УДК 004.75

В.А. Десницкий, И.В. Котенко

КОНФИГУРИРОВАНИЕ ВСТРОЕННЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В РАМКАХ СЕРВИСОВ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Десницкий В.А, Котенко И.В. **Конфигурирование встроенных систем защиты информации в рамках сервисов обеспечения комплексной безопасности железнодорожного транспорта.**

Аннотация. В работе представлена концепция разработки комбинированной защиты встроенных устройств, применимая в процессе разработки механизмов защиты информации систем и сервисов обеспечения комплексной безопасности железнодорожного транспорта. Предлагаются модель процесса конфигурирования компонентов защиты встроенных устройств, а также методика конфигурирования, разработанные с учетом экспертных знаний в предметной области информационной безопасности встроенных устройств. Цель конфигурирования – найти такую конфигурацию защиты, которая реализует все необходимые требования защиты и ограничения со стороны платформы устройства, удовлетворяет заданным критериям ресурсопотребления и не содержит известных видов несовместимостей компонентов защиты.

Ключевые слова: встроенные устройства, информационная безопасность, конфигурирование.

Desnitsky V.A., Kotenko I.V. **Configuring embedded information protection systems within services providing complex security on rail transport.**

Abstract. The paper encompasses a design conception for combined embedded device security to be applied within the development process of protection mechanisms for systems and services of complex security on rail transport. A model and technique proposed are intended for configuring embedded device security components developed taking into consideration expert knowledge in the embedded security field. The goal of the configuration process is to find a security configuration that meets all necessary security requirements and constraints of the device platform, satisfies set resource consumption criteria and does not contain known types of security component inconsistencies.

Keywords: embedded devices, information security, configuring process.

1. Введение. Информационно-телекоммуникационные системы поддержки процессов на железнодорожном транспорте (ЖТ) представляют многоуровневые сетевые и распределенные архитектуры, включающие различные стационарные и мобильные встроенные устройства, взаимодействующие между собой в режиме реального времени. При этом в рамках бизнес-процессов ЖТ встроенные устройства предоставляют специализированные функции коммуникации, ввода информации, контроля, информирования, обработки и хранения данных и событий безопасности автоматизированных информационно-телекоммуникационных систем ЖТ. Такие системы характеризуются

динамически изменяемой топологией сети и отличающимися видами коммуникаций между ее отдельными узлами, а также заранее не фиксированным набором задействованных устройств и функционирующих агентов.

Основными особенностями встроенных устройств являются узкая направленность целевых функций устройств, меньшая по сравнению с другими типами вычислительных систем производительность и наличие ограничений на объемы аппаратных ресурсов. Поэтому задача защиты таких систем требует специализированных способов проектирования механизмов защиты, которые, во-первых, базировались бы на экспертных знаниях в области разработки и анализа конкретного вида устройств и, во-вторых, помимо реализации защиты от заданного вида угроз учитывали бы также нефункциональные (ресурсные) требования к механизму защиты.

Основная трудность при разработке защищенных встроенных устройств обуславливается слабой структуризацией и формализацией области знаний информационной безопасности. Спецификой данной области является появление новых экспертных знаний, их устаревание и потеря актуальности, необходимость сбора информации из различных источников с разными уровнем доверия и практической применимостью – из индустрии встроенных устройств, аналитических отчетов, научных работ в областях информационной безопасности и программной инженерии, на основе опыта работы с существующими информационно-телекоммуникационными системами, путем анализа защищенности отдельных устройств и аудита безопасности системы в целом.

Разработка встроенных систем защиты в рамках сервисов многоуровневой интеллектуальной системы комплексной безопасности железнодорожного транспорта включает:

(1) анализ существующих моделей нарушителя с учетом целей и возможностей предполагаемых нарушителей систем ЖТ, определение функциональных свойств защиты и свойств программно-аппаратной совместимости;

(2) определение ограничений ресурсопотребления платформы устройства;

(3) формирование репозитория компонентов защиты встроенных устройств, определение их свойств;

(4) проведение анализа несовместимостей компонентов защиты на основе экспертных знаний в области безопасности встроенных устройств процессов управления железнодорожного транспорта;

(5) проведение оценки ресурсопотребления компонентов защиты на основе автоматизированного модуля тестирования с использованием эмулятора встроенного устройства;

(6) многокритериальный выбор компонентов защиты на основе учета показателей ресурсопотребления с использованием эвристик по выбору порядка учета критериев ресурсопотребления.

В [9] обосновывается необходимость и важность исследования вопросов разработки защищенных встроенных устройств на основе комбинирования программных и программно-аппаратных средств защиты, характеризующихся повышенным уровнем предоставляемой защиты и приемлемыми энергетическими и вычислительными расходами. В качестве пути достижения компромисса между защищенностью устройства и его ресурсопотреблением в [5] авторы предлагают использование «реконфигурируемых примитивов безопасности» на основе динамической адаптации архитектуры устройства в зависимости от состояния устройства и его окружения. Предлагаемая в [5] адаптация основывается, во-первых, на возможности динамического переключения между несколькими механизмами, встроенными в устройство, и, во-вторых, на возможности обновления элементов этих механизмов защиты.

В отличие от [5] в настоящей работе предлагается подход к конфигурированию компонентов защиты встроенных устройств на основе экспертных знаний предметной области с учетом показателей ресурсопотребления [1], при котором нахождение эффективных с точки зрения ресурсопотребления решений основывается на выборе компонентов защиты с учетом нефункциональных ресурсных требований к устройству, а также функциональных свойств защиты и ограничений программно-аппаратной совместимости.

2. Конфигурирование компонентов защиты встроенных устройств. В работе предложена структурно-функциональная модель процесса конфигурирования компонентов защиты встроенного устройства. Модель включает совокупность действий и программно-технических средств, которые должны применяться разработчиком в процессе конфигурирования. Под конфигурированием компонентов защиты встроенного устройства понимается процесс разработки системы защиты устройства путем комбинирования отдельных компонентов защиты (конфигураций) с учетом их свойств, ограничений, возможных связей и требований к ним со стороны устройства и других компонентов защиты.

Взаимодействие между встроенным устройством и компонентами защиты, которые в него интегрируются, включает предоставление устройству некоторого защитного функционала при условии получения от устройства требуемых объемов аппаратных ресурсов, соответствия свойств программно-аппаратной совместимости между компонентами и устройством и корректности связей между отдельными компонентами.

Требования к безопасности устройства, а также возможности компонентов защиты и конфигураций выражаются с использованием функциональных булевых свойств. Примерами функциональных свойств защиты являются «конфиденциальность данных, хранимых локально на устройстве», «аутентичность коммуникационного канала» для внешних коммуникаций, «наличие удаленной аттестации платформы устройства» [4]. Каждое такое свойство достигается путем применения одного или нескольких программных или программно-аппаратных модулей защиты.

Ресурсные требования задаются как линейные ограничения «сверху» на значения показателей ресурсопотребления, которые, в свою очередь, представляют собой величины расхода аппаратных ресурсов устройства. В частности, учитываются показатели для коммуникационного и вычислительного ресурсов, а также ресурса хранения.

Для задания различных характеристик программно-аппаратной совместимости используются булевы свойства – свойства программно-аппаратной совместимости компонента защиты и платформы устройства (как например, поддержка семейства операционных систем Android 4.x).

Задача, которую решает конфигурирование – путем анализа спецификации встроенного устройства, его особенностей и свойств найти такую конфигурацию защиты, которая, во-первых, реализует все необходимые функциональные свойства защиты, удовлетворяет всем ресурсным ограничениям и ограничениям программно-аппаратной совместимости, в-третьих, удовлетворяет заданным критериям ресурсопотребления и, в-четвертых, не содержит известных видов несовместимостей компонентов защиты.

В основу процесса конфигурирования закладываются экспертные знания предметной области, включающие, в частности, знания о типовых шаблонах защиты и сопоставлении конкретным требованиям защиты релевантных шаблонов, знания о возможных конфликтах и несовместимостях между компонентами защиты, знания о критично-

сти аппаратных ресурсов встроенных устройств на основе эвристического анализа существующих систем со встроенными устройствами.

На рис. 1 приведена многоуровневая диаграмма, раскрывающая структуру модели процесса конфигурирования. На диаграмме снизу вверх последовательно располагаются действия, которые должны быть выполнены в процессе конфигурирования встроенного устройства. На нижнем уровне приведены действия, отвечающие за получение исходных данных процесса конфигурирования, – спецификация встроенного устройства и компонентов защиты. На среднем уровне показаны действия, ответственные за формирование данных путем анализа, проводимого на нижнем уровне, – извлечение данных из спецификаций и определение функциональных свойств защиты, нефункциональных ресурсных свойств, критериев ресурсопотребления, свойств программно-аппаратной совместимости. На верхнем уровне показаны действия, которые реализуют основные функции, вовлеченные в процесс конфигурирования, включающие фильтрацию компонентов защиты, верификацию конфигураций, проверку несовместимостей компонентов и функции выбора наиболее эффективных конфигураций защиты. Действия выстроены снизу вверх согласно порядку их выполнения в процессе конфигурирования.

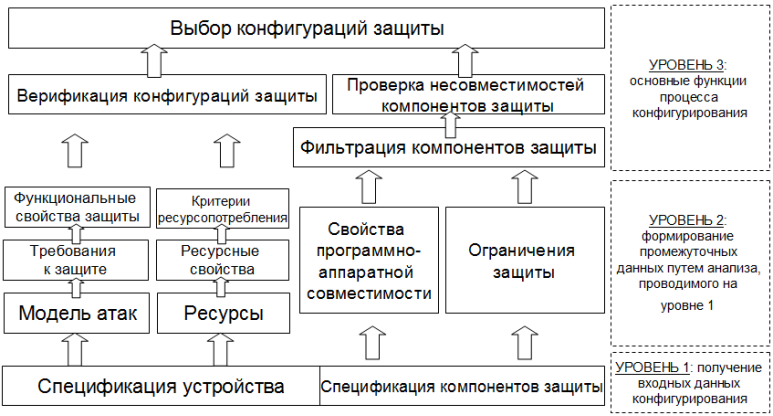

Рис. 1. Структура процесса конфигурирования.

На рис. 2 приведена диаграмма, описывающая верхнеуровневое представление модели процесса конфигурирования. Показаны данные (*прямоугольники*) и действия процесса (*прямоугольники со скругленными углами*), а также обобщенные связи между ними (*направленные*

стрелки). Определение возможных видов атак, которым подвержено встроенное устройство, осуществляется аналитически с использованием существующих классификаций нарушителя встроенного устройства по уровню взаимодействия нарушителя со встроенным устройством и по возможностям нарушителя.

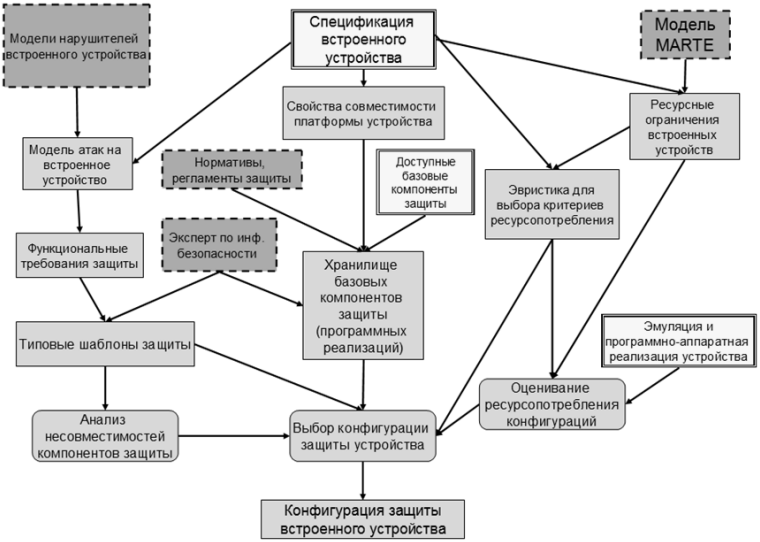

Рис. 2. Представление модели процесса конфигурирования.

В [8] выделяются четыре типа нарушителя в соответствии с типом доступа к встроенному устройству, который способен осуществить нарушитель:

- *тип 1* – нарушитель взаимодействует с устройством через сеть Интернет;
- *тип 2* – нарушитель находится в непосредственной близости от устройства, но не имеет физического доступа к нему;
- *тип 3* – нарушитель имеет физический доступ к устройству, но без возможности доступа к встроенным в него электронным компонентам;
- *тип 4* – нарушитель имеет полный доступ к устройству и к его электронным компонентам.

В [3] нарушители встроенного устройства разделяются на три уровня в соответствии с возможностями нарушителя:

- уровень 1 – у нарушителя нет полного знания о системе, есть доступ только к общедоступному оборудованию, приоритет использования существующих уязвимостей, новые почти не создаются;
- уровень 2 – у нарушителя есть информация о конкретной системе, есть доступ к средне-сложному оборудованию;
- уровень 3 – нарушитель представляет собой организацию, у которой есть доступ к лабораторному оборудованию любой сложности и которая может создавать группы нарушителей уровня 2.

В соответствии с приведенными классификациями, модель нарушителя включает множество категорий нарушителя, каждая из которых определяется парой *(тип доступа, уровень возможностей)*. Для каждой категории проводится анализ защищенности устройства от конкретного вида нарушителя. Такой анализ позволяет в зависимости от особенностей устройства, его целей, назначения, функций и программно-аппаратного обеспечения сузить множество видов нарушителей, которые, способных выполнять эффективные атаки.

Каждому функциональному свойству защиты ставится в соответствии некоторый типовой шаблон защиты, который его реализует. Типовой шаблон представляет собой защитный алгоритм в виде комплексного компонента защиты, который параметризуется набором криптографических примитивов виде базовых компонентов защиты. Разработчику доступно хранилище имеющихся в наличии типовых шаблонов и базовых компонентов защиты, которые он может использовать в процессе конфигурирования. Используемый подход к определению возможных угроз встроенного устройства, называемым статическим тестированием, представлен более детально в [2, 10].

3. Методика конфигурирования. Методика конфигурирования раскрывает более детально последовательность действий, которые необходимо выполнить в процессе конфигурировании компонентов защиты встроенного устройства (рис. 3).

Методика состоит из следующих трех стадий:

- *предварительной*;
- *стадии формирования требований и ограничений*;
- *стадии проведения многокритериального выбора*.

На предварительной стадии проводится анализ спецификации устройства и моделей нарушителей. Результатом стадии являются множества возможных атак на устройство и свойств программно-аппаратной совместимости.

Стадия формирования требований и ограничений включает определение функциональных требований защиты, задание типовых шаб-

лонов защиты для каждого требования. Применение действующих нормативов и стандартов позволяет среди имеющихся базовых компонентов защиты отобрать те, которые отвечают требованиям стойкости в соответствии с моделью атак и актуальными видами нарушителей встроенного устройства [7].

В соответствии с возможными регламентами, принятыми в организации, при отборе допустимых компонентов защиты могут учитываться также внутренние решения организации разработчика относительно предпочтительности тех или иных видов компонентов защиты (например, решения о предпочтении использования тех или иных аппаратных средств защиты).

Помимо учета требуемого уровня защиты проводится фильтрация базовых компонентов защиты на основе анализа свойств программно-аппаратной совместимости. Выходом стадии является построение множества допустимых конфигураций защиты устройства, из которых в дальнейшем производится выбор наиболее эффективных в соответствии с заданными критериями.

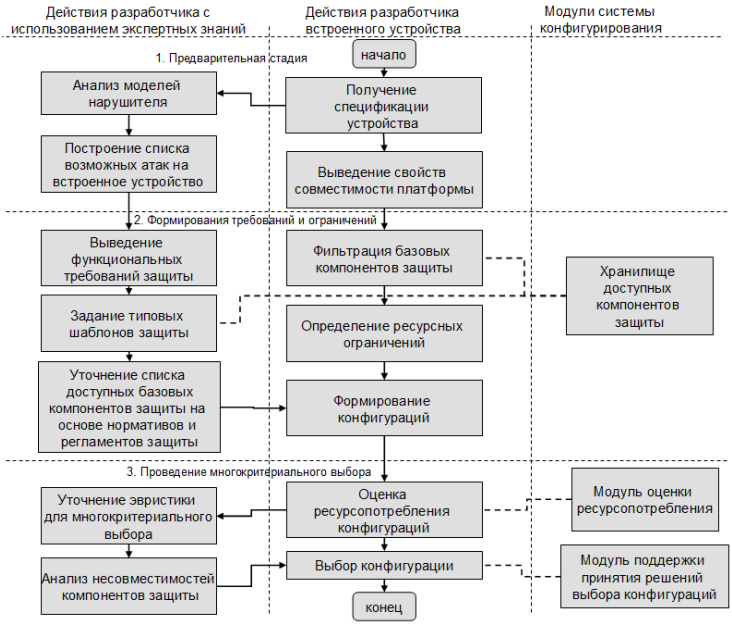

Рис. 3. Методика конфигурирования.

Стадия проведения многокритериального выбора включает определение показателей ресурсопотребления для конфигураций защиты с использованием модуля оценки ресурсопотребления [6], уточнение эвристики многокритериального выбора, анализ несовместимостей компонентов защиты и собственно осуществление выбора наиболее эффективной конфигурации защиты с использованием программного модуля поддержки принятия решений выбора конфигураций.

Использование эвристики разработчиком встроенного устройства включает: выявление релевантных признаков, определение на их основе порядка аппаратных ресурсов устройства и, собственно, осуществление процедуры выбора конфигураций на множестве допустимых конфигураций.

Модуль оценки ресурсопотребления реализуется на эмуляторе целевой платформы устройства и вызывается разработчиком итеративно для оценки ресурсопотребления с использованием заданного набора типовых шаблонов при автоматической подстановке комбинаций базовых компонентов защиты в рамках каждой итерации.

Эвристический анализ несовместимостей компонентов защиты направлен на выявление известных видов скрытых несовместимостей, в которые вовлечены компоненты защиты встроенных устройств. В общем случае несовместимость рассматривается, как связь между двумя или более компонентами защиты и представляет собой ситуацию конфликта между функционалами защиты нескольких компонентов или компонента и программно-аппаратная платформа устройства.

Особенностью таких несовместимостей является то, что они, как правило, проявляются лишь при определенных условиях и поэтому являются трудно обнаружимыми в процессе тестирования функций готовых устройств. Более раннее выявление несовместимостей на стадии комбинирования компонентов защиты способствует сокращению количества итераций процесса разработки устройства.

Знания об известных видах несовместимости формируются путем моделирования и экспертного анализа существующих и разрабатываемых комбинированных механизмов защиты встроенных устройств.

Рассматриваются следующие три типа несовместимостей:

- *тип 1* – несовместимости, возникающие вследствие недостаточной согласованности некоторого компонента защиты и спецификации устройства;
- *тип 2* – противоречия между функциями защиты нескольких компонентов защиты;

• *тип 3* – несовместимости данного типа проявляется вследствие того, что базовые компоненты защиты, входящие в состав некоторого комплексного компонента защиты помимо требований к устройству могут выдвигать, также, требования к другим базовым компонентам защиты этого комплексного компонента.

Способ разрешения обнаруженных несовместимостей – индивидуален, он определяется разработчиком в зависимости от специфики конкретной несовместимости и вовлеченных в нее компонентов защиты. В качестве вариантов разрешения могут рассматриваться пересмотр конфигураций защиты, изменение способа интеграции компонентов в рамках типового шаблона защиты, корректировка требований к защите или спецификации устройства.

Ниже приведены примеры каждого из приведенных типов несовместимостей.

• использование защищенного хранилища важных пользовательских данных с применением аппаратного модуля TPM [60], а также дублирование хранящихся данных при помощи дополнительного модуля хранения; исходя из предположения спецификации, что устройство имеет в своем составе лишь один модуль TPM, дублирование данных в незащищенном виде автоматически делает бесполезным использование TPM (*несовместимость типа 1*);

• компонент резервного копирования данных и компонент гарантированного уничтожения определенных данных устройства при наступлении определенного события, будучи примененными к одному и тому же массиву данных (*несовместимость типа 2*); устранение такой несовместимости потребует особого сценария интеграции данных компонентов;

• требования безопасности регламентируют организацию избыточного хранения данных с использованием нескольких защищенных модулей хранения при помощи RAID-принципа, однако параметры этих модулей (например, емкость или скорость записи) отличаются, что сделает невозможным выполнение данного требования защиты (*несовместимость типа 3*).

Выбор на множестве допустимых конфигураций осуществляется с использованием метода лексикографического упорядочения заданных критериев ресурсопотребления. Каждый критерий представляет собой набор аппаратных ресурсов и определенный порядок на нем. Упорядочивание осуществляется на основе эвристики, определяющей важность учета выбранных, критически важных аппаратных ресурсов устройства.

Эвристика построена на основе экспертных знаний, полученных в результате анализа трех рассматриваемых индустриальных систем со встроенными устройствами [2]. Выделяется серия признаков встроенных устройств и предоставляемых ими сервисов, имеющих влияние на вопросы ресурсопотребления для каждого ресурса. Вводится трехбалльное ранжирование ресурсов по их критичности для выполнения целевых функций устройства (0 - ресурс некритичен; 1 - низкая критичность; 2 – высокая).

Экспертным путем для устройств каждой из трех анализируемых систем каждому признаку ставится в соответствие определенный ранг. Ранги, полученные на основе экспертных оценок анализируемых систем, принимаются в качестве рангов самих признаков, которыми обладают данные системы, и поэтому они могут использоваться для экспресс-ранжирования ресурсов устройства его разработчиком без дополнительного участия экспертов.

При конфигурировании компонентов защиты встроенного устройства выявляются присущие устройству признаки из списка имеющихся. После чего каждому ресурсу ставится в соответствие максимальное значение ранга по всем выполняющимся признакам, которые соответствуют данному ресурсу.

В результате рассматриваемые аппаратные ресурсы упорядочиваются в соответствии с убыванием их рангов.

К учитываемым признаком относятся, например, для энергоресурсов – наличие постоянного источника питания, необходимость эпизодического доступа к источнику питания, высокая зависимость достижения целей устройства от энергоресурсов и другие.

Модуль поддержки принятия решений выбора конфигураций представляет собой программное средство, запускаемое и используемое разработчиком встроенного устройства.

На рис. 4 приведен фрагмент пользовательского интерфейса при конфигурировании устройства моделируемой системы управления ЖТ.

Данное средство предоставляет пользовательский интерфейс для задания информации об имеющихся компонентах защиты, их свойствах, требованиях со стороны устройства в терминах свойств и ограничений, критериях ресурсопотребления.

Результатами работы данного модуля является информация о конфигурации, признанной в качестве наиболее эффективной в соответствии с заданными критериями.

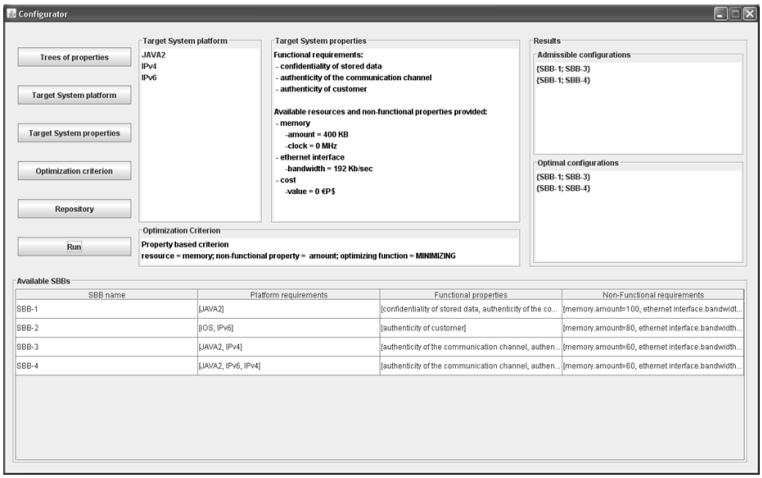

Рис. 4. Фрагмент программного интерфейса программного модуля принятия решений в процессе конфигурирования.

Отметим, что таких конфигураций может быть несколько, и в таком случае окончательный выбор может быть обусловлен экспертными предпочтениями.

4. Заключение. Одной из тенденций в области разработки встроенных устройств, в том числе для обеспечения комплексной безопасности железнодорожного транспорта, является делегирование функций экспертов по информационной безопасности разработчикам устройств за счет применения специализированных, в том числе автоматизированных методик и программных инструментов разработки, тестирования, оценки и анализа встроенных устройств. Вместе с тем, разработка комбинированных механизмов защиты встроенных устройств представляет слабо структурируемую и формализуемую область знаний.

Стремительное увеличение количества встроенных устройств и их повсеместное распространение ставят особенно остро вопросы разработки систем защиты для них от широкого круга угроз информационной безопасности. Ввиду специфики встроенных устройств, применение комбинированных механизмов защиты требует решения вопросов эффективного ресурсопотребления используемых программных и программно-аппаратных модулей защиты.

В работе предлагаются модель и методика разработки комбинированных механизмов защиты встроенных устройств на основе экс-

пертных знаний, полученных в области информационной безопасности встроенных устройств и обеспечения комплексной безопасности железнодорожного транспорта. Предложенный процесс конфигурирования характеризуется наличием анализа скрытых несовместимостей компонентов защиты и использованием автоматизированных программных моделей оценки ресурсопотребления и поддержки принятия решений выбора эффективных конфигураций защиты.

Литература

1. *Десницкий В.А., Котенко И.В., Чечулин А.А.* Конфигурирование компонентов комбинированной защиты встроенных устройств на основе решения оптимизационной задачи // Системы высокой доступности, №2, 2012, С. 50–56.
2. *Котенко И.В., Десницкий В.А., Чечулин А.А.* Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд, № 3, 2011, С. 68-75.
3. *Abraham D.G., Dolan G.M., Double G.P., Stevens J.V.* Transaction security system // IBM Systems Journal. Special issue on cryptology, No. 30, Issue 4, 1991, P. 206–229.
4. *Coker G., Guttman J., Loscocco P., Herzog A., Millen J., Hanlon B., Ramsdell J., Segall A., Sheehy J., Sniffen B.T.* Principles of remote attestation // Int. J. Inf. Secure, Volume 10. 2011, P. 63–81.
5. *Gogniat G., Wolf T., Burleson W.* Reconfigurable Security Primitive for Embedded Systems // Proceedings of System-on-Chip 2005 International Symposium, 2005, – P. 23–28.
6. *Köster F., Nguyen H., Obermeier S., Brändle M., Klaas M., Naedele M., Brenner W.* Information Security Assessments for Embedded Systems Development: An Evaluation of methods // Proceedings of 8th Annual Security Conference, 2009.
7. *Morris J., Kroening D., Koopman P.* Fault tolerance tradeoffs in moving from decentralized to centralized embedded systems // Proceedings of International Conference on Dependable Systems and Networks, IEEE Computer Society, 2004, P. 377–386.
8. *Rae A. J., Wildman L.P.* A Taxonomy of Attacks on Secure Devices // Department of Information Technology and Electrical Engineering, University of Queensland, technical report, 2003.
9. *Ravi S., Raghunathan A., Kocher P., Hattangady S.* Security in Embedded Systems: Design Challenges // ACM Transactions on Embedded Computing Systems, Vol. 3, No. 3, 2004, P. 461-491
10. *Ruiz J.F., Harjani R., Maña A., Desnitsky V., Kotenko I., Chechulin A.* A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components // Proceedings of the 20th Euromicro International Conference on Parallel, Distributed and Network-Based Computing (PDP2012), 2012, P. 261-268.

Десницкий Василий Алексеевич — к.т.н., научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН. Область научных интересов: методы защиты встроенных устройств, защиты программного обеспечения, политики безопасности. Число научных публикаций — 60. desnitsky@comsec.spb.ru, http://comsec.spb.ru/desnitsky; СПИИРАН, 14 линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Desnitsky Vasily Alekseevich — Ph.D., researcher, Laboratory of Computer Security Problems, SPIIRAS. Research interests: embedded system security, software protection methods, security policies. The number of publications — 60. desnitsky@comsec.spb.ru, http://comsec.spb.ru/desnitsky; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-2642, fax +7(812)328-4450.

Котенко Игорь Витальевич — д.т.н., проф., заведующий лабораторией проблем компьютерной безопасности СПИИРАН. Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер–терроризму. Число научных публикаций — более 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Kotenko Igor Vitalievich — Ph.D., Dc.Sci., Professor, Head of Laboratory of Computer Security Problems, SPIIRAS. Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism; The number of publications — more 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (проекты 13159-офи_м_РЖД, 13-01-00843-а и 11-07-00435-а) и программы фундаментальных исследований ОНИТ РАН.

Рекомендовано лабораторией проблем компьютерной безопасности СПИИРАН, заведующий лабораторией Котенко И.В., д.т.н., проф.
Статья поступила в редакцию 11.09.2013.

РЕФЕРАТ

Десницкий В.А., Котенко И.В. **Конфигурирование встроенных систем защиты информации в рамках сервисов обеспечения комплексной безопасности железнодорожного транспорта.**

Современные информационно-телекоммуникационные системы поддержки процессов на железнодорожном транспорте представляют собой сложные сетевые и распределенные архитектуры со встроенными устройствами, представляющими специализированные функции коммуникации, ввода информации, контроля, информирования, обработки и хранения данных и событий безопасности. Специфика встроенных устройств включает узкую направленность целевых функций и ограничения аппаратных ресурсов. Поэтому задача защиты таких систем требует специализированных способов проектирования механизмов защиты на основе экспертных знаний в области разработки и анализа конкретного вида устройств с учетом ресурсных требований к компонентам механизма защиты.

Разработка встроенных систем защиты в рамках сервисов многоуровневой интеллектуальной системы комплексной безопасности железнодорожного транспорта включает: анализ известных моделей нарушителя, определение функциональных свойств защиты, показателей ресурсопотребления и свойств программно-аппаратной совместимости, формирование репозитория имеющихся компонентов защиты и их свойств, проведение анализа несовместимостей компонентов защиты, проведение оценки ресурсопотребления компонентов защиты, осуществление многокритериального выбора на множестве допустимых конфигураций.

Предложены модель процесса конфигурирования компонентов защиты встроенных устройств, а также методика конфигурирования, разработанные с учетом экспертных знаний в предметной области информационной безопасности встроенных устройств. Используемые экспертные знания включают, в частности, знания о типовых шаблонах защиты и сопоставлении конкретным требованиям защиты релевантных шаблонов, знания о возможных конфликтах и несовместимостях между компонентами защиты, знания о критичности аппаратных ресурсов встроенных устройств на основе эвристического анализа существующих систем со встроенными устройствами.

В задачу конфигурирования входит путем анализа спецификации встроенного устройства, его особенностей и свойств найти такую конфигурацию защиты, которая, во-первых, реализует все необходимые функциональные свойства защиты, во-вторых, удовлетворяет всем ресурсным ограничениям и ограничениям программно-аппаратной совместимости, в-третьих, удовлетворяет заданным критериям ресурсопотребления и, в-четвертых, не содержит известных видов несовместимостей компонентов защиты.

SUMMARY

Desnitsky V.A., Kotenko I.V. **Configuring embedded information protection systems within services providing complex security on rail transport.**

Contemporary information and telecommunication systems supporting processes on rail transport represent complex network based and distributed architectures with embedded devices presenting specific functions for communication, entering data, checking, informing, processing and storing data and security events. Embedded device specificity includes narrow direction of business functions and hardware resource limitations. Therefore the problem of making secure such systems requires specific protection mechanisms on the base of expert knowledge in the field of design and analysis of particular device type, taking into account resource constraints to the protection mechanism components.

Development of embedded protection systems within services of multilevel intellectual system for complex rail transport security includes: analysis of known intruder models, determination of functional protection properties, resource consumption values as well as platform compatibility properties, forming a repository of available security components and their properties, analysis of security component incompatibilities, evaluation of security component resource consumption and multi criteria on the set of the admissible configurations.

A process model and technique for configuring embedded device security components proposed have been worked out taking into consideration expert knowledge in the field of embedded information security. In particular the expert knowledge used includes knowledge on typical protection templates and matching between concrete security requirements and relevant templates, knowledge on possible conflicts and incompatibilities between security components, knowledge on hardware resource criticality on the basis of heuristic analysis of existing systems with embedded devices.

The configuration task comprises analysis of embedded device specification, its peculiarities and properties to find such security configuration that, firstly, implements all necessary functional protection properties, secondly, satisfies all resource constraints and platform compatibility constraints, thirdly meet given resource consumption criteria and fourthly does not contains known kinds security component incompatibilities.