Vulnerability Testing of Wireless Access Points Using Unmanned Aerial Vehicles (UAV)

Vemi, S.G. and Panchev, C

Vulnerability testing of Wireless Access Points using Unmanned Aerial Vehicles (UAV)

Stephen Gergo Vemi, Christo Panchev

University of Sunderland, Sunderland, United Kingdom

vemi01@hotmail.com

christo.panchev@sunderland.ac.uk

Abstract: Wireless networks are essential part of our everyday life – we are using them at home, workplace, cafe shops and many other public places. Moreover, people trust such connections and readily use them to transfer sensitive information. With an explosive increase of their use we need expand the aspect of evaluating the security issues wireless networks. Majority of household are using the latest secured protocols the WPA2 with a government grade standard nowadays. These protocols are still vulnerable to dictionary attacks that are normally carried out by recording three-way handshakes between the wireless router and the connected client. This method is really common and widely used – its success depends on the strength of the password being used. The research presented here shows another efficient method of hijacking and breaking into home networks is by using a Man-in-the-Middle type attack. The proposed system is implemented on a Raspberry Pi carried by a drone. While until recently UAV's (Unmanned Aerial Vehicles) have been used mainly by militaries and some specialist organisations, nowadays they have become widely available, cheaper and user friendly. The use of a drone allows the system to cover a wide area of potential targets as well as relatively quickly move from one target and WiFi network to another. The system is based on war flying using commercially available drones (Wang, 2006). The main goal of this project is to be able to hijack a wireless connection session between a connected tablet PC and Access Point using WPA2 encryption. We will be able to automate a Man in the Middle attack just by flying the drone around a certain area, setting up a rogue access point and being able to harvest important credentials from the targeted wireless networks and connected devices. The system is based on a number of open source Wi-Fi penetration testing and configuration tools including iwconfig or airmon-ng and custom scripts. The drone payload (Raspberry Pi B+) is using two wireless dongles; one for monitoring the wireless networks and the other one for being the rogue access point. The Raspberry Pi is powered by a 1000 mAh battery and carried by a DJI Phantom Drone. The device is also capable of other types of attacks. Such as disconnecting devices from its currently connected networks or causing denial of service attack against wireless routers/hubs while remaining stealthy to the victim(s) and operating from a distance.

Keywords: drone, hijacking, wireless, raspberry pi, evil twin, rogue AP, war flying

1. Introduction

WPA and WPA2 are two similar security protocols mainly introduced after WEP's security has been proven inadequate. It was developed by Wi-Fi Alliance to enhance security o wireless networks. WPA refers to the IEEE 802.11i standard since 2003 and WPA 2 was introduced a year after in 2004 named IEEE 802.11i-2004 standard. People were able to relatively quickly implement the new security protocol by updating firmware on wireless network interface cards and then switching from WEP to WPA.

The new protocol called Temporal Key Integrity Protocol (TKIP) dynamically generates a new unique 128-bit for each packet being transferred. WPA includes a message integrity/spoof protection called Michael which was later upgraded with a new protocol called TKIP. TKIP includes a counter measure mechanism that detects attempt to break TKIP and block the attacker. TKIP is no longer considered as secure since 2012 on a revision of the 802.11 standard.WPA2 has replaced WPA and since 2006 WPA2 is a mandatory for all newly produced Wi-Fi devices. The new standard has two main new features such as CCMP and a new ARS-based encryption mode for a stronger security. WPA 2 is secure but still vulnerable to dictionary attacks conducted by recoding the 4-way handshake when the user gets connected to the AP and then running brute force attack against the collected file while using a list of random words. But this method is highly time-consuming. WPA2-ENT is made for enterprise networks and it's the most secured wireless protocol that requires RADIUS (Remote Authentication Dial In User Service) application.

The other weak point of WPA/WPA2 is WPS PIN (Wi-Fi Protected Setup). This feature enables users to join the network by entering an 8 digit PIN or pushing a button on the device. With this feature enabled system can be compromised within hours using tools such as Reaver or Wifite. Users have been advised to disable this feature as it comes turned on by default. (Mati, 2009) Another weakness of these secured protocols and mainly the users is attack method called Man in the Middle attack. Dencrypti passwords can take a very long time; MITM is the best possible solution for achieving high rate of success in wireless penetration testing against WPA2 within a short time span.

2. Methodology

In computer security and cryptography the man in the middle attack (MITM) is a method based on a sequence of actions consisting of capturing, altering or injecting messages into a communication channels between two end-points. This method requires the attacked to have the ability to monitor both communication channels and intercept all relevant messages and inject the new ones. One example of such attack consists of scenario where attacker sits between two communication end-points while the victims are forwarding messages to each other. The attacker is then capable of monitoring or even changing the content of each message. In order to avoid detection attacker acts as a proxy between the victims. However it requires high level of knowledge and it only can work if the attacker can impersonate each endpoint of the attack (Chen et al., 2007).

2.1 Payload – Raspberry Pi

Raspberry Pi The Raspberry Pi is a low cost, small credit-card sized multi-purpose computer (Stefan, 2013). It was created by Raspberry Foundation under two main figures Eben Upton and David Braben in England. It has all the essential ports such as HDMI for display connection, Ethernet port for wired network connection and number of USB ports depending on the model. It has a 700 MHz arm processor made by Broadcom - which can be overclocked with use of modified kernel to around 1GHz - and 512 MB of RAM. There are number of operating systems freely available to download from the official Raspberry Pi website. NOOBS has been released for supporting the development of the project by providing different range of Operating systems and purpose built firmware's such as Raspbian which is a modified version of a Linux Debian. In conclusion Raspberry Pi's B+ will be the best solution for the payload device since it is a relatively light weight and provides good computing capabilities.

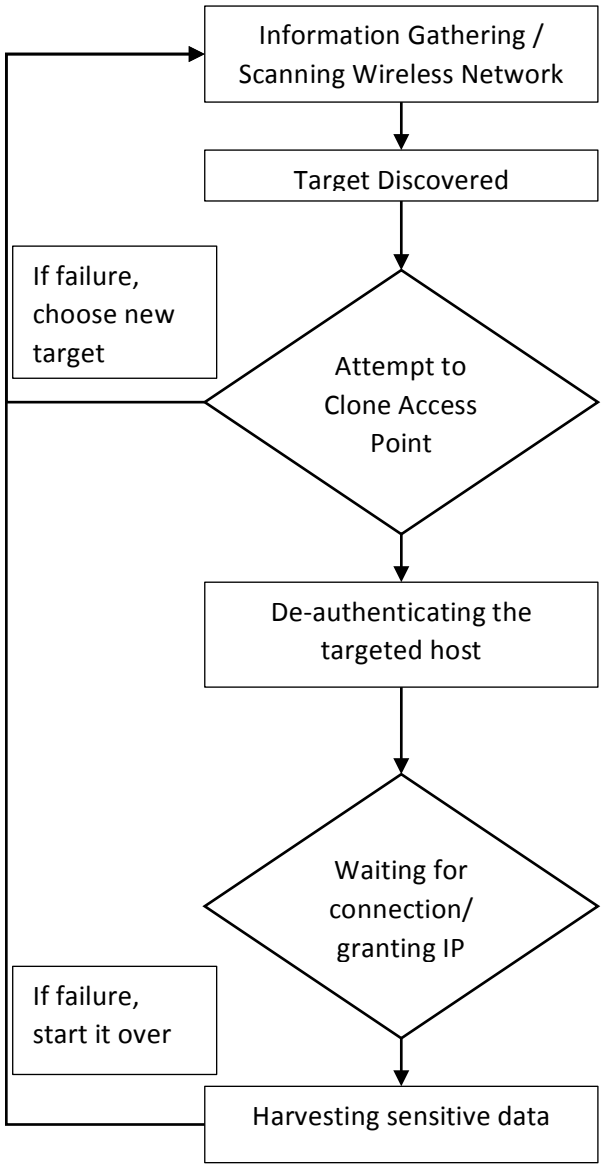
2.2 Required Configuration

As for the setting up the rogue Access point many different software tools such as dhcp or airmon-ng have been used. First of all the main part of this system is having a reliable AP with DHCP and DNS service installed and configured. For the DHCP service an application called dhclient been used. In this case the DHCP service is issued under 192.168.1.0/24 subnet. The configuration of the interface also needs to be changed according to the target's ESSID and changing the interface mode to master. All of which is a standard configuration for an interface acting as AP. There is one additional thing that we need to be change that is the "key" setting which represents the password that the victim would be using to get access to this rogue AP. So we set this to "off" which means that anyone will be able to get access to this network. For configuring the wireless interface "iwconfig" has been used.

The second wireless interface is working in a monitoring mode, scanning for available targets (APs) and their connected devices. Turning the wireless interface into monitoring mode can be done by using "airmon-ng". Once monitoring interface is up and running "airodump-ng" can be used for monitoring and capturing packets. Airodump-ng is also capable of distinguishing between multiple APs and their connected hosts.

Once the target has been selected the script will automatically change the ESSID of the primary network interface to the targeted AP one and it will start to inject ARP packets for de-authenticating the clients from its legit wireless access point - the one which ESSID it took. If the rogue AP's signal strength is higher than the original AP then the victim's device will automatically get connected to our wireless network.

User should not notice anything from the attack, unless the device notify it. The DHCP service will grant a suitable IP for the connected device. In order to remain stealth the solution can grant internet access to clients using a mobile device 4G network which will not disrupt the service. This could be done by modifying the port-forward settings of the device ("Kali Linux Evil Wireless Access Point," 2015).



3 Live Test Results

For the initial testing an Android tablet and a wireless hub been used. The script with the combination of tools explained above is able to hijack wireless connection from the tablet and automatically create a rogue access point accordingly to the target and it's connected AP. The device gets disconnected from its original router and due to stronger wireless signal of the rogue AP the victim will automatically get connected to the fake AP. The device only been tested against ordinary home routers so far but based on the tests results the host devices are the risk factors and not the APs. Since the victim is using the rogue network the attacker is able to monitor everything what the user does while it's connected to the wireless network. By using a drone the device will become more mobile and capable of covering a larger area. The drone could have a GPS system installed and it could fly autonomously simply following a pre programmed route. Once it's finished all the gathered data will be available to the attacker for revision. The preliminary test results can be seen in Table 1.

Vulnerability testing WAP 2 using rogue Access Point (preliminary test results)				
Testing	**Input**	**Expected**	**Actual**	**Working?**
Script load	Turning on the device	Booting up the device and runs the script	Booted and executed the	Yes

	and running the BASH script	automatically afterwards	script as expected	
Wlan0 – Monitoring mode	Part of script –automated	The script switches the wlan0 interface to monitoring mode	Changed to monitor mode as expected	Yes
Wlan1 – configure local Access Point settings	Part of script –automated	Creates a AP with all the configurations and also turns the interface to master mode	Access Point up and running	Yes
Looking for targets	The script looking for possible targets with connected hosts	Creates list of AP's and their hosts	Created the list and their hosts	Yes
Cloning the victim AP	The AP with the strongest signal will get selected	The AP's ESSID and BSSID gets cloned according to the list	It did clone the AP's ESSID and BSSID	Yes
Sending de-authentication packets to the selected target	The closest target gets selected by signal strength and its AP	The selected device get de-authenticated from its wireless access point	The device got de-authenticated	Yes
Get connected	The clone AP is waiting for connection	The rogue AP lets the user to get accessed to the wireless network	The victim got accesses to the network	Yes
DHCP service	The DHCP service is waiting new connection	The victim will be granted an IP address under 192.168.0.0/24 address	The victim got accesses and granted an IP address under 192.168.0.3	Yes

Table 1. Test results

4 Conclusions

Our initial results show that the proposed model is capable of hijacking WiFi sessions and potentially mounting a Man-in-the-Middle attack on APs and connected client devices. The design of this war flying WiFi-sniffing machine is providing high manageability and relatively

cheap solution. Previous case scenarios have already proven its functionality and efficiency. The system combines the functionality of war flying and it improves it by making it financially available and also easily manageable. Drones have made concerns all over the globe and they will have huge impact on our future without the making or right Air regulations. Future plans in terms of functional improvements of the artefact include implementation of a GPS tracking/guiding system as well as a completely automated system for cloning APs. With the right tools and features the device could become completely autonomous and areal.

References

Chen, Z., Guo, S., Zheng, K., Yang, Y., 2007. Modeling of Man-in-the-Middle Attack in the Wireless Networks, in: International Conference on Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. Presented at the International Conference on Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007, pp. 2255–2258. doi:10.1109/WICOM.2007.562

Kali Linux Evil Wireless Access Point [WWW Document], 2015. URL https://www.offensive-security.com/kali-linux/kali-linux-evil-wireless-access-point/ (accessed 1.28.15).

Mati, 2009. BackTrack WiFu AN INTRODUCTION TO PRACTICAL WIRELESS ATTACKS V.2.0 BASED ON AIRCRACK-NG. Offensive Security.

Stefan, S., 2013. Raspberry Pi for Secret Agents. PACKT.

Wang, W., 2006. Steal this Computer Book 4.0: What They Won't Tell You about the Internet. No Starch Press.