СПИСОК ЛИТЕРАТУРЫ:

1. *Губанов Д. А., Новиков Д. А., Чхартишвили А. Г.* Социальные сети: модели информационного влияния, управления и противоборства / Под ред. чл.-корр. РАН Д. А. Новикова. М.: Издательство физико-математической литературы, 2010. — 228 с.
2. Доктрина информационной безопасности Российской Федерации.
3. Аналитика фишинговых атак [Электронный ресурс]. URL: http://www.securelist.com/ru/analysis (дата обращения: 15.01.2013).
4. Федеральный Закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
5. Журнал «Information Security/ Информационная безопасность» [Электронный ресурс]. URL: http://www.itsec.ru (дата обращения: 18.01.2013).

А. М. Коротин, П. В. Смирнов

РЕАЛИЗАЦИЯ СРЕДСТВА ПРОЗРАЧНОГО ШИФРОВАНИЯ ФАЙЛОВ НА БАЗЕ СЕРТИФИЦИРОВАННОГО СКЗИ ДЛЯ ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX

В настоящее время одним из решений задачи обеспечения конфиденциальности информации, хранящейся в файловой системе, является шифрование. Существуют различные методы и способы шифрования. Например, пользователь может зашифровать свои файлы и хранить их в защищенном виде. При необходимости использования этих файлов пользователь должен расшифровать их, провести с ними нужные ему операции и затем снова их зашифровать. Неудобство данного способа шифрования состоит в том, что при каждом обращении к файлам пользователь должен сам расшифровывать, а затем зашифровывать их. Для него было бы гораздо удобнее, если бы система сама производила данные операции.

Прозрачное шифрование, известное также как шифрование в режиме реального времени, является методом шифрования, при котором данные зашифровываются и расшифровываются без участия пользователя с помощью драйвера, работающего в фоновом режиме и следящего за всеми обращениями к данным [1]. Основной целью этого метода шифрования является защита от атак, направленных на получение данных в обход операционной системы, т. е. путем загрузки через другую ОС или использования средства прямого доступа к жесткому диску.

На данный момент существует большое разнообразие средств прозрачного шифрования файлов на диске. Практически все они используют иностранные криптографические алгоритмы. Согласно перечню средств защиты информации, сертифицированных ФСБ России, по состоянию на 20 сентября 2012 г. [2], сертифицированные средства прозрачного шифрования существуют только для операционной системы Windows (например, КриптоПро CSP 3.6.1 [3]). Для операционной системы Linux на сегодняшний день таких средств нет. Начиная со сборки ядра 2.6.19, для осуществления технологии прозрачного шифрования используется шифрующая файловая система eCryptfs. Наиболее перспективным представляется внедрение российских криптографических алгоритмов в уже существующее и работающее средство, каким является eCryptfs. Аналогичным образом было спроектировано средство прозрачного шифрования КриптоПро EFS для ОС Windows [4], которое, по сути, является надстройкой над файловой системой EFS с набором дополнительно поддерживаемых функций, таких как контроль целостности информации.

Данная работа является продолжением исследований, которые были представлены в статье «О способах реализации прозрачного шифрования файлов на базе сертифицированного СКЗИ

для операционной системы Linux» [5]. В указанной статье описана архитектура средства eCryptfs, его принцип работы. Ее итогом было принятие решения, что для реализации средства прозрачного шифрования файлов на базе сертифицированного СКЗИ для ОС Linux целесообразно доработать штатное средство eCryptfs таким образом, чтобы файлы шифровались с помощью российского симметричного алгоритма в режиме ядра, а соответствующий симметричный ключ шифровался с помощью российского асимметричного алгоритма в режиме пользователя. Для этого необходимо обеспечить работу алгоритма ГОСТ 28147-89 в режиме ядра и работу алгоритма ГОСТ Р 34.10 2001 в режиме пользователя, причем обеспечивающий его работу PKI-модуль должен использовать стандарт сертификатов X.509. Это возможно осуществить с помощью сертифицированного СКЗИ, которое может работать как в режиме ядра, так и в режиме пользователя.

Управление открытыми и закрытыми ключами пользователя в шифрованной файловой системе eCryptfs реализовано с помощью API-функций инфраструктуры открытых ключей, ключевых модулей и дополнительных пользовательских утилит, таких как GnuPG, OpenCryptoki, TriuSerS TPM.

По умолчанию при установке средства eCryptfs копируются два ключевых модуля. Первый из них, passphrase, обеспечивает защиту симметричного ключа шифрования файла с помощью пары закрытого и открытого ключей, созданных на основе введенного пароля путем многократного его хеширования по алгоритму SHA-512. Второй ключевой модуль, openssl, предоставляет больше возможностей по защите симметричного ключа. Помимо защиты FEK с помощью пароля openssl также поддерживает возможность создания ключевого файла, содержащего закрытый ключ пользователя. Данные ключевые модули представляют собой динамические библиотеки ОС Linux .so. Эти динамические библиотеки лежат по умолчанию в директории /usr/lib/ecryptfs/.

Дополнительные пользовательские утилиты увеличивают степень защиты закрытого ключа пользователя и улучшают характеристики асимметричного шифрования в режиме пользователя.

Модуль PKI GnuPG использует пользовательский пароль для расшифровки закрытого ключа пользователя, который хранится в кольце ключей GnuPG и необходим для расшифровки симметричного ключа файла.

Модуль PKI TriuSerS TPM применяется для поддержки Trusted Platform Module. Это дает возможность использовать закрытый ключ, который хранится в аппаратном средстве, например токене.

Модуль PKI OpenCryptoiki обеспечивает механизм работы с открытым ключом с помощью различных аппаратных устройств, например криптографического ускорителя.

eCryptfs поддерживает возможность написания дополнительных модулей. Такие дополнительные модули могут взаимодействовать с существующими средствами PKI, которые используют стандарт сертификатов X.509.

Таким образом, для обеспечения работы с ключевым материалом на базе ГОСТ Р 34.10-2001 можно разработать дополнительный PKI-модуль на базе сертифицированного СКЗИ, например КриптоПро CSP, и обеспечить его связь со службой eCryptfs, работающей в режиме пользователя. Данный ключевой модуль будет представлять собой динамическую библиотеку для ОС Linux и располагаться вместе с остальными ключевыми модулями в директории /usr/lib/ecryptfs/.

СПИСОК ЛИТЕРАТУРЫ:

1. *Шайдеманн Ф.* Прозрачное шифрование файлов // Журнал сетевых решений. LAN. 2005. № 15.
2. Перечень средств защиты, сертифицированных ФСБ России (по состоянию на 20 сентября 2012 г.). [Электронный ресурс]: ФСБ России. URL: http://clsz.fsb.ru/certification.htm (дата обращения: 12.12.2012).

3. ЖТЯИ. 00050-02 30 01 Средство криптографической защиты информации «КриптоПро CSP». Формуляр.
4. ЖТЯИ. 00051-01 30 01 Средство хранения конфиденциальной информации «КриптоПро EFS». Формуляр.
5. *Коротин А. М., Смирнов П. В.* О способах реализации прозрачного шифрования файлов на базе сертифицированного СКЗИ для операционной системы Linux // Безопасность информационных технологий. 2012. № 2.

В. С. Кузнецов

ПРЕДСТАВЛЕНИЕ ИНФОРМАЦИОННЫХ АТАК В УСЛОВИЯХ ЭТАЛОННОЙ МОДЕЛИ OSE/RM

Целью доклада является структурирование угроз открытых информационных систем в соответствии с эталонной моделью POSIX OSE/RM. Согласно определению IEEE POSIX 1003.0 [1], открытой информационной системой называется система, которая реализует открытые спецификации на интерфейсы, сервисы (услуги среды) и поддерживаемые форматы данных, достаточные для того, чтобы дать возможность должным образом разработанному прикладному программному обеспечению быть переносимым в широком диапазоне систем с минимальными изменениями, взаимодействовать с другими приложениями на локальных и удаленных системах и взаимодействовать с пользователями в стиле, который облегчает переход пользователей от системы к системе.

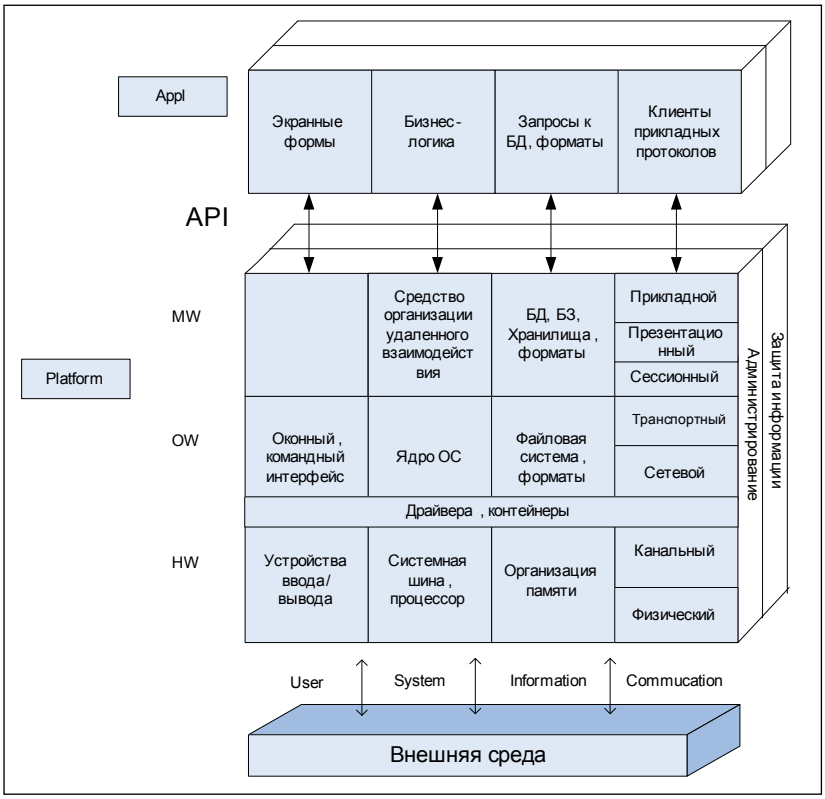

Рис. 1. Концептуальная модель OSE/RM

Если оказалось возможным структурировать информационные системы, то можно структурировать такое понятие, как угрозы безопасности данных систем. Стандарт [1] не потерял своей актуальности и продолжает активно развиваться [2, 3, 4]. В докладе классифицированы и