Introduction to the OWASP Top 10 – 2021

Risk A2: Cryptographic Failures

Key Concepts

Key Concept 1: Cryptography and Encryption

- Cryptography: the art and science of keeping messages secure
- Encryption: an algorithm for transforming messages (plaintext) into secure messages (ciphertext), most often using a key

Key Concept 2: Cryptanalysis

- The art and science of breaking secure messages

Additional Information

Cryptography is the art and science of keeping messages secure. Encryption the process by which we do this. As the quote goes, there are two types of cryptography: Cryptography that will stop your kid sister from reading your messages, and cryptography that will stop major governments from reading your messages. A2 is all about trying to implement cryptography correctly.

Cryptanalysis is the entire field dedicated to the art and science of breaking secure messages. For example, the most common letter in the English dictionary is E. Just with that information alone, you can perform cryptanalysis on encrypted plain English text messages and look for patterns.

The overarching field that encompasses both cryptography and cryptanalysis is called cryptology. Think of it as an equation: Cryptology = Cryptography + Cryptanalysis.

Definition

The use of weak, deprecated, or incorrect cryptographic algorithms.

- Sensitive data transmitted over a network without cryptography
- Insecure certificates or accessible keys and secrets
- Weak creation of random values used for keys or as seeds
- Use of older encryption algorithms

Additional Information

The definition of A2 of 2021 – Cryptographic Failures – is the use of weak, deprecated, or incorrect cryptographic algorithms. The simplest example of this is sensitive data transmitted over a network without it being encrypted. Another example involves the creation of secret keys which can be predicted.

The most common example of cryptographic failures involves the user of older encryption algorithms. Since their design, some older encryption algorithms have been broken using cryptanalysis.

When we say weak cryptographic algorithms, we refer to algorithms for which ways have been found to circumvent the security they provide. When we say deprecated cryptographic algorithms, we refer to algorithms that were designed, decades back, say in the 70s or 80s. Back then, computing power was much less, so they are not recommended to be used today.

Example

Bad Example

```
Cipher cipher =
Cipher.getInstance("DES/CBC/NoPadding");
Cipher.getInstance("DESede/CBC/PKCS5Padding");
Cipher.getInstance("AES/ECB/PKCS5Padding");
```

Good Example

```
Cipher cipher =
Cipher.getInstance("AES/GCM/NoPadding");
```

Additional Information

In pseudocode as a bad example, the first line in red uses the Data Encryption Standard or (DES) in Cipher Block Chaining (CBC) mode with no padding. DES was created in the early 1970s by an IBM team and adopted by the National Institute of Standards and Technology (NIST). DES is a deprecated algorithm, because newer symmetric ciphers have superseded it since then, and it is also weak, because of the flaws found with it.

As a good example, the line in blue specifies the Advanced Encryption Standard (AES), which replaced DES in the early 2000s. Note that for symmetric ciphers, it is not only about what algorithm you use, but also how the algorithm is configured and what mode it is using. Unlike Cipher Block Chaining (CBC), the Galois/Counter Mode (GCM) is considered much more secure and is widely adopted for its performance.

Challenges

Crypto knowledge is a rare commodity because

- The material to learn cryptography is challenging and difficult
- It is hard to verify the level of security crypto solutions attain
- It takes very senior and sophisticated developer resources

Additional Information

We now understand how cryptographic failures happen let us look at why they are common.

Crypto knowledge is a rare commodity because cryptography is difficult to learn. To add to this, it is hard to verify the level of security cryptographic solutions provide. All it takes is for the slightest misconfiguration of one parameter and your keys could be exposed, or you could be using weak parameters. To have a good understanding and working knowledge of crypto, requires serious time commitment.

Best Protection Strategies

MUSIC

Manage keys and secrets properly

Use up to date and strong cryptographic algorithms, protocols, and key sizes

Sensitive data requires more protection, so classify them correctly

Instrument encryption for data at rest and in transit

Configure cryptographic protocols well

Additional Information

Above you have some of the best protection strategies against A2 of the Top 10 – Cryptographic Failures.