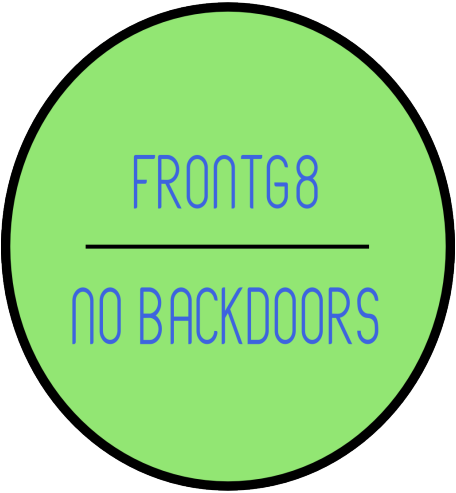




FRONTG8

NO BACKDOORS

frontg8

an opensource, closed-group, secure chatsystem

Ueli Bosshard, Tobias Stauber, Felix Morgner

Computer Science
Hochschule für Technik Rapperswil

May 29, 2015

1 Motivation

2 Mission

3 Demo

4 Technologies

5 Architecture

6 Effort

7 Quality

8 Conclusion

Motivation

- No control over data
- No control over storage
- Volatile datastorage
- Lack of Anonymity

Idea

- Self-hosted
- Strong Encryption
- a chat system - how hard can it be?
- Open-Source

Mission

opensource, closed-group, secure chatsystem

Setup

- Client on Thinkpad (Tobias)
- Client on MacBook (Ueli)
- Client on MacBookPro (Felix)
- Server on Novena

Demo

DEMO GODS



**PLEASE MAKE
THIS DEMO WORK**

C++

- C++14
 - Generic lambdas
 - Standard UDLs
 - New lambda captures
- Clang 3.6.1
- libc++

Python

- Python 3.4
 - 'asyncio' module
 - Enhanced consistency

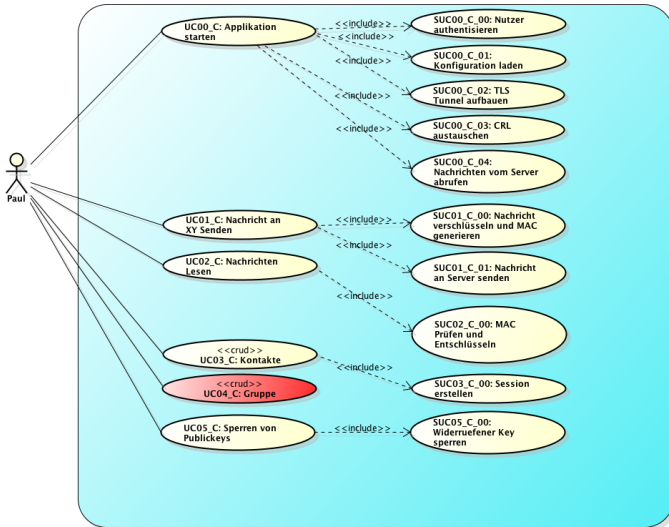
Libraries/Toolkits/Frameworks

- Protobuf
- OpenSSL
- Asio
- asyncio
- npyscreen

Development environment

- Linux (Debian/Ubuntu/Arch)
- OSX
- VIM 7.4

Usecases



Connection-Security

- Connection-Encryption (TLS)
- Certificate Validation
- Privacy

Message-Security

- End-to-End Encryption
- Asymmetric Based
- PRF: Symmetric Session Encryption
- HMAC

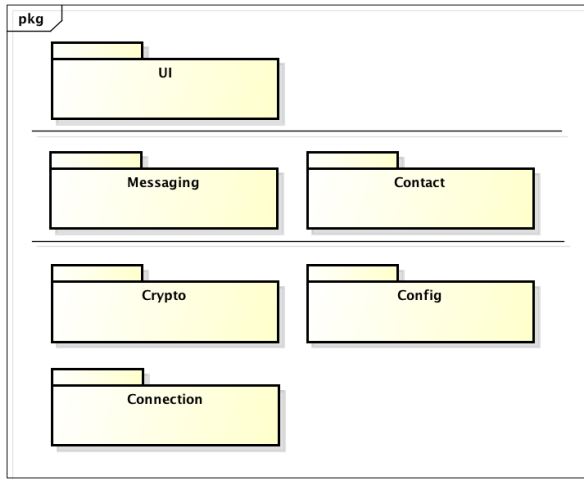
Abusecases



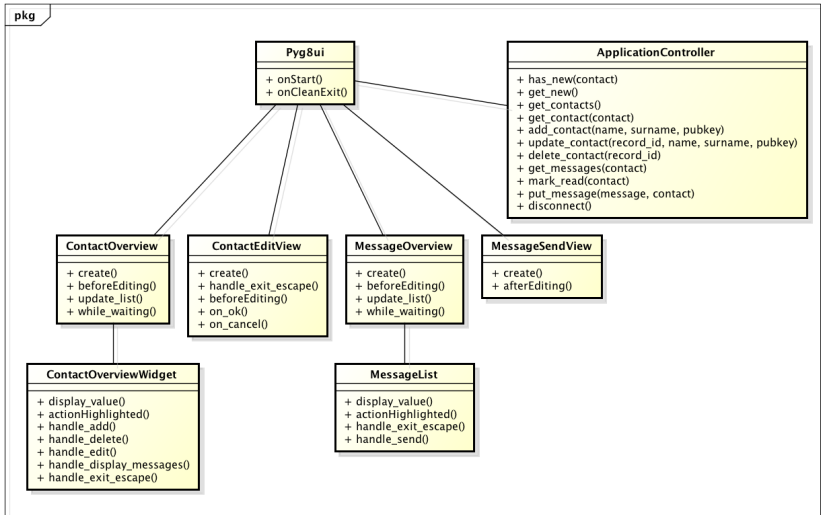
Protocol (UTF15)

- Based on Google Protobuf
 - Platform independent
 - C++, Java, Python, Ruby, ...
 - Extensible
- Custom header
- Client: 7 Message types
- Server: 5 Message types

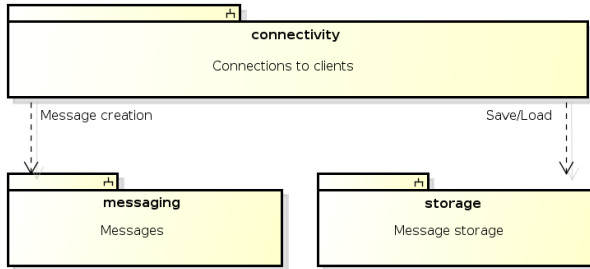
pyg8-Packages



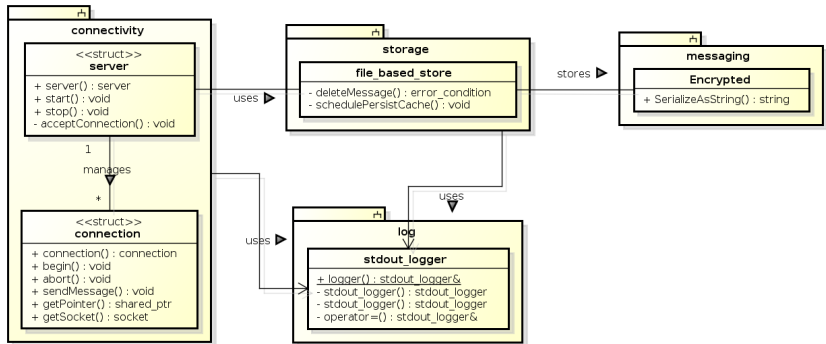
pyg8-Package UI



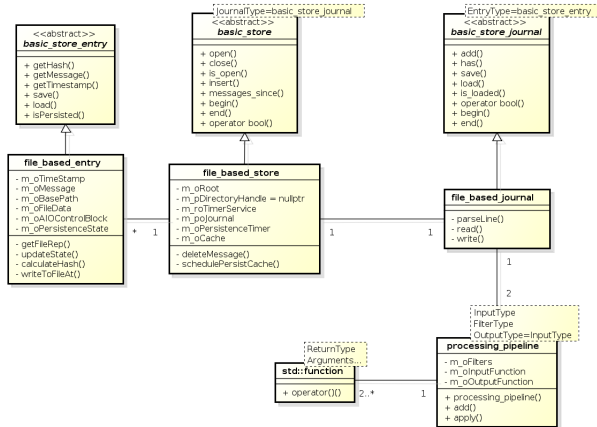
frontg8d-Packages



frontg8d-Overview



frontg8d-Storage



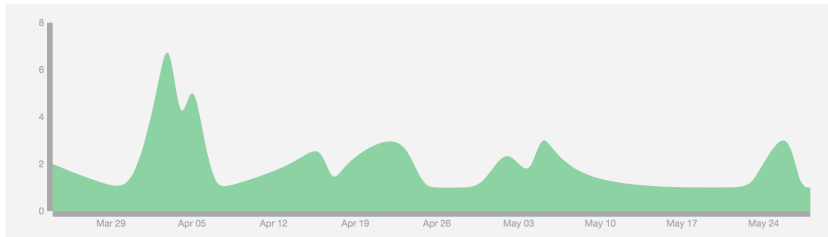
Effort

- 1471 Lines of Code in C++
- 1338 Lines of Code in Python
- 14 Classes in C++
- 22 Classes in Python
- 45 Tests in Server
- 44 Tests in Client
- 433 hours of work

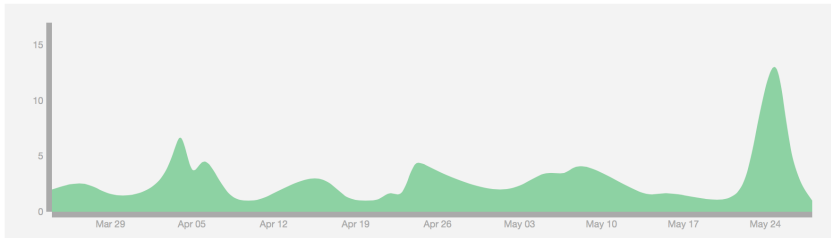
Distribution of Working Hours

Benutzer	2015-2	2015-3	2015-4	2015-5	Gesamtzeit
Felix Morgner	4.50	47.00	68.25	45.00	164.75
Tobias Stauber	4.75	48.05	60.75	19.50	133.05
Ueli Bosshard	8.50	44.00	47.25	36.25	136.00
Gesamtzeit	17.75	139.05	176.25	100.75	433.80

Commits Server



Commits Client

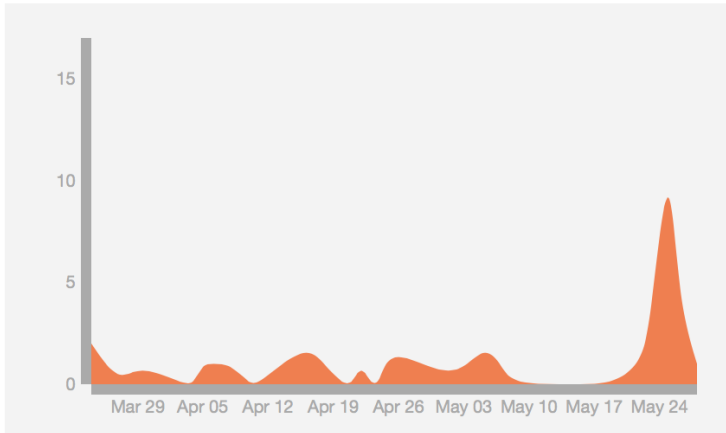


Commits fmorgner

Felix Morgner

36 commits

felix.morgner@gmail.com

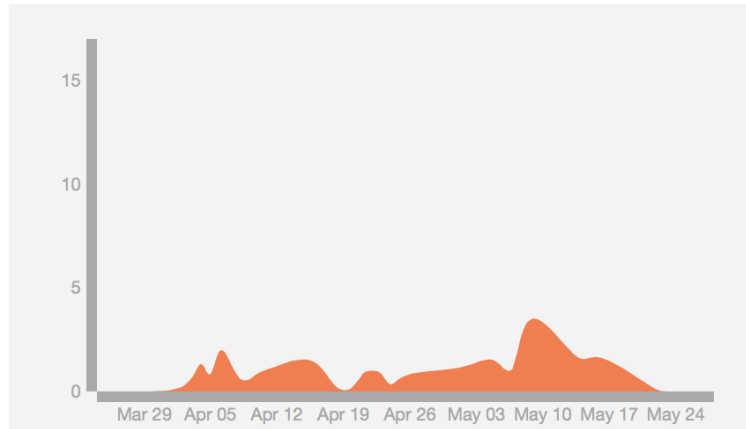


Commits tstauber

Stautob

25 commits

stautob@stautob.ch

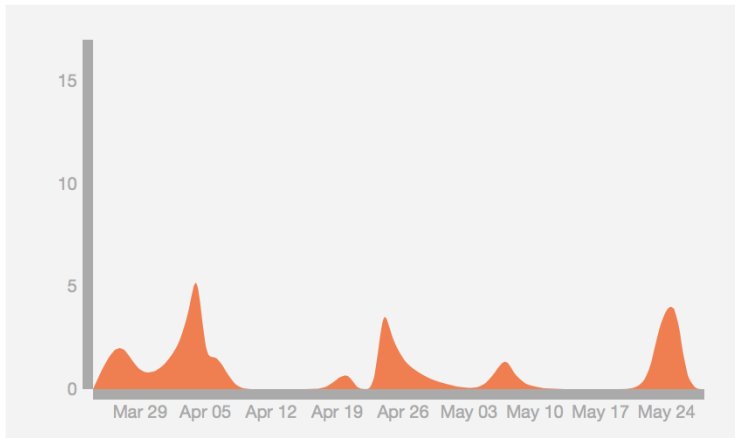


Commits ubosshar

Ueli Bosshard

32 commits

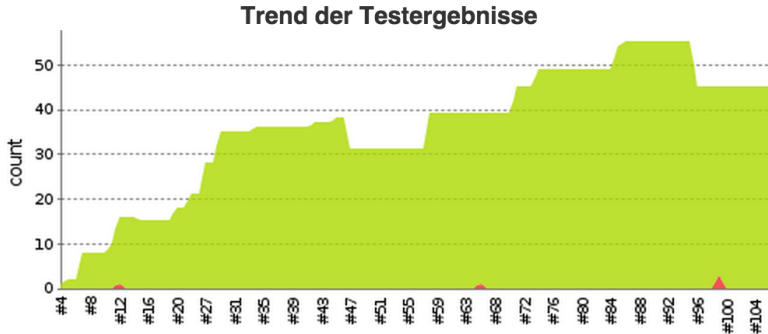
ueli@lilo.ch



Quality Control

- Jenkins
- Gerrit
- Static analysis
- Dynamic analysis
- Unit testing

Jenkins



[\(Nur Fehlschläge anzeigen\)](#) [Vergrößern](#)

Gerrit

[All](#)
[My](#)
[Projects](#)
[People](#)
[Documentation](#)

[Open](#)
[Merged](#)
[Abandoned](#)

Change **178** - **Merged**

Included in ▼ Patch Sets (1/1) ▼ Download ▼ ☆

Added support for editing contacts

Change-Id: If8202b3baa8712869a64d5d07ca96428c5d43caa

Owner

Felix Morgner

Reviewers

Jenkins BuildBot

Tobias Stauber [Add...](#)

Project

client

Branch

master

Topic

Updated

2 days ago

Cherry Pick

Revert

Code-Review +2 Tobias Stauber

Verified +1 Jenkins BuildBot

Author

Felix Morgner <felix.morgner@gmail.com>

May 26, 2015 6:44 PM

Committer

Felix Morgner <felix.morgner@gmail.com>

May 26, 2015 6:44 PM

Commit

fc3450f6f8e46b8a47ad441f981f0d6b9e2ff11

[\(gitweb\)](#)

Parent(s)

a18ee27a69b04690b80a3133eae60f8c94d15df2

[\(gitweb\)](#)

Change-Id

If8202b3baa8712869a64d5d07ca96428c5d43caa

[\(gitweb\)](#)

Files

Open All

Diff against: Base

File Path	Comments	Size
Commit Message lib/ui/Applicationcontroller.py lib/ui/Contacteditview.py		8 4 +9, -3

History

Expand All

Felix Morgner	Uploaded patch set 1.
Jenkins BuildBot	Patch Set 1: 'Build Started http://jenkins.frontg8.ch/jenkins/job/client/163/ '
Jenkins BuildBot	Patch Set 1: Verified+1 'Build Successful http://jenkins.frontg8.ch/jenkins/job/client/163/ : SUCCESS'
Tobias Stauber	Patch Set 1: Code-Review+2
Gerrit Code Review	Change has been successfully merged into the git repository.

Gerrit

All My Projects People Documentation

[Open](#) [Merged](#) [Abandoned](#)

[client / lib/ui/Contacteditview.py](#)

Patch Set **Base 1** Patch Set **1**

```
... skipped 33 common lines ...+100
34     self.pubkeyfile.value = ''
35
36     else:
37         self.name = "New Record"
38         self.record_id = ''
39         self.pname.value = ''
40         self.surname.value = ''
41         self.pubkey.value = ''
42         self.pubkeyfile.value = ''
43
44     def on_ok(self):
45         encoded_key = base64.b64encode(bytes(self.pubkey))
46
47         if self.record_id:
48             self._app_controller.update_contact(self.record_id,
49                                                 name=self.name,
50                                                 surname=self.surname,
51                                                 pubkey=self.pubkey)
52         else:
53             self._app_controller.add_contact(name=self.name,
54                                             surname=self.surname,
55                                             pubkey=self.pubkey,
56                                             keyfile=self.pubkeyfile)
57
58     self.parentApp.switchFormPrevious()
59
60     def on_cancel(self):
61         self.parentApp.switchFormPrevious()
```

```
... skipped 33 common lines ...+100
34     self.pubkeyfile.value = ''
35
36     else:
37         self.name = "New Record"
38         self.record_id = ''
39         self.pname.value = ''
40         self.surname.value = ''
41         self.pubkey.value = ''
42         self.pubkeyfile.value = ''
43
44     def on_ok(self):
45         decoded_key = base64.b64decode(bytes(self.pubkey))
46
47         if self.record_id:
48             self._app_controller.update_contact(self.record_id,
49                                                 name=self.name,
50                                                 surname=self.surname,
51                                                 pubkey=self.pubkey)
52         else:
53             self._app_controller.add_contact(name=self.name,
54                                             surname=self.surname,
55                                             pubkey=self.pubkey,
56                                             keyfile=self.pubkeyfile)
57
58     self.parentApp.switchFormPrevious()
59
60     def on_cancel(self):
61         self.parentApp.switchFormPrevious()
```

Gerrit

- 4-eyes principle
- Has to compile
- Unit tests have to run

Static/Dynamic analysis

- clang-analyze
- clang address sanitizer
- clang memory sanitizer

Unit testing

- Python 'unittest'
- Python 'unittest-xml-reporting'
- C++ 'CUTE'

Lessons learned

- A chat system - how hard can it be?
- Security is hard
- Anonymity is a nightmare
- Team communication
- Reviews help
 - A lot

Q&A

:wq