Каннер Андрей
kanner@okbsapr.ru
LFCE

Подход к верификации подсистемы управления доступом ОС Linux

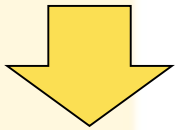
2020

Требования к разработке моделей безопасности КС

- Требования по БИ, устанавливающие уровни доверия к средствам ТЗИ и средствам обеспечения безопасности ИТ
- ГОСТ Р ИСО/МЭК 15408-3-2013. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ
- ГОСТ Р (проект) Защита информации. Формальное моделирование политики безопасности. Часть 1. Формальная модель управления доступом

Требования к разрабатываемой модели безопасности средств управления доступом

- в модели должны быть отражены реализуемые политики управления доступом и фильтрации информационных потоков
- должно быть подтверждено соответствие модели заявленным требованиям



Необходимо проводить **верификацию** с применением специальных **инструментальных средств**

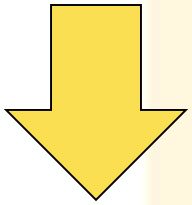
Верификация с использованием темпоральной логики Лэмпорта и метода Model Checking

Позволяет:

- в рамках формальной нотации на языке TLA+ описать:
  - ✓ все необходимые сущности и операции системы
  - ✓ свойства безопасности, необходимые для проверки во всех ее состояниях
- верифицировать **в автоматическом режиме** системы, заданные в виде конечных автоматов

Ограничения верификации

Метод Model Checking не осуществляет полноценную формальную верификацию системы



В TLA+ нотации модели безопасности введены **модельные значения** для некоторых сущностей системы - количества:

- пользователей
- субъектов
- объектов

IDs

Множества идентификаторв

$$UserIDs \triangleq 0 \,..\, 2$$

$$SubjectIDs \triangleq 0 \,..\, 2$$

$$ObjectIDs \triangleq 0 \,..\, 4$$

Переменные модели безопасности в нотации TLA+

Сущности:

- изменяются при выполнении операций
- их изменение влечет изменение состояния системы

A – множество произошедших доступов

O – множество объектов

S – множество субъектов

U – множество уч. записей пользователей

$$\text{VARIABLES } A,\ O,\ S,\ U$$

Переменные модели

$$vars \triangleq \langle A,\ O,\ S,\ U \rangle$$

Переменные модели безопасности в нотации TLA+

- в множество произошедших доступов можно добавить новый **элемент-кортеж**:
  - ✓ доступ субъекта с *s.sid*
  - ✓ к объекту с *o.oid*
  - ✓ по методу доступа *r* из множества *Accesses*

$$Accesses \triangleq \{\text{“read”}, \text{“write”}, \text{“list\_files”}, \text{“append”}, \text{“lookup”}, \text{“rename\_obj”}, \text{“rename\_cont”}, \text{“ucreate”}, \text{“udelete”}, \text{“change\_user\_perm”}, \text{“change\_ext\_attr”}, \text{“change\_cl”}, \text{“screate”}, \text{“sdelete”}, \text{“delete\_object”}, \text{“create\_object”}\}$$

$$A' = A \cup \{\langle s.sid,\ o.oid,\ r\rangle\}$$

- изменение переменных должно описываться в операциях (чтение, запись, дозапись, поиск объекта и т.д.)

Операции модели безопасности в нотации TLA+

- описываются в виде предикатов пред- и постусловий выполнения операции

Read

Операция чтения

$$Read(s,\ o) \triangleq$$
$$\land\ A' = A \cup \{\langle s.sid,\ o.oid,\ \text{“read”}\rangle\}$$
$$\land\ \text{UNCHANGED}\ \langle S,\ O,\ U\rangle$$

$$ReadD \triangleq$$
$$\exists\, s \in S :$$
$$\exists\, o \in O :$$

Проверка прав

$$\land\ \lor\ IsUserAdmin(s)$$

DAC

$$\lor\ \land\ DAC\_may\_do(s,\ o,\ \text{“read”})$$

MAC

$$\land\ MAC\_may\_read(s,\ o)$$

Lookup

$$\land\ \langle s.sid,\ o.oid,\ \text{“lookup”}\rangle \in A$$

Постусловия

$$\land\ Read(s,\ o)$$

Предикаты модели безопасности в нотации TLA+

Предикаты проверки дискреционного управления доступом

$$IsUserAdmin(s) \triangleq$$
$$\land SelectUser(s.uid).is\_admin = \text{TRUE}$$

$a \in Permissions$

$$DAC\_may\_do(s,\ o,\ a) \triangleq$$

$$\land\ \exists r \in SelectUser(s.uid).acls :$$
$$\land r[1] = o.oid$$
$$\land a \in r[2]$$

Предикаты проверки мандатного управления доступом

$$MAC\_may\_read(s,\ o) \triangleq$$
$$\lor o.cl \leq s.cl$$
$$\lor \text{“ccnr”} \in o.ext\_attr$$

Начальное состояние системы в нотации TLA+

$Init$

Инициализация

$$Init \triangleq \begin{array}{l} \land A = \{\} \\ \land S = \{s0,\ s1\} \\ \land O = \{o0,\ o1,\ o2\} \\ \land U = \{u0,\ u1\} \end{array}$$

- *u0* – администратор с max УК
- *u1* – модельный пользователь с min УК
- *s0* и *s1* – субъекты-процессы *u0 и u1*
- *o0* – корневой каталог файловой системы
- *o1* – вложенный контейнер
- *o2* – файл контейнера

Свойства безопасности в нотации TLA+

- представляются в виде инвариантов или темпоральных свойств
- инварианты описываются как предикаты, истинность которых проверяется в каждом возможном состоянии системы

Пример инварианта в нотации TLA+

MACSafety

Инвариант безопасности мандатного управления доступом для иерархии объектов в контейнере

$$
\begin{aligned}
&MACSafety \triangleq \\
&\quad \forall\, o \in O : \\
&\quad\quad \lor \land o.type \in Containers \\
&\quad\quad\quad \land \forall\, ch \in SelectAllChilds(o) : \\
&\quad\quad\quad\quad \land \lor ch.cl \leq o.cl \\
&\quad\quad\quad\quad\quad \lor \text{“ccnr”} \in o.ext\_attr \\
&\quad\quad \lor \neg o.type \in Containers
\end{aligned}
$$

IntegrityInv

Инвариант динамического контроля целостности

$$
\begin{aligned}
&IntegrityInv \triangleq \forall\, e \in SelectExecutables : \\
&(SubjectIDs \times \{e.oid\} \times \{\text{“write”}, \text{“append”}\}) \cap A = \{\}
\end{aligned}
$$

Спецификация модели безопасности в нотации TLA+

Spec

спецификация модели

$$Spec \triangleq Init \wedge \Box[Next]_{vars}$$

Invariants

Теорема, учитывающая все инварианты

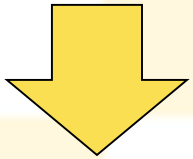
(доказывается в процессе верификации)

$$\begin{aligned} \text{THEOREM } Spec \Rightarrow \; & \wedge \Box TypeInv \\ & \wedge \Box OneAdminExists \\ & \wedge \Box MACSafety \\ & \wedge \Box NoCyclesInContainers \\ & \wedge \Box IntegrityInv \\ & \wedge \Box LinksSafety \end{aligned}$$

Результаты верификации модели безопасности подсистемы управления доступом «Аккорд-Х»

Использовались:

- инструментальное средство *TLC2 v2.15*
- СВТ с Intel Core i5-9400 (3.80 ГГц) и ОЗУ 16 ГБ, ОС Linux с ядром v5.4.38 (x86_64)



Затраченное время: от 12 мин. до 24 ч.

Количество проанализированных состояний: от 2 776 895

Каннер Андрей
kanner@okbsapr.ru
LFCE

Подход к верификации подсистемы управления доступом ОС Linux

Вопросы?

2020