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) {
```