Академия Федеральной службы охраны Российской Федерации

Спецификация модели управления доступом на языке TLA$^+$ и ее верификация

кандидат технических наук
Козачок Александр Васильевич

21 марта 2019 г.

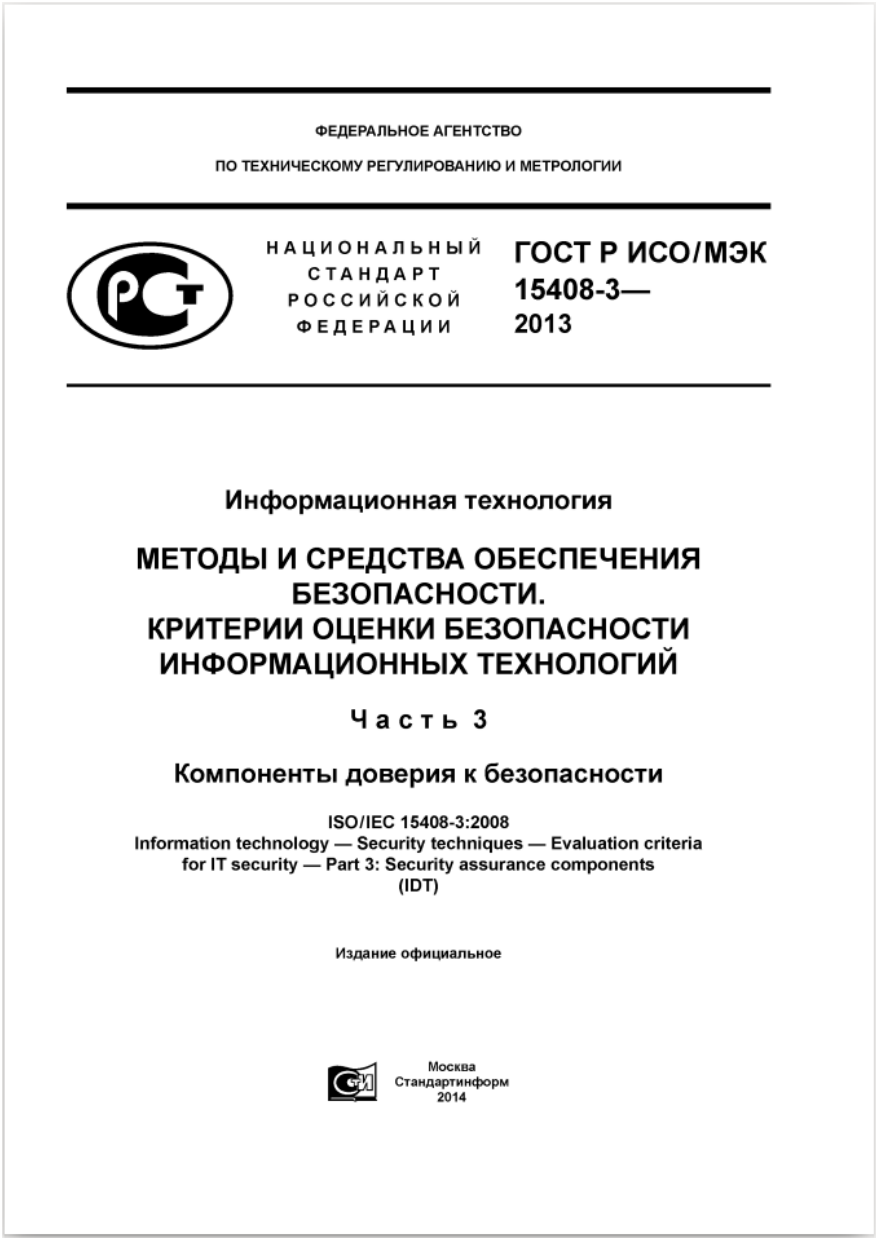
Структура доклада

1. Задача формального представления моделей управления доступом
2. Темпоральная логика действий Лэмпорта TLA$^+$
3. Спецификация модели управления доступом к электронным документам на TLA$^+$ [3]

Структура доклада

1. Задача формального представления моделей управления доступом
2. Темпоральная логика действий Лэмпорта TLA$^+$
3. Спецификация модели управления доступом к электронным документам на TLA$^+$ [3]

Актуальность задачи формального представления моделей управления доступом



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-3— 2013

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.
КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 3

Компоненты доверия к безопасности

ISO/IEC 15408-3:2008
Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components (IDT)

Издание официальное

Москва
Стандартинформ
2014

- ADV_SPM.1 "**Формальная** модель политики безопасности"
- Оценочный уровень доверия 5, предусматривает **полуформальное** проектирование и тестирование
- Оценочный уровень доверия 6, предусматривает **полуформальную верификацию** и тестирование проекта
- Оценочный уровень доверия 7, предусматривает **формальную верификацию** проекта и тестирование [1]

Структура доклада

Темпоральная логика действий Лэмпорта TLA$^+$ I

Темпоральные операторы логики Лэмпорта:

- $\Box$ – оператор "всегда в будущем";
- $\blacksquare$ – оператор "всегда в прошлом";
- $\bigcirc$ – оператор "в следующий момент времени";
- $\ominus$ – оператор "в предыдущий момент времени";
- $\Diamond$ – оператор "однажды в будущем";
- $\blacklozenge$ – оператор "однажды в прошлом";
- $\mathcal{U}$ – бинарный оператор "до тех пор пока";
- $\mathcal{S}$ – бинарный оператор "с тех пор как".

Формулы в темпоральной логике Лэмпорта

Логические формулы в рамках предлагаемой модели управления доступа задаются следующим образом (в форме Бэкуса-Наура):

$$\begin{aligned} \langle \phi \rangle \quad \models \quad & PredAction \mid p(t_1, \ldots, t_n) \mid \neg\phi \\ & \mid \phi \vee \phi \mid \phi \wedge \phi \mid \phi \rightarrow \phi \mid \forall x : \phi \\ & \mid \exists x : \phi \mid \Box\phi \mid \Diamond\phi \mid \bigcirc\phi \mid \phi\mathcal{U}\phi \\ & \mid \blacksquare\phi \mid \blacklozenge\phi \mid \ominus\phi \mid \phi\mathcal{S}\phi, \end{aligned} \tag{1}$$

где $PredAction$ – действия, p – предикат, $t_1, \ldots, t_n$ – термы, x – переменная.

Темпоральная логика действий Лэмпорта TLA$^+$ II

Соотношения между операторами TLA$^+$

$$\Diamond F \equiv \neg\Box\neg F \qquad \blacklozenge F \equiv \neg\blacksquare\neg F$$

$$\Diamond F \equiv (F \vee \neg F)\mathcal{U}F \qquad \blacklozenge F \equiv F\mathcal{S}(F \vee \neg F)$$

Пример спецификации на языке TLA$^+$ [2]:

MODULE *HourClock*

EXTENDS *Naturals*

VARIABLE *hr*

$$\begin{aligned} \mathit{Init} &\triangleq \mathit{hr} \in (1 \,..\, 12) \\ \mathit{Next} &\triangleq \mathit{hr}' = \text{IF } \mathit{hr} \neq 12 \text{ THEN } \mathit{hr} + 1 \text{ ELSE } 1 \\ \mathit{Spec} &\triangleq \mathit{Init} \wedge \Box[\mathit{Next}]_{\mathit{hr}} \end{aligned} \tag{2}$$

THEOREM $\mathit{Spec} \Rightarrow \Box\mathit{Init}$

Структура доклада

1 Задача формального представления моделей управления доступом

2 Темпоральная логика действий Лэмпорта TLA$^+$

3 Спецификация модели управления доступом к электронным документам на TLA$^+$ [3]

Спецификация модели на TLA$^+$ I

Общая спецификация и предикаты действий модели

Спецификация модели управления доступом на языке TLA+:

$$Spec \triangleq Init \wedge \Box[Next]_{vars}, \tag{3}$$

$Init$ – процедура инициализация переменных модели,
$Next$ – предикат действия, изменяющий состояние модели,
$vars$ – переменные модели, $\triangleq$ – символ "равно по определению".

$$\begin{aligned} Next \triangleq \quad & \vee CreateSubjectD \vee DeleteSubjectD \\ & \vee ReadD \quad \vee WriteD \\ & \vee AppendWD \quad \vee CreateObjectD \\ & \vee DeleteObjectD \quad \vee GrantRightsD \\ & \vee RemoveRightsD \vee IncludeObjectD \\ & \vee ExcludeObjectD \vee ApproveObjectD \\ & \vee ArchiveObjectD \vee CancelObjectD \\ & \vee CopyObjectD \quad \vee AssociateCopyD \end{aligned} \tag{4}$$

Спецификация модели на TLA$^+$ II

Определение переменных модели и типов данных, описывающих объекты и субъекты модели

$$\begin{aligned} &\text{VARIABLES } A,\ O,\ S, \\ &vars \triangleq \langle A,\ O,\ S \rangle, \end{aligned} \tag{5}$$

A – множество текущих (произошедших) доступов,

O – множество объектов,

S – множество субъектов.

$$\begin{aligned} Objects \triangleq [&oid : ObjectIDs,\ meta : ObjectMeta,\ body : ObjectBody, \\ &owner : SubjectIDs,\ grantm : GrantedRights, \\ &grantb : GrantedRights,\ incl : ObjectIDs, \\ &st : ObjectStates]. \end{aligned} \tag{6}$$

$$\begin{aligned} Subjects \triangleq [&sid : SubjectIDs,\ cnfl : ConfidLevels, \\ &intl : IntegrLevels,\ cat : \text{SUBSET } Categories, \\ &owner : SubjectIDs]. \end{aligned} \tag{7}$$

$$\begin{aligned} &Rights \triangleq \{\text{“read”}, \text{“write”}\}, \\ &GrantedRights \triangleq \langle sid : SubjectIDs,\ r : Rights \rangle. \end{aligned} \tag{8}$$

Спецификация модели на TLA$^+$ III

Инициализация начальных значений переменных модели

$$
\begin{array}{lcl}
s0 & \triangleq & [sid \mapsto 0,\ cnfl \mapsto 1,\ intl \mapsto 1, \\
 & & cat \mapsto \{\text{“c1”}, \text{“c2”}\},\ owner \mapsto 0], \\
s1 & \triangleq & [sid \mapsto 1,\ cnfl \mapsto 1,\ intl \mapsto 0, \\
 & & cat \mapsto \{\text{“c2”}, \text{“c3”}\},\ owner \mapsto 1], \\
o0 & \triangleq & [oid \mapsto 0, \\
 & & meta \mapsto [cnfl \mapsto 0,\ intl \mapsto 0], \\
 & & body \mapsto [cnfl \mapsto 0,\ intl \mapsto 0], \\
 & & cat \mapsto \{\text{“c1”}, \text{“c2”}\}, \\
 & & owner \mapsto 1, \\
 & & grantm \mapsto \{\langle 0, \text{“write”}\rangle, \langle 0, \text{“read”}\rangle\}, \\
 & & grantb \mapsto \{\langle 0, \text{“read”}\rangle\}, \\
 & & incl \mapsto \{\}, \\
 & & copy \mapsto \{\}, \\
 & & st \mapsto \text{“work”}], \\
Init & \triangleq & \wedge A = \{\} \\
 & & \wedge S = \{s0,\ s1\} \\
 & & \wedge O = \{o0\}.
\end{array}
\tag{9}
$$

Спецификация модели на TLA$^+$ IV

Предикат действия Read

$$
\begin{aligned}
&Read(s,\ o,\ r,\ op) \triangleq \\
&\qquad \land\ A' = A \cup \{\langle s.sid,\ o.oid,\ r,\ op\rangle\} \\
&\qquad \land\ \text{UNCHANGED}\ \langle S,\ O\rangle \\
&\\
&ReadD \triangleq \exists\, r \in Rights : \\
&\qquad \exists\, s \in S : \\
&\qquad \exists\, o \in O : \\
&\qquad \exists\, op \in ObjectParts : \\
&\qquad\qquad \land\ r = \text{“read”} \\
&\qquad\qquad \land\ o.cat \subseteq s.cat \\
&\qquad\qquad \land\ \lor\ \land\ op = \text{“meta”} \\
&\qquad\qquad\qquad\ \ \land\ s.cnfl \geq o.meta.cnfl \\
&\qquad\qquad\qquad\ \ \land\ \lor \{\langle s.sid,\ r\rangle\} \subseteq o.grantm \\
&\qquad\qquad\qquad\qquad\ \lor\ o.owner = s.sid \\
&\qquad\qquad\qquad \lor\ \land\ op = \text{“body”} \\
&\qquad\qquad\qquad\ \ \land\ s.cnfl \geq o.body.cnfl \\
&\qquad\qquad\qquad\ \ \land\ \lor \{\langle s.sid,\ r\rangle\} \subseteq o.grantb \\
&\qquad\qquad\qquad\qquad\ \lor\ o.owner = s.sid \\
&\qquad\qquad \land\ Read(s,\ o,\ r,\ op).
\end{aligned}
\tag{10}
$$

Спецификация модели на TLA$^+$ V

Предикат действия CreateSubject

$$
\begin{aligned}
&CreateSubject(sp,\ sid,\ cnf,\ int) \triangleq \\
&\quad \land S' = S \cup \{[sid \mapsto sid, \\
&\qquad\qquad intl \mapsto int, \\
&\qquad\qquad cnfl \mapsto cnf, \\
&\qquad\qquad cat \mapsto sp.cat, \\
&\qquad\qquad owner \mapsto sp.sid]\} \\
&\quad \land A' = A \cup \{\langle sp.sid,\ sid,\ \text{“screate”}\rangle\} \\
&\quad \land PrintT(\langle sp.sid,\ sid,\ \text{“screate”}\rangle) \\
&\quad \land \text{UNCHANGED } \langle O\rangle
\end{aligned}
\tag{11}
$$

$$
\begin{aligned}
&CreateSubjectD \triangleq \exists\, sp \in S : \\
&\quad \exists\, sid \in SubjectIDs : \\
&\qquad \land \forall\, ss \in S : sid \neq ss.sid \\
&\qquad \land \exists\, cnf \in ConfidLevels : \\
&\qquad\quad \exists\, int \in IntegrLevels : \\
&\qquad\quad \land sp.cnfl = cnf \\
&\qquad\quad \land sp.intl = int \\
&\qquad\quad \land CreateSubject(sp,\ sid,\ cnf,\ int)
\end{aligned}
$$

Спецификация модели на TLA$^+$ VI

Предикат действия CopyObject

$$
\begin{aligned}
CopyObject(s,\ o,\ x) \triangleq\ & \land O' = O \cup \{[oid \mapsto x, \\
& \quad meta \mapsto [cnfl \mapsto o.meta.cnfl, \\
& \quad intl \mapsto o.meta.intl], \\
& \quad body \mapsto [cnfl \mapsto o.body.cnfl, \\
& \quad intl \mapsto o.body.intl], \\
& \quad owner \mapsto s.sid, \\
& \quad grantm \mapsto o.grantm, \\
& \quad grantb \mapsto o.grantb, \\
& \quad cat \mapsto o.cat, \\
& \quad incl \mapsto o.incl, \\
& \quad st \mapsto \text{“approved”}, \\
& \quad copy \mapsto \{o.oid\}]\} \\
& \land A' = A \cup \{\langle s.sid,\ o.oid,\ \text{“copy”},\ x\rangle\} \\
& \land \text{UNCHANGED } \langle S\rangle
\end{aligned}
\tag{12}
$$

$$
\begin{aligned}
CopyObjectD \triangleq\ & \exists\, s \in S : \\
& \land O \neq \{\} \\
& \land \exists\, o \in O : \land o.owner = s.sid \\
& \qquad \land o.incl = \{\} \\
& \qquad \land o.st = \text{“approved”} \\
& \qquad \land s.cat \subseteq o.cat \\
& \qquad \land s.cnfl = o.meta.cnfl \\
& \qquad \land s.intl \geq o.meta.intl \\
& \qquad \land s.cnfl = o.body.cnfl \\
& \qquad \land s.intl \geq o.body.intl \\
& \qquad \land Cardinality(scp(o)) < 2 \\
& \qquad \land \exists\, x \in ObjectIDs : \forall\, oo \in O : \\
& \qquad\quad \land x \neq oo.oid \\
& \qquad\quad \land CopyObject(s,\ o,\ x)
\end{aligned}
$$

$$
\begin{array}{l}
ObjTypeInv \triangleq \\
\quad \land \forall\, o \in O : \land\, o.oid \in ObjectIDs \\
\qquad\qquad \land\, o.meta \in ObjectMeta \\
\qquad\qquad \land\, o.body \in ObjectBody \\
\qquad\qquad \land\, o.owner \in SubjectIDs \\
\qquad\qquad \land\, \{o.incl\} \subseteq \text{SUBSET } ObjectIDs \\
\qquad\qquad \land\, \{o.copy\} \subseteq \text{SUBSET } ObjectIDs \\
\qquad\qquad \land\, o.st \in ObjectStates \\
\qquad\qquad \land\, o.cat \in \text{SUBSET } Categories \\
TypeInv \triangleq \land\, S \subseteq Subjects \\
\qquad \land\, ObjTypeInv \\
\qquad \land \forall\, sn \in S : \text{IF } \exists\, sm \in S : \land\, sm \neq sn \\
\qquad\qquad\qquad\qquad\qquad\qquad \land\, sn.sid = sm.sid \\
\qquad\qquad\qquad \text{THEN FALSE} \\
\qquad\qquad\qquad \text{ELSE TRUE} \\
\qquad \land \forall\, on \in O : \text{IF } \exists\, om \in O : \land\, om \neq on \\
\qquad\qquad\qquad\qquad\qquad\qquad \land\, on.oid = om.oid \\
\qquad\qquad\qquad \text{THEN FALSE} \\
\qquad\qquad\qquad \text{ELSE TRUE}
\end{array}
\tag{13}
$$

Спецификация модели на TLA$^+$ VIII

Задание инвариантов модели: инвариант безопасности

$$
\begin{array}{l}
Safety \triangleq \ \wedge \forall\, o \in O : \ \wedge\ o.meta.cnfl \leq o.body.cnfl \\
\qquad\qquad\qquad\qquad\quad \wedge\ o.meta.intl = o.body.intl \\
\qquad\qquad\qquad\qquad\quad \wedge \text{IF } o.incl \neq \{\} \\
\qquad\qquad\qquad\qquad\qquad \text{THEN } \forall\, i \in o.incl : \\
\qquad\qquad\qquad\qquad\qquad\qquad \wedge \exists\, oi \in O : \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \wedge\ oi.oid \neq o.oid \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \wedge\ oi.oid = i \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \wedge\ o.grantm \subseteq oi.grantm \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \wedge\ o.grantb \subseteq oi.grantb \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \wedge\ o.st = oi.st \\
\qquad\qquad\qquad\qquad\qquad \text{ELSE } \text{TRUE} \\
\qquad\qquad\qquad\qquad\quad \wedge\ Cardinality(scs(o)) \leq 1 \\
\qquad\qquad\qquad\qquad\quad \wedge\ Cardinality(scp(o)) \leq 2 \\
\qquad\qquad\qquad\qquad\quad \wedge \exists\, s \in S : \\
\qquad\qquad\qquad\qquad\qquad \wedge\ o.owner = s.sid \\
\qquad\qquad\qquad\qquad\qquad \wedge \text{IF } o.grantm \neq \{\} \\
\qquad\qquad\qquad\qquad\qquad\qquad \text{THEN } \neg o.grantm \subseteq (\{s.sid\} \times Rights) \\
\qquad\qquad\qquad\qquad\qquad\qquad \text{ELSE } \text{TRUE} \\
\qquad\qquad\qquad\qquad\qquad \wedge \text{IF } o.grantb \neq \{\} \\
\qquad\qquad\qquad\qquad\qquad\qquad \text{THEN } \neg o.grantb \subseteq (\{s.sid\} \times Rights) \\
\qquad\qquad\qquad\qquad\qquad\qquad \text{ELSE } \text{TRUE} \\
\wedge \neg\exists\, o \in O : \ \wedge\ \vee\ o.st = \text{“archived”} \\
\qquad\qquad\qquad\qquad\qquad\qquad\quad \vee\ o.st = \text{“cancelled”} \\
\qquad\qquad\qquad\qquad\qquad\qquad \wedge\ \vee\ o.grantm \cap (SubjectIDs \times \{\text{“write”}\}) \neq \{\} \\
\qquad\qquad\qquad\qquad\qquad\qquad\quad \vee\ o.grantb \cap (SubjectIDs \times \{\text{“write”}\}) \neq \{\}
\end{array}
\tag{14}
$$

Верификация модели на TLA$^+$ методом "Model Checking"

- Верификация разработанной модели производилась с помощью инструментального средства TLC2 версии 2.13.
- Время, затраченное на верификацию, составило порядка 2835 минут (более 47 часов) на сервере с операционной системой Ubuntu 16.04, 24 ядра Intel Xeon E5-2620 v2 2,10 Ггц и 32 Гб оперативной памяти.
- Было проверено 16 284 800 554 состояний при средней производительности системы 5 743 616 состояний в минуту.

Теорема (О выполнении инвариантов для спецификации модели)

$Spec \implies \Box(TypeInv \wedge Safety)$

Библиография:

1. Моделирование и верификация политик безопасности управления доступом в операционных системах. /. — П. Н. Девянин, Д. В. Ефремов, В. В. Кулямин, А. К. Петренко, А. В. Хорошилов, И. В. Щепетков. — Институт системного программирования им. В.П. Иванникова РАН, 2018. — 181 с. — URL: http://www.ispras.ru/publications/2018/security_policy_modeling_and_verification/.
2. *Lamport Leslie*. — Specifying Systems, The TLA+ Language and Tools for Hardware and Software Engineers. — Addison-Wesley, 2002. — ISBN 0-3211-4306-X.
3. *Козачок А. В.* — Спецификация модели управления доступом к разнокатегорийным ресурсам компьютерных систем. — // Вопросы кибербезопасности. — 2018. — Т. 28, № 4. — С. 2—8.

Спасибо за внимание!

Вопросы?

конференция
РусКрипто

a.kozachok@academ.msk.rsnet.ru