LAB Assignment #3 for ECE 525

Description: Add Provisioning Data to DB

In this lab, you will add the provisioning data from lab2 to a master database. The database is used by a secure server (your laptop) to authenticate and to generate session encryption keys. It contains a subset of the 'device secrets'.

You will also add SiRF PUF challenges to a challenges database, that the device (CORA or ZYBO) will use in the authentication protocol.

Run the following sequence of commands. Note you will need to do a 'git pull' (see lab2) to complete this lab.

1) Make ProvisionData, DATABASE and PROTOCOL directories in the directory where you created lab2 and HOST2023 (called the BASE directory)

```
mkdir ProvisionData
mkdir DATABASE
```

Your directory structure should look like

```
lab2
HOST2023
ProvisionData
DATABASE
PROTOCOL
```

NOTE: DO NOT DO YOUR LABS in the github directory, HOST2023

2) cd into DATABASE

```
cd DATABASE
```

3) Copy all the files in the DATABASE directory on the website here. NOTE: There is a SQLSchemaScripts subdirectory!
(whatever copy method you use)

4) Make an output directory

```
mkdir output
```

5) Change back to BASE directory.

```
cd ..
```

6) cd into PROTOCOL

```
cd PROTOCOL
```

7) Copy all the files in the PROTOCOL directory on the website to your PROTOCOL directory (whatever copy method you use)
8) cd into ProvisionData and copy the files from the HOST2023 repository here

```
cd ../ProvisionData
cp -p ../HOST2023/ProvisionData/* .
```

9) Change to DATABASE

```
../DATABASE
```

10) Compile the programs.

```
make -f Makefile_AddChallengeDB
make -f Makefile_EnrollDB
make -f Makefile_add_PUFDesign_challengeDB
```

11) Create NAT_Master_TDC.db (non-anonymous timing database) (Note: You must have sqlite3 installed)

NOTE: If you need to start over with the database creation process, start by removing the databases (rm *.db) and re-running these scripts

```
sqlite3 NAT_Master_TDC.db < SQLSchemaScripts/SQL_PUFDesign_create_table.sql
sqlite3 NAT_Master_TDC.db < SQLSchemaScripts/SQL_PUFInstance_create_table.sql
sqlite3 NAT_Master_TDC.db < SQLSchemaScripts/SQL_VecPairs_create_table.sql
sqlite3 NAT_Master_TDC.db < SQLSchemaScripts/SQL_Vectors_create_table.sql
sqlite3 NAT_Master_TDC.db < SQLSchemaScripts/SQL_TimingVals_create_table.sql
sqlite3 NAT_Master_TDC.db < SQLSchemaScripts/SQL_PathSelectMasks_create_table.sql
sqlite3 NAT_Master_TDC.db < SQLSchemaScripts/SQL_Challenges_create_table.sql
sqlite3 NAT_Master_TDC.db < SQLSchemaScripts/SQL_ChallengeVecPairs_create_table.sql

sqlite3 Challenges.db < SQLSchemaScripts/SQL_PUFDesign_create_table.sql
sqlite3 Challenges.db < SQLSchemaScripts/SQL_PUFInstance_create_table.sql
sqlite3 Challenges.db < SQLSchemaScripts/SQL_VecPairs_create_table.sql
sqlite3 Challenges.db < SQLSchemaScripts/SQL_Vectors_create_table.sql
sqlite3 Challenges.db < SQLSchemaScripts/SQL_TimingVals_create_table.sql
sqlite3 Challenges.db < SQLSchemaScripts/SQL_PathSelectMasks_create_table.sql
sqlite3 Challenges.db < SQLSchemaScripts/SQL_Challenges_create_table.sql
sqlite3 Challenges.db < SQLSchemaScripts/SQL_ChallengeVecPairs_create_table.sql
```

12) Add the provisioning data to the database

NOTE: You will eventually need to ADD ALL Provisioning data to the database, i.e., ALL files in the HOST2023/ProvisionData directory. Do ‘git pull’ as needed and do the cp command above to copy the files from the HOST2023 repository to your local ../ProvisionData directory.

NOTE: If you want to do your files first, change the ’C_Jim_204’ to your filename prefix

NOTE: ALWAYS USE ZYBO, even if you have a CORA board in the following!

NOTE: CHECK output/enrollDB... file for errors.

NOTE: Add additional ‘enrollDB’ command lines for the other files in the ProvisionData directory.

My CORA files:

```
    enrollDB  NAT_Master_TDC.db  SR_RFM_V4_TDC  SRFSyn1  ZYBO  P1  Z_Jim_64  392  32  ../CHALLENGES/
SR_RFM_V4_Random_Rise_1000Vs_Fall_1000Vs_NumSeeds_10_vecs           0           ../ProvisionData/
Z_Jim_64_SR_RFM_V4_TDC_P1_25C_1.00V_NCs_2000_E_PUFNums.txt               >               output/
enrollDB_SR_RFM_V4_TDC_SRFSyn1_Cx_Vx.txt
    enrollDB  NAT_Master_TDC.db  SR_RFM_V4_TDC  SRFSyn1  ZYBO  P2  Z_Jim_64  392  32  ../CHALLENGES/
SR_RFM_V4_Random_Rise_1000Vs_Fall_1000Vs_NumSeeds_10_vecs           0           ../ProvisionData/
Z_Jim_64_SR_RFM_V4_TDC_P2_25C_1.00V_NCs_2000_E_PUFNums.txt               >>              output/
enrollDB_SR_RFM_V4_TDC_SRFSyn1_Cx_Vx.txt
```

```
enrollDB NAT_Master_TDC.db SR_RFM_V4_TDC SRFSyn1 ZYBO P3 Z_Jim_64 392 32 ../CHALLENGES/
SR_RFM_V4_Random_Rise_1000Vs_Fall_1000Vs_NumSeeds_10_vecs 0 ../ProvisionData/
Z_Jim_64_SR_RFM_V4_TDC_P3_25C_1.00V_NCs_2000_E_PUFNums.txt >> output/
enrollDB_SR_RFM_V4_TDC_SRFSyn1_Cx_Vx.txt
enrollDB NAT_Master_TDC.db SR_RFM_V4_TDC SRFSyn1 ZYBO P4 Z_Jim_64 392 32 ../CHALLENGES/
SR_RFM_V4_Random_Rise_1000Vs_Fall_1000Vs_NumSeeds_10_vecs 0 ../ProvisionData/
Z_Jim_64_SR_RFM_V4_TDC_P4_25C_1.00V_NCs_2000_E_PUFNums.txt >> output/
enrollDB_SR_RFM_V4_TDC_SRFSyn1_Cx_Vx.txt
```

My ZYBO files

```
enrollDB NAT_Master_TDC.db SR_RFM_V4_TDC SRFSyn1 ZYBO P1 C_Jim_204 392 32 ../CHALLENGES/
SR_RFM_V4_Random_Rise_1000Vs_Fall_1000Vs_NumSeeds_10_vecs 0 ../ProvisionData/
C_Jim_204_SR_RFM_V4_TDC_P1_25C_1.00V_NCs_2000_E_PUFNums.txt >> output/
enrollDB_SR_RFM_V4_TDC_SRFSyn1_Cx_Vx.txt
enrollDB NAT_Master_TDC.db SR_RFM_V4_TDC SRFSyn1 ZYBO P2 C_Jim_204 392 32 ../CHALLENGES/
SR_RFM_V4_Random_Rise_1000Vs_Fall_1000Vs_NumSeeds_10_vecs 0 ../ProvisionData/
C_Jim_204_SR_RFM_V4_TDC_P2_25C_1.00V_NCs_2000_E_PUFNums.txt >> output/
enrollDB_SR_RFM_V4_TDC_SRFSyn1_Cx_Vx.txt
enrollDB NAT_Master_TDC.db SR_RFM_V4_TDC SRFSyn1 ZYBO P3 C_Jim_204 392 32 ../CHALLENGES/
SR_RFM_V4_Random_Rise_1000Vs_Fall_1000Vs_NumSeeds_10_vecs 0 ../ProvisionData/
C_Jim_204_SR_RFM_V4_TDC_P3_25C_1.00V_NCs_2000_E_PUFNums.txt >> output/
enrollDB_SR_RFM_V4_TDC_SRFSyn1_Cx_Vx.txt
enrollDB NAT_Master_TDC.db SR_RFM_V4_TDC SRFSyn1 ZYBO P4 C_Jim_204 392 32 ../CHALLENGES/
SR_RFM_V4_Random_Rise_1000Vs_Fall_1000Vs_NumSeeds_10_vecs 0 ../ProvisionData/
C_Jim_204_SR_RFM_V4_TDC_P4_25C_1.00V_NCs_2000_E_PUFNums.txt >> output/
enrollDB_SR_RFM_V4_TDC_SRFSyn1_Cx_Vx.txt
```

13) Add challenge to NAT_Master_TDC.db

```
add_challengeDB NAT_Master_TDC.db SR_RFM_V4_TDC SRFSyn1 Master1_OptKEK_TVN_0.00_WID_1.75 ../CHAL-
LENGES/SR_RFM_V4_Random_Rise_1000Vs_Fall_1000Vs_NumSeeds_10 ../CHALLENGES/
optKEK_qualifing_path_TVN_0.00_WID_1.75_SetSize_64000 1 > output/
add_challengeDB_SRFSyn1_Master1_OptKEK_TVN_0.00_WID_1.75.txt
```

14) Make a copy of the NAT_Master_TDC.db to AT_Master_TDC.db (anonymous timing database)

```
cp NAT_Master_TDC.db AT_Master_TDC.db
```

15) Add challenges to Challenges.db

```
add_PUFDesign_challengeDB Challenges.db SR_RFM_V4_TDC SRFSyn1 CORA P1 Cxx 392 32 ../CHALLENGES/
SR_RFM_V4_Random_Rise_1000Vs_Fall_1000Vs_NumSeeds_10_vecs 0 > output/
add_challengeDB_SRFSyn1_Master1_OptKEK_TVN_0.00_WID_1.75_Challenges.txt
add_challengeDB Challenges.db SR_RFM_V4_TDC SRFSyn1 Master1_OptKEK_TVN_0.00_WID_1.75 ../CHAL-
LENGES/SR_RFM_V4_Random_Rise_1000Vs_Fall_1000Vs_NumSeeds_10 ../CHALLENGES/
optKEK_qualifing_path_TVN_0.00_WID_1.75_SetSize_64000 0 > output/
add_challengeDB_SRFSyn1_Master1_OptKEK_TVN_0.00_WID_1.75_Challenges.txt
```