Symmetric attacks: assessment

CATALDO BASILE

< CATALDO.BASILE@ POLITO.IT >

POLITECNICO DI TORINO

Agenda

- stats

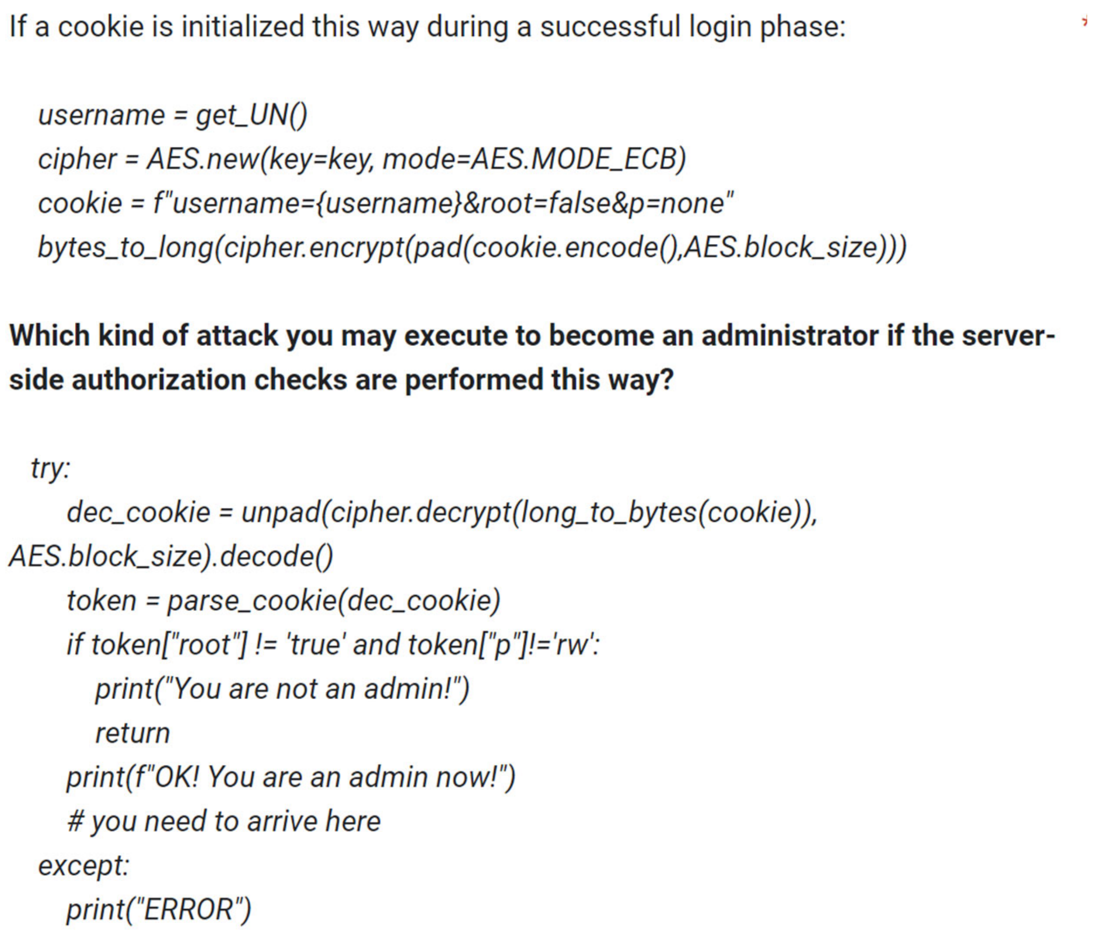
- 4 attacks
  - from the exams

Preliminary stats

Please fill in this form as I use it for statistical purposes

- https://docs.google.com/forms/d/e/1FAIpQLSd1lyzDITZ4wfi3JwbQCY6nvateq8G6jHUgnLpECsykDGa47w/viewform?usp=dialog

Attack #1



If a cookie is initialized this way during a successful login phase:

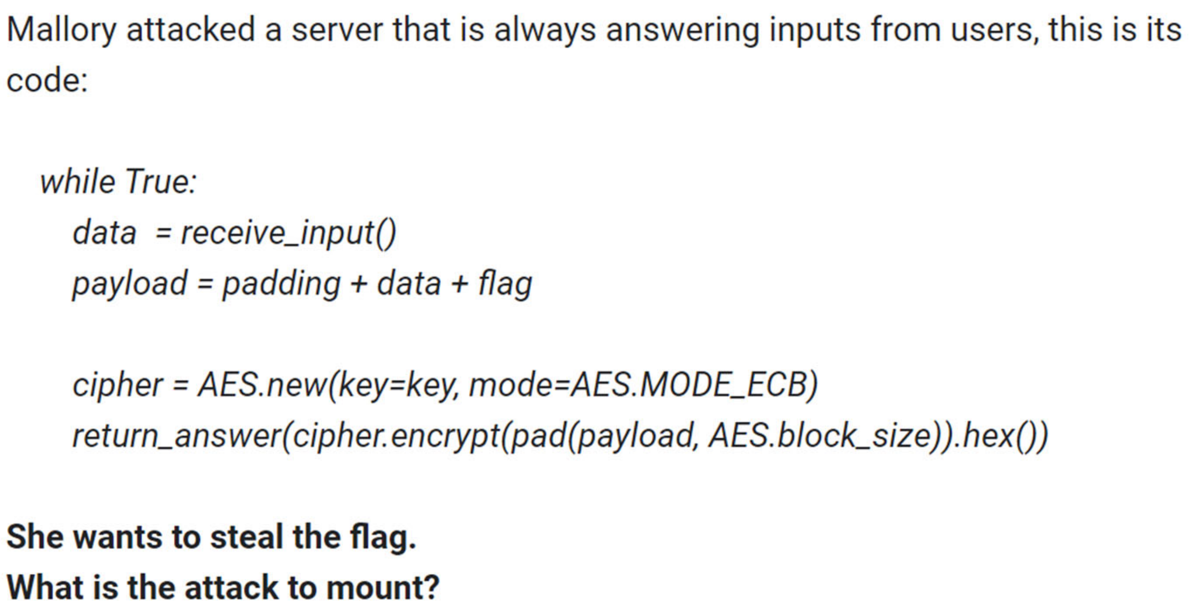
```
username = get_UN()
cipher = AES.new(key=key, mode=AES.MODE_ECB)
cookie = f"username={username}&root=false&p=none"
bytes_to_long(cipher.encrypt(pad(cookie.encode(),AES.block_size)))
```

Which kind of attack you may execute to become an administrator if the server-side authorization checks are performed this way?

```
  try:
      dec_cookie = unpad(cipher.decrypt(long_to_bytes(cookie)),
AES.block_size).decode()
      token = parse_cookie(dec_cookie)
      if token["root"] != 'true' and token["p"]!='rw':
          print("You are not an admin!")
          return
      print(f"OK! You are an admin now!")
      # you need to arrive here
    except:
      print("ERROR")
```

- question 1
  - https://docs.google.com/forms/d/e/1FAIpQLSceHSEtCMQdkDcK4JZl0LVndfrLfS5WPklkpX-lLK1Aafhg1w/viewform?usp=dialog
- question 2
  - https://docs.google.com/forms/d/e/1FAIpQLScAEJYvBeilUjCxT7LI38VIBDVELJ90nue85ZKg31P6W52htw/viewform?usp=dialog

Attack #2



Mallory attacked a server that is always answering inputs from users, this is its code:

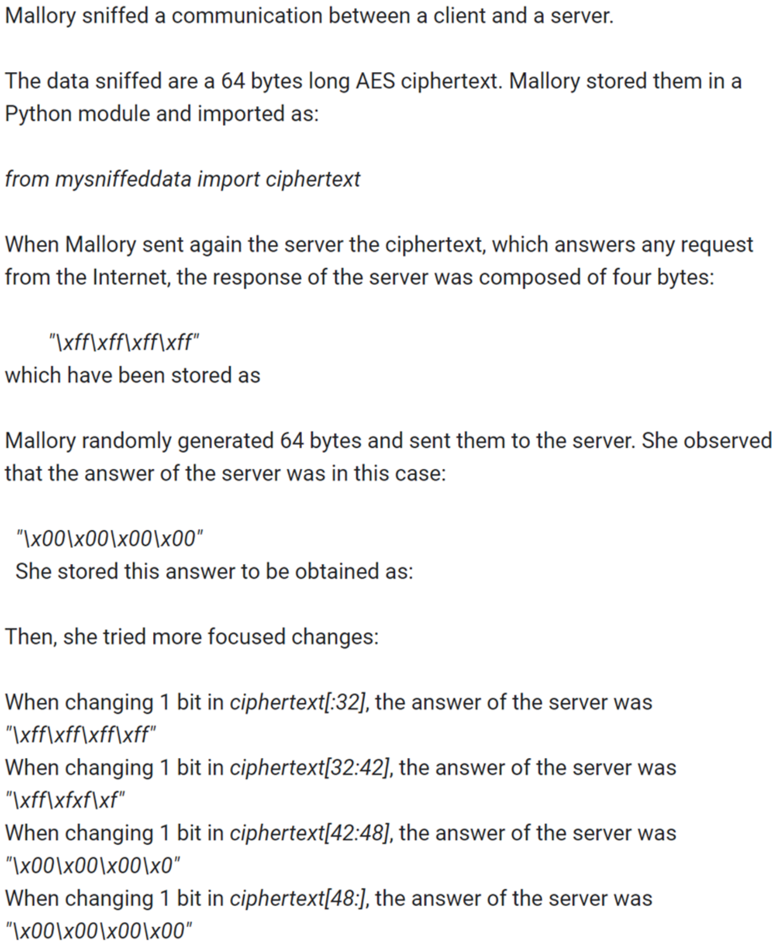
```
while True:
    data  = receive_input()
    payload = padding + data + flag

    cipher = AES.new(key=key, mode=AES.MODE_ECB)
    return_answer(cipher.encrypt(pad(payload, AES.block_size)).hex())
```

She wants to steal the flag.
What is the attack to mount?

- question 1
  - https://docs.google.com/forms/d/e/1FAIpQLSfu3numoCIKbpMOyxiYLjYOShc1W7GBQOataHaJrsJN1bAawA/viewform?usp=dialog
- question 2
  - https://docs.google.com/forms/d/e/1FAIpQLSeInWnGejQ8SsfIAQSWccvrGshoxPcCfNnuRUruTHVFURl0qw/viewform?usp=dialog

Attack #3



Mallory sniffed a communication between a client and a server.

The data sniffed are a 64 bytes long AES ciphertext. Mallory stored them in a Python module and imported as:

from mysniffeddata import ciphertext

When Mallory sent again the server the ciphertext, which answers any request from the Internet, the response of the server was composed of four bytes:

"\xff\xff\xff\xff"
which have been stored as

Mallory randomly generated 64 bytes and sent them to the server. She observed that the answer of the server was in this case:

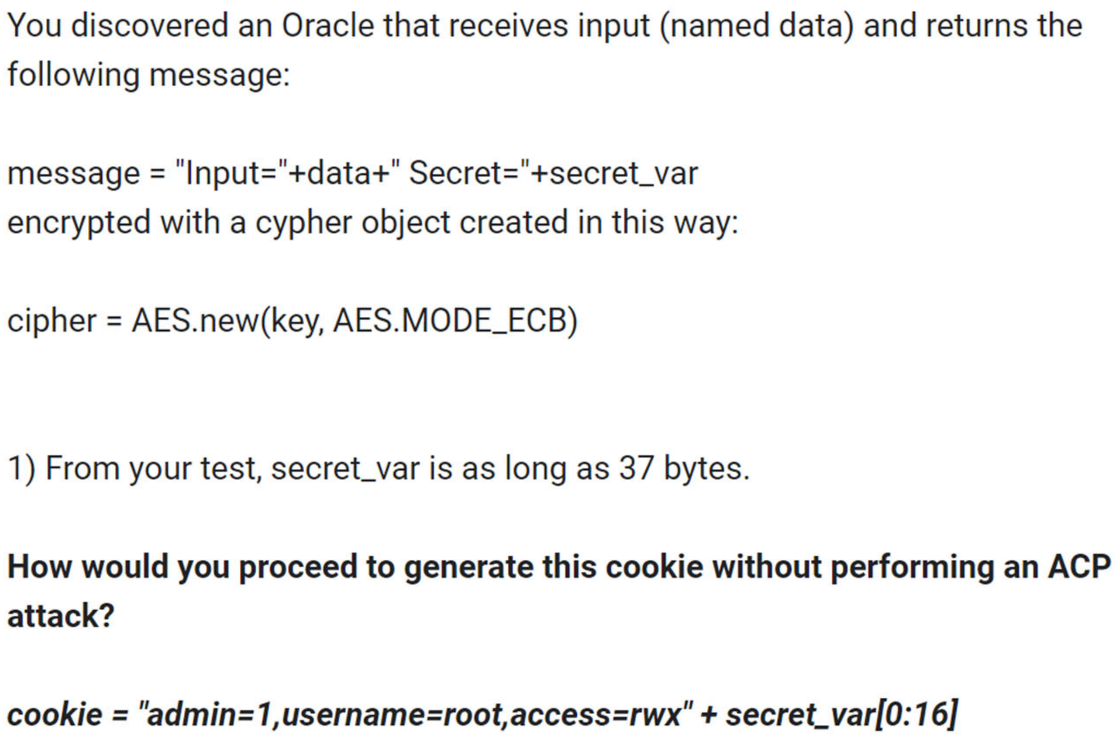
"\x00\x00\x00\x00"
She stored this answer to be obtained as:

Then, she tried more focused changes:

When changing 1 bit in *ciphertext[:32]*, the answer of the server was *"\xff\xff\xff\xff"*
When changing 1 bit in *ciphertext[32:42]*, the answer of the server was *"\xff\xfxf\xf"*
When changing 1 bit in *ciphertext[42:48]*, the answer of the server was *"\x00\x00\x00\x0"*
When changing 1 bit in *ciphertext[48:]*, the answer of the server was *"\x00\x00\x00\x00"*

- question 1
  - https://docs.google.com/forms/d/e/1FAIpQLSfiFns5FfogzLcibVOCCTkFitvgPbzm4OKC4Np-A_DCdgH5sQ/viewform?usp=dialog
- question 2
  - https://docs.google.com/forms/d/e/1FAIpQLSeB2SWBNiXwc2RZ6wExy-DWRltulM92wf4BmAM3-Ly_A_4AqA/viewform?usp=dialog
  - question 3
    - https://docs.google.com/forms/d/e/1FAIpQLSezAPY2AcFUVYcjs89j3jTfm17qcY9-7zXuBW-8FlSmUGCVbQ/viewform?usp=dialog
  - question 4
    - https://docs.google.com/forms/d/e/1FAIpQLSfjEYLl1xLXAtftLYqxhLPfIP_8Az3wMBL9EnyAoTmuABvieg/viewform?usp=dialog

Attack #4



You discovered an Oracle that receives input (named data) and returns the following message:

message = "Input="+data+" Secret="+secret_var
encrypted with a cypher object created in this way:

cipher = AES.new(key, AES.MODE_ECB)

1) From your test, secret_var is as long as 37 bytes.

How would you proceed to generate this cookie without performing an ACP attack?

cookie = "admin=1,username=root,access=rwx" + secret_var[0:16]

- question 1
  - https://docs.google.com/forms/d/e/1FAIpQLSf_SoAoJKBDtBQXYQl-r-J58izUlsBwcJbqjAGErRBstsD9wA/viewform?usp=dialog
- question 2
  - https://docs.google.com/forms/d/e/1FAIpQLSeXEco4UK65xECjrjSSCdiEw3-_o1-7lR2WYPnQw9x3ZT_mhw/viewform?usp=dialog