Andrew Zurn

Reading 9

Summarized Article: cacm.acm.org/magazines/2012/9/154574-cryptdb-processing-queries-on-an-encrypted-database/fulltext

Other Article: www.reuters.com/assets/print?aid=USBRE99J02u20131020

Data security and privacy has been a large and important aspect within the computing industry, especially considering the most recent leaks from Adobe and always in the new Oracle exploits on Java applications. In his article, Raluca Ada Popa, “CryptDB: Processing Queries on an Encrypted Database”, Popa describes how large of a problem security is. He states,

Theft of private information is a significant problem for online applications. For example, a recent investigation found that at least eight million people’s medical records were stolen as a result of data breaches between 2009 and 2001, and in a recent attack on the Sony Playstation Network, attackers apparently gained access to about 77 million personal user profiles, some of which included credit card information.

As such, Popa and his team of researchers introduce and analyze a new system, called CryptDB, which massively improves the security of many databases that many online applications use.

The essential features that CryptDB provides is that it can run on any standard SQL DBMS, but that it can query over encrypted data, rather than decrypting it, querying, re-encrypting the data, and sending it to the client. Popa states that “CryptDB is the first practical system that can execute a wide range of SQL queries over encrypted data. The key insight that makes our approach practical is that most SQL queries use a small set of well-defined operators, each of which we are able to support efficiently over encrypted data.” He goes onto say that “CryptDB requires no changes to the internals of the DBMS server, and should work with most standard SQL DBMSes.” For CryptDB to do all of this, Popa points out four key step that CryptDB takes in order to provide this security, which actually are a fairly standard set of procedures no out of the normal for security matters, but are powerful enough to insure that data remains secure.

Overall, Popa’s article was quiet fascinating, especially after learning from my CS331 class about the processes a DBMS takes in order to query specific data. Knowing that it would be fairly easy to implement this might just prove to be advantageous to many online applications, and thus we could possibly see this system being implemented on a large scale in the coming years. In short, CryptDB seems to be a stunning solution to a very real world problem, and would maintain the current relational models, and allow for an easy implementation onto already used DBMSes.