Different Types of Encryption

You have probably heard "**encryption**" used in several contexts and with different words around it. Generally, **encryption** refers to the mathematical process of making a message unreadable except to a person who has the **key** to "**decrypt**" it into readable form. Encryption is the best existing technology we have to protect information from government, service providers, and technically skilled hackers, and it has developed to the point that it is virtually impossible to break when applied correctly.

When we talk more specifically about the kind of information we are encrypting, it can be a clue to exactly how the encryption is being applied and what it's protecting users from.

In this guide, we'll look at two major ways encryption is applied: to data in transit and to data at rest.

Encrypting data in transit

Data "in transit" is information that is moving over a network from one place to another. When you send a message on a messaging app, for example, that message moves from your device, to the app company's servers, to your recipient's device. Another example is web browsing: when you go to a website, the data from that webpage travels from the website's servers to your browser.

There are two ways to **encrypt** data in transit: **end-to-end encryption** and **transport-layer encryption**. You will often hear these phrases associated with securing your communications (e.g. texts, emails) or securing your web browsing traffic. These refer to the type of security a certain app, website, or platform supports, and you can use the type of encryption a service supports as one important factor when deciding what services are right for you.

End-to-end encryption ensures that information is turned into a secret message by its original sender (the first "end"), and decoded only by its final recipient (the second "end"). This means that no one can "listen in" and eavesdrop on your activity, including wifi cafe snoops, your Internet service provider, and even the website or app you are using itself. Somewhat counter-intuitively, just because you access messages in an app on your phone or information from a website on your computer does *not* mean that the app

company or website platform itself can see it. This is a core characteristic of good encryption: even the people who design and deploy it cannot themselves break it.

Not to be confused with end-to-end encryption is **transport-layer encryption**. While end-to-end encryption protects messages, for example, *all* the way from you to your recipient, transport-layer encryption only protects them as they travel from your device to the app's servers and from the app's servers to your recipient's device. In the middle, your messaging service provider—or the website you are browsing, or the app you are using—can see unencrypted copies of your messages. Because the company's servers can see (and often store) your messages, that may leave them vulnerable to being requested by law enforcement or leaking if the company's servers are compromised.

A key question to ask to differentiate end-to-end and transport-layer encryption is: Do you trust the app or service you are using? Do you trust its technical infrastructure? How about its policies to protect against law enforcement requests? If the answer is "no," then you need end-to-end encryption.

Overall, end-to-end encryption provides much stronger security than transport-layer encryption.

A key question to ask to differentiate end-to-end and transport-layer encryption is: Do you trust the app or service you are using? Do you trust its technical infrastructure? How about its policies to protect against law enforcement requests? If the answer is "no," then you need end-to-end encryption. If the answer is "yes," then a service that supports only transport-layer encryption may suffice for you—but it is generally better to go with services that support end-to-end encryption when possible.

Encrypting data at rest

Data "at rest" is data that is stored somewhere: on a cell phone, laptop, server, or external hard drive, for example. When data is at rest, it is not moving from one place to another.

A common example likely to be most relevant to your learners is device or **"full-disk" encryption**. When you enable full-disk encryption, you encrypt all the information stored on a cell phone or laptop and protect it with a passcode or other login method. On a cell phone, this will usually look like a lock screen that requires a passcode, **passphrase**, or **fingerprint**. (However, beware! A lock screen does not always mean that full-disk

encryption is enabled. On a laptop, this will usually mean that getting into the device requires a passphrase.)

Full-disk encryption gives a device a layer of protection against physical attempts to break in. Some examples might include abusive spouses, parents, roommates, co-workers or employers, school officials, police officers and other law enforcement officials, or other people who at some point have physical access to the device.

Apple's OS X, Linux, and high-end versions of Windows all have built-in **full disk encryption**, but it is usually not turned on by default. On mobile phones, Android offers it under its "Security" settings, and Apple devices such as the iPhone and iPad describe it as "Data Protection" and turn it on if you set a passcode. Although you can find in-depth descriptions of full-disk encryption options online, be aware that these options change frequently and instructions can become out of date quickly. If you are preparing for a training where you will teach full-disk encryption, be sure to give yourself a refresher on the most up-to-date options and settings.

What Encryption Does *Not* Do

Encryption is not a cure-all. Even if you are sending encrypted messages, the message has to be decrypted by the person with whom you are communicating. Encrypted communications can be compromised by compromising your “endpoints,” i.e. the devices that you are using for communication. Additionally, the person with whom you are communicating can take screenshots or keep logs of your communication.

Putting it all together

Together, encrypting both data in transit and at rest will offer you more comprehensive security than using just one or the other.

If you send unencrypted messages (not encrypting your data in transit) from an encrypted cell phone (encrypting your data at rest), those messages will still be vulnerable to network eavesdropping and interception.

For example, if you send unencrypted messages (not encrypting your data in transit) from an encrypted cell phone (encrypting your data at rest), those messages will still be vulnerable to network eavesdropping and interception from governments, service providers, or technically skilled attackers. The record of the messages on your phone,

however, will be protected from someone physically trying to view them on your phone if they don't have the passcode.

Conversely, if you send end-to-end encrypted messages (encrypting your data in transit) on an unencrypted device (not encrypting your data at rest), those messages will be resistant to snooping and eavesdropping on the network. If someone gets physical access to your phone, however, they will be able to access and read the messages.

But if you send end-to-end encrypted messages (encrypting your data in transit) on an encrypted device (also encrypting your data at rest), those messages will be resistant impermeable to snooping and eavesdropping on the network, and protected from someone physically trying to view them on your phone if they don't have the passcode.

Encrypting your data both while it's in transit on the network and while it's at rest on your device is ideal for protecting yourself from a wider range of potential risks.

Are you teaching encrypting data in transit—specifically, transport-layer encryption and end-to-end encryption tools—in your workshop? This GIF, showing messages in Google Hangout and end-to-end encrypted OTR, might help learners to understand encryption in practice.