

Intro to Computer Security COMP 2300

Professor Sashank Narain

UMASS Lowell, Fall 2024

Class Project, Milestones 1-3

**Authors: Patricia Antlitz, Andrew Jacobson, Paul Warwick, Flower Letourneau**

**The README.md of this project contains all instructions on how to properly run it.**

**GitHub Repository:** <https://github.com/andrewjacobson5/secureFTP>

This project makes use of certificates to establish a mutual TLS connection which is used to secure the communication channel between the client and the server. This confirms both the client and server have certificates signed by the same Certificate Authority. Although the certificates are being properly generated, they are not fully integrated into the code quite yet. As of right now the main form of data security is password hashing and deletion, error handling and garbage collection. The certificates functionalities will be fully implemented on the part two of this project.

Given this information, to run this code, you must first generate the certificates:

You can run either `make generate-certificates` OR

`./generate_certificates.sh` if you have a **Unix or Linux** system.

You can run either `make generate-widows-cert` OR

`./generate_windows_cert.sh` if you have a **Windows** machine. Please note, the

windows certificate generation was not tested since none of us had a windows machine available at the moment to try it out.

This project also makes use of the **bcrypt** library. To run the code, you might need to use a virtual environment.

You can run the following commands on **Unix or Linux**: `python3 -m venv venv`

and then: `source venv/bin/activate`

For **Windows**: `python3 -m venv venv`

and then: `.\venv\Scripts\activate`

After activating your virtual environment, you can install **bcrypt**:

Run `make install` to automatically install the dependencies OR run `./requirements.txt`

Now you are ready to run this program.

You can use `make run` to start or simply run the `main.py` file. Remember you can always use `make clean` to remove unnecessary files such as certificates once you finish running the program, and you can also run `deactivate` to deactivate the virtual environment.

Certificate generation:

```

secureFTP -- -zsh -120x35

patriciaantlitz@Patricias-MBP-2 secureFTP % cd
patriciaantlitz@Patricias-MBP-2 % % cd Documents/UMASS/FALL\ 2024/Intro\ to\ Cyber\ Defense
patriciaantlitz@Patricias-MBP-2 Intro to Cyber Defense % cd secureFTP
patriciaantlitz@Patricias-MBP-2 secureFTP % ls
Makefile      generate_certificates.sh  ssc
README.md     generate_windows_cert.sh  venv
docs          requirements.txt
patriciaantlitz@Patricias-MBP-2 secureFTP % make generate-certificates
./generate_certificates.sh
patriciaantlitz@Patricias-MBP-2 %

```

## Create and activate an environment and install the required dependencies

The image shows a code editor interface with a file explorer on the left and a terminal window on the right.

**File Explorer (Left):**

- SECUREFTP
  - venv
    - certs
      - ca\_cert.pem
      - ca\_cert.srl
      - ca\_key.pem
      - client\_cert.pem
      - client\_key.pem
      - client.csr
      - server\_cert.p...
      - server\_key.pem
      - server.csr
    - docs
      - LICENSE
      - SECURITY.md
    - src
      - contacts.py
      - encrypt.py
      - main.py
      - menu\_options.py
      - mutual\_cert.py
      - user.py
      - utils.py
    - venv
    - .gitignore
    - generate\_certificate...
    - generate\_windows\_...
    - Makefile
    - README.md
    - requirements.txt
  - OUTLINE

**Terminal Window (Right):**

secureFTP --zsh -- 120x35

```
patriciaantlitz@Patricias-MBP-2 secureFTP % ls
Makefile                                docs                                requirements.txt
README.md                               generate_certificates.sh            src
certs                                   generate_windows_cert.sh            venv

patriciaantlitz@Patricias-MBP-2 secureFTP % python3 -m venv venv
patriciaantlitz@Patricias-MBP-2 secureFTP % source venv/bin/activate
(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % make install
pip3 install -r requirements.txt
Collecting bcrypt==4.2.0 (from -r requirements.txt (line 1))
  Using cached bcrypt-4.2.0-cp39-abi3-macosx_10_12_universal2.whl.metadata (9.6 kB)
Using cached bcrypt-4.2.0-cp39-abi3-macosx_10_12_universal2.whl (472 kB)
Installing collected packages: bcrypt
Successfully installed bcrypt-4.2.0

patriciaantlitz@Patricias-MBP-2 secureFTP %
[notice] A new release of pip is available: 24.2 -> 24.3.1
[notice] To update, run: pip install --upgrade pip
(venv) patriciaantlitz@Patricias-MBP-2 secureFTP %

patriciaantlitz@Patricias-MBP-2 secureFTP % git pull origin main
From github.com:andrewjacobs/5/secureFTP
* branch          main          -> FETCH_HEAD
Successfully rebased and updated refs/heads/milestone_1-3_Pati.
(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % git status
On branch milestone_1-3_Pati
Your branch is ahead of 'origin/milestone_1-3_Pati' by 7 commits.
(use 'git push' to publish your local commits)

nothing to commit, working tree clean
(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % git push
Enumerating objects: 5, done.
Counting objects: 100% (5/5), done.
Delta compression using up to 8 threads
Compressing objects: 100% (3/3), done.
Writing objects: 100% (3/3), 502 bytes | 502.00 KiB/s, done.
Total 3 (delta 2), reused 0 (delta 0); pack-reused 0
remote: repository update: 100% (3/3), completed with 3 local objects
```

Run the program – the program will create an users.json file

```

@ README.md > # Secure File Transfer Project > ## Version 1 - Milestone 1:
[(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % ls
Makefile          docs
README.md         generate_certificates.sh
certs             generate_windows_cert.sh
[(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % make run
python3 src/main.py
# this code runs on port 8443

No users are registered with this client.
Do you want to register a new user (y/n)?
Server started with mutual TLS
n
QUITTING kill it by:
Mutual TLS server
[(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % make run
python3 src/main.py

No users are registered with this client.
Do you want to register a new user (y/n)?
Server started with mutual TLS
y
Enter Full Name: Patricia Antlitz
Enter Email Address: patricia_antlitz@student.uml.edu
Enter Password:
Re-Enter Password:
Passwords Matched.
User PATRICIA ANTLITZ Registered Successfully!
[(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % git pull origin main
Your branch is ahead of 'origin/milestone_1-3_Pati' by 7 commits
nothing to commit, working tree clean
[(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % git push
objects: 100% (5/5), done.
compression using up to 8 threads
objects: 100% (3/3), 502 bytes
docs 3 (delta 2), reused 0 (delta 0), pushed 0
[(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % ls
Makefile          generate_certificates.sh
README.md         generate_windows_cert.sh
certs             requirements.txt
src               venv

```

Error  
handling

File  
Created

LOGIN

```

((venv) patriciaantlitz@Patricias-MBP-2 secureFTP % make run
python3 src/main.py
{
  "patricia_antlitz@student.uml.edu": {
    "full_name": "PATRICIA ANTLITZ",
    "password": "JDJiJDEyJFBL0VJ5dUloQkltcm9GbTVLWVlPaHVIT183bnpxBjdnZnBMVxkxPbmguWDhDL0t3OVQuVmdL",
    "contacts": [
      {
        "contact_name": "Luna Tuna",
        "contact_email": "luna@e.com"
      }
    ]
  }
}
An User Exists in This Machine.
Enter 'L' to login, or 'R' to register a new user:
Server started with mutual TLS
1
LOGIN
Enter Email Address: patricia_antlitz@student.uml.edu
Enter Password:
WELCOME TO SECUREDROP!
User PATRICIA ANTLITZ Logged in Successfully!
Type 'help' For Commands: help
Help Menu:
'ADD' -> Add a new contact
Enter One of the Options Above: add
Enter Contact's Full Name: Luna Tuna
Enter Contact's Email: luna@e.com
New Contact: Luna Tuna with email luna@e.com was added to patricia_antlitz@student.uml.edu's contact list
Mutual TLS server
((venv) patriciaantlitz@Patricias-MBP-2 secureFTP %
Your branch is ahead of 'origin/milestone_1-3_Pati' by 7 commits.
(use 'git push' to publish your local commits)
nothing to commit, working tree clean

```

User selection is  
NOT case sensitive

Contacts

After adding different users and more contacts:

```

{} users.json > {} patricia_antlitz@student.uml.edu > [ ] contacts > {} 3
1
2 {
3   "patricia_antlitz@student.uml.edu": {
4     "full_name": "PATRICIA ANTLITZ",
5     "password": "JDJiJDEyJFBL0VJ5dUloQkltcm9GbTVLWVlPaHVIT183bnpxBjdnZnBMVxkxPbmguWDhDL0t3OVQuVmdL",
6     "contacts": [
7       {
8         "contact_name": "Luna Tune",
9         "contact_email": "luna@e.com"
10      },
11      {
12        "contact_name": "Carol The Carrot",
13        "contact_email": "carol@carrot.com"
14      },
15      {
16        "contact_name": "Mr Monkey",
17        "contact_email": "mr@monkey.com"
18      },
19      {
20        "contact_name": "Snakie",
21        "contact_email": "snake@toy.com"
22      }
23    ]
24  },
25  "lunathemaltese@email.com": {
26    "full_name": "LUNA TUNE",
27    "password": "JDJiJDEyJFBL0VJ5dUloQkltcm9GbTVLWVlPaHVIT183bnpxBjdnZnBMVxkxPbmguWDhDL0t3OVQuVmdL",
28    "contacts": [
29      {
30        "contact_name": "George",
31        "contact_email": "lunasbff@email.com"
32      },
33      {
34        "contact_name": "Birdie",
35        "contact_email": "lunasfavtoy@email.com"
36      }
37    ]
38  }
39 }

```



Contact Overwrite:

```
[(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % make run
python3 src/main.py
{} users.json > {} lunathemaltese@email.com > [ ] contacts > {} 1 > [ ] contact_email
An User Exists in This Machine.
{} patricia_antlitz@student.uml.edu": {
{} "contacts": {
Enter 'L' to login, or 'R' to register a new user:
Server started with mutual TLS
1 {}
LOGIN {}),
{} "lunathemaltese@email.com": {
Enter Email Address: lunathemaltese@email.com
[Enter Password: "password": "JDJlJDEyJEVpdjRFdz8hMDJ5NHB2dUZjRVJQb2UuZEFuL3FJZDB5ajNFeVJlb3hjY
{} "contacts": {
U {}
WELCOME TO SECUREDROP!
User LUNA TUNE Logged in Successfully!
{} "contact_email": "lunasbff@email.com"
Type 'help' For Commands: help
{}
Help Menu: {} "contact_name": "Squeaky",
M {} "contact_email": "lunasfavtoy@email.com"
'ADD' -> Add a new contact
Enter One of the Options Above: add
Enter Contact's Full Name: Squeaky
Enter Contact's Email: lunasfavtoy@email.com
Existing Contact UPDATED to Squeaky for email address: lunasfavtoy@email.com
Mutual TLS server
(venv) patriciaantlitz@Patricias-MBP-2 secureFTP %
```

From:

```
{
  "contact_name": "Birdie",
  "contact_email": "lunasfavtoy@email.com"
}
```

To:

```
{
  "contact_name": "Squeaky",
  "contact_email": "lunasfavtoy@email.com"
}
```

Error Handling:

```
(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % make run
python3 src/main.py

An User Exists in This Machine.

Enter 'L' to login, or 'R' to register a new user:
Server started with mutual TLS
f
Invalid choice, please try again.

Enter Correct Selection: t
Invalid choice, please try again.

Enter Correct Selection: g
Invalid choice, please try again.

Enter Correct Selection: e
Invalid choice, please try again.

Enter Correct Selection: h
Invalid choice, please try again.

Enter Correct Selection: t
Invalid choice, please try again.

Enter Correct Selection: l
LOGIN

Enter Email Address: 
```

3 attempts on credentials:

```
[(venv) patriciaantlitz@Patricias-MBP-2 secureFTP % make run  
python3 src/main.py
```

An User Exists in This Machine.

Enter 'L' to login, or 'R' to register a new user:

Server started with mutual TLS

1

LOGIN

Enter Email Address: lunathemaltese@email.com

[Enter Password:

Email and Password Combination Invalid.

Enter Email Address: lunathemaltese@email.com

[Enter Password:

Email and Password Combination Invalid.

Enter Email Address: lunathemaltease@email.com

[Enter Password:

Email and Password Combination Invalid.

Mutual TLS server

(venv) patriciaantlitz@Patricias-MBP-2 secureFTP %