# Wireless Security

## Abstract

There has been an increased demand for wireless networks due to the proliferation of laptop computers and mobile devices such as smart phones, tablets, and watches. With the development and release of new wireless devices as well as improvements in wireless technology, wireless security has been increasingly important. This survey paper will explore the improvement made to wireless security and make suggestions where future effort should be directed.

## Introduction

Wireless network connections are quickly becoming the most common way to connect personal devices to the network for Internet connectivity. Wireless networks are a part of daily life. They are prevalent in cafes, bookstores, airports, fitness gyms, work places, restaurants, etc. We did not get to today’s implementation of wireless networks without having learned some invaluable lessons along the way. The goal of this survey paper is to research existing protocols of wireless security and how the latest standard can be improved.

## Open System Authentication

Open System authentication is the default authentication protocol for 802.11. It authenticates anyone requesting authentication. A client will send an authentication request to an Access Point and the Access Point responds with an authenticate response The client then sends an Association Request to which the Access Point replies with an Association Response. The connection between the client and Access Point is then established.

### Tools

Wireshark is an open source multi-platform graphical user interface network traffic analysis tool that can be used to capture wireless network packets. With an open and unsecured wireless network, an actor can eavesdrop and capture all packets transmitted among clients of wireless network. Any data within those packets that is not encrypted at the application level will appear as plaintext. For example, if a user were to log into a server using Telnet over an open wireless network connection, the username and password would be exposed and parsed by Wireshark or any other network traffic analysis utility.

## Hidden or Cloaked Wireless Networks

Lucent defined a proprietary access control mechanism known as a “closed network”. Closed networks may be open networks that do not broadcast their Service Set Identifier. In theory, only those knowing the Service Set Identifier may attempt to associate with the closed network. However, cloaking networks is ineffective. While cloaking the Service Set Identifier hides networks from active scanning tools such as NetStumbler, the Access Point name is broadcast whenever an authorized system connects to the network. This is part of the association of the request packet. Intercepting the association request packets is trivial with tools such as kismet.

### Tools

Kismet is a graphical tool that enables passive detection and reconnaissance. Kismet is an 802.11 layer 2 wireless network detector, sniffer, and intrusion detection system. It works with any wireless network card which supports raw monitoring (RFMON) mode. Kismet listens for broadcast beacons issued by an access point which specify its Service Set Identifier. By using passive detection, it is very difficult for the victim network to detect that passive reconnaissance is taking place. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting closed networks, and inferring the presence of non-beaconing networks via the monitoring of data traffic.

## WEP

Wired Equivalent Privacy (WEP) protocol was an initial attempt to secure wireless network traffic. The goal was to restrict access to clients having the private, shared WEP key. The way shared key authentication works is by the following sequence of steps:

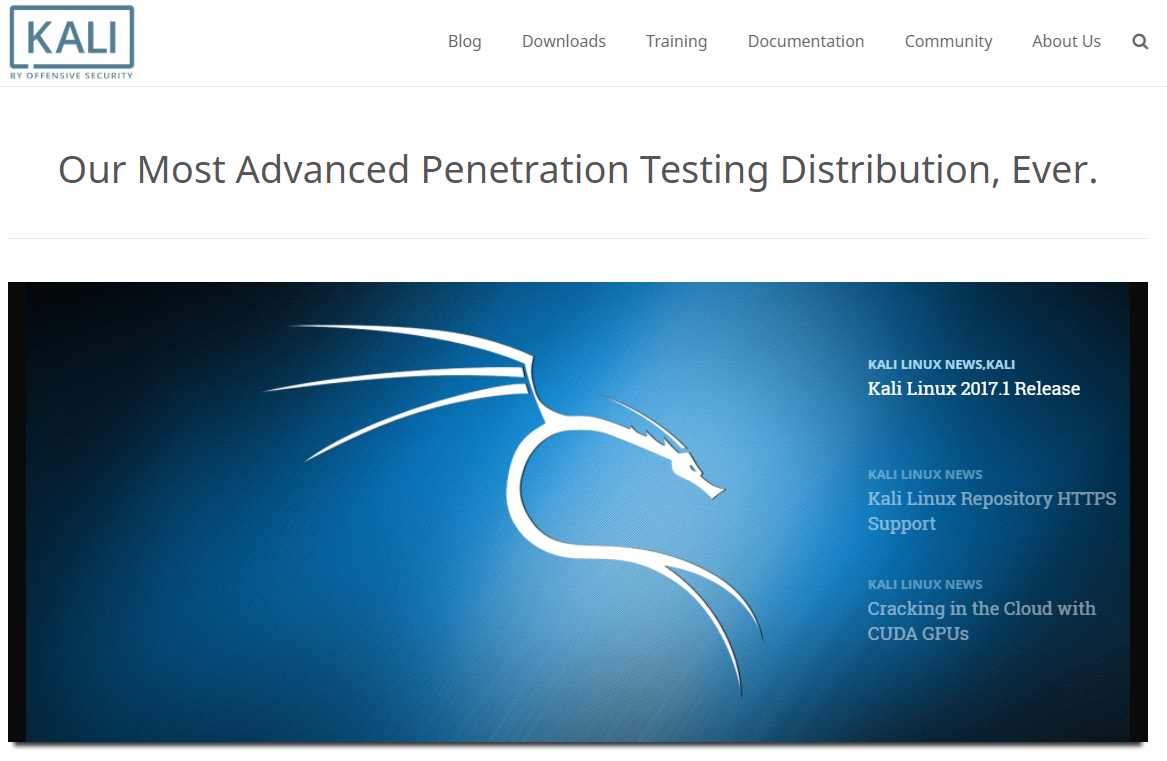
1. The client sends an authentication request to the Access Point.  
2. The Access Point responds to the client with a 128-bit challenge text.  
3. The client returns challenged encrypted with a shared key.  
4. The Access Point validates the encrypted response.  
5. The connection between the client and Access Point is established if the challenge matches.

However, WEP has a critical weakness. The Access Point challenge text is sent as plain text. This means that the encryption is XOR’d with the encryption stream and the known initialization vector simplifies cracking.

### Tools

#### Kali Linux

Kali Linux is a Debian derived open source project maintained and funded by Offensive Security for digital forensics and penetration testing. Kali Linux comes pre-installed with over 300 penetration testing programs. Kali Linux can run natively from a computer hard drive or as a Live CD or USB. It is a supported platform of the Metasploit Framework.



#### Airmon-ng

Airmon-ng is a bash script designed to turn wireless cards into monitor mode. It auto-detects which card you have and runs the right commands. It is necessary to enable monitor mode for wireless network interface cards in order to break WEP encryption.

#### Airodump-ng

Airodump-ng is part of the aircrack-ng suite. Airodump-ng is a packet capture tool for aircrack-ng. It allows dumping packets directly from WLAN interface and saving them to a pcap or IVs file. Airodump-ng is first used to list all available access points and clients. In monitor mode, one can view details of wireless devices and the associated channel number. Also in monitor mode, airodump-ng can be used to capture wireless traffic on a specific channel or SSID.

It is an alternative to Kismet because it does not have a visual component. Airodump-ng is more of a packet dump tool than a reconnaissance tool. It cannot change channels without restarting and it cannot drill down to particular networks.

#### Aireplay-ng

Aireplay-ng injects specially generated ARP-request packets into an existing wireless network in order to generate traffic. By sending these ARP-request packets again and again, the target host will respond with encrypted replies, thus providing new and possibly weak IVs.

Aireplay-ng supports single-NIC injection/monitor.

Aireplay-ng is also used to deauthenticate a “good” client. This may need to be run a few times in order to “kick” a client off.

#### Aircrack-ng

Aircrack-ng is a 802.11 WEP key cracking program. Aircrack-ng will recover a WEP key once a sufficient number of encrypted packets have been captured with airodump-ng.

## WPA

## WPA2

## WPA Enterprise

## Improvements