ECFS:
An Enterprise-Class Cryptographic File System for Linux

U. S. Rawat, Jaypee University of Engineering & Technology, India

Shishir Kumar, Jaypee University of Engineering & Technology, India

ABSTRACT

Proposed is a secure and efficient approach for designing and implementing an enterprise-class cryptographic file system for Linux (ECFS) in kernel-space. It uses stackable file system interface to introduce a layer for encrypting files using symmetric keys, and public-key cryptography for user authentication and file sharing, like other existing enterprise-class cryptographic file systems. It differs itself from existing systems by including all public-key cryptographic operations and public-key infrastructure (PKI) support in kernel-space that protects it from attacks that may take place with a user-space PKI support. It has a narrower domain of trust than existing systems. It uses XTS mode of AES algorithm for file encryption for providing better protection and performance. It also uses kernel-keyring service for improving performance. It stores the cryptographic metadata in file's access control list (ACL) as extended attributes to ease the task of file sharing. A secure protocol has also been designed and implemented to guard against various possible attacks, when its files are accessed remotely over an untrusted network.

Keywords: *Cryptographic File System, Network File System (NFS), Private-Key Store (PKS), Public-Key Infrastructure (PKI), Stackable File System*

INTRODUCTION

Data security in modern computing systems is a cumbersome issue. Network connections and remote file system services, while convenient; often make it possible for an intruder to gain access to sensitive data by compromising only a single component of a large system. Because of the difficulty of protecting information in a reliable way, sensitive files are often not stored on networked computers. It leads to inconvenience in accessing files by authorized users and puts them out of the reach of useful system services such as backup. Hence, data protection system is vital in any organization where classified and confidential data need to be shared and secured simultaneously.

Cryptographic file system may be used for data security that does data encryption/decryption in secure, efficient and transparent manner for the user. Other issues such as key management, file sharing among multiple users, secure remote access, backups and data recovery must also be resolved for enterprise deployment.

DOI: 10.4018/jisp.2012040104

In this paper, the design and implementation of ECFS (an enterprise-class cryptographic file system) for Linux in kernel-space is proposed that takes in account all aforementioned issues. ECFS makes a crucial distinction between the kernel and user-space from security perspective. It incorporates an advanced key management scheme that excludes user-space processes which gains temporary root privileges from domain of trust.

The rest of this paper is organized as follows. The next section introduces popular cryptographic file systems and motivation to develop the proposed system. Subsequent sections explain overall ECFS architecture, key management scheme, various cryptographic operations and implementation details. Next, secure protocol for remote file access and its implementation details are described. Finally performance and security evaluation of proposed system is presented, along with conclusion and identified future work.

RELATED WORK AND MOTIVATION

Encryption services by cryptographic file systems can be placed in user-space, device layer level or kernel-space. Kernel-space systems are more efficient and secure than user-space systems. In device layer systems, single key is being used for encryption, so file sharing is not possible among multiple users.

CFS (Blaze, 1993) is the first cryptographic file system for Unix, implemented as a user-space NFS (network file system) server. Then, TCFS (Cattaneo et al., 2001) is implemented in kernel-space as modified NFS client, but it accesses two user-space servers: nfsd and xattrd. These prior realizations suffer from poor performance, because of context switches and data copies between user-space and kernel-space. They use common mount wide key that limits there use for multiuser scenarios. EncFS (http://www.arg0.net/encfs) is another cryptographic file system in user-space that does not require superuser access to mount it. It uses FUSE library (http://freecode.com/projects/fuse) to interact with kernel VFS (virtual file system). It also suffers from poor performance like other user-space cryptographic file systems.

dmCrypt (http://code.google.com/p/cryptsetup/wiki/DMCrypt), device mapper crypto target, is cryptographic file system for Linux at device layer level in kernel-space. Device mapper infrastructure in Linux kernel provides a generic way to create virtual layers of block devices. dmCrypt uses this to implement cryptographic operations using kernel Crypto API (Cooke & Bryson, 2003). The user specifies symmetric cipher, an encryption mode, a key and an initialization vector, and then creates a new block device in /dev using dmsetup utility. User then mounts filesystem on new block device created. Now all the writes to this device will be encrypted and reads decrypted. Using dmsetup utility is complicated, because the user has to remember all the parameters passed to the utility. The cryptsetup utility is created as a wrapper around dm-setup to make management tasks simpler as part of LUKS (Linux Unified Key Setup) project (http://code.google.com/p/cryptsetup). LUKS for dmCrypt is enhanced version of dmCrypt. It stores all necessary setup information in the partition header, enabling the user to transport or migrate his data seamlessly. dmCrypt does not support file sharing among multiple users as single key is used for cryptographic operations.

Cephus (Fu, 1999) is the first cryptographic file system which presents file sharing among multiple users using public-key cryptographic technique. It uses per-file symmetric keys for encryption and user-specific public private-key pairs for user authentication, which enable fine-grained sharing. It encrypts each file with a symmetric encryption key and that key is encrypted with the public-key of the users who have authorized access to the file.

Kernel-space cryptographic file systems like NCryptfs (Wright, 2003), eCryptfs (Halcrow, 2005), TransCryptDFS (Modi et al., 2010), uses stackable file system interface approach (Zadok & Badulescu, 1999) to introduce a layer of encryption that can fit over any

Related Content

Forty Years of Federal Legislation in the Area of Data Protection and Information Security

John Cassini, B. Dawn Medlin and Adriana Romaniello (2011). *Pervasive Information Security and Privacy Developments: Trends and Advancements (pp. 14-23).*
www.igi-global.com/chapter/forty-years-federal-legislation-area/45800?camid=4v1a

Planning for Hurricane Isaac using Probability Theory in a Linear Programming Model

Kenneth David Strang (2013). *International Journal of Risk and Contingency Management (pp. 51-66).*
www.igi-global.com/article/planning-hurricane-isaac-using-probability/76657?camid=4v1a