Development and Implementation of Anti Phishing Wi-Fi and Information Security Protection APP based on Android

Tianjun Chen*, Dexin Kong, Yuxin Hong

College of Overseas Education, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, 210023

*Corresponding author: tianjunchen@njupt.edu.cn

Abstract. In the era of information revolution, China's Internet construction has achieved unprecedented development. However, in the current public WiFi, the proportion of phishing WiFi with high risks is very high. This paper designs and implements a tool to detect wireless network security. It starts with the following: attack, defense, and detection. Firstly, based on the key technology of wireless attack, five functional modules of wireless attack system are designed. Then, by analyzing the shortcomings of traditional detection methods, a lightweight phishing attack detection scheme for the public is explored. The scheme is based on TMM algorithm and HDT algorithm. Finally, a phishing attack detection tool for operator network is designed and implemented based on the scheme, which can provide consumers with basic user information to connect WLAN, and detect the network effectively. The results show that all functions of the detection tool designed in this paper can run normally. It can meet the detection requirements of wireless phishing AP in the current environment and achieve the expected purpose, which has extensive market value and good scientific significance.

Keywords: component; WLAN; Free WIFI; Wireless Network Security; Phishing.

1. Introduction

1.1. Background:
In the era of information revolution, China's Internet construction has achieved unprecedented development. As a part of Internet access, WiFi has gradually become an indispensable part of social life. According to data released by iPass, China ranked fourth in the world in the number of WiFi hotspots in 2015, with more than 50 million public WiFi hotspots. However, WiFi network security problems are becoming more serious. In the current public WiFi, the proportion of phishing WiFi with high risks is very high. At present, these public WiFi has become an emerging channel for criminals to steal users' privacy and cheat users out of money. According to the report of the second National Cyber Security Awareness Week in China, the economic losses caused by free phishing WiFi traps are as high as 5 billion yuan every year. Therefore, the research on anti-phishing WiFi is imperative.
1.2. Contemporary work

In the field of attack research, the attacks against the bottom layer mainly include the interference of MAC and PHY and the spoofing attack. MAC interference types include selective collision request sending / allowing sending, data / ACK, etc. Its principle is to use the unique transmission mechanism of data link layer to cause channel blocking. Full frequency jammer with variable interference range proposed by Liu Yonglei, Jin Zhigang, etc., and use 802.11g wireless signal cross mechanism to achieve the function of a wireless channel interfering with all channels. As for high layer attack, the research team of China's Zer One group launched the "wireless encryption WPA / WPA2 distributed cracking project" in 2008.

All the above researches are based on the bottom layer attack, there are also many high layer attacks. In 2001, Itsik Mantin and others published an analysis report on RC4 encrypted data stream cracking, and pointed out the feasibility of the cracking scheme. The subsequent FMS attacks provide sufficient evidence for the feasibility of this solution. Compared with the WEP encryption, the WPA / WPA2 encryption is still in its infancy, with few tools and a single way.

In the field of defence research, Gu Yang and his group proposed the detection technology of phishing AP based on wireless device's characteristic fingerprint, which uses the inherent characteristic fingerprint of wireless device to distinguish phishing AP. Sheng Y, Tan K proposed to build a fingerprint database about RSS signal strength to detect phishing AP by collecting RSS signal value of AP and using Gaussian mixture model. During the detection, the RSS of the target AP is collected, and the RSS value is matched with the established fingerprint database. If the corresponding RSS information of the AP is not found in the fingerprint database, the AP can be determined as a phishing AP.

For an individual user, the above scheme is not easy to implement, so a mass oriented, user-based lightweight detection scheme is needed.

We develop an Android based app with pretty interface, reliable WiFi security test and information security. Specifically, we will call the mobile phone sensor to detect the nearby AP, then use the network means to track its address, IP, other network parameters and then carry out security analysis to evaluate the security of the nearby AP. Then the system automatically block the data transmission when detecting the risk of intrusion.

2. Principal of phishing AP

An attacker can easily set up a phishing AP. First, a wireless AP is built through simple configuration of a laptop with some analysis software. Second, the attacker then consigns the same SSID, MAC address, channel, and encryption as a legitimate AP. Finally, wait or entice a legitimate user to connect to a phishing AP. According to the IEEE802.11 protocol standard, the closer a wireless phishing AP is to the user, the more likely it is to succeed. When there are multiple aps with the same configuration around, the wireless client will select the AP with the strongest signal to connect according to the wireless network card. Therefore, as long as the attacker has the same information as the legal AP and improves the signal strength or gets closer to the victim, it is easier to achieve the attack effect.

Attackers often set up fishing aps near shopping malls, hotels, cafes or libraries. By phishing AN AP, an attacker can intercept users' sensitive information, such as account and password, by launching a man-in-the-middle attack. You can also manipulate DNS servers or control routers to launch phishing attacks.

2.1. Attack method:

2.1.1. Active Attack. Active attack is that phishing AP sends false connection cancellation request frame to the attack target so that the target device breaks connection with the real AP. Then, the punishing AP will get connected with the target device. The target user use punishing AP to surf the internet with a danger that all the data flows pass through punishing AP. The hacker can get information from those data flows. Attackers need to cooperate with DoS attack to achieve the goal after building phishing AP.

DoS attack can be divided into four types.
1) Authentication Flood
The attacker first uses randomly generated MAC address to pose as virtual wireless users, and then uses these virtual wireless terminals to send a large number of false requests to the target wireless access point. A large number of user authentication request frames will consume the memory of the wireless access point, at this time, it will disconnect the association with the connected users. This attack mode is only applicable to APs with small number of users.

2) Deauthentication Flood
It transfers the user’s wireless device from state three to state one by sending the authentication cancellation frame to it by posing as the legitimate wireless access point. Then, the client is disconnected from the legitimate wireless access point. Generally, after the user's wireless device finds that the network connection is disconnected, it will request the wireless access point for re Association and authentication again, so as to obtain the network service again. The attacker can use this method to repeatedly send the authentication cancellation frame to the user equipment, so that all the user equipment can get a long time of denial of service.

3) Association Flood
Wireless access points have a "connection status table" that stores information about connected devices. The attacker attempted to fill in the "connection status table" of the access point by sending a large number of connection requests from virtual wireless devices. When the table overflows, no one can connect again.

4) Disassociation Flood
It transfers the state 3 of the wireless device to the state 2 by sending the disassociation frame to the legitimate wireless device by posing as the legitimate access point. When the user's wireless device finds that the network connection is disconnected, it will request the wireless access point for re Association and authentication again, so as to obtain the network service again. The attacker can use this method to repeatedly send the disassociated frame to the user equipment, so that all the user equipment can get a long-term denial of service.

By launching DoS attack to break the connection between target user and legitimate wireless access point. The user’s wireless device will get connected to the punishing AP. Just set the name of Punishing AP to the name of legitimate AP. Because the process of client switching the AP with the same name is completed in the system, the AP with the strongest RSSI will be connected without display by default.

2.1.2. Passive Attack.
Attackers cheat wireless devices by setting up a false access point with the same SSID, same channel and encryption mode as the legitimate access point, which usually has stronger RSSI than the legitimate access point. Within its signal coverage, the wireless terminal will automatically connect to the false access point.

2.2. Fishing ap establishment:
In order to construct a fishing WIFI, we need to have wireless network adapter, Kalilinux operating system, isc-dhcp-server, Airtrack-ng suite which used to send data, SSL strip which used to break through SSL encryption, Ettercap which used to sniff hijacking.

1) Install DHCP Service
We use language “apt-get install isc-dhcp-server” to install DHCP service. Then we need to configure some files. The configuration files are in / etc / default / ISC DHCP server and / etc / DHCP respectively / dhcpd.conf. The former can be configured with listening port, here take WLAN 0 as an example. After configuring the DHCP file, disconnect the WLAN 0 network and assign an IP address, for example “ifconfig wlan0 192.168.1.2/24”.

2) Launch DHCP Service
Here, we apply language “service isc-dhcp-server start”.

3) Build Hot spot
First of all, we need to add execute permission and then AP establishment, DHCP establishment, sslstrip opening, ettercap opening.
3. App detection ideas
Existing wireless AP detection tools are basically based on the SSID and encryption method to determine the reliability of wireless hotspots. These methods have obvious disadvantages and cannot effectively identify the pseudonymous hotspots in the same environment. When the same SSID access points exist in the wireless environment, if two access points of the same information, and users have been connected one of the hotspots, so wireless terminal will automatically choose the strongest connection RSSI AP, the operating system determines the different AP belong to the same organization, with the same SSID not do judgment of different access points. A phishing AP is naturally stronger than a legal AP in order to lure victims. Another way to detect false hotspots is to establish a database by collecting information about security access points, and then compare the information about access points stored in the database to determine whether the hot spot manufacturer and geographic location information are consistent with the information in the database. However, the information in the database is limited and time-sensitive, so not all access point information can be saved in the database, and it is easy to misjudge a legitimate access point as an illegal access point.

The detection system in this paper firstly uses fingerprint characteristics of wireless network to judge step by step, and finally uses TMM and HDT to detect the extra number of wireless hops in the wireless link to conduct depth detection of phishing WiFi. This method can accurately detect the phishing AP with high camouflage and prompt the user to ensure the security.

3.1. HDT
In HDT algorithm, both server IAT and the ratio of server IAT and AP IAT are used as the judgement basis. In HDT algorithm, ratio of server IAT and AP IAT is defined as SAIR. Assume that $\alpha$ is SAIR and $\sim{\Delta A}$ is IAT of AP. And $\alpha, \Delta A$ are which in ideal condition.

$$\alpha = \frac{\Delta A}{\Delta A}, \quad \tilde{\alpha} = \frac{\tilde{\Delta A}}{\Delta A}$$

![Figure 1](image)

**Figure 1** AP IAT illustration in an ideal network environment

Based on IEEE 802.11 standard, the average value of $\alpha$ is theoretically differentiable between the normal AP scenario and the attacked scenario, and therefore can be used to effectively detect double evil attacks.

$$E(\tilde{\Delta A})_{\text{one-hop}} = 2T_{\text{DIFS}} + 2T_{\text{SIFS}} + 2E(t_{\text{up}}) + L_{\text{ACK(MAC)}} + L_{\text{ACK(TCP)}} + L_{\text{F}}$$

There are two theorems in IEEE 802.11.

Theorem 3: in one-hop channel, as for 802.11b, $E(\alpha_{\text{one-hop}}) \leq E(\tilde{\alpha}_{\text{one-hop}}) = 1.00$. As for 802.11g, $E(\alpha_{\text{one-hop}}) \leq E(\tilde{\alpha}_{\text{one-hop}}) = 1.11$.

Theorem 4: in two-hop channel, as for 802.11b, $E(\alpha_{\text{two-hop}}) \geq E(\tilde{\alpha}_{\text{two-hop}}) = 1.74$. As for 802.11g, $E(\alpha_{\text{two-hop}}) \geq E(\tilde{\alpha}_{\text{two-hop}}) = 1.94$.

These two theorems provide us strong evidence that $\alpha$ can be used to divide normal AP and punishing AP. Because normal AP’s $\alpha$ is smaller than punishing AP’s.

3.2. TMM
By collecting IAT of the server, it creates IAT sequence and then processes the sequence to get threshold. If the threshold value can match the characteristics of single hop wireless link, it can be concluded that
the wireless user uses the single hop access point for data interaction with the server, that is, it can be determined that the access point is legal, otherwise, it is determined that the access point is phishing.

In the process of data training, the second average technology is used to get the detection threshold value. The specific steps are as follows: 1) Obtain the server IAT in the single hop wireless link; 2) Calculate the mean and standard deviation of IAT in the case of single hop wireless link, expressed as $u_{1,\text{NAP}}$ and $\sigma_{1,\text{NAP}}$; 3) filter out IAT beyond the range of $[u_{1,\text{NAP}} - \sigma_{1,\text{NAP}}, u_{1,\text{NAP}} + \sigma_{1,\text{NAP}}]$; 4) by using the remaining IAT values to calculate the secondary average value from $u_{2,\text{NAP}}$. 5) In the same way, the second average value of IAT in the case of two hop wireless link is calculated. 6) The average value $T_{\theta}$ of $U_{2,\text{EAP}}$ and $U_{2,\text{NAP}}$ is calculated. As a boundary value to distinguish whether to communicate with the server through single hop wireless link or two hop wireless link. In addition, we also need to calculate the server IAT in the case of legitimate access point from $T_{\theta}$. The percentage of deviation in this case is expressed as $P_1$. Then the percentage in the case of phishing attack access point is calculated, and the probability in this case is expressed as $P_2$. Then a logarithmic likelihood is obtained by SPRT technique.

Here are some variables that need to be used in the detection phase: combine the collected server IAT into a sequence, and use $\{\delta\}_{i=0}^{n}$ To show. Use $y_i$ to indicate whether the IAT value of the i-th server belongs to phishing attack. Its value is a binary variable (0, 1). That is to say, if $\delta_i \geq T_{\theta}$, then $y_i = 1$ is judged as phishing attack; otherwise, $y_i = 0$, it is the working condition of legal access point. Through the above judgment, we get another sequence, $\{y_i\}_{i=1}^{n}$, which indicates that the judgment result is a phishing access point and a sequence that is a legal access point. In a real wireless environment, suppose $H_0$ Sequence is a set of legitimate access points, $H_1$ sequence is a collection of phishing access points. We can obtain $P(y_i = 1 | H_1) = \theta_1$ and $P(y_i = 1 | H_0) = \theta_0$. We assume $\theta_0 = P_1, P_1 = p_2$, then we can get log-likelihood ratio $A_n$:

$$A_n = \ln \frac{P_{y}(y_1\ldots y_n|H_1)}{P_{y}(y_1\ldots y_n|H_0)} = \frac{\prod_{i=1}^{n}P_{y}(y_i|H_1)}{\prod_{i=1}^{n}P_{y}(y_i|H_0)} = \sum_{i=1}^{n} \ln \frac{P_{y}(y_i|H_1)}{P_{y}(y_i|H_0)}$$

According to SPRT technology, this section calculates the log likelihood ratio by random walk of the threshold value calculated from the training data. If $y_i = 0$, reduce its length by $\ln(1 - \theta_1) - \ln(1 - \theta_0)$, if it $y_i = 1$, add $\ln(1 - \theta_1) - \ln(1 - \theta_0)$.

Suppose $f_a$ and $f_p$ are the error rate and misjudgment rate of wireless client selection, respectively. In each random, if it meets $A = \ln f_a - \ln (1 - f_p)$, then it is valid access. If $B = \ln (1 - f_a) - \ln f_p$, then it is regarded as phishing access.

4. RESULT

This is our app interface. Our programming concept is based on simplicity. So our interface only retains the necessary information. A simple list of all available WiFi. When a user tries to connect to a WiFi, the program will detect the WiFi. If the detection result is dangerous, the connection will be terminated directly. When WiFi is secure, the display is as shown in the figure.
By detecting the legitimate AP and the fake AP established in this paper, the experimental results show that the phishing AP attack detection system is used to test the phishing AP attack, and the average detection success rate reaches 97.5%. After code optimization, some reasons for detection failure were found out:

Sometimes the program searching wireless network will appear loop phenomenon. When there are too many wireless access points around, the module program will appear search dead loop phenomenon.

For wireless AP with low RSSI, the sent detection frame is not responded for a long time, which may cause errors in subsequent detection.

To sum up, the phishing attack system of wireless access point can quickly realize covert phishing attack and successfully steal user information. The phishing WiFi detection system based on the client has a success rate of 97.5% in the detection of operator type phishing AP, and can accurately detect phishing attacks.

In the era of information revolution, WiFi has gradually become an indispensable part of social life. However, due to the openness of wireless Internet, people's security and privacy are very vulnerable to be infringed. This paper builds a phishing attack platform by studying the phishing attack and detection technology of the existing wireless network, and builds an Android-based PHishing WiFi detection and prevention APP based on TMM algorithm and HDT algorithm. Due to other factors such as time, the project in this paper also has some defects. After being prompted to connect to risk WiFi, although WiFi will be forced to be disconnected, there is no reporting function, and risk warning is not marked on the name of WiFi, which may cause the user to connect wrongly again. In future studies, the detection of phishing attacks should be extended to more types of malicious AP detection. In the future, with the enhancement of network security protection technology, users will get more reliable and convenient Internet experience.

References
[1] YuHuawei, “Research and implementation of wireless fishing detection technology based on client”, unpublished.
[2] Dushuqin, YiQ, “Wlan security system based on the 802.1 and AES [C]”, International Conference on Computer Application and System Modeling, IEEE,2010:V6-102-V6-105.
[3] Adam Stubblefield, John Ioannidis, Aviel D.Rubin, “Using the Fluhr Mantin and Shamir Attack to break WEP[J]”, Network and Distributed System Security, 2001:1-8.
[4] Lynn M, Baird R, “Advanced 802.11 attack [J]”, Black Hat Briefings,2002.
[5] Zisiadis D, Kopides S, Varalis A, “al.Enhancing WPS security [C]”, Wireless Days, IEEE,2013:1-3.
[6] Wiedmann U, Lillie TL, Sneiderman RP, “Methods and systems for automated configuration of
802.1x clients”, U.S. US 8019082 B 1 [P], 2011.

[7] Sheng Y, Tan K, Chen G, “Detecting 802.11 MAC layer spoofing using received signal strength [C]”, INFOCOM 2008, The Conference on Computer Communications IEEE, IEEE, 2007:1768-1776.

[8] James S, Kasera SK, “On fast and Accurate detection of unauthorized wireless access points using clock skews [J]”, IEEE Transactions on Mobile Computing, 2009, 9 (3): 449-462