CRYPTO CHALLENGE 1:

Dangers of unauthenticated encryption

[Publish Date]

European Cyber Security Challenge 2019

Bucharest, Romania

1. Initial Write-Up

Description:

You are a working in a Europol unit on an organized crime investigation. The mission is a large scale operation to end a European criminal enterprise smuggling contraband within different countries.

You have intelligence on the criminal operations through undercover operatives, network surveillance and other sources. You have also the capability to intercept and eavesdrop on their communications.

The criminals have become suspicious and have started using encryption in their communications. You still have access to the encrypted communications and control over the message lines. In addition, you have inside knowledge on their operations and the codes that they are using in their communications. However, you do not have access to the keys they are using in encrypting their communications.

You have intercepted the following encrypted message:

c8c9e50477760d1664e0dd6bc17d50c1aacfe40f30350e116fa1c765d63c5d8f

Your inside intelligence tells you that it is the unauthenticated encryption of the message:

Bring bananas to the cafe today!

You know that this means that the criminals are trying to set up a casual meeting in a public place, where you cannot make the arrests safely. You know that the code for bringing the contraband is "oranges" and you also know that one of their drop-off points is in the port, where you can easily arrest the criminals safely.

You know that the encryption is done using AES encryption in Counter mode with a 128 bit key and an unknown (but fixed) initialization vector (IV). They also use plain ASCII encoding of their text before encryption.

Your challenge is to provide a ciphertext that decrypts to:

Bring oranges to the port today!

under the same key and IV as the original encrypted message. Because there has been no authentication on the message this should go undetected by the recipients and you can successfully carry out your operation.

You only have one try to get this right or the operation fails!

2. Challenge specifications

- Category: Crypto
- Difficulty : Medium/Hard
- Expected time to solve: 3-4 hrs

3. Technical specifications

Not applicable. All necessary data given in section 2.

4. Questions and answers

1. CTF Specific questions:

Q/A that can be directly introduced in a CFT format. This year upload of files can be included, also REGEXPs.

Question:

What is the encryption of the challenge phrase “Bring oranges to the port today!” under the same key and IV as the original ciphertext?

Answer:

c8c9e504777600056befd46fc17d50c1aacfe40f302600057ea1c765d63c5d8f

Question:

What is the XOR difference that yields the correct ciphertext?

Answer:

0d130f0f0904000000000000000000130e141100000000000000

Question:

What is the XOR difference that yields the correct ciphertext under some other, unknown key?

Answer:

0d130f0f0904000000000000000000130e141100000000000000

Question:

What is the XOR difference that yields the correct ciphertext under some other, unknown IV?

Answer:

0d130f0f0904000000000000000000130e141100000000000000

2. Non-Flag specific:

Open Questions: Answers that may need a minimum development. (No suitable for CTF but useful for training and for a better understanding of the challenge) Multiple choice answer

Question:

Can you apply the same technique to other modes of operation in AES?

Answer:

Yes, but in a limited fashion. For example, in CBC mode similar attack works, but it requires changing the IV instesad of the ciphertext directly. If used in the middle of the ciphertext, it will render some of the ciphertext unreadable after decryption.

Question:

Can you apply similar technique to other forms of encryption?

Answer:

Yes. Similar attacks work against any stream cipher that just XORs the keystream to the plaintext. This attack also works against one-time pads.

Question:

How to defend against these types of attacks?

Answer:

Authenticated encryption for example using AES in a authenticated encryption mode (e.g. GCM) or prociding authentication tags via message authentication codes (e.g. HMAC).

Non-Flag specific examples:

5. Attack Scenario

Description:

The attacker can change parts of the encrypted message at will. If the attacker knows parts of the original plaintext, he can change these to ones that will cause harm to the recipient (e.g. false information).

6. Installation instructions

Description:

This exercise does not require any installation by the organisers. If the hard option (only one try) is chosen, then the organisers need to set up the answering process in such a way that it closes after one try.

7. Tools needed

Description:

The challenge can in principle be solved with pen and paper, if enough time is available. In reality, some programming tools are useful in generating the solution for the challenge. These can be C/C++, Java, Python or other programming languages and their respective environments.

8. Artefacts Provided

Description:

None besides this document.

9. Walkthrough (writeup)

Description:

First the contestants need to familiarize themselves with AES and the counter (CTR) mode. It is provably secure, but does not provide authentication of the encrypted messages. Because AES in the counter mode is essentially a stream cipher, this means that the keystream generated by the AES cipher is XORed to the plaintext to provide the ciphertext.

To generate the alternative ciphertext, the contestants need to find out the (binary) difference between the original plaintext and the target plaintext. This can be done by converting the text strings into binary (given the ASCII encoding) and computing the XOR between these binary vectors.

Once this difference has been found, the contestants need to XOR this difference to the original ciphertext. The result is the answer to the challenge and the flag of this exercise.

Reading:

Ferguson, Niels, Bruce Schneier, and Tadayoshi Kohno. "Cryptography Engineering: Design Principles and Practical Applications." (2012). Chapter 4

Aumasson, Jean-Philippe. Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press, 2017. Page 71

Katz, Jonathan, and Yehuda Lindell. Introduction to modern cryptography. Chapman and Hall/CRC, 2014. Chapter 3.6.4

AES CTR mode (Wikipedia) https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Counter_(CTR)

PyCrypto programming package https://www.dlitz.net/software/pycrypto/api/current/