конференция РусКрипто

Методика автоматизированного тестирования реализаций криптографических протоколов

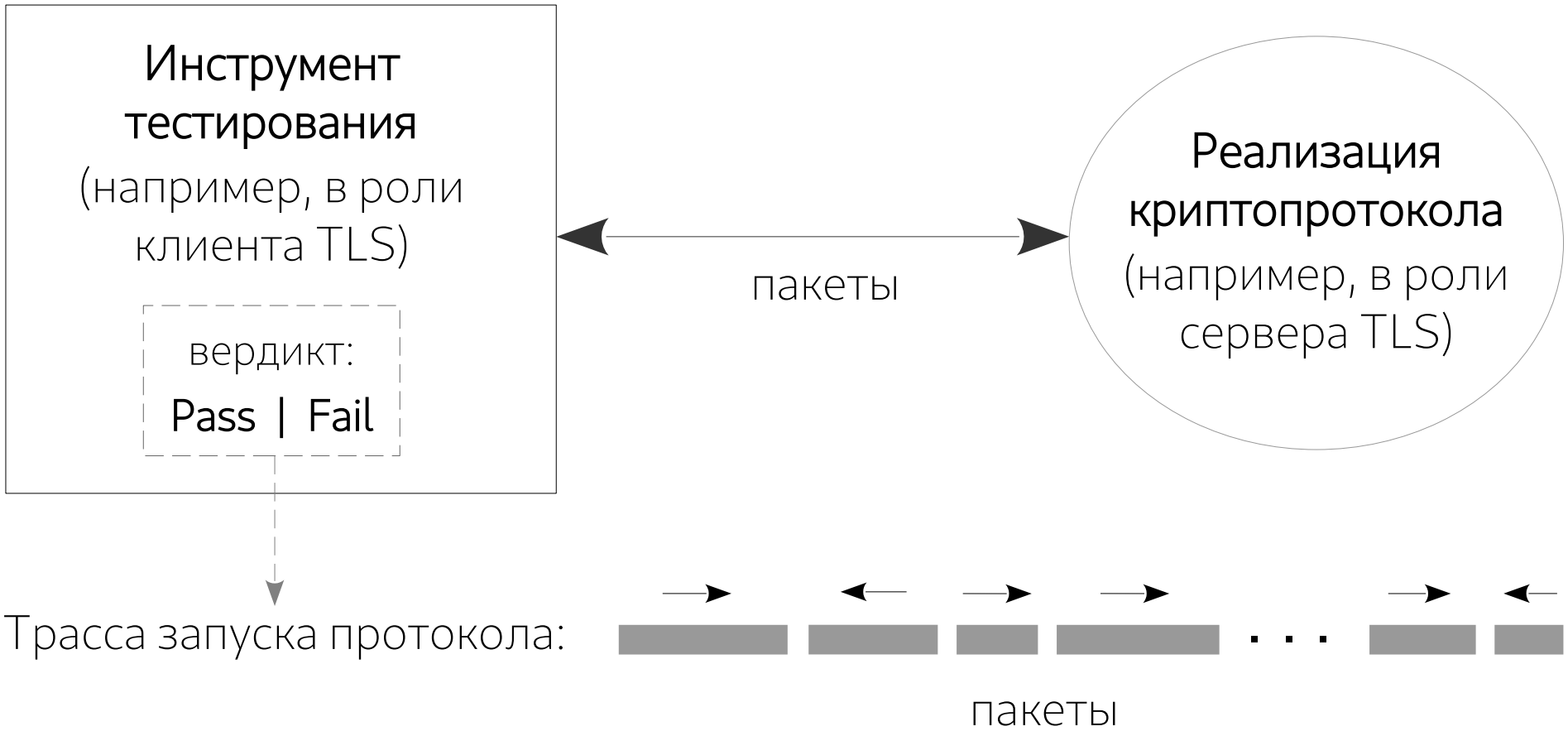
Сергей Прокопьев <s.e.pr@mail.ru>

Институт системного программирования им. В.П.Иванникова РАН

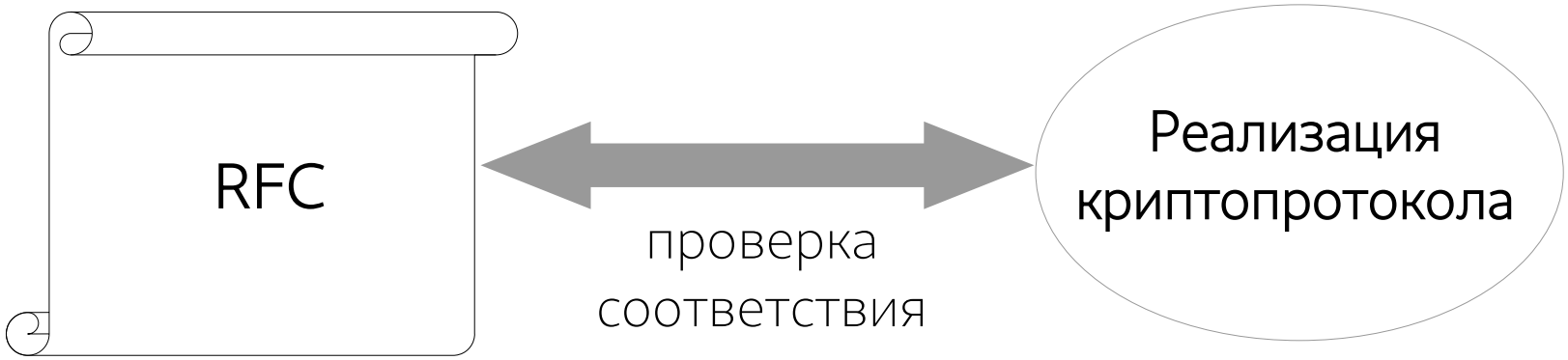
АО «НПК «Криптонит»

22-25 марта 2022 г.

Единичный тест



Цель тестирования

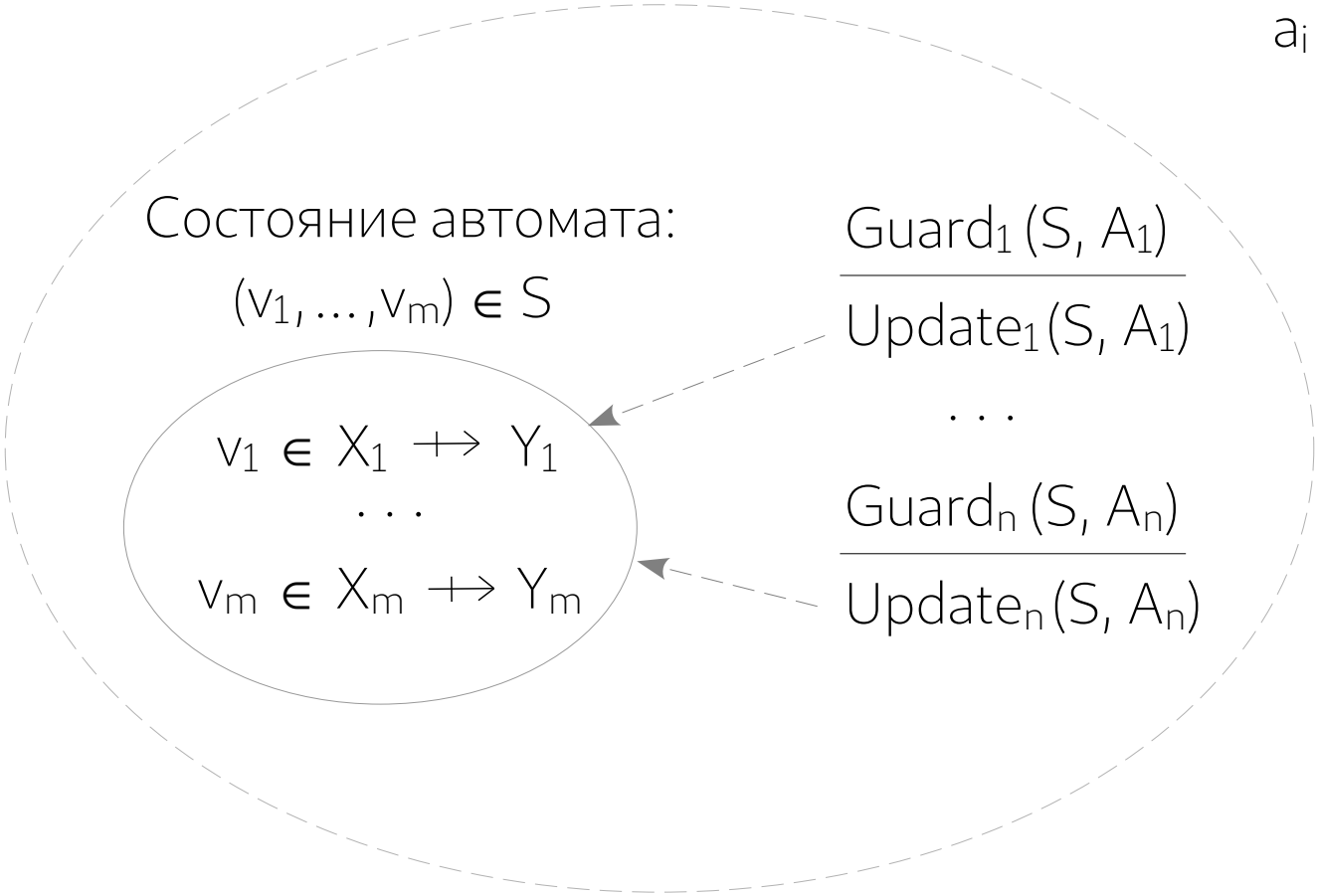


Сильная цель: гарантия встречной совместимости (interoperability) протестированных реализаций

Выразительные автоматные модели

ABZ: ASM, Alloy, B, TLA+, VDM, Z, UniTesK, NCT и др.

Guard/Update-автомат



Сообщения протокола:

$\bar{a}_i = (f_{i1}, f_{i2}, \ldots, f_{ik}) \in A_i, \; i \in 1..n$

Трасса запуска протокола: $\bar{a}_{j1}, \bar{a}_{j2}, \ldots, \bar{a}_{jl}$

Оценка качества тестовых наборов

Факторизация множества трасс автомата
через атомарные предикаты гардов

$$Guard_i(S, A_i) = \neg P_1(S, A_i) \;\&\&\; P_2(S, A_i) \;||\; (P_3(S, A_i) \Rightarrow P_4(S, A_i))$$

$$[P_1,\ P_2,\ P_3,\ P_4]$$

[True, False, False, True]

Примеры "предикатных" критериев покрытия: SC, DC, CDC, MCDC и др.

Аналог MCDC (Chilenski, Miller; 1994) для Guard/Update-автомата:

Для каждого гарда $Guard_i$ и каждого входящего в него предиката P_j :

1) есть тесты, в которых P_j обращается как в истину, так и в ложь;
2) есть тест, в котором существует состояние автомата, в котором значение $Guard_i$ существенно зависит от атомарного предиката P_j.

Методика автоматизированного тестирования на базе С2-машины

Дано:

- формальный язык спецификаций криптопротоколов;
- инструмент тестирования:
  - автоматически генерирует тестовый набор по спецификации;
  - предоставляет интерфейс подстройки алгоритма генерации тестового набора.

Методика:

Шаг 1. Разработка формальной спецификации протокола.

Шаг 2. Выбор "предикатного" критерия покрытия.

Шаг 3. Выбор конфигурации ОТ.

Шаг 4. Сокращение спецификации под конфигурацию ОТ.

Шаг 5. Настройка параметров генератора тестового набора с учетом выбранного критерия.

Шаг 6. Если целевой показатель покрытия достигнут, то возврат на Шаг 3 (выбор новой конфигурации). Иначе возврат на Шаг 5.

Характеристики методов тестирования на базе Guard/Update-автоматов

Метод тестирования	UniTESK (ИСП РАН; 1998)	NCT (K.L. McMillan, L.D. Zuck; 2019)	Тестирование на базе C2-машины (автор; 2021)
Оценка качества тестовых наборов	"Предикатные" критерии	–	"Предикатные" критерии
Автоматизация построения тестового набора из модели	Слабая	Сильная (используются SMT-решатели)	Сильная (SMT-решатели не используются)
Host-языки	Java, Python, C#	Ivy	Haskell
Сложность применения метода	Высокая	Средняя	Низкая
Примеры применения	TLS 1.2, EAP (Н.Пакулин, А.Никешин, В.Шнитман; 2014, 2018)	QUIC (транспортный слой)	TLS 1.2, TLS 1.3

Группировка пар guard/update по последовательностям

Спецификация протокола: (seqElemDef, controlDef)

"Sessions" →
"Packets" →
"TLSRecords" →
"HandshMess" → "ClientCipherSuites"
→ "ClientHelloExts" → "ClientSupportedGroups"
→ "ClientPointFormats"
→ "ClientSignatureAlgs"
→ "ClientSupportedVersions"
→ "ClientKeyShares"
→ "ServerHelloExts"
→ "CertRequestExts" → "CertRequestSigAlgs"
→ "Certificates" → "CertificateExts"

$\frac{Guard_{R1}(S)}{Update_{R1}(S)}$
. . .
$\frac{Guard_{Rn}(S)}{Update_{Rn}(S)}$
$Ready_{R}(S)$

$\frac{Guard_{HM1}(S)}{Update_{HM1}(S)}$
. . .
$\frac{Guard_{HMk}(S)}{Update_{HMk}(S)}$
$Ready_{HM}(S)$

дерево последовательностей

Структуры элементов последовательностей

$$\mathbf{seqElemDef} \in S \times SeqIndex \longrightarrow SeqElemStruc$$

состояние автомата

позиция элемента в дереве последовательностей

SeqElemStruc ::= V FieldName | Sequence SeqName | F FunID [SeqElemStruc]

Примеры возможных структур элемента последовательности "TLSRecords" :

```
F Concat
 [V "Version",
  V "RecordType",
  F LengthBE2
     [Sequence
          "HandshMess"],
  Sequence
       "HandshMess"]
```

```
F Concat
  [V "Version",
   V "RecordType",
   F LengthBE2 [...],
   F EncryptAES128
      [Sequence
           "HandshMess",
       V "Key",
       V "IV"]]
```

```
F Concat
  [V "Version",
   V "RecordType",
   F LengthBE2 [...],
   F EncryptAES128
       [V "Payload",
        V "Key",
        V "IV"]]
```

Нотация C2-машины.

Фрагмент спецификации структуры пакета протокола TLS

```
packetDef = Sequence "Records" tlsRecord
  where
  tlsRecord =
   B [Vi "ContentType"    # OfLen 1,
      Vi "LegacyVersion" # OfLen 2,
      withLen 2
       (Select (Vi "ContentType")
         [Case [0x14] changeCipherSpecMsg,
          Case [0x15] (maybeProtected alertMsg),
          Case [0x16] (maybeProtected handshakeMsgs),
          Case [0x17] protectedRecord])]

handshakeMsgs = Vi "HandshMessSequence" ##
  Sequence "HandshMess" handshMsg
  where
  handshMsg =
   B [Vi "HandshType" # OfLen 1,
      withLen 3 (Vi "HandshakeMsg" ##
        Select (Vi "HandshType")
         [Case [0x00] helloRequest,
          Case [0x01] clientHello,
          Case [0x02] serverHello,
          Case [0x04] newSessionTicket,
          Case [0x05] endOfEarlyData,
          Case [0x08] encryptedExtensions,
          Case [0x0d] certificateRequest,
          Case [0x0b] certificate,
          Case [0x0c] serverKeyExchange,
          Case [0x0f] certificateVerify,

clientHello = Vi "ClientHel
 B [C [0x03,0x03],
    helloRandom Clnt,
    withLen 1 (V2_ Clnt "Se
    withLen 2 (V2 "ClientSu
      Sequence "ClntSuites"
    withLen 1 (C [0x00]),
    withLen 2 (Sequence "Cl
  where
  clientExtension =
   B [Vi "ClientExtenID" # 
      withLen 2 (Vi "Client
        Select (Vi "ClientE
         [Case [0x00,0x00] 
          Case [0x00,0x0a] 
          Case [0x00,0x0b] 
          Case [0x00,0x0d] 
```

конференция РусКрипто

Спасибо за внимание!

Сергей Прокопьев <s.e.pr@mail.ru>

Институт системного программирования им. В.П.Иванникова РАН

АО «НПК «Криптонит»