

ADV_SPM — Формальные модели политики безопасности на практике



Хорошилов Алексей Владимирович
khoroshilov@ispras.ru



Институт системного программирования РАН

ГОСТ Р 15408-3-2013 Критерии оценки безопасности ИТ

Задание по безопасности

ASE_INT

Введение ЗБ

ASE_CCL

Утверждение о соответствии

ASE_SPD

Определение проблемы безопасности

ASE_OBJ

Цели безопасности

ASE_ECD

Определение расширенных компонентов

ASE_REQ

Требования безопасности

ASE_TSS

Краткая спецификация ОО

Оценка уязвимостей

AVA_VAN

Анализ уязвимостей

Разработка

ADV_SPM

Моделирование политики безопасности

ADV_FSP

Функциональная спецификация

ADV_TDS

Проект ОО

ADV_IMP

Представление реализации

ADV_ARC

Архитектура безопасности

ADV_INT

Внутренняя структура

Тестирование

ATE_COV

Покрытие

ATE_DPT

Глубина

Поддержка жизненного цикла

ALC_CMC

Возможности УК

ALC_CMS

Область УК

ALC_DEL

Поставка

ALC_DVS

Безопасность разработки

ALC_FLR

Устранение недостатков

ALC_LCD

Определение ЖЦ

ALC_TAT

Инструменты и методы

ATE_FUN

Функциональное тестирование

ATE_IND

Независимое тестирование

Композиция

ACO_COR

Обоснование композиции

ACO_DEV

Свидетельство разработки

ACO_REL

Зависимости компонентов

ACO_CTT

Тестирование составного ОО

ACO_VUL

Анализ уязвимостей композиции

Руководства

AGD_OPE

Руководство по эксплуатации

AGD_PRE

Подготовительные процедуры

ADV_SPM - Моделирование политики безопасности

ASE

Задание по безопасности

Описание ОО,
его компонентов и среды

Проблема безопасности

Угрозы

Политики
безопасности
организации

Предположения

Цели безопасности

Цели
безопасности
ОО

Цели
безопасности
среды

Требования безопасности

Требования
доверия

Функциональные
требования

ADV

Разработка

Функциональная
спецификация

Архитектура
безопасности

Описание проекта

Внутренняя
структура

Реализация

ADV_SPM - Моделирование политики безопасности

ASE

Задание по безопасности

Описание ОО,
его компонентов и среды

Проблема безопасности

Угрозы

Политики
безопасности
организации

Предположения

Цели безопасности

Цели
безопасности
ОО

Цели
безопасности
среды

Требования безопасности

Требования
доверия

Функциональные
требования

ADV

Разработка

Модель ПБ

Функциональная
спецификация

Архитектура
безопасности

Описание проекта

Внутренняя
структура

Реализация

ADV_SPM - Моделирование политики безопасности

ASE

Задание по безопасности

Описание ОО,
его компонентов и среды

Проблема безопасности

Угрозы

Политики
безопасности
организации

Предположения

Цели безопасности

Цели
безопасности
ОО

Цели
безопасности
среды

Требования безопасности

Требования
доверия

Функциональные
требования

11.5.4 ADV_SPM.1 Формальная модель политики безопасности ОО

Зависимости: ADV_FSP.4 Полная функциональная спецификация

11.5.4.1 Элементы действий разработчика

11.5.4.1.1 ADV_SPM.1.1D

Разработчик должен представить формальную модель ПБО для [назначение: *список формально моделируемых политик*].

11.5.4.1.2 ADV_SPM.1.2D

Для каждой политики, охваченной формальной моделью ПБО, в модели должны быть отражены значимые фрагменты изложения ФТБ, которые составляют данную политику.

11.5.4.1.3 ADV_SPM.1.3D

Разработчик должен представить формальное доказательство соответствия между какой-либо формальной функциональной спецификацией и моделью ПБО.

11.5.4.1.4 ADV_SPM.1.4D

Разработчик должен продемонстрировать соответствие между функциональной спецификацией и моделью ПБО.

11.5.4.2 Элементы содержания и представления свидетелей

11.5.4.2.1 ADV_SPM.1.1C

Модель ПБО должна быть изложена в формальном стиле с предоставлением вспомогательного пояснительного текста согласно требованиям и в ней должны быть идентифицированы моделируемые политики ФБО.

11.5.4.2.2 ADV_SPM.1.2C

Для всех моделируемых политик в модели ПБО должно быть определено понятие «безопасность» для данного ОО и должно быть представлено формальное доказательство того, что ОО не может перейти в небезопасное состояние.

ADV

Разработка

Модель ПБ

Функциональная
спецификация

Архитектура
безопасности

Описание проекта

Внутренняя
структура

Реализация

ADV_SPM - Моделирование политики безопасности

ASE

Задание по безопасности

Описание ОО,
его компонентов и среды

Проблема безопасности

Угрозы

Политики
безопасности
организации

Предположения

Цели безопасности

Цели
безопасности
ОО

Цели
безопасности
среды

Требования безопасности

Требования
доверия

Функциональные
требования

ADV

Разработка

Модель ПБ

Функциональная
спецификация

Архитектура
безопасности

Описание проекта

Внутренняя
структура

Реализация

Цели моделирования ПБ

- повышение доверия за счёт
 - наличия формальной модели политики безопасности, снижающей риски
 - неправильного понимания требований
 - неверной реализации требований
 - установления соответствия между функциональной спецификацией и этой моделью

Формальная верификация

- доказательство отсутствия внутренних противоречий в модели ПБ
- доказательство недостижимости "небезопасных" состояний
- доказательство соответствия между формальной функциональной спецификацией и моделью ПБ

Формальная верификация

- **доказательство отсутствия внутренних противоречий в модели ПБ**
- **доказательство недостижимости "небезопасных" состояний**
- **доказательство соответствия между формальной функциональной спецификацией и моделью ПБ**

Язык спецификаций Event-B

- средства формализации модели
 - состояние
 - события
 - инварианты
- система доказательства корректности моделей
 - автоматическое доказательство
 - интерактивное доказательство

Пример: FRU_PRS – Приоритет обслуживания

15.2 Приоритет обслуживания (FRU_PRS)

15.2.1 Характеристика семейства

Требования семейства FRU_PRS позволяют ФБО управлять использованием находящихся под контролем ФБО ресурсов пользователями и субъектами так, что высокоприоритетные операции под контролем ФБО всегда будут выполняться без препятствий или задержек со стороны операций с более низким приоритетом.

15.2.2 Ранжирование компонентов

FRU_PRS.1 «Ограниченный приоритет обслуживания» предоставляет приоритеты для использования субъектами подмножества ресурсов под контролем ФБО.

FRU_PRS.2 «Полный приоритет обслуживания» предоставляет приоритеты для использования субъектами всех ресурсов под контролем ФБО.

15.2.3 Управление: FRU_PRS.1, FRU_PRS.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) назначение приоритетов каждому субъекту в ФБО.

15.2.4 Аудит: FRU_PRS.1, FRU_PRS.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) Минимальный: отклонение операции на основании использования приоритета при распределении ресурса.

б) Базовый: все попытки использования функции распределения ресурсов с учетом приоритетности обслуживания.

15.2.5 FRU_PRS.1 Ограниченный приоритет обслуживания

Иерархический для: Нет подчиненных компонентов.

Зависимости: отсутствуют

15.2.5.1 FRU_PRS.1.1

ФБО должны установить приоритет каждому субъекту в ФБО.

15.2.5.2 FRU_PRS.1.2

ФБО должны обеспечить доступ к [назначение: *управляемые ресурсы*] на основе приоритетов, назначенных субъектам.

15.2.6 FRU_PRS.2 Полный приоритет обслуживания

Иерархический для: FRU_PRS.1 Ограниченный приоритет обслуживания

Зависимости: отсутствуют.

15.2.6.1 FRU_PRS.2.1

ФБО должны установить приоритет каждому субъекту в ФБО.

15.2.6.2 FRU_PRS.2.2

ФБО должны обеспечить доступ ко **всем совместно используемым ресурсам** на основе приоритетов, назначенных субъектам.

Event-B: Состояние

- Переменные
- Инварианты как определение типа

MACHINE

MO >

SEES

- CO

VARIABLES

- S >Субъекты
- SP >Функция приоритетов субъектов
- O >Объекты
- R >Текущие "доступы"
- Q >Очередь

INVARIANTS

- inv1: $S \subseteq \mathbb{N}$ not theorem >
- inv2: $SP \in S \rightarrow P$ not theorem >
- inv3: $O \subseteq \mathbb{N}$ not theorem >
- inv4: $R \in S \leftrightarrow O$ not theorem >
- inv5: $Q \in S \leftrightarrow O$ not theorem >

Event-B: Операции

```
◦ access:  
  ANY  
    ◦ S >  
    ◦ O >  
  WHERE  
    ◦ grd1:  $s \in S$   
    ◦ grd2:  $o \in O$   
    ◦ grd3:  $\forall x \cdot x \in S \wedge x \mapsto o \in R \Rightarrow SP(s) > SP(x)$   
    ◦ grd4:  $\forall x \cdot x \in S \wedge x \mapsto o \in Q \Rightarrow SP(s) \geq SP(x)$   
  THEN  
    ◦ act1:  $R := \{x \mapsto y \mid (x \mapsto y \in R \wedge y \neq o) \vee (x = s \wedge y = o)\}$  >  
    ◦ act2:  $Q := \{x \mapsto y \mid (x \mapsto y \in Q \wedge (x \neq s \vee y \neq o)) \vee (x \mapsto y \in R \wedge y = o)\}$  >  
  END
```

```
◦ free:  
  ANY  
    ◦ S >  
    ◦ O >  
  WHERE  
    ◦ grd1:  $s \in S$   
    ◦ grd2:  $o \in O$   
    ◦ grd3:  $s \mapsto o \in R$   
  THEN  
    ◦ act1:  $R := R \setminus \{s \mapsto o\}$  >  
  END
```

Event-B: Инварианты

MACHINE

M0 >

SEES

- C0

VARIABLES

- S >Субъекты
- SP >Функция приоритетов субъектов
- O >Объекты
- R >Текущие "доступы"
- Q >Очередь

INVARIANTS

- inv1: $S \subseteq \mathbb{N}$ not theorem >
- inv2: $SP \in S \rightarrow P$ not theorem >
- inv3: $O \subseteq \mathbb{N}$ not theorem >
- inv4: $R \in S \leftrightarrow O$ not theorem >
- inv5: $Q \in S \leftrightarrow O$ not theorem >
- inv6: $\forall s, o. s \in S \wedge o \in O \wedge s \mapsto o \in R \Rightarrow s \mapsto o \notin Q$ not theorem >
- inv7: $\forall s, o. s \in S \wedge o \in O \wedge s \mapsto o \in Q \Rightarrow s \mapsto o \notin R$ not theorem >
- inv8: $\forall s1, s2, o. s1 \in S \wedge s2 \in S \wedge s1 \neq s2 \wedge o \in O \wedge s1 \mapsto o \in R \Rightarrow s2 \mapsto o \notin R$ not theorem >
- inv9: $\forall sr, sq, o. sr \in S \wedge sq \in S \wedge o \in O \wedge sr \mapsto o \in R \wedge sq \mapsto o \in Q \Rightarrow SP(sr) \geq SP(sq)$ not theorem >

Интерактивное доказательство

access/inv9/INV Имя сгенерированного утверждения

☐ $\forall sr, sq, o \cdot$
 $sr \in S \wedge sq \in S \wedge o \in O \wedge$
 $sr \mapsto o \in R \wedge sq \mapsto o \in Q$
 $\Rightarrow$
 $SP(sr) \geq SP(sq)$

☐ $s \in S$

☐ $o \in O$

☐ $\forall x \cdot$
 $x \in S \wedge x \mapsto o \in R$
 $\Rightarrow$
 $SP(s) > SP(x)$

☐ $\forall x \cdot$
 $x \in S \wedge x \mapsto o \in Q$
 $\Rightarrow$
 $SP(s) \geq SP(x)$

Набор гипотез

Selected Hypotheses

☒ Goal $\forall sr, sq, o \cdot$ **Цель доказательства**
 $sr \in S \wedge sq \in S \wedge o \in O \wedge$
 $sr \mapsto o \in \{x, y \cdot (x \mapsto y \in R \wedge y \neq o) \vee (x = s \wedge y = o) \mid x \mapsto y\} \wedge$
 $sq \mapsto o \in \{x, y \cdot (x \mapsto y \in Q \wedge (x \neq s \vee y \neq o)) \vee (x \mapsto y \in R \wedge y = o) \mid x \mapsto y\}$
 $\Rightarrow$
 $SP(sr) \geq SP(sq)$

Proof Control Statistics Rodin Problems Инструменты автоматического доказательства

Окно ввода команд доказательства

Event-B Explorer

Дерево сгенерированных утверждений

- change_priority/grd3/WD
- change_priority/inv2/INV
- change_priority/inv4/INV
- change_priority/inv5/INV
- change_priority/inv6/INV
- change_priority/inv7/INV
- change_priority/inv8/INV
- change_priority/inv9/INV
- change_priority/act2/WD
- change_priority/act3/WD
- unsuccessful_access/grd3/WD
- unsuccessful_access/inv5/INV
- unsuccessful_access/inv6/INV
- unsuccessful_access/inv7/INV
- unsuccessful_access/inv9/INV
- access/grd3/WD
- access/grd4/WD
- access/inv4/INV
- access/inv5/INV
- access/inv6/INV
- access/inv7/INV
- access/inv8/INV
- access/inv9/INV

Symbols Cache Hypothesis

МРОСЛ-ДП модель

- Констант: 34
- Аксиом: 30
- Переменных состояния: 60
- Инвариантов: 248
- Событий: 75
- Число уровней уточнения: 4
- Размер: 4393 строк
- Утверждений для доказательства: 2962



Формальная верификация

- доказательство отсутствия внутренних противоречий в модели ПБ
- доказательство недостижимости "небезопасных" состояний
- **доказательство соответствия между формальной функциональной спецификацией и моделью ПБ**

ADV_SPM - Моделирование политики безопасности

ASE

Задание по безопасности

Описание ОО,
его компонентов и среды

Проблема безопасности

Угрозы

Политики
безопасности
организации

Предположения

Цели безопасности

Цели
безопасности
ОО

Цели
безопасности
среды

Требования безопасности

Требования
доверия

Функциональные
требования

ADV

Разработка

Модель ПБ

Функциональная
спецификация

Архитектура
безопасности

Описание проекта

Внутренняя
структура

Реализация

Формальная функциональная спецификация

- Только статические свойства интерфейса ОО
 - формальное соответствие модели ПБ малополезно
- Поведенческая спецификация ОО как чёрного ящика
 - формальное соответствие показывает, что ФТБ корректно перенесены на уровень интерфейса
 - практика для небольших систем

Выводы

- Моделирование ПБ работает
 - как инструмент верификации функциональных требований
 - как инструмент верификации проектных решений, отражённых в требованиях
- Формальное доказательство соответствия поведенческой функциональной спецификации может быть значительно более трудоёмко
- ⇒ имеет практический смысл разделение ADV_SPM на два элемента

Спасибо!



Хорошилов Алексей Владимирович
khoroshilov@ispras.ru



Институт системного программирования РАН