

# Egg Beater

# Executive Summary:

## Purpose

- ❏ Create an encryption system that provides superior file security
- ❏ Tool for generating encryption keys from fingerprints
- ❏ Open Source

# Executive Summary: Design and Methodology

- ❏ MVC Architecture
  - ❏ Alterations
- ❏ Agile Development
  - ❏ Modified Test-Driven Development
    - ❏ Unit Testing
    - ❏ Acceptance Testing
  - ❏ Object-Oriented Programming
    - ❏ Embedded Modifications

# Research

## GUI frameworks

-  Qt

-  Wxwidgets

## Fingerprint modules

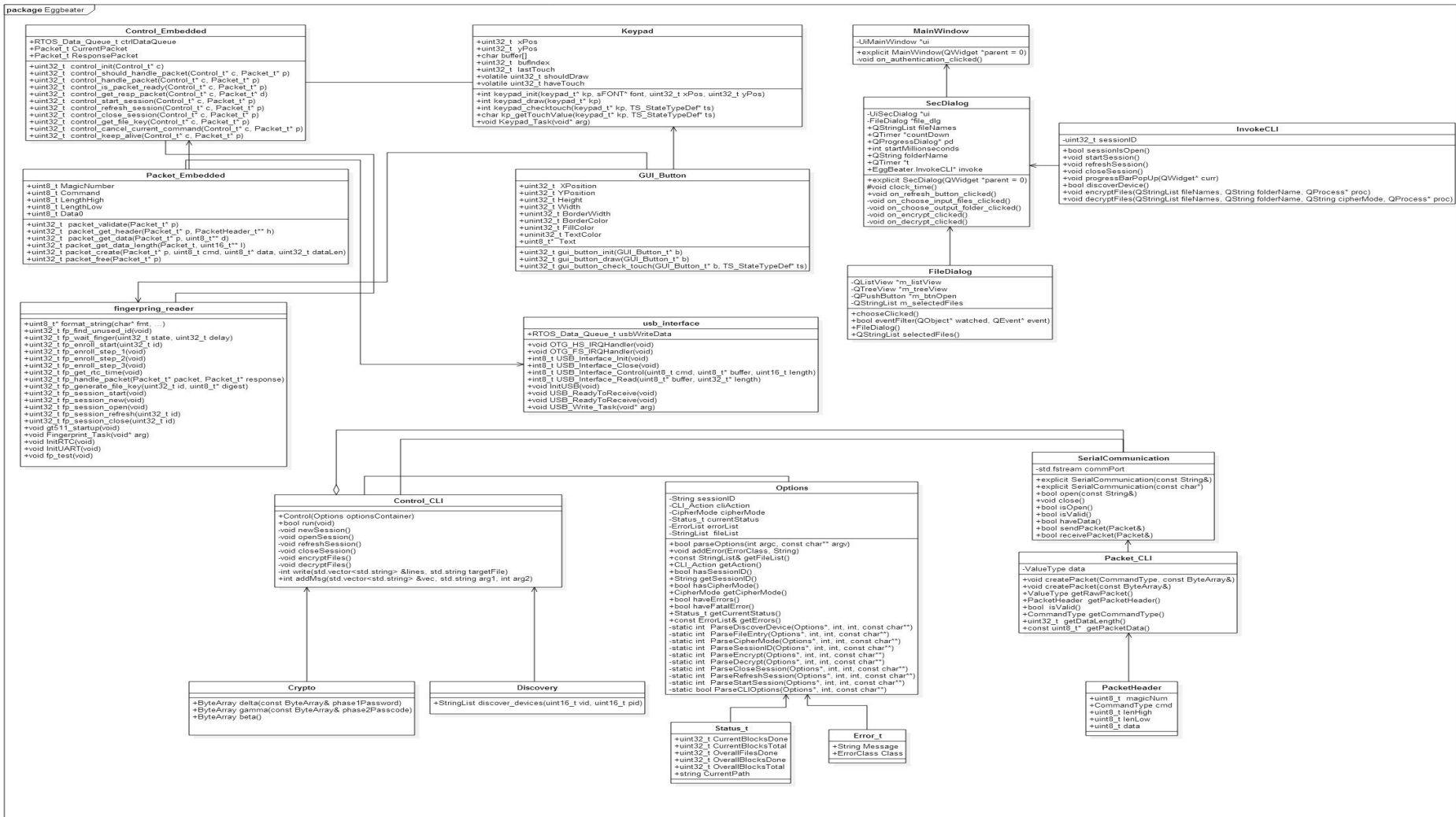
-  GT511C1R

## Encryption libraries

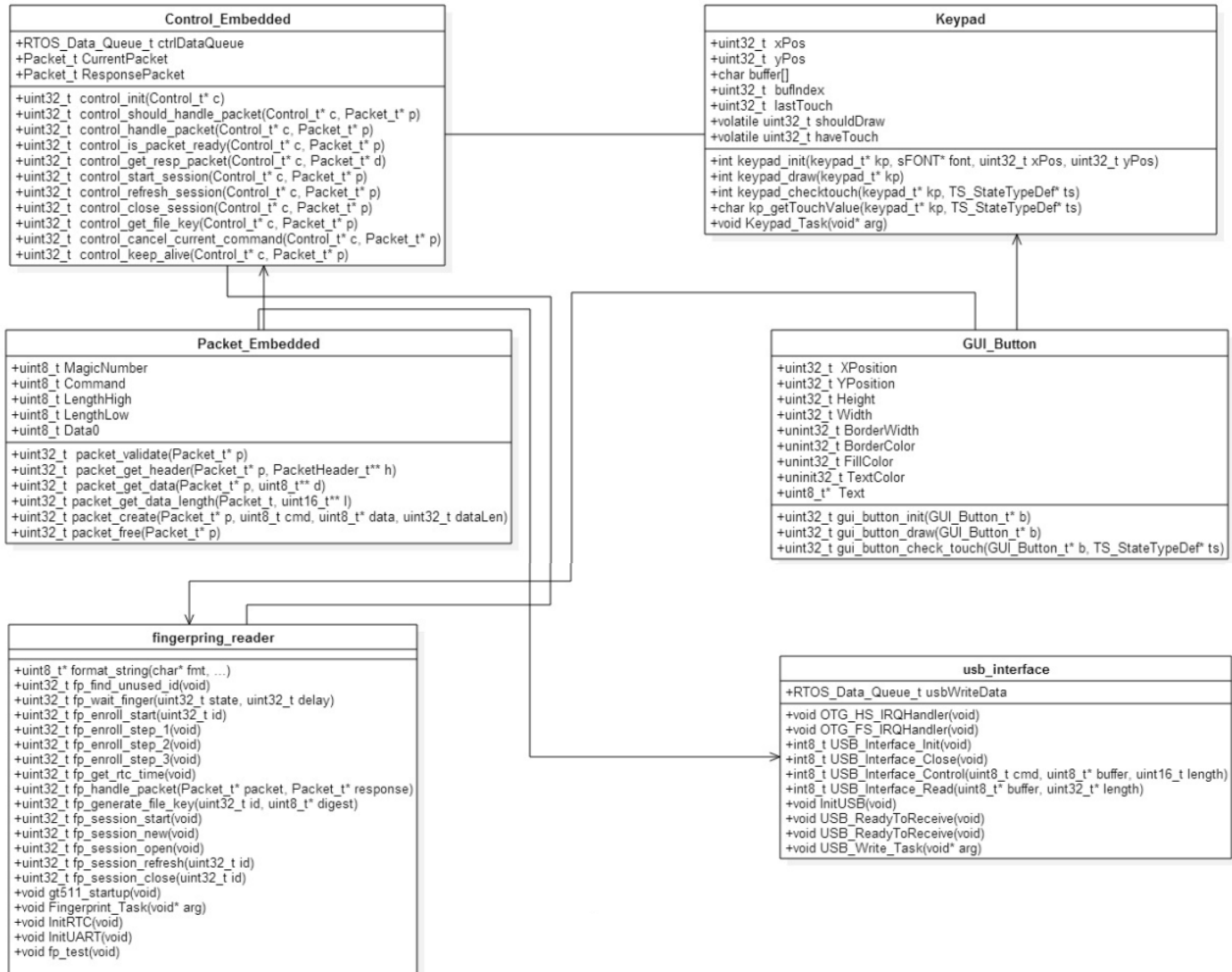
-  Crypto++

-  OpenSSL, OpenAes, CyaSSL

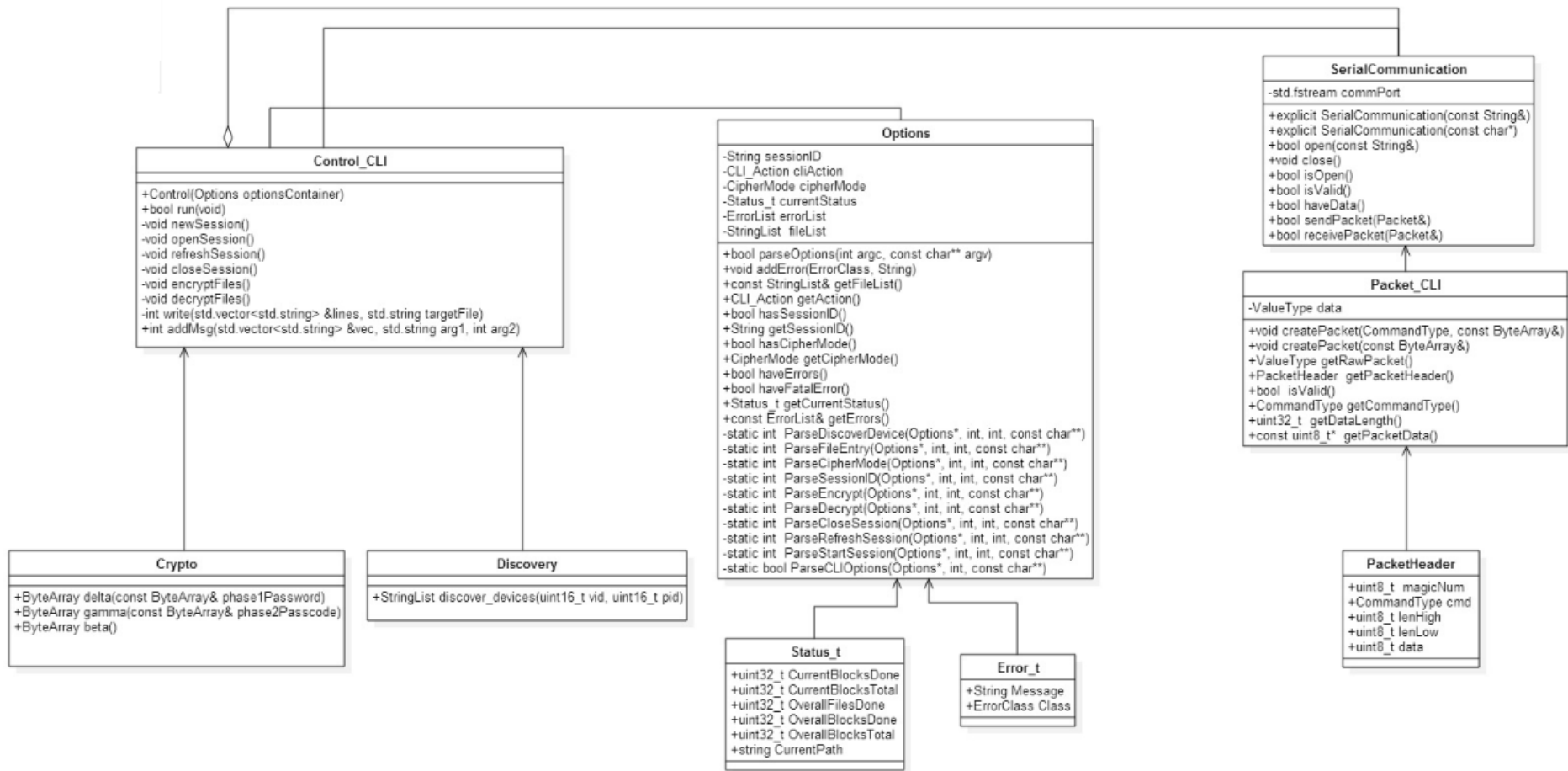
# Design: Overall



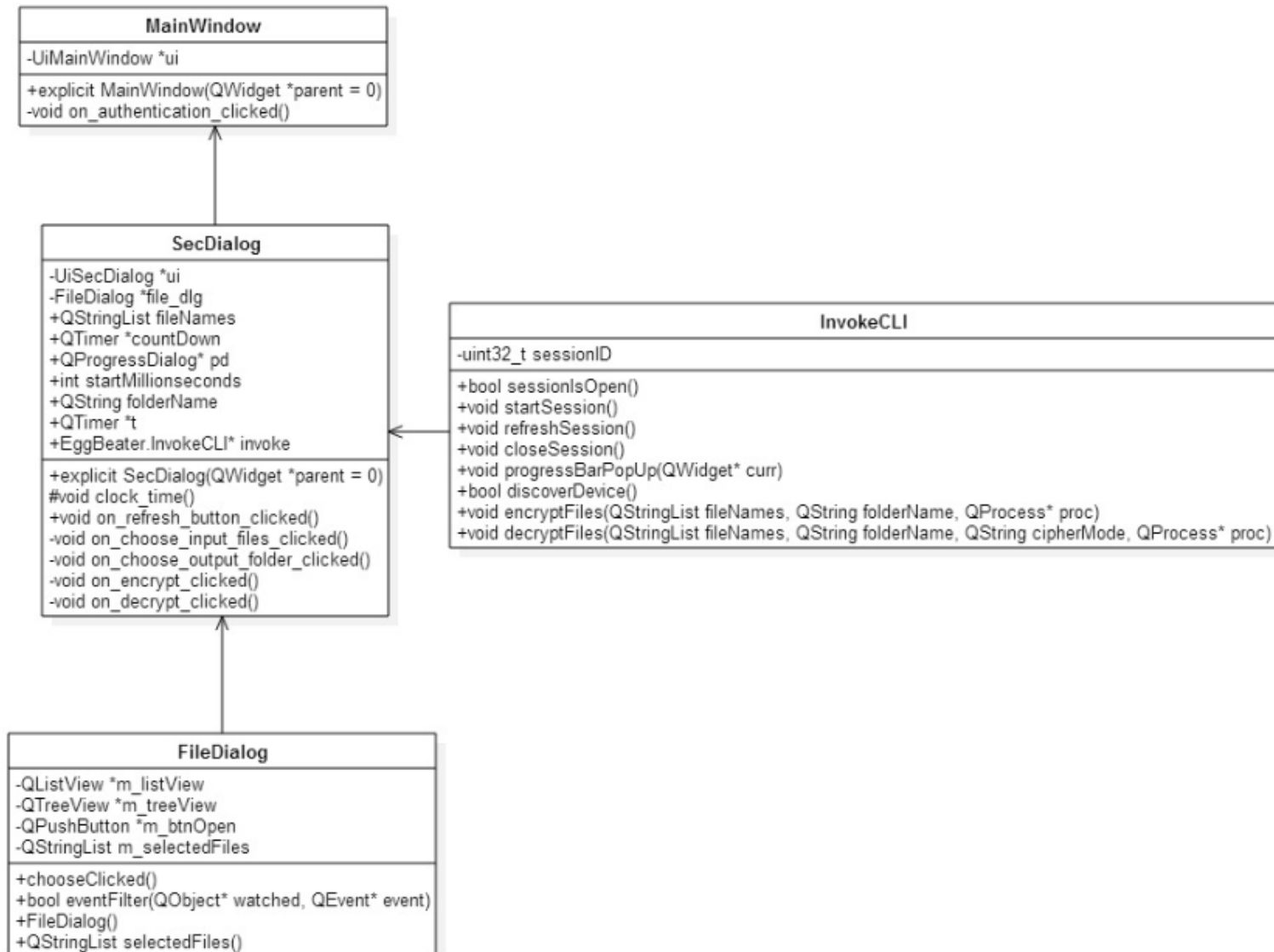
# Design: Embedded



# Design: Command line

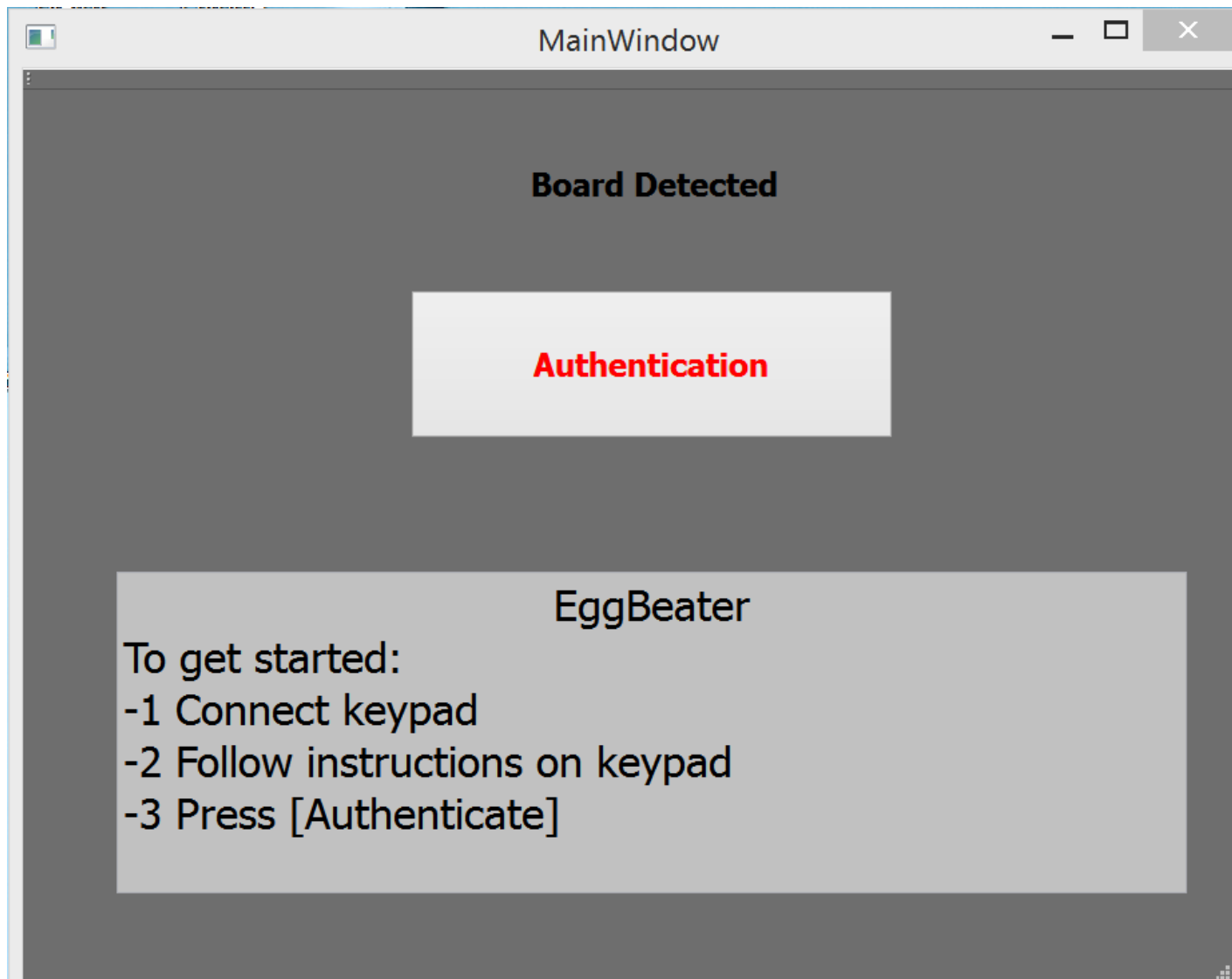


# Design: GUI





# Final GUI Mockup



# Final GUI Mockup(cont.)

Dialog

Time untill lockout: 00 : 09 : 29

Refresh

Encrypt

Decrypt

Pending Inputs:

24%

Pending Outputs:

24%

Input File(s) or Folder(s):  
MAX 10 Files

Destination Folder:

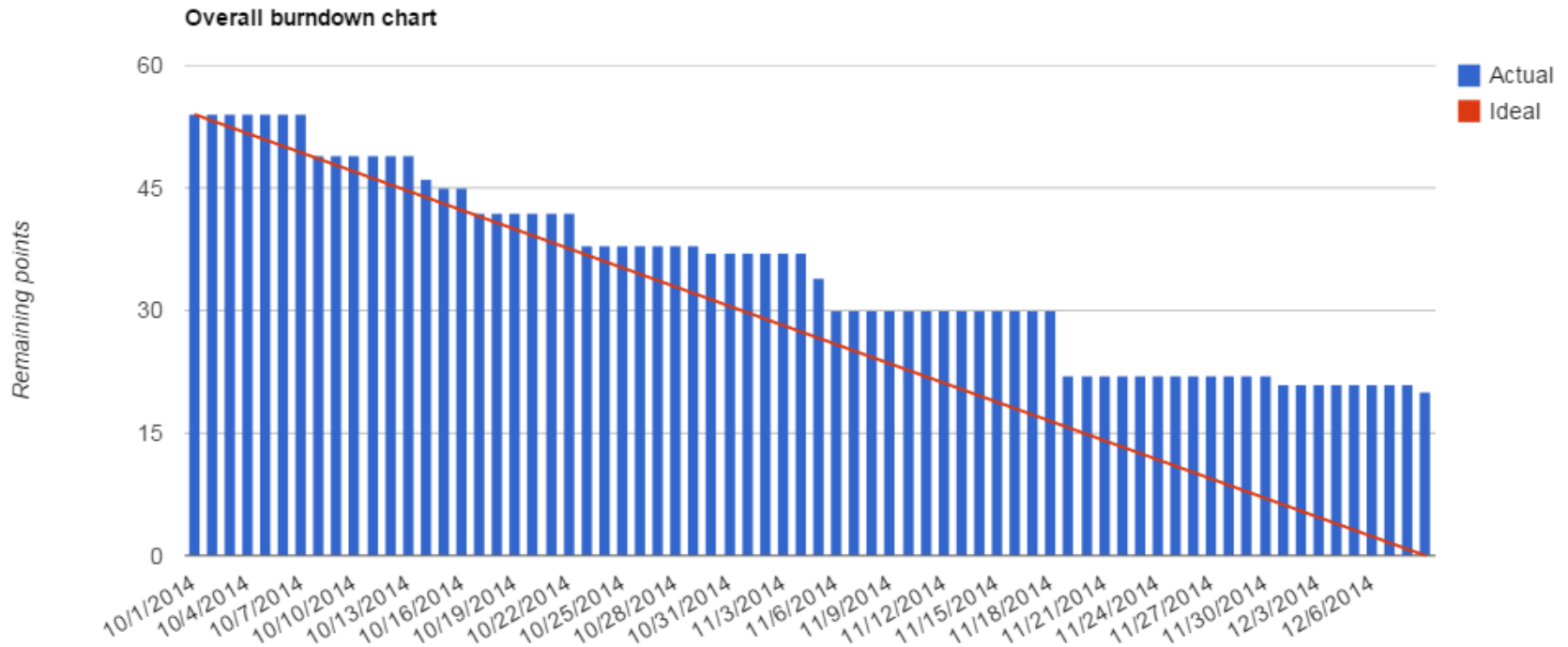
File Name

Folder Name

Select

Select

# Top-Level Burndown



# Testing

- Unit testing
  - Crypto
  - Command Line
- Acceptance testing
  - Hardware interactions
  - Device discovery

# Test Coverage

- ❏ Test Coverage
  - ❏ Example -> Encryption Modes
  - ❏ 37 Unit Tests & 3 Acceptance Tests
  - ❏ Qt

# Test Coverage: Example

```
bob@Lappy2 /cygdrive/c/Stuff/CSCI 430/eggbeater/cli
$ tests/CryptoPP_tests.crypto.elf
[=====] Running 13 tests from 1 test case.
[-----] Global test environment set-up.
[-----] 13 tests from CryptoFixture
[ RUN    ] CryptoFixture.encrypt_cfb_1
encrypt #sink bytes: 16
[ RUN    OK ] CryptoFixture.encrypt_cfb_1 (1 ms)
[ RUN    ] CryptoFixture.encrypt_cfb_2
encrypt #sink bytes: 16
[ RUN    OK ] CryptoFixture.encrypt_cfb_2 (0 ms)
[ RUN    ] CryptoFixture.encrypt_cfb_3
encrypt #sink bytes: 16
[ RUN    OK ] CryptoFixture.encrypt_cfb_3 (0 ms)
[ RUN    ] CryptoFixture.encrypt_cfb_4
encrypt #sink bytes: 16
[ RUN    OK ] CryptoFixture.encrypt_cfb_4 (0 ms)
[ RUN    ] CryptoFixture.encrypt_ofb_1
encrypt #sink bytes: 16
[ RUN    OK ] CryptoFixture.encrypt_ofb_1 (0 ms)
[ RUN    ] CryptoFixture.encrypt_ofb_2
encrypt #sink bytes: 16
[ RUN    OK ] CryptoFixture.encrypt_ofb_2 (0 ms)
[ RUN    ] CryptoFixture.encrypt_ofb_3
encrypt #sink bytes: 16
[ RUN    OK ] CryptoFixture.encrypt_ofb_3 (0 ms)
[ RUN    ] CryptoFixture.encrypt_ofb_4
encrypt #sink bytes: 16
[ RUN    OK ] CryptoFixture.encrypt_ofb_4 (0 ms)
[ RUN    ] CryptoFixture.encrypt_gcm_1
encrypt #sink bytes: 32
[ RUN    OK ] CryptoFixture.encrypt_gcm_1 (0 ms)
[ RUN    ] CryptoFixture.encrypt_gcm_2
encrypt #sink bytes: 32
[ RUN    OK ] CryptoFixture.encrypt_gcm_2 (0 ms)
[ RUN    ] CryptoFixture.encrypt_gcm_3
encrypt #sink bytes: 32
[ RUN    OK ] CryptoFixture.encrypt_gcm_3 (0 ms)
[ RUN    ] CryptoFixture.encrypt_gcm_4
encrypt #sink bytes: 32
[ RUN    OK ] CryptoFixture.encrypt_gcm_4 (0 ms)
[ RUN    ] CryptoFixture.encrypt_gcm_5
encrypt #sink bytes: 32
[ RUN    OK ] CryptoFixture.encrypt_gcm_5 (0 ms)
[-----] 13 tests from CryptoFixture (2 ms total)

[-----] Global test environment tear-down
[=====] 13 tests from 1 test case ran. (2 ms total)
[ PASSED ] 13 tests.
```

# Metrics

- Cyclomatic Complexity
  - Embedded
    - Average Complexity = 3.44
    - Problem Methods
  - Command Line Interface
    - Average = 2.44

# Maintainability

- Split design between three domains
  - Embedded
  - Core tool (command line)
  - GUI wrapper of core tool



# Extensibility

- Software
  - Encryption Schemes
  - GUI options
  - Mac Compatibility
  - Linux Compatibility
    - Qt works!
- Hardware
  - Microcontroller
  - Keypad

# Presented By

Robert Beat  
Sterling Miller  
Sam Adams  
Yuki Ishikawa  
Taha Ainaddin  
Sam Whitsett  
Andrew Barton