ЭЛЕКТРОННЫЕ КЛЮЧИ ЗАЩИТЫ ПРОГРАММНЫХ ПРОДУКТОВ.

КОМПАНИЯ "АКТИВ" ВЫБИРАЕТ МИКРОКОНТРОЛЛЕРЫ NXP

И.Кокорева

Компания "Актив", российский производитель систем информационной безопасности, и компания NXP Semiconductor, независимый производитель полупроводниковых компонентов, представили новые модели электронных ключей Guardant – Guardant Stealth III Sign и Guardant Stealth III Time, созданные на базе 32-разрядных ARM микроконтроллеров NXP серии LPC2000. Презентация продуктов состоялась в рамках семинара компании "Актив", который прошел на 19-й выставке "Информационные технологии и компьютеры. Softool 2008".

Электронные ключи Guardant предназначены для защиты программного обеспечения и активно используются компаниями по всей России. Представленные модели Guardant Stealth III Sign и Guardant Stealth III Time – это продолжение линейки аппаратных средств защиты от нелегального копирования ПО, выпускаемых компанией "Актив" уже в течение 14 лет.

Электронные ключи этих моделей созданы на основе микроконтроллеров семейства LPC2000 со специализированной версией микрокода, разработанной совместно специалистами компаний NXP и "Актив". Данное решение позволяет существенно улучшить характеристики новых моделей электронных ключей и обеспечить надежную защиту конечного изделия. При этом стоимость ключей осталась доступной широкому кругу потребителей.

Вот мнения руководителей компаний о совместной работе.

Генеральный директор компании "Актив" Константин Черников: "Выпуск крупносерийной продукции на новой аппаратной основе – очень непростой шаг. Но качество и богатые возможности продукции NXP помогли нам принять решение. Важным фактором явилось то, что с крупнейшей микроэлектронной компанией можно оперативно решать сложные технические и организационные вопросы. Мы имели возможность в этом убедиться, так как уже несколько лет производим на чипах NXP заказную продукцию".

Директор по продажам NXP Semiconductors в регионе СНГ и стран Балтии Ванда Швандерова: "NXP работает в тесном сотрудничестве с локальными компаниями. Совместная разработка кода и достигнутое соглашение о поставке "Активу" микроконтроллеров с индивидуальной заводской прошивкой – еще один пример результативного взаимодействия с российскими производителями электронной техники. Мы надеемся, что предложенное решение позволит упростить технологический процесс производства электронных ключей Guardant и сделает эту продукцию еще более конкурентоспособной. Компания "Актив" является крупным производителем электронных устройств для рынка информационной безопасности, и это добавляет значимости нашим совместным проектам. Я надеюсь, что наше сотрудничество будет и дальше развиваться так же динамично".

Guardant – средство защиты интеллектуальной собственности разработчиков и издателей компьютерных программ. Это программно-аппаратный комплекс, состоящий из электронных ключей и программного обеспечения Guardant.

Электронные ключи имеют небольшие размеры, подключаются к USB- или LPT-порту компьютера. Базовым элементом ключей Guardant является микропроцессор. Все модели имеют энергонезависимую память. Программное обеспечение Guardant предназначено для организации взаимодействия между защищаемой программой и электронным ключом, "привязки" программы к ключу. Защита Guardant – это гибкий инструмент с широкими возможностями. Технологии Guardant позволяют с максимальной надежностью защитить любое программное обеспечение.

Далее представлены основные характеристики защиты Guardant.

- Стойкость ко взлому. Аппаратный ключ – интеллектуальное устройство, недоступное для прямого анализа извне.
- Хорошая совместимость ключа защиты и объекта. Ключ и защищенная программа взаимодействуют при помощи драйверов, работающих на основе документированных функций операционной системы.
- Защита не зависит от конкретного компьютера и операционной системы. При смене компьютера защита остается работоспособной.
- Большой срок службы. Электронный ключ – надежное устройство. Он будет работать многие годы.

Основные защитные механизмы Guardant: аппаратные ал-

горитмы преобразования данных; защищенные ячейки; многоуровневый механизм защиты доступа к операциям с ключом; аппаратные запреты на чтение/запись содержимого памяти; защищенный протокол обмена с ключом; аппаратная блокировка отладочных средств.

Аппаратные алгоритмы – это математические алгоритмы, реализующие функции вида У = F(X). Они выполняются микропроцессором электронного ключа без использования вычислительных мощностей компьютера. На основе аппаратных алгоритмов строятся сложные схемы взаимодействия между защищенной программой и ключом. Пользователи могут сами создавать и настраивать аппаратные алгоритмы. Аппаратные алгоритмы позволяют производить следующие операции: симметричное шифрование, поточное шифрование, электронную цифровую подпись, генерацию псевдослучайных чисел.

Настоящая защита – это защита, которая составляет единое целое с защищенной программой. На основе данных, необходимых для работы защищаемого приложения, генератор исходных текстов создает исходный код со встроенными функциями защиты. Генератор в полной мере использует возможности аппаратных алгоритмов и Guardant API. Программисту остается только скомпилировать созданный код с исходным текстом приложения.

В электронных ключах работает технология безопасного удаленного обновления памяти – Trusted Remote Update (TRU), т.е. вся информация для дистанционного обновления расшифровывается и обрабатывается внутри ключа. Нет возможности "подсмотреть" или фальсифицировать данные, записываемые в ключ.

Наряду с аппаратными алгоритмами в памяти электронного ключа можно создавать ячейки. Защищенная ячейка – это контейнер с данными, обращение к которому осуществляется по его номеру. Она может иметь уникальные пароли на чтение и обновление. Активация/деактивация ячеек осуществляется по уникальным паролям.

Guardant Stealth III – электронный ключ, предназначенный для эффективной защиты локального программного обеспечения. Он выполнен па базе защищенного микроконтроллера, обладает EEPROM-памятью объемом 2048 байтов и выпускается только в варианте US B.

В Guardant Stealth III реализованы симметричные и однонаправленные алгоритмы преобразования данных. Возможно создание до 78 аппаратных алгоритмов в одном ключе. Технология защищенных ячеек, реализованная в Stealth III, расширяет возможности по хранению и управлению данными и аппаратными алгоритмами. Также ключ поддерживает механизм безопасного удаленного обновления TRU.

Guardant Net III – электронный ключ для защиты программ, работающих в компьютерных сетях. Ключ выполнен на базе защищенного микроконтроллера и оснащен EEPROM-памятью объемом 2048 байтов. Guardant Net III – это полный аналог Guardant Stealth III с дополнительными функциями, которые обеспечивают работу в сети.

Ключ содержит симметричные и однонаправленные аппаратные алгоритмы. Поддерживает технологии защищенных ячеек и TRU, а также основные возможности электронных ключей предыдущих поколений. Поддерживаемые сетевые протоколы – TCP/IP или любой из интерфейсов NetBIOS.

Сетевой ключ вместе со специальной программой – менеджером лицензий – устанавливается на сервер или на одну из рабочих станций в сети. Защищенная программа опрашивает электронный ключ при помощи сетевого протокола. С помощью сетевых ключей можно также ограничить доступ неавторизованного персонала к ключу защиты. Сервер с ключом может располагаться в отдельной комнате, куда имеет доступ только администратор информационной системы.

Использование сетевых ключей позволяет снизить стоимость защиты, так как для защиты всего программного обеспечения в локальной сети достаточного одного ключа Guardant Net III. Хотя стоимость сетевых ключей выше локальных, при пересчете на количество защищенных копий ПО получается, что сетевые ключи значительно экономичнее.

Guardant Stealth III Sign – новая модель в семействе Guardant. Это электронный ключ для надежной и эффективной защиты компьютерных программ от нелегального копирования. Он сделан на современной аппаратной платформе, основой которой являются высокопроизводительные 32-разрядные RISC-микроконтроллеры. Ключ оснащен энергонезависимой EEPROM-памятью объемом 4 Кбайта.

Guardant Stealth III Sign поддерживает все возможности ключей Stealth III и обладает новыми, уникальными характеристиками. Это быстрый, защищенный электронный ключ. Благодаря аппаратной реализации алгоритма электронной цифровой подписи Stealth III Sign устанавливает новый уровень стойкости и предлагает новые защитные механизмы. Stealth III Sign работает в 10 раз быстрее Guardant Stealth III за счет усовершенствованного протокола обмена и новой аппаратной платформы.

Guardant Stealth III Time – старшая модель в линейке электронных ключей Guardant, предназначенная для защиты локального программного обеспечения. Обладает всеми возможностями Stealth III Sign, а также имеет часы реального времени и независимый источник питания.

Параметры исполнения аппаратных алгоритмов (функций шифрования и ЭЦП) привязаны к показаниям часов внутри электронного ключа, и за счет этого выполняется надежное лицензирование по времени. Если установленное в аппаратном алгоритме время еще не наступило или уже прошло, то выполнение аппаратного алгоритма блокируется.

Сочетание аппаратного алгоритма электронной цифровой подписи и часов реального времени позволяет создавать на основе Guardant Stealth III Time стойкие защитные механизмы и надежно лицензировать программное обеспечение по времени.