COM 402 exercises 2025, session 10: Trusted Hardware and Trusted Computing

Exercise 10.1

In the following scenarios explain whether you need isolation, attestation, or both. Explain what would happen if these properties were not met.

1. An IoT sensor signs a message authenticating itself to the central server that collects measurements.
2. We use a TPM to ensure secure booting of a server located in an isolated room in the basement of a bank.
3. Intel SGX is used to perform biometric access control on a backend server in the cloud.

Exercise 10.2

What would be a better security practice to avoid fraudulent transactions: giving the mayor of the city the right to execute the signature in the HSM, or have the HSM require the credentials of two census civil servants to permit the operation (justify your answer).

Exercise 10.3

Alice runs a certificate authority, and needs a secure machine to store the CA keys and sign certificate requests. What are the challenges, advantages or disadvantages if Alice runs their signing infrastructure:

1. General purpose CPU
2. Enclave running on commercial processor
3. Dedicated hardware security module (HSM)

Exercise 10.4

- Recall that in a secure boot supported by a TPM, TPM_Startup(ST_CLEAR) is run to reset the PCRs. What would go wrong if TPM_Startup(ST_CLEAR) could be called at any time after boot?

Exercise 10.5

- During attestation of software, what could go wrong if the following steps of the protocol do not happen:
    1. The challenger does not send a Challenge (also known as Nonce)
    2. Application and challenger perform a key exchange to establish a secure channel.

Exercise 10.6

- When using trusted hardware, should we care about covert channels[1]?

[1] `https://fas.org/irp/nsa/rainbow/tg030.htm#2.1`

Exercise 10.7

- In Dynamic Data Authentication, would encrypting the PIN verification solve the YesCard problem? If yes, justify. If no, propose a solution.

Exercise 10.8

- Is there any timing side-channel in the following code? If a timing side-channel exists, (1) explain how to exploit it. (2) change the code to prevent the attack (Hint: try to make time measurements useless for the adversary).

Example A:

```
Bool CheckPin(string check, string pin){
    for (int i = 0; i < 4; i++)
        if (check[i] != passcode[i])
            return false;
    return true;
}
```

Example B:

```
// exp(d, C, n) computes C**{d} mod n
Func exp(d, C, n){
    out = 1;
    for (i = 0; i < d.size(); i++){
        out = (out * out) % n;
        if (d[i] == 1)
            out = (out * C) % n;
    }
    return out;
}
```

Example C:

```
// This function computes the dot product of two vectors
// The contents of the vectors are confidential
int dotproduct(int *veca, int *vecb, int len) {
  int acc = 0;
  for(int i = 0; i < len; i++)
    acc += (veca[i] + vecb[i]);

  return sum;
}
```