What is a Wi-Fi-Pineapple?

There only seems to be one true way anyone can defeat it and that’s by not letting it attach to your network via hardline or over Wi-Fi (WPA2-Enterprise or WPA2 Personal (CCMP-AES) with a strong passphrase) … the key thing is don't give it access. Pineapples love open Wi-Fi -Hotspots like Coffee Shops and Hotels. Remember nothing in life is free and basically anywhere easy access can be had with little authentication, bad Karma can be unleashed upon the un-expecting public

KARMA (a type of Man in the Middle attack) attacks are really based towards a user’s device: the “client”. The unsuspecting user’s device (computer, phone, etc.) is looking at an SSID and its last known good network was "SCC", which has been cloned to look real. Even though the real network “SCC” most likely uses WPA2-Enterprise w/Radius authentication, the victim’s device sends that SSID in the Probe Request message to any AP (and other known networks as well it has attached to in an attempt to get online), and the Pineapple is placed somewhere in the network. The rogue AP(Pineapple) sees this and updates the SSID list to be that SSID, the "SCC" in this case, and the client’s device sees this, then does the initial association, but the authentication sequences for WPA2/WPA2 Enterprise are never started and the Pineapple starts collecting information.

So how does one beat this?

To start, by always keeping your client up to date - newer devices don't send out the SSID in the probe request message … it's just sends "out a broadcast SSID, and then it picks and chooses the appropriate one. If the known good AP is a member of a well-built security network (WPA2 PSK/Enterprise) then you’re a little safer. Unfortunately, most networks aren’t that well designed. If your equipment is on the higher end of performance and quality and you have settings that have been tightened up, you’ll have a chance of setting up layers of security that can help you out with this. However, the default client management in Windows, Mac, Android, iOS, and Linux don't require authentication to be enabled, even on known networks.

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. However, dial up modems are rare in the modern computer landscape and almost functionally obsolete on a laptop being used away from a home or office with a functioning landline telephone system.

http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&sqi=2&ved=0ahUKEwjD7f\_S2P7RAhVGwVQKHXvWB3MQFgguMAI&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FRADIUS&usg=AFQjCNE3nnh7hcq2HmwhiSyMbfN1cPicpg&sig2=9to5yCszvfJk6-k4yz8sfg&bvm=bv.146094739,d.cGw

Radius servers and clients aren’t going to fix/solve Pineapple Karma attacks on their own, but they can keep a pineapple off the wireline controlled by the Radius server. Just remember that the pineapple doesn't need to be there; it all depends on what the pineapple operator wants to do with its ill-gotten information.

UTM (Universal Threat Management) can help in areas controlled by the network operator to keep rogues off the LAN. They can also detect and mitigate, to some degree, a pineapple in the area. There are documented cases where a UTM did detect a rogue AP, then started knocking clients off the rogue AP by sending de-authentication frames at the pineapple.

General protection measures are always recommended.

* keep your software up to date - since most networks aren't going to screen spyware for you, make sure your defenses are good.
* Use of anti-virus software (keeping it up to date and running system scans) and a personal firewall if you are concerned about your data and your system's integrity
* when using a work computer, use any VPN client you are given. It never hurts to use one even for default browsing, as it means your traffic will be routed through the network and some level of privacy is being applied.
* Never do unsecured transactions of sensitive data - always make sure HTTPS or SSL is on when you're sending a credit card, personal info, or other information you want kept private. In

So how can I be safe?

Turn off wireless auto-connect in the properties so that you are asked to connect each time (but remember, when you want more security you’ll give up convenience)

At home use ARP –a to find your devices to your router Look for a mac address, if the address is different then what you’re connected to, then you may have been attacked especially if there are duplicated SSID listed.

a) Don't use open Wi-Fi in public areas, or use it very sparingly

b) If one must, then VPN is an absolute necessity, even if only PPTP - VPN operates at a higher layer than a Pineapple does, so even if your client is (owned/pwned), the VPN will keep the upper layer of the network protocol traffic safe.

c) SSL verification - a bit of work, but keeping your browser current, and having only trusted SSL certs in your keychain can help - but SSLstrip can defeat this

d) Use a browser that supports HSTS, meaning that it'll first use HTTPS before falling back to HTTP - most modern browsers do this - Chrome, Safari, Firefox

Darren Kitchen, who created Wi-Fi Pineapple (SxS2012), aggressively touted this hacking tool. While Kitchen maintained that he sells his project mainly to security professionals, most reputable professionals have plenty of other ways to conduct valid security audits. There are many free products on the Internet that are specifically made for security professionals that do a much better job for legitimate needs of managing Wi-Fi networks.

So, exactly who is buying Wi-Fi Pineapple? One has to wonder, as Kitchen’s marketing seems to target novice hackers rather than security professionals. At the very least, Wi-Fi Pineapple is a good reminder that you should always protect your communications in Wi-Fi hotspots. Use a virtual private network such as Private Wi-Fi. Otherwise, you could be Wi-Fi Pineapple’s next Bad Karma victim.