

Факультативный материал
для самостоятельного ознакомления

(По материалам портала BI.ZONE)

Насколько прочно аппаратное обеспечение (АО)?

Насколько прочно АО?

В 1988г. «червь» Морриса менее чем за день «положил» всю сеть ARPANET (прообраз сети Интернет). Вирус был написан студентом Корнельского университета в исследовательских целях и использовал известные уязвимости в ПО. Ущерб от незапланированно масштабной атаки исчислялся десятками миллионов долларов. Это стало одним из первых серьезных потрясений цифрового мира.

Нельзя сказать, что специалистам тех лет не хватало квалификации, чтобы создавать безопасное ПО. Другим был образ мышления: о безопасности никто не задумывался, не было понимания, зачем тратить на нее деньги, время и ресурсы.

Насколько прочно АО?

С тех пор прошло много времени, осведомленность специалистов - программистов, администраторов, руководителей - значительно выросла. Стала очевидной громадная разница между просто работающим кодом и безопасным кодом. Появились техники противодействия эксплуатации, повсеместно применяются практики безопасной разработки, регулярные проверки кода и многое другое.

На формирование нового типа мышления ушло много времени, были понесены колоссальные убытки - процесс оказался болезненным. Зато именно образ мышления и соответствующая культура разработки, сформированные путем дорогостоящих ошибок, дают теперь результаты, а не какие-то модные современные технологии.

Жизнь налаживается, ПО становится безопасней, а эксплуатировать ошибки в ПО все сложнее.

Что может пойти не так?

«Железо» (АО)!

Парадоксальная ситуация складывается с отношением к безопасности АО

Насколько прочно АО?

АО - корень доверия и фундамент всей системы. Так ли это?

Функционирование вышележащих слоев опирается на его работу. Компрометация «железа» неминуемо ведет к компрометации всей системы, каким бы безопасным ни был софт.

Например, если производитель положит в основу своей разработки уязвимый микроконтроллер, он впустую потратит ресурсы на создание защитных мер в ПО: атакующий может легко обойти их, применив атаку на интегральную схему.

Безопасность АО находится в плачевном состоянии. Можно провести прямые параллели с состоянием безопасности ПО 20 лет назад: надлежащий аудит отсутствует, редкие специалисты понимают, как разрабатывать защищенное «железо», не сформирован образ мышления, подразумевающий необходимость проверки безопасности АО.

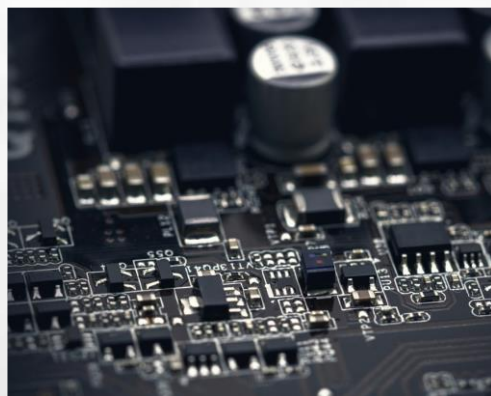
Ситуация усугубляется тем, что уязвимости в АО нельзя исправить выпуском обновления, как это делается с софтом. Производитель здесь не поможет: ошибки в АО останутся там на весь срок эксплуатации, а это может быть и десять лет, и пятнадцать, и больше. Если в АО обнаружат уязвимость, пользователю придется выбирать: либо заменить АО (что может быть очень дорого), либо работать с уязвимыми устройствами (что неприемлемо для любой инфраструктуры).

Насколько прочно АО?

Для устранения неоднозначности следует рассматривать компьютерную систему как иерархию из трех уровней:

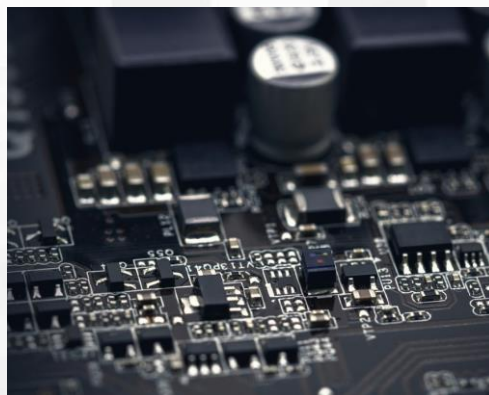
software - программное обеспечение;
firmware - встроенное ПО (прошивка);
hardware - аппаратное обеспечение.

У современного «железа» такие же проблемы, что и у софта:
трояны, бэкдоры, недокументированные (недекларированные)
ВОЗМОЖНОСТИ



Насколько прочно АО?

Если «железо» не защищено должным образом,
программные способы защиты **бесполезны.**



Атаки на встраиваемые системы

Аппаратные уязвимости Spectre и Meltdown, раскрытые в начале 2018 г., вызвали большую шумиху и затронули миллионы пользователей и организаций. Однако, несмотря на бесчисленные обсуждения, убытки от них не выглядят катастрофическими.

Даже репутация компаний Intel и AMD, в процессорах которых нашли уязвимость, пострадала не сильно. Так опасны ли атаки на встраиваемые системы для бизнеса? Или весь вопрос только в «правильном» и «неправильном» подходе к «железу», и эта проблема беспокоит лишь разработчиков, сражающихся за право считаться более технически подкованными?

К сожалению, это не так. Действительно, успешные аппаратные атаки попадают в поле зрения не каждый день: многие организации предпочитают публично не заявлять о таких инцидентах. Тем не менее известны случаи, когда недостаток внимания к безопасности встраиваемых систем приводил к серьезнейшим последствиям.

Осветим наиболее показательные примеры успешных аппаратных атак и предположить, кто может оказаться следующей целью злоумышленников.

Атаки на встраиваемые системы

«встраиваемая система» это совокупность низкоуровневого встроенного ПО (прошивка) и аппаратного обеспечения, которые работают в тесной взаимосвязи. Рассматривать безопасность этих составных частей по отдельности не имеет смысла.

- в 2004 г. Европейская медиакомпания Canal Plus оценила свои потери из-за пиратства в 1,2 млрд. долларов.
- по данным Imaging Supplies Coalition (ISC), годовой оборот контрафактных тонеров и картриджей для печатающих устройств по всему миру достигает 3 млрд. долларов.
- по данным ассоциации UK Interactive Entertainment (UKIE), в 2010 г. убыток, нанесенный пиратством индустрии игровых консолей, составил около 2,3 млрд. долларов.
- согласно отчету Европейской группы по обеспечению безопасности банкоматов (EAST), в 2017 г. количество атак в Европе выросло на 231%.

В связи с активным развитием *интернета вещей* и *промышленного интернета* у злоумышленников появились новые направления для атак.

Атаки на встраиваемые системы

Многие *автомобили* сегодня поддерживают подключение к удаленным сервисам через интернет, а управление практически всеми системами автомобиля (подушки безопасности, тормозные и аудиосистемы, круиз-контроль и др.) осуществляется с помощью электронных блоков управления (ECU), соединенных CAN-шиной.

Проанализировав прошивку электронных блоков, злоумышленник может найти цепочку уязвимостей, позволяющую провести удаленную атаку по сети. Такие возможности эксплуатации несут серьезную угрозу как безопасности пассажиров, так и репутации производителя.

Смартфон - один из главных инструментов современного человека. Он выполняет столько функций, что порой в нем хранится чуть ли не вся жизнь владельца: личная переписка, фотографии, данные банковских карт и многое другое. Неудивительно, что вопросами безопасности смартфонов занимаются с первого дня их выхода на рынок.

Однако зачастую эта проблема считается индивидуальной заботой пользователей, в то время как смартфон многих работников компаний - окно в корпоративную сеть и способ быстрого доступа к защищаемой информации. Такая важная роль этого цифрового устройства предъявляет очень высокие требования к безопасности его аппаратно-программного обеспечения и требует от производителя ответственного подхода к разработке.

Классификация атак на встраиваемые системы

1. Атаки на внешние протоколы

- Атаки на проводные протоколы
- Атаки на беспроводные протоколы

2. Атаки на встроенное программное обеспечение

- Обратная разработка встроенного ПО
- Обратная разработка конфигурационной прошивки ПЛИС
- Эксплуатация логических уязвимостей
- Эксплуатация бинарных уязвимостей
- Закладки в ПО

3. Атаки на принципиальную электрическую схему

- Обратная разработка печатной платы
- Пассивные и активные атаки на внутрисхемные сигналы
- Аппаратные закладки в устройстве

Классификация атак на встраиваемые системы

4. Атаки на интегральные схемы

- Атаки по второстепенным каналам
 - по времени
 - по энергопотреблению
 - по электромагнитному излучению
- Атаки методом индуцированных сбояв
 - по тактирующему сигналу
 - по питанию
 - оптическим импульсом
 - электромагнитным импульсом
 - путем смещения базового напряжения на подложке
- Инвазивные атаки
 - обратная разработка ИС
 - микрозондовый анализ
 - модификация кристалла ИС
- Аппаратные закладки в ИС

Атаки на внешние протоколы

Протоколы задают формат взаимодействия между отдельными устройствами и компонентами и могут быть определены как минимум на двух уровнях: логическом и физическом.

На логическом уровне определяется формат полей сообщения, способ кодирования данных, перечень поддерживаемых команд и, возможно, диаграмма состояний. Физический уровень - фундамент для логического уровня: на нем определяются параметры, форма и вид модуляции или манипуляции сигнала, который переносит сообщение.

Именно физический уровень ранее был барьером для атакующего: для взаимодействия с ним нужно специальное оборудование, а купить или самостоятельно создать его могли единицы. Сегодня ситуация изменилась - появилось множество доступных и недорогих устройств для работы по всевозможным протоколам.



Атаки на внешние протоколы

Атаки на внешние протоколы (USB, Bluetooth, CAN и другие)-наиболее высокоуровневые атаки на устройство и, как правило, наиболее простые с точки зрения ресурсов, которые необходимы атакующему.

Объясняется это просто: большинство протоколов документированы, для них существуют готовые адаптеры, модули приема и передачи, работа с ними поддерживается различным ПО.

Кроме того, для атак такого рода достаточно доступа к среде передачи сообщений (кабелю, шине и др.), а физического взаимодействия с устройством не требуется - неоспоримое преимущество для атакующего.

С другой стороны, такие атаки довольно ограничены и могут быть эффективными лишь в отсутствие должных мер защиты.

Атаки на внешние протоколы

Для проведения атаки злоумышленник анализирует внешние коммуникации целевого устройства, определяет используемые протоколы, разбирает передаваемые команды и данные, а в случае реализации активных атак - подготавливает собственное программно-аппаратное решение для взаимодействия с целевым устройством.

Большинство протоколов документированы. Для атак на них злоумышленнику не нужно исследовать внутренние алгоритмы, заложенные в программное и аппаратное обеспечение целевого устройства. А вот атаки на защищенный протокол требуют большей подготовки: атакующий должен изучить его структуру, прежде чем он сможет получать передаваемые по протоколу данные и взаимодействовать с целевым устройством с его помощью. Порой необходимо провести анализ встроенного ПО, чтобы понять строение протокола.

Атаки на внешние протоколы

Важно отметить, что большинство протоколов разрабатывались с прицелом на быструю и надежную передачу данных, и с этой задачей они справляются хорошо. Однако при разработке не уделялось должного внимания их безопасности. В результате во многих известных протоколах все сообщения, принятые по какому-то каналу, считаются доверенными или передаются в незашифрованном виде (особенно часто такое бывает в случае проводных протоколов).

В классификации отметим два вида протоколов и, соответственно, интерфейсов в зависимости от того, как передается сообщение:

- с помощью электрического сигнала - проводные протоколы;
- с помощью электромагнитных волн — беспроводные протоколы.

Атаки на внешние протоколы

Интересный факт

Модуляция сигнала - изменение параметров несущего сигнала в соответствии с аналоговым модулирующим сигналом.

Пример — частотная модуляция (FM), которая используется в радиовещании.

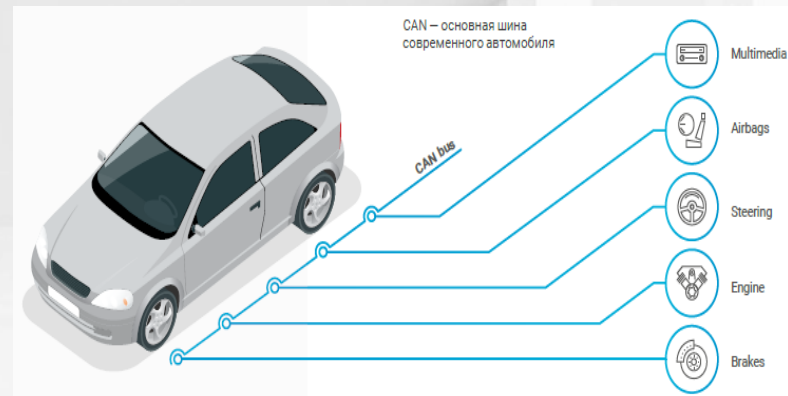
Манипуляция сигнала - частный случай модуляции: в качестве информационного сигнала берется последовательность дискретных значений.

Пример — квадратурная фазовая манипуляция (QPSK), которая используется в системах сотовой связи CDMA и спутниковом телевидении.

Атаки на внешние протоколы (проводные протоколы)

Интересный факт

Одноплатный компьютер Raspberry Pi, который часто используют для работы с проводными протоколами и прототипирования электронных устройств, разрабатывался как бюджетная система для обучения информатике.



Основная идея атак на проводные протоколы заключается в перехвате передаваемых сообщений, а также в подделке и отправке нелегитимных сообщений на устройство.

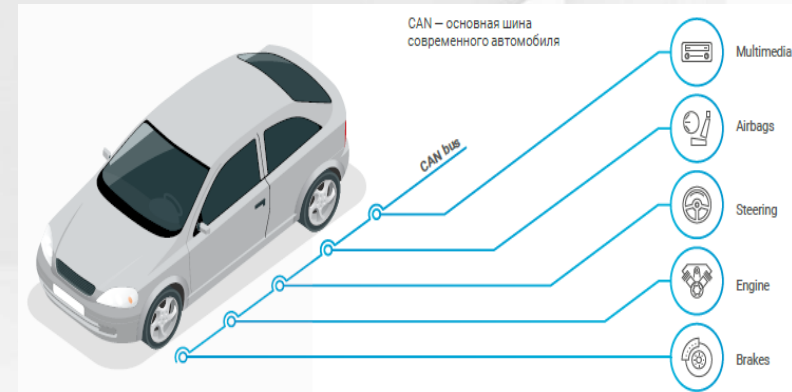
Несколько десятилетий назад эта задача требовала серьезной инженерной подготовки, однако с появлением одноплатных компьютеров (Raspberry Pi, BeagleBone и др.) и отладочных плат с использованием различных микроконтроллеров (Arduino, Teensy и др.) ситуация изменилась. Помимо получившейся удобной связки «персональный компьютер - отладочная плата», задачу сильно упрощают:

- разнообразие доступных плат расширения, адаптеров на все случаи жизни;
- множество готовых библиотек;
- интуитивно понятные среды разработки, которые практически не предъявляют требований к уровню подготовки программиста;
- доступность специальных инструментов, которые раньше использовались исключительно профессионалами (осциллографы, логические анализаторы).

Атаки на внешние протоколы (проводные протоколы)

Интересный факт

Вероятность невыявленной ошибки в CAN-шине оценивается как $4,7 \times 10^{-11}$ степень).



Современные протоколы работают на высоких частотах, требуют точной синхронизации и быстрого отклика (скорости реакции). Иногда даже микроконтроллеры, работающие на частотах в сотни МГц, не способны обеспечить стабильного взаимодействия - в таком случае для соответствия высоким требованиям используют программируемые логические интегральные схемы (ПЛИС). Ранее их стоимость была серьезным барьером для любителей, теперь же сравнима со стоимостью отладочных плат с микроконтроллерами.

Все это заметно снижает порог входа для атакующего.

Атаки на внешние протоколы (проводные протоколы)



Яркий пример атаки на проводные протоколы - управление критически важными системами автомобиля посредством CAN-шины. CAN - основная шина современного автомобиля, используется повсеместно, а с 2008 г. обязательна для всех транспортных средств, продаваемых в Европейском союзе. Основной упор при ее создании делался на надежность передачи сообщений, вероятность необнаруженной ошибки исключительно мала.

Однако разработчики не предусмотрели аутентификации между электронными блоками управления на шине: они все по умолчанию считаются доверенными.

В таких условиях нарушителю стоит лишь получить доступ к шине, и автомобиль попадет под его полный контроль. Один из самых реалистичных сценариев атаки - установка в автомобиль аппаратной или программной закладки в обслуживающих центрах (автомойка, сервисный центр и др.) для удаленного управления транспортным средством.

Атаки на внешние протоколы (проводные протоколы)



Атака на банкомат методом black box

Другой известный пример - атака методом blackbox на банкоматы. Банкомат разделен на защищенную зону, где установлен диспенсер с банкнотами, и сервисную часть, где находится управляющий компьютер. Получить доступ к диспенсеру непросто: он помещен в сейф с толстыми металлическими стенками и сложным замком.

А вот вскрыть замок сервисной зоны можно без специальных инструментов, и этим пользуются злоумышленники. Управляющий сигнал на выдачу денежных средств передается от ПК к диспенсеру по проводным интерфейсам, как правило USB-шине (SDC-шина у старых моделей банкоматов).

Атакующему достаточно изучить формат используемых команд и собрать устройство, которое будет вместо управляющего ПК подключаться к диспенсеру и подавать сообщение на выдачу наличных.

Атаки на внешние протоколы (проводные протоколы)



Атака на банкомат методом black box

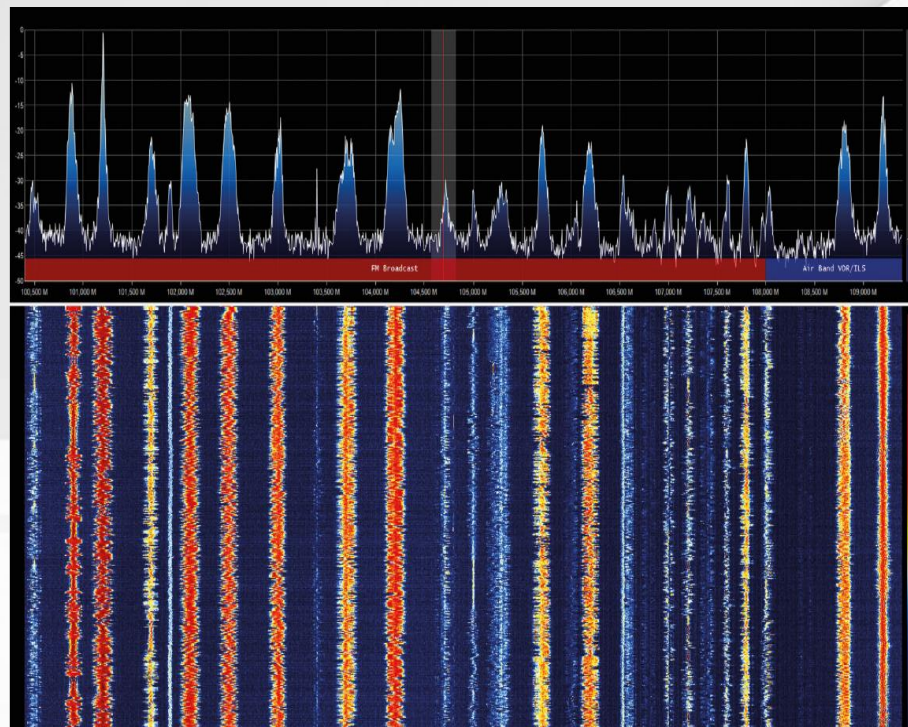
Меры защиты от атак на проводные протоколы

Для защиты от подобных атак необходимо реализовывать криптографически защищенные протоколы с аутентификацией взаимодействующих узлов, защитой от подделки и повторной отправки сообщений.

Атаки на внешние протоколы (беспроводные протоколы)

Интересный факт

Множество автомобильных систем PKES (passive keyless entry and start) уязвимы для атаки методом «длинная рука». Ее проводят с помощью двух модулей, которые обмениваются сигналами друг с другом. Первый модуль находится в нескольких метрах от ключа-брелока, второй - рядом с автомобилем, а расстояние между модулями может достигать пары сотен метров.



Спектр радиосигнала

Первый модуль считывает данные с ключа и транслирует сигнал на второй модуль, второй модуль ретранслирует его на автомобильную сигнализацию. Запрос от авто к брелоку передается в обратной последовательности. Так PKES заставляют поверить, что легитимный владелец просит открыть и завести авто, что она и делает, к радости злоумышленников.

Атаки на внешние протоколы (беспроводные протоколы)

Беспроводные протоколы нашли применение всюду, от радиоуправляемых игрушек до военных систем защищенной радиосвязи.

Среди всего разнообразия можно выделить несколько протоколов, которые тесно связаны с компьютерными системами и постоянно используются в повседневной жизни, например Wi-Fi и Bluetooth.

Ввиду доступности оборудования, ПО и спецификаций безопасность этих протоколов довольно хорошо исследована специалистами. Описание обнаруженных уязвимостей, примеры атак и ПО можно легко найти в открытом доступе.

Исследование безопасности других протоколов бывает связано со сложностями: например, порой необходимое оборудование недоступно простым пользователям, спецификация протоколов защищена, использование определенных частот ограничено законодательством. Это замедляет работу независимых специалистов - а пока бреши в защите не обнаружены, у отрасли создается ложное ощущение безопасности. Усугубляет ситуацию то, что ограничения останавливают только добросовестных исследователей, а злоумышленники продолжают искать уязвимости.

Атаки на внешние протоколы (беспроводные протоколы)



SDR-приемопередатчик

Интересный факт

В основе работы современных SDR лежат принципы цифровой обработки сигналов (ЦОС). Одно из фундаментальных утверждений в этой области - теорема Котельникова - в англоязычной литературе называется теоремой Найквиста - Шеннона.

Проводить атаки на беспроводные протоколы стало проще с появлением программно-определяемого радио (SDR). Оно изменило способ работы с радиоэфиром: современные SDR могут не только прослушивать эфир в пассивном режиме, но и сами передавать сообщения, что злоумышленники используют для активных атак. В некоторых случаях достаточно записать легитимный сигнал, содержащий команду, и в нужный момент передать его обратно в эфир, чтобы управлять принимающим устройством (replay-атака). SDR стоит недорого, софт для обработки принятых сигналов и формирования собственных распространяется бесплатно в исходных кодах и удобен в использовании - все это снижает порог вхождения для атакующего.

Радиосигнал передается в общей для всех среде, и это открывает большие возможности для проведения атак. Интересный пример - подмена базовой станции. Согласно алгоритму работы GSM, сотовый телефон выбирает станцию с наиболее сильным сигналом. Атакующий создает ложную базовую станцию и переключает на себя абонентов, находящихся поблизости. Это позволяет ему прослушивать разговоры абонентов и читать их СМС.

Атаки на внешние протоколы (беспроводные протоколы)



SDR-приемопередатчик

Другой пример - установка радиопомех. Такое воздействие на беспроводные протоколы активно используют вооруженные силы в ходе боевых действий – РЭБ – радиоэлектронная борьба.

Однако злоумышленники тоже могут применить эту атаку, чтобы нарушить целостность передаваемых данных - например препятствовать отправке сообщения тревоги от инкассаторского автомобиля к центру мониторинга.

Атаки на внешние протоколы (беспроводные протоколы)

Меры защиты от атак на беспроводные протоколы

Чтобы обезопасить себя от подобных атак, нужно использовать только криптографически защищенные протоколы с аутентификацией взаимодействующих узлов, защитой от подделки и повторной посылки сообщений.

Работа устройства в различных диапазонах, смена рабочих частот и применение широкополосных шумоподобных сигналов затрудняют радиоэлектронное подавление.

Атаки на встроенное ПО

Современные встраиваемые системы - это симбиоз аппаратного и программного обеспечения. Зачастую атаки на них преследуют единственную цель - получить код, реализующий функциональность устройства.



Встроенное ПО можно найти на различных уровнях функционирования устройства, от привычных приложений под управлением операционной системы (ОС) до микрокода процессора или кода из масочной памяти (ROM), «отлитой» в кремнии. Дополнительное разнообразие вносит и множество архитектур систем, начиная от классических, фон-неймановской и гарвардской, до совершенно уникальных. Чтобы в полной мере понимать значение тех или иных программных конструкций, необходимо знать, какая архитектура используется.

Процесс получения встроенного ПО сильно различается в зависимости от места его хранения и защитных мер, предусмотренных производителем для противодействия извлечению ПО. Если атакующий имеет дело с незащищенным устройством, зачастую ему достаточно подключить микроконтроллер или микросхему памяти к программатору и снять дамп.

А чтобы получить встроенное ПО из сертифицированного защищенного криптопроцессора, вероятно, потребуется комбинация инвазивных атак - их мы рассмотрим далее.

Получив код, атакующий анализирует его, чтобы извлечь заложенные алгоритмы или найти ошибки (уязвимости, англ. vulnerability), пригодные для последующей эксплуатации (exploitation). Уязвимости можно разделить на несколько групп, но самая критическая из всех - уязвимость нулевого дня (0-day). Это неустраненные ошибки, о существовании которых производитель не знает, поэтому не выпускает исправлений для них. В результате они присутствуют в последних версиях ПО, которые считаются наиболее защищенными. Для злоумышленника наибольший интерес представляют уязвимости нулевого дня, позволяющие провести удаленное выполнение кода (RCE): при успешной эксплуатации атакующий получит контроль над системой без физического доступа к ней.

Атаки на встроенное ПО

Обратная разработка встроенного ПО

Обратную разработку (reverse engineering) применяют, когда нужно понять принцип работы ПО с защищенным исходным кодом. Для этого атакующему нужно восстановить алгоритм из машинного кода, в который преобразуется написанная разработчиком программа. Сам процесс преобразования исходного кода в машинный необратим: часть высокоуровневой информации при этом теряется. Поэтому обратную разработку нельзя автоматизировать - здесь всегда требуется работа аналитика. Процесс анализа во многом зависит от того, в каком формате представлен машинный код. Исполняемые файлы, предназначенные для работы в рамках операционной системы, содержат множество полезной информации в своих служебных полях, что значительно упрощает исследование. Но так бывает далеко не всегда.

Например, встроенное ПО, работающее без использования ОС или под управлением ОС реального времени, хранится в памяти устройства в неструктурированном, «сыром» виде. Для анализа ПО в таком формате атакующий в первую очередь должен изучить спецификации на установленный микроконтроллер и компоненты устройства, чтобы определить карту памяти процессора и назначение данных в различных регионах памяти.

Интересный факт

Термины big-endian и littleendian, обозначающие порядок байтов, сперва не имели отношения к информатике. В сатирическом произведении Джонатана Свифта «Путешествия Гулливера» описаны вымышленные государства Лилипутия и Блефуску, между которыми много лет идет война из-за разногласия по поводу того, с какого конца следует разбивать вареные яйца. Тех, кто считает, что их нужно разбивать с тупого конца, в произведении называют big-endians («тупоконечники»), с острого - little-endians («остроконечники»).

Споры между сторонниками big-endian и little-endian в информатике также часто носят характер «религиозных войн». В компьютерный лексикон термины big-endian и littleendian ввел Д. Коэн (Danny Cohen) в 1980 г. в статье «On holy wars and a plea for peace» («О священных войнах и призыв к миру»).

Атаки на встроенное ПО

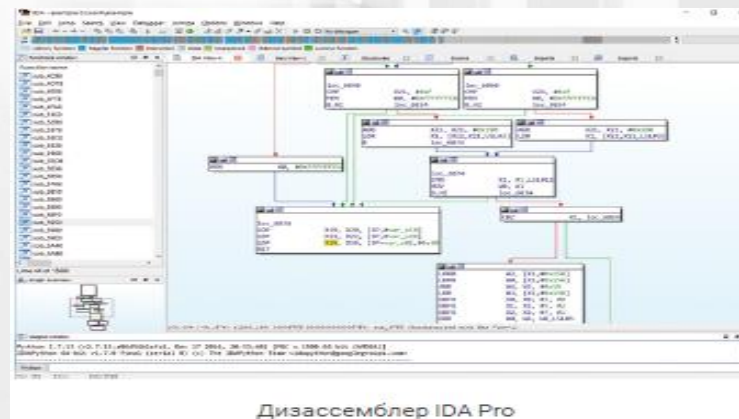
Обратная разработка встроенного ПО

Преобразование машинного кода в формат, пригодный для чтения человеком, производится *дизассемблером* (IDA Pro, Radare2 и др.). Для корректного дизассемблирования необходимо верно определить, где в бинарном дампе находятся код, где данные и какая архитектура набора команд (ISA) используется. В большинстве встраиваемых систем это будут хорошо известные архитектуры: ARM, MIPS, PIC, PowerPC и другие. Дизассемблеры отлично справляются с задачей их анализа.

Для некоторых существуют *декомпиляторы* (decompiler), например Hex-Rays Decompiler, JEB, способные выдавать C-подобный листинг, что существенно облегчает понимание кода. Если устройство использует нестандартную архитектуру процессора, может понадобиться написание собственного дизассемблера. Анализ нестандартной архитектуры - задача нетривиальная: иногда его нельзя провести без обратной разработки ИС процессора.

```
1 int64 __fastcall sub_B4F0(__int64 a1, __int64 a2)
2 {
3     __int64 v2; // x30
4     __int64 v3; // x20
5     __int64 v4; // x21
6     unsigned __int64 v5; // x19
7     __int64 v6; // x0
8     __int64 v7; // x1
9     int v8; // w19
10
11     v3 = a1;
12     v4 = a2;
13     v5 = ReadStatusReg(ARM64_SYSREG(3, 0, 4, 1, 0));
14     nullsub_1(v2);
15     sub_6044D8((__QWORD *)(&v5 + 16) + 1024i64) + 104i64;
16     v6 = sub_1AC1E0((__QWORD *)(&v5 + 16) + 1024i64, v4);
17     v7 = *(__QWORD *)(&v5 + 16);
18     if (v6)
19         v8 = 196610;
20     else
21         v8 = 196609;
22     sub_A2120((__QWORD *)(&v7 + 1024) + 104i64);
23     return sub_B2F8(0xBu, v8, v3);
24 }
```

Декомпилированный код



Дизассемблер IDA Pro

Атаки на встроенное ПО

Обратная разработка встроенного ПО

Существенно облегчают задачу обратной разработки встроенного ПО методы динамического анализа: отладка (debug) и эмуляция кода (emulation). Функции *отладки* используют сами производители устройств, когда устраняют неисправности в процессе разработки. Отладочные интерфейсы делятся на два вида:

- программные - реализуемые ОС;
- аппаратные - исполненные в составе ИС (например, JTAG).

Эмуляторы позволяют провести выполнение кода и оценить результаты его работы в полностью контролируемом окружении без использования оригинального устройства. Многие качественные эмуляторы под самые различные архитектуры находятся в открытом доступе и распространяются в исходных кодах (QEMU и др.).

Исследование встроенного ПО методом обратной разработки - зачастую первый этап в подготовке атаки на устройство. Это помогает правильно спланировать атаку, найти бинарные или логические уязвимости, а в некоторых случаях анализа прошивки достаточно для компрометации устройства.

Например, если она содержит жестко закодированный пароль суперпользователя, его извлечение позволит получить полный контроль над системой.

Меры защиты от обратной разработки встроенного ПО

Наиболее эффективная защита встроенного ПО от обратной разработки - противодействие получению кода.

Если же код получен, его обратная разработка - лишь дело времени и затраченных сил. Тем не менее существуют методы, которые позволяют затруднить анализ: удаление отладочной информации, обфускация кода, приемы антиотладки и анти-дизассемблирования.

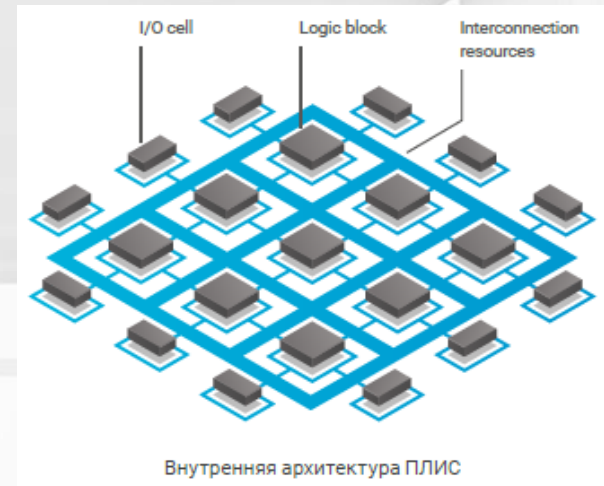
Атаки на встроенное ПО

Обратная разработка конфигурационной прошивки ПЛИС

С некоторым допущением можно считать встроенным программным обеспечением конфигурационную прошивку программируемой логической интегральной схемы (ПЛИС, англ. FPGA), хотя в ней содержатся данные, управляющие состоянием внутренних элементов ПЛИС, а не инструкции, выполняемые процессором.

Чтобы понять суть атаки на ПЛИС, необходимо представлять особенности этой интегральной схемы. Она служит удобным средством проектирования цифровой логики: если в классических ИС логика устройства жестко задается на этапе производства, то ПЛИС программирует сам пользователь. Для этого используются языки описания аппаратуры (HDL), такие как Verilog и VHDL.

По синтаксису они схожи с классическими языками программирования, но сильно отличаются по сути, так как призваны описать логику цифрового устройства, а не последовательно выполняемые инструкции.



В отличие от микроконтроллеров, ПЛИС может обрабатывать большое количество данных параллельно, точно соблюдает временные интервалы и отлично синхронизируется с внешними сигналами.

За счет этих преимуществ ПЛИС оказывается идеальным инструментом для критичных ко времени реакции и быстродействию операций, поэтому она часто применяется в военной, авиационной и космической отраслях.

Атаки на встроенное ПО

Обратная разработка конфигурационной прошивки ПЛИС

Цикл разработки под ПЛИС состоит из последовательности процедур:

разработка требований к будущему проекту,

- программирование логики на HDL-языке,
- синтез,
- оптимизация,
- размещение,
- трассировка,
- создание файла конфигурационной прошивки (bitstream).



Внутреннее устройство ПЛИС упрощенно можно описать следующим образом. Основную роль выполняют два элемента: программируемые макроячейки (logic blocks) и конфигурируемые соединительные ячейки (interconnection resources).

Первые содержат набор конфигурируемых цифровых вентилях (триггеры, LUT и др.), вторые определяют, в какой последовательности и каким образом коммутировать макроячейки. Также ПЛИС содержит целый ряд других компонентов: аппаратные умножители, системы фазовой автоподстройки частоты (PLL), схемы ввода-вывода (I/O cells) и др.

Чтобы определить, в каком режиме будут работать эти элементы, ПЛИС конфигурируется с использованием данных из файла bitstream. Обратная разработка конфигурационного файла ПЛИС позволяет извлечь алгоритмы, заложенные производителем в устройство, а при желании модифицировать их и использовать в своих целях.

Атаки на встроенное ПО

Обратная разработка конфигурационной прошивки ПЛИС

Зачастую для получения конфигурационной прошивки атакующему даже не нужно взаимодействовать с самой ПЛИС. Дело в том, что большинство современных ПЛИС не содержат микросхему ПЗУ, а хранят текущую конфигурацию в SRAM - быстродействующей энергозависимой памяти, содержимое которой будет потеряно при отключении питания. Как правило, для постоянного хранения конфигурации используется внешняя флеш-память, данные с которой с помощью специализированного протокола загружаются на ПЛИС при ее включении. В такой ситуации атакующему достаточно получить доступ к внешней памяти, чтобы добраться до файла bitstream.

В отличие от большинства наборов команд, используемых микроконтроллерами, формат bitstream обычно защищен и уникален для каждого производителя. Отсутствие открытой спецификации существенно усложняет анализ, но в последнее время появляются проекты в открытом доступе, которые ставят целью документировать формат и разработать ПО для анализа bitstream.

ПЛИС используют при реализации многих инновационных технологий. Процесс программирования для нее довольно затратен и требует привлечения высококвалифицированных специалистов, поэтому в случае атаки на ПЛИС речь идет, как правило, о краже интеллектуальной собственности и уникальных разработок.

Атаки на встроенное ПО

Обратная разработка конфигурационной прошивки ПЛИС

Меры защиты от обратной разработки конфигурационной прошивки ПЛИС

Распространенная мера защиты - шифрование bitstream. Ключ при этом хранится в ПЗУ небольшого размера внутри ПЛИС и прошивается на этапе программирования. Однако существуют способы обойти и такие меры защиты.

Атаки на встроенное ПО

Эксплуатация логических уязвимостей

Эксплуатация логических уязвимостей (logical vulnerability) - это намеренное использование ошибки в реализации ПО или в логике его работы. Уязвимости, позволяющие проводить такие атаки, возникают в результате некорректной обработки пограничных случаев, неправильной реализации логики переходов внутренних состояний и криптографических алгоритмов. Как правило, они не зависят от используемого языка программирования, микроархитектуры системы, бинарных форматов кода и данных и других низкоуровневых особенностей.

Обнаружить логические ошибки на этапе разработки сложно, как и заметить логические атаки во время работы ПО. При эксплуатации логических ошибок не повреждается память (memory corruption), программное обеспечение функционирует в точном соответствии с алгоритмом, описанном в исходных кодах ПО. Проблема лишь в том, что поведение системы отличается от поведения, ожидаемого программистом.

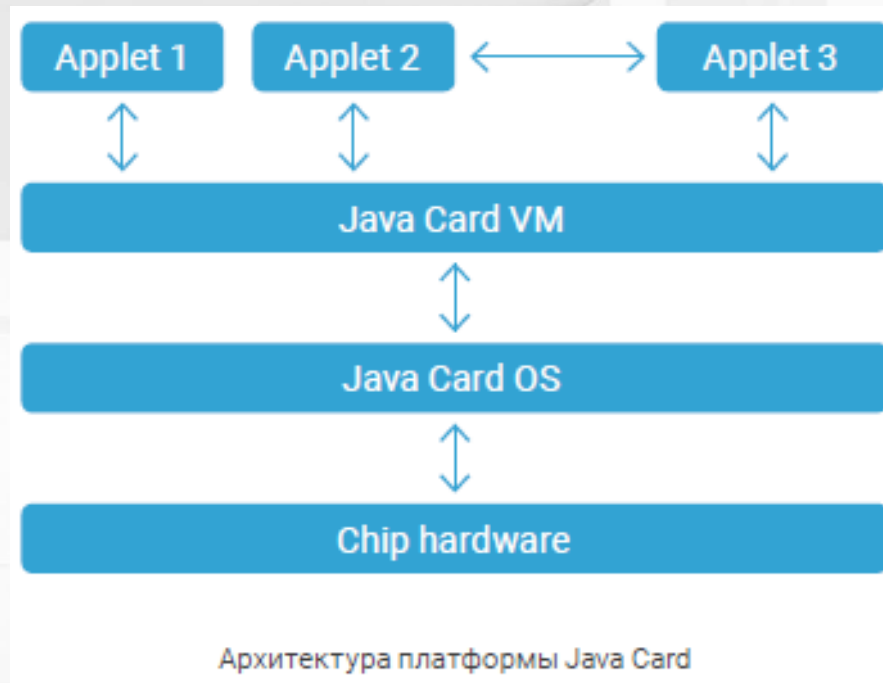
Интересный пример логической ошибки - уязвимость CVE-2017-5689 в реализации технологии Intel AMT. Эта технология предоставляет удаленный и внеполосный доступ для выполнения действий, которые обычно требуют физического доступа к компьютеру. С этим мощным инструментом можно удаленно изменять настройки и управлять безопасностью устройства в обход функций ОС, даже если оно выключено (но подключено к электросети). Найденная в Intel AMT уязвимость заключается в том, что фактически процедура авторизации принимает пустую строку за верный ответ вне зависимости от того, какой на самом деле пароль был установлен для доступа к системе.

Атаки на встроенное ПО

Эксплуатация логических уязвимостей

Другой иллюстрацией логических атак, эксплуатирующих слабости в реализации защищенного окружения, являются атаки с использованием апплетов (приложений) в экосистеме Java Card.

Эта платформа описывает стандартную среду исполнения на смарт-картах, чтобы один и тот же апплет мог работать на картах от различных производителей.



Атаки на встроенное ПО

Эксплуатация логических уязвимостей

Меры защиты от логических уязвимостей в ПО

Для выявления логических уязвимостей на этапе разработки необходимо проводить аудит исходного кода системы и тестирование логики работы ПО на правильную обработку пограничных случаев и нестандартных последовательностей команд и данных.

Код, написанный на Java, компилируется в байткод Java Card Virtual Machine (JCVM) и выполняется на смарт-карте под контролем встроенной ОС.

По спецификации Java Card апплеты, относящиеся к различным пакетам (package), не имеют доступа к данным друг друга (исключение - специально экспортированные объекты). Однако производители смарт-карт из-за ограниченных вычислительных ресурсов карты зачастую не реализуют достаточного количества проверок во время выполнения апплета, полагаясь на верификацию во время создания пакета. В некоторых случаях такой подход позволяет атакующему создать вредоносный апплет, эксплуатирующий слабости в реализации виртуальной Java-машины, и получить доступ к данным других апплетов, встроенной ОС и криптографическому материалу.

Интересный факт

CVE-2014-1266, или goto fail, - яркий пример логической уязвимости. Лишняя строка кода в функции верификации сертификата на iOS привела к тому, что часть запланированных проверок никогда не проводилась. В результате злоумышленник мог перехватывать и модифицировать пакеты в сессиях, защищенных SSL и TLS. Иными словами, эта уязвимость позволяла проводить MitM-атаку с подменой трафика.

Атаки на встроенное ПО

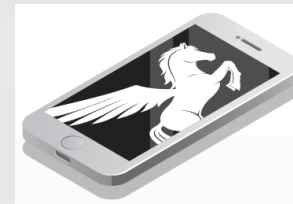
Эксплуатация бинарных уязвимостей

Интересный факт

Культовый учебный материал по эксплуатации бинарных уязвимостей – статья «Smashing the stack for fun and profit», опубликованная в электронном журнале Phrack в 1996 г.

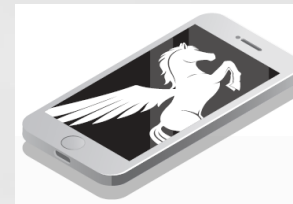
Эксплуатация бинарных уязвимостей (binary exploitation) - это намеренное использование ошибки в скомпилированном приложении. Такая атака подразумевает повреждение структур кода или данных в памяти процесса при помощи манипуляции входными данными.

В отличие от логических уязвимостей, бинарные сильно зависят от низкоуровневых особенностей ПО. Из-за этого при создании эксплоита (программы или скрипта, эксплуатирующего уязвимость) атакующему приходится учитывать бинарные конструкции, в которые преобразуется код после компилирования, специфику работы операционной системы, организацию адресного пространства, архитектуру системы и многое другое. Поэтому для подготовки успешной атаки злоумышленнику в первую очередь нужно получить копию ПО и проанализировать его на предмет ошибок.



Атаки на встроенное ПО

Эксплуатация бинарных уязвимостей



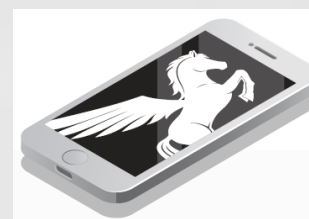
Меры защиты от бинарных уязвимостей в ПО

Меры защиты от бинарной эксплуатации уязвимостей во встроенном ПО можно разделить на две группы:

- предотвращение ошибок. Аудит исходного кода, использование статических анализаторов кода, использование более безопасных языков программирования - все это позволяет устранить ошибки до выпуска устройства;
- усложнение эксплуатации (hardening). Современные компиляторы поддерживают множество различных механизмов, которые затрудняют эксплуатацию и реализуют дополнительные проверки во время исполнения кода. Операционные системы, в свою очередь, содержат собственные средства противодействия таким атакам. Совместное использование указанных методов позволяет существенно усложнить написание стабильно работающего эксплоита.

Атаки на встроенное ПО

Эксплуатация бинарных уязвимостей



Поиск уязвимостей в ПО ведут разными методами. Чаще всего проводят обратную разработку встроенного программного обеспечения, получают высокоуровневое представление о коде и пытаются выявить ошибки в алгоритмах его работы.

Дополнительно, для автоматизации, применяют метод фаззинга (fuzzing) - подачи случайных или мутированных (на основе обратной связи) данных на вход ПО с целью проявления ошибок.

Иногда одного эксплоита недостаточно. Современные системы безопасности строятся по принципу изолированных уровней с выделенными интерфейсами для взаимодействия между ними.

При таком подходе компрометация внешнего слоя не ведет к компрометации внутренних нижележащих уровней. Поэтому, чтобы добраться до наиболее критических систем и данных, злоумышленник должен применить цепочку эксплоитов.

Яркий пример использования такого набора эксплоитов - коммерческое шпионское ПО Pegasus.

Когда владелец смартфона под управлением iOS переходил по вредоносной ссылке, мобильное устройство попадало под полный контроль атакующего. Спецслужбы, для которых разрабатывался Pegasus, получали возможность удаленно читать сообщения, отслеживать перемещения, записывать разговоры и не только.

Атаки на встроенное ПО

Закладки в ПО



Программная закладка (software backdoor) - скрытно внедренная в ПО функциональность, которая при определенных условиях позволяет осуществлять несанкционированный доступ к ресурсам системы. Если закладка реализована компетентно, заметить ее практически невозможно: зачастую она выглядит как программная ошибка. Даже если ее обнаружат, разработчик может правдоподобно отрицать злой умысел.

Программную закладку можно внедрить на различных этапах жизненного цикла устройства.

Практически неограниченные возможности по созданию бэкдора есть у разработчиков ПО;

- закладку могут установить при промышленном производстве;
- слабым звеном является и цепочка поставок.
- Однако скрытую функциональность для атаки можно внедрить не только при создании устройства или на пути к конечному пользователю, но и гораздо позже - например с установкой обновлений. Массовое заражение сетевым червем NotPetya в июне 2017 г., по мнению специалистов, началось именно с бэкдора, установленного с обновлением ПО.

Закладки также встраивают в криптографические алгоритмы: задают внутренние константы в специальные значения, что ослабляет стойкость алгоритма. В дальнейшем злоумышленник может это использовать, например, для прослушки защищенного канала, алгоритм шифрования которого содержит такую закладку.

Другой нашумевший пример программных закладок - бэкдоры, внедренные производителями в прошивки бюджетных маршрутизаторов. О них стало известно в результате многочисленных исследований. Цель установки закладок не ясна, но злоумышленники могут использовать такой инструмент, к примеру, для создания ботнета из устройств.

Атаки на встроенное ПО

Закладки в ПО



Меры защиты от закладок в ПО

Защита от данной атаки - нетривиальная задача. Обнаружить программную закладку, внедренную на этапе разработки, крайне сложно. Для этого необходимо анализировать подозрительные активности и проводить аудит системы.

Чтобы предотвратить внедрение бэкдоров на этапе эксплуатации, следует тщательно контролировать физический доступ к устройству и проверять устанавливаемые обновления.

Атаки на принципиальную электрическую схему

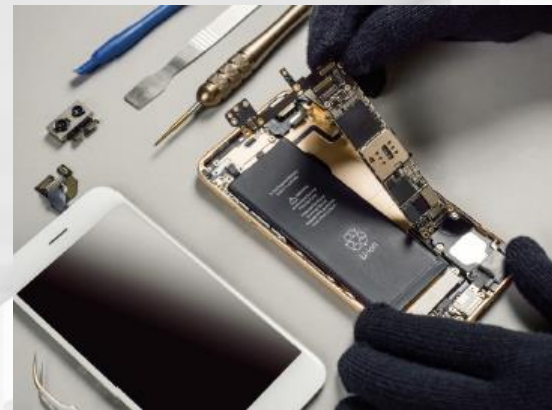
Анализ принципиальной электрической схемы проводят для того, чтобы понять логику ее работы, обнаружить недокументированные возможности, воспроизвести ее функциональность или выполнить модификацию.

При анализе сперва, как правило, изучают пользовательскую документацию, спецификации и различную информацию из открытых источников. Иногда уже на этом этапе удастся обнаружить данные о найденных уязвимостях или попытках обратной разработки исследуемого устройства.

После анализа общедоступной информации приступают к разборке устройства. В одних случаях для этого достаточно снять корпус, открутив пару винтов, а в других требуется кропотливая работа. Порядок снятия и расположение отдельных частей устройства документируют (самый простой способ - фотографировать объект на всех этапах разборки).

Следующая задача - идентифицировать комплектующие, из которых состоит встраиваемая система, и сделать предположения об их назначении.

Основная же часть анализа заключается в обратной разработке печатных плат (PCB - printed circuit board), входящих в состав устройства.



Атаки на принципиальную электрическую схему

Обратная разработка печатной платы

Техника обратной разработки печатной платы заключается в идентификации всех компонентов на плате и получении информации об их соединении между собой.

Часть электронных компонентов, размещенных на печатной плате, удастся легко идентифицировать по маркировкам на их корпусах или на самой плате.

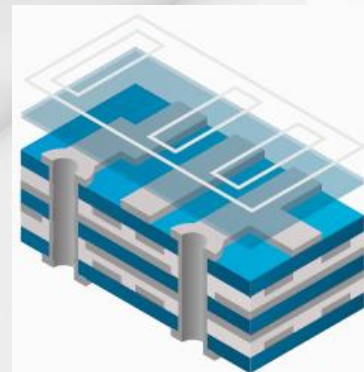
Зная маркировку, атакующий быстро найдет техническую спецификацию электронного компонента и однозначно определит его назначение. Некоторое представление о функциональности может дать и логотип производителя.

Если на корпусе микросхемы никакой информации нет, его можно удалить и добраться до кристалла ИС:

маркировка непосредственно на нем позволит точно провести идентификацию. Однако такой способ не всегда работает: в случае заказных интегральных схем маркировки могут отсутствовать даже на кристалле ИС. С учетом того, что технической спецификации на заказные интегральные схемы обычно нет в открытом доступе, определить их функциональность бывает трудно.

После идентификации электронных компонентов атакующий приступает к системному анализу архитектуры печатной платы. Как правило, визуальный осмотр и тест на непрерывность (прозвонка) электрической схемы позволяют получить грубую схему соединения компонентов и подсистем платы между собой.

На данном этапе идентифицируют полигоны земли и питания, определяют наличие порта отладки (JTAG-интерфейс) и шины связи между функциональными узлами. Наличие JTAG-интерфейса, объединяющего интегральные схемы в тестовую цепочку, может существенно упростить процесс обратной разработки печатной платы.



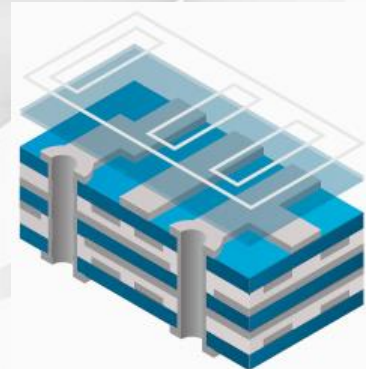
Устройство многослойной печатной платы

Атаки на принципиальную электрическую схему

Обратная разработка печатной платы

Если грубой схемы недостаточно для проведения атаки, то на следующем этапе атакующий получает подробную электрическую схему. Для ее построения нужны фотографии всех слоев платы. Сделать такие фотографии - тривиальная задача в случае с односторонними и двусторонними платами. Если же плата многослойная, для получения информации о соединении электронных компонентов друг с другом атакующему нужно сперва получить доступ к каждому слою.

Для этого используют разрушающую технику послойного препарирования или неразрушающую технику снятия изображения с помощью компьютерной томографии.



Устройство многослойной печатной платы

Интересный факт

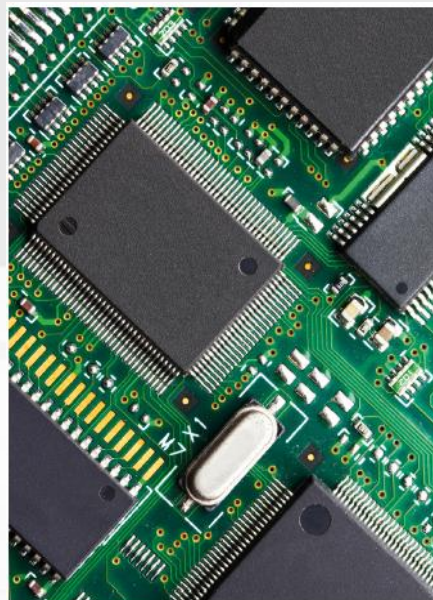
Как правило, многослойная плата состоит из внутренних слоев, связующего материала и внешних слоев. Внутренние слои формируют из «ядра» - двустороннего ламинированного медью стеклотекстолита. Наружные слои выполняют из медной фольги. Соединение слоев обеспечивает препрег - смолистый связующий материал.

Атаки на принципиальную электрическую схему

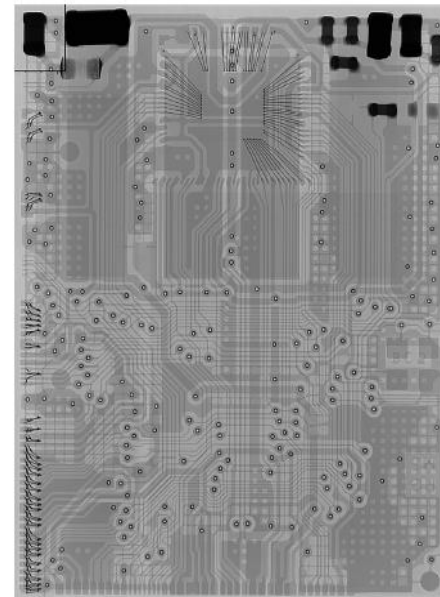
Обратная разработка печатной платы

При послойном препарировании атакующий удаляет паяльную маску и все электронные компоненты с двух сторон печатной платы, а потом снимает слой за слоем и делает фотографии каждого.

Инструментами для послойного препарирования выступают наждачная бумага, дремель, фрезерная или шлифовальная установка.



Печатная плата



Компьютерная томография печатной платы

Компьютерная томография требует куда более дорогостоящего оборудования, однако позволяет и получить изображения слоев, и сохранить работоспособность печатной платы.

Это бесспорное преимущество в том случае, когда у атакующего ограничен запас образцов для исследования.

Атаки на принципиальную электрическую схему

Обратная разработка печатной платы

Изображения слоев атакующий обрабатывает, строит таблицу соединений и в результате получает электрическую схему печатной платы. Анализ этой информации позволяет атакующему:

- понять принцип работы устройства;
- клонировать устройство с целью подделки;
- идентифицировать области, в которые можно добавить вредоносную функциональность;
- определить местоположение JTAG-интерфейса, позволяющего извлекать дампы памяти и производить отладку ПО.

Одно из наиболее распространенных применений данной атаки - кража интеллектуальной собственности. Подтверждением этому служит огромное количество китайских подделок оригинальных электронных устройств. Также взлом многих встраиваемых систем, например игровых консолей, был бы невозможен без предварительного обратного проектирования печатных плат, входящих в их состав.

При активной атаке на внутрисхемные сигналы атакующий взаимодействует с JTAG и заложенными производителем интерфейсами передачи данных, получает несанкционированный доступ к аппаратной части устройства и извлекает из него секретную информацию.

Интересный факт

JTAG (Joint Test Action Group) - название рабочей группы по разработке стандарта IEEE 1149. Позднее это сокращение стало прочно ассоциироваться с разработанным этой группой специализированным аппаратным интерфейсом на базе стандарта IEEE 1149.1.

Атаки на принципиальную электрическую схему

Обратная разработка печатной платы

Меры защиты от обратной разработки печатной платы

Обеспечить абсолютную защиту от обратной разработки - сложная задача. Однако можно сделать процесс обратной разработки более дорогостоящим и трудоемким с помощью специальных мер:

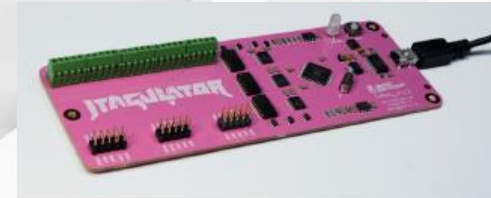
- антивандальные крепежи, винты заказной формы, заливка печатной платы эпоксидной смолой усложняют разбор устройства;
- активные системы контроля целостности корпуса устройства с автономным источником питания при обнаружении вскрытия стирают критически важную информацию из памяти;
- отсутствие маркировок на микросхемах и шелкографии на печатной плате усложняет идентификацию электронных компонентов;
- BGA-корпуса позволяют скрыть выводы микросхемы.

Атаки на принципиальную электрическую схему

Пассивные и активные атаки на внутрисхемные сигналы

При пассивной атаке на внутрисхемные сигналы атакующий перехватывает информацию, которой обмениваются электронные компоненты на печатной плате. Как правило, обмен информацией идет по различным интерфейсам передачи данных (UART, I2C, SPI, ISO/IEC 7816). Выделив их расположение на печатной плате и подключившись к ним логическим анализатором, атакующий может:

- извлечь частично или полностью прошивку устройства;
- собрать дампы памяти из данных, передающихся по шине;
- проанализировать ход выполнения встроенного ПО;
- проанализировать взаимодействие функциональных блоков.



Устройство для автоматизированного поиска
JTAG-интерфейса

Если у устройства есть отладочный порт, злоумышленнику крайне удобно проводить активную атаку с его помощью. Такие порты, дающие доступ к служебным консолям, находятся на многих устройствах - их используют для отладки на этапе разработки, через них проводят настройку и техобслуживание на этапе эксплуатации. Определив, по какому интерфейсу и протоколу передаются данные, атакующий может получить доступ к служебной консоли, что даст ему практически неограниченные возможности для работы с устройством.

Интересный факт

В процессорах Intel, начиная с семейства Skylake, запущенного в производство в 2015 г., доступ к JTAG можно получить через порт USB 3.0 при помощи новой технологии Direct Connect Interface (DCI). Получив физический доступ к устройству и активировав интерфейс DCI, атакующий может обойти практически любые защитные механизмы, реализованные в софте.

Атаки на принципиальную электрическую схему

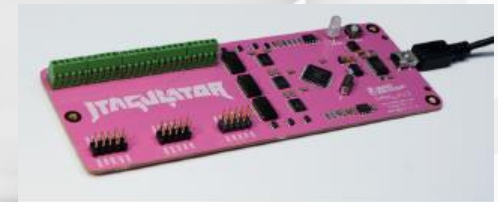
Пассивные и активные атаки на внутрисхемные сигналы

Очень часто отладочные порты остаются в IoT-устройствах (роутерах, IP-камерах и др.). В результате даже любитель может получить полный контроль над такой системой или снять дампы прошивки для последующего анализа. Обнаруженные в ПО таких устройств уязвимости в последнее время все чаще используют для организации огромных ботнетов.

Если внешние отладочные порты отсутствуют, атакующий, как правило, пытается получить доступ к JTAG - аппаратному интерфейсу для отладки, программирования и тестирования микросхем. Обычно у JTAG нет внешних выводов для подключения, но получить доступ к нему можно, подпаявшись к его контактам на печатной плате.

JTAG невероятно полезен для разработчиков при проектировании, тестировании и производстве, поэтому его используют практически во всех встраиваемых системах. Однако он также полезен при проведении атаки, так как дает низкоуровневый доступ к процессору и памяти в обход средств обеспечения безопасности. В результате атакующий получает практически неограниченные возможности для анализа и обратной разработки устройства. В частности, он может:

- прочесть память и записать в нее данные,
- извлечь прошивку,
- выполнить пошаговую отладку прошивки,
- выполнить произвольные инструкции в центральном процессоре.



Устройство для автоматизированного поиска JTAG-интерфейса

Атаки на принципиальную электрическую схему

Пассивные и активные атаки на внутрисхемные сигналы

Меры защиты от атак на внутрисхемные сигналы

Для защиты устройства от атак на внутрисхемные сигналы можно использовать следующие меры:

- сокрытие или устранение отладочных портов,
- отключение JTAG или установка на него парольной защиты,
- применение проприетарных протоколов передачи данных,
- организация аутентификации для доступа к служебным консолям.

В некоторых случаях злоумышленник может получить доступ даже к отключенному JTAG-интерфейсу - такую возможность дает атака методом индуцированных сбоев на ИС.

Поэтому важно понимать угрозы для каждого уровня, на котором функционирует устройство и знать соответствующие меры защиты.

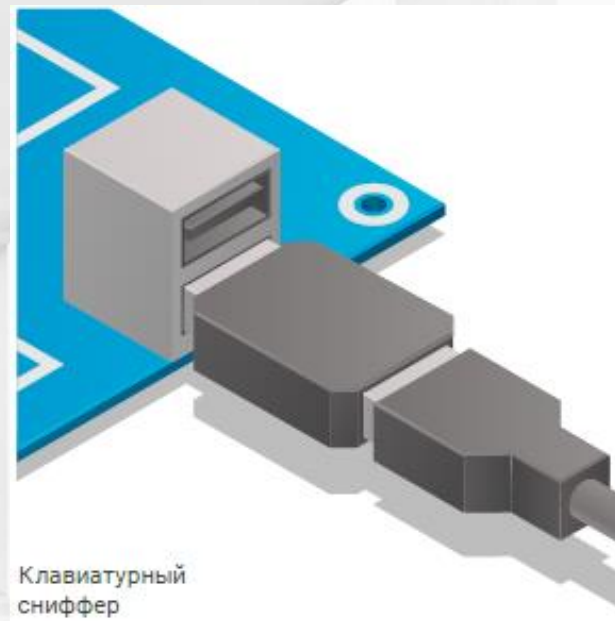
Атаки на принципиальную электрическую схему

Закладки в устройстве

Аппаратная закладка (hardware backdoor) - скрытно внедренное в электронную схему техническое приспособление, которое позволяет вывести систему из строя или получить несанкционированный доступ к секретным данным или программному обеспечению. Бэкдор можно внедрить на любом этапе жизненного цикла устройства, от проектировки до установки системы у конечного пользователя. От этапа, на котором бэкдор был внедрен, зависит сложность обнаружения закладки. Чтобы найти скрытую функциональность, замаскированную опытным инженером-конструктором на этапе проектирования, придется провести полную или частичную обратную разработку устройства.

Если злоумышленники установили закладку в уже готовое устройство, обнаружить ее значительно проще: для этого достаточно сравнить устройство с немодифицированным.

Простой пример аппаратной закладки - клавиатурные шпионы (снифферы), которые регистрируют данные, вводимые с клавиатуры, и сохраняют их во встроенную флеш-память. Их можно внедрить в саму клавиатуру, в системный блок или замаскировать под переходники.



Атаки на принципиальную электрическую схему

Закладки в устройстве

О других реализациях такого вида злонамеренного вмешательства сообщают документы, опубликованные Эдвардом Сноуденом в 2013 г. В них описаны технологии и устройства, которые АНБ использует для организации шпионской деятельности. Одно из таких приспособлений - подключаемый USB-разъем COTTONMOUTH-I.

Он содержит радиопередатчик и обеспечивает скрытый беспроводной доступ к интересующему компьютеру. Также это приспособление может использоваться для установки троянских программ на объект проникновения.



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08

COTTONMOUTH - 1



(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

Устройство для электронного шпионажа (из каталога АНБ)

Атаки на принципиальную электрическую схему

Закладки в устройстве

Меры защиты от закладок в устройстве

Как и в случае с программными закладками, защититься от грамотно установленных аппаратных закладок достаточно сложно. Обратная разработка всех устройств в инфраструктуре - мера утопическая, но вполне разумным будет:

- закупать оборудование у проверенных поставщиков,
- периодически проводить его аудит,
- тщательно контролировать физический доступ к используемым системам.

Атаки на принципиальную электрическую схему

Атаки на интегральные схемы

Интегральная схема (ИС, англ. IC - integrated circuit) - это устройство, состоящее из множества связанных микроэлектронных компонентов: транзисторов, резисторов, конденсаторов и диодов, - изготовленных на полупроводниковой подложке.

ИС используются во всех окружающих нас встраиваемых системах: мобильных телефонах, банковских картах, бытовой технике, компьютерах и др. Помимо функций управления, они также реализуют механизмы обеспечения безопасности.



Рассмотрим актуальные атаки, которые позволяют обойти механизмы защиты ИС и получить доступ к хранящейся на них секретной информации.

Особенность и опасность данных атак в том, что они проводятся на самом низком уровне функционирования системы. Так как ИС - основа для всех вышележащих механизмов обеспечения безопасности, успешная атака означает компрометацию всего устройства.

По степени вмешательства в функционирование устройства атаки можно разделить на два вида:

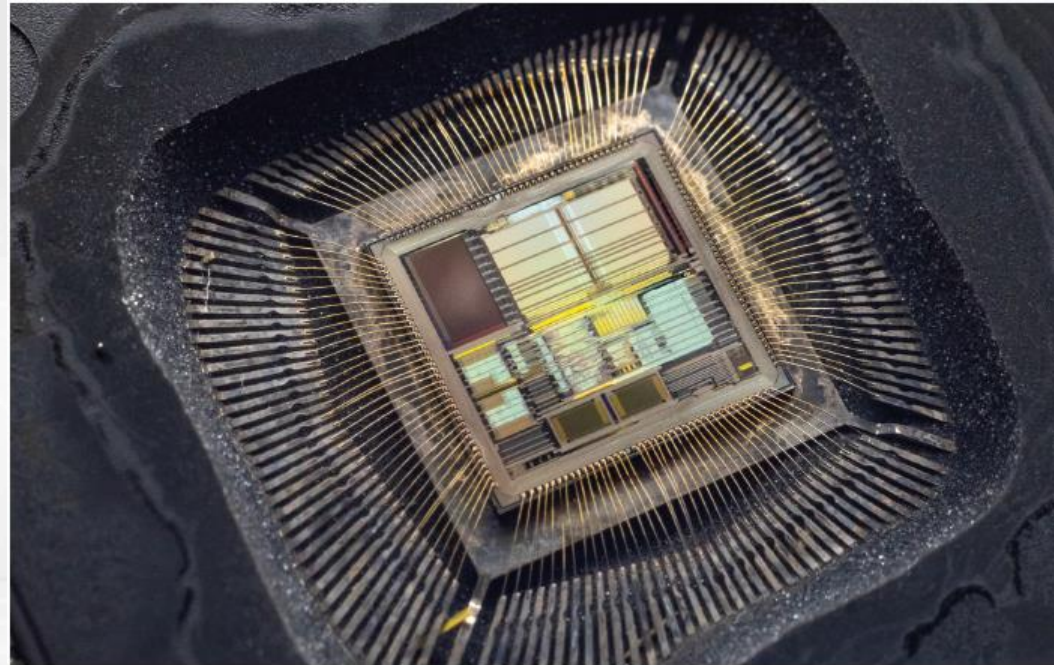
- *пассивные атаки* - не влияют на работу устройства. При них атакующий извлекает секретную информацию через побочные каналы утечки;
- *активные атаки* - нарушают нормальный ход работы устройства. Их проводят для обхода защитных мер и извлечения секретной информации. Атаки такого рода будут рассмотрены в разделе «Атаки методом индуцированных сбоев».

Атаки на принципиальную электрическую схему

Атаки на интегральные схемы

Интересный факт

Наиболее распространенный среди любителей способ декапсуляции - химический. Он подходит для удаления пластикового корпуса микросхемы, сравнительно прост и не требует дорогостоящего оборудования. Обычно используют смесь азотной и серной кислот.



Декапсулированная ИС

Интересный факт

Первая система на кристалле (SoC) была разработана в 1974 г. для электронных часов Pulsar компании Hamilton Watch Company.

Атаки на принципиальную электрическую схему

Атаки на интегральные схемы



В некоторых случаях для проведения атак обоих типов необходимо вскрыть микросхему, не повредив при этом кристалл ИС, то есть выполнить декапсуляцию. Декапсуляция (decapsulation) - процесс частичного или полного удаления корпуса микросхемы для обеспечения доступа к кристаллу. В зависимости от того, как именно удаляют корпус, выделяют несколько видов декапсуляции:

- лазерная декапсуляция - корпус разрушают импульсами сфокусированного лазерного луча;
- химическая декапсуляция - материал корпуса растворяют горячими высококонцентрированными кислотами;
- механическая декапсуляция - часть корпуса микросхемы удаляют режущим инструментом, например фрезой;
- плазмохимическая декапсуляция - корпус разрушается за счет совместного действия химической реакции и ударов ионов в потоке фокусированной плазмы.

Конкретный случай и материал корпуса могут требовать совмещения методов декапсуляции. Иногда единственный способ обойти механизмы безопасности ИС или извлечь информацию из нее - провести *инвазивную атаку*. Такие атаки открывают практически неограниченные возможности, но вызывают необратимые физические изменения кристалла ИС и порой приводят к ее полному разрушению.

Атаки на принципиальную электрическую схему

Атаки по второстепенным каналам

Процессы, происходящие в ИС, подчиняются законам физики. Когда устройство производит вычисления, оно потребляет электроэнергию, испускает излучение, рассеивает энергию и затрачивает на это некоторое время. Указанные эффекты возникают не беспорядочно: они зависят от внутреннего состояния устройства и обрабатываемых данных в конкретный момент времени. Если атакующий сможет зарегистрировать эти явления с необходимой точностью, то такие непреднамеренные (unintended) интерфейсы станут для него скрытыми каналами утечки секретных данных.

Атаки с применением этого метода называются атаками по второстепенным каналам (АВК, англ. SCA - side-channel attacks).

Один из наиболее показательных примеров - атака по времени на процедуру проверки пароля. Алгоритм, проверяющий правильность введенных данных, может быть реализован несколькими способами. Самый простой и распространенный - алгоритм посимвольного сравнения: он поочередно сравнивает байты из введенного текста с байтами из секретной фразы и останавливает исполнение, как только встречает несовпадение.

Сам алгоритм корректен, но на реальном процессоре он становится уязвимым: на каждую операцию затрачивается время, в том числе и на операцию сравнения. Атакующий может измерить время работы алгоритма и выяснить, сколько символов из введенной фразы совпадает с секретной. Это позволяет подбирать пароль посимвольно, что гораздо быстрее, чем проводить полный перебор всех возможных фраз. Здесь хорошо видна ключевая особенность АВК: атака нацелена не на алгоритм, который безопасен, а на его практическую реализацию.



Атаки на принципиальную электрическую схему

Атаки по второстепенным каналам

Приведенный пример помогает быстро понять принцип АБК, но не иллюстрирует потенциал таких атак в полной мере. Возможности метода гораздо шире. Атакующий может:

- получить ключи криптографических алгоритмов. Это особенно актуально для криптографических сопроцессоров и смарт-карт: они производят процедуры шифрования и криптографической подписи, сохраняя ключ в секрете. Безопасность систем, где применяются эти устройства, основана именно на секретности ключа и невозможности его извлечения с физического носителя. Если атакующий получает ключ, безопасность системы полностью компрометируется;
- произвести точную синхронизацию своих действий с внутренними процессами устройства. Это помогает проводить атаки методом индуцированных сбояв (АМИС), которые будут рассмотрены далее. Для АМИС нужны триггеры - отправные точки для синхронизации. Если в этом качестве не удастся использовать внешние сигналы ИС, атакующий может с помощью АБК выделить паттерн, например в осциллограмме энергопотребления, и осуществить привязку по времени к нему;
- получить последовательности исполняемых процессором инструкций (трассы кода). Такой подход используется для обратной разработки ПО, когда нет возможности получить дампы памяти устройства. Метод основан на профилировании работы процессора: при выполнении каждой инструкции внутреннее состояние ИС изменяется строго определенным образом, в результате у каждой инструкции получается характерная кривая энергопотребления. Для получения трассы кода атакующему необходимо лишь распознать паттерны, соответствующие инструкциям, на осциллограмме.



Атаки на принципиальную электрическую схему

Атаки по второстепенным каналам

Интересный факт

Книга «Murdoch's pirates», основанная на журналистском расследовании, в деталях рассказывает историю противостояния медиакомпаний, провайдеров спутникового ТВ и пиратов.



Интересный факт

В 2007 г. АНБ рассекретило статью Д. Фридмана «TEMPEST: a signal problem» (1972). Это одна из первых известных работ, посвященных АБК.

Интересный факт

В 2018 г. Сэм Зелуф (Sam Zeloof) в домашней лаборатории создал ИС методом фотолитографии. На тот момент инженер-любитель заканчивал школу.

Атаки на принципиальную электрическую схему

Атаки по второстепенным каналам



Общие меры защиты от АБК

Модификация криптографических алгоритмов затрудняет проведение любой атаки такого класса. Один из вариантов модификации - наложение случайной, различной каждый раз маски на промежуточные значения криптографических вычислений. В этом случае найти зависимость между секретными данными и осциллограммами гораздо сложнее.

Также для защиты от данного класса атак используют рандомизацию порядка шифрования, внутренний генератор тактового сигнала с плавающей частотой, внедрение случайных задержек и прерываний. Это осложняет выравнивание осциллограмм для проведения дифференциального и корреляционного анализов, о которых мы расскажем в главах «АБК по энергопотреблению» и «АБК по электромагнитному излучению».

Так как для большинства методов АБК нужны значительные наборы данных, один из эффективных способов защиты - ограничение количества криптографических операций для одного секретного ключа.

Например, в банковских картах делают счетчик количества транзакций. Если его значение выходит за предусмотренные производителем границы, карта блокируется, что не дает собрать достаточное количество данных. В повседневном использовании это не создает проблем: обычный пользователь за срок действия карты совершает значительно меньше транзакций (в крайнем случае карту могут заменить в отделении банка).

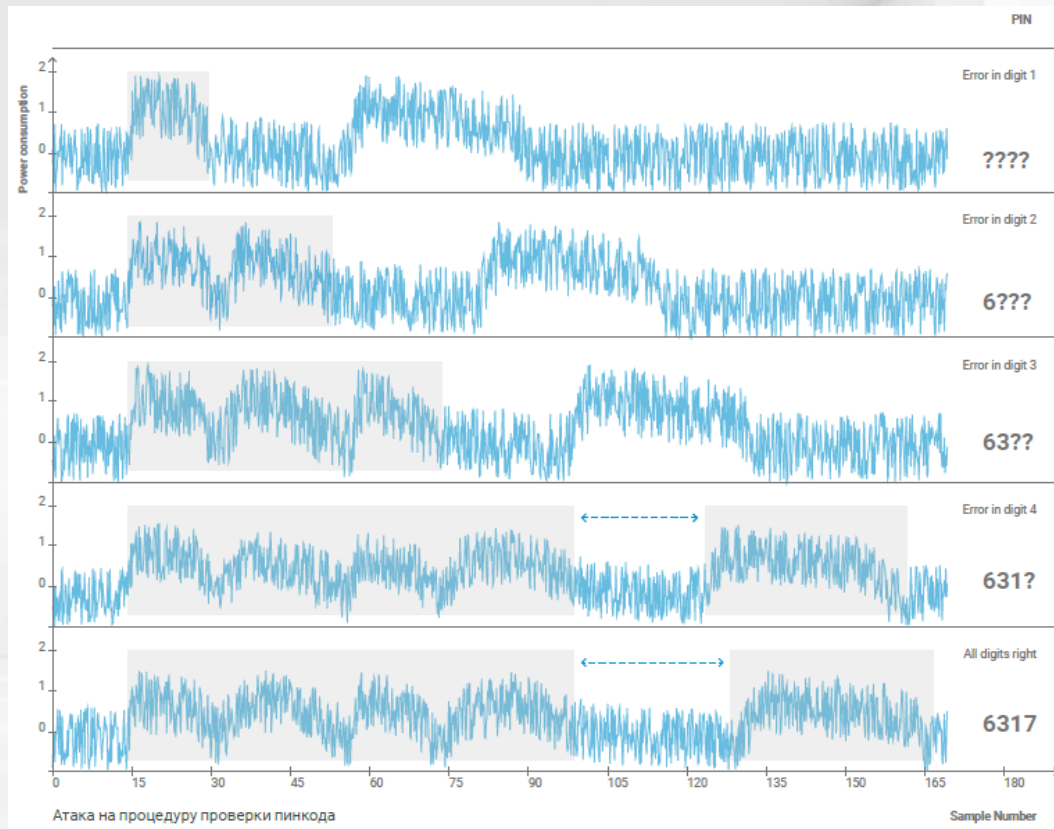
Атаки на принципиальную электрическую схему

АВК по времени

Каждая логическая операция, выполняемая на кристалле ИС, занимает определенное время. Часто это время находится в некой зависимости от входных данных.

Атака по времени (timing attack) - это атака по второстепенным каналам, в которой атакующий пытается скомпрометировать механизмы защиты с помощью анализа времени, затрачиваемого на исполнение алгоритмов, связанных с обеспечением безопасности (шифрования, проверки пароля и др.). Известно, что время выполнения криптографических алгоритмов должно быть постоянным вне зависимости от значений (именно значений, а не объемов) входных данных.

Рассмотрим, как атакующий может извлечь секретный ключ, если это условие не выполняется. Для примера возьмем алгоритм DES - в нем конечная перестановка P в функции Фейстеля в первом раунде зависит от входных данных и секретного ключа. Если время работы перестановки зависит от количества единичных битов во входном значении, атакующий может делать предположения о небольшой части секретного ключа, строить модель затрачиваемого времени и рассчитывать корреляцию с реальными данными. Чем больше ее значение, тем выше вероятность, что предположение верно.

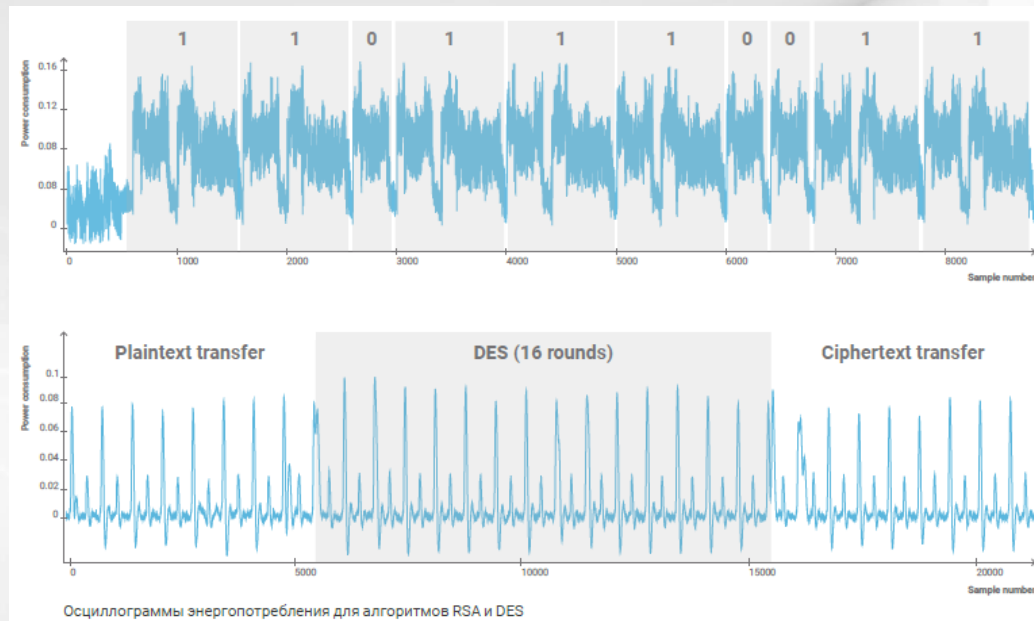


Атаки на принципиальную электрическую схему

АВК по времени

Иллюстрация на предыдущей странице демонстрирует, как выглядят осциллограммы энергопотребления ИС в ходе проверки пин-кода: отчетливо видна зависимость между временем выполнения алгоритма и количеством совпадающих цифр.

Один из интересных способов применения АВК по времени - эксплуатация упомянутых ранее уязвимостей Spectre и Meltdown. Атаки используют ошибку в реализации спекулятивного выполнения команд и в механизме предсказания ветвлений. Второстепенным каналом при этом выступает время, затрачиваемое на чтение кэшированных данных. Анализ этого времени позволяет атакующему узнать содержимое защищенных участков памяти. Особенность данных атак в том, что они могут быть выполнены исключительно из ПО, не требуют дополнительного оборудования и легко масштабируются.



Меры защиты от АВК по времени

В качестве мер защиты от АВК по времени необходимо:

- использовать алгоритмы шифрования и авторизации с константным временем выполнения, не зависящим от значения входных данных;
- корректно реализовывать алгоритмы обеспечения безопасности в механизмах оптимизации вычислений процессора.

Атаки на принципиальную электрическую схему

АВК по энергопотреблению

Криптографическое устройство на различных этапах работы потребляет различное количество электроэнергии. Если ИС реализована с использованием КМОП-логики (CMOS), его энергопотребление напрямую зависит от изменения логических состояний МОП-транзисторов. АВК по энергопотреблению (power analysis) основана на анализе мощности, которую потребляет ИС во время работы криптографического алгоритма или выполнения критических с точки зрения безопасности операций.

Для проведения данной атаки необходим инструмент, способный с высокой точностью измерять потребляемый ИС ток. Для этой цели подходят современные цифровые осциллографы: они могут показать даже небольшую разницу в энергопотреблении, а также отфильтровать высокочастотные составляющие, мешающие анализу.

Рассмотрим наиболее известные методы АВК по энергопотреблению.

Простой анализ питания (SPA - simple power analysis) подразумевает визуальную оценку осциллограмм энергопотребления без использования статистических и математических методов извлечения информации. Повторяющиеся на графике паттерны означают однотипные операции.

Интересный факт

В некоторых случаях для проведения успешной АВК на незащищенные устройства достаточно самого простого осциллографа. Например, в докладе CheapSCAtе компании Riscure показано, как извлечь ключ шифрования из микроконтроллера ATmega328 с оборудованием общей стоимостью менее 60 долларов.

Атаки на принципиальную электрическую схему АВК по энергопотреблению

Такой анализ может быть полезен для идентификации используемого криптографического алгоритма, если он неизвестен. Например, 16 повторяющихся пиков на графике могут означать 16 раундов DES (см. осциллограмму на с. 63). В некоторых случаях такой метод позволяет полностью извлечь секретный ключ. Так, для работы алгоритма RSA требуется возводить большие числа в степень. Эта операция обычно разбивается на последовательность более простых операций - возведение в квадрат и умножение. Какие операции будут выполнены на данном шаге алгоритма (возведение или возведение и умножение), определяет единственный бит из секретного ключа. Выделив на графике два различных паттерна, атакующий может по ним определить все биты ключа.

Дифференциальный анализ питания (DPA – differential power analysis) предназначен для извлечения из осциллограмм скрытой информации, невидной невооруженным глазом. Он основан на применении статистических методов и закона больших чисел Чебышева. В отличие от предыдущего метода, где требуется малое количество экспериментов, для работы дифференциального анализа необходимо собрать тысячи, а в некоторых случаях миллионы осциллограмм (трасс). Принцип работы метода заключается в следующем: собранные трассы разделяются на две группы на основании одного бита из промежуточного значения в алгоритме шифрования (как правило, в первом или последнем раунде). В свою очередь, это значение зависит от обрабатываемых данных и небольшой части секретного ключа. Если атакующий правильно подберет эту часть ключа, то разность (англ. difference, откуда возникло название метода) между двумя группами трасс даст пик. Таким образом можно получить весь секретный ключ по частям. Как правило, этот метод применяется для симметричной криптографии.

Атаки на принципиальную электрическую схему АВК по энергопотреблению

Корреляционный анализ питания (CPA - correlation power analysis) основан на использовании коэффициента корреляции между трассами и весом или расстоянием Хэмминга для промежуточных значений алгоритма. Принцип работы схож с предыдущим методом: атакующий подбирает секретный ключ по частям, делая предположения о его возможных значениях. На основе предположения и известных входных или выходных данных строится модель энергопотребления для конкретного промежуточного значения в алгоритме (как правило, в первом или последнем раунде). Если предположение верное, корреляция модели с реальными трассами даст пик.

Метод применяется в основном для извлечения секретного ключа из симметричных шифров.

Рассмотренные методы - самые распространенные схемы проведения АВК по энергопотреблению.

Интересный факт

Welch's t-test - это адаптация t-критерия Стьюдента. Критерий Стьюдента был разработан Уильямом Госсетом для оценки качества пива в компании «Гиннесс».

Из-за обязательств по неразглашению коммерческой тайны (руководство «Гиннесса» считало таковой использование статистического аппарата в своей работе) Госсет опубликовал статью в 1908 г. в журнале «Биометрика» под псевдонимом Student (Студент).

Атаки на принципиальную электрическую схему АВК по энергопотреблению

Меры защиты от АВК по энергопотреблению

Для предотвращения АВК по энергопотреблению можно использовать следующие защитные меры:

- балансировка потребляемой мощности - добавление фиктивных регистров и логических элементов, которые выполняют бесполезные операции, но выравнивают энергопотребление и делают его одинаковым для всех инструкций;
- сглаживание неравномерностей в энергопотреблении - установка буферизирующих блоков в цепи питания;
- организация двунаправленной транзисторной логики - проектирование кристалла ИС таким образом, что каждый сигнал кодируется одновременно двумя различными значениями: логическими «0» и «1». В этом случае энергопотребление постоянно и не зависит от промежуточных вычислений криптографического процессора.

Атаки на принципиальную электрическую схему АВК по энергопотреблению

Однако известны и более совершенные методы:

атаки высокого порядка (high-order attacks), шаблонные атаки (template attacks) и др. Очень часто для успешной реализации АВК по энергопотреблению выполняют дополнительную обработку трасс: проводят выравнивание (aligning), крайне важное для дифференциального и корреляционного анализа, и обработку сигналов (signal processing) для фильтрации шумов и выделения полезной составляющей. Так как сбор большого количества трасс может занять продолжительное время, перед проведением атаки разумно убедиться в ее целесообразности.

Иными словами, каким-то образом проверить, что данное устройство создает утечку через побочные каналы. Для этого, как правило, собирают два набора трасс: первый со специально подобранными входными данными, второй со случайными - и используют критерий Крамера-Уэлча (Welch's t-test) для определения утечки.

Первая статья в открытом доступе, «Differential power analysis», где описывались простой и дифференциальный анализы энергопотребления, была опубликована в 1999 г. Полом Кочером. Она показывала, как на практике можно провести АВК по энергопотреблению на аппаратную реализацию DES. С тех пор в этой области ведутся активные исследования, и сейчас можно найти множество работ по данной тематике.

Атаки на принципиальную электрическую схему АВК по электромагнитному излучению

Все электронные устройства во время работы испускают электромагнитное излучение. Каждый проводник, по которому течет электрический ток, создает магнитное поле. В результате вокруг ИС генерируется переменное электромагнитное (ЭМ) поле малой мощности, которое может стать источником информации о внутренних процессах. Получение такой информации - цель атак по электромагнитному излучению (EM side-channel attack).

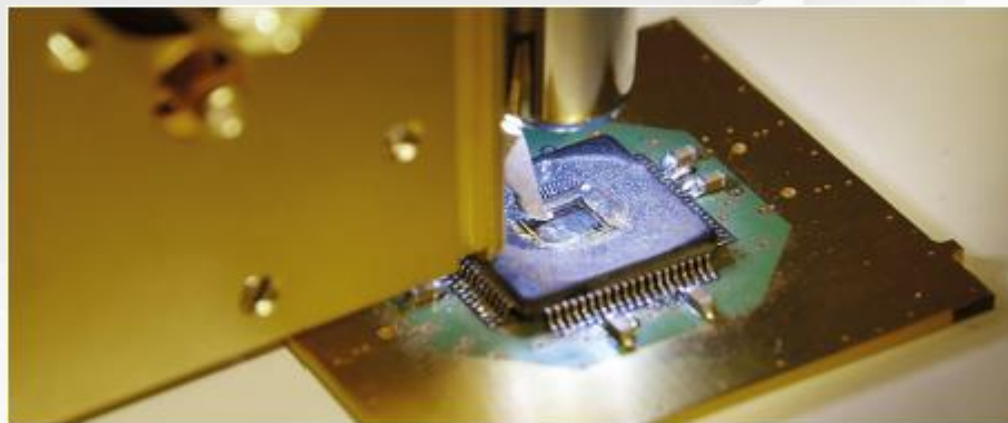
Электромагнитное излучение кристалла ИС регистрируют с помощью осциллографа и специального зонда, в основе которого лежит катушка индуктивности. Используя манипуляторы для высокоточного позиционирования образца, атакующий перемещает зонд вдоль плоскости кристалла и ищет область с наибольшей интенсивностью электромагнитного излучения. Как правило, это то место, где расположены транзисторы, участвующие в процессе криптографических вычислений.

Последняя особенность крайне важна для понимания сильных сторон АВК по ЭМ-излучению. В отличие от АВК по энергопотреблению, где потребляемая мощность регистрируется для всей ИС, использование миниатюрного ЭМ-пробника дает атакующему возможность действовать избирательно.

Атаки на принципиальную электрическую схему АВК по электромагнитному излучению

Для простоты проектирования и из-за конечной скорости распространения сигналов элементы (триггеры, логические вентили), из которых строится функциональный узел, расположены близко друг к другу, а не размещены по всей площади ИС.

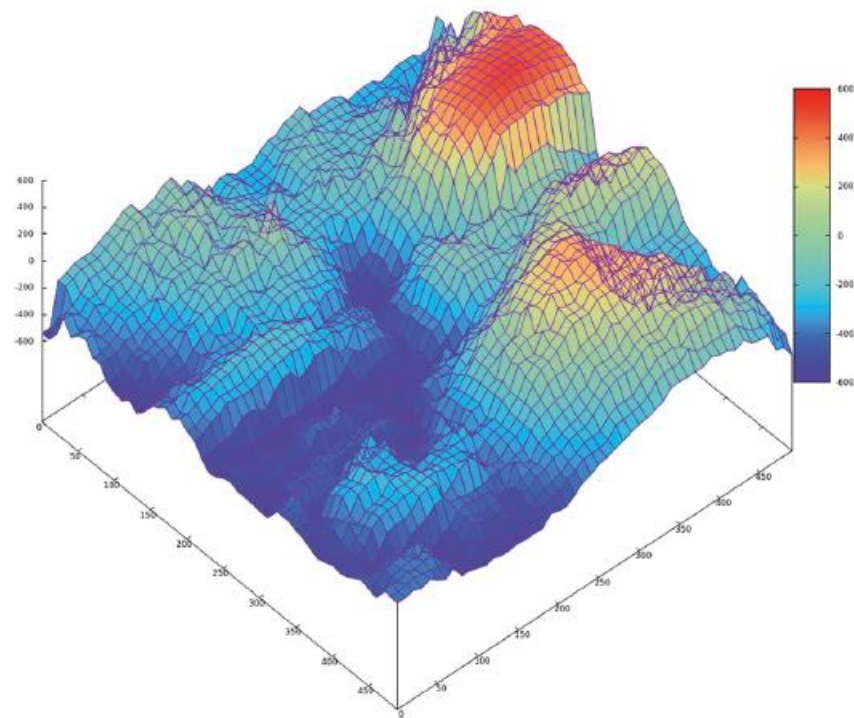
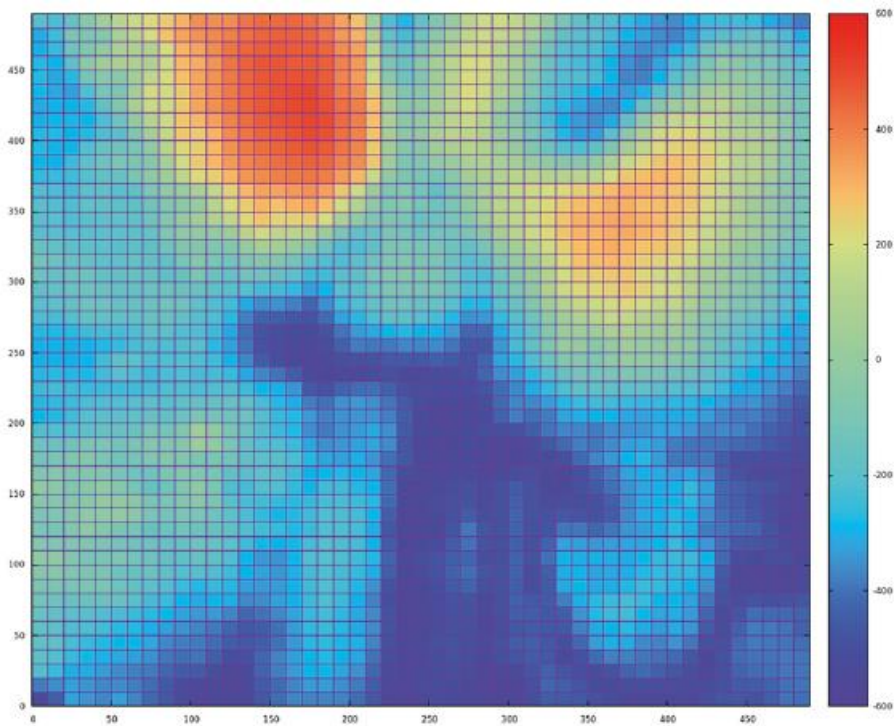
Установив пробник непосредственно над блоком шифрования, атакующий существенно улучшает качество принимаемого сигнала и обходит контрмеры, например фильтры в цепи питания.



Установка для регистрации ЭМ-излучения. Источник: langer-entw.de

Дополнительно, для выделения интересующего излучения на определенной частоте, во время обработки сигналов могут быть применены цифровые частотные фильтры.

Атаки на принципиальную электрическую схему АВК по электромагнитному излучению

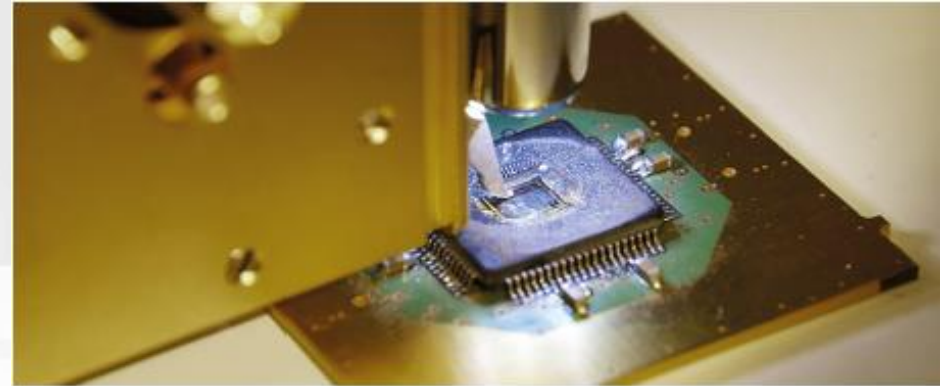


Графики интенсивности ЭМ-излучения

Атаки на принципиальную электрическую схему АВК по электромагнитному излучению

Рассмотрим наиболее известные методы АВК по ЭМ-излучению.

При *простом электромагнитном анализе* (SEMA - simple electromagnetic analysis) атакующий извлекает секретный ключ, визуально анализируя осциллограмму. Этот подход аналогичен простому анализу питания, только вместо осциллограммы энергопотребления используется график электромагнитной активности ИС. Данный метод, как правило, эффективен против реализаций ассиметричных алгоритмов шифрования и требует от атакующего глубокого понимания криптографического устройства и реализации алгоритма.



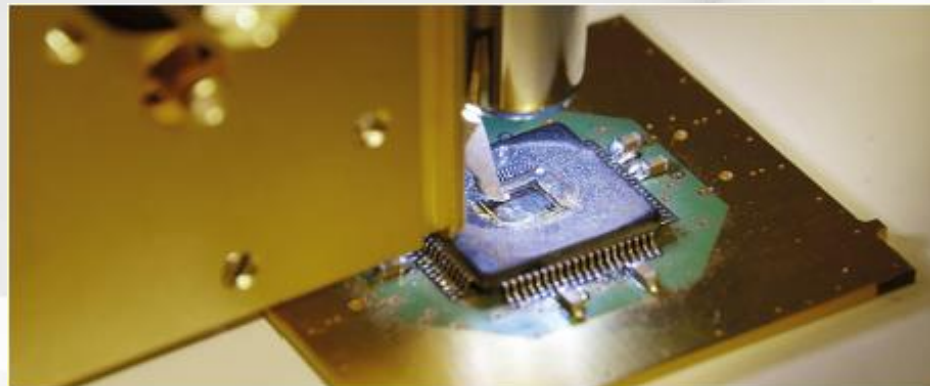
Установка для регистрации ЭМ-излучения. Источник: langer-entw.de

Когда невозможно достичь желаемого результата с помощью простого электромагнитного анализа, применяют *дифференциальный электромагнитный анализ* (DEMA - differential electromagnetic analysis) - более сложную, но и более эффективную атаку против реализаций криптографии с симметричным блочным шифрованием. Подход аналогичен методу дифференциального анализа питания и позволяет извлечь скрытую информацию из большой выборки осциллограмм электромагнитного излучения. Данный метод меньше зависит от деталей реализации.

Атаки на принципиальную электрическую схему АВК по электромагнитному излучению

АВК по электромагнитному излучению - атака пассивная и неразрушающая. Однако, чтобы улучшить принимаемый ЭМ-сигнал, атакующий может выполнить декапсуляцию микросхемы и зарегистрировать излучение с помощью пробника непосредственно у кристалла ИС.

Первые статьи, затрагивающие АВК по электромагнитному излучению, были опубликованы в 2001 г. - атака осуществлялась при помощи нескольких антенн, расположенных вблизи кристалла ИС смарт-карты. С тех пор, помимо атак на ПЛИС и микроконтроллеры, стали известны случаи успешных неразрушающих атак на реализацию криптографических алгоритмов в современных смартфонах.

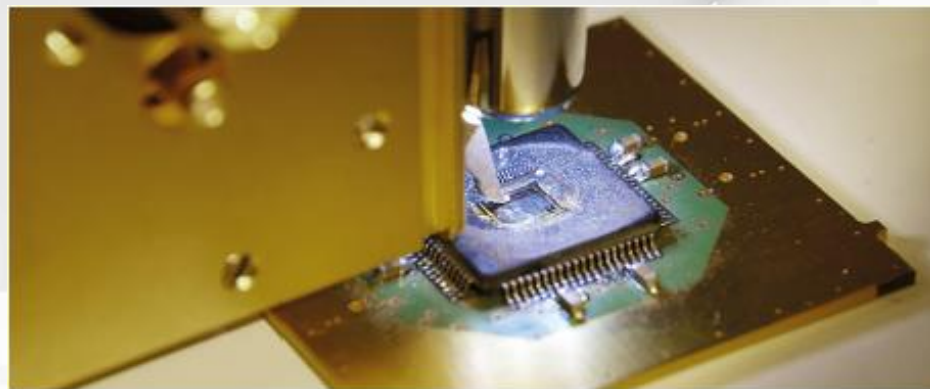


Установка для регистрации ЭМ-излучения. Источник: langer-entw.de

Атаки на принципиальную электрическую схему АВК по электромагнитному излучению

Одна из последних и наиболее интересных разновидностей АВК по электромагнитному излучению - атака screaming channels.

Она затрагивает ИС, на которых реализованы модули беспроводной связи, например Wi-Fi и Bluetooth. В таких системах аналоговые радиочастотные приемопередатчики и схемы цифровой логики находятся на одной кремниевой подложке близко друг к другу. Из-за этого непреднамеренные утечки информации, возникающие во время выполнения криптографических вычислений, могут смешиваться с радиосигналом, усиливаться и передаваться в эфир.



Установка для регистрации ЭМ-излучения. Источник: langer-entv.de

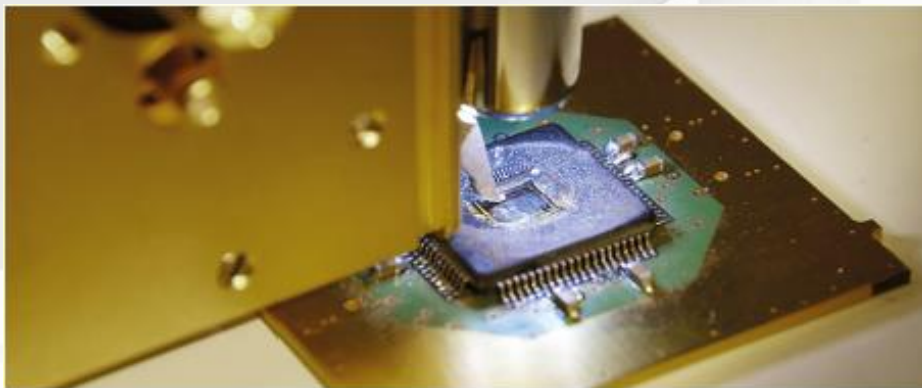
В результате криптографические ключи удастся извлечь на расстоянии до 10 м от устройства. Впервые данная разновидность АВК по электромагнитному излучению была описана в статье Джованни Камурати и др. в 2018 г. (G. Camurati et al. Screaming channels: when electromagnetic side channels meet radio transceivers).

Атаки на принципиальную электрическую схему АВК по электромагнитному излучению

Интересный факт

Для регистрации электромагнитного излучения используют различные пробники, но все они, как правило, являются модификациями двух основных видов: пробников магнитного поля (Н-поля) и электрического поля (Е-поля).

- Пробник Н-поля регистрирует колебания, вызванные изменением токов. Конструктивно представляет собой катушку или петлю. Чувствителен к ориентации по отношению к направлению поля.
- Пробник Е-поля регистрирует колебания, вызванные изменением напряжения. Обычно выполняется в виде небольшой штыревой антенны. Слабо чувствителен к ориентации в пространстве.



Установка для регистрации ЭМ-излучения. Источник: langer-entw.de

Атаки на принципиальную электрическую схему АВК по электромагнитному излучению

Меры защиты от АВК по электромагнитному излучению

Обезопасить устройство от АВК по ЭМИ проблематично, но специальные меры помогут затруднить ее проведение.

Один из самых эффективных способов противодействия - помешать атакующему зарегистрировать электромагнитный сигнал на физическом уровне.

Как правило, для этого проводят модернизацию схемы с целью уменьшения ЭМИ.

Атаки методом индуцированных сбоев

Атаки методом индуцированных сбоев (АМИС, англ. FI - fault injection), или атаки внесения неисправностей, - это разновидность аппаратных атак, при которых атакующий добивается нетипичного поведения устройства за счет внесения кратковременных сбоев в состояния внутренних логических элементов ИС.

Различают два основных подкласса по типу индуцированных сбоев:

- *модификация алгоритма.* Атака этого подкласса приводит к пропуску или некорректному выполнению инструкций процессора. В результате атакующий может обойти предусмотренные защитные механизмы, например проверку корректности введенного пинкода;
- *внесение ошибки в вычисления криптографического процесса.* Данный подкласс атак основан на применении метода дифференциальных искажений (DFA - differential fault analysis), предложенного А. Шамиром в 1996 г., для извлечения секретного ключа. Суть атаки в том, что при сбое в вычислениях шифрующее устройство выдает некорректные данные, сравнение которых с верными позволяет раскрыть внутренние состояния системы и в конечном итоге узнать секретный ключ.

Интересные факты

Устройство unlooper для вывода смарт-карт из бесконечного цикла использует АМИС.

Для извлечения секретного ключа может хватить единственного сбоя в работе криптографического алгоритма. Например, достаточно одной ошибки, чтобы полностью скомпрометировать алгоритм асимметричного шифрования RSA CRT (реализация RSA, использует китайскую теорему об остатках для ускорения работы).

Атаки методом индуцированных сбоев

Общие меры защиты от АМИС

Существует ряд защитных мер - как аппаратных, так и программных, - которые способны затруднить

проведение любой атаки методом индуцированных сбоев:

- внутренний дрейфующий генератор тактового сигнала - затрудняет синхронизацию времени внесения ошибки и генерацию сбоя;
- внесение случайных задержек в ход выполнения программы - существенно усложнит подбор времени для внесения сбоя;
- внедрение верификации, включающей проверку валидности принятых решений, адресов и данных - может предотвратить успешное внесение сбоя. Для реализации данной меры используется двойная проверка важных с точки зрения безопасности условий, а также проверка контрольных сумм уязвимых данных. Если верификация не пройдена, устройство должно перейти в заблокированное состояние или стереть свои секретные данные;
- использование счетчика исключений, которые генерируются в устройстве при внесении сбоев. Если значение счетчика выходит за границы, предусмотренные производителем, то устройство блокируется и не позволяет провести необходимое количество атак.

Атаки методом индуцированных сбояв

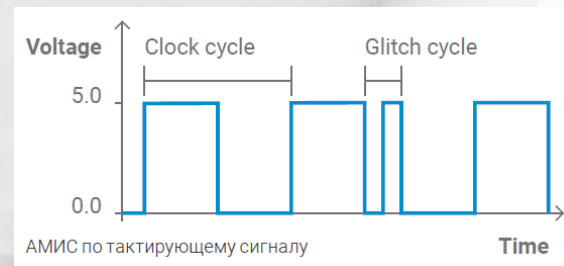
АМИС по тактирующему сигналу

Чтобы успешно провести такую атаку, крайне важно выбрать подходящее время для внесения сбоя. Как правило, для синхронизации используют ПЛИС, которая отсчитывает определенное количество тактов после некоторого выбранного атакующим события (триггера).

Если выбор триггера представляет затруднения (например, в случае внесения случайных задержек в работу алгоритма), используют методы АВК для поиска паттерна по сторонним каналам в реальном времени (realtime pattern matching). Это позволяет с высокой точностью подбирать момент для внесения сбоя.

При АМИС оптическим и электромагнитным импульсом, а также АМИС путем смещения базового напряжения на подложке важно выбрать не только время, но и конкретное место на кристалле ИС для внесения сбоя.

С помощью высокоточных столиков для позиционирования образца и специальных манипуляторов в автоматизированном режиме проводят поиск наиболее подходящей области для атаки. Как правило, для атакующего представляет интерес внесение ошибок в работу центрального процессора, криптопроцессора и дешифраторов памяти.



Атаки методом индуцированных сбоев

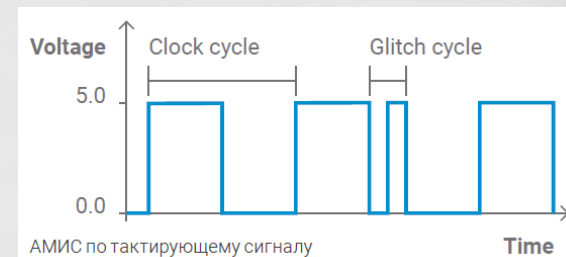
АМИС по тактирующему сигналу

В кристалле ИС электрический сигнал распространяется неравномерно и не достигает каждой точки электрической схемы одновременно - этому мешают различия в длине проводников, а также задержки в логических элементах. Чтобы обеспечить корректную работу устройства, производитель задает максимальную тактовую частоту, которая определена максимальной задержкой прохождения электрического сигнала среди элементов ИС.

Если внести кратковременный сбой в тактовый сигнал, заставив его выйти за пределы определенной производителем частоты, атакующий может добиться того, что будет некорректно выполнена единственная инструкция, а после возобновится нормальная работа процессора.

АМИС по тактирующему сигналу (clock glitching) основана на внесении именно таких сбоев. Заметим, что она применяется только к устройствам, для которых тактовый сигнал задается внешним генератором.

Данный вид АМИС начал широко использоваться в середине 1990-х гг. для атаки на смарт-карты спутникового телевидения. Современные смарт-карты защищены от нее за счет встроенного генератора тактирующего сигнала. Однако атака не потеряла актуальности: в работе «When clocks fail. On critical paths and clock faults» (М. Aqoyan et. al.) за 2010 г. описаны тонкости ее работы и приведена демонстрация успешного применения против алгоритма AES, реализованного на ПЛИС.

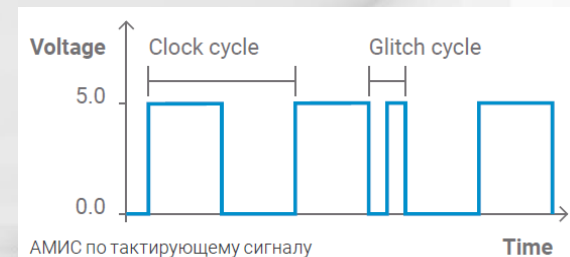


Атаки методом индуцированных сбоев АМИС по тактирующему сигналу

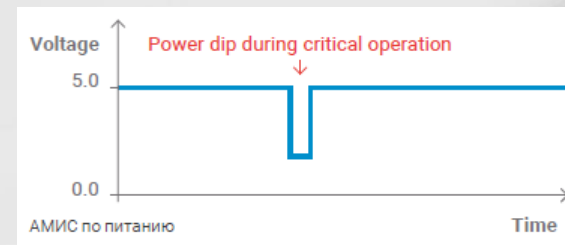
Меры защиты от АМИС по тактирующему сигналу

Для защиты от данного вида атаки могут быть использованы:

- схема мониторинга тактовой частоты, которая выполняет перезагрузку ЦП, если частота выходит за границы предусмотренного диапазона;
- внутренний генератор тактирующего сигнала.



Атаки методом индуцированных сбоев АМИС по питанию



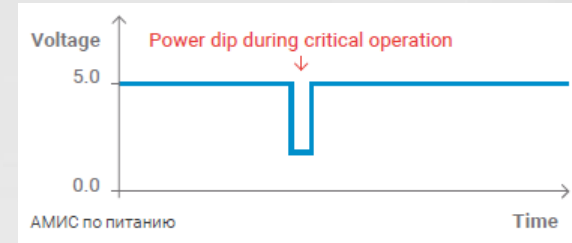
Интересные факты

Яркий пример АМИС по питанию - обход защитных механизмов на ARM микроконтроллере STM32 F2, подробно описанный в работе «Wallet.fail». Это исследование безопасности аппаратных криптокошельков демонстрирует, что самые защищенные технологии не помогают, если АО уязвимо.

Кремний прозрачен для электромагнитного излучения в инфракрасном диапазоне. Эта особенность помогает проводить атаки с обратной стороны кристалла ИС (обычно применяют лазерный импульс с длиной волны 1064 нм).

Атаки методом индуцированных сбояв

АМИС по питанию



Обычно в кристалле ИС полное напряжение питания, например 3,3 В, принимается за логическую единицу, а нулевое напряжение - за логический ноль. В зависимости от того, какой сигнал подан на затвор транзистора, он находится или в открытом, или в закрытом состоянии.

Однако при кратковременном понижении питающего напряжения логические элементы ИС переключаются медленнее, некоторые сигналы не успевают распространиться за отведенный такт, поэтому нельзя предсказать, в каком состоянии «защелкнутся» триггеры. В результате нарушится нормальное функционирование устройства: инструкция исполнится некорректно или вовсе будет пропущена, могут возникнуть ошибки при чтении или записи данных в память. Именно такого поведения и пытается добиться атакующий при АМИС по питанию (power glitching).

Иногда АМИС по питанию можно провести без какого-либо специального оборудования, лишь с помощью программного обеспечения.

Примером служат атаки Rowhammer и CLKSCREW. Принцип работы CLKSCREW заключается в следующем: атакующий получает доступ к системе контроля напряжения и частоты процессора и обеспечивает стрессовые условия работы устройства, что приводит к появлению ошибок в вычислениях. Применение метода дифференциальных искажений позволяет узнать секретный ключ.

Атаки методом индуцированных сбоев АМИС по питанию

Меры защиты от АМИС по питанию

Защитной мерой от данной атаки может выступать схема мониторинга напряжения, которая выполняет перезагрузку ЦП, если напряжение выходит за границы предусмотренного диапазона.

Атаки методом индуцированных сбоев АМИС оптическим импульсом

Полупроводниковые транзисторы чувствительны к свету: воздействие оптическим импульсом может инициировать переключение их состояния.

Эта особенность легла в основу АМИС оптическим импульсом (optical FI, laser FI).

Техническое оборудование для атаки обычно включает стол для точного позиционирования образца, микроскоп и инфракрасную камеру, а также сильный источник оптического излучения, например фотовспышку или лазерную установку.

С помощью фокусированного лазерного импульса атакующий генерирует кратковременный сбой в определенных элементах кристалла ИС.



Установка для АМИС оптическим импульсом. Источник: riscure.com

Для проведения АМИС оптическим импульсом атакующему необходимо получить доступ к поверхности кристалла ИС - провести декапсуляцию, а часто и утончение кремниевой подложки.

Второе позволяет достичь наилучшего результата при атаке с обратной стороны кристалла (backside).

Атаки методом индуцированных сбояв АМИС оптическим импульсом

АМИС оптическим импульсом - одна из самых применяемых атак своего класса, так как механизмы защиты от нее реализованы лишь на небольшом количестве ИС. Впервые подобные атаки на защищенные смарт-карты и микроконтроллеры описали С. Скоробогатов и Р. Андерсон в 2003 г. в статье «Optical fault induction attacks». Они спрогнозировали, что АМИС оптическим импульсом может оказаться серьезной проблемой для индустрии - и оказались правы.



Установка для АМИС оптическим импульсом. Источник: riscure.com

Атаки методом индуцированных сбоев АМИС оптическим импульсом

Меры защиты от АМИС оптическим импульсом

Для предотвращения данной атаки можно использовать следующие меры:

- защитный экран в верхних слоях металлизации для защиты транзисторов от воздействия оптического излучения (эффективно против атак с фронтальной стороны кристалла);
- оптические датчики, которые реагируют на лазерное излучение;
- датчики света, срабатывающие при вскрытии корпуса ИС.

Атаки методом индуцированных сбоев АМИС электромагнитным импульсом

Данная атака основана на кратковременном воздействии сильным электромагнитным импульсом (ЭМИ) на определенную область кристалла ИС. Это вызывает изменение в токах в устройстве и приводит к кратковременному сбою в работе внутренних логических элементов. Согласно последним исследованиям, эффект, который данная атака производит на логические элементы ИС, схож с эффектом от АМИС по тактирующему сигналу.

АМИС ЭМИ (electromagnetic fault injection) по своей природе является неразрушающей и не оставляет практически никаких следов на атакуемом устройстве, хотя в некоторых случаях требует декапсуляции: это увеличивает эффективность применения электромагнитного импульса.



Установка для АМИС электромагнитным импульсом. Источник: langer-emv.de

Атаки методом индуцированных сбоев АМИС электромагнитным импульсом

Преимущество данной атаки - возможность обхода мер защиты, которые предотвращают проведение других АМИС, например датчиков лазерного излучения или системы мониторинга линии питания.

Использование миниатюрного пробника позволяет с высокой точностью выбирать место внесения сбоя и воздействовать только на область интереса, не затрагивая другие функциональные блоки ИС.

Идея данной атаки была предложена Ж. Ж. Квискватером и Д. Самайдом в 2002 г. (J.J. Quisquater, D. Samyde. Eddy current for magnetic analysis with active sensor). Они показали, как можно вносить ошибку в криптографические вычисления, при помощи источника электромагнитного импульса собственной разработки. Сегодня эта атака - одна из самых эффективных, так как защитные меры от нее реализовать достаточно сложно.



Установка для АМИС электромагнитным импульсом. Источник: langer-emv.de

Атаки методом индуцированных сбояв АМИС электромагнитным импульсом

Меры защиты от АМИС электромагнитным импульсом

В качестве аппаратной меры защиты от АМИС ЭМИ возможно применение датчика синхронизации (timing sensor), который отслеживает корректное прохождение сигнала по пути с наибольшей задержкой. Программные меры защиты (перечислены ранее в обзоре АМИС) также могут быть использованы для защиты от данной атаки.

Атаки методом индуцированных сбояв

АМИС путем смещения базового напряжения на подложке

Создание положительного или отрицательного смещения напряжения на подложке кристалла ИС - известная техника управления производительностью и статической потребляемой мощностью. Идея данной атаки (RBBI / FBBI FI) заключается в кратковременном воздействии импульсом высокого напряжения на кремниевую подложку с помощью генератора импульса и проводящего зонда. В результате пороговое напряжение переключения транзисторов смещается, что приводит к кратковременным сбоям в работе устройства.



Установка для АМИС путем смещения базового напряжения на подложке. Источник: riscure.com

Для успешной реализации этой АМИС необходимо провести декапсуляцию кристалла ИС и утончить кремниевую подложку, чтобы уменьшить ее сопротивление.

Эта атака, как и АМИС ЭМИ, позволяет обойти большинство известных мер защиты: системы мониторинга питания и тактирующего сигнала, датчики лазерного излучения и др. Однако у нее есть важное преимущество: за счет особенностей проводимости кремния здесь возможна меньшая область воздействия и, соответственно, большая точность.

Атаки методом индуцированных сбоев

АМИС путем смещения базового напряжения на подложке

Данная техника внесения кратковременных сбоев относительно новая для отрасли. Впервые ее предложила группа исследователей в 2012 г. (Ph. Maurine et al. Yet another fault injection technique: by forward body biasing injection).

Из-за этой новизны еще не появилось проверенных временем мер защиты от указанного типа АМИС, так что все исследования на данную тему заслуживают пристального внимания.



Установка для АМИС путем смещения базового напряжения на подложке. Источник: riscure.com

Меры защиты от АМИС путем смещения базового напряжения на подложке

В качестве защитной меры от данной атаки рекомендуется располагать по всей поверхности кристалла ИС массив датчиков, которые производят тестовые вычисления на каждом процессорном такте и сравнивают вывод с ожидаемым результатом.

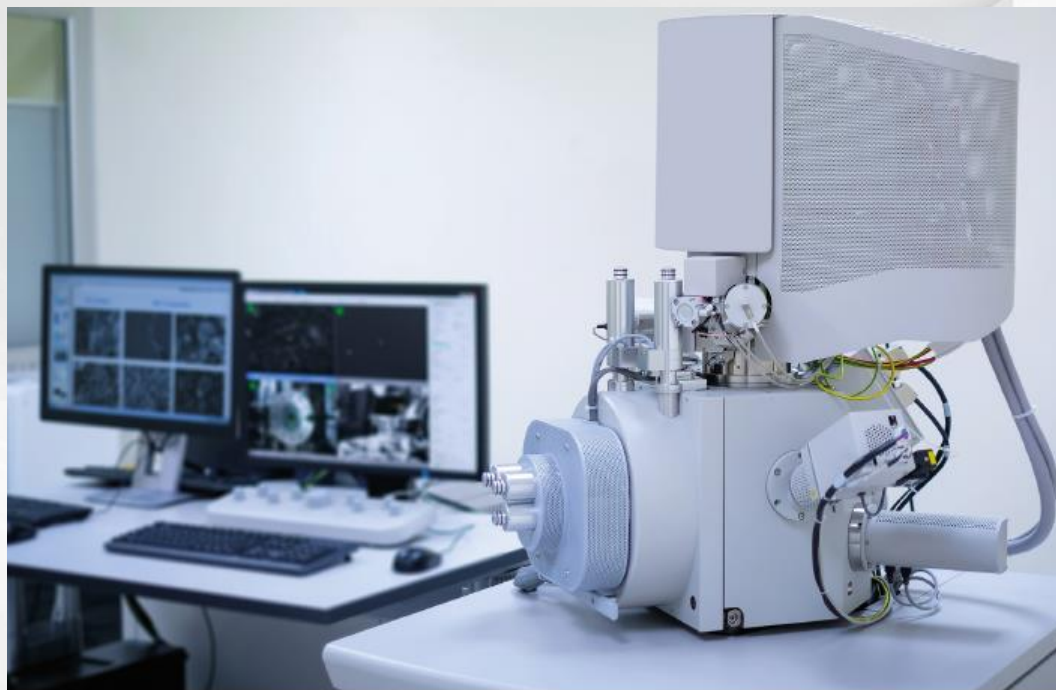
При возникновении сбоя вычисления будут выполнены неверно, что может служить сигналом для стирания секретных данных или остановки работы всей ИС.

Инвазивные атаки

Инвазивные атаки (invasive attacks) - это разновидность аппаратных атак, для реализации которых необходим прямой доступ к внутренним элементам кристалла ИС. Воздействия такого рода дают атакующему почти неограниченные возможности для извлечения информации и исследования функциональности электронного устройства. Обычно для этих атак нужны специализированное дорогостоящее оборудование и высокий уровень подготовки.

Последствие всех инвазивных атак - необратимое изменение физических свойств кристалла ИС.

Чтобы лучше понимать, как проводят данные атаки, необходимо иметь общее представление о внутреннем строении кристалла ИС. Упрощенно говоря, он включает МОП-транзисторы на кремниевой подложке и многослойную систему проводников, разделенных диэлектриком, которая обеспечивает соединение транзисторов друг с другом. Сверху кристалл защищен пассивирующим слоем (passivation) - барьером против влажности и воздуха, которые могут ему навредить.



Сканирующий электронный микроскоп

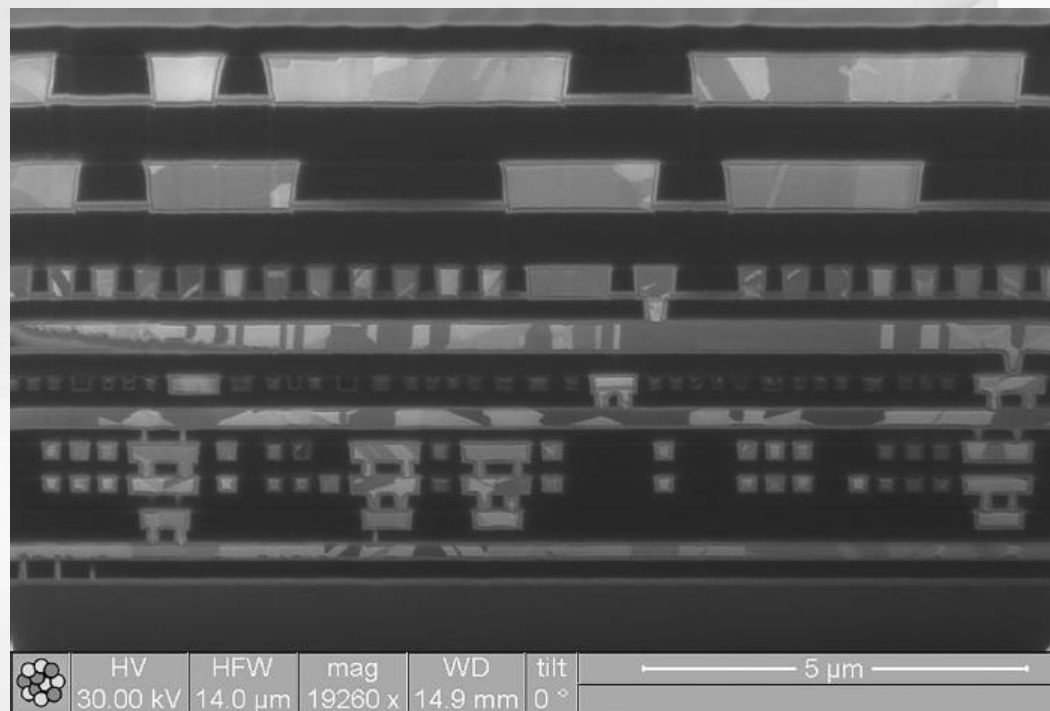
Инвазивные атаки

Для подготовки микросхемы к инвазивным атакам нужно выполнить декапсуляцию, тем самым освободив кристалл ИС от корпуса, и частично или полностью удалить пассивирующий слой.

Наиболее известные примеры применения инвазивных атак - упомянутые ранее подделка картриджей для принтеров, контроллеров для игровых консолей и смарт-карт, открывающих доступ к просмотру платного телевидения. Но пиратством цели таких атак не ограничены: злоумышленники могут их использовать также для кражи интеллектуальной собственности и извлечения секретной информации из устройств.

Условно инвазивные атаки можно разделить:

1. обратная разработка,
2. микрозондовый анализ
3. модификация кристалла ИС.



Кроссекция ИС

Однако на практике их проводят в комплексе, поэтому мы не будем рассматривать защитные меры в отдельности для каждой атаки. Вместо этого мы приведем общий список мер в конце раздела, когда подробнее опишем суть и цели конкретных видов инвазивных атак.

Инвазивные атаки

Обратная разработка ИС

Обратная разработка позволяет получить представление о структуре, алгоритмах и логике работы, заложенных производителем в ИС. Идея данной атаки - в извлечении информации о соединении микросэлектронных компонентов друг с другом и последующем анализе электрической схемы, реализованной в кристалле ИС.

Для проведения обратной разработки необходимо выполнить депроцессинг (deprocessing, delayering). Эта процедура противоположна производству кристалла ИС: она заключается в последовательном удалении слоев металлизации вплоть до кремниевой подложки, на которой расположены транзисторы. Существует несколько методов послойного препарирования кристалла ИС: жидкостное травление (wetchemistry etching), плазменное травление (RIE - reactiveion etching), а также различные виды полировки (например, CMP - chemical-mechanical polishing). Как правило, при депроцессинге используют все выше перечисленные методы.

Интересные факты

Предел оптического микроскопа - 150 нм, объекты меньших размеров уже неразличимы. Для получения изображений с большим разрешением применяют электронные, рентгеновские и атомно-силовые микроскопы.

Чтобы получить изображения кремниевой подложки, нужно удалить все слои металлизации. Для этого часто используют химический метод - травление с помощью плавиковой кислоты (это единственная кислота, которая разъедает стекло). Недостаток такого способа - опасность: приходится работать с сильно ядовитой кислотой.

Инвазивные атаки

Обратная разработка ИС

Для выбора методов и формирования стратегии процедуры депроцессинга атакующий анализирует изображения поперечного сечения исследуемого кристалла ИС (IC cross section): определяет количество слоев, их толщины, используемые при производстве материалы. Этот анализ подсказывает, какие методы в какой последовательности нужно применить для депроцессинга.

Во время препарирования кристалла атакующий с помощью оптического (optical microscope) или сканирующего электронного микроскопа (SEM – scanning electron microscope) фотографирует каждый слой. Полученные изображения обрабатывают и в результате получают таблицу соединений кристалла ИС. Она позволяет смоделировать работу кристалла и проанализировать области, представляющие интерес для атакующего.

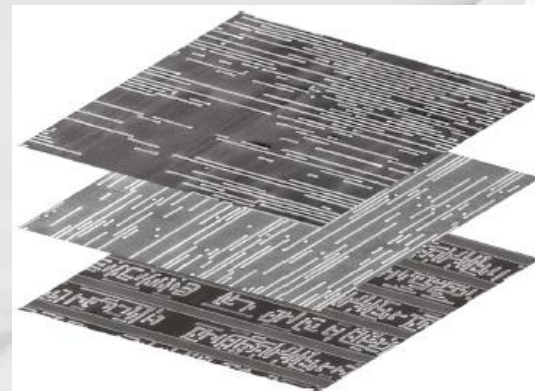


Инвазивные атаки

Обратная разработка ИС

Добравшись до определенного слоя, атакующий при помощи оптической и электронной микроскопии может извлечь информацию из масочных ПЗУ (ROM): в каждой ячейке памяти хранится один бит информации - нуль или единица, - а ее конкретное значение хорошо различимо на изображении. Для получения полного дампа ROM нужно распознать значения всех бинарных ячеек (обычно это выполняют в полуавтоматическом режиме с помощью специализированного ПО) и установить порядок следования строк и столбцов в массиве памяти (определяют с помощью обратной разработки схемы адресации или простым перебором).

Иначе обстоит ситуация с электрически стираемым перепрограммируемым ПЗУ (EEPROM и Flash). Состояние ячеек данного вида памяти считать с изображения проблематично (хотя такие методы и существуют). Связано это с тем, что все ячейки устроены одинаково, а информация в них хранится с помощью заряда в плавающем затворе. Чтобы считать информацию из такого вида ПЗУ, может потребоваться комбинация микрозондового анализа и модификации кристалла ИС.

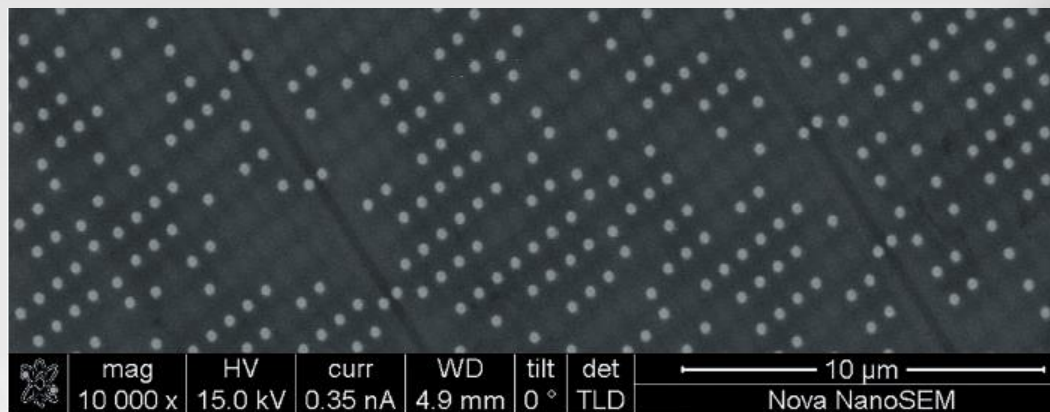


Обработка изображений
слоев ИС

Инвазивные атаки

Обратная разработка ИС

Когда речь идет о микроконтроллерах или смарт-картах, атакующий обычно проводит обратную разработку как аппаратной, так и программной части кристалла ИС. Например, довольно часто встречается ситуация, когда атакующему удалось извлечь данные из энергонезависимых ЗУ, но они зашифрованы на аппаратном уровне.



Масочная память (ROM)

В этом случае на кристалле ИС выделяют область, отвечающую за шифрование и расшифрование данных, и выполняют анализ этого участка.

Выяснив алгоритм или ключ, данные из энергонезависимого ЗУ дешифрируют и дизассемблируют, и атакующий получает возможность анализировать встроенное ПО.

В результате проведения данной атаки интегральная схема необратимо разрушается и теряет работоспособность.

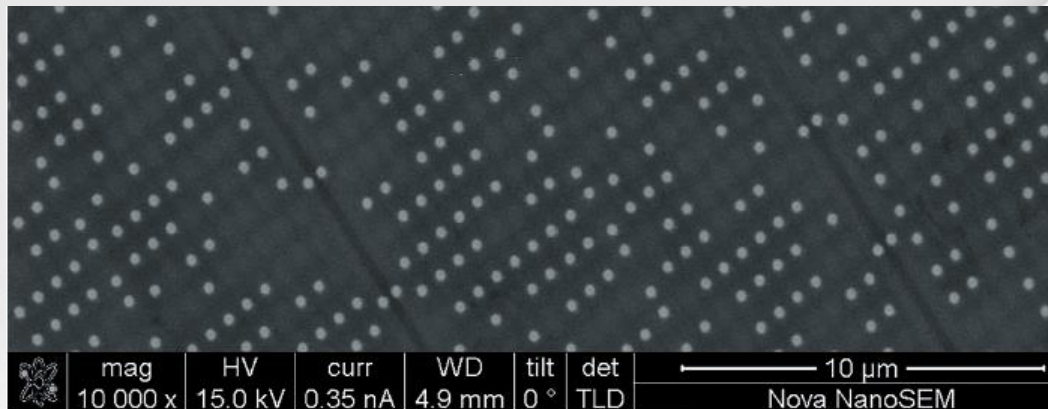
Инвазивные атаки

Обратная разработка ИС

Интересные факты

Для автоматизации задач обратной разработки ИС (соединение изображений, распознавание логических ячеек и трассировка соединений), как правило, используют программные решения.

Пример коммерческого ПО - CHIPJUICE от французской компании Texplained.



Масочная память (ROM)

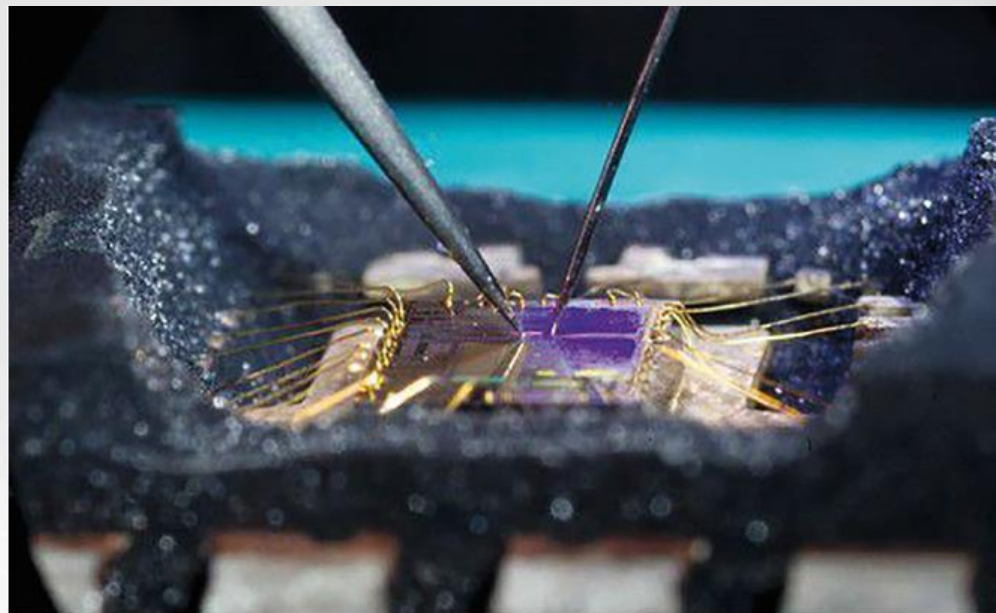
Содержимое EEPROM может быть стерто ультрафиолетовым излучением.

Это иногда используют для обхода защитных мер ИС, например для стирания установленных битов защиты (если они выполнены в виде отдельных EEPROM-ячеек).

Инвазивные атаки

Микрозондовый анализ

Основной инструмент для микрозондового анализа (microprobing) - зондовая станция (probe station). Она включает комплект технических средств на базе оптического или электронного микроскопа и предназначена для точного позиционирования зондов на контактные площадки полупроводниковых устройств, создания электрических контактов в необходимых точках для регистрации или подачи сигналов. В результате проведения этой атаки сохраняется работоспособность и исходная функциональность интегральной схемы.



Микрозондовые пробники. Источник: aisee.fraunhofer.de

Интересные факты

Изменение заряда в ячейке EEPROM основано на квантовом туннельном эффекте.

У оптического микроскопа в микрозондовых станциях большое фокусное расстояние: это нужно для позиционирования игл.

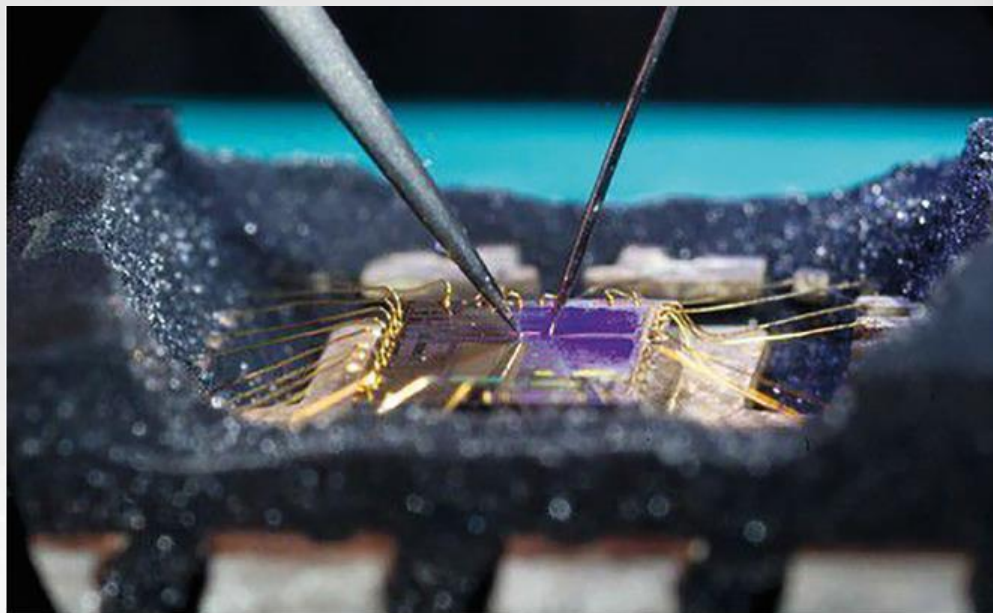
Инвазивные атаки

Микрозондовый анализ

Чтобы зонды могли установить электрический контакт с проводниками в верхнем слое металлизации, необходимо точно удалить пассивирующий слой.

Как правило, для этой операции используют технологию лазерной резки. Сфокусированный лазерный луч удаляет только определенные участки пассивирующего слоя, открывая зондам доступ к нужным электрическим линиям.

Иногда шина данных, к которой необходимо подключиться, не выведена на верхний слой металлизации, а расположена во внутренних слоях. Чтобы получить доступ к таким проводникам, используют систему фокусированного ионного пучка (ФИП, англ. FIB - focused ion beam).



Микрозондовые пробники. Источник: aisee.fraunhofer.de

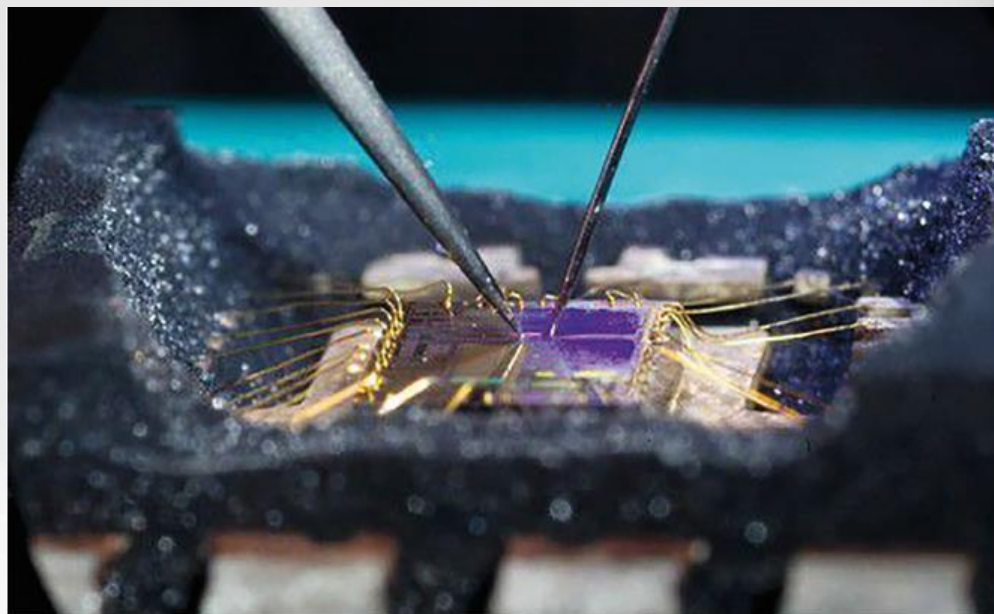
Интересные факты
Микрозондовые иглы делают из вольфрама. Разрешение современных ФИП - около 5 нм.

Инвазивные атаки

Микрозондовый анализ

Такая система дает возможность изменять структуру кристалла ИС с высокой точностью (единицы нанометров) путем удаления или нанесения материала (проводника или диэлектрика).

Это позволяет вывести контакты к внутренним сигналам на поверхность ИС и подключиться к ним с помощью микрозондовой станции.



Микрозондовые пробники. Источник: aisee.fraunhofer.de

Микрозондирование бывает *пассивным* и *активным*.

В первом случае атакующий считывает интересующие его данные, не вмешиваясь в вычислительные процессы ИС. Во втором случае атакующий воздействует на устройство, посылая в определенный момент электрические сигналы. Это позволяет изменить нормальный ход работы и обойти меры защиты, предусмотренные производителем ИС.

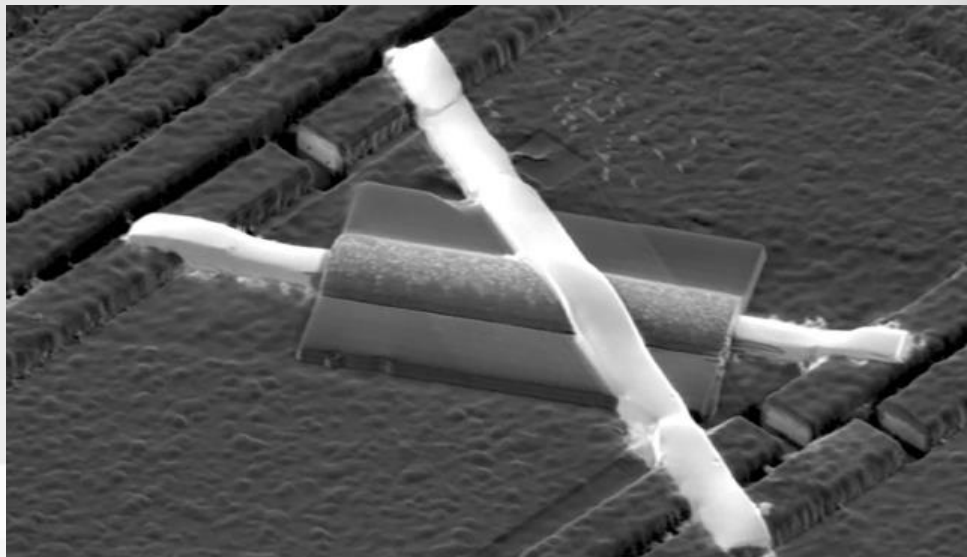
Инвазивные атаки

Модификация кристалла ИС

При модификации кристалла ИС атакующий вносит изменения в заложенную производителем электрическую схему, чтобы извлечь информацию и обойти различные защитные меры.

Обычно при подготовке к этой атаке предварительно проводят частичную обратную разработку кристалла ИС: не имея представления о его внутреннем устройстве, невозможно внести в него осмысленную модификацию.

Яркий пример использования данной атаки - извлечение защищенного от чтения содержимого энергонезависимого перепрограммируемого ЗУ (EEPROM).



Модификация ИС с помощью ФИП. Источник: nanoscopeservices.com

Интересные факты

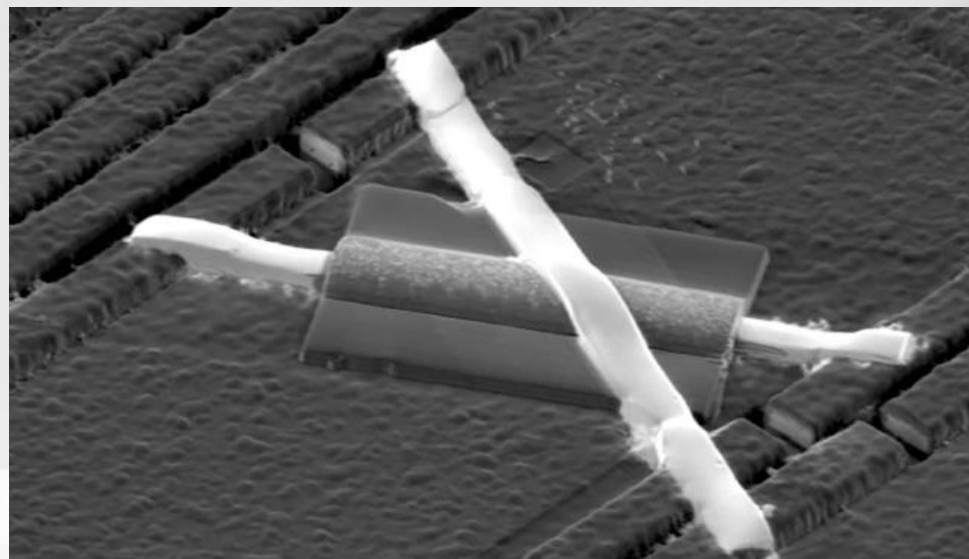
Проводник или диэлектрик наносят на поверхность образца так: вводят специальные газы в рабочую камеру и осаждают атомы фокусированным ионным пучком.

Для ФИП нужен стабильный источник. Самые распространенные источники ионов - так называемые жидкометаллические, в которых используется галлий. Температура плавления галлия - около 30 °С.

Инвазивные атаки

Модификация кристалла ИС

Один из вариантов модификации ИС позволяет отключить механизм безопасности, удаляющий данные из EEPROM. Эта мера защиты активируется при попытке несанкционированного доступа или при нарушении целостности защитного экрана (shield).



Модификация ИС с помощью ФИП. Источник: nanoscopeservices.com

Однако для очистки содержимого такого вида памяти нужно высокое напряжение стирания, которое генерирует специальная схема с накачкой заряда (charge pump).

Оборвав электрическую линию, связывающую ЗУ с этой схемой, атакующий может больше не беспокоиться о защитных мерах: сигнал на удаление никогда не дойдет до EEPROM.

Инвазивные атаки

Модификация кристалла ИС

Модификация кристалла позволяет также извлекать зашифрованное содержимое из EEPROM (или Flash) - для этого нужно нарушить нормальную работу ядра процессора, отвечающего за ход выполнения программы.

Адрес инструкции, которая в следующий момент времени будет считана из EEPROM и выполнена ядром, определяется счетчиком команд (program counter). Подключившись с помощью микрозондовой станции к выходной шине данных ЗУ, атакующий может наблюдать последовательность выполняемых инструкций – но получить полный дамп памяти таким образом не удастся. Связано это с нелинейным исполнением программ: условия, циклы и возвраты – эти инструкции постоянно перенаправляют поток выполнения.

Однако с помощью ФИП атакующий может получить доступ к схеме управления регистром инструкций (instruction register) и сигналом с микрозонда перевести его в режим хранения в нужный момент времени. Это позволит «защелкнуть» в регистре одну единственную инструкцию, которую будет выполнять процессорное ядро и тем самым последовательно увеличивать счетчик команд. Таким образом атакующий может линейно считать содержимое EEPROM с шины данных. Эта техника называется linear code extraction и работает в том числе для зашифрованной памяти.

Атакующему лишь нужно снимать сигналы непосредственно перед регистром инструкции, так как к нему они приходят уже в расшифрованном виде.

Инвазивные атаки

Модификация кристалла ИС

Интересный факт

Кристалл американских микропроцессоров CVAX содержит фразу «СВАКС... Когда вы заботитесь довольно воровать настоящий лучший». Именно так разработчики микропроцессора перевели на русский язык фразу «CVAX - when you care enough to steal the very best» («CVAX - когда озаботились тем, чтобы украсть самое лучшее»).

Послание оставили советским инженерам, на случай если те попробуют скопировать решение. Иронично, что сама фраза - пример копирования. Это измененный слоган известного поставщика поздравительных открыток, фирмы Hallmark Cards: «When you care enough to send the very best («Когда вы заботитесь о том, чтобы послать самое лучшее»).

Инвазивные атаки

Модификация кристалла ИС

Общие меры защиты от инвазивных атак

Для защиты кристалла ИС от инвазивных атак можно использовать следующие меры:

- шифрование содержимого ПЗУ, препятствующее анализу дампов памяти;
- защитный экран в верхних слоях металлизации, при нарушении целостности которого подается сигнал на стирание EEPROM;
- датчики света, которые срабатывают при декапсуляции микросхемы и нарушают функциональность устройства;
- физически неклонируемые функции (PUF - physically unclonable functions), используемые для активации устройства;
- маскировка логических элементов - техника расположения стандартных ячеек с различной функциональностью в активном слое таким образом, чтобы они казались идентичными. Если для обратной разработки ИС с этой мерой защиты использовать автоматизированные средства, таблица соединений может выйти ошибочной;
- аппаратная обфускация - техника создания более сложной схемы устройства, имеющей такую же функциональность, как и оригинальная. В результате увеличиваются время и стоимость обратной разработки.

Инвазивные атаки

Закладки в ИС

Внедрение аппаратных закладок - одна из самых изощренных атак на интегральную схему. В результате внедрения бэкдора в производимую ИС атакующий получает несанкционированный доступ к данным или полный контроль над ПО, несмотря на все защитные меры.

Обычно закладки внедряют еще на этапе разработки и производства ИС. К сожалению, особенности работы полупроводниковой индустрии предоставляют множество возможностей для этого. Треть производителей отдают изготовление ИС на аутсорсинг, а при проектировании микросхем многие используют сторонние готовые блоки. В результате найти полностью доверенного производителя трудно. Пока эта ситуация не изменится, интегральные схемы останутся уязвимыми для злонамеренного вмешательства и внедрения аппаратных закладок.

Жизненный цикл разработки новой интегральной схемы состоит из трех основных частей:

1. проектирование,
2. производство,
3. тестирование и проверка.

Интересный факт

Физически неклонируемые функции по своей природе бывают:

- оптические (пузыри воздуха в стекле),
- кремниевые (произвольные задержки распространения сигнала),
- магнитные (структура магнитной полосы).

Инвазивные атаки

Закладки в ИС

Проектирование интегральной схемы начинается с составления спецификации. Теоретически на данном этапе злоумышленники могут внести изменения в функциональность и протоколы, однако на практике это маловероятно. Куда более реальна угроза атаки непосредственно в процессе проектирования.

Во-первых, из-за постоянно увеличивающейся сложности проектов и из-за ограничений по времени разработчики часто используют уже готовые сторонние IP-блоки и библиотеки - а они могут содержать вредоносную функциональность.

Во-вторых, при работе в известных системах автоматизированного проектирования с общепринятыми доверенными инструментами разработки многие инженеры-конструкторы запускают сторонние TCL-скрипты, не являющиеся доверенными.

Интересный факт

Методы АВК способны обнаружить недеklarированные возможности ИС. Интересное исследование на эту тему – работа С. Скоробогатова и К. Вудса «Breakthrough silicon scanning discovers backdoor in military chip».

Инвазивные атаки

Закладки в ИС

Этап производства включает подготовку масок и полупроводниковых пластин, где задействованы производственные процессы окисления, диффузии примесей, ионной имплантации, металлизации и литографии. Довольно часто заказчик отдает процесс фотолитографии на аутсорсинг и не контролирует его. На этом этапе злоумышленник может изменить параметры производственного процесса, конфигурацию маски или добавить злонамеренную схему, подменив GDSII-файл с информацией о топологии интегральной схемы.

Этап тестирования заключается в подаче на вход ИС тестового вектора данных и проверке корректности ожидаемых выходных значений. Тестирование способно выявить внедренную закладку, но злоумышленники могут подготовить испытательные вектора или оборудование таким образом, чтобы скрыть встроенный бэкдор.

Производитель ИС может и сам намеренно внедрить аппаратную закладку в разрабатываемое устройство, чтобы в будущем иметь возможность нарушить нормальный режим работы или получить несанкционированный доступ к секретным данным клиента.

Яркий пример использования аппаратных закладок - внезапный отказ сирийской системы воздушной обороны в сентябре 2007 г., когда израильские самолеты бомбили предполагаемый ядерный реактор в Сирии. Считается, что микроконтроллеры в сирийском радаре были изготовлены со скрытым бэкдором внутри. При полете израильских самолетов систему воздушной обороны дистанционно заблокировали, и израильские вооруженные силы смогли беспрепятственно атаковать стратегически важный объект.

Инвазивные атаки

Закладки в ИС

Меры защиты от закладок в ИС

Чтобы гарантировать отсутствие аппаратных закладок в произведенной ИС, необходимо сделать все этапы разработки доверенными (что довольно сложно в условиях современной бизнес-модели) или провести обратную разработку ИС (что не все производители могут себе позволить).

Наиболее реальная мера защиты - проведение серьезного тестирования готовой ИС самими разработчиками или в доверенном испытательном центре.