УДК 004.75

В.А. Десницкий

МЕТОДИКА ВЕРИФИКАЦИИ СЕТЕВЫХ ИНФОРМАЦИОННЫХ ПОТОКОВ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ СО ВСТРОЕННЫМИ УСТРОЙСТВАМИ

Десницкий В.А. **Методика верификации сетевых информационных потоков в информационно-телекоммуникационных системах со встроенными устройствами.**
Аннотация. В работе представлена методика верификации сетевых информационных потоков информационно-телекоммуникационных систем со встроенными устройствами. Цель методики – оценка защищенности разрабатываемой системы и проверка соответствия информационных потоков в реальной системе заданным политикам. Проводимая верификация базируется на методе «проверки на модели» с использованием программного средства SPIN. Верификация информационных потоков проводится на начальных этапах проектирования и обеспечивает более раннее обнаружение противоречий в используемой политике безопасности и несоответствий топологии сети требованиям информационно-телекоммуникационной системы.
Ключевые слова: информационная безопасность, информационные потоки, встроенные устройства.

Desnitsky V.A. **A technique for verification of network information flows in information and telecommunication systems with embedded devices.**
Abstract. The paper comprises a technique of information flow verification for information and telecommunication systems with embedded devices. The goal of the technique is to evaluate the security level of the constructed system and check the compliance between real information flows and the set policies. The conducted verification is based on model checking with the use of SPIN tool. Implementation of such verification is fulfilled at initial design stages and provides earlier detection of contradictions in the used security policy and inconsistencies between the network topology and requirements of the information system.
Keywords: information security, information flows, embedded devices.

1. Введение. Наличие ограничений на аппаратные ресурсы встроенных устройств обуславливает сложность существующих средств защиты, в том числе криптографических алгоритмов, которые традиционно используются для поддержки процессов защиты персональных компьютеров, серверов, сетевых структур. В результате разработка защищенных информационно-телекоммуникационных систем со встроенными устройствами требует специализированных подходов к проектированию механизмов их защиты [1–3, 12–13], которые могли бы обеспечить должный уровень защищенности системы не только путем применения дополнительных модулей защиты, но, также, за счет особенностей архитектуры системы [14]. Комплексный анализ системы, проводимый на различных этапах процесса разработки, как

один из путей достижения этой цели, способствует выявлению и последующему устранению архитектурных ошибок и недоработок, которые, в свою очередь, снижают уровень защищенности системы и отдельных ее элементов.

Целью методики верификации сетевых информационных потоков является оценка защищенности, проверка корректности политики безопасности этой системы и определение уровня соответствия информационных потоков в реальной системе требованиям и ограничениям политики безопасности.

Под информационным потоком понимается совокупность передаваемой информации между двумя и более взаимодействующими объектами системы. Политика безопасности информационных потоков – это набор требований, ограничений и правил, направленных на определение того, какие из информационных потоков системы являются разрешёнными, а какие запрещенными. При этом модель безопасности должна описывать все возможные информационные потоки, определять критерий безопасности системы и формулировать правила управления информационными потоками.

Проведенная работа является логическим продолжением работы, представленной в [5], в которой предложен комплексный подход к анализу информационных потоков для построения защищенных систем со встроенными устройствами. Данный подход включает в себя анализ информационных потоков на трех уровнях:

- аппаратном (проводится анализ связей между микросхемами [8]);
- программном (анализируется исходный код программ, выполняющихся на встраиваемом устройстве [12]);
- сетевом (анализируются сетевые соединения в системах, включающих встраиваемые устройства).

Анализ потоков на каждом из трех уровней раскрыт детально в современной научно-технической литературе [11, 12] но в случае анализа потоков во встроенных устройствах подобный анализ имеет свои особенности, которые недостаточно представлены в существующих публикациях. При этом работ, посвященных верификации сетевых информационных потоков, значительно меньше, чем исследований программно-аппаратных потоков. Понятие информационного потока широко используется при оценке безопасности маршрута и оценке эффективности сети [6, 15]. Хотя эти исследования не связаны напрямую с типами данных, передаваемых информационными потоками в

сети, но, тем не менее, они могут быть использованы при моделировании информационных потоков.

Информационные потоки между узлами сети, как правило, специфицируются в виде ориентированного ациклического графа. Таким образом, для выявления скрытых каналов к этому графу может быть применен топологический анализ, описанный в работе [13].

В настоящей работе применяется метод «проверки на модели» [7] для верификации правил политик безопасности, описывающих информационные потоки. Работы по анализу информационных потоков проводятся в рамках выполнения задач по проекту SecFutur [9]. Данный проект посвящен разработке процесса проектирования безопасных информационно-телекоммуникационных систем со встроенными устройствами. При этом верификация политик безопасности, в части контроля корректности сетевых информационных потоков, является составной частью процесса проектирования.

2. Подход к верификации. Верификация сетевых информационных потоков на начальных этапах проектирования относится к методам статического анализа системы. Выполнение такой верификации обеспечивает более раннее выявление противоречий в рамках политики безопасности, а также несоответствий топологии сети требований и ограничениям информационно-телекоммуникационной системы. Статический подход заключается в анализе структуры информационно-телекоммуникационной системы и ее характеристик (политик безопасности, бизнес-логики), то есть моделей системы на разных уровнях абстракции.

В отличие от динамического анализа, который включает тестирование готовых к использованию устройств на основе специализированных тестовых векторов атак, предлагаемый подход к верификации позволяет сократить количество и объем действий, которые необходимо повторно провести после исправления обнаруженных ошибок проектирования и уязвимостей.

К преимуществам статического подхода к верификации можно отнести возможность гарантировать безопасность системы при условии совпадения поведения модели и реальной системы. Недостатки данного подхода: большой объем вычислительных ресурсов, необходимый для анализа сложных моделей; ложные срабатывания, то есть предупреждения о потенциальных информационных потоках, которых в реальной системе не будет; и неполнота, так как проверяется не реальная система, а ее модель.

Проведение проверки корректности информационных потоков на некоторой модели системы обуславливается тем, что проверка потоков на реальной сети была бы технически значительно более сложной вследствие необходимости привлечения специализированного оборудования, программных средств и квалифицированного персонала.

При проведении верификации в части контроля сетевых информационных потоков, недостаточно парных сравнений правил политики, а нужен анализ их срабатываний «в динамике». Так, к примеру, необходимо выявить не только правило, которое ни разу не сработает из-за некоторого одного более приоритетного правила (что относительно легко было бы сделать и без моделирования), но из-за некоторого набора правил (выявление чего без использования «проверки на модели» является значительно более сложной задачей).

По сравнению с традиционными сетевыми структурами, верификация информационных потоков со встроенными устройствами отличается наличием более разветвленной топологии сети с учетом разнообразных встроенных устройств с различными видами программно-аппаратных интерфейсов, являющимися точками входа и выхода информационных потоков, а также изменчивость таких систем – узлов, топологии, типов коммуникаций, сетевых протоколов на всем протяжении работы системы.

Проверка корректности информационных потоков осуществляется путем последовательного перебора правил политики в порядке уменьшения их приоритета до факта первого срабатывания. Использование приоритетов правил позволяет организовать более гибкое управление взаимосвязанными правилами политики с возможностью задания правил по умолчанию.

Выделяется один из наиболее важных типов аномалий, на выявление которых направлена верификация, – аномалия «затемнения». Наличие такой аномалии предполагает, что правило никогда не срабатывает из-за того, что имеется одно или несколько правил, его «перекрывающих». Аномалия свидетельствует об ошибке в политике, которую необходимо пересмотреть.

Для верификации правил политик в части проверки корректности сетевых информационных потоков применяется метод «проверки на модели» [4, 7] с использованием инструмента SPIN и языка спецификации PROMELA.

Информационные потоки и правила политики специфицируются на основе следующих кортежей:

$$\texttt{InformationFlow} = \langle \texttt{host}_1, \texttt{host}_2, \texttt{user}_1, \texttt{user}_2, \texttt{interface}_1, \texttt{interface}_2, \texttt{type} \rangle,$$

$$\texttt{FilteringRule} = \langle \texttt{host}_1, \texttt{host}_2, \texttt{user}_1, \texttt{user}_2, \texttt{interface}_1, \texttt{interface}_2, \texttt{type}, \texttt{action} \rangle,$$

где host1, host2 – хосты отправителя и получателя соответственно; user1, user2 –пользователь-отправитель и пользователь-получатель; interface1, interface2 – виды аппаратных интерфейсов отправителя и получателя; type – тип информационного потока.

Под типом информационного потока понимается тип данных, которые он содержит. Типы потоков различаются, как в соответствии с разновидностью передаваемой информации (например, пользовательские данные, критически важные данные, контрольные суммы, ключи шифрования, сертификат защиты и др.), так и в соответствии с формой, в которой информация представлена (например, незашифрованное и зашифрованное сообщения, сжатое сообщение).

Применение метода «проверки на модели» заключается в переборе состояний, в которые может перейти система в зависимости от появляющихся информационных потоков и ответов модуля, принимающего решения о разрешении или отклонении таких запросов на основе политик. При этом последовательность действий при переборе зависит от условий, которые сформулированы на языке линейной темпоральной логики и выражают корректные состояния системы [9, 10]. Состояние системы определяется набором значений переменных, а изменение состояния вызывается выполняющимися в ней параллельными процессами.

Процесс, который должен выполняться в очередной момент времени, выбирается случайным образом. Система верификации рассматривает все возможные последовательности шагов для заданных процессов и выдает сообщения о потенциально некорректном состоянии. После этого в качестве результата верификации выдается «трасса», то есть последовательность шагов, ведущая к некорректному состоянию системы относительно заданных условий. Входными данными методики верификации сетевых информационных потоков являются специфицированные правила политики контроля сетевых информационных потоков и структура сети, содержащей встроенные устройства, а также ожидаемые виды аномалий (рис. 1).

Входные данные, включающие в себя описание политики, компьютерной системы и аномалий, преобразуются во внутренний формат

системы верификации. Затем строится обобщенная модель процесса верификации правил фильтрации, представленная в виде конечного автомата. Эта модель инициализируется входными данными во внутреннем формате. Аномалии в модели выражены формальными утверждениями. Для метода «проверки на модели» эти формальные утверждения будут являться свойствами корректности, нарушение которых приводит исследуемую систему в некорректное состояние. На финальном этапе обобщенная модель для верификации правил фильтрации верифицируется специальными программными средствами, реализующими метод «проверки на модели». В процессе верификации выявляются все некорректные состояния системы. На завершающем этапе полученные результаты верификации интерпретируются. Если были обнаружены аномалии, то создается описание, содержащее данные об информационном потоке, приводящем к возникновению аномалии, а также тип аномалии [5, 10].

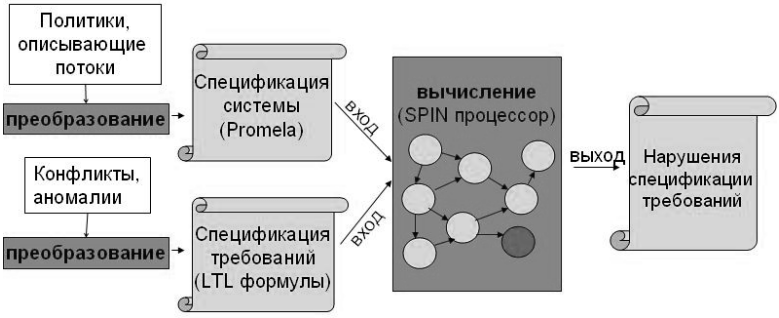

Рис. 1. Представление процесса верификации.

3. Методика верификации. Предложенная в работе методика верификации информационных потоков включает следующие основные стадии:

- формирование некоторого множества тестовых потоков (потоки формируются на основе граничных значений правил политики как всевозможные комбинации их параметров);
- применение правил политики последовательно к каждому информационному потоку; при этом при каждом срабатывании использованное правило помечается как «сработавшее хотя бы раз»;
- осуществление поиска на множестве правил для выявления правил, которые не сработали ни разу.

Методика верификации в качестве результата выдает множество пар $< A, (B_1,...B_n) >$, где A – аномальное правило, $B_1,...B_n$ – правила, которые его «затеняют». При этом $B_1,...B_n$ являются правилами с более высоким приоритетом и определяются дополнительной прогонкой всех используемых потоков, которые удовлетворяют условиям правила A через все вышестоящие.

Методика верификации была осуществлена на практике с целью проверки корректности политики безопасности системы автоматизированного контроля расхода электроэнергии потребителями компании Mixed-Mode (Германия). Вследствие технических упрощений ограничением осуществленной методики является задание параметров правил политики лишь на основе задания либо определенных значений правил (конкретных хостов, интерфейсов, пользователей), либо с использованием группы специальных идентификаторов any, обозначающих все возможные значения определенного параметра. В общем случае методика предполагает задание заранее не фиксированных множеств параметров и любых их подмножеств (в частности использование конструкций вида «все возможные значения за исключением a_1, a_2, a_3»).

Правила верифицированной политики были сформированы, исходя из имеющихся спецификаций рассматриваемой информационно-телекоммуникационной системы. В политику искусственно был введен ряд экземпляров аномалий «затенения», имитирующих типовые ошибки в процессе ее разработки. При этом методика позволила выявить каждую из внесенных аномалий. На основе результатов методики первоначальная политика была скорректирована, после чего методика была применена снова, и новая политика была признана свободной от аномалий.

Рассмотрим фрагмент использованного описания требований политики безопасности в части контроля сетевых информационных потоков для системы автоматизированного контроля расхода электроэнергии потребителями: *не конфиденциальные данные генерируются доверенным устройством измерения и сохраняются временно на нем. Эти данные отображаются на локальном дисплее устройства; любому пользователю разрешено считывать не конфиденциальные данные с использованием исключительно локального интерфейса устройства измерения*. На рис. 2 приведен фрагмент политики безопасности, на котором задано два правила политики на языке PROMELA, специфицирующих данное требование и представляющих аномалию «затенения» (правило 0 представлено на строках 82 – 92 и правило 1 – на

строках 94 – 104). В соответствии с расположением правил, правило с номером 0 имеет больший приоритет по сравнению с правилом с номером 1. Аномалия возникает в результате ошибочного указания значений интерфейсов устройства-источника потока (*interface1*).

```
82      rule0.user1 = any_user;
83      rule0.user2 = any_user;
84      rule0.interface1 = any_interface;
85      rule0.interface2 = any_interface;
86      rule0.host1 = TM;
87      rule0.host2 = any_host;
88      rule0.type = Privacy_non_relevant_data;
89      rule0.action = allow;
90      rule0.isHeld = false;
91      rule0.id = 0;
92      storage.policyRules!rule0;
93
94      rule1.user1 = any_user;
95      rule1.user2 = any_user;
96      rule1.interface1 = local_interface;
97      rule1.interface2 = any_interface;
98      rule1.host1 = TM;
99      rule1.host2 = any_host;
100     rule1.type = Privacy_non_relevant_data;
101     rule1.action = deny;
102     rule1.isHeld = false;
103     rule1.id = 1;
104     storage.policyRules!rule1;
```

Рис. 2. Пример правил, содержащих аномалию «затенения».

На рис. 3 показано окно, выдающее «трассу» применяемого средства SPIN. В частности, показано, что правило с номером 1 отмечено как аномальное.

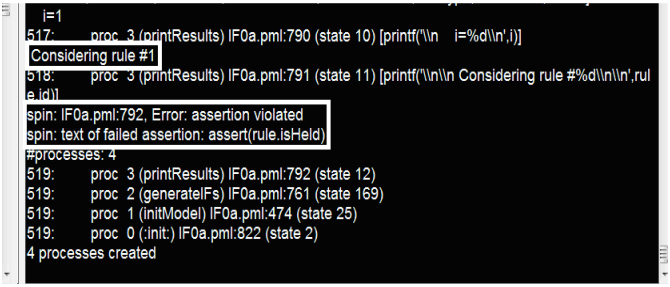

Рис. 3. Результаты выполнения методики
с использованием средства SPIN.

Осуществление методики верификации информационных потоков, предложенной в данной работе, позволяет повысить уровень за-

щищенности как отдельных встроенных устройств, так и систем, содержащих встроенные устройства. В отличие от существующих подходов, предложенная методика позволяет получить комплексную оценку безопасности системы с точки зрения информационных потоков.

4. Заключение. Предложенная методика предоставляется разработчикам как некоторый шаблон для написания программ на языке PROMELA. Входные данные методики задаются непосредственно в тексте программы на основе конструкций языка. Верификация выполняется в режиме командной строки и извлечение результатов связано с анализом выдаваемых «трасс» процесса выполнения.

В дальнейшем планируется расширение множества учитываемых видов аномалий, разработка графического интерфейса пользователя, при помощи которого разработчик сможет задавать в удобном виде все необходимые входные данные, сохранять и редактировать их, а также автоматического генератора отчетов в удобном пользователю формате на основе таблиц, структурированных документов.

Литература

1. *Десницкий В.А., Котенко И.В.* Проектирование защищенных встроенных устройств на основе конфигурирования // Проблемы информационной безопасности. Компьютерные системы, № 1, 2013, С 44–54.
2. *Десницкий В.А., Чечулин А.А.* Модели процесса построения безопасных встроенных систем // Системы высокой доступности, № 2, 2011. С. 97-101.
3. *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.
4. *Полубелова О.В., Котенко И.В.* Методика верификации правил фильтрации методом “проверки на модели” // Проблемы информационной безопасности. Компьютерные системы, № 1, 2013, С. 151–168.
5. *Чечулин А.А., Котенко И.В., Десницкий В.А.* Анализ информационных потоков для построения защищенных систем со встроенными устройствами // Системы высокой доступности, 2012, № 2, С. 116–122.
6. *Agaskar A., He T., Tong L.* Distributed Detection of Multi-hop Information Flows with Fusion Capacity Constraints // Signal Processing, IEEE Transactions on, vol. 58, no. 6: IEEE, 2010, P. 3373–3383.
7. *Baier C., Katoen J.-P.* Principles of Model Checking // The MIT Press, 2008, P. 984.
8. *Braghin C., Sharygina N., Barone-Adesi K.* A model checking-based approach for security policy verification of mobile systems // Formal Aspects of Computing Journal, 2011. P. 627–648.
9. *Chechulin A., Kotenko I., Desnitsky V.* A Combined Approach for Network Information Flow Analysis for Systems of Embedded Components // Lecture Notes in Computer Science, Springer-Verlag, Vol. 7531. The Sixth International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-2012). October 17-19, 2012, St. Petersburg, Russia. P.146-155.

10. *Desnitsky V., Kotenko I., Chechulin A.* Configuration-based approach to embedded device security // Lecture Notes in Computer Science, Springer-Verlag, Vol. 7531. P. 270-285.
11. *Hedin D., Sabelfeld A.* A Perspective on Information-Flow Control // Proceedings of summer school Control Tools for Analysis and Verification of Software Safety and Security, Marktoberdorf, Germany. IOS Press, 2011.
12. *Pistoia M., Chandra S., Fink S., Yahav E.* A Survey Of Static Analysis Methods For Identifying Security Vulnerabilities In Software Systems // IBM Systems Journal, 2007. P. 265-288.
13. *Rae A., Fidge C.* Identifying Critical Components during Information Security Evaluations // Journal of Research and Practice in Information Technology, 2005. P. 391–402.
14. *Ruiz J. F., Desnitsky V., Harjani R., Manna A., Kotenko I., Chechulin A.* A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components // 20th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP 2012). Garching/Munich. February 2012, P. 261–268.
15. *Sprintson A., El Rouayheb S., Georghiades C.* A New Construction Method for Networks from Matroids // In Proceedings of the 2009 IEEE international conference on Symposium on Information Theory (ISIT'09), 2009.

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.

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 09.09.2013.

РЕФЕРАТ

Десницкий В.А. **Методика верификации сетевых информационных потоков в информационно-телекоммуникационных системах со встроенными устройствами.**

Ограничения на аппаратные ресурсы встроенных устройств обуславливают сложность использования традиционных средств защиты, в том числе криптографических алгоритмов, которые применяются для защиты персональных компьютеров, серверов и сетевых структур. Поэтому решение вопросов защиты систем со встроенными устройствами требует специализированных подходов к разработке механизмов защиты, которые могли бы обеспечить должный уровень защищенности не только путем использования дополнительных средств защиты, но и за счет особенностей архитектуры системы. Анализ информационной системы со встроенными устройствами на различных этапах процесса проектирования, как один из путей достижения этой цели, позволяет избежать архитектурных недоработок и ошибок, которые, в свою очередь, снижают уровень безопасности системы.

Методика верификации сетевых информационных потоков является основным результатом работы. Цель методики – оценка уровня защищенности разрабатываемой системы со встроенными устройствами, проверка корректности политики безопасности этой системы и определение уровня соответствия информационных потоков в реальной системе заданным политикам.

Используется метод «проверки на модели» для верификации правил политики безопасности, задающих сетевые информационные потоки с использованием инструмента верификации SPIN. Данный тип верификации относится к методам «статического» анализа системы, и ее проведение на начальных этапах проектирования обеспечивает раннее выявление противоречий в рамках политики безопасности, а также несоответствий топологии сети информационной системы. В отличие от «динамического» анализа, который включает тестирование готовых устройств на основе тестовых векторов атак, предлагаемый подход к верификации позволяет сократить количество и объем действий, которые необходимо провести повторно после исправления обнаруженных ошибок проектирования.

Рассматривается один тип аномалий, на выявление которых направлена верификация, аномалия «затемнения». Наличие данной аномалии предполагает, что правило никогда не срабатывает из-за того, что имеется одно или несколько правил, его «перекрывающих». Аномалия свидетельствует о вероятной ошибке в политике, и ее необходимо пересмотреть.

Преимущество методики – возможность гарантировать безопасность системы при условии совпадения поведения модели и реальной системы. К недостаткам методики можно отнести: большой объем вычислительных ресурсов, используемых при анализе сложных моделей; «ложные срабатывания», то есть предупреждения о нарушениях потоков, которых в реальной системе не будет; неполноту, так как проверяется не реальная система, а ее модель.

SUMMARY

Desnitsky V.A. **A technique for verification of network information flows in information and telecommunication systems with embedded devices.**

Hardware resource constraints on embedded devices lead to complexity of application of traditional protection means including cryptographic algorithms used to provide security of personal computers, servers and network architectures. Hence to solve issues of protection of information and telecommunication systems with embedded devices requires specific approaches to design of security mechanisms providing the proper security level of the system not only through extra protection means, but at the expense of architecture peculiarities of the system. As a way to achieve this goal an analysis of information system with embedded devices at various design stages allows avoiding architectural defects and errors lessening security level of the system.

A verification technique for checking network information flows represents an important result of the work. The goal of the technique is to evaluate the security level of the developed system with embedded devices, check correctness of the security policy and determine the level of accordance of information flows of the real system to the assigned policies.

In order to verify security policy rules describing information flows model checking approach was applied by the use of a software tool SPIN. Such verification relates to the methods of static system analysis. Its implementation at initial stages of the system design provides earlier revelation of contradictions within the security policy as well as inconsistencies of the information system topology. In contrast to dynamic analysis, which comprises testing implemented devices on the basis of testing attack vectors the proposed verification approach allows lessening the amounts of actions to be conducted repeatedly after correction of detected design errors.

We regarded one anomaly type, shadowing anomaly, which the verification is targeted to. A presence of this anomaly supposes the rule is never held due to a fact that there is one of a number of other rules overriding it. The anomaly witnesses a probable error in the policy, therefore it should be subject to a revision.

The advantage of the proposed verification is the possibility to guarantee security of the system under the condition of met behavior of the model with to the physical system. The shortcoming is a great volume of computational resources involved in analysis of complex models, false positive alarms (i.e. warnings about potential information flows that will not be in the real system) and incompleteness, since a model (not the real system) is checked.