Cipher DB Crypt Plugin

Защищенные базы данных в СУБД Firebird v3.0

ООО «Сайфер БИС»
Влад Ковтун
Леонид Белясник

Суть проблемы

Обеспечение конфиденциальности данных хранящихся в БД:

- Персональных данных
- Чувствительных данных (медицинских, банковских и т.д.)

Суть проблемы

Согласно требований:

- КСЗИ
- ISO/IEC 27001:2013
- PCI-DSS
- HIPPA
- FERPA

Существующие подходы

- Шифрование соединения
- Шифрование файлов БД
  - Шифрование всего раздела (уровень ФС)
  - Шифрование указанных файлов (уровень ФС)
  - Использование специальных инструментов (BitLocker, TrueCrypt и другие)
- Шифрование данных в БД (TDE)
  - **Прозрачное шифрование пространства таблиц, постранично**
- Шифрование полей в БД (AL)
  - На основе паролей в SQL

Существующие решения

Что предлагается в мире СУБД:

- Oracle DB Enterprise (TDE, AL)
  - Ключ в файле
  - Ключ на устройстве
- Microsoft SQL Server Enterprise (TDE, AL)
  - Ключ в файле
  - Ключ на устройстве
- MongoDB Enterprise (TDE, AL)
  - Ключ в файле
  - Ключ на устройстве
  - Основан на OpenSSL

Существующие решения

Что предлагается в мире СУБД:

- MySQL Enterprise (TDE, AL)
  - Ключ в файле
  - Ключ на устройстве
- MySQL/MariaDB/Percona (AL)
  - Пароль в SQL/DB
- PostgreSql (AL)
  - Используется pgcrypt (plugin общего назначения)
  - Пароль в SQL/DB
- SQLite

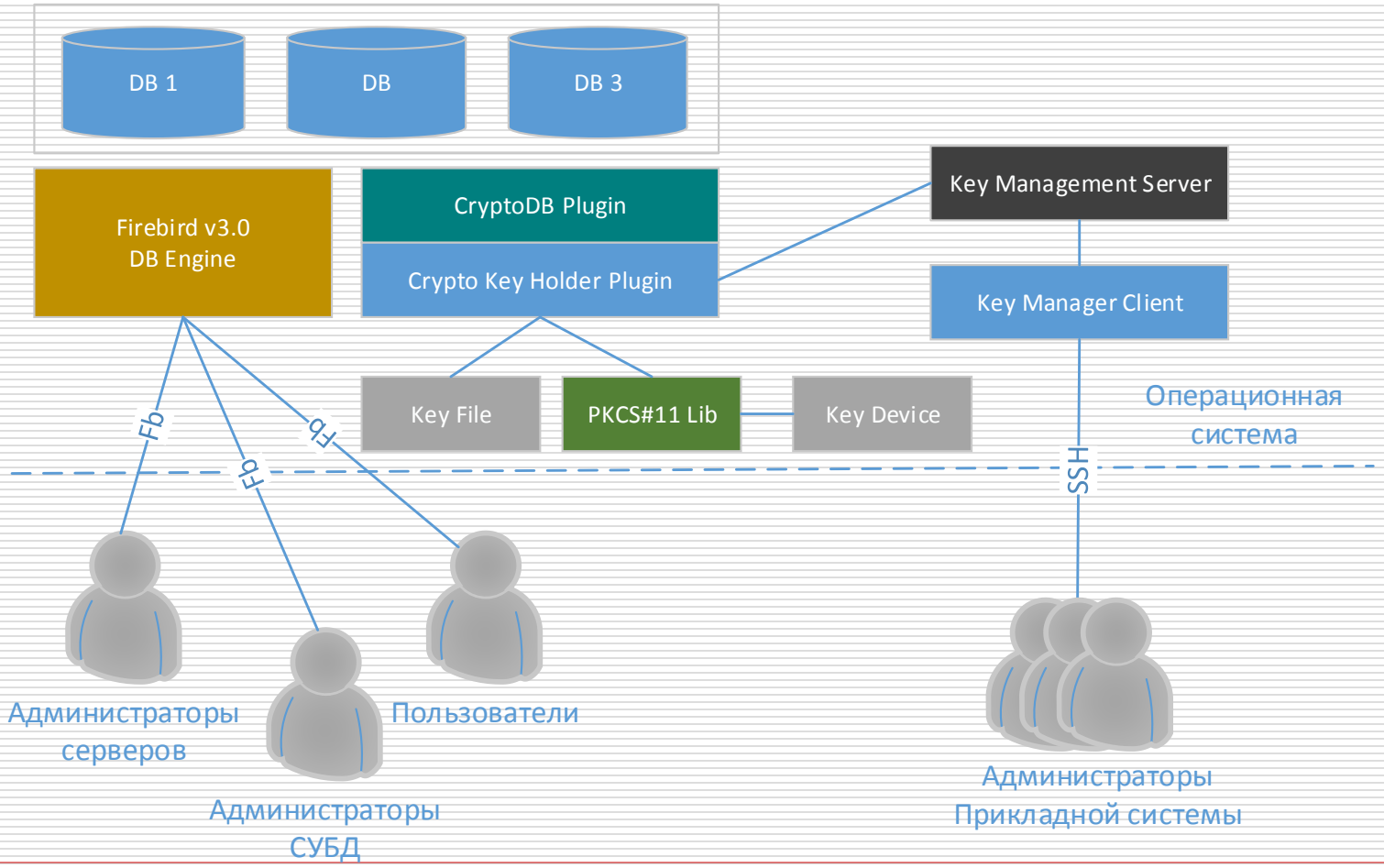
Что предлагаем мы?

- СУБД Firebird v3.0
  - Промышленная СУБД
  - Открытый исходный код
  - Большие объемы данных
  - Высокая стабильность
- Систему шифрования БД для СУБД Firebird v3.0
  - Plugin для доступа к ключу
  - Plugin для шифрования БД
  - Сервер управления ключами

Решаемые задачи

- Шифрование данных в БД
- Защищенное хранение ключа
- Разграничение доступа администраторов к физическим данным
- Распределение секрета между администраторами

Архитектура решения



Криптографические алгоритмы

- Для шифрования данных используются:
  - ДСТУ 7624:2014 (ECB, CBC, CFB, OFB, CTR)
  - ГОСТ 28147-89 (ECB, CBC, CFB, OFB, CTR)
  - AES (ECB, CBC, CFB, OFB, CTR)
  - TDEA (ECB, CBC, CFB, OFB, CTR)
- В основе лежит библиотека «Шифр+» v2.0 (проходит государственную экспертизу)

Поддерживаемые платформы

СУБД Firebird v3.0 поддерживает:

- Windows
  - x86
  - x86-64
- Linux
  - x86
  - x86-64

Условия эксперимента #1

Сервер:

- CPU: Intel Core i7-2600 CPU @ 3,40GHz
- CPU Cores: 4 x 3,41 GHz (with HT - 8)
- HDD: SATA III 120GB
- RAM: 4096 MB
- OS: Debian GNU/Linux 8 (64-bit)
- Linux version 3.16.0-4-amd64
- СУБД: Firebird v3.0.1 x86-64

Условия эксперимента #1

- БД:
  - Таблиц: 5 (200 тыс. записей в каждой)
  - Без индексов
  - Размер: 957056 KB (~ 1 ГБ)
- Шифры:
  - ГОСТ 28147-89 (ДКЕ №1)
  - ДСТУ 7624:2014 (256/256)
- Все операции выполняются локально (isql)

Производительность #1

Первичное полное зашифровывание БД и последующее полное расшифровывание, МБ/с

Алгоритм	E-CTR	D-CTR	D-CTR SSD	E-OFB	D-OFB	D-OFB SSD
ГОСТ 28147	11,12	11,15	16,79	12,00	11,54	18,55
ДСТУ 7624	10,52	9,75	14,56	10,40	10,04	15,23

Шифрование выполняется в фоновом режиме, что не сильно влияет на общую производительность СУБД

Условия эксперимента #2

Сервер:

- CPU: Intel Core i7-2600 CPU @ 3,40GHz
- CPU Cores: 4 x 3,41 GHz (with HT - 8)
- HDD: SATA III 120GB
- RAM: 4096 MB
- OS: Debian GNU/Linux 8 (64-bit)
- Linux version 3.16.0-4-amd64
- СУБД: Firebird v3.0.1 x86-64

Условия эксперимента #2

Клиент:

- CPU: Intel Core i5-6400 CPU @ 2,70GHz
- CPU Cores: 4 x 2,7 GHz
- HDD: SSD SATA III 120GB
- RAM: 8 GB
- OS: Windows 10 (64-bit)
- Клиент СУБД: IBExpert v.2016.9.4.1
- NET: Gigabit Ethernet

Условия эксперимента #2

- БД:
  - Таблиц: 5 (200 тыс. записей в каждой)
  - Без индексов
  - Размер: 957056 KB (~ 1 ГБ)
- Шифры:
  - ГОСТ 28147-89 (ДКЕ №1)
  - ДСТУ 7624:2014 (256/256)
  - TDEA (192)

Условия эксперимента #2

- Подготовка:
  - из SQL-скрипта создается необходимое количество пустых БД;
  - проводятся замеры на незашифрованной БД;
  - Проводятся замеры во время шифрования БД одним из алгоритмов;

Условия эксперимента #2

- Операций над данными в БД
  - вставка большого количества записей (пределах 1 ГБ) в 5 таблиц
  - создание резервной копии
  - выборка большого количества данных разных типов (200 тыс. записей, около 1 ГБ)
  - обновление текстового поля в 5 таблицах
  - удаления данных из 5 таблиц

Производительность #2

Алгоритм	Select, ss	Insert, mm:ss|MB	Update, ss,ms|MB	Delete, ss|MB
ГОСТ 28147-CTR	5:266	27:36:593 984	22:16	20:469
ГОСТ 28147-OFB	5:47	25:43:594 984	18:266 1015	20:684 1030
ДСТУ 7624-CTR	5:01	24:06:47 984	19:106 1015	20:745 1030
ДСТУ 7624-OFB	4:983	22:53:94 984	17:188 1015	20:57 1030
TDEA (3DES)	7:125	26:24:47 984	25:641 1015	27:437 1030
Без шифрования	4:766	23:16:453 984	12:328 1015	20:297 1030

Производительность #2

Алгоритм	Резервное копирование, с	Использование CPU, %
ГОСТ 28147-CTR	32	25
ГОСТ 28147-OFB	29	24
ДСТУ 7624-CTR	28	25
ДСТУ 7624-OFB	29	24
Без шифрования	14	17

Вопросы?

Спасибо за внимание!

ООО «Сайфер БИС»

Влад Ковтун
Леонид Белясник

email: vk@cipher.kiev.ua, lb@cipher.kiev.ua
www: http://cipher.kiev.ua