THE UNIVERSITY OF CHICAGO

Strongbox: Fast Secure Storage for Mobile Devices

Bernard Dickens, Ariel Feldman, Haryadi Gunawi, Henry Hoffmann

University of Chicago

Abstract

Full disk encryption (FDE) is especially important for mobile devices because they both contain large amounts of sensitive data and are easily lost or stolen. Yet, the conventional approach to FDE, AES in XTS mode, is 3–5x slower than unencrypted storage. Authenticated encryption based on stream ciphers like ChaCha20 is already used as a faster alternative to AES in other contexts, such as HTTPS, but the conventional wisdom is that stream ciphers are a unsuitable for FDE. Used naively in disk encryption, stream ciphers are vulnerable to many- time pad attacks and rollback attacks, and mitigating these attacks with on-disk metadata is generally believed to ruin performance.

In this paper, we argue that recent developments in mobile devices invalidate this assumption and make it possible to use fast stream ciphers for disk encryption. Modern mobile devices rely on NAND-flash storage with a Flash Translation Layer (FTL), which functions very similarly to a Log-structured File System (LFS), and include trusted hardware such as Trusted Execution Environments (TEEs) and secure storage areas. Leveraging these two trends, we propose StrongBox, a stream cipher-based FDE layer that is a drop-in replacement for dm- crypt, the standard Linux disk encryption module based on AES-XTS. StrongBox introduces a system design and on-disk data structures that exploit LFS's lack of overwrites to avoid costly rekeying and a counter stored in trusted hardware to implement rollback protection. We implement StrongBox on an ARM big.LITTLE mobile processor and test its performance under multiple popular production LFSes. We find that StrongBox generally improves read performance by over $1.6\times$ and write performance by over $1.2\times$ compared to dm-crypt while offering stronger integrity guarantees.

Motivation

Aliquam non lacus dolor, *a aliquam quam* [2]. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Nulla in nibh mauris. Donec vel ligula nisi, a lacinia arcu. Sed mi dui, malesuada vel consectetur et, egestas porta nisi. Sed eleifend pharetra dolor, et dapibus est vulputate eu. **Integer faucibus elementum felis vitae fringilla.** In hac habitasse platea dictumst. Duis tristique rutrum nisl, nec vulputate elit porta ut. Donec sodales sollicitudin turpis sed convallis. Etiam mauris ligula, blandit adipiscing condimentum eu, dapibus pellentesque risus.

Aliquam auctor, metus id ultrices porta, risus enim cursus sapien, quis iaculis sapien tortor sed odio. Mauris ante orci, euismod vitae tincidunt eu, porta ut neque. Aenean sapien est, viverra vel lacinia nec, venenatis eu nulla. Maecenas ut nunc nibh, et tempus libero. Aenean vitae risus ante. Pellentesque condimentum dui. Etiam sagittis purus non tellus tempor volutpat. Donec et dui non massa tristique adipiscing.

Design and Implementation

1. Lorem ipsum dolor sit amet, consectetur.
2. Nullam at mi nisl. Vestibulum est purus, ultricies cursus volutpat sit amet, vestibulum eu.
3. Praesent tortor libero, vulputate quis elementum a, iaculis.
4. Phasellus a quam mauris, non varius mauris. Fusce tristique, enim tempor varius porta, elit purus commodo velit, pretium mattis ligula nisl nec ante.
5. Ut adipiscing accumsan sapien, sit amet pretium.
6. Estibulum est purus, ultricies cursus volutpat
7. Nullam at mi nisl. Vestibulum est purus, ultricies cursus volutpat sit amet, vestibulum eu.
8. Praesent tortor libero, vulputate quis elementum a, iaculis.

StrongBox vs Dm-crypt under F2FS

Fusce magna risus, molestie ut porttitor in, consectetur sed mi. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque consectetur blandit pellentesque. Sed odio justo, viverra nec porttitor vel, lacinia a nunc. Suspendisse pulvinar euismod arcu, sit amet accumsan enim fermentum quis. In id mauris ut dui feugiat egestas. Vestibulum ac turpis lacinia nisl commodo sagittis eget sit amet sapien.

Conclusion

- The conventional wisdom: securing data at rest requires one must pay the large performance overhead of encryption with the AES-XTS block cipher instead of using a stream cipher.
- The proliferation of NAND-flash FTL/LFS and secure hardware on modern/mobile devices overturn the conventional wisdom, making it practical to use a stream ciphers to secure data at rest.
- We propose StrongBox, a stream cipher-based FDE layer and drop-in replacement for dm-crypt. StrongBox exploits LFSs lack of overwrites and the availability of trusted hardware to overcome the limitations of stream ciphers.
- Our results show that under F2FS, StrongBox provides upwards of $2times$ improvement on read performance and $1.21times$ improvement on write performance over a standard dm-crypt configuration.

References

[1] A. B. Jones and J. M. Smith. Article Title. *Journal title*, 13(52):123–456, March 2013.

[2] J. M. Smith and A. B. Jones. *Book Title*. Publisher, 7th edition, 2012.

StrongBox source is available on GitHub @ `https://github.com/ananonrepo2/StrongBox`