Project C - Review

Assignment 1 (5/5p)

The instructions were clear and easy to repeat. 5p

Assignment 2 (4/4p)

Good description how the EK and SRK dump was obtained. 4p

Assignment 3 (6/10p)

3.3.2

1. Accurate description of the difference between signing and identity keys. 2p
2. Storage keys is correct, there are other keys which can be used for file encryption such as binding or legacy. 1p
3. The EK is used. The key which is not recommended is legacy keys. It's there to enable legacy software to still use keys stored in hardware. 0p

3.3.3

Correct tree hierarchy, although it should not be possible to create C. Children of migratable parents also needs to be migratable, they do not change from non migratable to migratable. 3p

Assignment 4 (11/16p)

3.4.2

1. It is not possible. If a parent is migratable so must the child. 0p
2. Correct, TPM_AuthorizeMigrationKey is the first TPM command to be executed. 2p
3. Correct, converts the blob for usage of the keys. 2p
4. TPM_Loadey is correct according to "https://trustedcomputinggroup.org/wp-content/uploads/TPM-Main-Part-3-Commands_v1.2_rev116_01032011.pdf" . 2p
5. The TSS handles the transfer and the connections to the TPMs while the TPMs are creating and loading the blob. 0p

3.4.4

1. Well documented, forgot to mention if the migration worked or not for the different keys. 1p
2. Correct, although only a reference to the document "https://trustedcomputinggroup.org/wp-content/uploads/TPM-Main-Part-3-Commands_v1.2_rev116_01032011.pdf" . No real description. 2p
3. Correct, rewrap is used to directly move the key. 2p

Assignment 5 (0/6p)

Not done. 0p

Assignment 6 (0/15p)

Not done. 0p

Assignment 7 (0/10p)

Not done. 0p

Assignment 8 (0/5p)

Not done. 0p

Assignment 9 (4/4p)

Nice little program, good description. 4p

Overall points (30/75).

Nice structure and easy to read. Assignment 5 to 8 is not done, although assignment 9 is. Your mark is 3.