Code Concerns Exercise

JD Kilgallin

CPSC:480

10/12/22

Photo: Dani Berry, Moby Games
Known for: Creator of first online game, creator of first 4-player game, creator of first game sold in a box, first recipient of Lifetime Achievement Award from Computer Game Developers Assn

Code Concerns Exercise

JD Kilgallin

CPSC:480

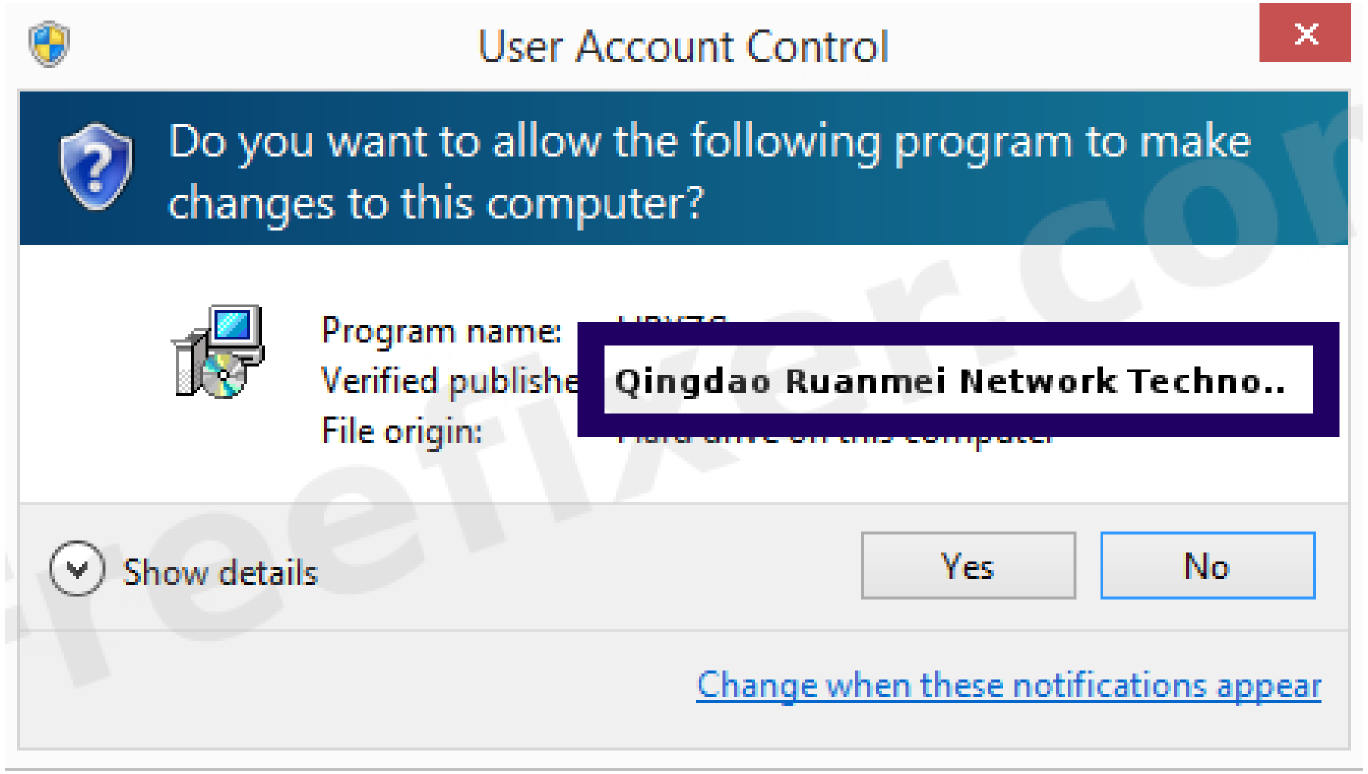
10/12/22

Notes

- Midterm course eval feedback indicates you're generally satisfied with the class. Top request was more recap and summary slides.
- If you put in a Keyfactor referral request, it's pending and will be in by end of the week. If you'd like to submit one, email me your resume.
- Project 2 is due this Sunday, +2% early submission Friday, +1% early submission Saturday. Team participation survey due Monday.
- Today's exercise is due 11:59 PM **tomorrow**, to avoid conflict with P2.
- Project 3 will be assigned next Wednesday, to be due November 13

Public Key Infrastructure (PKI)

- The backbone of communications security.
- Used for all HTTPS requests as well as SSH and other protocols built on SSL and/or TLS.
- Also used for document/ code signing, email encryption, and other identity or data security tasks.



User Account Control

Do you want to allow the following program to make changes to this computer?

Program name:

Verified publishe Qingdao Ruanmei Network Techno..

File origin: Hard drive on this computer

PKI and certificates

- PKI consists of a *Certificate Authority (CA)* that issues *end-entity certificates* to specific identities for specific purposes.
- A certificate contains information about the identity and authorized purpose for the cert, a digital signature from the CA, and a *public key.*
- Each certificate has a corresponding *private key* that is mathematically related to the public key. Content that is encrypted with the public key can only be decrypted with the private key, and content that is signed with the private key can be verified with the public key.
- As long as the private key is only accessible to the intended party, you know that nobody else can read content encrypted with the public key and that nobody can tamper with content signed by the private key.

PKI and Keyfactor

- A large organization could have hundreds of thousands of certificates; several for each user, workstation, and server the company owns.
- A connected-device manufacturer could have hundreds of *millions*, with one or more on each device.
- A large cloud application like news, hotel or retail websites could have thousands at any one time, with thousands more needed each day.
- Keyfactor helps organizations securely issue, manage, renew, and automate tasks related to usage of these certificates.
- A Keyfactor deployment consists of a certificate management platform connected to one or more CAs, and one or more (usually many more) *agents* which can be installed on a machine and communicates with the platform to manage certs locally on that machine.

Keyfactor C Agent

- A distributed software component that communicates with the Keyfactor platform to manage digital certificates and keys on a device (e.g. car, smartlock, pacemaker).
- The agent makes an HTTP request to Keyfactor to acquire an agent *session*, which contains a list of *jobs* for the agent. Each job will start with another HTTP request to get configuration details for that job.
- A job can be any of the following:
  - Inventory – Look at pre-defined locations on the device, identify any certificates and keys at that location, and send the certificates to Keyfactor.
  - Manage – Take a certificate from Keyfactor and add or remove it at a pre-defined location on the device.
  - Enrollment – Generate a new key and Certificate Signing Request (CSR), pass it to Keyfactor to have a certificate issued, and install the certificate+key.
  - Fetch logs – Collect local agent logs and pass to Keyfactor.

Exercise source code

- Clone, fork, or view https://github.com/kilgallin/Keyfactor-CAgent
- Review this high-level description of the code:
  - "lib" folder holds 3rd-party code for base64 and JSON formatting
  - "openssl_wrapper" and "wolfssl_wrapper" folders hold interfaces to cryptography libraries used for generating keys and certificates.
  - agent.c contains the main function and core session registration and job scheduling logic.
  - inventory.c, management.c, enrollment.c, and fetchlogs.c hold implementations of the respective job types.
  - All other .c files hold helper code related to one particular aspect or concern of the agent program. You will also find .h, .json, .txt/.md files and a makefile.
  - Some of the code includes pre-processor switches to build the code for different hardware systems. You can gloss over these for this assignment.

Exercise overview

- Form groups of 2-3 students.
- Identify how the Keyfactor C Agent decomposes its concerns into multiple files (the agent would typically be incorporated as one module of a larger firmware package for a device).
- Identify how the Keyfactor C Agent handles cross-cutting concerns.
- Identify inconsistencies or omissions in handling of concerns.
- Write a report.

Exercise details

1. For each .c file in the root folder (minus utils.c), identify its main concern and write a sample corresponding requirement ("As a user, I want ___").
2. For each of the following cross-cutting concerns, identify blocks of code in three different files that relate to the concern and briefly describe how/why; state the filename and line numbers for each block.
   - Logging (excluding blocks in logging.c/.h)
   - Data validation
   - Persistence
   - Licensing
   - Memory management
   - Select one other cross-cutting concern of your choice
3. Identify one of the above cross-cutting concerns that the agent might be able to handle better in at least one case and briefly explain how.
4. Identify one challenge that might be likely to come up with localization of the agent, & explain how the code could be modified to make this easier.

Submission

- Write up a document (approximately 1-2 pages) with the responses for items 1-4. Include the names of everyone involved.
- One member of the 2-3-person team should submit to "exercise 4" on Brightspace as PDF by **Thursday, Oct 13, 11:59 PM** (tomorrow).
- Grading:
  1. 26% (1% per concern analysis, 1% per requirement)
  2. 54% (3% per block)
  3. 10%
  4. 10%

References

- A Salute to Dani Berry. Luke Plunkett. Feb 2012. Kotaku.
- Qingdao Ruanmei Network Technology Co.,Ltd. 2022. Freefixer.
- What is PKI? Ted Shorter et al. 2022. Keyfactor.
- How to Regain Control of Compromised IoT Device Certificates. JD Kilgallin. June 2019. Liveworx.
- Keyfactor C Agent. J Proch, R Lillback, J Kilgallin, and S Shin. 2017-2022. Keyfactor.

- *Reading for next lecture:*
    - *Keyfactor Coding Standards on Brightspace*
    - *Avoid Else, Return Early by Tim Oxley*