What is End-to-End Encryption?

End-to-End Encryption (E2EE) is a method of secure communication that enhances security measures while data is in-transit. This practice prevents third parties from accessing data while in-transit from one system to another. The concept of End-to-End Encryption has been available for over two decades while many reiterations have occurred since the introduction of the smartphone. End-to-End Encryption services for the consumer market have been perfected through Mobile Messaging Applications such as WhatsApp, iMessage, and Telegram.

End-to-End Encryption offers a unique way to send secure messages. End-to-End Encryption uses encryption keys, or algorithms to decipher the information sent, allowing the data to be scrambled and unscrambled between users. The data is encrypted using a set of public or private keys to authenticate users. Once the recipient receives the message, it is then decrypted and displayed in plaintext for viewing. The main goal behind End-to-End Encryption is providing security between the user and the recipient and privacy against third party's and Malicious Actors and Hackers,

For example, imagine that a note is being passed from one student to another in a classroom. The note, written in plaintext, is sent by the sender and received by the recipient. But what are the chances of the note being intercepted by the teacher or another student in the classroom? Because the note is written in plaintext, there would be nothing to stop a third party from viewing or stealing the note.

But imagine if the note was encrypted through End-to-End Encryption. First, the contents of the note would be encrypted in a randomized set of numbers or letters. The note would have no way of being intercepted and the contents of the note would be completely private and intact. Once received, the note would then be decrypted and the recipient would be able to read it.

Today, instead of sending physical notes, we now rely on mobile devices, tablets, applications, the internet, all of the great technology that we take for granted. And now we have the ability to send and receive messages that are completely private to the sender and the recipient. This would eliminate the possibility of having a third party intercept the message and would give the sender and receiver security and privacy in what they send.

Advantages of End-to-End Encryption?

There are many advantages of using End-to-End Encryption when sending and receiving data. Being able to securely send and receive messages can be crucial in many different forms of communication. End-to-End Encryption has it's advantages and business use cases in

applications such as WhatsApp, iMessage, and Telegraph. These applications have given users a wide range of security and privacy features and settings by utilizing concepts like End-to-End Encryption.

Privacy Protection is one of the largest advantages. The ability to secure data and prevent third party's from intercepting that data is a crucial role that End-to-End Encryption can fill. The protection of Personal Identifiable Information (PII) has become an integral part of security and privacy.

Securing the integrity of data is another advantage of End-to-End Encryption. By encrypting and decrypting plaintext messages, applications such as WhatsApp, iMessage, and Telegraph give the sender and the recipient a secure method of keeping their data intact, while protecting and securing sensitive information being sent between users.

Highly Sensitive Data Exchange is another method which End-to-End Encryption is assisting users by securing the messages and data. When users are exchanging highly sensitive data such as financial or medical records, End-to-End Encryption provides the preferred method of security when it comes to highly sensitive data exchange.

By utilizing End-to-End Encryption, the sender and the recipient are bypassing the high risk associated with a cyber attack. A Cyber Attack is a breach of personal data. In many cases, businesses or a person that is a victim of a Cyber Attack will experience both private or public embarrassment. This can also impact an organization's reputation.

When a company is storing and accessing a client's data, it is important that the proper security measures are in place. By using security measures like End-to-End Encryption, they are taking the necessary steps to protect their clients and employees. If this does not happen, it can impact the integrity and reputation of the company.

The Technology Behind End-to-End Encryption

The technology behind End-to-End Encryption can range from simple and straightforward to highly complex. For this blog it will be best to provide a basic understanding of End-to-End Encryption by understanding the technology.

End-to-End Encryption begins with distribution of keys. Private and Public keys are algorithms that give users and recipients the ability to encrypt and decrypt their messaging data. Let's think of this in the context of a safety deposit box at a bank.

Imagine entering the local branch of a bank to use a safety deposit box. In this instance, two keys are needed to open the box. One key is held with the bank and the other key is held by the

customer. Both keys are needed in the process of opening and closing the box. Without both keys, the box cannot be opened.

End-to-End Encryption works in the same context. In this example, the message is the safety deposit box. Instead of physical keys, the user is provided with a private digital key that will allow the recipient to decrypt the message. Without the two keys, the sender and receiver of a message cannot view the message in plaintext.

The most common form of End-to-End Encryption is Symmetric encryption. This method uses a private key to encrypt and decrypt the message. Both keys are needed to unlock the message. By using symmetric encryption, you can use as many of the same keys as you need to encrypt the data through a timeframe or session. This is called Session Key Encryption.

To implement this, the administrator will assign a set of letters in place of the plaintext data that is being sent. These sets of letters are called algorithms and they are used for implementing End-to-End Encryption. Algorithms are a process or set of rules to be followed by a computer in calculations or other problem-solving operations. In the case of Encryption, the algorithms are strings of letters that are presented in a unique way. These strings of letters are scrambled to create a coded message. Below is an example.

Imagine the message being sent is “BAM.”

- Three characters passed B is E. Start at B (C, D, E.).
- Three characters passed A is D. Start at A (B, C, D).
- Three characters passed M is P. Start at M (N, O, P).

If the plaintext message is “BAM,” and the encrypted message is “EDP.”

We decrypt this message by moving each character three spaces forward and we see that BAM was the original message. This is encryption. This prevents anyone other than the sender and recipient from viewing the message in-transit.

This is called a Ciphertext. We have changed the plaintext format to a ciphertext. This can get complicated quickly, but just remember that systematic encryption uses the same key to encrypt and decrypt data.

End-to-End Encryption is most widely utilized through messaging applications that reside on a device such as a smartphone or laptop. Most vendors that provide these services require Two-Factor Authentication to access the device and the applications that reside on the device. This is a security measure in which a User ID and Password is required to access the device. It

provides additional levels of security to the device and can be essential for authenticating a user that participates in messaging services with End-to-End Encryption.

There are two forms of End-to-End Encryption most commonly used on smartphone and messaging applications such as WhatsApp, iMessage, and Telegraph. These are associated with a color scheme as well when the user and recipient are in communication. The color schemes are generally viewed as a highlighted color around the text.

Enhanced encryption is categorized as S/MIME and standard encryption is categorized as TLS. On a smartphone or in a messaging application like WhatsApp or Telegram, the color green is used to identify enhanced encryption (S/MIME). This is the safest and most reliable form of End-to-End Encryption.

The second is Standard Encryption (TLS). In Standard Encryption, the color Gray is used to identify TLS. Standard Encryption support is not guaranteed and is used from past communications with the email server. Lastly, when an icon like the Lock Icon we spoke about is featured in red, this is identified as an unencrypted service or site, and should not be deemed secure.

Smartphones and search engines incorporate colors and icons to allow the user to identify the level of encryption. The most common icon can be viewed in the far left corner of the URL address bar in a browser or search engine. The icon is commonly displayed as a Lock and is often associated with a color. The color of the Lock is either Green, Gray, or Red. These colors are used to identify the level of encryption.

What Types of Data Require End-to-End Encryption?

Let’s use another example. Imagine a system administrator, hired by an International Bank to maintain and store client data. On the job, they have access to thousands of pieces of customer data that is unique to each of the bank's customers. Because the Bank is required to adhere to Federal laws and regulations, it is required that the customer data is secure and remains private. This is an example of Personally Identifiable Information (PII), or sensitive data that is unique to an individual.

Data is defined as facts or figures of information that is stored on a computer. It varies greatly, but in this example the data is categorized as financial information from the bank's customers. Personally Identifiable Information is anything that is private to the individual that should not be used for public consumption outside of the Bank’s internal systems.

In present times, applications are widely used across multiple devices by multiple users. This provides a greater challenge for companies using or creating messaging applications such as WhatsApp, iMessage, and Telegram. In order to protect Personally Identifiable Information, institutions will utilize a wide range of privacy controls to make sure data is secure.

Medical records are another example of Personal Identifiable Information. Patient records are protected by the Federal Government through HIPAA Regulation. This means that medical data for each patient is required to remain private and secure when being utilized by a Hospital, Doctors Office, or Medical Lab. Many hospitals will use End-to-End Encryption to protect Electronic Medical Records (EMRs).

Smart Hospitals are encouraged and require the collection and utilization of data from patient records. They use the data from CT scans, MRIs, X-Rays and other medical tests to gather and store massive amounts of data. This is done to spur advancement and increase communication between healthcare staff. But because the collection of data has become important, this brings challenges to healthcare in storing and maintaining the amounts of data collected.

Data storage and security is required for medical data and records. One of the most secure ways to store medical data is through on-prem servers, storage, and networking. Because sensitive data is vulnerable to Phishing and Malware attacks, it's important for IT departments to secure medical data through End-to-End Encryption.

As the infrastructure of medical data increases, hospitals are investing more into Cloud Services rather than on-prem solutions. Cloud services often offer more flexibility and provide better communication between departments and medical staff. Through the use of the Cloud, medical organizations now have a more scalable approach to managing patient records and data.

Cloud storage is an important way that medical organizations are utilizing security measures such as End-to-End Encryption. Collaboration of information provides a better approach to handling patient data. With more and more devices being used in healthcare, and with complex applications being tied to these devices, cloud storage and End-to-End Encryption is paving the way for a more secure, more accessible option for healthcare and medical communities.

Mobile strategies have impacted hospitals and medical staff in a unique way. Because the use of mobile devices has become the new medium for accessing data, hospitals are required to use End-to-End Encryption as a part of their security measures.

But data does not have to be solely identified in the context of Banking or Healthcare. Personal Data is also important to the individual consumer and if you have ever messaged a friend using

iMessage, WhatsApp, or Telegraph, then chances are you have participated in End-to-End Encryption.

Personal data can be protected through End-to-End Encryption and much of the data located on personal smartphones extends beyond private messages. Calendars, contacts, notes, pictures, reminders, and voice memos are all forms of personal data that can be encrypted to maintain security and privacy for the individual users. Other forms of data such as Wallet Passes, Wifi Passwords, and W1 and H1 Bluetooth Keys can be categorized as additional data that requires security measures.

Depending upon the use case, many types of data now are required to be secure and private. Short Message Service (SMS) is a common way to encrypt private messages between the user and the recipient. This type of service is included in smartphone messaging as well as video conferencing services. This category of messaging allows for End-to-End Encryption through the default factory settings of the device.

Does Email Provide End-to-End Encryption?

Email has become a crucial part of how we live our lives. It is something that we access on a daily basis both personally and professionally. Participating in messaging services such as WhatsApp, iMessage, and Telegraph all require an email address to get started. Social media platforms and business systems now rely on email addresses for authentication and verification.

But email is interoperable, meaning that different email vendors can now communicate with a multitude of competing vendors. Gmail can communicate with Yahoo, which can communicate with ProtonMail and so on. When using these services, we are accepting the third party email vendor's Privacy Policies.

Email is an outlier when utilizing End-to-End Encryption. Most email vendors such as Microsoft’s Outlook or Google’s Gmail do not offer End-to-End Encryption as a default setting. Because emails are viewed as plaintext, the majority of them will not offer End-to-End Encryption as a default setting.

What is even more alarming is that End-to-End Encryption only works when the two parties are using the same email service and share a public key. Email services that do not use End-to-End Encryption run the risk of being decrypted by their email provider or a third party.

It is important to check the privacy settings of applications such as Gmail or Outlook. Default settings may not have End-to-End Encryption enabled, and it is up to the user to customize these settings so that it is included.

If an email is being sent using an email service that does not provide End-to-End Encryption using S/MIME or TLS, there is a good chance that the emails will not be secure. For S/MIME to function properly, a user must have a valid S/MIME certification from a trusted root.

Because End-to-End Encryption relies heavily on TLS encryption, email applications such as Google Gmail do not offer a fully encrypted solution. Because End-to-End Encryption is only offered when the two email providers support TLS encryption, it is impossible for Google to provide 100% encryption.

Encryption in-transit can relate to other forms of email encryption like Pretty Good Privacy (PGP). PGP is able to encrypt the content of an email so that only the sender and the recipient will be able to view the email. When Gmail receives a PGP encrypted email, Gmail is not able to catagorized the content of the email to search for it at a later date.

Encryption in-transit adds a substantial layer of privacy by encrypting only the content of the email and not the headers. This means that in theory, a third party could capture the delivery of a PGP encrypted email and will be able to view the address of the sender. The contents of that email however will be protected.

Who Offers End-to-End Encryption?

There are many vendors that offer End-to-End Encryption along with their devices and applications. Many conventional applications that we use include End-to-End Encryption. Apple products offer End-to-End Encryption through iMessage, Facetime, and Apple Wallet. WhatsApp and Telegraph also use End-to-End Encryption for video conferencing and messaging services. These messaging platforms use both text and video to provide communication. Apple provides End-to-End Encryption through iMessage and also offers End-to-End Encryption that integrates with all of their devices and operating systems; WatchOS, iOS, iPadOS.

One of the leading messaging vendors is WhatsApp. WhatsApp is available to use both personal and for business. WhatsApp, much like Apple does allow their users to store messages and data in their servers. Each company promises that no private data will be accessed by their internal employees, even if the data is stored in their cloud or on their device.

Telegram is another messaging vendor that utilizes End-to-End Encryption. It is considered a cloud based instant messaging system. Telegram’s platform provides End-to-End encryption through messaging and video conferencing services.

What makes Telegram truly unique is Secret Chat messaging. Unlike the cloud-based messages, Secret Chat can be accessed only on the device that the message was initiated on or accepted.

They can be deleted at any time and not stored locally. Secret Chat's use End-to-End Encryption, making it a secure way to message.

Because Telegram has a distributed infrastructure, data is spread out across multiple data centers. This makes it even more secure and less likely for hackers to be able to compromise their services. Telegram does not collaborate with Government organizations unless the situation is dire.

Unlike WhatsApp, Telegram is a Cloud-based messenger that lets a user access their data from multiple devices at once. Telegram allows the user to store and share all of their data across their devices simultaneously. Also, Telegram's API code is open which makes it user friendly for developers that are interested in creating their own applications.

It is important to understand the vendor's internal security and private policies. Do these vendors have access to customer data? This is where it gets murky. Because vendors operate through servers within their data centers, the data that is passed from the user to the recipient will pass through servers at some point.

They also have another layer of security within the datacenter called server-side disk encryption. This protects the data from being shared by outsiders that would intercept the messages. However this does not protect against the vendor from accessing the data.

Many think that Social Media sites such as Facebook and Instagram provide End-to-End Encryption through their messaging application, and this is correct. Facebook has included End-to-End Encryption through Facebook Messenger since 2016. Facebook has plans to extend this protection to both voice and video calls through 2023.

End-to-End Encryption in the Cloud.

Mobile Cloud providers give the mobile user the ability to use End-to-End Encryption when accessing their device and storing data. This data can be anything that is stored or accessed on the device such as messages, pictures, passwords, financial information, and documents.

This works by allocating a key to the specified device used by the user. The user will have a private key and the Cloud vendor will have a copy of that key. Also, it allows the mobile user the security and privacy to store their data in the cloud in a secure way. Only the user and the Cloud provider will have access to this data, and by allocating a private key, it offers End-to-End Encryption.

In regards to messaging services such as WhatsApp, many of these services have been victims of Malicious Actors and breaches. Because WhatsApp allows the users to backup their chats on

their devices or in the cloud, End-to-End Encryption is lost as soon as the user backs up their data. WhatsApp has responded to this loophole by creating disappearing messages. These types of messages are viewed once and then discarded .This prevents the data from being backed up, giving the user more security when using their services.

Basic cloud security is offered through Cloud service providers, or CSPs. These providers offer basic encryption services with HTTPS being the standard for secure communication. There are many advantages to these services such as security, prevention of theft, prevention of other cloud services accessing the data, customer satisfaction, regulatory requirements and even additional protection against outside threats.

Third Party access is a major security issue when communicating with CSPs. If the data is stored on a disk or other storage devices within the CSPs internal systems, this is considered data-at-rest. Encrypting and decrypting the data is done by using key exchanges between the two users and the devices.

Storage is important when understanding Cloud services. There can be several places that the data is stored when utilizing End-to-End Encryption. These environments can be either private, hybrid, or public clouds. Private being the most secure. Data-at-rest is stored on a physical storage media such as tape or disk. This type of data is stored in a data center or hosted on third party servers.

Storing private encrypted data is stored in a database. This is accessed by using public key encryption. In this process, a public and private key pair is used for each user. The vendor will only ever decrypt the private key temporarily if they have the user's password. This prevents Malicious Actors from being able to decrypt the data without a private key or a password. They would need both in order to access the data.

Data can also be stored in the cloud application. If the cloud vendor is a Software-as-a-service, or SaaS vendor, the level of encryption is typically very secure. Many Virtual Private Networks (VPNs) also provide excellent data encryption while in-transit. These services use a certificate management system that adds even another level of security.

One of the most important aspects of Cloud Security is how encryption keys and certificates are stored. Usually CSPs will provide different options for their clients, but it is critical for End-to-End Encryption to work seamlessly and securely. The keys or certificates must be stored and secured in a safe and reliable place. Having a CSP manage these keys is a good idea for the client, and adds even more security to their systems and devices.

Deployment of Cloud encryption software can be stored on storage media and through the operating system of the device. Many vendors now have a place to store encryption software and data, and big players are able to deploy this software across the cloud and private and public devices. Vendors such as Amazon Web Services and Microsoft Azure do this very well. Google Cloud is another vendor that is a good choice.

One of the most popular cloud vendors for mobile devices utilizing End-to-End Encryption is Apple's iCloud. Apple implements security technologies and best practices that can give the user strict policies to protect their data and information. Encryption is used when it is in transit and also when it is stored on the cloud in a decrypted format. Because Apple services such as iMessage use End-to-End Encryption, this means that only the user can access their data.

Resetting End-to-End Encryption.

It's important to understand that End-to-End Encryption is only as secure as the person using it. When a mobile phone is subject to a factory reset or if the End-to-End Encryption settings are disabled, the user will lose their data if it is not backed up. External backups could be utilized in the cloud or physically on a device such as an external hard drive.

If the data is not backed up and End-to-End Encryption is disabled, the user will lose their data. It is vital for mobile users to backup their data, and back it up frequently. Once a factory reset is implemented or the phone is damaged beyond repair, End-to-End Encryption services will lapse and the user data will be lost.

Most devices allow the user to reset End-to-End Encryption on their mobile device. This is done by accessing the settings within the device and deselecting End-to-End Encryption settings. Once these settings are deselected, the user will lose the protection and security that End-to-End Encryption provides, leaving the user vulnerable to cyber attacks.

Mobile devices such as the iPhone from Apple have strict policies when referring to resetting End-to-End Encryption. When a user configures a newly purchased iPhone, they have the option to back up their data in Apple's iCloud. If the user misplaces the phone or buys a new phone, they will need to create either new login credentials or keep their existing one.

During this configuration process a message from Apple will give the user the option to Allow or Reset the encrypted data. If the user chooses to reset End-to-End Encryption, the phone will begin to restore the data that is backed up on the iCloud. If the backup was not completed or configured, the data will be lost and End-to-End Encryption will be reset.

Can End-to-End Encryption Stop a Malicious Actor?

End-to-End Encryption has many benefits when included in messaging and video conferencing. It's main goal is to prevent third parties from viewing the messaging content between a sender and a recipient.

In regards to malicious breaches on your device, End-to-End Encryption falls short. Because End-to-End Encryption only offers security in-transit, or through the communication channel, Endpoints are always a concern.

An Endpoint is a remote computing device that communicates back and forth with a network to which it is connected. Examples include devices such as Laptops, Tablets, Smartphones, and Servers. Because there are now so many devices being connected to a network, Endpoints have become very susceptible to attacks.

Over the last few decades, modern security has relied heavily on antivirus software to protect Endpoints. Protecting Endpoints on the network has become a major concern for consumers and businesses and through different technology, solutions have been created to assist in preventing an attack.

Protection from attacks has evolved greatly from antivirus. Many antivirus vendors now offer different tools to protect Endpoints such as Exploit Protection, Endpoint Detection and Response, Analytics, and device controls to ward off potential threats.

Applications such as WhatsApp have security features but this messaging program has been exploited by Malicious Actors more than once. There have been several successful Hacks on WhatsApp.

Keeping Data Safe Best Practices.

There are a few important things to remember when keeping your data safe while utilizing End-to-End Encryption. Keeping Personal Identifiable Information safe from Malicious Actors is difficult but there are some best practices to keep in mind.

It's important to always use the same devices. Storing sensitive data and private messages should be used only on your personal computer or smartphone. This is one way to mitigate the risk of having a Malicious Actor compromising your sensitive data. When data is stored on multiple devices this gives the Actor a broader environment to do harm. It's important to store your data only on your personal device and limit the number of devices.

It’s important to always keep your system and software updated. Majority of software today is constantly updating and including new fixes to bugs and vulnerabilities within the code. IT’s important to keep all your devices up to date with the latest software updates and patches.

If it is possible, it would be a good idea to handle our encryption keys properly. Malicious Actors are good at exploiting modern encryption. If it’s possible, it would be a good idea to store all of your passwords and encryption keys or files in a password manager. This will segment the offline storage of the data and add another level of security to your data.

Lastly, it’s important to understand that encryption is not protecting your data, it is only protecting access to your data. Attacks such as Ransomware are one of the most disastrous forms of attacks. This type of attack gets access to your encrypted files and then holds them at ransom, typically until a fee is paid to the hacker. In many instances, even if the fee is paid, the data is still compromised and often the Hacker will not give the access back. By using End-to-End Encryption effectively you can minimize the chances that ransomware attacks will occur.

FAQs:

What is end-to-end encryption in WhatsApp?

WhatsApp End-to-End Encryption is used when messaging in WhatsApp Messenger. This ensures that only the sender and the receiver can read or listen to what is being sent. WhatsApp is protected with Signal encryption protocol that secures messages right before they leave a device. Once the message is received, it will be subject to adhere to the business’s own privacy practices.

What is End-to-End encrypted data stored in icloud?

Apple uses the iCloud for backup and recovery services. If the user forgets a password, they can access iCloud Data Recovery Service that can help decrypt the data so that the user can regain access to their data. Data types that are stored in the iCloud such as the users Keychain, Messages, Screen Time, and Health Data are not accessible through Apple’s Recovery Service.

What is End-to-End encrypted data on an iphone?

Apple uses End-to-End Encryption that requires the user to use two-factor-authentication for your Apple ID and set a password on the device. The data is protected with a key that is created through the information unique to the device, mirrored with the password of the user's choosing. Noone can access encrypted data through End-to-End Encryption, not even Apple employees.

What is End-to-End Encryption on Facebook Messenger?

End-to-End Encryption is available through Facebook Messenger. Since 2016, Facebook has included it in their messaging application. Facebook is now also offering End-to-End Encryption for video conferencing and audio calling. The content of the user's messages is protected the moment it leaves the user's device and is received by the recipient.

Is Gmail Encrypted End-to-End?

Gmail utilizes Transport Layer Security as the standard for email encryption. The message being sent is encoded and then decrypted as it passes through Google’s servers until it finally reaches the intended recipient. Gmail does not provide a true End-to-End Encryption solution.

Is iMessage End-to-End Encrypted?

Apple provides full End-to-End Encryption through their iMessage application. By using a cipher or algorithm, the message being sent between the sender and the recipient are completely encrypted. In this process, third parties are blocked from viewing the messages. Even Apple is not allowed to view messages through iMessage.