Université Libre de Bruxelles
INFO-F-405 - Project: Misuse of encryption

Nikita Veshchikov

2015-2016

The purpose of this project is to break encryption in some cases when a strong algorithm is misused. We are going to use an example of AES-128 CTR.

1 AES-128 CTR misuse scenario

A block cipher such as AES-128 is usually used with a mode of operation. For this project we will focus on the mode called CTR. The scenario of this project is the following: Alice and Bob are exchanging messages using AES-128 CTR, however they are always using the same key and initial value for the counter that is used in the CTR mode.

Here is an example of how Alice uses encryption to send messages to Bob using `openssl` command line tool:

```
openssl enc -aes-128-ctr -kfile secret.key \
-nosalt -iv DEADBEEFCAFEBABEDEADBEEFCAFEBABE \
-in lorem.txt -a -out lorem.enc
```

File named `secret.key` contains the secret passphrase that Alice and Bob use to generate the key. Files `lorem.txt`, `lorem.enc` and `secret.key` that were used for this example are available with this project description.

In this scenario you do not know the key, but you know that Alice always uses the same value for the `-iv` parameter (and all the options that she uses to call openssl are the same for each file that she encrypts).

2 Project details

You will be given a `zip` file that contains a number of secret encrypted messages. Each message is encrypted with the same secret key and your goal is to crack the code and obtain these secret messages.

At the end of this project you should deliver a short report (maximum 6 pages excluding bibliographic references and appendixes). Your report should contain:

1. short description of your code (diagrams) and implementation choices,
2. a description on how you obtained secret messages from ciphertexts (the vulnerability & the security problem),
3. a section where you describe difficulties that you met during this project (and solutions that you found),
4. a section that describe results of your project.
5. the appendix of this report should contain all the decrypted messages.

After the submission of the project you should also prepare a short (10 minutes) presentation that you should use for the defense of the project.

Each group will receive its own file with ciphertexts and you should use the file that was assigned to your group. However, you are allowed to break more than one set of ciphertexts (break files of other groups) and explain it in your report, in this case you will get some bonus points.

This project has to be done by groups of $5-6$ students. Each group should contain (if possible) at least one mathematician, at least one engineer and at least one computer scientist. A group must not consist of students that come from only one field (e.g. only engineers), there should be students of at least two different fields in each group (e.g. computer scientists and mathematicians) if possible.

The report should be submitted via UV before 23:55:00 on Monday, the 5th of December.

You are allowed to use any programming language as well as any number of computers that are available to you.

Good luck!