**********Draft**********

Crypto-Socket
Using AraratSnyapse Library
06/0720

**********Draft**********

This kernel7.img
Provides a remote shell to examing contents of micro sd
Provides the capability to encrypt text using AES GCM
Provides the capability to decrypt text using AES GCM

With only a few files
20-4-20 00:03:32 22 config.txt
Contents of config.txt
start_x=1
gpu_mem=128
7-6-20 17:03:18 2718380 kernel7.img
Linux Firmware
29-3-20 02:24:18 3798568 start_x.elf
29-3-20 02:23:56 52304 bootcode.bin
29-3-20 02:23:56 6745 fixup.dat
29-3-20 02:23:58 9817 fixup_x.dat
29-3-20 02:24:18 2884420 start.elf
29-3-20 02:24:18 3798568 start_x.elf

Files created
7-6-20 15:45:20 908 test0605encrypt.txt
7-6-20 15:45:42 922 test0605decrypt.txt

Remote shell telnet 192.168.1.245

File Edit Tabs Help

```
1-1-80                          1541  test0513.txt
29-3-20 02:24:20            27983872  test.h264
29-3-20 02:24:24                 500  test.html
1-1-80                          7848  test.j2k
6-4-20 17:37:26               196730  test_wr.bmp
7-5-20 13:31:50                 2582  ultibologging.log
29-3-20 02:24:24            27983872  v1.h264
29-3-20 02:24:30             1002763  v2.h264
29-3-20 02:24:30       <DIR>          www
2-4-20 17:31:26                65596  red.pgm
2-4-20 17:31:38                65596  grn.pgm
2-4-20 17:31:52                65596  blu.pgm
13-5-20 18:14:16                1024  Sred.bin
13-5-20 18:14:20                1024  Sgrn.bin
13-5-20 18:14:22              262144  rcgrn.bin
13-5-20 18:14:24                1024  Sblu.bin
13-5-20 18:14:24              262144  rcblu.bin
1-1-80                           111  Example 08 File Handling.txt
25-5-20 12:31:04              135100  blinky.bin
25-5-20 12:35:22              135100  catzip.bin
25-5-20 12:35:22              135100  leddigits.bin
3-6-20 16:24:56                  709  test0527a.txt
5-6-20 21:58:54                  214  test0603.txt
7-6-20 15:45:20                  908  test0605encrypt.txt
```

A connection from RaspBian to Ultibo System "telnet 192.168.1.245 5050".

To isolate the variables I added the following record

```
GCM = record
  SockData:AnsiString;
  EncryptionTagToDecrypt:AnsiString;
  {EncryptionTag1 during teststr 1 or teststr 3 encrypt}
  EncryptionTag1:AnsiString;
  {EncryptionTag2 during teststr 1 or teststr 3 decrypt}
  EncryptionTag2:AnsiString;
  EncryptionTag3:AnsiString;
  PlainStr:AnsiString;
  CryptStr1:AnsiString;
  BinCryptStr1:AnsiString;
  cryptstr: AnsiString;
  tagstr: AnsiString;
  teststr: AnsiString;
  {Must be 16, 24 or 32 bytes}
  MyKey: AnsiString ;
  MyIV: AnsiString;
  MyAAD: AnsiString;
  MyData: AnsiString;
end;
```

The crypted string of bytes from the encryption plus the string of bytes from the Tag needs to be sent to the decrypt process.
The decryption is dependent on the Tag.

telnet 192.168.1.245 5050
Trying 192.168.1.245...
Connected to 192.168.1.245.
Escape character is '^]'.

11234567890123456789012345678901 2:My Secret IV:My Extra Secret AAD:The quick brown testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstuvwxyz

This is what get written to the file test0605encrypt.txt
encrypt
11234567890123456789012345678901 2:My Secret IV:My Extra Secret AAD:The quick brown testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstuvwxyz

GCM1.PlainStr
The quick brown testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstuvwxyz
GCM1.EncryptionTag1
f56c32e2ea3343b31748823b65590a09
GCM1.EncryptionTag2
f56c32e2ea3343b31748823b65590a09
GCM1.MyKey
12345678901234567890123456789012
GCM1.MyIV

My Secret IV
GCM1.MyAAD
My Extra Secret AAD
Decrypted
The quick brown testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstuvwxyz
EncryptionTag
f56c32e2ea3343b31748823b65590a09
Bytes Crypt
0e599f59da22536d4fe2d6bd48c118e594d7ee54ba178f1c918dfd69dea863b7514a8a263a5e5846b15de04945412b3f6334f78109d079d0f8198199c7a2ca297f376f1f97d1e3e75473538b943a6824b01cae711e8c1fedf0837660b99efc554ca60904d613420c

telnet 192.168.1.245 5050
Trying 192.168.1.245...
Connected to 192.168.1.245.
Escape character is '^]'.

21234567890123456789012345678901 2:My Secret IV:My Extra Secret AAD:0e599f59da22536d4fe2d6bd48c118e594d7ee54ba178f1c918dfd69dea863b7514a8a263a5e5846b15de04945412b3f6334f78109d079d0f8198199c7a2ca297f376f1f97d1e3e75473538b943a6824b01cae711e8c1fedf0837660b99efc554ca60904d613420c:f56c32e2ea3343b31748823b65590a09

This is what get written to the file test0605decrypt.txt

decrypt
21234567890123456789012345678901 2:My Secret IV:My Extra Secret AAD:0e599f59da22536d4fe2d6bd48c118e594d7ee54ba178f1c918dfd69dea863b7514a8a263a5e5846b15de04945412b3f6334f78109d079d0f8198199c7a2ca297f376f1f97d1e3e75473538b943a6824b01cae711e8c1fedf0837660b99efc554ca60904d613420c:f56c32e2ea3343b31748823b65590a09

GCM2.tagstr
f56c32e2ea3343b31748823b65590a09

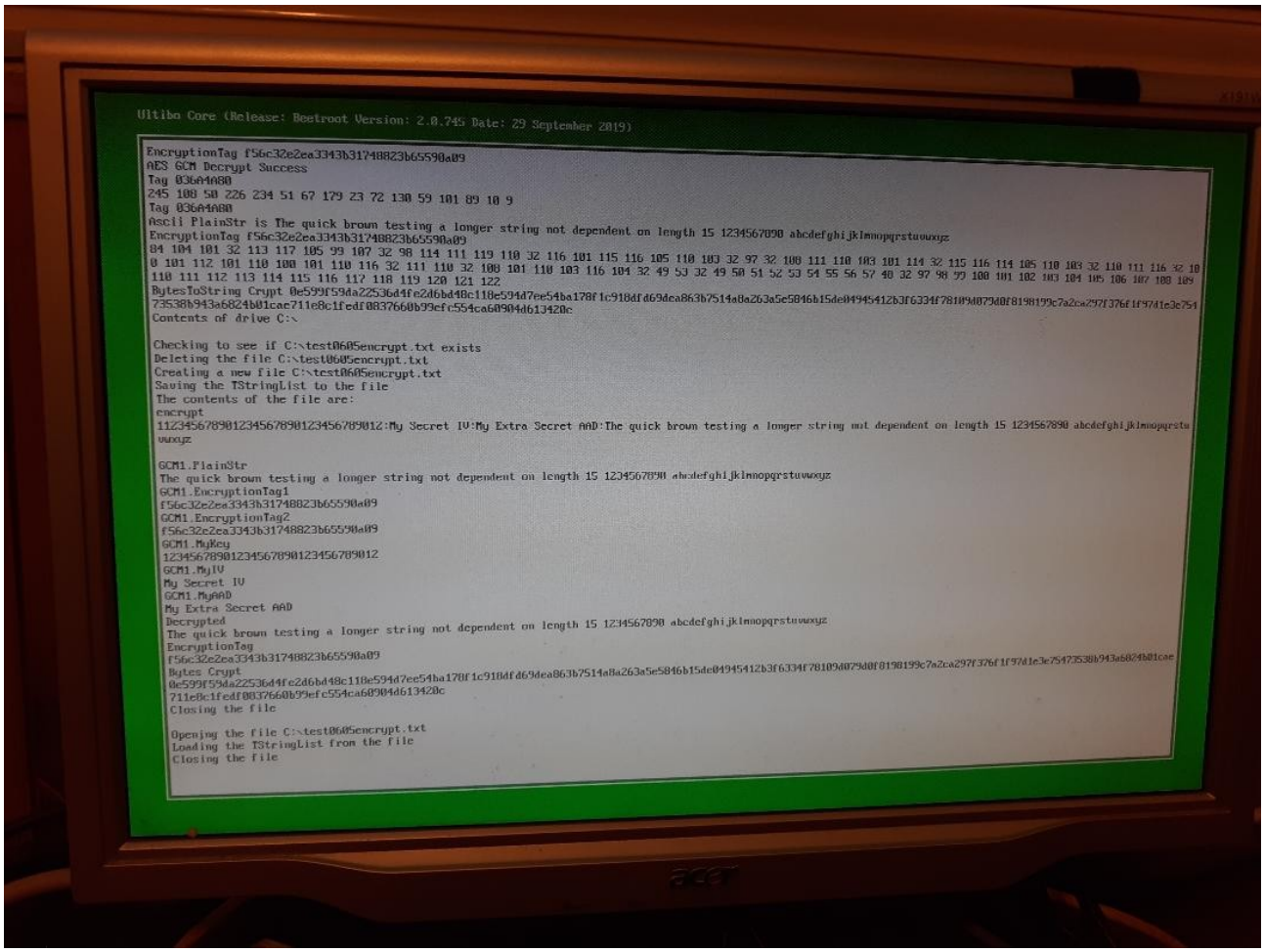
GCM2.PlainStr
The quick brown testing a longer string not dependent on length 15 1234567890 abcdefghijklmnopqrstuvwxyz
GCM2.EncryptionTag2
f56c32e2ea3343b31748823b65590a09
GCM2.MyKey
12345678901234567890123456789012
GCM2.MyIV
My Secret IV
GCM2.MyAAD
My Extra Secret AAD
GCM2.EncryptionTagToDecrypt
f56c32e2ea3343b31748823b65590a09
MyKey
12345678901234567890123456789012
MyIV
My Secret IV
MyAAD

My Extra Secret AAD
Decrypted

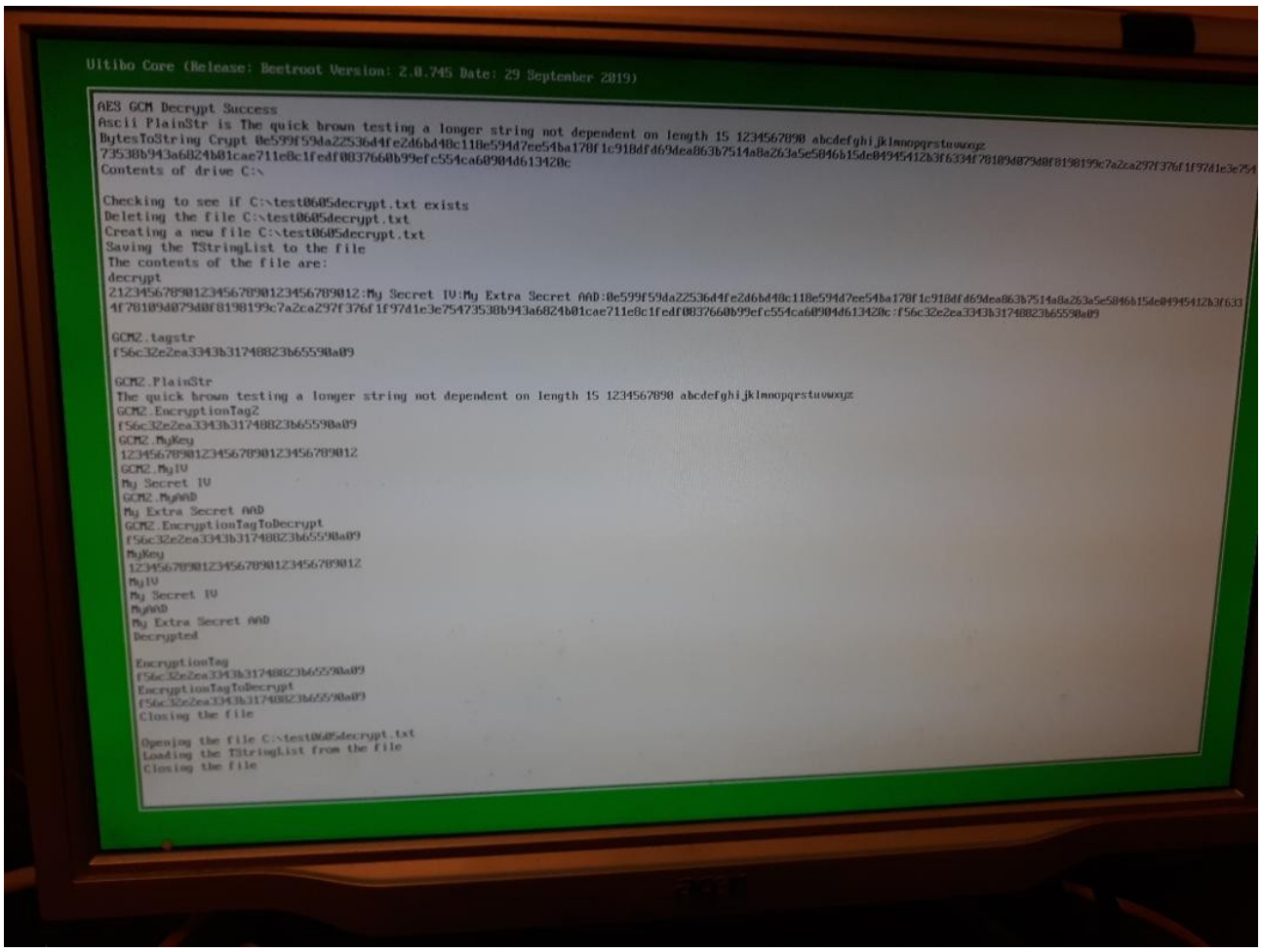
EncryptionTag
f56c32e2ea3343b31748823b65590a09
EncryptionTagToDecrypt
f56c32e2ea3343b31748823b65590a09

tftp 192.168.1.245
tftp> binary
tftp> get test0605encrypt.txt
Received 908 bytes in 0.0 seconds
tftp> get test0605decrypt.txt
Received 922 bytes in 0.0 seconds
tftp> quit

256 Bit encrypt



256 Bit decrypt



Background: Started with 2 projects test_crypto.lpi & Srv.lpi from github devlone Ultibo_Projects.

Commad line using FPC

Step 1
. ~/fpc.sh

Step 2
cd Ultibo_Projects/Crypto-Socket/Rpi3/ or cd Ultibo_Projects/Crypto-Socket/RPi2/

Step 3
compile

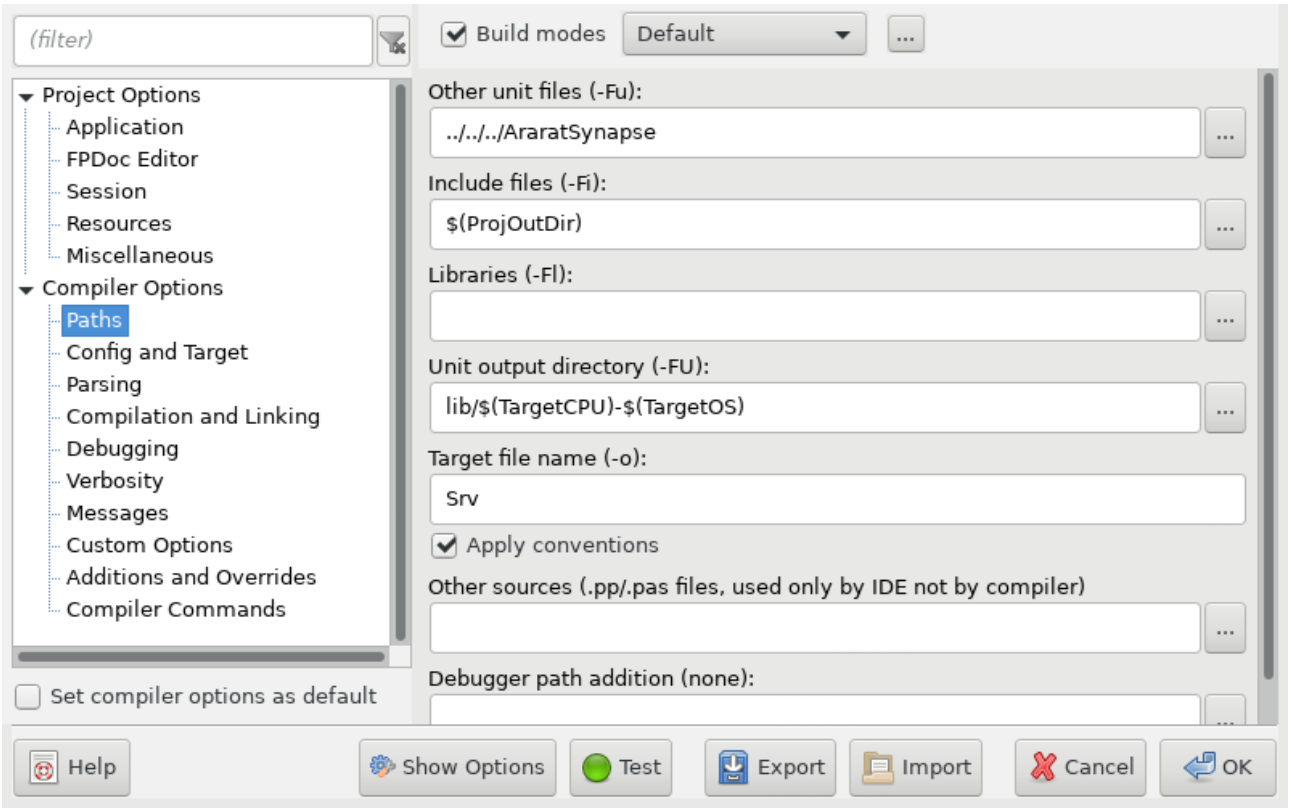
fpc -vi -B -Tultibo -Parm -CpARMV7A -WpRPI3B -Fu../../../AraratSynapse @/home/devel/ultibo/core/fpc/bin/RPI3.CFG -O2 Srv.lpr

or

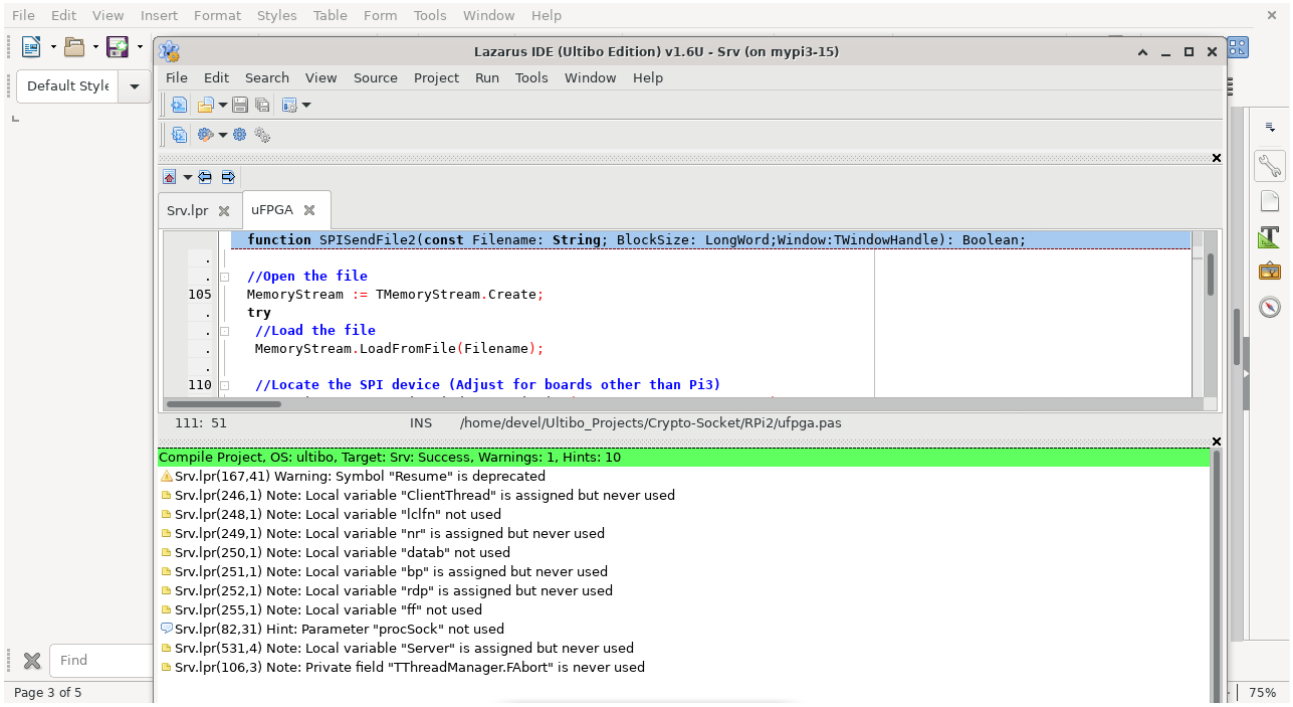
fpc -vi -B -Tultibo -Parm -CpARMV7A -WpRPI2B -Fu../../../AraratSynapse
@/home/devel/ultibo/core/fpc/bin/RPI2.CFG -O2 Srv.lpr
Transfer kernel7.img
./upker7.sh

Updating kernel7.img
tftp> tftp> Sent 2718380 bytes in 10.7 seconds
tftp> done

Compiling with Lazaraus.



Depress Run/Compile


Lazarus IDE (Ultibo Edition) v1.6U - Srv (on mypi3-15)
File Edit Search View Source Project Run Tools Window Help
Srv.lpr
uFPGA
function SPISendFile2(const Filename: String; BlockSize: LongWord;Window:TWindowHandle): Boolean;
//Open the file
105 MemoryStream := TMemoryStream.Create;
try
//Load the file
MemoryStream.LoadFromFile(Filename);
110 //Locate the SPI device (Adjust for boards other than Pi3)
111: 51 INS /home/devel/Ultibo_Projects/Crypto-Socket/RPi2/ufpga.pas
Compile Project, OS: ultibo, Target: Srv: Success, Warnings: 1, Hints: 10
Srv.lpr(167,41) Warning: Symbol "Resume" is deprecated
Srv.lpr(246,1) Note: Local variable "ClientThread" is assigned but never used
Srv.lpr(248,1) Note: Local variable "lclfn" not used
Srv.lpr(249,1) Note: Local variable "nr" is assigned but never used
Srv.lpr(250,1) Note: Local variable "datab" not used
Srv.lpr(251,1) Note: Local variable "bp" is assigned but never used
Srv.lpr(252,1) Note: Local variable "rdp" is assigned but never used
Srv.lpr(255,1) Note: Local variable "ff" not used
Srv.lpr(82,31) Hint: Parameter "procSock" not used
Srv.lpr(531,4) Note: Local variable "Server" is assigned but never used
Srv.lpr(106,3) Note: Private field "TThreadManager.FAbort" is never used