**ITC 134 2017**

How to Defeat a WIFI Pineapple

usenix white paper

Saving yourself from Pineapple wifi attacks

Eli Brown, Jess Allen, George Greer

How to defeat a wi-fi Pineapple

Eli Brown, Jess Allen, George Greer

Seattle Central College



Abstract

Presented to you in this white paper is a description of what a WiFi Pineapple is and a how-to for making sure you defend yourself against Pineapples.

In this paper, you will learn basic, proper techniques to ensure you don’t unknowingly connect to the WiFi through a Pineapple.

1 Introduction

A WIFI Pineapple Mark V, as it is formally known, is a small, hand-held device that when initial set-up has been performed, can act as a middle-man to an unsuspecting user and the resources they are accessing on the web without them ever knowing.

The Pineapple device uses an attack method known as Karma. Karma works by masking the known WiFi network that a user may have stored in their computer (ie. “Airport Free Wi-Fi”). The user has stored the authentication details of the airport they frequent for easy access when they need to check their email before their flight. The Pineapple device will mask as the network so the user, in actuality, without them knowing, has connected to the known WiFi network through the Pineapple device. Pineapple can now read all the information the user is accessing while using the WiFi network.

2 Research

WiFi Pineapple works by cloning an active WiFi connection, and “bumping” itself to the top of the list to be the first connected

3 Conclusion

Based on the knowledge we have gained through researching the best methods for protecting ourselves from unwanted connections, the most effective thing you can do is always re-authenticate your open internet connections. If you happen to find two versions of a network, one that is password protected, and one that is not, never chose the open connection.

Most places you go these days will have a WiFi password displayed. Always trust the “Secure Network”.

4 Bibliography