

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II



Corso di Laurea Magistrale in Ingegneria Informatica

Elaborato di Network Security

Wi-Fi Hacking Robot

Anno accademico 2020/2021

Autori:

Guido Guarnieri M63/0994

Umberto Gagliardini M63/1023

Introduzione

Contesto applicativo

Wi-Fi è un insieme di tecnologie per reti locali senza fili (WLAN) basato sullo standard IEEE 802.11, il quale consente a più dispositivi di essere connessi tra loro tramite onde radio e scambiare dati.

Una rete wireless deve garantire:

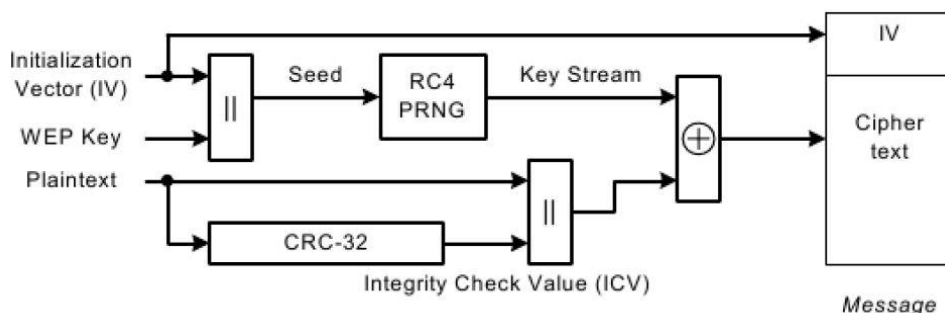
- **Confidenzialità**, soggetti non autorizzati non devono poter avere accesso ai dati;
- **Integrità**, i dati inviati devono arrivare a destinazione così come sono partiti, quindi non devono subire alterazioni durante il “tragitto”.

A seconda di come vengono implementate queste due proprietà si hanno sistemi di sicurezza diversi, in particolare i più noti ed utilizzati sono: WEP, WPA (TKIP) e WPA2 (CCMP), di cui il primo quasi del tutto non più utilizzato.

Per poter descrivere le operazioni eseguite dal tool bisogna *in primis* riportare una breve descrizione dei sistemi di sicurezza accennati:

- WEP

come chiave di sicurezza, per criptare i messaggi al fine di assicurare la segretezza, utilizza una stringa ottenuta concatenando una chiave WEP ed un IV come mostrato dallo schema seguente:

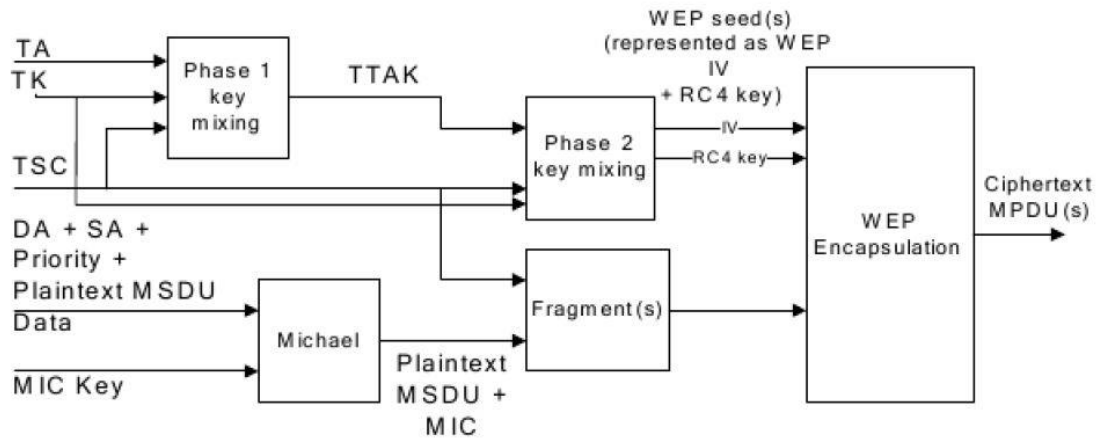


Incapsulamento WEP

Ma si può notare come l'Initialization Vector sia trasmesso in chiaro, quindi solo parte della stringa usata come seed per generare il key stream è ignota.

- TKIP

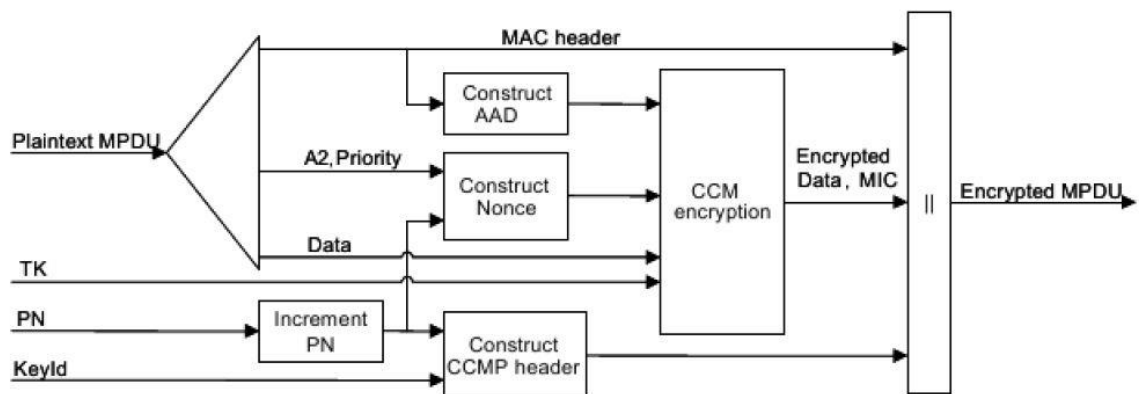
Questo sistema di sicurezza, standardizzato da WPA, in realtà è un'estensione di WEP che risolve alcune criticità ed utilizza due chiavi segrete per implementare integrità e sicurezza, ovvero la MIC key e la Temporal key:



Incapsulamento TKIP

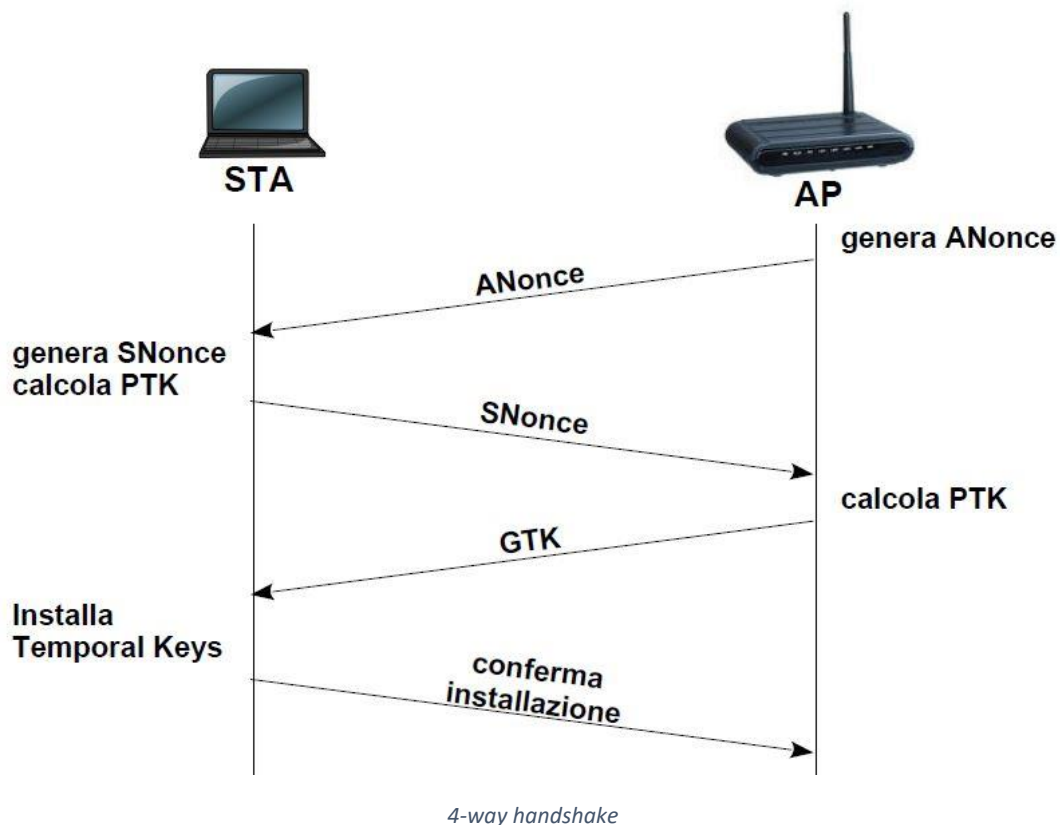
- CCMP

Rimuove il supporto a WEP ed effettua l'incapsulamento utilizzando una singola Temporal key:



Incapsulamento CCMP

Sia in TKIP che CCMP le chiavi sono in realtà calcolate a partire da una chiave principale, la quale viene ottenuta a seguito di un 4-way handshake tra station e access point:



Ed alla base di questo scambio di messaggi c'è ancora un'altra chiave, la quale può essere una Pre-Shared Key o una Pairwise Master Key nel caso del WPA Enterprise.

La PSK è scambiata offline ed è usata dalla maggior parte degli access point domestici, mentre la PMK è creata dinamicamente e distribuita da un Server. Quindi la vulnerabilità più banale di questi sistemi di sicurezza consiste in questa chiave, la quale se scoperta in qualche modo permette l'accesso alla rete.

Lo scopo di un attacco ad una rete Wi-Fi è quello di introdursi all'interno per poter poi intercettare tutti i pacchetti degli host, individuare eventuali vulnerabilità ed infine, sferrare attacchi sfruttando suddette vulnerabilità.

Un attacco ad una rete Wi-Fi può essere schematizzato nei seguenti passi:

- i. Individuazione access point;
- ii. Analisi degli access point individuati: metodi di sicurezza, canali, ESSID, BSSID ecc....;
- iii. Scelta di uno specifico attacco a seconda del metodo di sicurezza implementato:
 - a. WEP: brute force sulla chiave WEP catturando un numero elevato di Initialization Vector;
 - b. WPA-PSK: brute force sulla password dopo aver catturato il 4-way handshake o AP-fake-auth;
 - c. WPA Enterprise: per questo particolare metodo di sicurezza l'unico attacco possibile è il fake authentication utilizzando tool come Eaphammer, il quale simula anche un Autentication Server e permette di creare certificati falsi.

Specifica dell'applicazione

All'avvio del tool, viene chiesto all'utente con quale interfaccia wireless avviare la modalità monitor. In questo modo verranno mostrati a video tutti gli AP presenti in zona dando la possibilità all'utente di scegliere quale rete hackerare. A questo punto in base alla tipologia di rete scelta il software eseguirà una tecnica di attacco diversa.

- WEP: ricorrendo alla suite aircrack, avverrà una fake authentication associando il MAC address del proprio dispositivo all'AP in questione. Successivamente con l'obiettivo di voler collezionare un numero elevato (10^5) di pacchetti viene eseguita una injection di pacchetti ARP. In conclusione dopo il termine della raccolta di pacchetti avviene la vera e propria decifrazione della password.
- WPA: anche in questo caso si ricorre alla suite aircrack, inizialmente viene effettuato lo sniffing dei soli pacchetti scambiati tra stations e access point vittima con lo scopo di intercettare l'handshake; in contemporanea l'utente può scegliere di inviare pacchetti di de-autenticazione per forzare una riconnessione e di conseguenza ottenere l'handshake desiderato. Una volta ottenuto, il tool permette di eseguire un attacco brute force per ottenere la password del Wi-Fi ed in particolare permette di inserire un dizionario già a disposizione, di crearne uno con informazione della vittima o di crearne uno random specificando la lunghezza delle word.

Documentazione

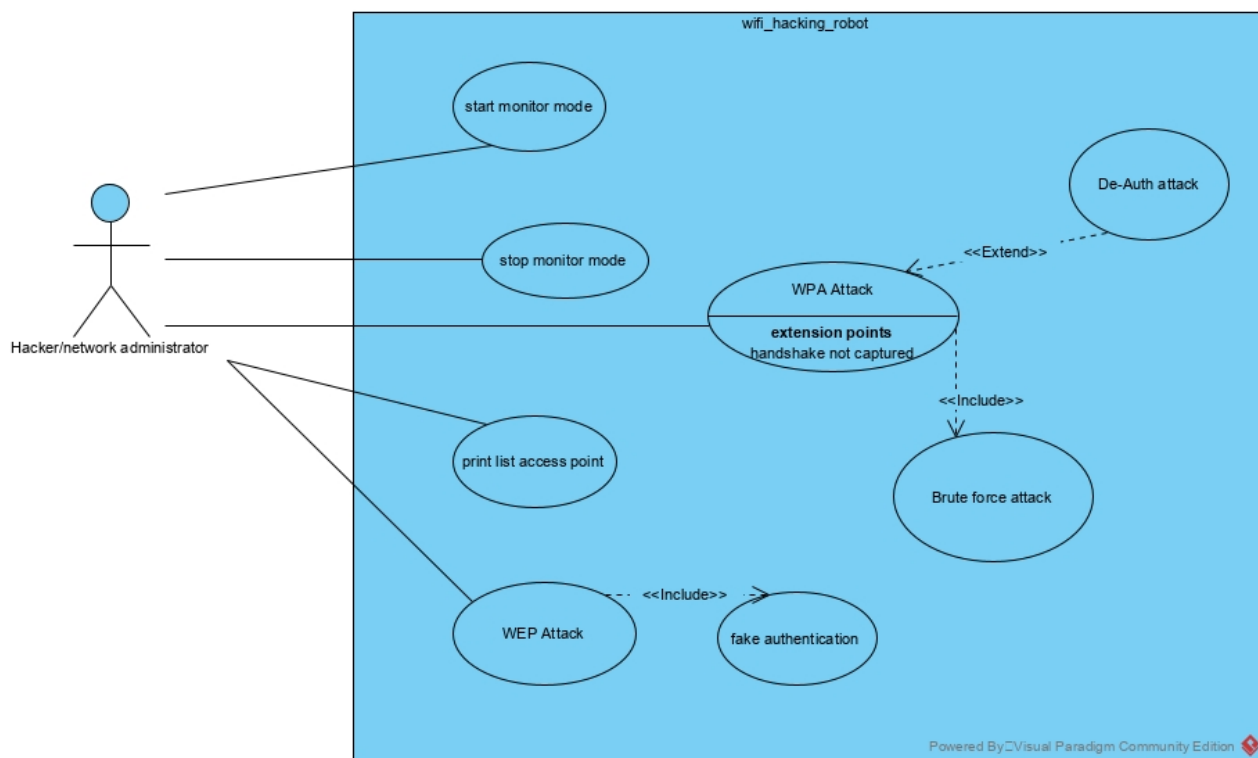
Requisiti funzionali

Casi d'Uso - Breve Descrizione

- **Start monitor mode:** L'interfaccia di rete wireless viene predisposta in modalità monitor
- **Stop monitor mode:** Viene interrotta la modalità monitor
- **Print access point list:** Stampa a video della lista di access point che è possibile hackerare.
- **WEP attack:** Viene innescato un attacco ad una rete che implementa WEP
- **WPA attack:** Viene innescato un attacco ad una rete che implementa WPA.
- **Fake authentication:** Associazione fasulla tra il proprio dispositivo e l'AP vittima.
- **De-auth attack:** injection di messaggi di de-authentication ad una station vittima.
- **Brute force attack:** Impiego di un dizionario per decifrare la password del Wi-Fi.

Attori

- Utente (hacker/network administrator)



Use Case Diagram

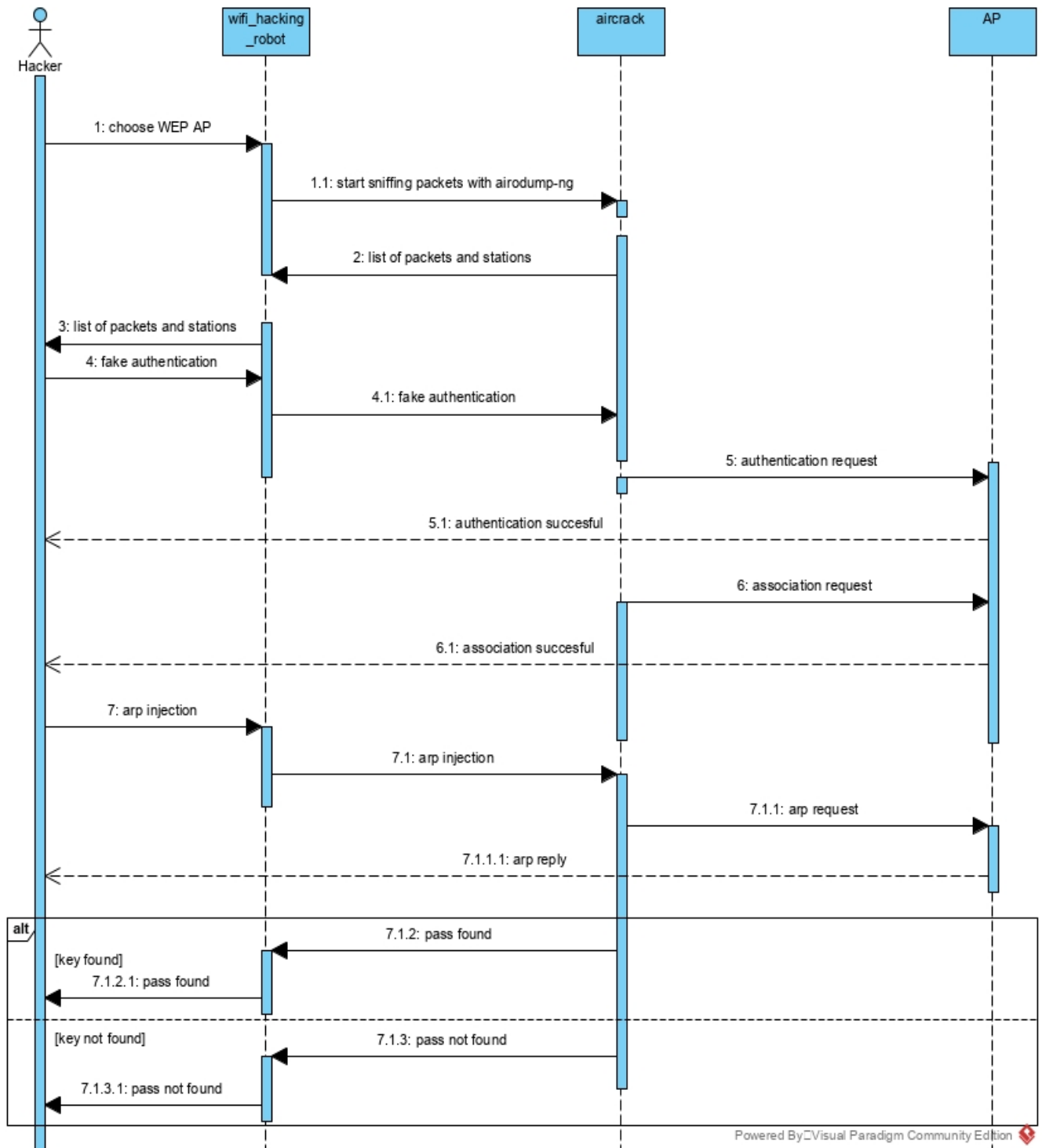
Requisiti non funzionali

Robustezza: Il software è dotato di misure di validazione dell'input.

Usabilità: per utilizzare il tool non c'è bisogno di nessuna conoscenza specifica di cyber-security.

Sequence diagram

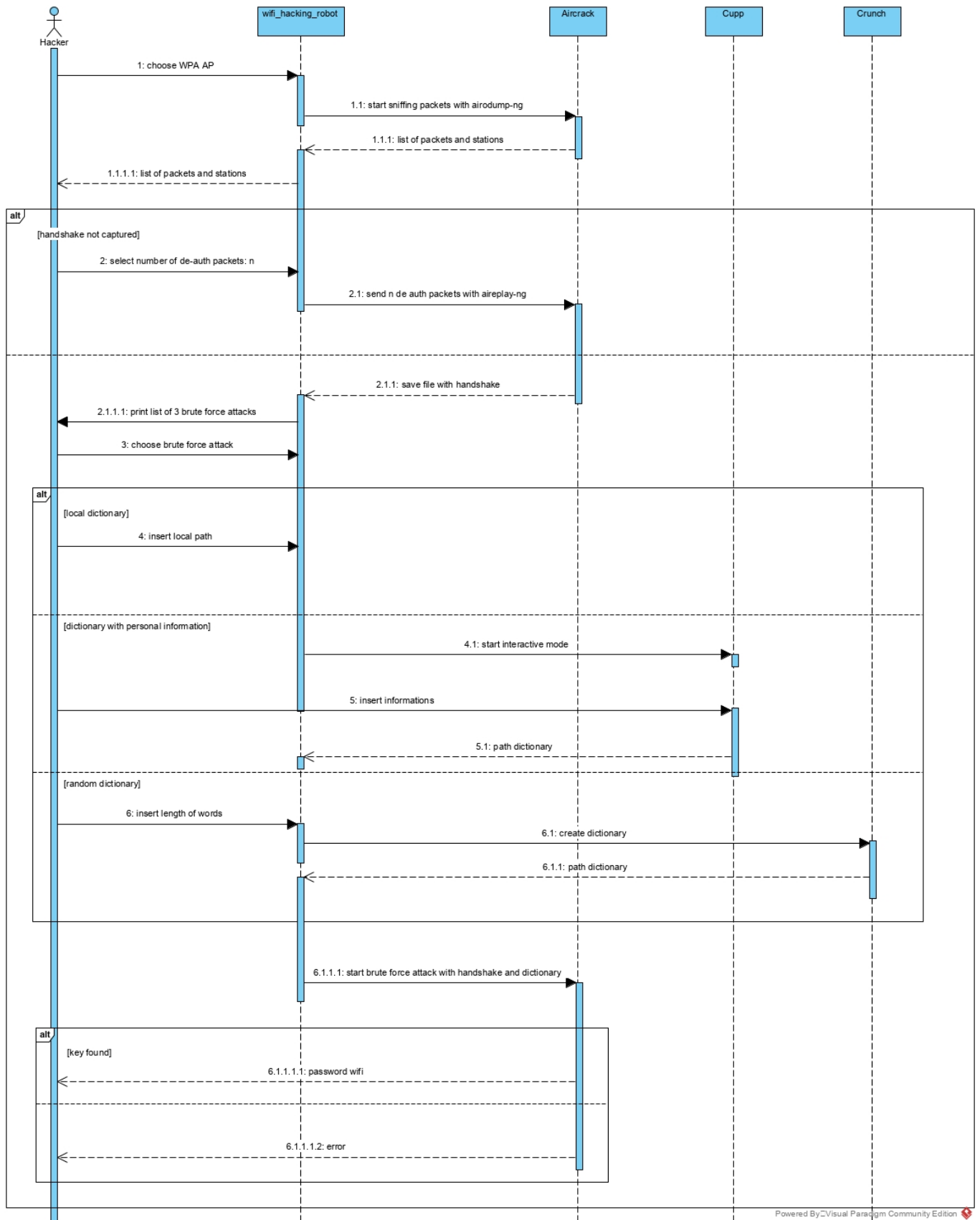
WEP attack



Powered By Visual Paradigm Community Edition

Sequence Diagram WEP attack

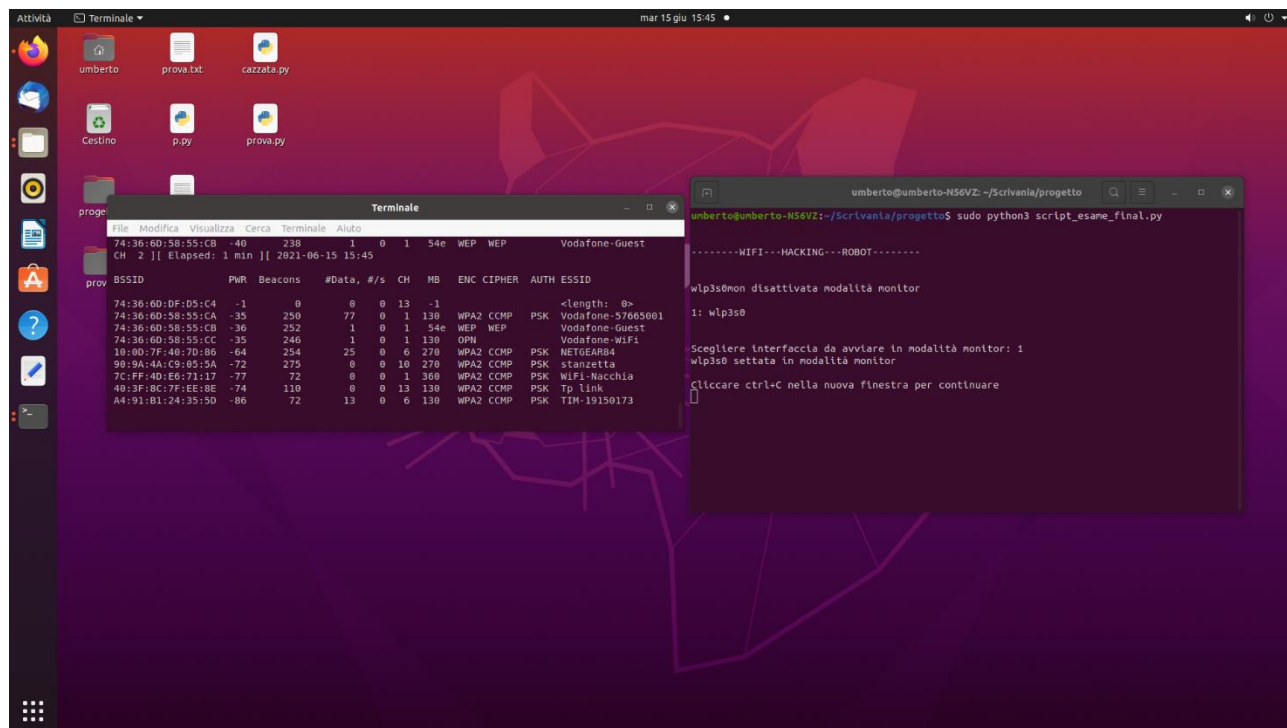
WPA attack



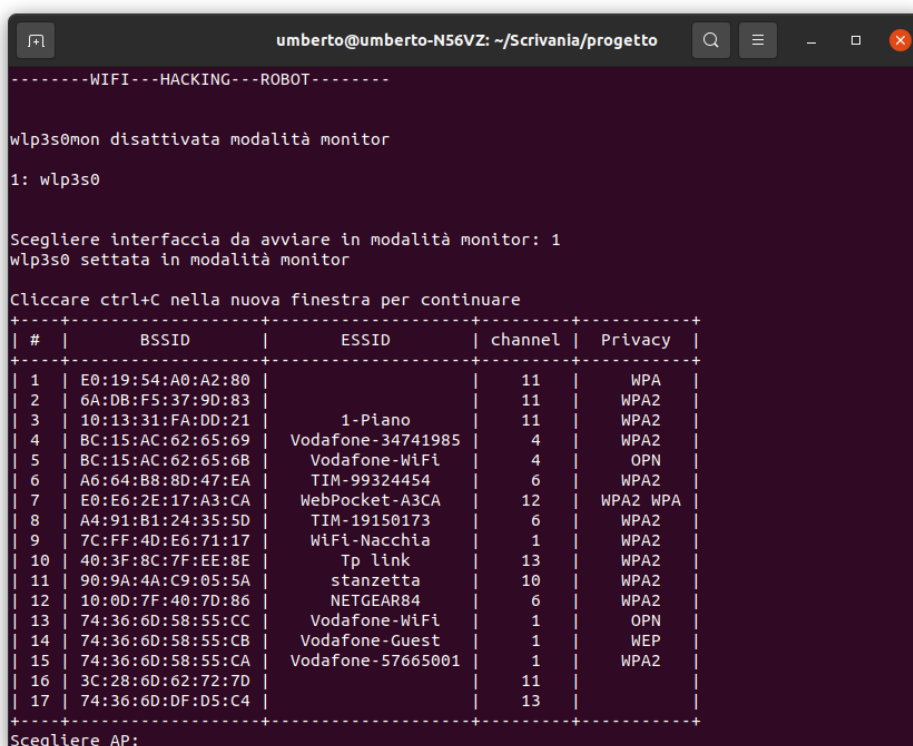
Sequence Diagram WPA attack

Guida all'utilizzo del tool

All'avvio del tool, viene predisposta automaticamente la modalità monitor della scheda di rete wireless. In questo modo l'utente può vedere diverse informazioni, come: BSSID, protocollo di crittografia utilizzato e tipo di autenticazione dell'Access Point.

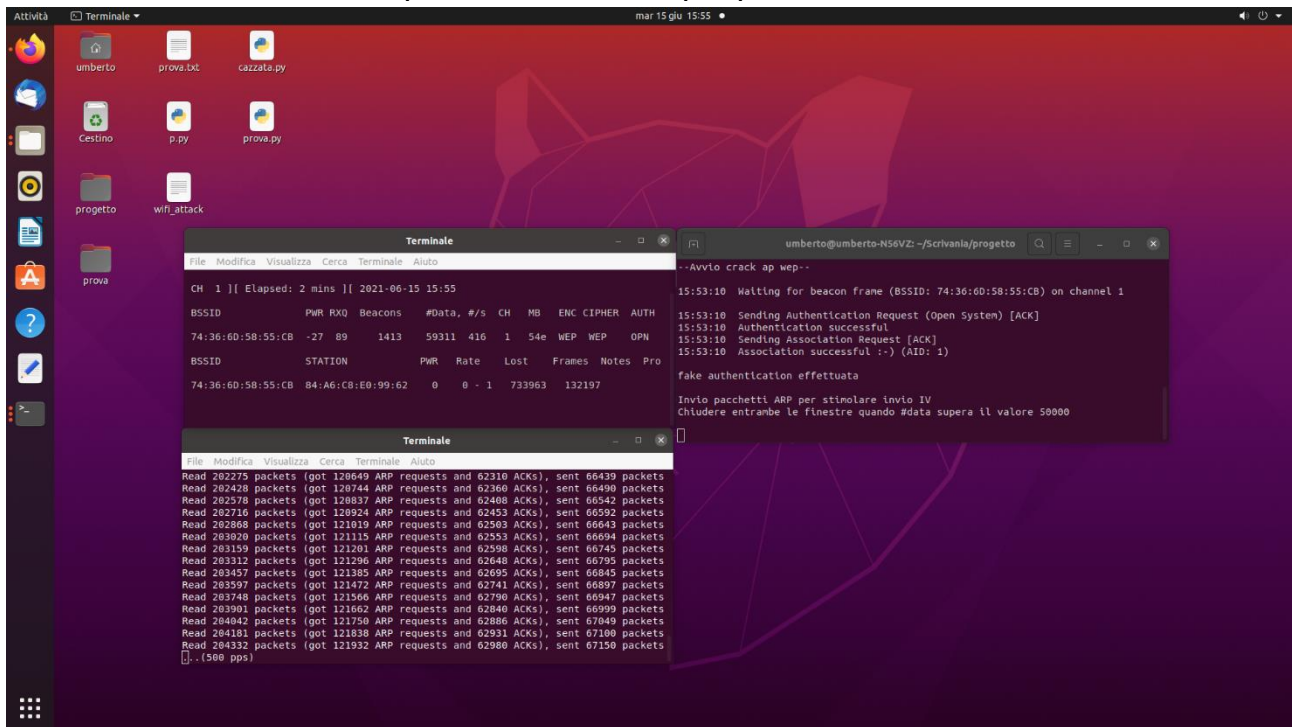


Successivamente verrà data all'utente la possibilità di scegliere quale rete attaccare. Si rende noto che non bisognerà specificare al tool se il protocollo utilizzato è WEP oppure WPA.



Attacco a rete WEP

Se l'utente sceglie un AP che utilizza protocollo WEP, il tool inizierà una fase di “fake authentication” (come è possibile osservare nella schermata a destra) per poi avviare una tecnica che prende il nome di “Arp Injection”. Allo stesso tempo, essendo ancora in ascolto, l'host cattura tutte le ARP request inviate dall'AP per poter collezionare IV.



Una volta raccolti abbastanza IV, il software avvalendosi del tool aircrack inizia la fase di cracking della password.

```
umberto@umberto-N56VZ: ~/Scrivania/progetto

Avvio crack wi-fi
Reading packets, please wait...
Opening hacking_info-01.cap
Read 283572 packets.

# BSSID ESSID Encryption
1 74:36:6D:58:55:CB Vodafone-Guest WEP (0 IVs)

Choosing first network as target.

Reading packets, please wait...
Opening hacking_info-01.cap
Read 283572 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 64565 ivs.
KEY FOUND! [ 50:72:6F:76:61 ] (ASCII: Prova )
Decrypted correctly: 100%

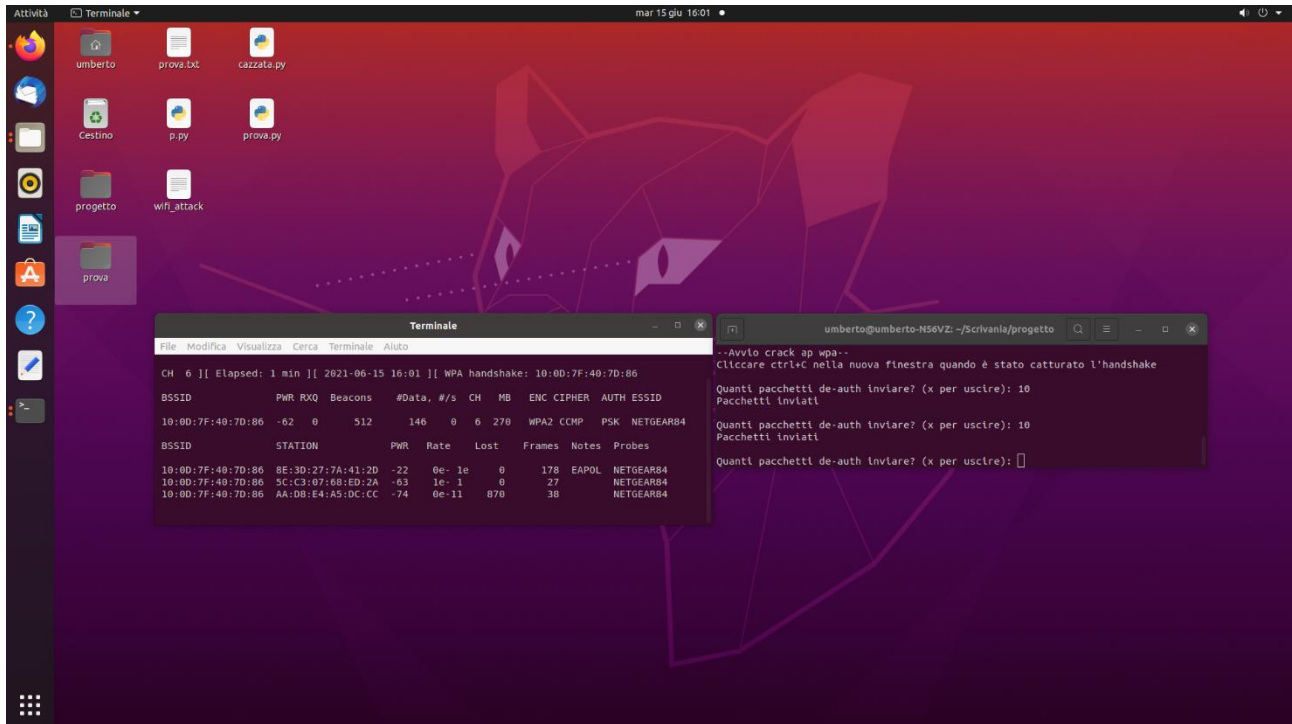
uscita tool...

wlp3s0mon disattivata modalità monitor

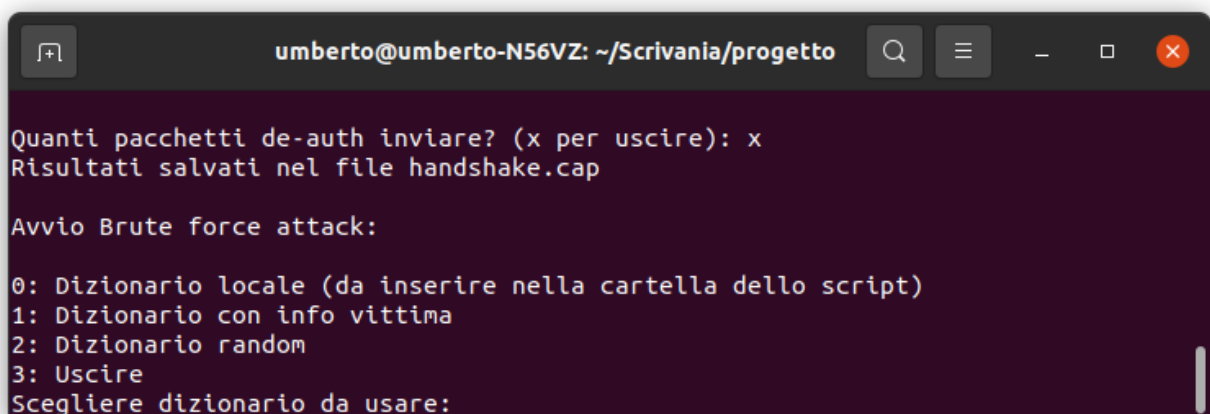
umberto@umberto-N56VZ:~/Scrivania/progetto$
```

Attacco a rete WPA

Mediante il tool aircrack, il programma comincia la fase di cattura dell'handshake tra station e AP. In particolare provvederà anche a inviare dei pacchetti di de-autenticazione in broadcast per mettere in condizione gli host di ricollegarsi alla rete e agevolare la cattura dell'handshake.



Una volta catturato l'handshake, l'utente dovrà decidere tra quali delle 3 tecniche messe a disposizione utilizzare per il cracking.



Dizionario locale

L'utente può scegliere di utilizzare un dizionario specifico inserendolo nella directory in cui si trova lo script.

```
umberto@umberto-N56VZ: ~/Scrivania/progetto
0: Dizionario locale (da inserire nella cartella dello script)
1: Dizionario con info vittima
2: Dizionario random
3: Uscire
Scegliere dizionario da usare: 0

Dizionario locale (da inserire nella cartella dello script)
Inserire nome file: dizionario_locale
Avvio crack wi-fi
Reading packets, please wait...
Opening handshake-01.cap
Read 8127 packets.

# BSSID          ESSID          Encryption
1  10:0D:7F:40:7D:86  NETGEAR84      WPA (1 handshake)

Choosing first network as target.
Reading packets, please wait...
Opening handshake-01.cap
Read 8127 packets.

1 potential targets

                                Aircrack-ng 1.6

[00:00:00] 9/11 keys tested (162.92 k/s)

Time left: 0 seconds                                81.82%

Current passphrase: heavysquirrel147

KEY FOUND! [ heavysquirrel147 ]
FE 88 04 69 84 5B B7 F9 B4 39 91 44 F1 D2 54 D8

Transient Key : 44 47 EE AA F7 D1 5A 55 20 D0 8E C7 52 C7 43 4F
               74 34 8A 43 86 6B F7 34 E8 71 B1 51 D5 DA C2 92
               DF 89 39 72 76 E6 F8 EA 3F 0F 55 F3 0F 74 85 5F
EAPOL HMAC   : C6 5C 2E 06 FF D5 2D A7 E6 15 8E 0B 7A 65 07 8D
uscita tool...

wlp3s0mon disattivata modalità monitor
umberto@umberto-N56VZ:~/Scrivania/progetto$
```

Dizionario creato a partire dalle informazioni della vittima

Mediante cupp, un potenziale utente può utilizzare tecniche di ingegneria sociale per poter creare un dizionario.

```
umberto@umberto-N56VZ: ~/Scrivania/progetto
Scegliere dizionario da usare: 1
Dizionario con info vittima
cupp.py!
# Common
# User
# Passwords
# Profiler
[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Umberto
> Surname: Gagliardini
> Nickname:
> Birthdate (DDMMYYYY): 04111997

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

> Pet's name:
> Company name:

> Do you want to add some key words about the victim? Y/[N]: n
> Do you want to add special chars at the end of words? Y/[N]: n
> Do you want to add some random numbers at the end of words? Y/[N]: n
> Leet mode? (i.e. leet = 1337) Y/[N]: n

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to dizionario_cupp.txt, counting 2883 words.
[+] Now load your pistolero with dizionario_cupp.txt and shoot! Good luck!
Avvio crack wi-fi
```

Dizionario random

L'ultimo strumento a disposizione prevede un tipico approccio a forza bruta per individuare la PSK

```
umberto@umberto-N56VZ: ~/Scrivania/progetto
Scegliere dizionario da usare: 2
Dizionario random
Numero minimo di caratteri: 2
Numero massimo di caratteri: 5
Crunch will now generate the following amount of data: 73645468 bytes
70 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 12356604

crunch: 100% completed generating output
Avvio crack wi-fi
```