# 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.

## 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

## WPA

## WPA2

## WPA Enterprise

## Improvements