Introduction to Encryption

Elizabeth Adelaide

March 28, 2017

Summary

Encryption is a tool to protect data and messaging. Several consumer applications use encryption. Developing an understanding of encryption and what apps are available can help secure personal data.

What is Encryption?

Encryption is a mathematical tool which can make it essentially impossible to read data without a password. Encryption relies on keys which can be used to decrypt information. In the majority of cases, private keys are used. The encryption process uses the private key to alter the data until it is unreadable. The data can only be readable with the private key. Private keys are essentially passwords, if you have the private key you have access to any information that is encrypted using that key. The problem with private keys is that they are difficult to share. Unless you decide to have back-alley meetings and exchange the password on a scrap piece of paper (to be burned after reading), there needs to be a secure way to share private keys. This is where public keys come into play.

Public keys are based on a specific use of mathematics to securely share information without revealing private keys. Public key encryption is slow, and the encryption will generally be used to share private keys. The private key will then be used to encrypt and decrypt the actual messages. One form of public key encryption is called RSA. There are many types of encryption, RSA is outdated, however newer encryptions use the same principles.

RSA starts with one person, who in computer security is referred to as Alice. Alice chooses two large prime numbers labeled p and q. These prime numbers are generally selected by a program which have a list of sufficiently large numbers. She then takes the product of these two numbers, pq. This product is the public key. The product is publicly available. The person who wants to send Alice a message, known as Bob, can use this public key to send a message. He can use a few mathematical tricks to send a message to Alice that can only be decoded by knowing the individual values of p and q. Since only Alice can decode it, the message can be securely sent to her.

There are several factors that determine how robust an encryption method is. The most basic attack against encryption would be to use a computer to try every possible key. This is referred to as a brute force attack. A good encryption method should be strong enough so that it will take many years to finish a brute force attack. Encryption methods can also be vulnerable to more specific attacks. Encryption methods such as AES and DSA are constantly scrutinized by mathematicians and security experts for any holes in the security. They are considered secure because no one has publicly stated any holes. Less popular encryption methods are likely to be less secure because there are less people actively searching for security holes in the method. It is best to use popular methods when choosing an encryption method.

A messaging app can then set up secure communication between two parties. Using `https://` also uses this form of encryption. Your messages cannot be monitored by an external party as long as there is this form of encrypted communication. External parties can gain access through other methods, and can collect meta data on your messages. Encryption only offers one level of protection against attacks. It is best to use a combination of good security practices when securing data and communications.

Security Concerns

Any data that is encrypted cannot be read by someone that does not have the private key. However there are several ways attackers can gain information about secure communication. It is important to consider these issues when attempting secure data storage or communication.

One basic security concern is not having encrypted data. Having a password does not necessarily mean that data is encrypted. It is often the default that data is not encrypted. Windows, Mac and Linux do not automatically encrypt data. Most messaging services do not encrypt data. Even if the device is password protected, it is fairly easy to gain access to the computer. This is especially true if the attacker can gain physical access to the device. It is important to check that any information that you desire to be protected is encrypted, and that any messaging is done between encrypted applications. Both applications must use encryption in order for the communication to be encrypted. It is also important to check that data is not cached in an insecure way. Caching is a procedure done by many applications. Google chrome will cache web pages so they reload faster. Microsoft office caches your documents to autosave. It is important to turn off caching if you are working securely, or to use applications that do not cache data.

Another concern is the security of passwords. User generated passwords are used in many applications to control access. Passwords that are short, common or intuitive are particularly vulnerable. Password attacks are commonly brute force, dictionary attacks or done through interpersonal knowledge. Brute force and dictionary attacks target large platforms. Brute force attacks try every combination of letters and numbers until they guess the password. This is effective against insecure platforms that do not properly prevent guessing attacks. Captchas and limiting the number of password attempts are a simple way to reduce vulnerability against brute force attacks. Passwords that are short are the most vulnerable to this type of attack. Dictionary attacks guess using a dictionary of common passwords. They might attack a platform by trying to guess a large number of users' passwords. Passwords such as “password” or other common words are particularly vulnerable. Platforms can increase their security by instituting password rules, however they must be careful not to apply too many rules to make it difficult for a human to use. Interpersonal knowledge is the most effective form of attack against a single person. Passwords that are shared, written down, or easily guessable are vulnerable to these attacks. Setting devices to delete all data after several failed attempts can also deter attackers.

Malware is another major concern in security. Effective malware can target a device and be able to operate past encryption methods. The malware cannot actually decrypt data, but can log passwords and read data when the user decrypts it. The threat of malware can be reduced by only installing trusted applications, and by using an up-to-date antivirus.

Finally metadata can be used by an attacker. While an attacker cannot read encrypted data, they can tell the origin and destination of encrypted communications, the amount of data. Sufficiently powerful attackers can log when a secure application was installed. This data can reveal patterns in communications.

There are many other concerns when using encrypted data, it is important to continue to improve security practices and to be wary of how data is stored and shared.

Common Applications

There are several applications which can secure data and communications. There are several factors to consider when choosing to use these apps. Applications that use their own encryption should be avoided. “Security through obscurity” is a practice that leads to security holes which reveal user data. Additionally applications that insecurely cache data should be avoided. Users must also use good security practices when using any application.

Messaging Apps

There have been several messaging apps which use encrypted messaging as a default feature. These apps include *Signal*, *Telegram*, *WhatsApp*, and *Facebook Messenger*. Each application has draw backs. All of these applications require both users to have the app installed. Communications to standard text users will not be secured. *Signal* is considered the most secure option. It offers password protection and automatic deletion of messages. The default option is encrypted messaging. *Telegram* is not an effective messaging app, because it uses its own encryption method. Additionally, it does not encrypt messages by default. *WhatsApp* offers default encryption. However, *WhatsApp* can reveal private information such as names, locations and friends which can be used in Doxxing. *Facebook Messenger* does not encrypt messages by default, however encryption can be turned on. *Messenger* also allows time sensitive messages. *Messenger* can be insecure due to the vulnerability of Facebook profiles. Both *WhatsApp* and *Messenger* are owned by Facebook, and face vulnerabilities to password attacks and Doxxing.

Browsers

Common browsers are Firefox, Google Chrome, Internet Explorer and Safari. All of these browsers can use some level of security by using only `https://` sites, and avoiding javascript. Using `https://` will prevent external parties from monitoring your browsing habits. Javascript can be used to download malware. Most browsers will also cache your data by default. Chrome particularly will cache your data and connect it to your google account. Additionally many sites, including Facebook, Google Search and Amazon will record your searches and information. Avoiding sites that record data can reduce your ability to be traced and monitored.

Tor or Onion Browser is considered a more secure browsers. Instead of directly connecting to a website's sever, Tor sends a layered encrypted message to at least four routing points. At each point a layer is removed. This system prevents simple tracking of internet use. A powerful attacker can attack several points of a Tor system and compromise the security, however in day-to-day use it is fairly secure. Tor also has several default features which increase security. It prevents javascript from gathering information, prevents downloads without permission and notifies you if there is an insecure connection.

VPNs (Virtual Private Networks) are a another tool to increase internet security. A VPN can be used for several reasons, it simply creates a private network as if you were only connecting to computers within your own home. For security, the VPN can allow a user to access the internet through an ISP (Internet Service Provider) that does not monitor or log traffic. VPNs can also avoid censorship by accessing the internet through another country. A VPN provider needs to be carefully chosen to be secure. For a secure connection that VPN should not be based in the fourteen eyes agreement (Australia, Canada, New Zealand, United Kingdom, United States of America, Denmark, France, Netherlands, Norway, Belgium, Germany, Italy, Spain, and Sweden). The five eyes, nine eyes and fourteen eyes agreements are between countries that share data with each other. A VPN based in a different country will be more likely to refuse to share data. A VPN should also not log your data, and should have high quality anti-malware services.

Data Storage

Stored data can be encrypted to ensure data can only be accessed through a password. It is important to remember that most data is not stored encrypted by default, even if there is a password. One of the simplest ways to store secure data is to have an encrypted portable hard drive, or flash drive. There are several tools to encrypt drives. Veracrypt is a popular and straightforward tool. Portable drives can be used to secure data, however it is important to be sure that the data is not cached on the unencrypted main drive.

A linux OS can also be installed on an encrypted drive or partition. Most linux distributions offer the option to encrypt the hard drive during installation. A basic linux OS such as Arch, Gnoppix, or freeBSD (which is technically not a linux distribution), can be run with a few secure applications. This approach also allows the use of these applications on any computer that the user has access to.

Additionally there are several tools which can encrypt individual files. This can be helpful for specific applications. It is important to ensure that there is no unencrypted data that is cached. Additionally, an individual file can reveal more metadata (size of file, data of creation, owner).