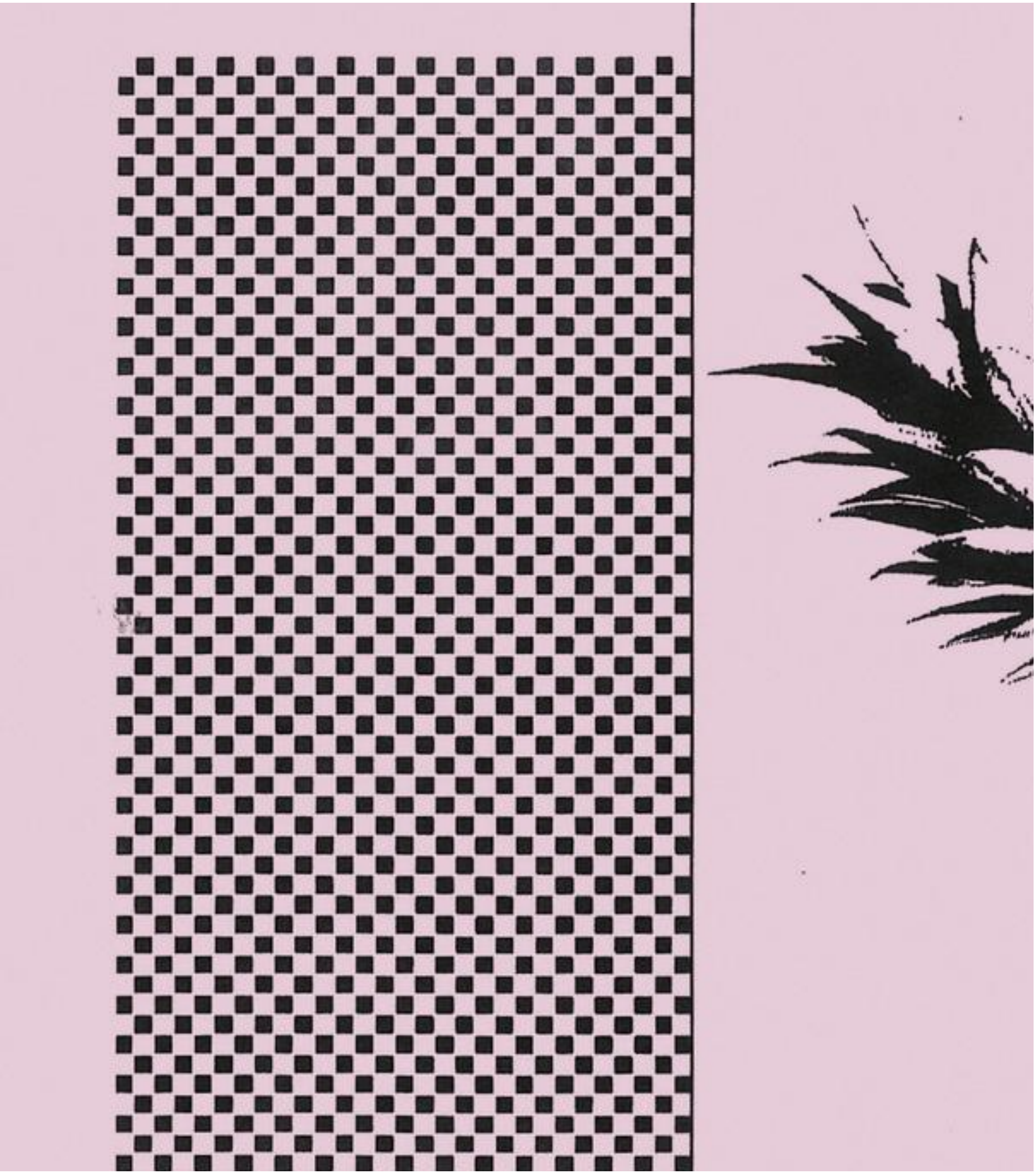

HOW HACKING WORKS

How a Wi-Fi Pineapple Can Steal Your Data (And How to Protect Yourself From It)

Daniel Oberhaus
Nov 20 2017, 8:43am

The Wi-Fi Pineapple enables anyone to steal data on public Wi-Fi networks. Here’s how it facilitates two sophisticated network attacks and how to protect yourself against them.

SHARE TWEET

This article is part of ***How Hacking Works****, Motherboard's guide to demystifying information security.*

In popular media, hackers are often portrayed as an elite cabal of ski mask aficionados and computer experts that can keyboard mash their way into any digital device. But what if I told you that you can also pwn almost any internet connected device around you, even if you can’t tell an SSL from an SSID?

Yes, my friend, the device you are looking for is a **Wi-Fi Pineapple**, which can turn anyone from hack to hacker for the low, low price of $99. Since it is so cheap and easy to use, it's important to understand how the Pineapple works in order to protect yourself against its attacks.

The Pineapple is a nifty little device first released in 2008 by **Hak5**, a company that develops tools for penetration testers, or "pentesters." Pentesters are usually hired by organizations to attack their own networks in order to expose vulnerabilities before they are discovered by some bad actors. The Pineapple allows pentesters to easily execute sophisticated attacks on public Wi-Fi networks to see how the attacks work and how to protect the network from those attacks.

Pineapples aren't much different than the normal Wi-Fi access points you use to get internet at home or in the office, just more powerful. They use multiple radios rather than just a single radio found in most routers. This means a Pineapple is able to interface with hundreds of devices at a time, rather than just a few dozen. Moreover, the Pineapple's web interface is optimized to execute complicated network attacks.

> ***Read More: The Motherboard e-Glossary of Cyber Terms and Hacking Lingo***

"When I invented the Wi-Fi Pineapple, I saw that Wi-Fi had inherent flaws that made it vulnerable to spoofing attacks," Darren Kitchen, the founder of Hak5, told me in an email. A spoofing attack is when a hacker impersonates a service or device in order to gain access to a victim's data.

“A lot of nefarious types had already taken advantage of these weaknesses, but the majority of people weren't aware of the problem,” Kitchen added. “I figured if information security people had access to a device that could easily exploit these flaws, it would raise awareness and get things fixed.”

Although the Pineapple has always had a cult following within hacker circles, it recently rose to prominence after it was featured as a major plot point in the shows ***Silicon Valley*** and ***Mr. Robot***.

In these shows the device was used to spoof a website and to execute a man-in-the-middle attack to hack the FBI, respectively. According to Kitchen, who served as a technical advisor on the *Silicon Valley* episode, the fictional depiction of the Pineapple in these shows isn't so far from the truth.

The Pineapple is an invaluable tool for pentesters, but its popularity is also due to the fact that it can be used for more nefarious purposes. Hackers can easily wield the device to collect sensitive personal information from unsuspecting users on public Wi-Fi networks.

It's important to keep in mind that just because you *can* pwn all the things with a Pineapple, doesn't mean it's legal or that you *should.* Owning a Pineapple is legal, but taking money out of someone's bank account by stealing their unencrypted password is not. The Pineapple just makes grabbing unencrypted passwords sent over Wi-Fi easier. I am not a lawyer, but in general, if you do not have explicit permission to use the Pineapple on a network that you own as well as from anyone who could reasonably connect to that network, you are treading in dangerous territory.

Again: Executing a Pineapple's exploits on a network you don't own if you're not a pentester working in a professional setting can quickly put you into illegal territory. Even if you don't get caught, you're still an asshole for doing it, so just...don't.

> ***Read More: The Motherboard Guide to Not Getting Hacked***

This guide is meant to be an informational glimpse into the world of network pentesting, as well as a reminder about the importance of personal information security. After showing you just a few of the ways a Pineapple can be used to pwn you, I'll also walk you through some simple steps you can take to make sure you're never on the wrong end of a malicious Pineapple attack.

Hak5 makes a few different versions of the Pineapple, but while putting together this article I used its cheapest model, which I bought at the DEF CON hacking conference for the purposes of this article: the Pineapple Nano. I configured it on a Windows computer, although it's also compatible with iOS and Linux systems.

The Pineapple Nano. Image: **Hak5**

The initial setup is a piece of cake. All you need to do is plug it into the USB port on your computer, navigate to the Pineapple's IP address and it'll take care of the rest. After you've updated your login information for the Pineapple, you're ready to try some exploits.

EXPLOIT #1: WALL OF SHEEP

Every year at DEF CON, one of the largest hacking conferences in the world, the Packet Hacking Village hosts the **Wall of Sheep**. This is essentially a running list of devices that have connected to an insecure network at DEF CON. The list is usually displayed on a large projector screen at the Packet Hacking village, where anyone can see not only the device's ID, but also the websites it was trying to access and any relevant credentials.

It's a light-hearted way of shaming people into better information security, and you can easily create your own Wall of Sheep using a Pineapple.

> ***Read More:* *72 Hours of Pwnage: A Paranoid N00b Goes to DEF CON***

All of the exploits for the Pineapple are freely available as downloadable modules on the Pineapple's dashboard and usually only take a single-click to download and install on the device. Once the Wall of Sheep module (called 'DWall') is installed on a Pineapple, any device that connects to it will basically be broadcasting their browsing traffic to the owner of the Pineapple.

The exception to this, of course, is if the would-be victim is using a Virtual Private Network (VPN) to encrypt their web traffic or only visiting pages secured by Secure Hypertext Transfer Protocol (HTTPS). This protocol **encrypts the data being routed between the website's server and your device** and effectively prevents eavesdroppers from seeing which websites you're visiting. HTTPS also helps protect your web habits from your internet service provider, which can only see the top level domain habits of its users (for instance, that you visited Motherboard, but not that you clicked on this article).

Although over **half the web has switched to HTTPS** from its insecure predecessor, HTTP, a 2017 **Google audit** found that nearly 80 percent of the top 100 websites don't deploy HTTPS by default. This means that anyone who inadvertently connects to a Pineapple and then browses to an HTTP version of the site is basically exposing all of their activity on that site, from pages visited to search terms, to the person wielding a Pineapple.

Many websites have both an HTTP version and an HTTPS version, which as we'll see in the exploit, is a security vulnerability that can be exploited by a Pineapple.

The original Pineapple released in 2008. Image: Darren Kitchen/Hak5

EXPLOIT #2: MAN-IN-THE-MIDDLE + EVIL PORTAL

Pineapple man-in-the-middle (MITM) attacks are really the main reason pentesters get this device.

MITM attacks are a way of eavesdropping on a user by inserting a Pineapple between the user's device and legitimate Wi-Fi access points (in terms of how data is routed through the network, not necessarily literally between them in meatspace). The Pineapple then pretends to be the legitimate Wi-Fi access point so it can snoop on all the information as it relays data from the device to the access point.

Another way of thinking about MITM attacks is that they are kind of like if someone dropped a letter in their mailbox and then a stranger opened up their mailbox, read the letter and then put it back in the mailbox to be sent.

> ***Read More:*** ***Turning Off Wi-Fi and Bluetooth in iOS 11 Doesn't Actually Turn Off Wi-Fi or Bluetooth***

So how does a Pineapple trick your device into think it is a legitimate access point? There is a **native feature on the Pineapple that scans for service set identifiers** (SSID)—the names of Wi-Fi networks—that are being broadcast from devices in its vicinity.

Any time you connect to a Wi-Fi network on your phone or computer, your device saves that Wi-Fi network's SSID in case you ever need to connect to that Wi-Fi network in the future. But this convenience comes with a major cost.

Let's say you connected to the Wi-Fi at your favorite local coffee spot, and its network is called "Human_Bean_wifi". After you've left the coffee shop, your phone or laptop will start broadcasting a signal that is basically asking if Wi-Fi access points around the device are "Human_Bean_wifi." It does this for any network you've connected to in the past.

"A quick reality check is usually all it takes to see if you've been duped by a Wi-Fi Pineapple."

Pineapples are able to take advantage of this feature by scanning for all the SSIDs being broadcast by devices in its vicinity. It then rebroadcasts these SSIDs so that it can trick devices into thinking it is an access point that has been connected to in the past. So to use the above example, the Pineapple will see that your phone is asking, "Is this network 'Human_Bean_wifi'?" and then start broadcasting its own signal that says "Yes, I am 'Human_Bean_wifi', connect to me."

Put another way, this would basically be like walking around with a set of keys to your house and asking every stranger you meet if they are your roommate. In most cases, those strangers will say “no,” but you also run the risk of running into an ill-intentioned stranger who will lie to you and say “yes, of course I am your roommate. Please let me in,” and then proceed to steal all your stuff.

> ***Read More: The Motherboard Guide to VPNs***

But getting devices to connect to a Pineapple is only half of executing a MITM exploit. An attacker also must be able to read the data being routed from the device through the Pineapple. There are a couple of ways to do this.

A Pineapple can be used to create an “**Evil Portal**,” which basically creates fake versions of websites to capture usernames and passwords, credit card information or other sensitive data.

These work by creating a local server on the attacker’s computer to host a web page that looks like a regular login page for a well trafficked service like Gmail or Facebook. These pages can easily be duplicated using free online services.

Then the attacker configures their Pineapple so that when any devices that are connected to it try to browse to a website like Twitter or Facebook, they will actually be redirected to the fake webpage being served by the attacker’s computer. If the victim enters their information on this page, their username and password will be revealed to the attacker without the user ever knowing they’ve been pwned.

Another way of gathering information about someone’s browsing habits with a MITM attack is to use modules built for the Pineapple that **block forced HTTPS encryption and read the data** that would otherwise have been secure.

For example, consider a website like Motherboard, which *is* secured with HTTPS. If you simply type in “motherboard.vice.com” in your URL search bar and press enter, you will be submitting an HTTP request to Vice’s servers. Vice’s servers will then field this request and respond to your device by directing it to a secure HTTPS version of the site. (This is the same for many major websites, such as Twitter).

Forcing users to an HTTPS version is a great way to beef up a website’s security, but it’s the user’s HTTP request in the beginning that can be exploited with a Pineapple. A module called SSLSplit is able to monitor HTTP requests from a user’s device when it is connected to the Pineapple. It will then route this request along to the appropriate server, but when the server responds with the secure HTTPS link, the Pineapple will “strip” away the secure layer and serve an HTTP version of the site back to the user.

At this point, the user will effectively be browsing an insecure version of the site, which will appear almost exactly the same. The only difference will be that a little lock icon will have disappeared from the upper left corner of the screen.

Always check for this lock icon in the upper left of your internet browser.

This attack clearly demonstrates the importance of encrypted communication protocols such as HTTPS. Without them, all the data being routed between the device and the access point can be easily read by anyone with a Pineapple.

HOW TO PROTECT YOURSELF FROM MALICIOUS PINEAPPLE USERS

The hacks discussed above are just the tip of the iceberg. Fortunately, there are a number of simple steps you can take to protect yourself from getting pwned by some asshole with a Pineapple.

BE WARY OF PUBLIC WI-FI NETWORKS

The easiest thing you can do is only connect to Wi-Fi networks you know and trust. Your home network, for instance, is almost certainly safe from a Pineapple attack. This is because a Pineapple must also have access to the network it is trying to monitor traffic on, so unless the attacker has access to your home Wi-Fi credentials, they won't be able to pwn you with a Pineapple.

Same goes for your office Wi-Fi—unless, of course, your office has hired a pentester to audit its network. The real danger of a Pineapple attack is on public networks—places like your local coffee shop or the airport are all prime places for an attack. Most people don't stop to check whether the "free_airport_wifi" access point is legit and connect without thinking.

When it comes to networking infosec, vigilance is key. The most secure option is to never use public Wi-Fi networks at all. That is a major pain in the ass, however, and will almost certainly drive up your cell phone bills for data use. (For what it's worth, your **cell phone isn't safe from IMSI catchers either**, but I digress).

VIRTUAL PRIVATE NETWORKS

If you must get on public Wi-Fi, your best bet is to get a VPN. VPNs are a secure way of surfing the net by first connecting to a VPN server before venturing onto the World Wide Web. The VPN server encrypts your data before routing it to its destination, essentially creating a protective shell for your data that makes it unintelligible to prying eyes. So even though an attacker may be able to see that your device has connected to their Pineapple, if you're using a VPN they won't be able to see the data they are routing.

"Using a VPN is still the best advice," Kitchen said. "When you use a VPN, anyone peering into your traffic is only going to see an encrypted mess. That goes for any eavesdropper—be it a Wi-Fi Pineapple, your ISP, an employer or even our wonderful government."

Choosing the right VPN **can be a really tough challenge**. Here's **a simple guide** with some suggestions.

HTTPS ONLY

Another good rule of thumb is to only visit websites secured with HTTPS (like Motherboard!) These days, most websites you're likely to visit on a day-to-day basis that have sensitive information on them have switched over to this security standard from HTTP, thanks to a concerted industry effort to push HTTPS, including Google's algorithms privileging sites with security over those that aren't encrypted. Still, Pineapple modules are able to force a connected device onto an insecure (HTTP) version of a site if the visitor didn't explicitly type https:// before the domain name.

Read More: Wikipedia's Switch to HTTPS Successfully Fought Government Censorship

"Unfortunately too many websites don't use HTTPS, and many that do are still susceptible to downgrade attacks," Kitchen told me. "If you're venturing anywhere off the beaten path, I'd advise against using this as your only line of defense. It's still important to stay vigilant and check for HTTPS, but pack a VPN too."

In short, always make sure to check the URLs of the websites you visit to make sure they're using HTTPS. Browsers like Chrome, Firefox, and **Opera** make checking website security easy with a small padlock icon that says "Secure" on the left hand side of the address bar and warning users before they visit an insecure site.

ALWAYS FORGET

Finally, it's important that whenever you are done connecting to a public Wi-Fi network that you configure your phone or computer to 'forget' that network. This way your device won't be constantly broadcasting the SSIDs of networks it has connected to in the past, which can be spoofed by an attacker with a Pineapple. Unfortunately there is no easy way to do this on an Android or an iPhone, and each network must be forgotten manually in the "Manage Networks" tab of the phone's settings.

Another simple solution is to turn off your Wi-Fi functionality when you're not using it —**though that isn't as easy to do on some devices anymore**—and don't allow your device to connect to automatically connect to open Wi-Fi networks.

Read More: WiFi Signals Can ID Individuals by Body Shape

While it's easy to get paranoid and wonder if there's a Pineapple waiting to pwn you any time you get a Wi-Fi connection, most Pineapple exploits can be easily avoided by simply staying vigilant about your network settings and internet experience. For all their prowess at manipulating electronics, hackers are still very much dependent on human error for their craft.

"The Wi-Fi Pineapple is really good at mimicking Wi-Fi networks you've connected to in the past," Kitchen said. "If you're at a park and your device says it's connected to an airplane's Wi-Fi, something is amiss. A quick reality check is usually all it takes to see if you've been duped by a Wi-Fi Pineapple."

SHARE TWEET

HOW TO MAN IN THE MIDDLE WI-FI PINEAPPLE DARREN KITCHEN HAK5

Watch This Next

11:05

Nuclear Fusion Energy: The Race to Create a Star on Earth