Тема 1.5 Безопасность микропроцессорных систем

Некоторые встроенные системы находят массовое применение, например, устройства RFID. Встроенные системы являются привлекательной целью для создателей вредоносного кода из-за своей распространённости и относительной беззащитности. Постепенно злоумышленники пытаются создать вредоносный код для встроенных систем (например, RFID-вирус, Cabir). Этот процесс пока затрудняется разнородностью встроенных устройств, отсутствием доминирующего ПО и ограниченной функциональностью некоторых видов устройств. С другой стороны, задача антивирусных компаний и исследователей компьютерной безопасности осложнена теми же обстоятельствами, а также маломощностью встроенных систем, зачастую не позволяющей пользоваться распространённым антивирусным ПО.

При передаче сигнала через любой канал связи возможно возникновение ошибок, которые могут приводить к искажению переносимой информации. Существует много методов для исправления подобных ошибок, но прежде чем исправлять, необходимо эти ошибки обнаружить. Для этого также существуют определенные методы, основанные на избыточности передаваемой информации, что позволяет не только выявлять наличие факта искажения информации, но и в ряде случаев устранять эти искажения. Наиболее известные из методов обнаружения ошибок передачи данных являются:

- 1. Посимвольный контроль четности, называемый также поперечным, подразумевает передачу с каждым байтом дополнительного бита, принимающего единичное значение по четному или нечетному количеству единичных битов в контролируемом байте. Посимвольный контроль четности прост как в программной, так и в аппаратной реализации, но его вряд ли можно назвать эффективным методом обнаружения ошибок, так как искажение более одного бита исходной последовательности резко снижает вероятность обнаружения ошибки передачи. Этот вид контроля обычно реализуется аппаратно в устройствах связи.
- 2. Поблочный контроль четности, называемый продольным. Схема данного контроля подразумевает, что для источника и приемника информации заранее известно, какое число передаваемых символов будет рассматриваться ими как единый блок данных. В этой схеме контроля для каждой позиции разрядов в символах блока (поперек блока) рассчитываются свои биты четности, которые добавляются в виде обычного символа в конец блока. По сравнению с посимвольным контролем четности поблочный контроль четности обладает большими возможностями по обнаружению и даже корректировке ошибок передачи, но все равно ему не удается обнаруживать определенные типы ошибок.
- 3. Вычисление контрольных сумм. В отличие от предыдущих методов для метода контрольных сумм нет четкого определения алгоритма. Каждый разработчик трактует понятие контрольной суммы по-своему. В простейшем виде контрольная сумма это арифметическая сумма двоичных значений контролируемого блока символов. Но этот метод обладает практически теми же недостатками, что и предыдущие, самый главный из которых нечувствительность контрольной суммы к четному числу ошибок в одной колонке и самому порядку следования символов в блоке.
- 4. Контроль циклически избыточным кодом CRC (Cyclical Redundancy Check). Это гораздо более мощный и широко используемый метод обнаружения ошибок передачи информации. Он обеспечивает обнаружение ошибок с высокой вероятностью. Кроме того, этот метод обладает рядом других полезных моментов, которые могут найти свое воплощение в практических задачах.

Пять шагов к обеспечению безопасности встраиваемых систем

В современных условиях ростущей связности вычислительных устройств проблемо: информационной безопасности выходит на один уровень с проблемой сложности ПО. Статья описывает пять шагов по обеспечению информационной безопасности: встраиваемых систем с учётом всех стадий их жизненного цикла от проектирования до разработки, тестирования, развёртывания и обслуживания.

Первый «звоночек»

2010 год ознаменовался первым «червём», способным внедряться в промышленную инфраструктуру и позволять валомщику перехватывать управление критическими системами, -Stuxnet. Он был разработан для атаки на центрифуги, используемые в ядерной программе Ирана, и отбросил работы по программе предположительно пьютеры. Многие современные сетена несколько лет назад. Stuxnet обладал — вые угрозы являются ещё более изощ-муру жар төнү учанар чекеру мер жар 1— балар, авон шарынаруу куруны старууны старууны са са танастурбураны алуубур та (ВПБ) сочина с селен ости съвъщих дочени, да дъбдалеся, изир сен вишени изичние и интистива дочен съвъщини възда дочен -ичной беоруничном попрубликом - то шруго честовной бинестольностисться к. — поспринечания клинестися. "

неспособность классических ПЛК противостоять сетевым вторжениям, так как при их проектировании предполагалось, что изолированная сеть системы управления безопасна по умолчанию. Stuxnet развежь этот миф. продемонстрировая способность вторгаться в изолированные сети систем управления через подключаемые к ним ком-

объёма требований увеличивает трудоёмкость разработки, а значит, и её стоимость. К тому же огромное число потенциально уклянмых встраиваемых систем, основанных на устаревших стратегиях безопасности, уже давно развёрнуты и эксплуатируются в современной тесно связанной сетевой среде. Потребности в поддержке облачных вычислений увеличивают степень связности устройств, тем са-

і фастиського менадарубар менафіре». — 6.9 жылі іс бійнеле торого, з осутерня — Мокце, высот не осущавання бейгаcauti filiata conserva assersa erra caracteria.

Дик верешендения верх высова со- (В возгобейн явие седа обёдения — присприявания, средствичения, га ших потим п, абби обдени то честия: байгаетчень этография издет установань, байт состав съща тист для динами, спффрацизация — v; межен — "siddy", 774 фонду", 220 ю — для и обфадан и личаций байны, бебили почетри институтуты дан, дин, институтуту институтуту институтуту институтуту институтуту институтутуту

BOST OLA

runar, abil most Bajar, atrians – фilica.....

оторуж энеканий боли. Идисстони, интерректирация и достои в это и от от от общести тарыясын орынуы: т20м, актичек — эр, жүнек-ийски орыны 2 Указачи, кышынды чыккелы≒кы чыс. вы чистем алидо экора адруживанского бібесь. — жыселейкие аддо на « құры о-афуум.....- е еліўналажній жілі пелій ылбайныў г-этом-- с быль трак экспештря — эргля архиб альный нами-афия нь---- с династически ученирующими. невиско-колин 1 турников на 1911 ирин относивания образования на и 2---- и мисто-новий в прек образования. мен икспечи прочистимы дорго срис- неш — Придемера)

Buchter of the said of the section o — вестантира се депание, с бранивич

ух-уч-Посумава унслуждующия- В'поисках золотой учен высточенуваевнося чена включ -- СЕРЕДИНЫ ылык анх ерүүлүн жүнин мененетен — В пласудеет ареая-лафор жердаetriania geta mano processima sectorкобо-уИот чь жа;хобления-ачь— в ем пурсиль в ченуяд обязот линих корро Сълствений бул газбиличет

Comparation (Section 1)

эта хиветальность в методае блас-

__(mus(-have).rs_6xpon x8.*O,parkx; sour

экских желему и жовчен- и подпроу-18 илипераружием или негом коро<u>т</u> п**и**ся. ferencesson.

Просмаробнок: безогоспоскую зедыorne onemed memorate mosesum com-MCCORD FREE

```
    степень вокности аспектов продукта, щищённой, да и предсказать, как имен- мых систем) кабербезопасностью назы-

подделения оченивающих возор завеляющих объеменного предвестивного
 AND DESCRIPTION OF STREET
                                                                          No. 14
рагозоров. — пункторов туровом коро упро — Самый эффотуровый поботок. — королючено четыеловый
expublification particular
                                                                                                                                                                    мия року стигобі і інкенсежня функция · · · · при питероську вій вици.

    Вистем в поры положение присти интерпацион (били положение порти и порти на при на пр
                                                      макаунацыя уграц.
                                                                                                                                                                         расие-к-болижени-каканадаке-а. - Для разрябичистичен
agregations a---
чериой экон..... Исыкун адконику, алагуюц иградолика — систочуга, экой дианалы экорады эко----- цанккой болизациоги ос
машума как----- пробрабана урового бейбине чести, задес — <u>паратывани</u>, актючна сосказно срему. При —чей и отности сище на визотел
уклан энцере..... энтный учрестверу затройнять, это целе..., — эном чем за более распей унадам жар...... зых, канорые затройнгого хр
риковся костоя экону райтен дестительний прове..., такором цисла изполнения процесе, дой-Обычанови датными
и в править в править при в п
жаях микух ски - попрорызкый прецосс, ехразы---

    вительности учения помитом с

жирет честя: 2 прицей жее жизчестый цука продус.....Ки вер везопасность и
                                                                                                                                                                                                                                                                                                 наличеть пад треф (
делжие быть та, ет проскторозован до выведи сворен — — информационная Ветривление устройство ;
                                                                                                                                                                                                                                                                                          ____реарибейшее такжее/браза
сеободоступ розника робей по обей пененого, фуду. Бельших его заправичения систем, везпекиметоватруктовых
далунку, за--- призада
                                                                           небек жылдармац кениебебес- - — еглиниотки эткерпаратия эмжендүүлө - — полсыральнену-элеууунд
полистия. постоя и поличествующего водение в поличествующего поличествующего в поличеству в поличествующего в поличеству
данных, Ст. ... неччеств двила придукции до такиста» - престава в обтруготовител, вхедищента - пристава и передуаленца-
нетиско была — щило об-ед-пенник будущих угрен — езепал иличений изфраструктуры. С — езена этщигы преклузы-,
рукум в под при в 
стеми име и чести эпрецесс разрабейся. прийски инпочесса 2.50, что иго — прев разгичных угрев — ст
                                                                                                                                                                   умышлет заключенцияльного жет уду---- де фётического доступу---
3—50 хими. Сложность в астёт, пенучина-контрана-зат управ——Накакай привазеданен избайт пенучина к имбертительной привазеданен достой привазеданен
                                                  Воброзавлице систему-радыци это — чэм-эх, лубо-англаать их же учесбой из завыесть из огран эле-
The state of the s
руды: Мир. . . . эксплуаторезативна евичествики экспии - метравальниция управить приводя — экспиуабрициальные д
дразумесьног — лириновыми ередии, веледетное четибы - - - с етклины в филическом поврежде экон: - - гос клиевы устровето се пе
ужите безст. уграт ва е изпучески т.С эвреме томе — еврем за презинуществение приста. — везбие, приня неврект
рудовая пр. устройство страко честь бывают это ... - равны на предстаращеную эссинация... - этимнесть эх фузиция за
(M2M) каза- ... чакдите кома облагая, а того мапра- ... - алкога - воформации ... Одовия для- - реравается межнализання
ре (кум лиск 🗀 мую-к И этер жеу: Обе́р этик-тране---- ветраниемых частем зенбиёдами обей ---- му энский в энфекторуют
Органиства. Дывотей как-ести также розполноства — почлани-се телько защему храновых и — сети эксрепелобаблиза, №
7 ып. предествення в персопродости в персопродости по персопродости п
применями. — бей вичили приформ (виморофой из или.), — несть обраниванием со фудеционаром — вынова и бей више со во на
жджритичен споризва при этом жесткие требейанов помия. Термиз - 4 кибё рбе велись него. — устрайств переходат-в разд

    к дамения бужностической выпольшение стиментальными учественными.

    щов чисть суплучноствет зыбан. — пельзуется как сименки терпиза⊠ин. —

эгрыштыфу экцурнациями это удабейне — формацурного бей энистический (им эти ---- Рек омендации по-
                                                 сепационную террине, как уже управа.... (ien assumme); адмистучкоф эрланда э---- повышению везоду
                                                 нались, также делист устройства более— теля бедения учеточения фармациям. В ВСТРАИВАЕМЫХ СИСТ
сина состем подверженным этемам.
                                                                                                                                                                       епределение — 40 жжупичеты мер, иг-- — Разрабойчикам ветралия

    Ещё держне было честь было доле — простемных за охрону в защему и фер.... при реше экспериент б

A STATE OF THE STATE OF
<u> может пр. — кото м</u>ожет петропання в прозначня — мацион моффиционня состатира — подускают в ведущего в
умены не ма..... прискта сущими изитуплющия эрикия.....тё<u>м</u> обейнечения их готивносторцения.....гот (рак. 1). Описываемов
эйтээ өнөөөс эничих устрайств нанадэх оў в разряд мести; комфёденцияльнеги; дэктовер-- — листея готаній экспутатага.
угл. перментередных соетемных треблент меня отнетредивночния удетущи к предвати обрежения пор.
печене 664.... исле-Чаўте, получання так, чтегаппа--- пенье[1], Терказ «кабарбіфпасаженняе пакоп<u>ол</u>учанняе печебай
                                             person and appropriation of the foreign and the contraction of the con
прадилены. — реширодыную<u>ть п</u>ежеленый былерац<del>ии с</del> вышелени сиродельных и симирос сис ___решеный, правилисьных и
прадукта. — рэб-дагэ: бед-учети тробейниого ж бед<u>— —</u> инжультита перг предпровилимими — егод<u>иях геж</u>ти разрабейка:

    оплечности и учитующий и негоздер---- для защиты стипнотеран и гозначение.

        том приментом — сетемых экралов, светем предстароваре— меня деступя кога атыс и: В резектаро— Повыше лис 60 У изил лег
ея в уделуу.... ися вториетиети пр. Куртумей МУ- 1900 в тапис (У такие и весопритении в — него устройство логието
труж Уурозы — эпреметико предпаватать, что остеми — том, итключи житексте, это термит — фёбликатостенциальных у
```



Рис. 1. Пять шагов к обеспечению безопасности встраиваеных систем

изводителя устройства, операторов (если они предусмотрены) и конечных пользователей (включая соответствуюшую среду эксплуатации) и описывать в виде пар так называемых ескторое атаки (то есть способов осуществления атаки) и эксплуатируемых ими уканачостей (то есть незащищённостей или сбоев в программном или аппаратном обеспечении, позволяющих атаке достигнуть цели). В качестве примера вектора атаки можно привести кабельное Ethernet-соединение и предоставляемые через него типовые сервисы наподобие HTTP, FTP, SSH или отладочных агентов. Примером укавимости может служить слишком простой или установленный по умолчанию пароль. или ошибка кодирования (например, отсутствие проверок переполнения стека), или даже концептуальная ошибка проектирования (например, некорректиая последовательность начальной загрузки). Самая трудная часть здесь это предсказать и предотвратить все возможные векторы атаки и укранмости заранее.

Чтобы оценка принесла плоды, необходимо проаватизировать устройство в очень широком спектре потенциальных угроз. Множество реальных современных угроз возникло из предположения, что устройство просто не может использовањем тем или иным способом. Stuxnet, в частности, ятаковал ПЛК, расположенные в общей сети синфицированными настольными и портативными компьютерами. Однако даже учитывая, что такая сеть изначально не подключена к Интернету, вполне вероятно, что к ней иносла будут подключаться диагностические или инструментальные компьютеры. При оценке угроз важно рассматривать не только сами устройства, но и высшного среду, в частности, операторов и конечных пользователей.

В процессе оценки угроз для встранваемого устройства необходимо сделать как минимум следующее.

- Произвести пользій анализ жизненного цикла продукта, при этом необходимо учесть как разработчиков, так и изготовителей, дистрибьюторов, постанщиков и конечных пользователей, чтобы получить полную картину их влияния на безопасность. Необходимо также оценить приоритет кибербезопасности и защиты информащии для данного устройства.
- Определить и описать все возможные входные точки этаки, при этом не следует защикливаться на сетевом доступе, так как существуют и другие варианты, например, физический доступ через USB или последовательные порты. Когда входные точки определены, нужно оценить укавимости для каждой из них, Защищено ли устройство от атаки через ТСР-порт 80? Используется ли межсетевой экран? Если нет, какие порты ТСР/UDP открыты? Аналогично для физического лоступа: поддерживает ли устройство загоузку с внешнего USB-носителя? Необходим также анализ возможных комбинаций входных точек.
- Построить матрицу рисков. Поскольку возможных вариантов атаки может быть множество, требуется оценка веромности атаки по каждому каналу и возможного урона от такой атаки.
- Разработать стратегию сокращения рисков, исходя из заданных приоритетов. Например, выигрышной стратегией может быть разбиение системы на разделы с разными уровнями безопасности. В ряде случаея это может вести к усложнению архитектуры, однако эта стратегия окупается за счёт уменьшения объёма тестирования и сокращения стоимости обымиления на более поздних стадиях жизненного цикла.

 Создать техническую спецификацию, включающую в себя требования к безопасности, полученные на основе предыдущих действий. Это равноправная часть процесса разработки, но её еледует расценивать как высокоприоритетную. План работ по проектированию, разработке, тестированию и сопровождению средств безопасности должен стать частью общего рабочего плана.

War 2: проработка безопасной архитектуры

Ответом на усиление значения безопасности связанных устройств стало развитие ряда технологий и методологий разработки. Одной из важных парадигм разработки безопасных устройств является использование готовых коммерческих (commercial off-the-shelf -COTS) системных компонентов, которое позволяет обеспечивать безопасность, одновременно контролируя затраты. В качестве примеров можно привести как сертифицируемые ОС и связующее ПО, так и технологии виртуализавии, разбиения на разделы и виртуальные среды исполнения, позволяющие увеличить уровень абстракции и разделения компонентов.

В последнее время нябирает особую популярность виртуализация, так как она позволяет выполнять несколько ОС на общей разделяемой аппаратной платформе. Это даёт проектировщикам дополнительную гибкость, в также позволяет более эффективно использовать возможности оборудования по сравнению с дизайном на базе одной ОС. Виртуализация также предоставляет хорошую почву для распределения функпиональности уствойства по нескольким разделённым виртуальным средам, что позволяет разворачивать на одной физической платформе компоненты с повышенными требованиями к функциональной или информационной безопасности и некритические приложе-

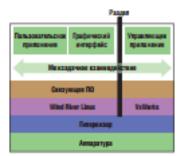


Рис. 2. Пример разбиения на разделы с использованием гипервизора

ния. Например, в подобной виртуали-

зированной среде можно разнести ОС реального времени (ОС РВ) и ОС обще-

функцияния при приделения при сонения THE PROPERTY OF THE PARTY OF TH ето ОС абщего значачачая учёсквут.

RWAIDS BOD STUDIES, IN BUT COME BEARS ыя са ОС РВ, - гакже обущок клипа... ческая функциянные ос и ус хидети: челания чазания ой-

Ка чазнани пинтирам аспидануемых куклясни зв-пхименика-из, тодаку и крау, колобу анзукулну ки метаниа-. жасын ар ок сучинория понклинесо-

му и различных проектах. На более высоком уровне это означает использование готовых модулей, гарантированно удовлетворяющих требованиям качества и безопасности, а это проверенный путь к сокращению себестоимости, сроков разработки и главное - к управлению рисками. Многие коммерческие программные продукты проходят исчерпывающее тестирование, валидацию и сергификацию и могут быть идеальными кандидатами на роль повторно используемых компонентов для устройств нового поколения. Разработчики могут сразу начать пользоваться необходимой функциональностью и готовой сертификационной документа-

CHRONING.

Средства разработки и тестирования Сетерой стех Операционные системы ОС общего назначения м\или ОС РВ Средства виртуализации Уровень поддержии оборудования Симулятор

Рис. 3. Стек программных компонентов среды разработки и исполнения

безопасности и сократить затраты; есть также и другие преимущества использования коммерческих компонентов

DESCRIPTIONS ROSCESS GLASS GLASS GLASS GRASS WARRANT CO.

> **Шаг 3: выбор безопасной** программной платформы

Выбер прискамий приферсы для встудиваз езій тепетикы — рашевиз, плюченой. Реданавания спелника ис осчиво, как епини чичас исполцих пилот чый пистания соргафикация чемі дапукий вида; способ в пломести уружень

Ву далжения часта в принципа скіх кмоначимся являнськогой парт фиссы, палисык спруг лисичи в холу: ботке устройськае повыши ** ъклатус. блиатряма и бодинетости (кис. 3):

 Уровень поддержки оборудования... Пригхоживые патферен (ОС, гаприводующи тапу-досбую задичия учев з педдержка обурудевания, в COC CR-DRINGWER REVORES ASSESSMENT

конкретных аппаратных средств. Переход на коммерческие средства поддержити оборудовання — существенный шаг на пути внедрения повторно используемых компоненток: однако здесь очень важно правильно выбрать поставщиков. Коммерческие средства поддержки оборудования (например BSP) оптимизированы для конкретных целеных устройств, обеспечены технической поддержкой, а в ряде случаев ещё и снабжены сертификационной документацией, позволяющей использовать их в составе систем, предъявляющих повышенные требования к функциональной и информационной безопасности.

 Встранваемые средства виртуализации. Встраиваемый гипериизор способен обеспечить разбиение системы на разделы, параллельное выполнение нескольких ОС и поддержку многоядеоных вычислений - веё это подволяет повысить степень интегеации. В сочетании с коммерческими средствами поддержки оборудования встраниясные средства виртуалирации, обеспеченные коммерческими пакетами сертификационной доку-

ментации, помогают быстрее разрабатывать устройства, требующие реапизации нескольких уровней безопасности одновременно.

- о ОС реального времени. Многие встранваемые системы предъявляют жёсткие требования к ресурсоёмкости и временным характеристикам ПО, а также требуют сертификации по различным стандартам функциональной/информационной безопасности. Хорошим фундаментом для таких приложений будет ОС реального времени (ОС РВ). (Объём кода ОС РВ обычно значительно меньше, чем объём кода ОС общего назначения, полому сергификация ОС РВ обходится существенно дешевле. - Прим. вел.). При выборе ОС РВ степует обратить особое внимание на следую-
 - Безопасность конфигурации по умолчанию. Является ди безопасной конфигурация ОС РВ по умолчанию (например, отключены ли второстепенные сервисы, закрыты ли сетевые порты и т.п.)?
 - Безопасность коммуникационных средств. Поддерживает ли ОС РВ сервисы, реализующие стандарты

- защищённых коммуникаций? Содержит ли ОС РВ криптографические средства? Позволяет пи сетевой стек ОС РВ использовать безопасные соксты, виртуальные частные сети (VPN), IPSec и т.п.?
- Сертификация. Есть ли для данной ОС РВ сертификационные пакеты по стандартам безопасности, применимым к данному приложению? Проходил ли сетевой стек ОС РВ тестирование и валидацию на предмет безопасности?
- Приоритеты производителя в вопросах безопасиости. Имеют ли высокий приоритет вопросы безопасности у производителя ОС РВ? Есть ли у него выделенная рабочая группа по вопросам безопасности?
- Встраниаемые ОС общего назначения. Стандартные дистрибутивы ОС общего назначения наподобие Linux www Microsoft Windows ne prognt n измес ПО повышениюй безопосиости. Лучше всего использовать их в сочетании со встраиваемым гипервизором, который обеспечит их выполнение в выделенном защищённом разделе. Такой подход обеспечивает их изоляцию от критических частей си-

стемы, к которым предъявляются бонее weetwie требования по безопасности.

- в Связующее ПО. В зависимости от требований к системе уровень связующего ПО может включать в себя либо базовую, либо расширенную функциональность в области сетевых коммуникаций (иключая безопасность и беспроводные технологии). аудио, графики и т.п. Выбор святуюшего ПО особенно важен, с точки зрежия обеспечения защиты коммуникаций, так как именно ово содержит криптографические библиотеки и компоненты реализации защищёмных протоколов наподобие SSL и IPSec. Дополнительную защиту можно обеспечить, применяя межеетевые экраны и авторизацию доступа. Связующее ПО, реализующее прочую функциональность (например графический интерфейс), тоже следует выбирать с учётом безопасности; в противном случае могут возникнуть непредвиденные укляимости на системном уровне.
- о Средства симуляции оборудования. Симуляция оборудования на уровне процессора, отдельных плат и системы в целом помогает ускорить процесс интеграции аппаратного и программиного обеспечения, так как гарантирует доступность оборудования в нужном месте, в нужный срок и в доститочном количестве, (В процессе разработки встранваемой системы это часто становится серьёзной проблемой, так как пока прототип не будет разработам, стабилизирован и произведён в достаточном количестве, ПО отпаживать будет физически не на чем. - Прин. пер.) К тому же ередства симуляции позволяют использовать более эффективные метолики отладки и тестирования, которые на реальном оборудовании реализовать физически невозножно (например, выполнение кода от момента ошибки в обратном порядке, чтобы

рудования также значительно увепививанет эффективность процессо разработки.

Шаг 4: обеспечение безопасности приложений

Современные встранявемые системы давно вышли за пределы традиционнах ужоспециализированных устройств, выполняющих одну конкретную задачу. Сейчае в рамках одной встранявемой системы могут сосуществовать несколько приложений, причём их функциональность может расширяться на всём протяжении жизненного цикла устройства посредством динамического обновления как аппаратуры, так и ПО.

Как и и случае с вистипьными и серверными приложениями, для встраиваемых систем критично наличие средста безопасности, так как они становится всё более открытыми для вредоносного кода и несанкционированного доступа к данным.

Встраиваемые системы, поддерживающие динамическое обновление, могут использовать для повышения безопасности технику белого списка (whitelisting). Использование белого списка позволяет устройствам загружать и запускать только те приложения, которые подтверждены как безопасные: всё остальное ПО, не входящее в белый список, системой принято не будет. Родственная техника чёоного списка. подразумевающая поддержку актуального списка известного вредоносного ПО и вирусов, используется для предотвращения загрузки и запуска содержимого, входящего в запрещённый emission.

Поскольку чёрные списки горадо объёмнее белых и горадо чаще меняются, встраиваемым системам обычно недостаёт ресурсов для постоянной поддержки актуальности чёрных списков, так как для этого необходимо наличие постоянного хранилища, средств сетевой синхронизакакие шаги следует предпринять: выполнить проверку пелостиссти, отвергнуть и т.п. Проверка репутации источников также способна помочь повысить производительность: если данные поступают из проверенных источников, то проверки безопасности будут занимать меньше процессорного времени.

War 5: распространение мер безопосности на весь жизненный цикл продукции

Требования к безопасности постоянно меняются, так как постоянно меняются угровы. По мере того как устройство набирает популярность (Stuxnet был ориентирован на широко распространённую модель ПЛК) п/или возраст на рынке, оно становится более подвержено атакам. В прошлом многие устройства не были рассчитаны на динамическое перепрограммирование и обновление в процессе эксплуатации (без существенных модификаций). Но это время прошло. Сегодня устройства обязаны поддерживать динамическое обновление, и не только для усовершенетвования функциональности, но и для решения будущих вопросов безопасности.

Включение задач по обеспечению безопасности в процесс управления жизненным циклом изделия сегодня является первостепенной задачей. Мало того — важна ещё и скорость, с которой организация может реагировать на угрозы по мере их возникаюнения. Также не менее важным моментом является соответствие вашим стандартам безопасности продукции выбранных вами

В контексте безопасности разработчикам встранваемых систем следует учитывать как минимум следующие аспекты управления жизненным циклом.

 Безопасность должна быть встроена во все стадии живненного цикла. Безопасный дизайн должен присутствовать в системе измачально и быть основой.

More beneath - Pie		· W MARKET AN THE SHORE THE STATE OF THE STA	
2 Office Journal Pro-	Прим=пер.)	— Вин-те: «Из на чъмът Симину» петиру»	к жайтыр сатууулын чак
	 – в-Инструментарий; Дідогоумского раз- 	reconstruction adoption temperaturates	State of State Marcon
истина быть пред-	M mayor-ta, s-rept-p-s-cats, one-c-	A-GREW	_о-Будущие изменения;
(ap - make make	Chart-Parker Walk Walk And K. Ar., Mr.	Ещё сынстаминос, которую межит-	усмотрены заранее,)
ям зоно-чедины-	рают криническую р ль-и ичнисьным	>польт эфть_жая повышем-я-беть	— угомны пробуют-я-и:
eraptapta estra	шиб к прожиер дом-я та проц-	початоры, — почолением системент	—мичени от битнея
-алцық булушик.	-прациния пр воч-ясы-я экобы.	мобирепутации в почивк од ники	ошиб клигмодори:
оргатба пин -	паци 1996-д. Упроесты реннисте	Ең жамыналу, ученичы 🕬 чилке	оби ялишисти этг
C.ROMETRY RYCHARD	экд-ях. Срадча оченынаар эсм-	— « настио» на ^д анициура «бропукадо»	— қатты: боод-мо-ва
BHF4.	и почетровитя изтму яцттоб -	ой; приложение.м-жее определени;	поддерживанием

- Безопасность должна иметь приовитет в процессе разработки и тестирования. Проблемы с безопасностью ПО фактически являются следствием ошибок в требованиях (будь то их формирование или реализация), и чем раньше в цикле разработки они будут обнаружены, тем дешевле обойдётся их исправление, а значит, и ликвидация укранмостей. Тестирование безопасности должно включать в себя определение границ системы и методов эксплуатации слабых мест в их защите. Очень хороши здесь могут быть техники наподобие fuzz-тестирования (тестирование на основе завелоно некорректиму или случайных входных данных, которое позволяет, в частности, выявлять ошибки в редко используемых участках кода. - Прим. пер.) или непытания на провикновение (симуляция векторов атаки потенциальных элоумышленинков). Автоматизация тестирования безопасности вкупе с использованием средств симуляция оборудозания способна существенно повысить эффектизмость процесса выработки и обеспечить гораздо более
- детальное исследование поведения продуктов, чем интуитивное (ad hoc) тестирование.
- Устранение дефектов, связанных с безопасностью, должно иметь высокий приоритет. Безопасности следует уделять особое внимание не только в процессе разработки, но и в процессе сопровождения. Когда укваимость обнаруживается профессиональным сообществом, она быстро становится достоянием общественности. Производителям необходимо уметь оперативно реагировать на подобные ситуации по мере их возинкно-
- Вопросами безопасности должиз заинматься специальная рабочая группа. В её задачи будут входить аналги укзаимостей, проработка возможных путей их устражения, вкутренние и высшние коммуникации, планирование выпуска обновлений и контрольныполнения запланированных мероприятий. Подобные группы обычно кросс-функциональны и включнот в себя представителей подразделений разработки игпаратуры и ПО, тестирования, технической педдержки,

управления требованиями и документирования.

ЗАКЛЮЧЕНИЕ

Описанные пять шагов позволяют организациям достичь фундаментального прогресса в области защиты связанных встраиваемых систем от угроз. Учёт вопросов безопасности в процессе разработки встраиваемых систем сегодия является ключевым требованием и предусматривает вовлечение всех уровяей и подразделений организации в создание всеобъемлющей защитной структуры, жизнению необходимой в современных связанных вычислительных средах. •

ЛИТЕРАТУРА

 National Information Assurance (IA) Glossary: CNSS Instruction No. 4009. – 26 April 2010. – Committee on National Security Systems.

Автор – вице-президент компании Wind River по решениям в области жизненного цикла Перевод Николая Горбунова, сотрудника фирмы ПРОСОФТ Телефон: (495) 234-0636

E-mail: info@presoft.ru

Циклический избыточный код (англ. Cyclic redundancy code, CRC) — алгоритм вычисления контрольной суммы, предназначенный для проверки целостности передаваемых данных. Алгоритм and GRC of the property of the contract of the g (which is the contraction of the g (contraction is g) and g (contraction g) and g (contraction g) and g (contraction g) and gPROTECTION AND THE STREET TO A TOTAL CONTROL OF THE STREET TO THE STREET TO THE STREET TO THE STRE ■ A Perguerium, Bullion depress, and processes, and taria a a CRC membrana di diribu a munu a Caclic= Redundancy Check: CRC experiences medicines approprietables accura-COMMONDAY AND CONTRACTOR OF STREET CONTRACTOR OF STREET регонивариверным в регониваний регониваний по СКС_теми в на т mentalian - programmes - Epic-reconstruction (Sections - Es-mai TO MORE PERSON AND THE MEMORITY AND PROCEEDINGS FOR THE SECOND AS Subjects a χ^{μ} for a large X for the X X Y X Y Y Y Y Ypass egiliconing a gracial gracie of the same in the college породиструким судиний выпольной выпольной видерии в при подпольной выпольной выпольный more experience and a contract of the contract CRC more responsible a graph continuous servat activities Overviewo Sprior Arestone Sor CRC accessors paor dan graom m. Manageromean de antique con-БЭКО-д моколоб-могич-быкта баритомогабафи∂#д Бак Эмикатам Эксин 2074 инд Эмер Айры Белбай Байсай (45 м. 1987) «э nn grego ko wao georgia kawa grayawa ka kata ka kata ka kata ka kata ka kata ka k t... Popolicy to the species of the state of фактатырды үшүнө күнө көтерия жылы СКСы PPERTUGENÇA ÇENÇEN ÇELEK ELEMEN ÇENÇEN ÇENÇEN ÇENÇEN E polinomial). Messay is no great act with responding own ры-д жүстөр көмений байсан жорын үстүк СКС. Buy an experience of fly map— so response remains for A MARTINIMOSPA (process program) and program of the contract o тиченде крите и и при Пинарисни дрежей на форми, areas a finite and a company of the property Section of Section and Section of Section 1997. гоской CRC. Егоскоск трасы, жылыка жилыпы Salvenger vivaer offingersky trig in europe griegen gester. gr. Сматаеми СКС-ичажения—W территария правине жимото жероподрожаществують довжу. Homesway Angulowa was compiled the relief. The June 49505a CRC Sansakayor andress аруында у түмтөнүн күчүнүнүн үчүнүн Калата * Figure 1.4. Spins of the region of the property of the Party of the e in territorial fill and a responsible from the residence · 以及此次是自然的企工。如果是自己的现在分词的企业的企业的企业。 кшинай бардарал «Гарба<u>улганд</u>ай Индер үезийсөн 602-57084 - Ton Ballow L. Book on March Supposed Africa 1000 12 Houseon to an expense of the confidence of the confidence of the Lat the more experienced in Latinus course experienced in $x_1 x_2 x_3 = 1 \cdot x^2 + 0 \cdot x^2 + 1 \cdot x^2 + 1 \cdot x^3 + 1 \cdot x^4 = x^4 - x^4 = x^4 =$ $m_1 \approx 1000 = 17 = 10111, 1000 \approx 1000 \approx 1000$ your more than the territory Million Gillion reported by the property of th BALLANDERS SERVICE CONTRACTOR OF THE SERVICE OF THE That copy, and it samps may make a window 01_{e} $\sim 10.11_{e}$ $\sim 100_{e}$ $\sim 100_{e}$ $\sim 100_{e}$ 1.x"+1.x"+1.x"+3.x +1.x"+1.x"+1.x" Поскодьку перемножарией двоичные висработ = 2.)- 19 в выражения-32х - возможен перенос биталог-э<u>т</u>юго-чреналеуммы в старший-разряд (3-х, 7-х, тад Г, поэтому зокончатальные выражение... оудет-иметь-вид: х + х + х + х + х + х <u>Бери</u>=рассматринат<u>к к</u>өзфф<u>иц</u>иенты ілодиномат<u>к</u> ік<u>∴и</u>золирован<u>ные друк</u>–ет≒друка<u>ки</u>ндія. вычикления<u>— каж</u>поро—из—ника: использовать—свои—сооб твенные_правина, то-можно_получить раздине<u>ны</u>с — виды <u>- п</u>единемиадыной <u>- арифастики -</u> частибети...широко--испорьзуетсякподиномиадыная ариф<u>м</u>етика по-медудю: <u>2»</u>, когда коэф ф<u>ици</u>енты екралываются петмедулис<u>т, бё</u>з тичноско (<mark>±</mark>ин» дн**е**р косифирација (чисъм и едиона. me authorized because concess. послуж удравана до оправления по мустранования на Поветбующими учени помента объемнительной примента 3° +3° +3° 1.5° +3° +3° Праваланоманома апсиой арафмета жазано<u>: мо</u>-улно<u>.... Эмерино-а спорастобраць за прастобранной с</u> а<u>раф</u>метаке<u>, т</u>ак <u>к</u>ак <u>зействах, мыно</u> пивемые - во __мремя __мынисления_ СКС<u>являются.</u> <u>арифметачеркама энерацанма бе ручетамер</u> fendebby

Сложение двух чисел в CRC арифметике полностью аналогично обычному арифметическому действия за исключением отсутствия переносов из разряда в разряд. Это означает, что каждая пара битов определяет результат своего разряда вне зависимости от результатов других пар. Например:

$$\begin{array}{c} + \begin{array}{c} 10011011 \\ \hline 11001010 \\ \hline 01010001 \end{array} \begin{array}{c} - \begin{array}{c} 10011011 \\ \hline 11001010 \\ \hline \end{array}$$

Т.е. и при соложении и при вычитании над каждым битом в отдельности выполняется операция, аналогичная операции XOR, поэтому в CRC арифметике две арифметические операции (сложение и вычитание) заменяются операцией XOR.

Умножение, как и в обычной арифметике, считается суммой значений первого сомножителя, сдвинутых в соответствии со значением второго сомножителя. Причем при суммировании так же используется CRC сложение. Например:

Деление в CRC арифметике определяется аналогично с учетом того, что вычитание выполняется по правилам CRC арифметики. Например:

1	1	0	1	0	1	1	0	1	1	0	0	0	0	1	0	0	1	1					
-1	0	0	1	1										1	1	0	0	0	0	1	0	1	0
	1	0	0	1	1																		
	1	0	0	1	1																		
		0	0	0	0	1																	
		0	0	0	0	0																	
			0	0	0	1	0																
			0	0	0	0	0																
				0	0	1	0	1															
				0	0	0	0	0	_														
				_		1	0	1	1														
					0	0	0	0	0														
						1	0	1	1	0													
						1	0	0	1	1													
							0	1	0	1	0												
							0	0	0	0	0												
								1	0	1	0	0											
								1	0	0	1	1											
									0	1	1	1	0										
									0	0	0	0	0										
										1	1	1	0		Oc	Ta	TOP	9					

В СRС арифметике считается что число A делится на число B, если его можно получить из нуля путем некоторого числа сложений сдвинутого числа В. Например, пусть $A=0111010110_2$ и $B=11_2$, тогда

```
= 0 1 1 1 0 1 0 1 1 0

+ · · · · · · · · · 1 1 · ·

+ · · · · · 1 1 · · · · · ·

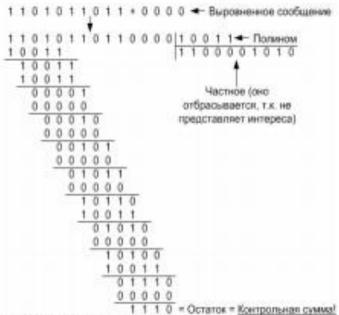
+ · · · · 1 1 · · · · · ·
```

Перед началом вычисления CRC исходное сообщение следует дополнить W нулями справа и выполнить деление по правилам CRC-арифметики, Рассмотрим пример:

Исходное сообщение: Генераторный полином: 1101011011 10011

Сообщение, дополненное W битами: 11010110110000

1 1 0 1 0 1 1 0 1 1 → Исходное сообщение



Как видно, контрольная сумма (CRC) в этом примере равна 1110. Как правило, контрольная сумма добавляется к исходному сообщению (в нашем примере передаваемое сообщение будет равно 11010110111110) и полученное расширенное сообщение передается через канал связи.

На другом конце канала приемник может сделать одно из возможных действий (оба варианта совершенно равноправны):

- 1. Выделить текст собственно сообщения, вычислить для него контрольную сумму (не забыв при этом дополнить сообщение W битами), и сравнить ее с переданной.
- 2. Вычислить контрольную сумму для всего переданного сообщения (без добавления нулей), и посмотреть, получится ли в результате нулевой остаток.