Zephyr RTOS Krypto Prozessor

Die Aufgabe ist einfach (formuliert), implementieren Sie in Zephyr RTOS einen Krypto Prozessor der allen in test.py durchgeführten Tests erfolgreich absolviert.

Die mitgelieferte Datei zephyr.elf st eine Referenezimplementierung (unter 64 Bit Ubuntu 20.04, zum Beispiel auch unter Windows 10 / WSL lauffähig). Eine korrekte Lösung verhält sich wie in diesem Dokument beschrieben.

Aufgabe und Eigenschaften des Krypto Prozessors

Der Kyprto Prozessor kann über eine serielle Schnittstelle angesprochen werden und führt für einen Benutzer AES-128 Operationen durch. Es wird das RTOS Zephyr in Version 2.4.0 als Basis verwendet. Diese Code ist damit prinzipiell auf einer Reihe von Microcontroller lauffähig. Wir verwenden als "Microcontroller Board" ein 64bit Linux (board **native_posix_64** in Zephyr Sprech). Da wird für die Linux Entwicklung keine SDKs benötigen muss dieses auch nicht installiert werden. Geben Sie beim Erzeugen der Buildumgebung daher bitte (**CROSS_COMPILE=** und **ZEPHYR_TOOLCHAIN_VARIANT=cross-compile**) an.

Das native_posix_64 Board implementiert eine virtuelle serielle Schnittstelle namens **UART_0**, sowie eine implementierung der crypo API mittels libtinycrypt **CRYPTO_TC**. Diese beiden Treiber sind zu verwenden.

main thread

Der Haupttread ihres Programmes soll alle andere Threads starten und dann nur mehr sporadisch eine Lebensmeldung von sich geben

uart_in thread

Der native_posix_64 UART Treiber unterstützt keine IRQ, darum ist lesen blockierend. Deswegen wird ein Thread benötigt der liest und sobald er ein Zeichen hat dieses in eine **message queue** schickt. Der processing threads konsumiert dieses Zeichen von dort. Wenn das zeichen '.' eingelesen wurde soll dieses als Echo auf der seriellen Schnittstelle wieder ausgegeben werden (s.a. uart_out_thread). Wenn der processing thread beschäftigt ist wird die Nachricht "BUSY" über die serielle Schnittstelle ausgegeben.

uart_out thread

Dieses Thread stellt sicher dass mehrere Threads Nachrichten auf die serielle Schnittstelle ausgeben können ohne sich gegenseitig zu stören (d.h. ein paar Bytes Nachricht 1, ein paar Nachricht 2 usw). Dazu liest er die zu senden Nachrichten aus einer **message queue** aus und schickt dieses Zeichen für Zeichen über die serielle Schnittstelle bevor er eine weitere Nachricht aus seiner queue holt.

processing thread

Dieses Thread führt die Krypto Operationen durch. Diese können u.U. sehr lange dauern. Der processing thread kann genau eine Nachricht in seiner **message queue** speichern, d.h. eine in Bearbeitung, eine wartet, bevor das System "BUSY" Meldungen erzeugen muss.

Standard KEY / IV

Der Standardschlüssel und IV sind jeweils 16 bytes 0x42 ('B').

Serielles Protokoll

serielle Verbindung möglich (aka alive)

Immer wenn eine '.' empfangen wird wird sofort ein '.' zurückgegeben

Kryptoprozessor verfügbar (aka avail)

Wenn ein 'P' empfangen wird Antwortet der processing thread mit "PROCESSING AVAIL"

Lade Schlüssel (aka key)

Ein 'K' gefolgt von 16 bytes AES-128 Schlüssel und einem beliebigen Zeichen (wird verworfen) lädt einen neuen Schlüssel in den Kryptoporzessor

Lade Initial Vecotr (aka iv)

Ein 'I' gefolgt von 16 bytes AES-128 Schlüssel und einem beliebigen Zeichen (wird verworfen) lädt einen neuen Schlüssel in den Kryptoporzessor

Decrypt in CBC Mode

Ein 'D' gefolgt von einem Byte Länge (Ciphertext, muss Vielfaches von Cipherblocksize sein) gefolgt von entsprechend langem Ciphertext und beliebiges Zeichen (wird verworfen). Der Kryptoprozessor entschlüssel mit dem key/iv in aes128-cbc und gibt den Plaintext auf der seriellen Schnittstelle zurück. "XERROR" wenn Fehler aufgetreten sind (z.B.: Länge).

Bewertung

Note	Umgesetzt
4	Dokumentation, test_00_connection_alive, test_01_availibility
3	test_03_decrypt_fault, test_04_decrypt_defaults
2	test_05_decrypt_key_iv
1	test_02_blocking

Dokumentation

Dokumentieren und Beschreiben Sie: west, ninja, Kconfig, DTS, threads und message_queues (ca. 8 Seiten)

Start des Kyprto Prozessors

Das sieht wie folgt aus, man beachte die Zeile mit UART_0, der Pfad der folgt benennt die virtuelle serielle Schnittstelle mit der man mit dem Krypto Prozessor kommunizieren kann. Die Ausgaben am Terminal dürfen Sie gestalten wie sie wollen! (man sieht hier dass der Prozessor via strg+c abgebochen wurde).

```
$ ./zephyr.elf
UART_0 connected to pseudotty: /dev/pts/4
*** Booting Zephyr OS build v2.5.0-rc1-131-g99a4af6c4ae8  ***
Serial Crypto starting on native_posix_64
uart_in_thread started
uart_out_thread started
processing_thread started
main is alive!
main is alive!
^C
```

Start der Testsuite

Die vollautomatische Testsuite besteht aus 6 Tests, diese können auch einzeln gestartet werden, z.B.:

```
 $ python3 -m test MyTests.test_05_decrypt_key_iv  -v /dev/pts/3
```

Diese 6 Tests überprüfen der Reihe nach:

- serielle Verbindung möglich
- Kryptoprozessor verfügbar
- BUSY Meldung implementiert
- Entschlüsselung schlägt ggf. fehlt
- Entschlüsselung mit default key/iv
- Entschlüsselung mit custom key/iv

Auszug aus Testsuite Run

```
$ ./test.py -v /dev/pts/4
test_00_connection_alive (__main__.MyTests) ... 000000.000 Q-RX reset_input_buffer
000000.000 Q-RX reset_input_buffer
000000.000 TX   0000  2E                                              .
000000.021 RX   0000  2E 0A                                           ..
000000.021 TX   0000  2E                                              .
000000.132 RX   0000  2E 0A                                           ..
```

Man sieht hier: Name des tests (test_00_connection_alive) und dann mit Zeitstempel: TX (gesendete) und RX (empfangene) daten, die esten 4 Ziffern sind (hexadezimal) das Offeset (macht nur Sinn wenn mehr wie 16 Daten gleichzeitig gesendet/empfangen werden).

Vollständiger Testsuite Run

```
$ ./test.py -v /dev/pts/4
test_00_connection_alive (__main__.MyTests) ... 000000.000 Q-RX reset_input_buffer
000000.000 Q-RX reset_input_buffer
000000.000 TX   0000  2E                                              .
000000.021 RX   0000  2E 0A                                           ..
000000.021 TX   0000  2E                                              .
000000.132 RX   0000  2E 0A                                           ..
000000.132 TX   0000  2E                                              .
000000.242 RX   0000  2E 0A                                           ..
000000.242 TX   0000  2E                                              .
000000.351 RX   0000  2E 0A                                           ..
000000.351 TX   0000  2E                                              .
000000.462 RX   0000  2E 0A                                           ..
000000.462 TX   0000  2E                                              .
000000.571 RX   0000  2E 0A                                           ..
000000.571 TX   0000  2E                                              .
000000.681 RX   0000  2E 0A                                           ..
000000.681 TX   0000  2E                                              .
000000.792 RX   0000  2E 0A                                           ..
000000.792 TX   0000  2E                                              .
000000.902 RX   0000  2E 0A                                           ..
000000.902 TX   0000  2E                                              .
000001.011 RX   0000  2E 0A                                           ..
ok
test_01_availibility (__main__.MyTests) ... 000000.000 Q-RX reset_input_buffer
000000.000 TX   0000  50                                              P
000001.001 RX   0000  50 52 4F 43 45 53 53 49  4E 47 20 41 56 41 49 4C  PROCESSING AVAIL
000001.001 RX   0010  41 42 4C 45 0A                                  ABLE.
ok
test_02_blocking (__main__.MyTests) ... 000000.000 Q-RX reset_input_buffer
000000.000 TX   0000  57                                              W
000000.000 TX   0000  50                                              P
000001.001 TX   0000  2E                                              .
000002.001 RX   0000  2E 0A 42 55 53 59 0A                            ..BUSY.
000002.002 TX   0000  2E                                              .
000003.002 RX   0000  2E 0A 42 55 53 59 0A                            ..BUSY.
000003.002 TX   0000  2E                                              .
000004.003 RX   0000  2E 0A 42 55 53 59 0A                            ..BUSY.
000004.003 TX   0000  2E                                              .
000005.003 RX   0000  2E 0A 42 55 53 59 0A                            ..BUSY.
000005.003 TX   0000  2E                                              .
000006.004 RX   0000  2E 0A 42 55 53 59 0A                            ..BUSY.
000006.004 TX   0000  2E                                              .
000007.005 RX   0000  2E 0A 42 55 53 59 0A                            ..BUSY.
000007.005 TX   0000  2E                                              .
000008.005 RX   0000  2E 0A 42 55 53 59 0A                            ..BUSY.
000008.005 TX   0000  2E                                              .
000009.006 RX   0000  2E 0A 42 55 53 59 0A                            ..BUSY.
000009.006 TX   0000  2E                                              .
000010.007 RX   0000  2E 0A 42 55 53 59 0A                            ..BUSY.
000010.007 TX   0000  2E                                              .
000011.008 RX   0000  2E 0A 42 55 53 59 0A 50  52 4F 43 45 53 53 49 4E  ..BUSY.PROCESSIN
000011.008 RX   0010  47 20 41 56 41 49 4C 41  42 4C 45 0A              G AVAILABLE.
ok
test_03_decrypt_fault (__main__.MyTests) ... 000000.000 Q-RX reset_input_buffer
000000.000 TX   0000  44                                              D
000000.101 TX   0000  02                                              .
000000.202 TX   0000  AA                                              .
000000.302 TX   0000  E3                                              .
000000.403 TX   0000  58                                              X
000001.505 RX   0000  58 45 52 52 4F 52 0A                            XERROR.
ok
test_04_decrypt_defaults (__main__.MyTests) ... 000000.000 Q-RX reset_input_buffer
000000.000 TX   0000  44                                              D
000000.101 TX   0000  20
000000.202 TX   0000  AA                                              .
000000.302 TX   0000  E3                                              .
000000.403 TX   0000  65                                              e
```

```
000000.503 TX   0000  27                                                '
000000.604 TX   0000  2C                                                ,
000000.705 TX   0000  81                                                .
000000.806 TX   0000  07                                                .
000000.906 TX   0000  8A                                                .
000001.007 TX   0000  B6                                                .
000001.108 TX   0000  11                                                .
000001.208 TX   0000  6B                                                k
000001.309 TX   0000  36                                                6
000001.409 TX   0000  18                                                .
000001.510 TX   0000  31                                                1
000001.611 TX   0000  D0                                                .
000001.711 TX   0000  F6                                                .
000001.812 TX   0000  A5                                                .
000001.912 TX   0000  D3                                                .
000002.013 TX   0000  C8                                                .
000002.114 TX   0000  58                                                X
000002.214 TX   0000  7E                                                ~
000002.315 TX   0000  94                                                .
000002.416 TX   0000  6B                                                k
000002.516 TX   0000  53                                                S
000002.616 TX   0000  0B                                                .
000002.717 TX   0000  79                                                y
000002.817 TX   0000  57                                                W
000002.918 TX   0000  54                                                T
000003.018 TX   0000  31                                                1
000003.119 TX   0000  07                                                .
000003.219 TX   0000  F1                                                .
000003.320 TX   0000  5E                                                ^
000003.421 TX   0000  58                                                X
000004.522 RX   0000  44 20 53 63 68 6F 65 6E  65 20 43 72 79 70 74 6F  D Schoene Crypto
000004.523 RX   0010  20 57 65 6C 74 0D 0D 0D  0D 0D 0D 0D 0D 0D 0D 0D   Welt............
000004.523 RX   0020  0D 0D 00                                          ...
ok
test_05_decrypt_key_iv (__main__.MyTests) ... 000000.000 Q-RX reset_input_buffer
000000.000 TX   0000  4B                                                K
000000.101 TX   0000  41                                                A
000000.201 TX   0000  41                                                A
000000.302 TX   0000  41                                                A
000000.403 TX   0000  41                                                A
000000.503 TX   0000  41                                                A
000000.604 TX   0000  41                                                A
000000.704 TX   0000  41                                                A
000000.805 TX   0000  41                                                A
000000.905 TX   0000  41                                                A
000001.006 TX   0000  41                                                A
000001.106 TX   0000  41                                                A
000001.207 TX   0000  41                                                A
000001.308 TX   0000  41                                                A
000001.408 TX   0000  41                                                A
000001.509 TX   0000  41                                                A
000001.610 TX   0000  41                                                A
000001.710 TX   0000  58                                                X
000001.912 TX   0000  49                                                I
000002.012 TX   0000  41                                                A
000002.113 TX   0000  41                                                A
000002.214 TX   0000  41                                                A
000002.315 TX   0000  41                                                A
000002.415 TX   0000  41                                                A
000002.516 TX   0000  41                                                A
000002.617 TX   0000  41                                                A
000002.718 TX   0000  41                                                A
000002.819 TX   0000  41                                                A
000002.919 TX   0000  41                                                A
000003.020 TX   0000  41                                                A
000003.121 TX   0000  41                                                A
000003.221 TX   0000  41                                                A
000003.322 TX   0000  41                                                A
```

```
000003.423 TX   0000  41                                                A
000003.523 TX   0000  41                                                A
000003.623 TX   0000  58                                                X
000003.724 TX   0000  44                                                D
000003.825 TX   0000  20
000003.925 TX   0000  55                                                U
000004.026 TX   0000  8F                                                .
000004.126 TX   0000  85                                                .
000004.227 TX   0000  68                                                h
000004.328 TX   0000  96                                                .
000004.428 TX   0000  87                                                .
000004.529 TX   0000  31                                                1
000004.629 TX   0000  42                                                B
000004.730 TX   0000  B1                                                .
000004.830 TX   0000  6D                                                m
000004.931 TX   0000  C8                                                .
000005.032 TX   0000  F2                                                .
000005.132 TX   0000  EA                                                .
000005.233 TX   0000  8F                                                .
000005.334 TX   0000  33                                                3
000005.434 TX   0000  4E                                                N
000005.534 TX   0000  DA                                                .
000005.635 TX   0000  7E                                                ~
000005.735 TX   0000  8F                                                .
000005.836 TX   0000  71                                                q
000005.936 TX   0000  37                                                7
000006.037 TX   0000  87                                                .
000006.138 TX   0000  7E                                                ~
000006.239 TX   0000  C2                                                .
000006.339 TX   0000  50                                                P
000006.440 TX   0000  AD                                                .
000006.541 TX   0000  73                                                s
000006.641 TX   0000  3A                                                :
000006.742 TX   0000  74                                                t
000006.842 TX   0000  03                                                .
000006.943 TX   0000  CF                                                .
000007.044 TX   0000  C0                                                .
000007.144 TX   0000  58                                                X
000008.245 RX   0000  44 20 53 63 68 6F 65 6E  65 20 43 72 79 70 74 6F  D Schoene Crypto
000008.245 RX   0010  20 57 65 6C 74 0D 0D 0D  0D 0D 0D 0D 0D 0D 0D 0D   Welt...........
000008.245 RX   0020  0D 0D 00                                          ...
ok
```

Ran 6 tests in 27.300s

OK