CS Capstone Progress Report

December 3, 2017

Privacy Preserving Cloud, Email, and Password Systems

Prepared for

OSU

Attila Yavuz ______________________ Signature ________ Date

Prepared by

Group 38

The Secret Bunny Team

Andrew Ekstedt ______________________ Signature ________ Date

Scott Merrill ______________________ Signature ________ Date

Scott Russell ______________________ Signature ________ Date

Abstract

This document provides a report of progress our team has made on our project this term. We outline a week by week summary of research and implementation of our project and capstone documents. We provide a retrospective of our progress throughout Fall term. This document provides us with point of reference for work done this term and a guideline for how to improve workflow in future terms.

CONTENTS

1 Project Purpose and Goals

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. This implementation will be executed through command line prompts and hosted on OSUs engineering servers. A user can use this system with a client-server model to perform actions, such as search or update, on a "cloud-based" database. User interface is not considered a priority as this project is not intended to be used in any commercial capacity. There are five primary goals of this project. First the implementation of David Cash's DSSE Algorithm. The following four aspects can be done in parallel: parallelization, optimization, cloud integration, and email integration. Finally benchmarking will be done during the final stages and after implementation of the previous items.

2 Current Status

Fall term was primarily used as the research and planning phase of our project. With all the capstone related documents we now have a clear understanding of what specifically we are implementing as well as technologies that are optimized for our specific implementation. We've spent this term researching searchable encryption, understanding both Bit Matrix and David Cash's algorithm and discussing points of interest with our client Attila Yavuz as well as his graduate student Thang Hoang. As such we do not have any code to demonstrate in this report but we are eager for winter term where the bulk of our implementation will take place. Being a research focused project we understand that because of this research we now have a better direction for our implementation than if we jumped right into programming.

3 Problems that impeded progress, with solutions

As we begin implementation of our capstone project it is important to be able to look back at progress throughout the term. If we can understand what went well and poorly we can use that information to be able to have a more cohesive plan for the following terms.

3.1 Time Conflicts

One of the primary difficulties we had this term was correlating schedules in order to meet up with group members, client, and TA. With Scott Merrill commuting from Eugene and Scott Russell having ROTC responsibilities in addition to everyone having a job on the side it was difficult for us to find times that work well with all of our schedules. For this reason we plan to figure out meetings and scheduling for winter and spring term in advance in order to prioritize time for Capstone.

3.2 Research/Implementation Project

Another source of much consternation was trying to fit our research-focused project into the strictures of capstone. As the term went on, our documents deviated more and more from the template for normal capstone projects, so we were often confused about what exactly to write, and whether we were

3.3 Project Scope

During the first couple weeks of learning about the project, we became worried that the scope was going to be too large to complete in the time available to us. It seemed like our client was perhaps treating the project as just another graduate research project, without accounting for the months of planning and documentation required by capstone. We conveyed these worries to the client and to the instructors and were ultimately able to get the scope narrowed to a more reasonably-sized project.

3.4 Getting Sick

Planning for unexpected events. Team members getting sick caused a few inconveniences with the inability to meet in person to discuss capstone documents. Although this is mostly unavoidable we can prepare extra time before deadlines to account for unexpected delays that may occur.

4 Week by Week Summary

4.1 Week 1

Week one of Capstone was focused on researching and selecting a top five list of projects that aligned with our interests. In addition we also used this week to set up our OneNote for weekly Blog Posts. Finally we submitted a fake resume to understand proper formatting and content in a professional environment.

4.2 Week 2

During week two we were assigned our project. We meet with our team for the first time to share communication info. We had a conversation with out client, Attila, to discuss how our more research-focused project fits into the capstone design along with his expectations for implementation. We set up a Signal group to communicate securely and initialized a Github for work. Attila provided us with papers and slides to review searchable encryption. We also started on the Problem Statement Document. A lot of this week's work was focused on communicating and understanding the specifics of the project with our client.

4.3 Week 3

During week 3 our team had a meeting with Thang, the graduate student of our client Attila, to give a high-level overview of our project. Specifically we focused on David Cash's Algorithm. Our client has three primary projects in mind, which to us seemed outside the range of what we could implement in the time frame provided. We planned to meet with Attila next week to discuss our concerns with work load for capstone. For capstone this week we worked on the requirements document, which serves as an outline for how we will be graded at the end of the term. More information about balancing a research and implementation project will be discussed in future weeks.

4.4 Week 4

Most of week 4 was spent working on the problem statement. Meetings with McGrath and Attila proved to reduce the initial scope that Attila had in mind to correlate to the capstone structure. Originally Attila envisioned a larger scale project but accounting for the time spent on capstone specific items he realized that the scope was too large for our knowledge and time constraints. Work over this week included looking over Thang's Bit Matrix implementation of DSSE, IM-DSSE, which will serve as a starting reference point going forward with the implementation next term. We also met with our Capstone TA, Andrew Emmott, for the first time and discussed his expectations from us.

4.5 Week 5

We met with our client to discuss the project requirements. McGrath was able to talk to Attila and explain the capstone project schedule, which relieved some of the pressure we were feeling about the scope of the project being too large.

We continued to look at IM-DSSE to get a feel for the project. The first requirement of project is to implement a similar proof-of-concept program, so seeing how IM-DSSE worked was helpful. All members of the team were able to get it to compile and run.

A team member wrote a prototype of David Cash's SSE in Python in order to get a better feel for how it worked.

Progress was hindered slightly by one of the team members getting sick and being out of commission for the latter half of the week.

4.6 Week 6

We continued to work on the requirements document. Our client was at a conference all week so they were unable to give feedback on the requirements document. We submitted our final draft anyway and requested extra time for client approval, which was granted.

We started thinking about how to split up the project components for the tech review. We decided loosely that I would tackle optimizations to the DSSE; SR would tackle email integration; and SM would tackle cloud integration, although this ended up changing later as we got a more clear understanding of the project.

We attended the class session on research-focused projects, which was helpful for understanding how our project fit into capstone, and how we would be documenting; the gist was that a project, we would be designing a roadmap for the problem we were researching and how we were going to tackle it.

4.7 Week 7

Our client returned from their travel and gave us feedback on the requirements doc. Aside from that, we mainly worked on planning the technology review this week. We had a little trouble coming up with enough tech review topics, but after talking to the instructors we were able to identify more. We also did a literature review as part of our tech review, because our project is a research project.

4.8 Week 8

This week our meeting with Tang addressed question we had pertaining to the Tech Review and how to break down the project into 9 meaningful components. During class we did a peer review of a rough draft of the tech review and covered components aspects, such as cost, that were not good rationale when making our choices.

4.9 Week 9

After meeting with our TA we were able to finalize our Tech review document and submit it. Our next assignment, the Design document was assigned. This assignment was for us to go into detail about the specifics of what we were going to be implementing as well as what we expected to discover from our research. Thanksgiving was also this week which cause a lull in progress as everyone too few days off to visit family and celebrate the holiday.

4.10 Week 10

This week we finished up our design document and began looking over our next assignment, the Progress report. The Progress report would consist of two parts: 1) a written account of the term including what went well and challenges we faced. 2) a slide show presentation with voice overlay discussion the progress of the term based heavily on what we wrote. In class we discussed the specific for that was expected in the recording, including advice on common mistakes to avoid. We also had our final meeting of the term with our client. In this meeting we talked about the progress report and what we plan to do moving forward.

5 Retrospective

What Went Well?	What Didn't Go Well?	What Can We Change?
Discussing capstone requirements with client to make the Project both Challenging and Attainable.	Finding time for everyone to meet with drastically different schedules.	Being able to schedule in advance to plan around time conflicts.
Group members work well together with a similar focus in security which matches the project as well as being flexible with schedules	Trying to fit the project to match capstone requirements (which do not normally fit a research based project)	Discussed goals with Attila and Kevin and were able to modify the Requirements and Design documents to match the goals of our project.
Turned in everything on time	It wasn't always clear how to adapt the assignments to a research-focused project	Ask for help and clarification earlier
	Team member had ongoing car trouble	Win the lottery, buy better cars
	Team member got sick for a week in the middle of the term	