ВЫБОР СКАНЕРА ДЛЯ РАДУЖНОЙ ОБОЛОЧКИ ГЛАЗА ПРИ ИСПОЛЬЗОВАНИИ УСТРОЙСТВ БИОМЕТРИЧЕСКОГО ПАРОЛЯ ВМЕСТО КЛАССИЧЕСКИХ КЛЮЧЕЙ И ПАРОЛЕЙ В БЫТОВЫХ ПРИБОРАХ

А.А. Гивойно, Г.В. Сечко

Всё большую популярность набирают приборы бытового характера, требующие пароля для доступа к своим функциям. Такие приборы (микроволновые печи, холодильники, автомобили и ряд других, содержат системы управления, включенные в вычислительную сеть физических объектов («Internet of Things», IoT-вещи), встроенные технологиями для взаимодействия друг с другом или с внешней средой [1] и являются типичными объектами защиты информации.

Для доступа к программному обеспечению IoT-вещей часто используют составной двухфазный ключ (второй присылается на почту или смс-оповещением непосредственно в момент входа в систему) или биометрические пароли. Самым надежным паролем является код дезоксирибонуклеи́новой кислоты (ДНК) — макромолекула, обеспечивающая хранение, передачу из поколения в поколение и реализацию генетической программы развития и функционирования живых организмов.

В докладе для защиты информации в предлагается второй по надёжности и более дешёвый, чем код ДНК пароль, получаемый путём сканирования радужной оболочки глаза пользователя(англ. — IRIS). С этой целью сравниваются различные сканеры для IRIS. Делается вывод о том, что USB-сканер Myris показывает в среднем лучшие результаты по сравнению с аналогами, однако следует отметить, что сканер VeriEye уступает лишь по нескольким параметрам. В нынешних реалиях актуальным фактором, влияющим на выбор сканера по параметрам надежности IRIS, защиты ключа от взлома и стоимости, может быть программное обеспечение более дешёвого VeriEye, которое является средством отечественной разработки.

Литература

1. *Гивойно А.А.* Защита информации при использовании устройств биометрического пароля вместо классических ключей и паролей в бытовых приборах // Сборник науч. тр. по матер. межд. заоч. НПК «Актуальные направления научных исследований XXI века: теория и практика», межд. НПК «Молодёжный форум: технические и математические науки» 9–12 ноября 2015 г., Воронеж. — № 7, часть 3 (18-3). Воронеж: ФГБОУ ВО «ВГЛТУ», 2015. 442 с. С. 465–468.

АЛГОРИТМЫ АУТЕНТИФИКАЦИИ САНКЦИОНИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ В МОБИЛЬНОЙ СРЕДЕ

Гондаг Саз Мостафа, В.А. Вишняков

Если нужно зашифровать данные в ОС Android, есть два варианта: API Java Crypto и API OpenSSL. Рассмотрим шифрование данных обоими способами.

Использовать API Java Crypto в Android несложно. Нужно создать ключ для шифрования. Для этого используется класс KeyGenerator в пакете javax.crypto.

```
mKey = null;
try {
kgen = KeyGenerator.getInstance("AES");
            mKey = kgen.generateKey();
            } catch (NoSuchAlgorithmException e) {
            e.printStackTrace();
}
```

Для шифрования данных с помощью OpenSSL в Android нужно написать собственный код, доступ к которому в Java осуществляется с помощью вызовов JNI. Здесь требуется больше работы, но и производительность будет выше. Нужно создать ключ и вектор инициализации.

```
1                   unsigned char cKeyBuffer[KEYSIZE/sizeof(unsigned char)];
2                           unsigned       char       iv[]       =
                           "01234567890123456";
3                   int opensslIsSeeded = 0;
4                           if (!opensslIsSeeded) {
```

Библиотека БГУИР

```
5                                   if (!RAND_load_file("/dev/urandom",
                                seedbytes)) {
6                                       return -1;
7                                   }
8                                   opensslIsSeeded = 1;
9                       }
10                                  if      (!RAND_bytes((unsigned      char
                                *)cKeyBuffer, KEYSIZE )) {
11                      }
```

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ КОРПОРАТИВНОЙ СЕТИ ПРЕДПРИЯТИЯ

П.А. Домино, С.Н. Петров

Сегодня число программных продуктов, используемых в любой компании, довольно велико. Также существует тенденция увеличения их количества, причем независимо от профиля компании.

Информация и технологии ее обработки играют ключевую роль в эффективном функционировании и управлении предприятием. Имея доступ к нужной информации — технологической, кадровой, маркетинговой или финансовой, — можно правильно оценить текущую ситуацию, принять своевременные решения. В то же время информация должна быть доступна только тем, кому она предназначена, и скрыта от сторонних наблюдателей.

Известно, что более 25% злоупотреблений информацией в информационных сетях совершаются внутренними пользователями, партнерами и поставщиками услуг, имеющими прямой доступ к сети. До 70% из них — случаи несанкционированного получения прав и привилегий, кражи и передачи учетной информации пользователей сети предприятия, что становится возможным из-за несовершенства технологий разграничения доступа и аутентификации пользователей. Совершенствование методов системы управления доступом и регистрации пользователей является одним из приоритетных направлений развития информационной сети предприятия. Аутентификация является обязательной частью управления доступом в сетях предприятий, без нее нет возможности ограничить доступ пользователей к конкретным информационным ресурсами.

Проведены обзор существующих механизмов аутентификации и сравнение на основе таких показателей, как надёжность и безопасность, эффективность, а так же затраты на установку и обслуживание.

Затраты на обслуживание и эффективность определялись как время, затраченное администратором системы, на ее установку и обслуживание, а также время, затраченное пользователем системы, для прохождения процедуры аутентификации.

Также учитывались финансовые затраты на установку системы, ее обслуживание, а также затраты злоумышленника, требуемые для успешного прохождения аутентификации с помощью определённого типа атаки. В качестве атаки по умолчанию рассматривалась атака методом грубой силы.

ШИФРОВАНИЕ ДАННЫХ С ХАОТИЧЕСКИМИ ИЗМЕНЕНИЯМИ РАУНДОВОГО КЛЮЧА НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА

Д.А. Жуковец

Большинство блочных алгоритмов шифрования одинаково шифруют блоки исходного текста. При этом, если исходное изображение черного цвета, то при шифровании получаем последовательность одинаковых зашифрованных блоков. Чтобы исключить это, в алгоритмах при шифровании используются режимы шифрования CBC, CFB и другие. Однако в режиме CBC (режиме сцепления блоков) при изменении одного бита в исходном тексте при наличии лавинного эффекта могут произойти не только вариации в зашифрованном изображении, но и неполное восстановление исходной информации.

Предлагаемый способ шифрования данных с хаотическими изменениями раундового ключа на основе динамического хаоса позволяет не только увеличить степень защищенности информации, но и обеспечить эффективность шифрования путем повышения стойкости алгоритма шифрования.

Библиотека БГУИР