Security Best Practices - Part 2c: Encryption

Kaneesha D. - 2018-06-14 - in Best Security Practices

2c. Encryption

TL/DR: Always use encryption where available, the stronger the better, however local laws may force you to surrender your encryption keys if mandated. Some countries do not even require permission from a court.

Encryption is the practice of turning normal text into gibberish. Encryption works by scrambling the original message with a very large digital number (key). This is done using advanced mathematics. Commercial-level encryption uses 128 bit key that is very, very hard to crack. The computer receiving the message knows the digital key and so is able to work out the original message.

The most secure encryption works on multiple tiered system;

- ***Encryption:*** This is the symmetric cipher algorithm with which all of your data is encrypted and decrypted. The symmetric cipher is used with an ephemeral secret key shared between you and the server. This secret key is exchanged with the Handshake Encryption.
- ***Authentication:*** This is the message authentication algorithm with which all of your data is authenticated. This is only used to protect you from active attacks. If you are not worried about active attackers you can turn off Data Authentication.
- ***Handshake:*** This is the encryption used to establish a secure connection and verify you are really talking to a Private Internet Access VPN server and not being tricked into connecting to an attacker's server. We use TLS v1.2 to establish this connection. All our certificates use SHA512 for signing.

Currently there are two main models of encryption available;

AES (Advanced Encryption Standard) is is a symmetric cipher based on the Rijandael block cipher that is currently the United States federal government standard. AES was adopted worldwide as the heir apparent to the now deprecated DES standard of 1977 and although there are published examples of attacks that are faster than brute force, the powerful AES technology is still thought to be computationally infeasible in terms of cracking. In addition, AES offers solid performance on a wide variety of hardware and offers both high speed and low RAM requirements making it a top-notch choice for most applications.

If you're using a Mac, the popular encryption tool FileVault is one of many applications that uses AES.

RSA is one of the first widely used asymmetric cryptosystems for data transmission. The algorithm was first described in 1977, and relies on a public key based on two large prime numbers and an auxiliary value in order to encrypt a message. Anyone can use the public key in order to encrypt a message but only someone with knowledge of the prime numbers can feasibly attempt to decode the message. RSA opened the doors to several cryptographic protocols such as digital signatures and cryptographic voting methods.

I*t's also the algorithm behind several open source technologies, such as GPG, which allows you to encrypt digital correspondence.*

In addition to AES and RSA, there is also **Elliptical Curve Cryptography (ECC)** and is among the most powerful and least understood forms of encryption used today. Proponents of the ECC approach cite the same level of security with faster operational times largely due to the same levels of security while utilising smaller key sizes. The high performance standards are due to the overall efficiency of the elliptic curve, which makes them ideal for small embedded systems such as smart cards. The NSA is the biggest supporter of the technology, and it's already being billed as the successor to the aforementioned RSA approach.

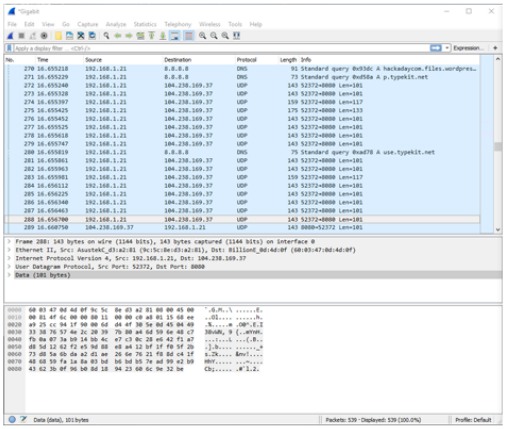
That sounds all great and technical, but what does this mean?

Basically put, it makes files and browsing habits completely nonsensical. This can be easily illustrated by capturing the data as it moves across a network using capturing software such as Wireshark.

To illustrate what happens over a network, we opted to capture data whilst connected to the Private Internet Access service on both the Ethernet card (Gigabit) and TAP adapter (Ethernet).

The Ethernet card is not protected as it sends the data to the TAP Adapter (which is the PIA service) to be encrypted and transmitted. In a normal network, the Ethernet card would transmit directly.

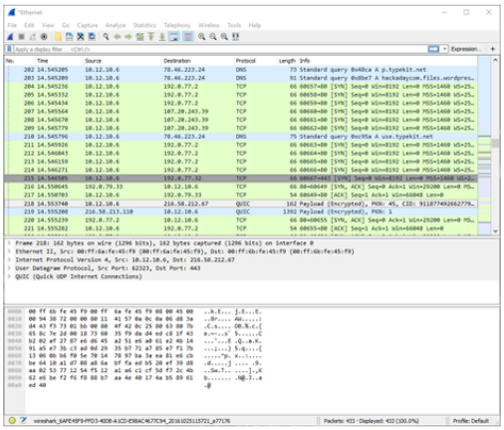
Network without a VPN or Encryption



As you can see, the traffic clearly shows my connected IP (104.237.169.37 which is actually a PIA IP), how I connect (Asus Router and Billion Modem) and what I'm browsing to (www.hackaday.com). Without a VPN or encryption, location and identity can easily be confirmed through IP and devices.

However the TAP adapter encrypts and transmits the data to the required servers. This protects the end user by providing privacy and security. The IP is not transmitted and hardware cannot be identified.

Network with VPN & Encryption



Please Note:

Although Private Internet Access opts to offer Elliptical Curve Encryption (ECC), the recent NSA revelations have raised concerns that certain or possibly all Elliptic Curves endorsed by US standards bodies may have backdoors allowing the NSA to more easily crack them.

There is no proof of this for curves used with signing and key exchange[†] and there are experts who think this to be unlikely. We therefore give users the option but display a warning anytime you select an Elliptic Curve setting. We also included the less standard curve secp256k1, which is what Bitcoin uses, was generated by Certicom (a Canadian company) instead of NIST (as the other curves were), and seems to have less places to hide a backdoor.

† There is strong evidence that a random number generator which uses ECC was backdoored but it was not widely used.

Tags

Security

Related Pages

- Security Best Practices