A CM-based model for 802.11 networks security policies enforcement

Karl MABIALA DONDIA[a], Jing MA[b], FENG TAO[c]

School of Computer and Communication, Lanzhou University of Technology, CHINA

[a] kdondia@gmail.com, [b] 15193111242@163.com, [c] fengtj@lut.cn

Keywords: Wireless LAN, IEEE 802.11 standards, Continuous Monitoring, security policy.

Abstract.

In recent years, networks based on the 802.11 standards have gained a prolific deployment. The reason for this massive acceptance of the technology by both home users and corporations is due to the "plug-and-play" nature of the technology and the mobility. The lack of physical containment due to the inherent nature of the wireless medium makes maintenance very challenging from a security standpoint. This study examines, via continuous monitoring, various predictable threats that 802.11 networks can face, how they are executed, where each attack may be executed and how to effectively defend against them. The primary goal is to identify the key components of an effective wireless security policy.

Introduction

Increased flexibility, ease of use, cheapest way for Internet connectivity, environmental constraints are just some of the factors that have been in favor of the rapid emergence of the technology. Unfortunately, heightened security risks temper these powerful advantages. The risks are mainly related to the transmission media on which the technology is based on.

Wireless network communication involves no physical link to be established between the communication parties. It provides users with network connectivity without being tethered to a wired network. Since wireless signals spread over the air in an unguided manner, it has been a matter of security concerns for several years.

Many corporations see in the technology a good way for extending their main wired network, but they often fail in developing and implementing a security policy that considers the wireless-specific threats.

As with any good idea, this recent focus on the technology has caused people to stop and think about several ways to overcome the underlying network limitations to achieve the same level of services and capabilities of its wired counterpart--making it "*more secure"*. This work focuses on the threats to wireless LAN environments, how to mitigate them and consequently how to use the information gathered from continuous monitoring as a knowledge base to enforce the security policy.

Background

Wireless LAN security issues. Before looking at the various protocols and mechanisms that may be used to provide an acceptable level of security to the wireless clients, we should try to understand what the needs of those users of the technology are. To begin, we can say that wireless users want the same level of services and capabilities that they have commonly come to expect from the wired counterpart; that is Confidentiality, Integrity and Availability (CIA).

Wireless networks do suffer from some of the same security issues as wired networks, --- misuse, hackers, information leakage, violation of confidentiality, and so on --- but they also have their own security issues as well. Those additional risks are mostly due to the fact that wireless networks are not contained or closed thus making wireless environments more prone to cyber

criminal activities. In the case of a composite network --- Wired – Wireless --- it is possible to use the WLAN as an entry point into the wired network.

All that can be said with any certainty is that the lack of physical containment is the major limitation of the technology. Because we cannot control or secure the physical aspect of the network, the only option is to secure the access control and transmission aspects of the network. Those two features are provided by means of encryption and authentication.

Wireless Security protocols. Many protocols have been made in the realm of making wireless environments more secure. The following list itemizes those protocols, their level of security and the encryption methods used.

a. Wireless Equivalent Privacy (WEP)

WEP was the first major security protocol for encrypting wireless traffic --- Layer 2 encryption. As its name suggests, it was designed to provide the same level of security that we have commonly come to expect with its wired counterpart.

WEP has been introduced in the 802.11b standard and is based on the RC4 encryption algorithm. Two versions were proposed, one with a 64-bits key length and the other with a 128-bits length. These keys are actually 40 bits and 104 bits long respectively because they include an Initialization Vector (IV) that is 24-bits long as part of the key strength. Those keys are used to encrypt the plaintext message and its checksum --- The Integrity Check Value (ICV). The Cipher text was therefore determined using the following formula:

$$C = [M \,||\, ICV\,(M)] + [RC4\,(K \,||\, IV)]. \quad (1)$$

Two of the problems with the proposed scheme include:

- The use of static keys;
- The initialization vector sent in plaintext.

b. WiFi Protected Access (WPA)

WPA was developed by WiFi Alliance as a stopgap measure to overcome WEP problems. WiFi Protected Access got around with some of WEP problems by incorporating the Temporal Key Integrity Protocol (TKIP); that is, it allowed WPA to create dynamic rather than static keys by ensuring the uniqueness of the key with which each data packet is encrypted. WPA also provides for passphrases (pre-shared keys) as an authentication method in small environments (WPA Personal) as well as 802.1X authentication (WPA–Enterprise).

TKIP, like WEP, uses a key scheme based on the RC4 encryption algorithm. TKIP provides the following features:

- Per-packet key mixing;
- A Message Integrity Check (MIC);
- A re-keying mechanism.

c. WiFi Protected Access 2 (WPA 2)

Unlike the two previous security protocols, which use the RC4 encryption algorithm, WPA 2 is primarily based upon the AES encryption algorithm but can also use TKIP as an optional mode to maintain backwards compatibility. The IEEE 802.11i standard also called WPA 2 is designed to provide secured communication over wireless. It is an enhancement of WEP in the areas of encryption, authentication and key management. IEEE 802.11i is based on WPA, which was a quick fix of the WEP weaknesses.

The 802.11i standard has the following key components:

- Temporal Key Integrity Protocol (TKIP);
- Counter-Mode/CBC-MAC Protocol (CCMP);
- IEEE 802.1X authentication framework;
- EAP over LANs (EAPOL)–A key protocol in 802.1X for key exchange.

d. 802.1X

802.1X is a port-based Network Access Control standard. It is not part of the 802.11 standards but is used as an authentication method in most 802.11 networks and wired networks as well. This standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as varying the encryption keys dynamically. 802.1X ties a protocol called Extensible Authentication Protocol (EAP) to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, one-time passwords, certificates, etc.

Three major components are part of the architecture:

- The Supplicant: the user that wants to be authenticated;
- The Authentication Server: typically a RADIUS server;
- The Authenticator: A wireless access point.

Wireless Network continuous monitoring

Continuous Monitoring (CM) is the process of auditing system configurations in a timely manner. CM is a vulnerability-centric approach, focusing on configuration and software weaknesses. We use this approach to evaluate the level of security that the security protocols discussed above can provide to a corporate WLAN, their limitations as well as auxiliary threats to the WLAN --- rogue access points, misbehaving users --- in order to define an effective security policy.

The protocols discussed so far can provide an acceptable level of security to the corporate network, but do not ensure how well the users adhere to the policy. The policy is here to clearly define the term ‘’acceptable”. In fact, it is precisely at those times when the network is attacked that the need of a well- thought security policy is most keenly felt.

Cracking WEP. WEP can be attacked due to the weak 24-bits initialization vectors (IV) that may be sent out periodically in plaintext. The key is to collect as many weak IVs as possible but these may be few and rare. Sometimes it may be necessary to help the traffic generation process along.

We used Aireplay-ng and its companion tool Aircrack-ng to carry out the attacks on WEP. Aireplay-ng was used to inject frames with the goal of generating a huge amount of traffic in the wireless network. Aircrack-ng was used to crack the key after we got enough IVs have been collected.

Aircrack-ng uses several methods to attack WEP IVS (Fig. 2):

- Dictionary attacks;
- Brute-force attacks;
- FMS/KoreK method – uses statistical analysis to crack the WEP key;
- PTW --- Requires ARP packets.

Cracking WPA & WPA2. WPA and WPA2 use similar methods to generate traffic, so similar methods can be used to crack keys for both the encryption protocols. Since the IVs are dynamic in WPA, we no longer need to capture them. The information we need to capture is contained in the transmission between the AP and STA when establishing connection. This is known as the WPA handshake.

To recover the passphrase, we essentially used a dictionary or brute force attack (Fig. 3).

Rogue/Fake Access Points. A rogue Access Point is a Wireless AP that has either been installed on a secure network without explicit authorization of the Network administrator or has been created by an attacker to conduct a Man-In-The-Middle attack. In either case, these APs are not authorized for operation on the network and do not conform to the security policy of the WLAN representing a security risk.

They are typically used to capture credentials or other data by getting STA connecting to them. They can be real APs or Fake APs --- Software AP broadcasting from the attacker machine (Fig. 4).

WLAN security policy model

In the previous section, we examined some salient threats to WLAN. These are by no means the only viable taxonomy, but it is sufficient to cover most of the interesting attacks on 802.11 networks.

Based on the observations made, we will now lay out a general model for Wireless security policy easy to draft, maintain and enforce.

Security policy development life cycle. This part introduces the idea that you should see the policy modeling as composed of steps that accomplish sub-goals rather than a single activity.

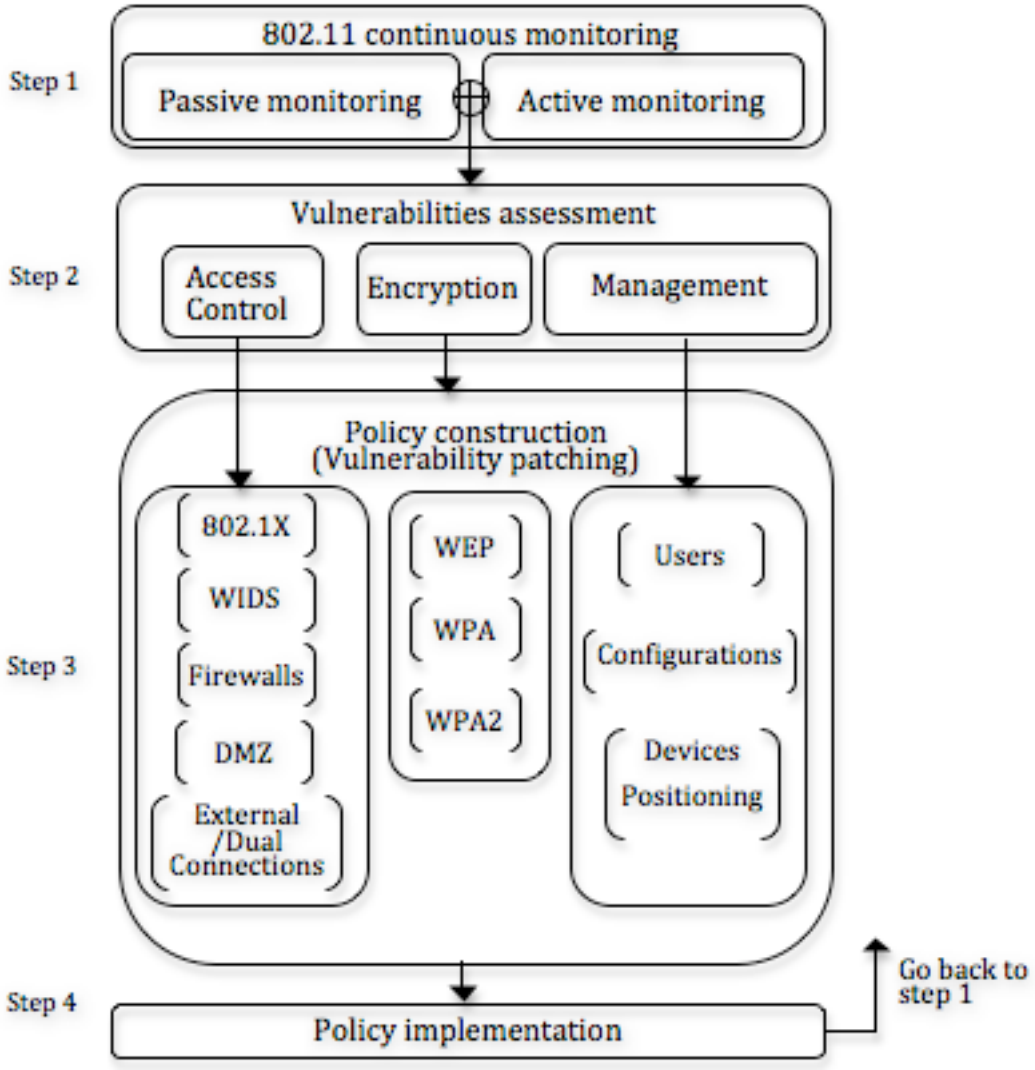

Fig. 1 Wireless Security policy development life cycle.

The methods used in each step of the cycle can be thought of like Lego blocks:

- The first step is to clearly model the system you are building from scratch or change by performing both passive and active monitoring.
- The Second step involves a complete understanding of the wireless-specific threats. It is a summary of the observation made in the previous step --- what can go wrong with the Access control, encryption mechanisms in use.
- The third step consists of addressing the security threats by choosing a set of the security technologies that best suits your system.
- The fourth step consists of validating the policy just layed out. Methods of penetration testing (performing attacks against the system) can be used to test the effectiveness of the policy. It can be a step of further understanding of security requirements.

A Wireless security policy example. Security is important for enterprises for a wealth of reasons, and a well-run corporation needs formal, written security policies. Policies set the appropriate expectations regarding the use and administration if the corporate IT assets.

Some of the best practices for wireless configurations and connections that we will discuss include:

a. Design

Security should be designed into the infrastructure and not added later. It is important to have a holistic view of the entire network to better consider the risks to wired and wireless networks and implement a layered security for all networks.

b. Standards

After the assessment of the security needs comes the phase of characterizing the approaches to satisfy the security requirements. Security standards enable organizations to practice safe security techniques to mitigate the threats to security.

c. Clients

- The Clients must be configured to the highest level of security that their hardware, OS, and AP support. Legacy clients must be removed or upgraded;
- Limit "Bring-Your-Own-Device", exceptions made to only what is absolutely necessary and enforce BYOD device configurations and policies when they are used;
- Restrict and monitor guest access to the Wireless network;
- Use WPA/WPA2 only–no WEP!
- Use 802.1X throughout the wireless network.

d. APs

Secure Access Points by hardening, controlling access and controlling traffic. Harden the APs as much as is practical:

- Change APS default settings (Administrator account, SSID, DHCP range, IP address);
- Configure remote administration;
- Configure secure protocols such as HTTPS, etc.
- Change Channel and band;
- Control access to APs from Clients:
  - MAC filtering;
  - 802.1X authentication for enterprise use;
  - Use of Strong keys;
  - Use PKI certificates;
  - Use WPS where practical.
- Configure Port and Service filtering;

- Use Enterprise-level devices behind the WAP for more in depth filtering and access control (e.g. Firewalls, NACs, etc.).

e. External / Dual connections

- Connection to the Corporate Wired network or other Wireless networks must be carefully controlled. The considerations to pay attention to include interfaces, authentication, resource access, etc.
- All connections to other networks must be protected by border devices --- firewalls, routers, etc.
- Only allow a prescribed set of users in from the wireless network and limit the resources that can be accessed from the Wireless clients.
- Disallow multiple connections from devices while connected to the corporate network;
- Separate groups of wireless users by privilege and access needs (e.g. Guests, Users, Administrators).

Summary

The Wireless technology has done well, keeping up with the increasing demand of high-speed networks and the trend toward ever-increasing mobility. The growth of high-speed wireless access further enhances the ability to use enterprise information resources and services everywhere. Those powerful advantages come along with very serious security concerns; high on the list of such problems is the unbounded nature of the transmission media --- The AIR.

Throughout this study, we have been using Continuous Monitoring to present the key components of a formal Wireless Security policy. The information gathered is an important source regarding the security protocols, their vulnerabilities, the misbehaving users and best practices for wireless network configuration.

This policy goes far beyond the simple idea of "keep the intruders out"; it spans the network design, the protocol implementation to data access aspects and specifies rules for individuals or groups of individuals throughout the organization.

References

[1] Woodward A: *Recommendations for wireless network security policy: an analysis and classification of current and emerging threats and solutions for different organisations*[C]//AISM. 2005: 133-140.

[2] Green J: *Building global security policy for wireless LANs. Aruba Wireless Networks*. Sunnyvale, CA[J]. 2006.M.A. Green: *High Efficiency Silicon Solar Cells* (Trans Tech Publications, Switzerland 1987).

[3] Potter B:Wireless security's future[J]. Security & Privacy, IEEE, 2003, 1(4): 68-72.

[4] Lapiotis G, Kim B, Das S, et al. *A policy-based approach to wireless LAN security management* [C]//Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference on. IEEE, 2005: 181-189.

[5] Manley M E, McEntee C A, Molet A M, et al. *Wireless security policy development for sensitive organizations* [C]//Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC. IEEE, 2005: 150-157.

[6] Information on http://www.tradepub.com/?pt=adv&page=AirTight%20Networks

[7] Hui LI , Xin Wen Fu: *Wireless Networks – 802.11 WIFI exploration*(2010)

[8] Kelcey Tietjen: *Wireless Traffic Analysis* (2010)

Appendix

This appendix is a handful of traffic monitoring, wireless encryption protocols cracking and fake AP creation representative examples. The approach used here is referred to as "Knowing the attack to better defend against it".

1. **WEP attack in practice**

a. Fake authentication attack

The aim of fake authentication is to associate with the AP, which assists in injection attacks.

```
root@bt:~# aireplay-ng -1 0 -e Dondia_Test -a 8C:21:0A:5A:3F:8C -h 48:02:2a:58:df:99 mon0
05:47:15 Waiting for beacon frame (BSSID: 8C:21:0A:5A:3F:8C) on channel 1

05:47:15  Sending Authentication Request (Open System) [ACK]
05:47:15  Authentication successful
05:47:15  Sending Association Request [ACK]
05:47:15  Association Successful :-) (AID: 1)
```

Fig. 2.1: Fake authentication Attack.

b. De-authentication attack

This attack is used to send Deauthentication frames to both an AP and a connected client hence forcing the client to re-authenticate itself. The client, by re-authenticating itself generates ARP traffic that may contain WEP IVs that we need to collect to help us in the WEP cracking process.

```
root@bt:~# aireplay-ng -0 0 -e Dondia_Test -a 8C:21:0A:5A:3F:8C -c A8:86:DD:D0:70:CC mon0

06:31:50 Waiting for beacon frame (BSSID: 8C:21:0A:5A:3F:8C) on channel 3
06:31:51 Sending 64 directed DeAuth. STMAC: [A8:86:DD:D0:70:CC] [ 0|64 ACKs]
06:31:51 Sending 64 directed DeAuth. STMAC: [A8:86:DD:D0:70:CC] [ 0|64 ACKs]
06:31:52 Sending 64 directed DeAuth. STMAC: [A8:86:DD:D0:70:CC] [ 0|64 ACKs]
06:31:53 Sending 64 directed DeAuth. STMAC: [A8:86:DD:D0:70:CC] [ 0|64 ACKs]
:
:
06:32:11 Sending 64 directed DeAuth. STMAC: [A8:86:DD:D0:70:CC] [ 0|64 ACKs]
```

Fig. 2.2: De-authentication Attack.

c. Replay Attack

This is one of the best attacks used to attack WEP. The aim of this attack is to force ARP traffic to and from the client and AP. This ARP traffic, particularly ARP responses can contain new IVS. This attack can be used in conjunction with other attacks such as Fake authentication or De-authentication attack.

```
root@bt:~# aireplay-ng -1 0 -e Dondia_Test -a 8C:21:0A:5A:3F:8C -h 48:02:2a:58:df:99 mon0
```

```
root@bt:~# airodump-ng mon0 -c3 -bssid A8:86:DD:D0:70:CC -w arp_cap
```

```
root@bt:~# aireplay-ng -3 -b A8:86:DD:D0:70:CC  -h 48:02:2a:58:df:99 mon0
06:31:50 Waiting for beacon frame (BSSID: 8C:21:0A:5A:3F:8C) on channel 3
Saving ARP requests in replay_arp_-1022-122758.cap

You should also start airodump-ng to capture replies

Read 169 packets (got 0 ARP requests and 0 ACKS), sent 0 packets … (0 pp
Read 172 packets (got 0 ARP requests and 0 ACKS), sent 0 packets … (0 pp
Read 175 packets (got 0 ARP requests and 0 ACKS), sent 0 packets … (0 pp
Read 179 packets (got 0 ARP requests and 0 ACKS), sent 0 packets … (0 pp
Read 183 packets (got 0 ARP requests and 0 ACKS), sent 0 packets … (0 pp
:
:
Read 5690 packets (got 0 ARP requests and 0 ACKS), sent 0 packets … (0 pp
```

Fig. 2.3: Replay Attack.

d. Cracking WEP

We used Aircrack-ng to parse capture files and crack WEP keys. Aircrack-ng can be run from several capture files at once and can also use multiple ESSIDs.

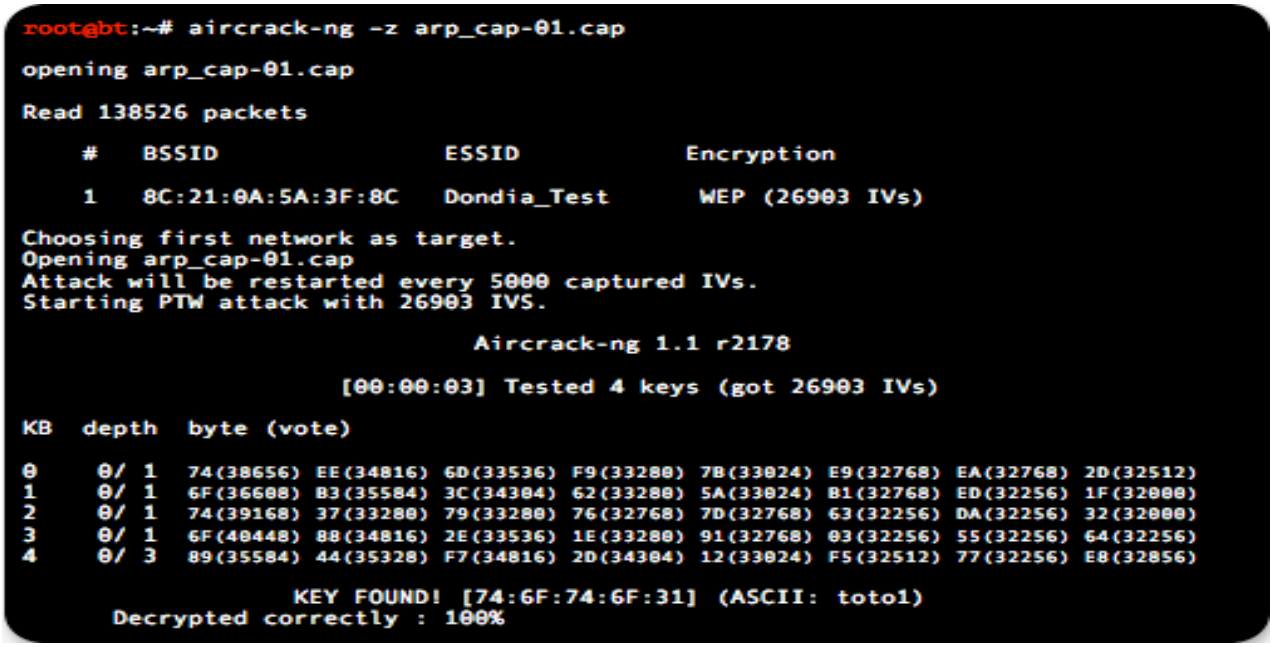

Fig. 2.4: Cracking WEP.

2. **WPA/WPA2 attack in practice**

After the capture of at least one WPA/ WPA2 handshake, we used a brut force attack for recovering the encryption key.

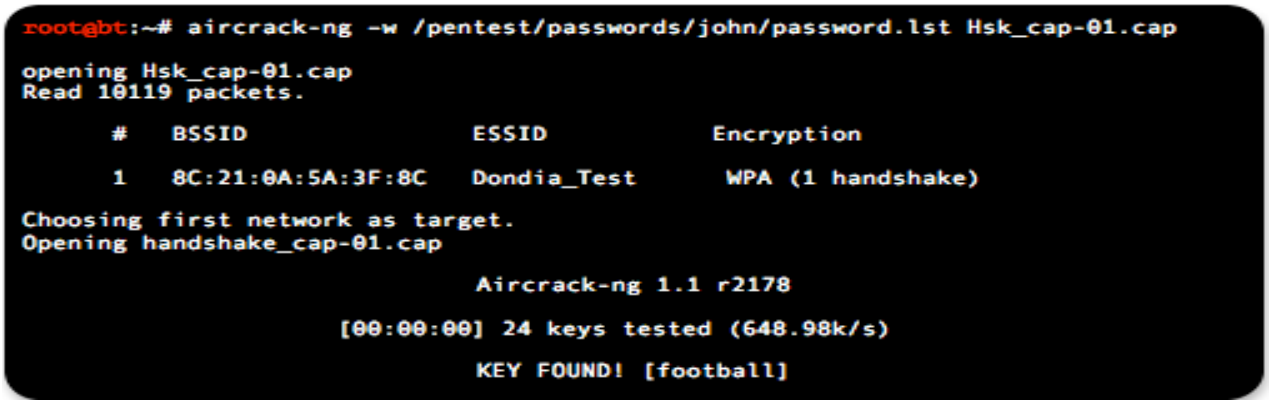

Fig. 3: Cracking WPA/WPA2

3.**Fake Access Point**

We used the utility Airbase to create a Fake AP:

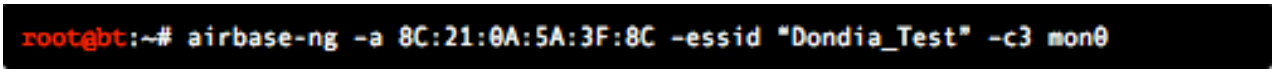

Fig. 4: Fake Access Point