

Capstone Progress Report

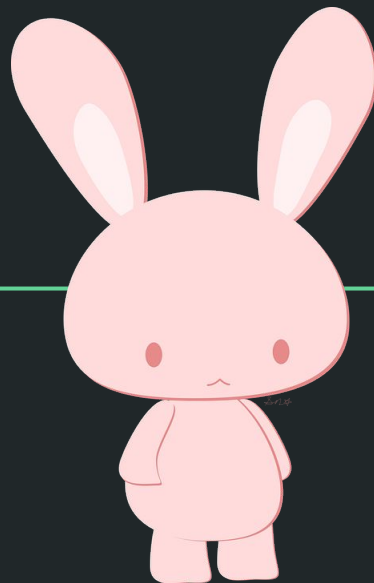
Winter 2017 Midterm

Andrew Ekstedt

Scott Merrill

Scott Russell

The Secret Bunny Team: Privacy Preserving Cloud & Email Encryption



Project overview

Privacy Preserving Cloud & Email Encryption

The "Privacy Preserving Cloud, Email and Password Manager" Capstone project is a research-oriented project that aims to find a way to implement the DSSE scheme proposed by David Cash.



CC0 Creative Commons
No attribution required

Last term (recap)

Current Progress

What we're working on currently

- DSSE Algorithm
- POP3 Email Integration
- Tokenization
- Update/Delete



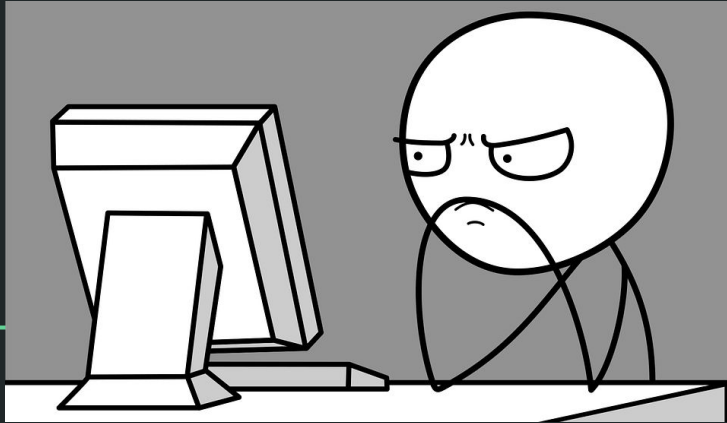
Future plans

Future Project Implementations

- Cloud Integration
- Benchmarking
- Parallelization/Optimization



Retrospective



Problems

- mysterious linker errors with mailio and boost
- getting gmail to send repeated emails for testing
- meeting problems
 - TA MIA
 - Attila sick week 3
 - Team communication/meetings

What went well?

- Our code compiles :)
- Successful implementation of Libraries
- Discussion Progress with Client/TA

Plans for 2nd half of Term

- Our client has sent us in a small change of focus
- Our main focus is getting the three levels of the core DSSE implemented.
 - The idea behind this, is the core DSSE is the more challenging part and the most important for research purposes.
 - Optimization and Implementation of Cloud/Server will come after, as they are not the main reason for this project.

Live Demos

POP3 Email Demo

- Mailio Library
- Email Setup
- Script Examples for pulling emails.

Client/Server demo

- Live demo of client/server interaction
- Code walk-through

Planning for Engineering Expo

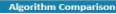


Andrew Ekstedt, Scott Merrill, Scott Russell
Sponsored by: Attila Yavuz with Thang Hoang

Andrew Ekstedt, Scott Merrill, Scott Russell
Sponsored by: Attila Yavuz with Thang Hoang

Storage service offered by cloud providers bring vast benefits to human society. However, this service also brings privacy concerns to the users.

Thus, there is a need to develop a new cryptographic primitive that allows the user to query data outsourced to the cloud, while preserving its privacy.



This section will also discuss how our benchmarks align to the motivation behind the project. Being a focus on the research and comparison of different algorithms.



Cloud Storage: We are using Amazon S3 as our Cloud Storage Database. This Cloud Storage database is encrypted using the scheme explained by David Cash. This is also implemented as a Storage Only Server.

Benchmarks

1. **Conclusion:** A Java Implementation of the Cash-DSSE Algorithm. This is primarily used as a comparison between the same algorithm, but different languages.

1. Round-Trip Delay: Testing for RTD takes are perform on a slow (WIFI)

Conclusions

The conclusion should give a clear result from the research and benchmarking. Therefore we should determine, from our testing and research, which of the three algorithms we compared had the best overall speed, security, and usability based on benchmarking.

Primary References

- [illegible]

- What we plan to do to display our code at expo
- Things we may need
- Anything we still need to work out:
 - Example: Is there going to be a live display?

Conclusion

Image Sources

1. <https://pixabay.com/en/analytics-information-innovation-3088958/>
2. <https://pixabay.com/en/keyboard-key-success-online-621830/>
3. <https://pixabay.com/en/cloud-computing-computers-2116773/>
4. <https://pixabay.com/en/rabbit-characters-pink-cute-animal-2403904/>
5. <https://pixabay.com/en/whiteboard-white-board-blank-303145/>

All images are licensed under Creative Commons CC0