and save the 31 network interactive process data packet. Statistical results such as shown in Table 2.

Table 2. Statistical Results

name	Occurrence numbe
1.ieee80211_ioctl.c Integer overflow	1
2.Apple Mac OS X 10.3.9 and 10.4.7 AirPort in wireless driver Multiple stack-based buffer overflow	2
3.Apple Mac OS X 10.4.7 AirPort of wireless driver API integer overflow	4
4.Through the 802.11 response frame contains Broadcom BCMWL5. SYS wireless device Drivers Based on the stack buffer	20
5. Intel 2200 bg802. 11 wireless Mini - PCI driver Denial of Service Attacks Incidents total	4
	31

The 31 interactive data packet to replay testing, we found that security gateway all appear to restart phenomenon. From the statistics we can see, all 31 processing error is all due to Wi-Fi agreement wireless drive contains deformity content processing error by.

(5) Positioning holes. Vulnerability detection personnel analysis assessment of these issues, at the same time informs the research development of security gateway vendor to help them as soon as possible to locate the problem and repair. From the results of developer's feedback, they have positioning of the holes, and have completed the security patches.

5. Conclusion

This paper introduces the basic concepts in fuzzy test; we study and design a framework of fuzzy test technology for the wireless network protocol vulnerability discovery Practical tests show that if the framework working in black box testing methods could find existing network protocol in wireless. This also proves that fuzzy test can be better applied to the black box of vulnerability discovery.

Acknowledgements

This work was supported by Henan provincial natural science foundation research project.

References

[1] Ayewah N, Hovemeyer D, Mergenthaler JD. Using static analysis to find bugs soft ware. *IEEE Soft ware*. 2008; 25(5): 22-29.
[2] ABHISHEK K, SANTHI T, CAMANILO G. A Novel Approach for Evaluating and Detecting Low Rate SIP Flooding Attack. *International Journal of Computer Application.* 2011; 26(1): 31-36.
[3] Wondracek G, Comparetty PM, Kruegel C, Etc. *Automatic network protocol analysis*. Proceedings of the 15th Annual Network and Distributed System Security Symposium. 2008; 77-84.
[4] Banks G, Cova M, Felmetsger V, et al. *Toward a stateful network protocol fuzzer*. Proceeding of the 9th Inform at ion Security Conference (ISC). 2006.
[5] Huang YW, Huang SK, Lin TP, et al. *Web application security assessment by fault inject ion an d behavior monitoring*. Proceedings of the 12th International World Wide Web Conference. New York, NY, U SA: ACM Press. 2003; 148-159.
[6] Kaksonen R, Laakso M, Takanen A. *Soft ware security assessment through specification mutations and fault injection*. Proceeding of Communications and Multimedia Security Issues of the New Century. 2001.
[7] Oehlert P. Violating Assumptions with Fuzzing. *IEEE Security and Privacy*. 2005; l3 (2): 58-62.
[8] CHRISTIAN S, STEFAN T, KARIN P, etc. Security Test Approach for Automated Detection of Vulnerabilities of SIP-based VoIP Soft phones. *International Journal on Advances in Security*. 2011; 4(1&2): 95-105.
[9] Agrwal Sudhir, Jain Sanjeev, Sanjeev Sharma. A Survey of Routing attacks and Security Measures in Mobile Ad Hoc Networks. *Journal of Computing.* 2011; l(3): 41-48.
[10] Ehsan Hearn, Mohammad Jail Piranha. *SELECTOR: An Intelligent Evaluation System for Routing Protocols in Wireless Ad Hoc and Sensor Networks*. Proceeding of 3rd International Conference on Electronics Computer Technology, ICECT. Kanyakunari, India. 2011; 300-305.