Boston Key Party CTF 2014 Crypto 200

原创

JDIIDJ 于 2014-03-06 12:23:09 发布 959 收藏
分类专栏： CTF 文章标签： 密码学 计算机安全 CTF


```
MITM II: Electric BoogalooCrypto : 200
Chisa and Arisu are trying to tell each other two halves of a very important secret! They think they're saf
http://bostonkeyparty.net/challenges/mitm2-632e4ecc332baba0943a0c6471dec2c6.tar.bz2
```

没什么可讲的，纯实现题。。。

```
#!/usr/bin/python
# -*- coding: utf-8 -*-

import base64
import sys
import SocketServer
import mitmlib
import socket

class Person(object):
 def __init__(self, ip, port):
  self.s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
  self.s.connect((ip, port))
  print "connected to %s" % ip

 def gen_share(self):
  self.secretshare, self.publicshare = mitmlib.mkshare()

 def send_share(self):
  self.s.sendall(str(self.publicshare[0]) + "," + str(self.publicshare[1]))

 def recv_share(self):
  got = self.s.recv(2048).split(',')
  self.partpubshare = tuple([int(got[0]), int(got[1])])
  self.aeskey = mitmlib.mksecret(self.secretshare, self.partpubshare)

 def recv_check(self):
  msg = self.s.recv(400)
  #print msg
  check = mitmlib.decrypt(self.aeskey, msg)
  #print check
  return check

 def send_enc(self, msg):
  self.s.send(mitmlib.encrypt(self.aeskey, msg))
```

```
  self.s.send(mitmlib.encrypt(self.aeskey, msg))


 def recv_secret(self):
  return mitmlib.decrypt(self.aeskey, self.s.recv(400))

 def send_magic(self, magic):
  self.s.send(magic)
 def recv_magic(self):
  magic = self.s.recv(50)
  print magic

if __name__ == '__main__':
 arisu = Person('54.186.6.201', 12345)
 chisa = Person('54.186.6.201', 12346)

 chisa.send_magic("アリスです")
 chisa.recv_magic()

 arisu.recv_magic()
 arisu.send_magic("千佐だよ")

 arisu.gen_share()
 chisa.gen_share()

 arisu.recv_share()
 arisu.send_share()

 chisa.send_share()
 chisa.recv_share()

 cnt = 0
 while cnt < 19:
  cnt += 1
  print cnt
  check_a = arisu.recv_check()
  chisa.send_enc(check_a)
  check_b = chisa.recv_check()
  arisu.send_enc(check_b)
 secret = arisu.recv_secret()
 print secret
 chisa.send_enc(secret)
 print chisa.recv_secret()
```