Dissertation Outline

Intro

```
motivation/problem
hypothesis/aims
    primary/secondary/tertiary aims
    mention johns hopkins medical records achievement
    why can't this work for us
what needs altered or expanded upon
contribution
    policy produced
  language definition
    software produced
  server setup
    how these meet the aims
outline/reading guide
```

Background

```
access control
encryption
    classical (1-to-1)
    modern (1-to-many)
public key infrastructure
resource server
```

openabe library
pyopenabe bindings

Analysis/Requirements

security considerations
why resources need secured
why ABE is best for this
what the ABE implementation must be able to do
deployment considerations/conditions
assumed physical security of MK server
issuing of user keys

enrolment requirements

case studies

Design

design of the policy language

how does it meet the case studies

formal definition

user key design

SSO login to provide attributes

signed manually by 'cold' server - offline

processed by admin staff

deployment scenario

architecture diagrams

how servers will communicate

how user will interact

tool for building policies

filename searching

Implementation

discuss openabe library toolset

translating policy language to openabe compliant

use of bindings

python flask to build servers

use of flask to build web servers

provide simple GUIs

wraps the pyopenabe bindings for encryption/decryption

python client server

local only

insecure by design (stores plaintext user key in local DB)

mongoDB for storage

file metadata storage on res server

provides basic search functionality

user data (incl. key) on local client

fuzzy finder for filename searching

Evaluation

security evaluation

risk assessment
assets
risks
measures
analysis
successfully achieved
encrypt/decrypt resources
issue user keys properly (JSON request to MK server)
store on a resource server
retrieve from server by search
client tool to handle all above by GUI
store issued attributes and types globally as a record
local, proof-of-concept authentication system
extraction from .cpabe, .key files
extract policy from .cpabe files
extract user attributes from .key files
failed to achieve
CLI tool for encrypt/decrypt with pyopenabe bindings
full compatibility with openabe library
metadata header for files encrypted with toolset

Conclusion

summarise
confirm solution to original problem
future work
problems (compatibility with openabe lib)
extraction by regex issues
deployment