International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 9
***Article Received:** 25 July 2021 **Revised:** 12 September 2021 **Accepted:** 30 September 2021*

Wireless Networks Encryption

Satyanarayana Asundi
Sr. Software Developer.

Abstract

The COVID 19 pandemic has brought with it a lot of disruptions to the way people conduct their day-to-day activities. One of the disruptions that has been obtained is the way people work. Because of the need to maintain social distance to manage the spread of the disease, many companies have advised their employees to work remotely from their homes. This has brought about many issues of data management and security. Technology giant Apple is one of the companies that has had to make numerous changes to the way their devices operate to maintain confidentiality, integrity, and availability of data. In the subsequent paragraphs, we will discuss some of the challenges that have presented to Apple Company and how the company's executive and IT teams are overseeing these challenges to ensure business continuity.

“We are committed to protecting Data” being the theme of Apple to protect user’s data while using apple devices and is doing the job by building most advanced mobile operating system with security architectures that address major requirements of mobile, watch, TV, and desktop/MacBook.

Challenges

The first challenge that Apple has faced is the use of wireless networks. With employees now dispersed in different geographical locations working from home, it is almost impossible to provide corporate networks that will reach all of them. Most of the employees are connected to their personal networks. This poses as a challenge to the company's data management strategies. In a typical working environment, there is a distinct corporate network that is monitored by IT administrators. This ensures the company of the safety of its data as accessed by its end users.

Apple embraces the use of cloud technology. This means it has services like Desktop as a service, software as a service, and infrastructure as a service, among others. This works because employees can access their work resources by logging into the company's wireless network. Now that the company's employees are widespread in distinct locations, this becomes difficult. Further, it is difficult to control how these sites are accessed with the employees' widespread nature.

Mobile Devices

The company also must deal with the challenge of mobile devices. When the company sends employees home to work from home, there is a likelihood that they will be working from their own devices. This poses as a challenge to the data of the company. In the company, all end-user devices are encrypted. This ensures that there is no chance of penetration through end-users into the data of the company. However, when employees are using their own devices, there are some devices that are not encrypted. This places the data of the company at risk of being accessed through these end-user devices.

Apple Company provides training and policies for its employees in the best way to ensure that they have encrypted their devices. Using strong passwords, multiple encryption strategies, and fingerprint scanners, Apple employees make sure that they have safely encrypted the company's data. This way, the company is assured of all its data safety even when dispersed teams are working from various locations. Alternatively, the company provides some of the employees with laptops that have already been encrypted with the best encryption methods. This further ensures the safety of the company's data.

Mobile devices are also easy targets of social engineering hackers. These may be friends or strangers who will ask to use a mobile phone and access essential information. When using wireless networks, these mobile devices function as a vulnerability because some users have limited encryption skills. With poor encryption, sometimes access to wireless networks like WIFI makes it easier for hackers to get into devices. Once they are in, because the storage is single, they can access all information on the mobile device and use it for their malicious intentions.

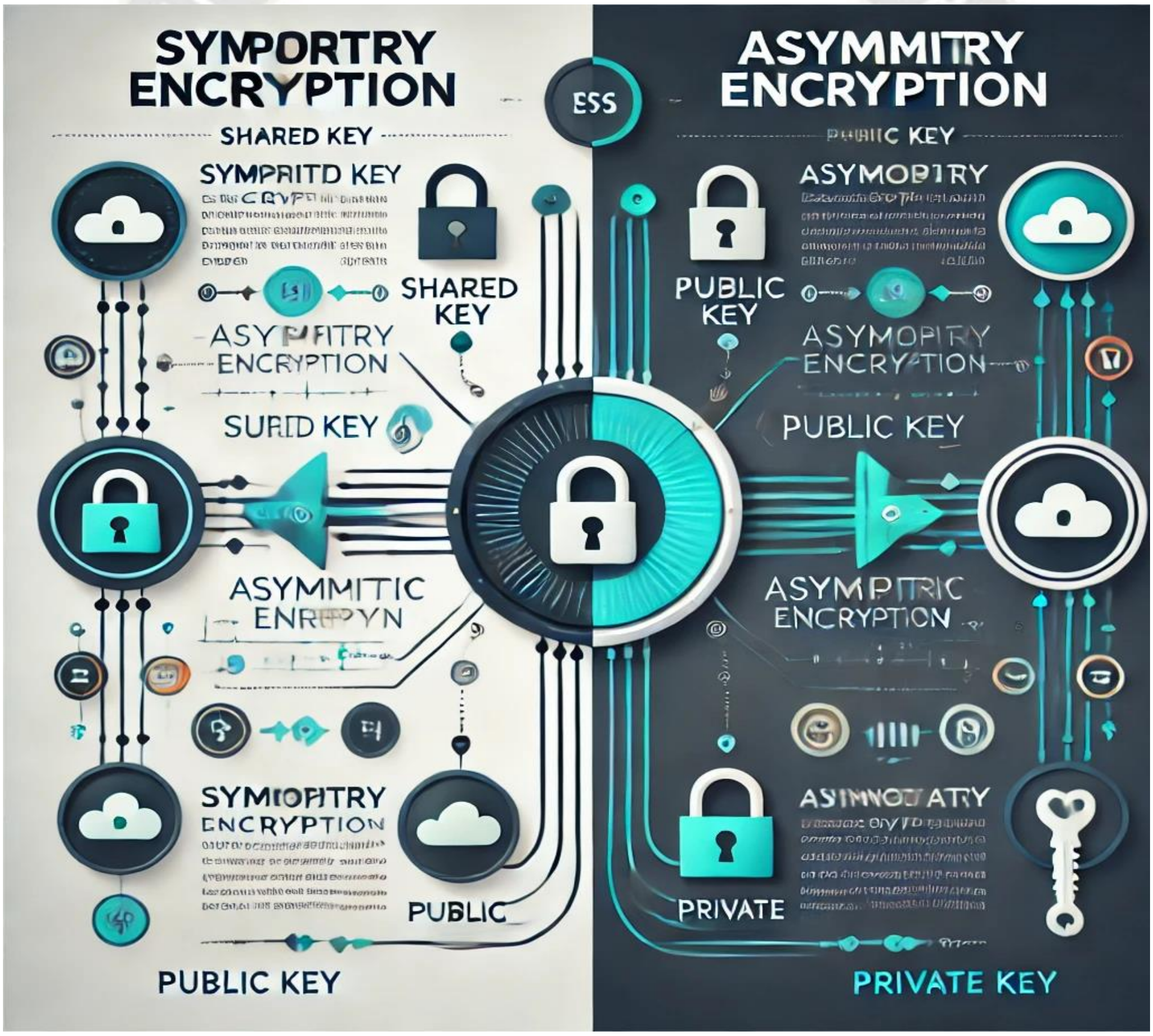
***Article Received:** 25 July 2021 **Revised:** 12 September 2021 **Accepted:** 30 September 2021*

Authentication

When using mobile devices, it is easier to identify remote users and authenticate them. First, there will be the issue of unique user IDs and Passwords. Remote users can use such information to log into their devices. Such user IDs and passwords have strong combinations that are guided by password policies and will enable strong encryption and protection of the information in the mobile device. Local users can be identified using fingerprint scanners, which are on mobile devices or facial recognition algorithms. The fingerprint scanners identify the exact prints of a user and cannot be modified. On the other hand, facial recognition systems use a person's facial features to develop a unique equation that is used each time the person wants to get access to their mobile device.

Asymmetric Encryption

The mobile device will use asymmetric encryption. Asymmetric encryption is one where there is both a public and a private key. The public key will be available to everyone who would like to send information from their devices to our mobile phone device (RapidSSL, 2020). They will use the public key to encrypt this information and send it securely. However, only the owner of the mobile device will have the private key to decrypt this information. Using this encryption system allows the owners of the device to send and receive messages securely without interference by malicious third parties. This protects the integrity and confidentiality of the data in such mobile devices.



Threats

Working from home has placed a challenge on Apple's welfare because it exposes the company's data to many threat actors. Threat actors may be in the family or friends' circle of an employee. With the possibility of gaining access to the employee's personal computer, this places an elevated risk to the company's data. These threat actors could use simple reverse engineering tactics to enter the company's data with malicious intent.

Before sending the employees to work from home, Apple sensitized its employees on the best ways to avoid compromising their data by threat actors. The company advises its employees to keep company material and work strictly professionally and not to share any information related to the company with anyone, including their closest family members. This is a way that the company ensures that there is no intentional or unintentional leaking of information that may compromise the company's welfare.

The common threats to the mobile device industry are the issue of cyber-attacks. These devices are prone to be attacked by hackers. Using online malware in advertisements or promotional messages, they can appeal to mobile devices' users. When they open such emails or click on the links, they are exposed to the malware. This makes mobile devices difficult to get rid of malware attacks. Apple had an issue with its encryption system where the FBI wanted access to their devices. They have developed more robust encryption systems that keep its users' privacy maintained (Menn, 2020).

Vulnerabilities

Working away from the company places the data of the company to many vulnerabilities. As discussed above, some employees may not have sufficient encryption in place to protect the company's data. Others may be placing the company's data at risk unintentionally by accessing internet sites that contain ransomware and other online bugs. Because of the lack of restrictions like there are in the workplace, the company's vulnerabilities in the company increase.

Every single employee using their personal or company personal computer is counted in the fraction of the company's cyber-physical surface. With the increased number of employees using their devices and different networks, the vulnerabilities increase because of the company's cyber-physical surfaces. This exposes the company to many potential threats. The company has invested in robust asymmetric encryption strategies. This allows the company and its employees to send and receive information vital for business continuity while keeping out any malicious third parties.

Security Measures and Policies

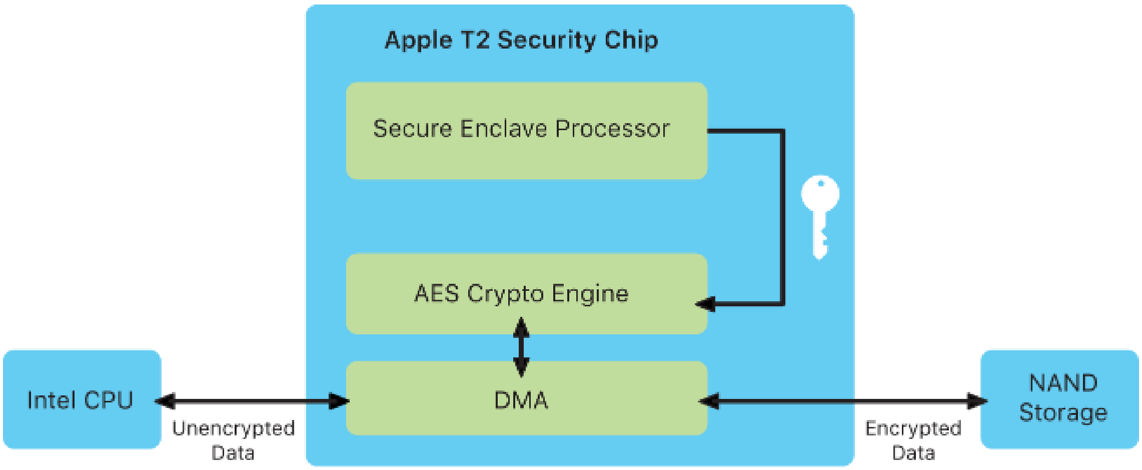
There are many security measures and policies that Apple places on its employees. First, the internet policies of the company have been made more stringent. Those employees who have been issued with personal computers that are considered the company's property are expected to use such devices strictly for the business of the company. No personal use of computers is expected. Instances of non-compliance attract punishments, which may be as severe as the loss of job contracts.

Such restrictions on the use of the internet ensure the security of the company's data. When using the company's computers, employees are only supposed to access sites that have been whitelisted as safely by the IT department. This reduces any possibility of being hacked. Further, these personal computers are fitted with the latest encryption methods. In addition, there are strong password policies to ensure that the information is safe from any malicious third parties. This helps the company maintain the integrity, confidentiality, and availability of its data.

Apple Platform Security

Apple uses secure boot chain, system, and application security to allow trusted code and apps to run on the device. These devices have additional encryption to protect user data even when the device is lost, they can remote wipe the whole device using secure data erasure method which has protected information. IOS uses an encryption methodology called Data Protection whereas File Vault protects Mac OS.

Apple had dedicated AES engine using AES-256 crypto engine between flash storage and Hard disk which makes encryption efficient. Using this dedicated AES engine, it is hard for any program to interpret them directly or indirectly. Below figure represents the architecture of AES engine. Secure enclave processors play a vital role in generating UID’s and GUID’s as per the cryptographic keys are generated uniquely to each device.



The AES Cryptographic engine supports line-speed encryption on the DMA path on Mac computers with the Apple T2 Security Chip.

Hardware Security

Apple devices like IOS, iPad OS, TV OS and watch OS except Mac OS have their own built processor and have security capabilities designed into chip level. The main component in all the devices is Secure Enclave coprocessor and all MacBook's have a T2 Security chip which helps encrypt data at rest, secure boot in Mac OS when using Touch ID.

Communication

Emails are the primary communication tool for every company. Emails are used to send files, receive files, send, and receive instructions and memos and sometimes are even used for video calls. It is important for the company's internal and external communications. With many employees in the company working from home, it is expected that Apple will use its email resources even more. This creates a challenge for the company. There needs to be strong encryption of the emails of the company. This ensures that there is no intentional or unintentional leakage of the emails of the company. These emails contain information sensitive to the company, and any leakage could damage the company.

Apple has a stringent email policy that dictates how the company's email resources are used and how issues of non-compliance are addressed. The company expects emails from the company to be always encrypted. This allows for secure communication between the company and its stakeholders. Further, official company email addresses are to be used strictly for professional purposes with the only little amount being used by the employees for personal communication only if such usage brings an advantage to the company. Forwarding of emails from the company to any third party is prohibited. This allows for the protection of communication between the company and its internal and external stakeholders.

Employees working from home often must send and receive documents vital for Apple's business continuity. It is important to maintain the integrity of such documents being received by the company and the employees. Any changes to the contents of a business, especially sensitive information, could result in many negative impacts on the company. To avoid instances of using information that has been compromised, Apple uses hashing technology to verify documents.

How this technology works is that any time the company sends or receives a document from its affiliate, it is cross-checked for authenticity. When a document is written and saved, it automatically is assigned to have a hash value, a string of unique characters. The string is unique because it is only used for the document as it is. If any single thing is changed in the document, the hash value is completely changed. This helps in authenticating documents such that, when a document is received, its hash value is cross-checked by the system against the original hash values it generated on the other computer. This allows the company to determine the authenticity of documents it receives. It allows the company to use only authentic documents in their business processes.

Databases

Databases that store sensitive information in the company must be protected from any external interference. Some of the sensitive information to Apple Company include corporate information, credit card information of clients, vendor information, employee payroll and health records, social security numbers of clients, and other personally identifiable information of the company employees and clients. Apple encrypts its databases with multiple encryption systems.

First, there is access restricted only to certain employees in the company. This is called Role-Based Access Control. Only those who are authorized to access the database can do so. These people also must use a chain of command forms that allows them to record the time of login, purpose, and sign against their names and post. 24-hour CCTV surveillance and a physical guard protect the physical database. The doors are fitted with RFID tags that can only open to those who have such levels of clearance and fingerprint scanners. This allows for the information in the databases to be secured. In the cloud repositories, backups of this critical information are stored in multiple sites through what is known as redundancy. This always allows access to information, thus business continuity.

Authentication of users is also important in data protection. Remote users are authenticated using passwords that allow them access to information about the company. These passwords are guided by strong password policies and make them impossible to decrypt. With the use of a password, employees who are not on the company's premises are logged on into their workspaces from such remote sites. Onsite users are authenticated using their RFID Tags as they enter the premises. In addition, the onsite employees also have login information that they clay into the end-user computers before they can be accepted into the systems. These passwords and user information are personal and confidential to the person and, as such, exceedingly difficult to impersonate the person.

The company recognizes that, at times, its employees may be traveling and can log into the non-corporate wireless networks. In such instances, the company advises on sites that are considered backlisted. When employees are using the company's personal computers, such sites that maintain malware and bugs are automatically blocked and restricted from access. This protects the company from being attacked using such networks and end-users who log into the networks.

Password Policies & Guidelines

The policies that need to be in place for Apple include password policies, internet, and WI-FI use policy and email use policy. Password policies will dictate how employees will dictate how employees protect their personal computers and accounts from access by malicious third parties. The policy guides strong password protection that ensures robust protection and difficulty of decryption. Appropriate internet and Wi-Fi use policy guides employees on the best way to use the internet and WIFI resources to prevent attacks online (Raleigh, 2016). Finally, an acceptable email use policy will ensure that there is secure communication between the company and all its stakeholders without leaking any sensitive information.

The case study on the Capital One breach identified some vulnerabilities that are on cloud storage (Fruhlinger, 2020). The case study identified some of the most common mistakes that companies make, such as storing the credit card numbers in a common bucket with other non-sensitive company information. Insights from this study help in improving the company’s encryption and data management to avoid similar situations.

If I am a Chief Information Governance officer in any mobile devices company, I will use architecture that combines the use of asymmetric encryption and hashing technology. The data I am going to protect includes personal communication between the users of the devices and their friends, families, or work. This will also include personally identifiable information like phone numbers, home addresses, and other sensitive information. The mobile devices connected to the internet of things devices like smartwatches will also contain other information like the person's health records. This information is critical for protection. Users of mobile devices also use their devices for work in companies that advocate Bring Your Own Device. The information about their work must also be protected.

The biggest challenges faced by the mobile devices industry include increased vulnerability, unsecured networks, and internet sites, and poor encryption. With the increased use of mobile devices, there is an increased chance of exposure to cyber-attacks. Mobile devices do not have sufficient protection, like computers. When there is access to some sites over the internet, they increase vulnerabilities to attack.

Law and Regulations that affect Mobile Industry

Laws and regulations that affect the mobile devices industry include the Americans with disabilities act and privacy laws. The Americans with disabilities act mandate that all mobile device companies ensure there is a way through which all the people with disabilities can communicate effectively. Privacy laws mandate that all mobile devices are made secure so that there is no leakage of personally identifiable information that may be harmful if leaked to the public.

Encryption

The company has trained its employees in the best encryption strategies to use while in the process of accessing networks from their locations. Because most of the employees have their own personal networks, they can be trained in how to encrypt them safely. This allows the employees to safely access the company's resources without posing a threat to the company's data management. By using these encryption strategies, the data of the company is kept safe from malicious third parties.

The encryption can be subjected to efficiency tests by using key size, the vulnerability to known attacks, the flexibility of application, and the randomness of a cipher. . Key size efficiency: AES-256 offers 2^{256} combinations, making it impervious to brute-force attacks. The key size of the encryption matters to determine the impossibility of decrypting. By assessing the vulnerability to attacks, we can ensure we have eliminated all known vulnerabilities (Panda, 2016). Finally, the randomness of cipher evaluates the encryption ability to stand the test of several types of data encryption. Randomness testing: Utilizing Shannon entropy ($\Delta H = -\sum p(x) \times \log2\ p(x)$) ensures the unpredictability of encrypted data.

It is expected that the encryption key size is large enough to protect the phone, and the randomness of the cipher ensures that all types of data in their mobile device are protected. The development of more robust cryptographic techniques with better encryption technologies will help the mobile devices industry to develop its cryptography better.

References

1. Apple Platform Security
2. https://support.apple.com/guide/security
3. Fruhlinger J. (2020) what is a cyber-attack? Recent examples show disturbing trends. CSO online. Retrieved from https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html
4. https://support.apple.com/guide/security
5. Menn, J. (2020) Exclusive: Apple dropped plan for encrypting backups after FBI complained - sources. ("4. ethical issues outcomes.docx - Running head: APPLE VS...") Reuters. Retrieved from https://www.reuters.com/article/us-apple-fbi-icloud-exclusive-idUSKBN1ZK1CT
6. Panda, M. (2016, October). Performance analysis of encryption algorithms for security. In 2016 International Conference on Signal Processing, Communication, Power, and Embedded System (SCOPES) (pp. 278-284). IEEE. Retrieved from https://ieeexplore.ieee.org/abstract/document/7955835/
7. Raleigh, A. (2016). The necessity of having effective workplace policies: Potential risks for employers. Governance Directions, 68(4), 211. Retrieved from https://search.informit.com.au/fullText;dn=084834362364181;res=IELBUS
8. RapidSSLonline (2020) *Fundamental Differences between Symmetric and Asymmetric Encryption.* Retrieved from https://www.rapidsslonline.com/blog/fundamental-differences-between-symmetric-and-asymmetric-encryption/