Light database encryption design utilizing multicore processors for mobile devices

ABSTRACT

The confidentiality of data stored in embedded and handheld devices has become an urgent necessity more than ever before. Encryption of sensitive data is a well-known technique to preserve their confidentiality, however it comes with certain costs that can heavily impact the device processing resources. Utilizing multicore processors, which are equipped with current embedded devices, has brought a new era to enhance data confidentiality while maintaining suitable device performance. Encrypting the complete storage area, also known as Full Disk Encryption (FDE) can still be challenging, especially with newly emerging massive storage systems. Alternatively, since the most user sensitive data are residing inside persisting databases, it will be more efficient to focus on securing SQLite databases, through encryption, where SQLite is the most common RDBMS in handheld and embedded systems. This paper addresses the problem of ensuring data protection in embedded and mobile devices while maintaining suitable device performance by mitigating the impact of encryption. We presented here a proposed design for a parallel database encryption system, called SQLite-XTS. The proposed system encrypts data stored in databases transparently on-the-fly without the need for any user intervention. To maintain a proper device performance, the system takes advantage of the commodity multicore processors available with most embedded and mobile devices.

Keyword: Storage security; Embedded devices; SQLite RDBMS; Performance; Multicore CPU; XTS encryption