Intro to Cybersecurity - Ex 2
Insecurity of CTR-Mode for Cloud Service

Submit by May 21, 2019

Last modified: 30 April 2019

Bug bounty. This is the first time that we give this exercise, so there may be bugs. To incentivise you to report bugs to us as early as possible we will reward the first ones who report a bug three bonus points (which will be added to the exercise part of the overall grade). We will decide whether a bug-report is entitled for those points or not. Please report to *ay.cs.biu@gmail.com* if you find any problem in the exercise.

Description. In this exercise you will use python's cryptographic API to implement an insecure cloud service that receives a filename from the user and stores the encrypted content of the file in its internal memory (in our case the cloud's internal memory is just private class's fields).

Next, you will write a function that receives a cloud object (with some content already encrypted and stored in its internal memory) and you will decrypt its encrypted memory *without knowing the key that the cloud uses*, only by using its Read/Write APIs.

There are three relevant files for the exercise, see the comments in the files for exact instructions and function signatures.

1. **cloud.py** - This is the class of the cloud that you need to implement.
2. **breakcloud.py** - This is the code that dectypts the cloud plaintext.
3. **cloudtest.py** - An example of how we will test your code, you don't know which file will be chosen for the test, of course. Note that the example assumes a specific key and counter, i.e. they are fixed rather than being generated randomly. In your implementation you should generate them randomly (just like in the example file). The test don't have a full implementation because this is exactly your task in the exercise :-)

Additional comments.

- For your convenience, an example of usage of AES-CTR is in aesctr.py.
- Use python 2.7. To use the crypto modules install 'pycrypto' (not 'crypto').
- Use a 256-bits key (32 bytes) version of AES. Initialize the counter with 0 (which is the default).

Submission. Create a directory and rename it to you ID. Inside the directory there should be 3 files:

1. me.text – contains 2 lines, first line is your ID, second line is your name.
2. cloud.py – your implementation of the given file.
3. breakcloud.py – your implementation of the given file.