CS CAPSTONE PROBLEM STATEMENT

OCTOBER 19, 2017

PRIVACY PRESERVING CLOUD, EMAIL, AND PASSWORD SYSTEMS

PREPARED FOR

OSU

ATTILA YAVUZ _____ *Signature* _____ *Date*

PREPARED BY

GROUP 38

ANDREW EKSTEDT _____ *Signature* _____ *Date*

SCOTT MERRILL _____ *Signature* _____ *Date*

SCOTT RUSSELL _____ *Signature* _____ *Date*

Abstract

We want to be able to store private data on the cloud in such a way that the provider cannot decrypt it, yet we can still perform keyword searches efficiently. Our project will be to implement and build on algorithms developed by Attila Yavuz and David Cash which could potentially solve this problem. We will demonstrate practical searchable encryption of documents, email, and possibly passwords.

Contents

1 Motivation

In today's technological world privacy is of key importance. Faced with the growing public panic over mass surveillance, companies have caught onto the significance of security and are creating products with strong encryption built in. Web browser makers like Chrome and Mozilla are pushing for a secure-by-default world where every website has an SSL certificate, marking those without as untrusted. Apple is positioning themselves as a privacy-conscious company by building strong encryption features into recent iPhone models. Billions of users are flocking to secure chat apps like Signal and WhatsApp.

Despite these advances, there are many areas where security is lacking. There is currently limited research into encrypted emails. You can use GPG to encrypt messages, but then you lose the ability to quickly search your messages. This problem can be addressed by giving your email provider a copy of your decryption keys, but now they have the ability to read all your email, defeating the purpose of encryption. A similar problem exists for cloud storage systems: Google Drive will transparently encrypt your files for you, but Google necessarily hangs onto a copy of the encryption keys, which means that Google has the ability to decrypt your files any time they want.

There has been some research into searchable encryption, but no open-source implementations of the algorithms that have been developed. The need for a fast and efficient open-source implementation of dynamic searchable encryption is the basis for our research.

2 Goals

Our primary goal is to demonstrate a practical, open-source implementation of searchable encryption on a cloud provider.

Attila's research group has previously developed and implemented an algorithm for searchable encryption [1], however there is another scheme which was developed by David Cash which is asymtotically more efficient [2] in some areas; for example, the size of the encrypted index is smaller. The source code for David Cash's implementation is not publicly available, so our first project will be to build an open-source implementation of David Cash's scheme, and to demonstrate that it works by building a client-server system that runs on Amazon EC2.

The second project is to apply our searchable encryption program to the problem of encrypted email. This will probably involve writing a daemon which downloads messages from an email provider like gmail and adds them to an encrypted database. Presumably we would want to throw some email-specific UI and search functionality on top. This part of the project is TBD and we expect to learn more about what is possible after we complete the first part of the project, and as we start working on this part.

A third project is to implement a password manager using ORAM (oblivious RAM), which is a random-access data structure that hides memory access patterns from observers. Current searchable encryption schemes leak some access patterns whenever you search, so a password manager service implemented with such a scheme could learn for example that you always access a site at a certain time of day. By obscuring the access patterns with ORAM, we can prevent the server from learning this information. This is a streach goal of the project and will be persued if we have time after tackling the first two goals of this project. As it is not directly related to David Cash's scheme.

3 Metrics

There are two metrics, equally important: correctness and performance.

The first metric is correctess. The software should return the correct set of documents when searching for a keyword. It should be able to dynamically add and delete files from the search index and return correct search results using the modified index.

The second metric is performance. For the secure cloud, we want to aim for under a hundred milliseconds to search for a file. Attila has measured the previous implementation to be able to perform a search in around 10 milliseconds or less, even with an index containing millions of files, so this should be doable. Performance for the email database is TBD. The password manager (if we get to it) will be less performant due to the overheads of ORAM, but we want to aim for 100 milliseconds.

REFERENCES

[1] A. A. Yavuz and J. Guajardo, "Dynamic searchable symmetric encryption with minimal leakage and efficient updates on commodity hardware," Selected Areas in Cryptography (SAC) 2015, Sackville, New Brunswick, Canada, August 2015, http://web.engr.oregonstate.edu/~yavuza/Yavuz_DSSE_SAC2015.pdf.

[2] D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rou, and M. Steiner, "Dynamic searchable encryption in very-large databases: Data structures and implementation," Cryptology ePrint Archive, Report 2014/853, 2014, http://eprint.iacr.org/2014/853.