Sean Evans
Emma Romstadt
Kevin Geisler
CS 6058
Data / Security and Privacy
Spring 2018
Project 3

Project 3: Searchable Encryption

Description

The searchable encryption tool has four major functions, including key generation, encryption, token generation, and search.

The keygen function outputs a random sequence of 256 bits in binary format to two output files, one key for the AES encryption and decryption, and one key for the Psuedorandom Function (PRF).

The encryption function uses AES-256 CBC mode encryption to encrypt file data, and builds a searchable index. The searchable index is built by tokenizing the input plaintext data files, then applying the PRF on the tokens.

The token generation function takes an input token, applies the PRF, and appends the resulting data to a file.

The search function iterates over PRF tokens in the token file, uses each PRF token to search the index for encrypted files contain the token, and then decrypts and outputs the matching files.

Implementation Details

The searchable encryption tool was implemented using C++, and uses the C++ Standard Library and Standard Template Library (STL), OpenSSL, and Boost Libraries.

The Boost filesystem library was used to build file paths, check file types, and iterate over files within a directory in an OS agnostic manner.

The OpenSSL library was used to perform AES-256 CBC mode encryption and decryption, and to perform AES-256 ECB mode encryption for the PRF.

The key generation functionality was implemented using the C++ Standard Library's random number generator device and uniform integer distribution filter to generate a sequence of random bytes.

The build system for the tool was implemented using CMake.

The tool was built and tested on a Windows 10 x64 system in the Cygwin x64 environment.

Running Time Of Searchable Encryption Index Creation and Search

	INDEX GENERATION	INDEX SEARCH
ITERATIONS	100	100
MIN RUN TIME	17329800 ns	705500 ns
MAX RUN TIME	36159200 ns	841100 ns
MEAN RUN TIME	19307636 ns	729562 ns
MEDIAN RUN TIME	18438750 ns	721100 ns