CryptDB Final Project - Eric Marriott

For my final project, I chose CryptDB. CryptDB is a novel method of securing the data in a DBMS (database management system), and solves many problems. The first of these is information leakage from active connections, which hackers that gain access to the network between the application server and the DBMS server, or the servers themselves, can collect. The second problem solved by CryptDB is passive monitoring by somebody with administrative privileges at the DBMS server, who can make unrestricted queries, or just view the plaintext of a database file. CryptDB solves these problems by acting as a proxy server between the user and DBMS server (or between the application and DBMS server), which the user authenticates with by password, which decrypts a keychain. The proxy uses the unencrypted keychain to encrypt queries sent by the user, processing the user-defined columns into different ‘onion’ columns, which are so named because of their layered encryption schemes. Each layer of encryption has its own purpose, and all are homomorphic in some sense (except for the top layer of most onion layers, RND, which is just a block-cipher without homomorphic properties), meaning that they can be used to perform certain operations (such as equality or summation) on encrypted data without decrypting the data. The proxy keeps track of which layers are on what column, and what columns are which, and translates the user’s queries into SQL queries on the encrypted data on the DBMS, keeping the DBMS server from ever seeing decrypted data. This method also guarantees that when a user is logged out, their keychain is encrypted, so not even the proxy can handle the user’s data, meaning absolutely no data leakage. CryptDB is not without its shortcomings (lack of advanced SQL functions, and being slow compared to vanilla DBMSes), however - but the fact that it sits on top of an unmodified DBMS which can still be used for traditional purposes is another major plus.

This project reports on the inner workings, the types of encryption and ‘onions’, and various issues, as well as goes into how to compile, write queries, and various ways to process encrypted data in the presentation. The report goes over the installation and running of the servers in more detail, with instructions on how to run the scripts and the code, as well as also going into some detail about the working of the CryptDB software. This project also goes over a basic way to interface Java programs with CryptDB.

Please note that I do not own any Microsoft software, as that is a bit out of my budget - so the Powerpoint files in the file are exported from Google Drive, making them look kind of funky. The included PDF files look fine, however. The scripts directory contains all the code and data, of which the details for running is contained in the report. You will need an Ubuntu 12.04 or 13.04 computer or virtual machine to run CryptDB and the scripts; the requirements are gone into more in depth in the report.

Link to YouTube presentations
Long -
Part 1/2: https://www.youtube.com/watch?v=I40xRtBe87g
Part 2/2: https://www.youtube.com/watch?v=K4AauL8xx0A
“Short” (6 minutes, 38 seconds) -
Part 1/1: https://www.youtube.com/watch?v=DdF86x8H8Vc