1. Слайд

Здравствуйте уважаемая комиссия. Тема моего проекта разработка программно-аппаратной платформы с возможностью защищенного хранения информации и защищенными протоколами передачи информации.

1. Слайд

Актуальность. По данным BSA (Business Software Alliance), доля нелегальных копий программных продуктов в России составляет 95 % — это дает основание относиться к компьютерному пиратству как к национальному бедствию.

Рассмотрены следующие решения сторонних разработчиков:

Hardlock, HASP (Hardware Against Software Piracy), eToken от компании Aladdin(Россия). Sentinel RMS, Sentinel LDK, Sentinel HL от компании SafeNet(США).

Заказчиком были отмечены следующие недостатки:

* Завышенная стоимость: стоимость одного ключа от перечисленных производителей начинается от 3000 рублей, в то время наш ключ стоит 200 рублей за штуку.
* Отсутствие гибкости аппаратной части ключа: нет возможности внести изменения во встроенной в ключ программы, нельзя вынести критически важные части алгоритмы на ключ.
* Наличие готовых эмуляторов в общем доступе: в сети интернет существуют эмуляторы, которые позволяют использовать ПО без наличия физического ключа.
* Короткие сроки жизни для ранее созданных систем защит (менее 6 месяцев) из-за широкой распространенности на рынке программного обеспечения. Одно из наших преимуществ состоит в том, что о нас никто не знает.

1. Слайд

Цель: создать систему, предназначенную для хранения критически важных данных во flash памяти микроконтроллера в защищенном виде. Flash память должна хранить константы, алгоритм работы и другую ключевую информацию защищаемого ПО.

Система должна выполнять следующие функции:

1) Обеспечивать защиту данных от несанкционированного доступа

2) Производить форматирование содержимого flash и EEPROM памяти микроконтроллера при обнаружении несанкционированного доступа

3) Форматировать память по завершению условий лицензии

4) Иметь защищенный протокол взаимодействия микроконтроллера и ПК

5) В случае форматирования осуществлять вывод причины форматирования, серийного номера ключа и времени форматирования

1. Слайд

На стороне защищаемого программного обеспечения (Полиграф), сторонним программистом была разработана библиотека взаимодействия с ключом по средствам виртуального COM порта. В библиотеке реализован код аналогичный тестовым функциям, разработанным в тестовом проекте на языке processing.

1. Слайд

Форматирование flash и EEPROM памяти микроконтроллера происходит в случае запуска ключа с отличными от заданных по умолчанию конфигурационными и блокировочными байтами.

Форматирование так же происходит при вводе пароля более N раз, по команде форматирования от защищаемого ПО, при истечении срока действия лицензии.

Ключ форматируется при попытке откорректировать время на ПК.

Превышено число неверных команд, Аппаратный сброс МК. Замыкание ножки RST на GND, Понижение питания МК. Срабатывание подсистемы Brown-out Detection(BOD)

Подключение посторонних приборов к МК.

1. Слайд

При запуске ключа происходит инициализация подсистемы USB. Далее происходит проверка «установлен ли флаг форматирования». Если да, то память микроконтроллера форматируется, если нет, то при наличии нулевого байта программы по адресу 0x0000 происходит прыжок в область приложения. А так же если ключ отформатирован, есть возможность получить причину форматирования, время форматирования и серийный номер ключа.

1. Слайд

Основная программа постоянно находится в режиме ожидания приветствия(handshake) от ПК. Если ключом принято приветствие и командный пакет, то ключ выполняет действия соответствующие команде, а иначе на ПК отправляется ошибка ожидания с кодом 0xFF.

1. Слайд

Для того что бы проверить работоспособность ключа был создан тестовый проект в среде processing на языке java. А так же тесты проводились сторонним разработчиком защищаемого программного обеспечения.

1. Слайд

Каждая ножка микроконтроллера представляет собой конденсатор, который может некоторое время сохранять заряд. Данная особенность была использована для проверки подключения сторонних приборов к ключу. При подаче 5 вольт на ножке постепенно накапливается напряжение. Был произведен замер напряжения на ножке в течение 800мс и построен график. Зная значения напряжения в нормальных условиях, были определены допустимые коридоры значений при выходе, за которые происходит форматирование памяти.