свойствах бумаги, в приводах, конденсаторах, электродах и устройствах с полевой эмиссией [2].

В результате проделанной работы были измерены электрические свойства бумаги на основе УНТ. Снята вольтамперная характеристика бумаги, вычислены холловская подвижность носителей, слоевая концентрация носителей, слоевое сопротивление.

Литература

1. *Елецкий А. В.* Углеродные нанотрубки и их эмиссионные свойства // Успехи физических наук. 2002. №4. С. 401–417
2. http://amos.indiana.edu/library/scripts/buckypaper.html

РЕАЛИЗАЦИЯ ФУНКЦИЙ ПРОВЕРКИ СЕРИЙНЫХ НОМЕРОВ ДЛЯ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

А. Н. Сидоревич

ВВЕДЕНИЕ

С целью защиты программного обеспечения используется метод серийных номеров для регистрации или активации программного продукта. Как правило, серийный номер высылается пользователю, прошедшему этап регистрации и оплатившему ее стоимость.

Различают статические серийные номера (одинаковые для всех пользователей) и динамические (различные для разных пользователей, разных конфигураций компьютеров и т.п.). Статический номер не обеспечивают надежной защиты – его можно подсмотреть у соседа или знакомого, а затем дома ввести и зарегистрировать продукт. Сложнее подобрать динамический номер – последовательность байт, зависящую от имени пользователя, параметров операционной системы, номера сетевой карты, а также программных и аппаратных средств. Пользователь может самостоятельно выбрать имя, под которым регистрируется продукт и в этом случае регистрационный ключ зависит от заданного логина. Иногда для получения ключа требуется вместе с некоторой суммой предать производителю значение, сгенерированное программой (это может быть зашифрованный номер винчестера, сетевой карты и т.п.).

ПРОСТОЕ СРАВНЕНИЕ С ЭТАЛОНОМ

Одной из первых реализаций этого метода было непосредственное сравнение с эталоном – байт за байтом, в этом случае регистрационный номер можно без труда извлечь из самой программы.

Наиболее простым способом является поиск строковых констант в исполнимом файле, возможно среди них и будет правильный пароль.

Если же программа была упакована, то поиск в файле ничего не даст. Тем не менее, все еще остается возможность поиска строк в памяти запущенного приложения или исследование при помощи отладчика.

Таким образом, в действительности данный метод не обеспечивает реальной защиты

СРАВНЕНИЕ ЧЕРЕЗ ХЕШ-ОБРАЗ

Усложним процедуру проверки так, чтобы не использовалось явное представление эталонной строки. Сравнение должно происходить через некий характерный признак, присущий строке. Таким признаком может служить хеш-образ строки. Код должен содержать функцию расчета хеш-значения от входной строки и процедуру проверки ключа.

Теперь в таблице ссылок на текстовые строки дизассемблер не обнаружит ничего подозрительного. Однако если обратить внимание на участок кода в дизассемблере, который проверяет правильность введенного ключа, то можно обнаружить операцию сравнения рассчитанного хеш-значения с эталонным. В случае выполнения равенства условный переход передаст управление на блок, выводящий сообщение об успешной регистрации, в противном случае мы увидим сообщение типа «Wrong password!!!».

Таким образом, достать значение серийного номера, не получилось. Можно попробовать обратить функцию расчета числового значения от серийного номера, но это не всегда возможно.

Можно сделать вывод – использование хеш-функций позволяет производить проверку вводимого ключа без необходимости хранения непосредственного его значения в программе.

В теории это выглядит хорошо. Но, как и в большинстве защищаемых систем, слабость находится в другом месте. Конечная цель взломщика – получить работоспособную копию программы. Гораздо проще подменить, например, эталонное значение, с которым происходит сравнение хеш-образа или просто изменить условный переход так, чтобы управление попадало на нужную ветвь программы.

Проиллюстрируем сказанное. Пусть взломщик хочет, чтобы правильным паролем программа считала строку «hacker». Для этого ему нужно найти ее хеш-образ. Далее используя шестнадцатеричный редактор необходимо заменить эталонное значение на полученное.

Еще один способ изменения кода программы – это замена условного перехода на безусловный или вообще отключение его. Можно отключить

условный переход, исправив байты команды JNZ SHORT на JMP SHORT. Управление предается сразу на ту часть программы, отвечающую за выполнение действий при правильной регистрации.

Из рассмотренного видно, что использование хеш-функций само по себе еще не обеспечивает защиты. Необходимы некоторые дополнительные меры, которые не позволят взломщику так просто модифицировать код программы.

ИСПОЛЬЗОВАНИЕ ШИФРОВАНИЯ

Пусть в программе происходит вычисление хеш-образа для предварительной проверки введенного ключа. Если выбрана хорошая хеш-функция свободная от коллизий и результат ее выполнения совпал с эталонным, то можно гарантированно утверждать, что был введен истинный ключ. Это дает нам право использовать введенное значение ключа в некоторых вычислениях, например шифровании. Взломщик же может повлиять на процедуру сравнения хеш-значения с эталоном, но узнать само значение ключа ему не удастся.

В результате успешного прохождения этапа предварительной проверки ключа происходит передача управления в процедуру шифрования, иначе происходит выдача предупреждающего сообщения. В вызываемой процедуре происходит шифрование исполняемого кода и последующая передача на него управления. При правильно введенном ключе, в результате шифрования на месте выбранных разработчиком байт должны оказаться истинные команды. Если взломщик изменит процедуру предварительной проверки, то при неправильно введенном ключе могут появиться неправильные машинные инструкции, которые могут привести к краху программы, но в любом случае не к выполнению того, что положено.

Использование шифрования является несколько затратным делом, по сравнению с прочими приемами логических защит, зато гораздо надежнее и практически неуязвимо.

Какие атаки может предпринять взломщик? Если ему не известен правильный серийный номер и зашифрованный код имеет значительный объем, то при условии надежности алгоритма шифрования и достаточной длине ключа шифрования взлом подобной системы эквивалентен взлому криптоалгоритма и не представляется возможным.

Можно предложить еще один способ защиты программы. Суть заключается в шифровании правильным ключом самой процедуры проверки вводимого ключа. Разумеется, пока пользователь не введет правильный ключ, никакой процедуры проверки он не получит. А если введет правильный, то является очевидным, что процедура проверки уже не нужна.

На процедуру проверки возлагаются такие обязанности, как расшифрование защищенного исполнимого кода, проверка целостности некоторых участков или всей программы, инициализация ряда важных для работы переменных и т.п. Именно по вышеперечисленным причинам изъять процедуру проверки не получится.

ЗАКЛЮЧЕНИЕ

Одним из наиболее качественных методов защиты программ является криптографическое преобразование информации. Согласно правилу Кирхгофа, стойкость криптозащит определяется исключительно стойкостью секретного ключа. Даже если алгоритм работы такой защиты известен, это не сильно упрощает его взлом. При условии правильного выбора длины ключа, криптозащиты не ломаемы в принципе

При реализации процедуры проверки серийного номера наиболее уязвимые места – это операция сравнения и передача управления на определенную ветвь кода. Однако операцию сравнения нужно использовать для предварительной проверки введенного ключа, так что ее результат является лишь защитой от ошибочного набора номера. Чтобы исключить возможность передачи управления на участок кода, отвечающий за последствия правильного ввода номера, необходимо использовать шифрование этого кода на основе ключа, генерируемого из введенного серийного номера.

УСТРОЙСТВО КАРДИОМОНИТОРИНГА НА ОСНОВЕ МОБИЛЬНОГО ТЕЛЕФОНА КЛАССА «SMARTPHONE»

А. В. Столяров

На протяжении многих лет различные заболевания, связанные с сердечно-сосудистой системой, держат печальную пальму первенства в списке болезней человека и приводят к существенному сокращению продолжительности его жизни. Всем хорошо известно, что для любых болезней, наряду с профилактикой, исключительно важным является их раннее обнаружение и диагностика. Это обуславливает значительное внимание, уделяемое вопросам создания и развития современных средств автоматизированного инструментального исследования сердечно-сосудистой системы человека.

Наиболее распространенным и доступным для широкого круга людей методом инструментального исследования сердечно-сосудистой системы была и остается электрокардиография, основу которой составляет реги-