Киренберг А.Г., Артемов Г. И. Использование аппаратного скриптора в прикладных задачах информационной безопасности // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 1(27) с. 75–80

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056.5

ИСПОЛЬЗОВАНИЕ АППАРАТНОГО СКРИПТОРА В ПРИКЛАДНЫХ ЗАДАЧАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

[1] Киренберг А.Г., [2] Артемов Г. И.
Кузбасский государственный технический университет им. Т.Ф. Горбачева, Кемерово, Россия (650000, г. Кемерово, ул. Весенняя, 28), email: [1]ag-k@yandex.ru, [2]21t013@kuzstu.ru

Для удобства работы с компьютером или информационной системой существуют различные вспомогательные устройства. Но некоторые из них кроме удобства работы несут в себе некоторые угрозы с точки зрения информационной безопасности, или иначе говоря – создают определенные уязвимости. Однако, это не означает, что их нежелательно использовать. Важным моментом при эксплуатации таких устройств является неукоснительное соблюдение правил и политики информационной безопасности, принятой в организации.

Ключевые слова: : информационная безопасность; скриптор; HID-совместимое устройство; bad-USB устройство; Arduino

USING HARDWARE SCRIPTOR IN APPLIED TASKS OF INFORMATION SECURITY

[1] Kirenberg A.G., [2] Artemov G.I.,
Kuzbass State Technical University. T.F. Gorbachev, Kemerovo, Russia (650000, Kemerovo, st. Spring, 28), [1]ag-k@yandex.ru, [2]21t013@kuzstu.ru

For the convenience of working with a computer or information system, there are various auxiliary devices. But some of them, in addition to the convenience of work, carry some threats from the point of view of information security, or, in other words, create certain vulnerabilities. However, this does not mean that they are undesirable to use. An important point in the operation of such devices is the strict observance of the rules and policies of information security adopted in the organization.

Keywords: information security; scriptor; HID-compatible device; bad-USB device; Arduino

В современном мире любой цивилизованный человек уже не представляет себя в отрыве от информационной среды, с которой он взаимодействует не только на работе или во время учебы, но и в быту. Сама среда и сопутствующие ей информационные технологии развиваются стремительно, затрагивая практически любые аспекты нашей жизни. Каждый год на рынке появляются новые цифровые устройства и гаджеты, способные облегчить работу в

информационной среде. Однако, некоторые устройства при определенных условиях могут быть как средством защиты цифрового пространства человека, так и одновременно содержать в себе угрозу для информационной безопасности человека или даже всей организации или предприятия. Все зависит от того, у кого в руках оказалось это устройство и с какими целями его планируют использовать.

Любая информационная среда или система для взаимодействия с пользователем требует ввода аутентификационных данных – как минимум, логина и пароля. С каждым годом требования к защите информации ужесточаются, а значит и пароли становятся сложнее, что в свою очередь влечет за собой вероятность ошибок при вводе по причине невнимательности ввода или забывчивости (последнее характерно для организаций, где предусмотрена регулярная смена паролей).

В связи с этим возникает потребность в автоматизации быстрого и безошибочного ввода аутентификационных данных и безопасности их хранения. Для этой и некоторых других целей возможно использовать специальное электронное устройство, условно именуемое как **«аппаратный скриптор»** (далее — АС), о применении которого и идет речь в данной статье.

АС представляет собой плату Arduino с интерфейсом USB, которая сопоставима по размеру с обычным флеш-накопителем. Для ОС компьютера скриптор определяется как PnP HID-совместимое устройство, поэтому она может эмулировать клавиатуру и мышь [1]. Данную плату можно купить в интернете.

АС называется именно так, потому что выполняемый скрипт хранится в чипе, распаянном на плате (рисунок 1), а взаимодействие со скриптом (то есть эмуляция мыши и клавиатуры) реализуется после подключения АС в USB-порт, причем без участия файловой системы компьютера, поскольку АС не является носителем информации как таковым, в отличие от флеш-накопителя, который монтируется к файловой системе. Взаимодействие со скриптом происходит на аппаратном уровне, а значит, АС можно считать самостоятельным устройством.

Рисунок 1 – Примерный внешний вид АС (без корпуса)

Как уже упоминалось, АС может эмулировать действия пользователя: ввод данных с клавиатуры и мыши. Таким образом, его можно настроить на выполнения задач различной сложности. Но возможности АС не ограничиваются только вводом данных, с его помощью можно выполнить достаточно широкий спектр задач как рядовых пользователей, так и обслуживающих ИТ-специалистов, а также специалистов в области информационной безопасности (далее — ИБ-специалистов).

В качестве первого примера рассмотрим использование АС для рядового пользователя. Рядовому пользователю может быть необходимо заполнение различных форм данных, причем не только логина и пароля. Примерами таких форм могут являться: форма регистрации на сайтах, форма ввода данных банковской карты для оплаты через Интернет, форма ввода пароля архива и т. п. Такой способ будет отличаться быстротой, удобством и надежностью, так как АС избавит от необходимости ручного ввода данных, а удобство и надежность достигаются тем, что громоздкие данные для авторизации не нужно хранить на бумажном носителе или на компьютере [2].

Несмотря на то, что аутентификационные данные хранятся браузером в зашифрованном в виде, это не является достаточной защитой, поскольку специальное вредоносное ПО (стиллеры) способно ее обходить. Пользователь также может использовать мастер-пароль для браузера, что имеет бóльшую степень защиты, но данный пароль должен быть сложным, а значит для его быстрого и безошибочного ввода на помощь снова может прийти АС.

Вторым примером использования АС для рядового пользователя может стать быстрая помощь человеку, который обладает лишь начальными навыками владения компьютером (например, пожилые люди), или который имеет ограниченные возможности по здоровью (ОВЗ). Естественно, для подготовки к использованию АС такими людьми предварительно потребуется однократная помощь программиста для создания и записи скрипта в устройство. Дополнительным преимуществом для вышеуказанных категорий лиц при использовании АС является безошибочное и гарантированное открытие подлинного сайта, на котором предполагается можно безопасно вводить персональные данные. Для этой цели необходимо кроме аутентификационных данных пользователя указать верный URL-адрес сайта, после чего скрипт автоматически будет открывать его, что исключит обращение к фишинговому ресурсу, имеющему похожий URL-адрес.

Третьим, несколько экзотичным примером использования АС не ИТ-специалистом является «абсолютная» блокировка компьютера до тех пор, пока АС вставлен в USB-порт. В этом случае даже при вводе в систему верных логина и пароля система будет блокироваться, причем можно задать нужную периодичность и задержку.

Теперь рассмотрим возможные примеры эксплуатации АС продвинутыми пользователями или ИТ / ИБ-специалистами. Одним из примеров такой эксплуатации АС может являться, например, запуск специального антивируса, нацеленного на поиск вредоносных объектов определенного типа или запуск ПО категории antimalware, восстановление работы системы по точкам восстановления при наличии неполадок в ОС. Также возможно, кому-то будет удобнее с помощью АС автоматизировать и задачи самой ОС, например, перемещение файлов на раздел диска типа BitLocker, резервное копирование данных, восстановление конфигурации виртуальных машин в компьютерном классе после

занятий. Для этого обслуживающий инженер или лаборант вставляет поочередно в каждый учебный компьютер АС и скрипт восстанавливает первоначальные настройки виртуальных машин, либо запускает процедуру импорта «чистой конфигурации» с сетевого хранилища.

Как уже упоминалось выше, АС может стать отличным инструментом в руках ИБ-специалиста. Он может быстро проверить компьютер на предмет возможного запуска посторонних скриптов/программ, например, выполнить проверку любых системных файлов на предмет модификации и целостности, в т.ч. и системного реестра или системного файрвола, создать «карантинную» зону в системе путем создания запретных правил в файрволе, и даже отключить доступ в интернет на уровне сетевой карты. Таким образом, с помощью АС можно максимально быстро пресечь утечку данных через интернет и начать «лечение» системы, разблокировать файлы, если они были заблокированы вредоносными процессами. Это не полный перечень сценариев использования АС ИБ-специалистами.

Программирование (запись нужного скрипта) АС происходит довольно просто. Сначала необходимо написать необходимый скрипт на языке программирования С и загрузить его в память микроконтроллера. Данные действия реализуются через программу Arduino IDE. Следует учитывать, что после записи скрипта он автоматически запускается (побочный эффект записи, так как АС автоматически переподключается к порту USB), поэтому все подготовительные и проверочные действия необходимо проводить на виртуальной машине, либо технологическом компьютере.

Обобщённый алгоритм использования АС представлен на рисунке 2:

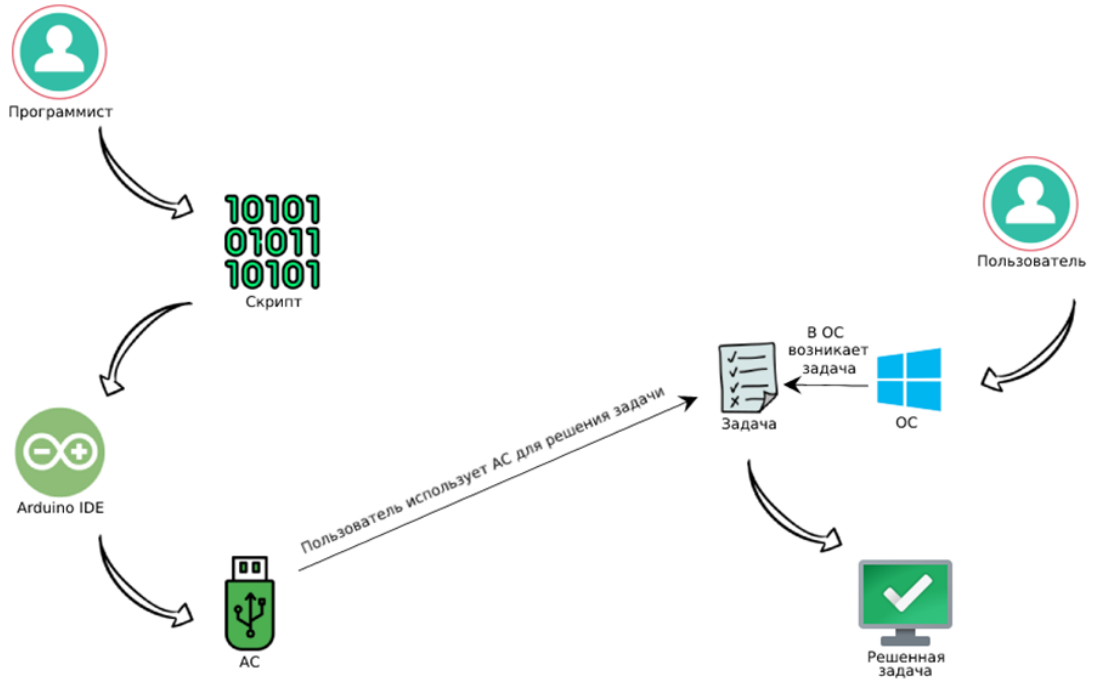

Рисунок 2 – Обобщённый алгоритм использования АС

Несмотря на возможности, которые открываются при использовании АС, есть и негативный побочный эффект, заключающийся в том, что это устройство может являться инструментом в руках злоумышленников, что отрицательно скажется на информационной безопасности корпоративной ИС или отдельного рабочего места сотрудника. Если система не защищена и у злоумышленника есть доступ к информационной системе (физический доступ

компьютеру рабочего места сотрудника), то он может вставить свой АС со своим скриптом в любой USB-порт и за несколько секунд произвести злоумышленные действия по отношению к данному компьютеру или даже всей корпоративной ИС, поскольку обычно к ней по сети подключаются все рабочие места сотрудников. Например, злоумышленник может быстро украсть пароли и отправить их к себе на сервер, создать в системе backdoor («тайный вход» в систему) или скрытую учетную запись с правами администратора, что даст ему возможность подключиться из любой локации к корпоративным ресурсам организации, выполнить любой скрипт, имеющий деструктивных характер.

Однако, для устранения вышеуказанного негативного побочного эффекта при использовании АС существует защита. Так, например, в Антивирусе Касперского и в Dr.Web есть функция проверки HID-совместимых устройств, т.е. тех, которые заранее не были зарегистрированы в системе на определённый USB-порт. Кроме того, подобную защиту от использования несанкционированных устройств может обеспечить программно-аппаратный комплекс «Соболь» или программный комплекс защиты рабочего места Secret Net Studio.

В частности, принцип проверки HID-совместимых устройств в Антивирусе Касперского выглядит следующим образом:

Когда к компьютеру подключается USB-устройство, определенное операционной системой как клавиатура, программа предлагает пользователю ввести с этой клавиатуры или с помощью экранной клавиатуры (если она доступна) цифровой код, сформированный программой. Эта процедура называется авторизацией клавиатуры. Если код введен правильно, программа сохраняет идентификационные параметры – VID/PID клавиатуры и номер порта, по которому она подключена, в списке авторизованных клавиатур. Авторизация клавиатуры при ее повторном подключении или перезагрузке операционной системы не требуется. При подключении авторизованной клавиатуры через другой USB-порт компьютера программа снова запрашивает ее авторизацию [3].

ПАК «Соболь» и ПО Secret Net Studio запоминают эталонный набор разрешенных портов и подключаемого оборудования и при подключении постороннего оборудования блокируют доступ к ОС на аппаратном и программном уровне соответственно.

Таким образом, аппаратный скриптор — удобный и эффективный инструмент для рядового пользователя, обслуживающих ИТ-специалистов и специалистов по информационной безопасности. Тем не менее, использование данного устройства не избавляет от необходимости соблюдения политики и правил информационной безопасности, принятых в каждой конкретной организации. Как показывает статистика - самая большая угроза в информационной безопасности исходит не от внешних злоумышленников, а от внутренних пользователей. Так, например, по данным источника «The CEO’s Guide to Cybersecurity, BCG» (сентябрь 2021) примерно до 77% утечек данных происходят по вине человека и только 23% обусловлено различными технологическими уязвимостями, что подтверждено на рисунке 3.

Рисунок 3 – Соотношение угроз информационной безопасности организаций и предприятий

Список литературы

1. BadUSB. URL: https://ru.wikipedia.org/wiki/BadUSB (Последнее обращение: 14.01.2023)
2. BadUSB — новый тип уязвимости USB-устройств. URL: https://habr.com/ru/sandbox/87861 (Последнее обращение: 14.01.2023)
3. Защита от атак BadUSB. URL: https://support.kaspersky.com/KESWin/11.5.0/ru-RU/176739.htm (Последнее обращение: 14.01.2023)

References

1. Bad USB. URL: https://ru.wikipedia.org/wiki/BadUSB (Last accessed: 01/14/2023)
2. BadUSB is a new type of USB device vulnerability. URL: https://habr.com/en/sandbox/87861 (Last access: 01/14/2023)
3. Protection against BadUSB attacks. URL: https://support.kaspersky.com/KESWin/11.5.0/en-RU/176739.htm (Last accessed: 01/14/2023)