Joseph Fulkerson

9/29/20

Assignment [A] Cryptography

ITMS 548

**Strengths:**

Cryptography has many benefits and the first obvious one is security. Cryptography is the basis for encryption and is the guard for the information from unauthorized users. Cryptography contains certain techniques that defend against forged key signatures and spoofing. Hashing is a common function in cryptography and ensures the protection of the user data. Cryptography provides a non-repudiation service which means users can not dispute any denial of passage.

**Weakness:**

Cryptography ensures protection and security of files and data, but sometimes the user trying to access the data is the correct user and cryptography has now made it more difficult to access. Sometimes legitimate users can struggle to access data if the service being offered is complex. Cryptography alone is not an all alone fix for securing data. It is an important component, but it cannot ensure total data protection. Finally, the system’s ability to properly secure data. Cryptography can only go as far as the system it is being implemented in. If the system has vulnerabilities the Cryptography integrity may not matter due top backdoor system vulnerabilities

**Type 1 Cryptographic Product:**

Type 1 products refer to NSA endorsed classified or controlled cryptographic items. This only refers to products themselves and not information, key services, or controls. Type 1 products contain NSA approved algorithms. Only available to U.S. Government users and contractors, as well as federally sponsored contributors. These products are used to protect systems requiring high level of security clearance and access. Type 1 certification is a rigorous process that includes testing and formal analysis of cryptographic security, functional security, tamper resistance, and security of the product manufacturing and distribution process.

**Type 3 Cryptographic Product:**

A Type 3 product is a device for use with Sensitive, but unclassified information on non-national security systems. Devices using NSA approved encryption algorithms including three-key Triple DES and AES. These encryption methods are used to encrypt non classified government and commercial data and information. These systems must be developed using established commercial standards and containing NIST approved cryptographic algorithm modules evaluated by the National Information Assurance Partnership.

**Federal Information Processing Standard 140-2:**

The FIPS 140 publication series is a coordination of requirements put out by the National Institute of Standards and Technology. Cryptographic modules need means of security to be considered viable confidential data banks. These levels set standard requirements that must be met from physical hardware to cryptographic algorithm implementation. Modules need to be validated of their standard level by a federal agency to ensure that the hardware, software, firmware are capable of containing sensitive unclassified information.

FIPS 140-2 security levels go from level 1 to level 4 where level one represents the lowest level of security while level four is the highest level of security. Level one contains a basic cryptographic module that has at least one approved algorithm security function. There are no specific hardware requirements for this level. A laptop or personal computer is an example of a level one module. Level two builds of level one requirements but extends further to require features showing evidence of tampering. This also includes physical locks that are tamper proof and pick resistant. Level three is the implementation of a response to level one and two security breaches. If something is tampered with at the security level of three. The cryptographic module can lockdown and detect and intruders of the data and attempt to divert or secure the data furthermore. Level four is the final level which relies on the use of physical intrusion detection. If a level four module is breached there is a high probability that it will be detected.

**Symmetric and Asymmetric Encryption:**

Diagram

Description automatically generatedDiagram

Description automatically generated Asymmetric and symmetric encryption are similar in their implementation of keys to access encrypted information Although the type of key needed is different and provides different benefits and factors that make each type of encryption very different. Symmetric encryption uses a single key for encryption and decryption while asymmetric encryption utilizes a public key for encrypting data and a private key to decrypt. This means that runtimes of each algorithm are different. Symmetric encryption is faster because it does not need to execute a high computational algorithm Whereas asymmetric needs to compute an algorithm that uses a large amount of computation to verify the decrypting key. Common algorithms for symmetric encryption include DES, 3DES, AES, and RC4 while asymmetric commonly use Diffie-Hellman and RSA. Symmetric encryption is used in areas where you are exchanging bulk amounts of data.

In the diagrams above you can visually see how each process is different from the style of collecting the keys and using them to decrypt the information. Asymmetric encryption uses a key to encrypt the information. This key is only used when encrypting and is not the same key that needs to be used to decrypt the text. This is what makes this process more time consuming. To decrypt the information, you need to have access to the private key that decrypts the data. In symmetric encryption this is not needed, and only the key used to encrypt can be used to decrypt that information.

**Key Management Plan (KMP):**

The importance of a key management plan can first be addressed when you can identify the objectives of the application you are applying an algorithm to. Applications storing data securely should develop an algorithm that supports objective data that stays at rest. While an application that requires data transmission and reception should use an algorithm that supports objective data and data in transit. These factors will determine the type of encryption algorithm being implemented. This will then determine what keys will be used and how you will manage them for proper data security and data transmission.

Key management plan is important for properly dispersing keys to give access to encrypted information. It is also important to properly manage these keys to ensure the integrity of the system those keys allow access to. A key management plan allows for easy peer authentication communication to take place as well as give you the ability to manage and create security associations for key management. This managements plan also provides key generation mechanisms that produce access keys to encrypted information. the last use is for the protection of threats that can compromise systems in the chance of a denial-of-service attack.