ПРОЦЕСС ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ СО ВСТРОЕННЫМИ УСТРОЙСТВАМИ

Десницкий В.А.

Лаборатория проблем компьютерной безопасности,
СПИИРАН,
Санкт-Петербург, Россия

РусКрипто'2013, 29 марта 2013 г.

Содержание

- Проектирование защищенных систем со встроенными устройствами
- Актуальные работы в предметной области
- Верификация политик безопасности информационных потоков
- Программный прототип

Введение

- Проектирование защищенных информационных систем со встроенными устройствами
  - Разработка и уточнение стадий процесса проектирования в рамках «компонентного подхода» к проектированию
- Специфика встроенных устройств:
  - Существенные ограничения на ресурсы устройств => слабая производительность
  - Устройства узкоспециализированного назначения => специфичные виды угроз
  - Мобильность и автономность устройств, меняющееся окружение, разнообразие программно-аппаратных интерфейсов => специфичные множества атак

Процесс проектирования защищенных систем со встроенными устройствами

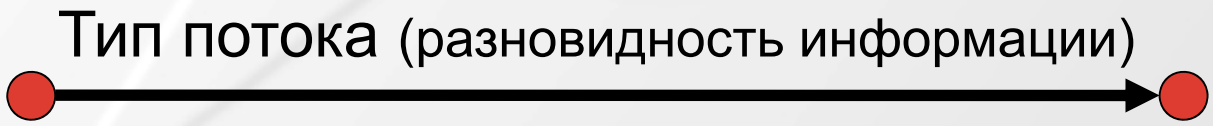
- Тенденции к комплексному комбинированному проектированию защиты систем со встроенными устройствами
  - Комплекс методик и инструментов для проектирования, композиции, верификации, тестирования, оценки систем и отдельных устройств в части защиты устройств и предоставляемых ими сервисов
  - Повышение уровня автоматизации процесса проектирования
- Примеры существующих и разрабатываемых методик проектирования:
  - Конфигурирование защиты (композиция компонентов защиты на основе оптимизации ресурсопотребления)
  - Доменно-специфичное проектирование защиты (DSM & CSM-модели) и шаблоны защиты (security patterns)
  - Статическое тестирование с использованием моделей нарушителя (аналитическое моделирование)
  - Анализ несовместимостей компонентов защиты
  - **Верификация корректности информационных потоков системы**

Актуальные работы

- Ключевые проблемы проектирования встроенных устройств:
  - *Myagmar S., Lee A.J., Yurcik W. Threat Modeling as a Basis for Security Requirements // Symposium on Requirements Engineering for Information Security, 2005*
  - *Rae A.J., Wildman L.P. A Taxonomy of Attacks on Secure Devices // Australian Information Warfare and IT Security, 20–21 November 2003, Australia, pp. 251–264, 2003.*
  - *Kommerling O., Kuhn M.G. Design principles for tamper-resistant smartcard processors // Proceedings of the USENIX Workshop on Smartcard Technology, pp. 9–20, Chicago, May 10–11, 1999.*
- Модели проектирования систем со встроенными устройствами:
  - *Rein A., Rudolph C., Ruiz J.F. Building Secure Systems Using a Security Engineering Process and Security Building Blocks // Zertifizierung und modellgetriebene Entwicklung sicherer Software (ZeMoSS-Workshop), 2013, http://subs.emis.de/LNI/Proceedings/Proceedings198.html*
  - *Eby M., Werner J., Karsai G., Ledeczi A. Integrating Security Modeling into Embedded System Design // Engineering of Computer-Based Systems, pp. 221-228, 2007*
  - *Nadjm-Tehrani S., Vasilevskaya M. Towards a Security Domain Model for Embedded Systems // 13th IEEE International High Assurance Systems Engineering Symposium, IEEE, 2011.*
  - *Mana A., Ruiz J.F. A Security Modelling Framework for Systems of Embedded Components // 13th IEEE International High Assurance Systems Engineering Symposium, IEEE, 2011*
  - *Rudolph C. Security Engineering and Modelling of Set-top Boxes // RISE'12, Workshop on Redefining and Integrating Security Engineering at ASE/IEEE International Conference on Cyber Security 12, IEEE, 2012*

Верификация политики безопасности информационных потоков (ИП) системы

- Использование SPIN (http://spinroot.com) – «проверка на модели» (Model Checking) для выявления конфликтов и несоответствий в политике безопасности
- Определение потоков и модели системы на языке PROMELA (PROcess MEta Language)



- User-source
- Node-source
- Interface-source

- User-target
- Node-target
- Interface-target

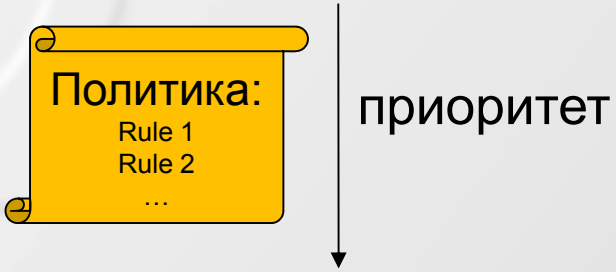
aFlow := (Us, Ns, Is, Ut, Nt, It, T)

Модель системы

- Модель содержит описания
  - Сетевых сущностей
    - Устройства и аппаратные интерфейсы
  - Топологии системы
    - Связей между сущностями
  - Ролей
    - Пользователей и групп пользователей
  - Целей защиты
    - Требования и предположения (политика безопасности)

Представление политики

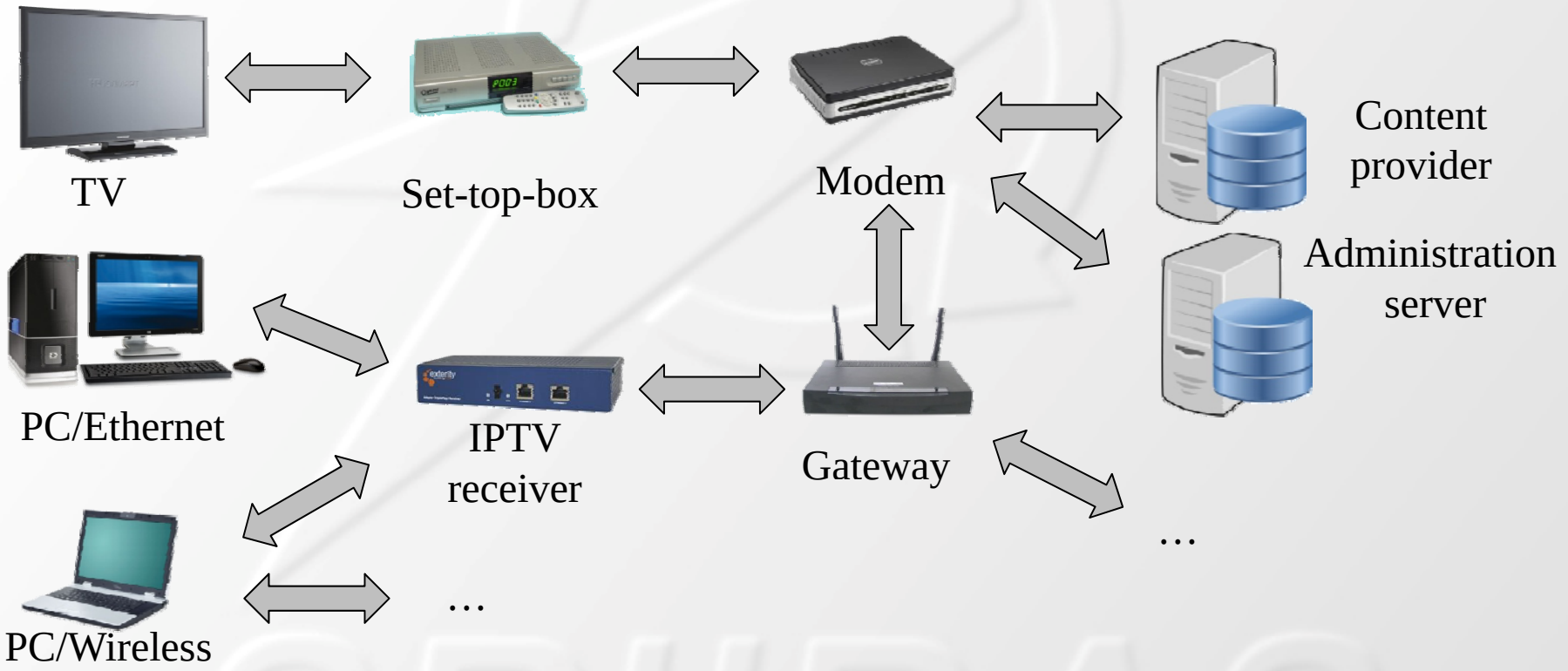
- Использование приоритетов
  - Для каждого потока лишь одно правило срабатывает



- Параметры правил:
  - фиксированные значения,
  - any-значения
  - Задание групп значений

Rule1 := (flow1, allow/deny)
Rule2 := (flow2, deny/allow)

Применение для контроля ИП в телекоммуникационных системах (1/2)



Применение для контроля ИП в телекоммуникационных системах (2/2)

Модель системы:

- Users:
  - customer, operator, technician, etc.
- Nodes:
  - TV device, customer PC, set-top-box, gateway, content provider, etc.
- Interfaces:
  - wire, wireless, Ethernet, Wi-Fi, etc.
- Types of flows:
  - paid content, free content, control and authentication data, encrypted data, DRM protected data, etc. *(the ones may intersect)*

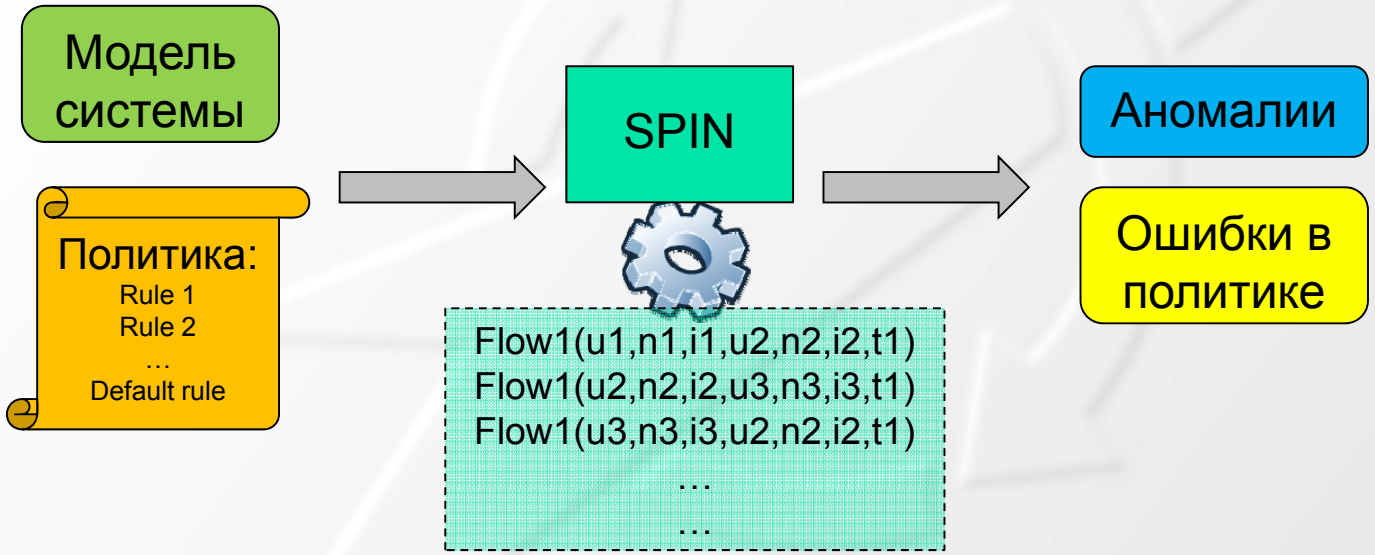
Пример потока:

flow1 := (customer, customer PC, Wi-Fi, any, Administration server, any, authentication data)

Пример правила политики:

(flow1, allow)

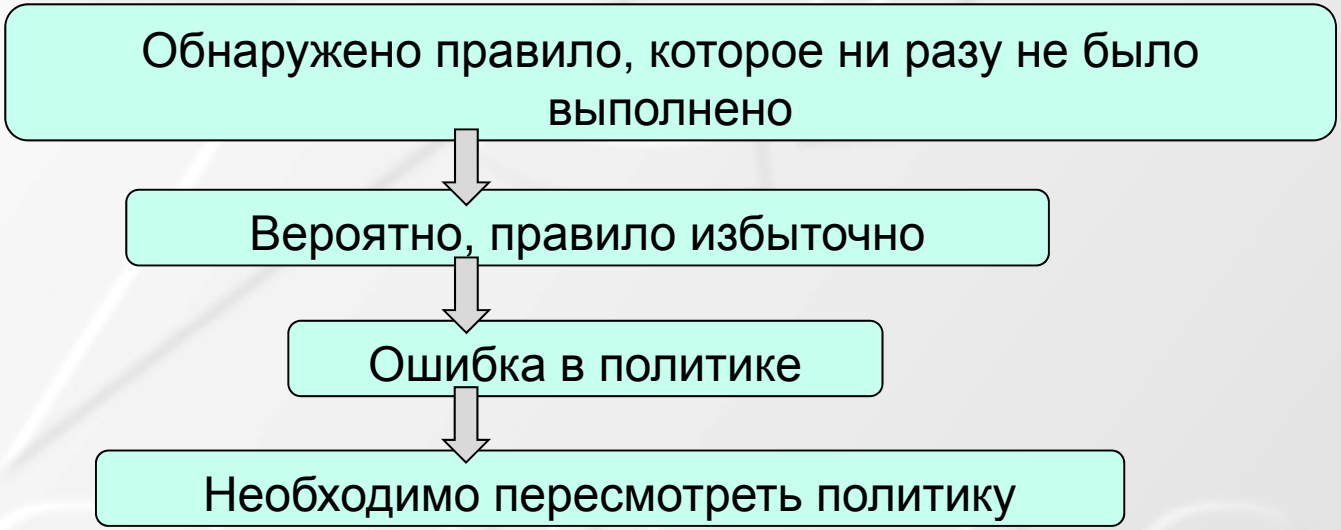
Верификация на основе SPIN



- SPIN моделирует большое число потоков между хостами сети (вплоть до 100 000 и более)
  - Выявление противоречивых/избыточных правил политики
  - Проверка выполнимости правил политики
  - Тестирование корректности политики на заранее подготовленных контрольных примерах

Пример аномалии

Исходя из полноты множества моделируемых потоков при верификации правил:



Преимущества

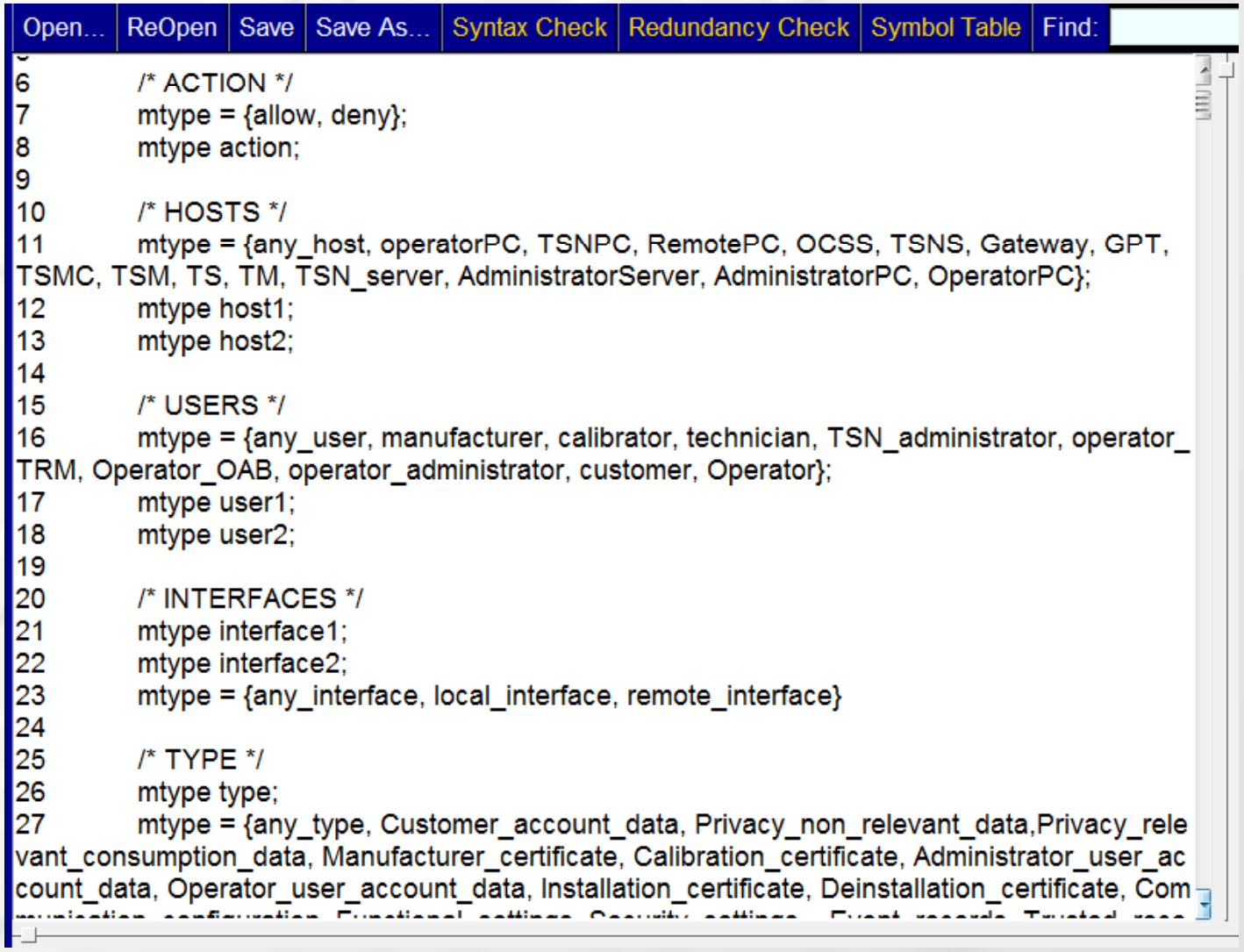
- Автоматизированная методика верификации политики безопасности информационных потоков
- Применима на различных стадиях процесса проектирования (*vs. динамическое тестирование устройств и системы на основе тестовых векторов*)
  - Технически более простое => позволяет ускорить процесс разработки
  - Позволяет перенести часть тестирования на более ранние стадии процесса разработки => позволяет сократить количество итераций процесса
- Для полноценного анализа политики не достаточно парного сравнения правил – нужен анализ срабатываний правил «в динамике» => применяется «Model Checking»

Программный прототип (1/4)

- Система: автоматизированной системы контроля расхода электроэнергии потребителями *(компания Mixed-Mode, Германия, www.mixed-mode.de)*
- Цель: поиск избыточных правил политики управления ИП для
- Текущие ограничения проведенной методики:
  - Один тип конфликтов «затемнение»
  - Без учета топологии системы
- Ограничения прототипа:
  - Задание входных данных в терминах языка PROMELA
  - Результаты верификации – последовательности «логов»

Программный прототип (2/4)

Описание моделируемой системы:



Программный прототип (3/4)

Определение правил:

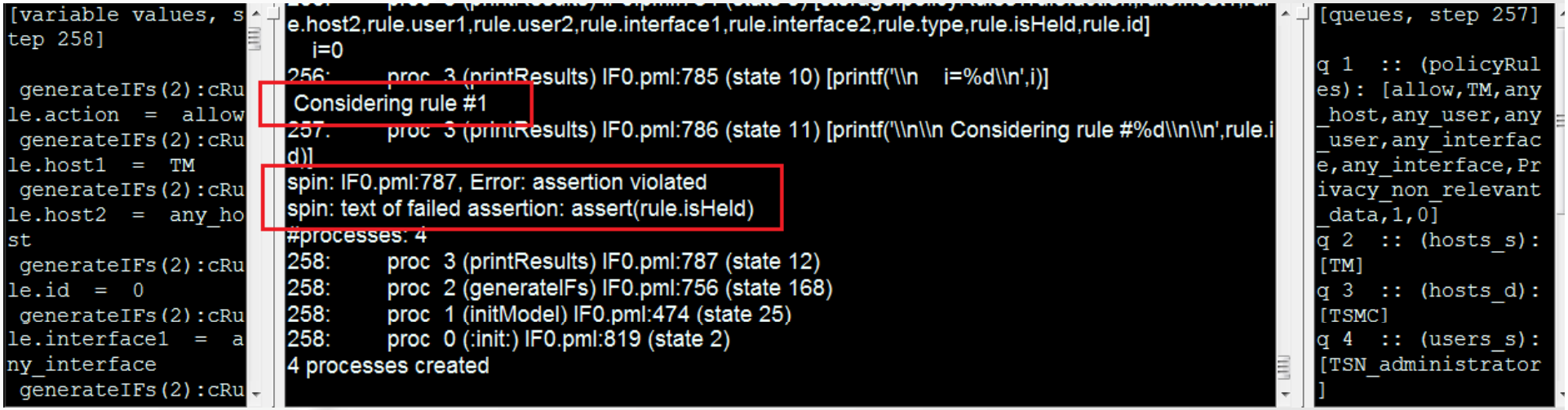
Open... | ReOpen | Save | Save As... | Syntax Check | Redundancy Check | Symbol Table | Find:

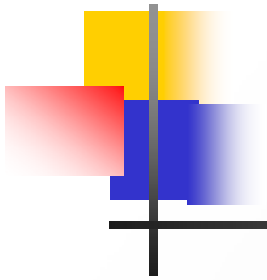
```
nformation which can be read from existing electromechanical meters and it is not considered to
be privacy relevant. */
81
82          rule0.user1 = any_user;
83          rule0.user2 = any_user;
84          rule0.interface1 = any_interface;
85          rule0.interface2 = any_interface;
86          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;//Privacy_relevant_consumption_data;
101         rule1.action = deny;
102         rule1.isHeld = false;
103         rule1.id = 1;
104         storage.policyRules!rule1;
```

```
Spin Version 6.2.2 -- 6 June 2012
iSpin Version 1.1.0 -- 7 June 2012
TclTk Version 8.5/8.5
1 E:/Work/SecFutur/doc/Information flows/IF0.pml:1
```

Программный прототип (4/4)

Результаты верификации:





Заключение

- Дальнейшая работа:
  - Уточнение списков типовых конфликтов правил политики контроля информационных потоков
- Совершенствование прототипа:
  - Введение в модель топологии системы
  - Реализация «front-end» и GUI
  - Реализация генератора отчетов

Контактная информация

Десницкий Василий Алексеевич (СПИИРАН)

desnitsky@comsec.spb.ru

http://comsec.spb.ru/Desnitsky

Благодарности

Работа выполняется при финансовой поддержке РФФИ, программы фундаментальных исследований ОНИТ РАН (проект 2.2) и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

ВОПРОСЫ?