Все, что следует знать о безопасной загрузке

С увеличением числа подключенных устройств возрастает необходимость в обеспечении защиты данных встраиваемых систем. В качестве первой меры на этом пути применяется безопасная загрузка (Secure Boot). Мы рассмотрим наиболее важные вопросы ее реализации на примере одного из распространенных процессоров в современной электронике — i.MX6 от компании NXP Semiconductors.

Натан Падуин (Nathan Padoin)

Что такое «безопасная загрузка»?

Процесс Secure Boot[1] позволяет аутентифицировать загрузочные образы и код операционной системы (ОС) на аппаратном уровне до того, как они получат разрешение на использование при фактической загрузке. Оборудование предварительно настроено таким образом, чтобы воспринимать только аутентифицированный код, сгенерированный с помощью набора удостоверений защиты. Безопасная загрузка гарантирует, что программа инициализации и ОС — те самые версии от производителя, в которые не были внесены изменения злоумышленником или вредоносным процессом.

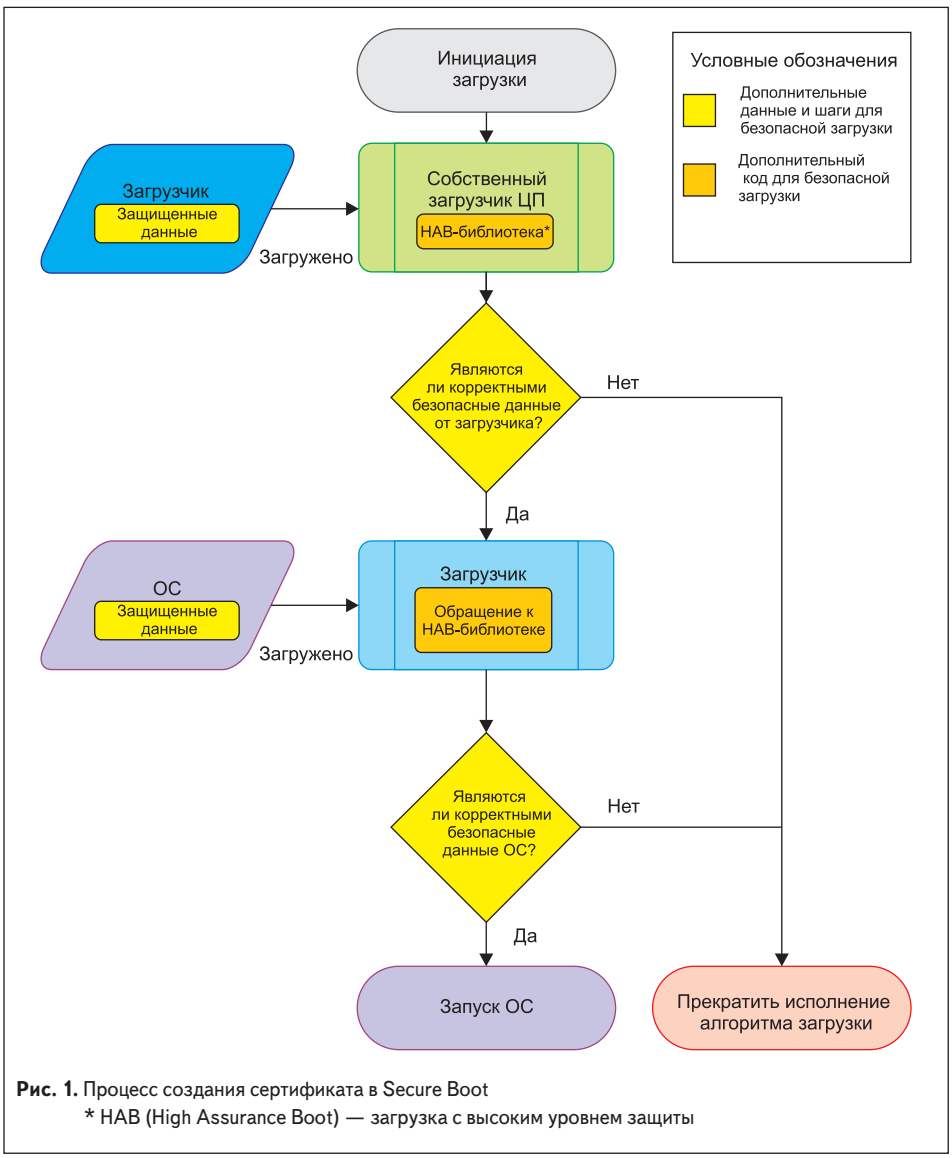

Рис. 1. Процесс создания сертификата в Secure Boot
* HAB (High Assurance Boot) — загрузка с высоким уровнем защиты

В любом однопользовательском устройстве Secure Boot является важным средством. Особенно заметна роль безопасной загрузки в электронных устройствах, предназначенных, например, для чтения электронных книг. В их составе часто применяется процессор i.MX6, например i.MX6 Solo или DualLite со встроенным контроллером дисплея E-Ink. Поскольку процессор i.MX6 специально создан для устройств чтения электронных книг, а не для компьютерных вычислений общего типа, в таких приложениях при загрузке используется защищенная среда Linux.

Однако не во всех случаях безопасная загрузка однозначно востребована. В частности, ее применение при включении телефона, работающего под управлением ОС Android, ограничивает возможности запуска конечным пользователем заказных программ. Как бы то ни было, Secure Boot препятствует несанкционированной загрузке операционной системы или стороннего загрузчика на пользовательское устройство.

Как осуществляется безопасная загрузка i.MX6

После создания загрузочных образов программ в устройствах на базе процессора i.MX6 процесс Secure Boot генерирует набор защищенных ключей в соответствии с SSL-сертификатом, созданным для этой цели (рис. 1).

В дальнейшем такие ключи понадобятся при создании защищенного набора команд, которые

[1] Secure Boot — протокол, являющийся частью спецификации UEFI (интерфейса между операционной системой и микропрограммами, управляющими низкоуровневыми функциями оборудования). Задача Secure Boot заключается в проверке подписи выполняемых UEFI-образов, для чего в ней предусмотрена асимметричная криптография. Secure Boot не является обязательным протоколом для реализации производителями.

скомпилированы и добавлены к загрузочному образу определенной программы с помощью инструментов от поставщика процессора. На следующем этапе процессор воспользуется начальным загрузчиком и проверит данные сертификата, сгенерированные средствами компиляции Secure Boot.

Защищенные команды станут выполняться только в том случае, если данные ключей в загрузочном образе операционной системы в точности совпадут с данными ключей, хранящимися в защищенном хранилище в процессоре. Далее он проверит криптографический хэш образов на соответствие тем, что определены защищенными командами. Если они совпадают, процессор загрузит и выполнит образ программы.

При прохождении этого процесса через внутренний загрузчик центрального процессора (ЦП) у пользователя имеется возможность обратиться в библиотеку Secure Boot из своего загрузчика кода. Это позволяет загружать образ операционной системы и проверять ее подлинность тем же способом, которым загрузчик ЦП устанавливает подлинность загрузчика программного обеспечения.

К концу этого процесса ОС загрузится в проверенной защищенной среде. Можно быть полностью уверенным, что это допустимая загрузка, поскольку каждый ее этап прошел проверку на аутентичность с помощью хэширования ключей в процессоре.

Настройка Secure Boot

Корневые ключи генерируются посредством SSL-сертификата, хэшируются и записываются в ЦП в результате однократного программируемого и необратимого процесса. Как только в процессор был установлен такой ключ, его нельзя изменить, что служит одной из гарантий безопасности.

Поступающий образ загрузки помечается с помощью этого ключа, и данные, полученные при подписи, объединяются с образом. Процессор сверяет поступающий ключ образа со своим ключом и, если они совпадают, сверяет образ с ключом, только что согласованным с процессором. Если они соответствуют друг другу, образ выполняется. Так выстраивается цепочка от загрузчика ЦП к загрузчику операционной системы. Существуют и другие особенности Secure Boot, но для простоты мы ограничимся примером с процессором i.MX6.

В этом процессе используются инструменты для подписи кода CST (Code Signing Tools) и средство MfgTool (см. рис. 2), которые предоставляются компанией NXP для Secure Boot и разработки приложений. Набор CST служит для создания сертификатов подписи, а также для данных Secure Boot, добавляемых в код загрузчика операционной системы, и для защищенных данных, записанных путем пережигания плавких перемычек в ЦП.

На устройстве, выполненном на основе i.MX6, при безопасной загрузке применяется средство MfgTool для записи защищенных данных в процессор на производстве и для загрузки и выполнения кода.

Аппаратная поддержка безопасности у процессора i.MX6

В аппаратной реализации процессора i.MX6 имеется ряд встроенных специализированных механизмов безопасности, наиболее важными из них представляются одноразовые плавкие перемычки для записи поступающего ключа. После пережигания они не подлежат восстановлению, и хэш-ключ становится постоянным и неизменным. Однако существует возможность объединить в один хэш-ключ несколько ключей. Следовательно, можно аннулировать взломанный ключ, что является существенным требованием встраиваемых систем.

Еще одним средством обеспечения безопасности системы является внутренний загрузчик ЦП — статический фрагмент кода, который также прошел проверку на безопасность. Таким образом осуществляется поддержка цепочки безопасности вплоть до уровня операционной системы.

Процессор i.MX6 имеет и встроенный ускоритель аппаратного криптографического алгоритма. Исполнение таких алгоритмов, как хэширование симметричного алгоритма блочного шифрования (Advanced Encryption Standard, AES) и Triple DES, SHA1 и SHA256, может ускоряться процессором, что значительно быстрее позволяет выполнять операции по обеспечению безопасности.

Возможные проблемы безопасной загрузки

Наиболее очевидная и требующая решения проблема в Secure Boot — обеспечение собственной безопасности. Если ключи утеряны, злоумышленник может подписать свой код в соответствии с ключом, который находится в процессоре. Таким образом, в дополнение к аппаратным средствам необходимо создать условия для безопасной записи ключа.

Другая чрезвычайно важная проблема заключается в том, что процессор, сконфигурированный для безопасной загрузки, не загрузится, если у него отсутствует образ с правильной подписью. Следовательно, любые ошибки, возникшие при прожигании хэш-ключа в процессоре, могут привести к тому, что он перестанет запускать код из-за несоответствия прожженному хэшу. В этом случае процессор нельзя уже будет использовать по назначению.

Напротив, в защищенный процессор невозможно загрузить сторонний код, что позволяет безопасно загружать код с накопителей, например с SD-карт, флэш-памяти NAND, или использовать другие режимы загрузки программного обеспечения в процессор путем загрузки образа через USB-порт.

Итак, все стадии по подготовке оборудования и процессора должны быть надежно защищены. Следует также убедиться, что загрузчик подготовлен к прохождению этих стадий. А значит, он должен заходить в библиотеку Secure Boot на процессоре, чтобы аутентифицировать каждый следующий этап в цепочке загрузки.

Неполная блокировка

Безопасная загрузка защищает не всю систему — только программное обеспечение запускаемой операционной системы. В результате злоумышленники могут написать вредоносное программное обеспечение Linux, работающее поверх ОС, после успешной загрузки, и тогда возникнет угроза безопасной работе всей системы в целом.

Аутентификация Secure Boot

При необходимости обеспечить полную безопасность имеется возможность осуществлять проверку подлинности отдельных частей файловой системы и другого кода. Запущенный на i.MX6 процесс Secure Boot работает по принципу определенных фрагментов памяти с определенным криптографическим хэшем и соответствующей информацией о подписях. В таком случае можно загружать корневую файловую систему ОС и другие файлы ключей в заданную область памяти вместе с корректным набором защищенных команд, что при необходимости позволит аутентифицировать любые другие части системы.

В заключение мы поделимся несколькими полезными рекомендациями по использованию Secure Boot для устройств, выполненных на базе процессора i.MX6.

1. Обеспечение безопасности всего процесса

При использовании безопасной загрузки с помощью Secure Boot следует убедиться, что связанные процессы работают с ней сообща. Утечка ключей нарушает созданную систему безопасности.

2. Высокий уровень шифрования

Убедитесь, что используемые алгоритмы шифрования соответствуют современным требованиям и пригодны для решения поставленной задачи.

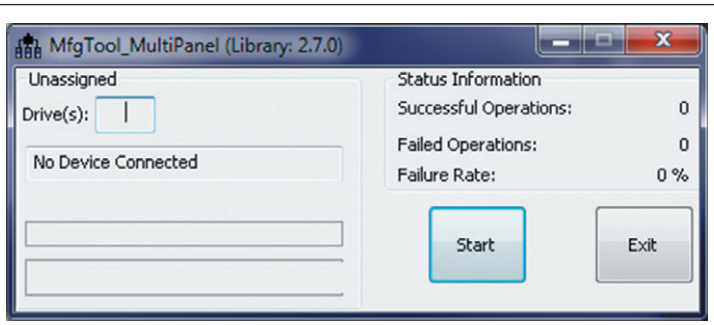

Рис. 2. Окно для работы со средством MfgTool, которое используется для загрузки подписанного кода на устройство

Поскольку Secure Boot для устройств на процессоре i.MX6 поддерживает несколько старых и взломанных комбинаций, есть некоторая вероятность создания не вполне надежных ключей.

3. Тщательная проверка кода

Для обеспечения полной безопасности приложения необходимо, чтобы остальная часть кода в загрузчике, ОС и другом ПО была корректно написана с учетом нужд Secure Boot и не ухудшала требований к безопасности.

На каждом этапе процесса загрузки должен проверяться каждый последующий этап перед его непосредственным выполнением. Если этого не сделать или сделать частично, безопасный вызов того или иного процесса не гарантируется.

4. Поэтапная аутентификация

Для полной гарантии безопасности следует выполнить аутентификацию как можно большего объема загружаемого кода и удостовериться, что он соответствует методам, установленным для библиотек. Secure Boot может только проверять подписи, и любой подписанный образ воспринимается процессором как защищенный.

Убедитесь, что каждая отдельная часть написанного кода вызывается в процессоре в библиотеку Secure Boot. Обращение в нее позволяет продолжить аутентификацию образов, поскольку большинство плат с i.MX6 проходит многоэтапный процесс загрузки: собственный загрузчик ЦП загружает SPL; в свою очередь, SPL загружает ПО, осуществляющее загрузку операционной системы. Чтобы каждый из указанных этапов был безопасным, необходимо его аутентифицировать на предыдущем шаге.

5. Правильная аутентификация процесса загрузки

Требуется, чтобы написанный код действительно выполнял безопасную загрузку и аутентификацию каждого следующего шага.

U-Boot — наиболее распространенный загрузчик для i.MX6. Эта программа поддерживает Secure Boot на процессорах i.MX6. U-Boot следует корректно настроить, что не так сложно. Кроме того, когда большая часть работы уже выполнена за программиста, вероятность ошибки уменьшается. ■