Wi-Fi Direct to Hell

Attacking Wi-Fi Direct Protocol Implementations

Andrés Blanco
6e726d@gmail.com

Abstract

Today Wi-Fi is everywhere and is by far the most widely used wireless networking protocol. During the last couple of years, Wi-Fi security research was mainly focused on WPA/WPA2 security mechanisms. But modern Wi-Fi firmwares and drivers support several protocols that could be targeted by attackers. This is the case of Wi-Fi P2P, also known as Wi-Fi Direct. This protocol provides the ability to discover nearby devices and connect directly to each other via Wi-Fi without an intermediate access point.

Keywords: Wi-Fi Direct; Wi-Fi P2P; Wi-Fi Alliance; Network Security

I. Introduction

On April 2010 the Wi-Fi Alliance[3] released the first public version of Wi-Fi- Peer-to-Peer (P2P) Technical Specification; this document defines the architecture and protocols in order to facilitate device-to-device connectivity based on the IEEE 802.11 infrastructure mode. In this section, I shall introduce a simplified version of the IEEE 802.11[1] and the Wi-Fi Direct[2](Wi-Fi P2P) architectures.

The IEEE 802.11 standard offers different modes to form a wireless network, where the infrastructure mode is the most widely deployed. This mode has two main actors, the Access Point(AP) and the Station(STA), where the AP provides access to the distribution services for associated STAs. There's is another mode called Independent Basic Service Set(IBSS), also known as Ad Hoc, where two STAs are able to communicate directly without the need of an AP. For some reason, the last mentioned mode fails to gain support in the market.

Instead of trying to enhance the Ad Hoc mode, Wi-Fi Alliance decided to build a solution based on the infrastructure, mode making it easier for networks to coexist and give Wi-Fi Direct Devices(P2P Devices) the flexibility to be connected to infrastructure networks and create P2P Groups simultaneously. For a P2P Device to communicate it needs to find other P2P Device and form a P2P Group, which is almost the same as a wireless network on IEEE 802.11 infrastructure mode. P2P Devices negotiate which is going to take the AP role, known as P2P Group Owner(P2P GO), during the group formation procedure. Once this procedure is completed, the P2P Group will act as a wireless network on IEEE 802.11 infrastructure mode, enabling legacy devices to discover and connect to the P2P Group.

II. P2P Discovery

In this section, I'm going to describe the similarities and differences between the IEEE 802.11 network discovery and the P2P discovery procedures.

On infrastructure mode, STAs can discover available networks and the APs to access them by a process called scanning. There are two types of scanning processes, passive and active. Passive scanning gives the STAs the possibility to discover networks without the need of transmitting frames by sweeping from channel to channel and processing the Beacon frames. These frames are transmitted by the AP to announce the network and its capabilities. In active scanning, the STA sweeps channels transmitting Probe Request frames if an AP receives

a broadcast Probe Request frame or one for the service set to which the AP belongs, it will transmit a Probe Response frame. Both Beacon and Probe Response frames have the necessary information for the STA to know if it's capable of joining the network, this information is transmitted in different components. Management frames use Information Elements(IE), a tag-length-value(TLV) structure used within data communication protocols, as generic containers to transmit variable length data. As it was mentioned before in section I, a P2P GO will act as an AP; meaning that discovering these P2P Devices is even possible for any IEEE 802.11 STA. Because P2P Groups SSID have to start with the P2P Wildcard SSID(DIRECT-) it's easy for anyone to recognize them. But P2P Devices that are not in the role of a P2P GO are not discoverable by a STA performing neither passive nor active IEEE 802.11 scan. The P2P Discovery[1] procedure consists of two device states: listen and search. P2P Devices use the Listen State to become discoverable. Devices in this state shall use a Social Channel(channels 1, 6 and 11 in the 2.4 GHz band and channel 2 in the 60 GHz band) to process Probe Request frames that contain the P2P IE and the P2P Wildcard SSID. On the search state, the device transmits Probe Response frames that contain the P2P IE and the P2P Wildcard SSID among other fields. A P2P Device that is performing a scan has to switch between the listen and search states to make itself discoverable and search for other P2P Devices simultaneously. There are also P2P Devices that are not scanning and just stay in the listen state, waiting for other P2P Devices performing the Discovery procedure. This is also the case of P2P Group Owners, that besides they announce as any IEEE 802.11 AP using the Beacon frame they are in the listen state in case a P2P Device performs a scan.

The protocol specification has also a definition for a service discovery procedure. This procedure allows performing service discovery queries to P2P Devices prior to the creation of a P2P Group. To perform this, Wi-Fi P2P uses Generic Advertisement Service (GAS) to transport this information as specified by 802.11u[4]. Service Discovery can perform queries from protocols such as the following:

- Bonjour
- UPnP
- WS-Discovery
- Display
- Peer-to-Peer services (P2Ps)

In practice, IEEE 802.11 network detector tools such as Kismet[7], Aircrack-ng[8] among others could discover P2P Devices that are in the Group Owner role. This is related to the fact that P2P GO are acting as an AP using IEEE 802.11 infrastructure mode. But as explained below, P2P Devices that are not P2P GO are not discoverable with these tools because they don't have support for P2P scanning.

III. Device Fingerprinting

At the beginning, most IEEE 802.11 device fingerprinting[5] was done only based on the MAC address. There is also more complex research on device fingerprinting based on the IEEE 802.11 stack or hardware implementations. But after the appearance of Wi-Fi Protected Setup(WPS)[6] the device fingerprinting became much easier at least for the devices in the AP role. The idea behind WPS was to simplify the security setup and management of Wi-Fi networks. One of the requirements from the WPS protocol specification is that it requires the AP to transmit the WPS IE on Beacon and Probe Response frames. This IE contains several fields with device information that helps the device fingerprinting. Information such as the following:

- Manufacturer
- Model Name
- Model Number
- Serial Number
- Device Name

[1] there is an out-of-band discovery process that it is not cover in this document

WPS is used by Wi-Fi P2P for provisioning purposes[2] and its support is a mandatory requirement for P2P Devices. As mention in section II, P2P Devices use Probe Response frames to perform the discovery process, and WPS specification requires that these frames contain the WPS IE with the device information, making the device fingerprinting procedure quite easy.

IV. P2P Group Formation

P2P Group Formation is used to negotiate which P2P Device is going to take the P2P GO role, exchange credentials for the P2P Group and determine its characteristics. Group Formation procedure uses the authentication provided by the WPS specification. Once the two P2P Devices have found each other as described on the P2P Discovery procedure, they can start the GO Negotiation phase, where a three-way handshake is done to negotiate who is going to take the P2P GO role and other characteristics of the P2P Group. One of the main purposes of this negotiation is to exchange the Group Owner Intent attribute that communicates a measure of desire of the P2P Device to become the P2P GO. Finally, when the P2P Devices have established their roles, the P2P Client will connect to the P2P GO to obtain credentials using WPS Provisioning.[3]

P2P Groups have an optional procedure called P2P Invitation, this procedure can be used by a P2P GO to invite a P2P Device to become a P2P Client in its P2P Group or a P2P Client to invite a P2P Device to join the P2P Group of which the P2P Client is a member.

P2P Groups can be divided into two types:

- **Persistent P2P Group:** A group for which credentials are stored by the P2P Devices and the P2P Group may be made available to be reused after the initial use.
- **Temporary P2P Group:** A group that is formed only when required and ceases to exist after the initial use.

V. P2P Legacy Support

Based on information from the Wi-Fi Alliance[9] there are 13296 Wi-Fi P2P certified devices until the day this document was written. But there are many vendors that have not certified their devices, do not support Wi-Fi P2P protocol or have created their own network protocols for device-to-device connectivity(for example Apple has two protocol specifications, AirDrop[10] and AirPlay[11]). As a solution to this issue, some vendors enforce the legacy support by default. For example, a P2P Device may autonomously start a P2P Group by becoming a P2P Group Owner and create a Persistent P2P Group and give support for legacy devices to join the P2P Group.

VI. Vulnerabilities

In this section, I shall explain some vulnerabilities I found in Wi-Fi P2P implementations.

i. HP Printers Wi-Fi Direct Improper Access Control

As it was mentioned before in section **??**, Legacy Support can be an issue if it's not implemented in a correct way. In this case HP Wi-Fi Printers have a hardcoded Wi-Fi Passphrase for the P2P GO set to '12345678'. This could give access to anyone that is near enough to establish a Wi-Fi connection without any user interaction or notification. Once connected the attacker can access printing services among others, such as the Embedded Web Server that has no authentication by default allowing not only access to sensitive information but also to modify device configuration. The Wi-Fi Direct on this printers has a implementation of a passphrase generator that generates insecure passphrases limited to 8 digits. Performing a brute force attack on a WPA2 four-way hand-

[2] the technical documentation of this protocol it's outside of the scope of this document

[3] there is an optional phase called Provision Discovery where the devices check if both devices support the WPS config method that they are going to use for Provisioning

shake of these characteristics can be done in minutes with modern computers.

ii. Samsung Printers Wi-Fi insecure default credentials

As the HP Printer, the Samsung Wi-Fi Printers have an insecure Wi-Fi Passphrase for the P2P GO. By default, the passphrase it is limited to 8 digits and the function to generate new ones has the same limitations as the HP Printers. Apparently, both vendors are using the WPS PIN generation function to generate the WPA2 passphrase.

iii. Samsung Smart TV Wi-Fi Direct Improper Authentication

Samsung Smart TVs have support for Wi-Fi Direct by default and its enabled every time the device is turn on. The system uses a blacklist/whitelist access control mechanism to avoid asking the user to authenticate devices every time they try to connect using WiFi-Direct. This access control mechanism uses the MAC address to identify the devices, making it easy for an attacker to get the necessary information to impersonate a whitelisted device and gain access to the Smart TV. The user will get notified about the whitelisted device connecting to the Smart TV, but no authentication is required. Once connected, the attacker has access to all the services provided by the TV, such as remote control service or DNLA screen mirroring. Should any of the services provided by the Smart TV be vulnerable, once connected the attacker could gain control of the device or use it to pivot and gain access to the network.

iv. WD TV Live Streaming Media Player Wi-Fi Direct Unauthenticated Access

WD TV Live Streaming Media Player has support for Wi-Fi Direct by default and there is not a proper access control. Giving access to anyone that is near enough to establish a Wi-Fi Direct connection without any user interaction or notification. This vulnerability exposes user information and partial control of the device. Giving unrestricted remote read/write file access on mounted storage devices using smb and access other remote services such as the remote control web service.

v. Android 4 WiFi-Direct Denial of Service

On Android 4 an attacker could send a specially crafted 802.11 Probe Response frame causing the Dalvik subsystem to reboot because of an Unhandled Exception on WiFiMonitor class. For more information on this vulnerability please visit the following link.

https://www.coresecurity.com/advisories/android-wifi-direct-denial-service

VII. Conclusions

i. Availability

P2P Devices are available for anyone to interact with, giving attackers a new target. Based on the information on the Wi-Fi Alliance web site, the ranges are just like any Wi-Fi device(with ranges up to 200 meters).

ii. Confusion

P2P Devices can be confusing and certain implementations do not have an easy way to configure the features or don't have an interface at all.

iii. Weakest Link

P2P Devices use WPS Provisioning. One of the configuration methods is called Push-Button-Configuration. There are ways to brute force this provisioning method making it possible for a confused user to press a button on a P2P Device and give access to the P2P Device(This attack can have similarities with a one-click phishing attack).

iv. Bridge

P2P Concurrent Devices can operate concurrently with an infrastructure network, this usually requires the P2P device to have multiple wireless network interfaces or support virtual network interfaces. Cross Connection capability can make a P2P Group act as a bridge between the P2P Clients connected to the P2P GO and the network the device is connected to. There is also the possibility that a P2P Device that doesn't support Cross Connection has a vulnerable network service that can be exploited to gain total or partial control of the P2P Device and turn it into a network entry point.

v. Attack Surface

The Android vulnerability described on section VI is quite old but it is a good example to show that Wi-Fi Direct vulnerabilities are not only limited to hardcoded credentials, MAC filtering implementations or pseudo phishing attacks extending the attack surface of the device. The Service Discovery procedures are also a good example of how the surface has been extended. Now it's possible to interact with a network discovery service such as UPnP at the P2P Discovery phase using Action frames.

VIII. References

References

[1] IEEE Std 802.11TM-2012 (Revision of IEEE Std 802.11-2007) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

[2] Wi-Fi Peer-to-Peer (P2P) Technical Specification

[3] Wi-Fi Alliance, https://www.wi-fi.org

[4] IEEE 802.11u-2011 - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 9: Interworking with External Networks

[5] Wikipedia Device Fingerprint, https://wikipedia.org/wiki/Device_fingerprint

[6] Wi-Fi Protected Setup, https://www.wi-fi.org/discover-wi-fi/wi-fi-protected-setup

[7] Kismet, https://kismetwireless.net

[8] Aircrack-ng, https://aircrack-ng.org

[9] Wi-Fi Direct-certified products, https://www.wi-fi.org/product-finder-results?certifications=34&items=30

[10] Use AirDrop on your iPhone, iPad, or iPod touch, https://support.apple.com/en-us/HT204144

[11] Use AirPlay or Screen Mirroring on your iPhone, iPad, or iPod touch ,https://support.apple.com/en-us/HT204289